Харьковский национальный университет радиоэлектроники

Академия наук прикладной радиоэлектроники

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

Адрес редакции:
Редакция журнала «Прикладная радиоэлектроника»
Харьковский национальный университет радиоэлектроники
просп. Ленина, 14, 61166, Харьков, Украина
Тел.: + 38 (057) 702 10 57
Факс: + 38 (057) 702 10 13
E-mail: are@kture.kharkov.ua
http://www.anpre.org.ua

СОДЕРЖАНИЕ

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Выпуск журнала «Прикладная радиоэлектроника» является тематическим и посвящен проблемным вопросам защиты информации. Представленные в журнале статьи в основном являются заказными. Они подготовлены специалистами по тематике, ориентируясь на задачи, которые решаются нашим спонсором – ПАТ «Институт информационных технологий.

Сегодня можно утверждать, что наша цивилизация стоит на рубеже создания электронного цифрового общества. В Европейском Союзе (ЕС) и в некоторой степени в Украине признано, что укрепление доверия в электронной онлайн среде является ключом к экономическому развитию. Отсутствие доверия заставляет потребителей, бизнес и руководство, при осуществлении трансграничных доверительных операций в электронном виде быть в некоторой степени неопределенности и принимать новые услуги с осторожностью. Также признано, что основополагающим принципом осуществления внутреннего рынка в ЕС должно быть отсутствие на территории государства-члена ограничений относительно предоставления доверительных услуг провайдерами доверительных услуг, расположенных в других государствах-членах ЕС.

Для Украины, на наш взгляд, очень важным является изучение и анализ возможностей использования европейского опыта с целью предоставления безопасных электронных услуг по электронной идентификации, электронной аутентификации электронной подписи, электронных печатей, электронных меток времени, электронных документов, услуг электронной доставки и проверки подлинности веб-сайта. Поэтому в первом разделе журнала представлены, на наш взгляд, методологические статьи, которые посвящены концептуальным положениям реализации доверительных услуг и безопасности облачных вычислений.

Во втором разделе журнала представлены статьи, которые посвящены теории и практике симметричных криптографических преобразований, в основном блочным симметричным шифрам, функциям хеширования и генераторам случайных последовательностей. По-прежнему актуальными являются исследования, связанные с исследованием криптографической стойкости симметричных шифров, функций хеширования и генераторов случайных последовательностей. На наш взгляд, серия статей в этом направлении позволяет получить уточненные оценки свойств симметричных шифров, функций хеширования и генераторов случайных последовательностей в части создания первоначальной неопределенности.

Серия статей третьего раздела посвящена асимметричным криптопреобразованиям. Прежде всего рассматриваются асимметричные преобразования в фактор-кольцах, которые получили название «преобразования в кольцах срезанных полиномов». Относительно этих преобразований важными есть задачи доказательства их стойкости, учитывая аппарат алгебраических решеток. Приводится фундаментальное решение задачи оптимизации процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Применение предложенного подхода открывает принципиально новую область возможностей для комплексного решения проблемы повышения стойкости защиты информации.

Серия из трех статей: «Параметры криптосистемы на кривой Эдвардса над расширениями малых простых полей», «Деление точки на два для кривой Эдвардса над простым полем» и «Криптостойкие кривые Эдвардса над простыми полями» написаны их авторами под руководством профессора А.В. Бессалова. Также мы считаем возможным публикацию статьи, автор М.В. Есина, которая посвящена анализу сложности преобразований на эллиптических кривых в различных базисах. Важными являются исследования, которые посвящены атакам специального вида и методам защиты от этих атак. Они представлены в статьях авторов Д.С. Балагуры и Д.В. Иваненко.

В четвертом разделе представлены статьи, которые можно отнести к сфере информационной безопасности. Так, в статье авторов В.В. Котенко, С.В. Котенко, К.Е. Румянцева и Горбенко Ю.И. приводится фундаментальное обоснование стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей.

В статье А.Н. Алексейчука и А.Ю. Грязнухина представлено решение задачи восстановления систематического линейного кода набора искаженных кодовых слов, наблюдаемых на выходе двоичного симметричного канала связи. Получены оценки сложности решения систем уравнений. В статье И.В. Олешко представлены предложения по совершенствованию протокола нулевых знаний. В статье А.А. Кузнецова, С.И. Приходько, Билал Хамзе представлены результаты исследования линейных блоковых кодов в частотной области. В статье А.А. Смирнова представлен алгебраический подход к формированию больших ансамблей дискретных сигналов с многоуровневой функцией корреляции, который основан на сечении циклических орбит групповых кодов. В статье В.А. Краснобаева, М.А. Маврина и А.А. Замулы, предложен метод повышения достоверности контроля данных, представленных в классе вычетов. В статье С.В. Николаенко представлен способ усиления безопасности пинг-понг протокола с парами перепутанных кубитов. Статья В.И. Заболотного и Е.В. Задорожной посвящена обоснованию способов защиты информации от конкурентной разведки с учетом возможности применения средств технических разведок. Исследования Т.А. Гриненко и А.П. Нарежного представлены работами по обоснованию необходимости применения кодов аутентификации сообщений (MAC) для обеспечения целостности и достоверности корректирующей информации в системе GPS/ГЛОНАСС. В статье А.В. Леншина предлагается комплексный метод проектирования и верификации комплексов средств защиты информации от несанкционированного доступа. Анализируется подход к созданию и использованию шаблонов для алгоритмов реализации услуг безопасности в формальной нотации Паронджанова.

Ректор ХНУРЭ,
член-корреспондент НАНУ,
профессор

М.Ф. Бондаренко

Заведующий кафедрой
БИТ ХНУРЭ, профессор

И.Д. Горбенко

МЕТОДОЛОГИЯ СОЗДАНИЯ И РАЗВИТИЯ ЭЛЕКТРОННОГО ЦИФРОВОГО МИРА И БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

УДК 681.3. 06 (07)

ПРОБЛЕМИ ТА ВИМОГИ ДО НАДАННЯ ДОВІРЧИХ ПОСЛУГ В ЄВРОПЕЙСЬКОМУ СОЮЗІ В ПЕРІОД 2015–2030 РР.

Ю. І. ГОРБЕНКО

Визначаються та наводяться результати аналізу основних проблемних питань та вимог, які викладені в пропозиціях проекту «Регламент Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку» ЄС, розглядаються у вигляді пропозицій та рекомендацій можливості використання певних чи усіх його положень відносно вимог в Україні.

Ключові слова: транскордонні електронні онлайн-послуги, безпечні електронні послуги щодо електронного підпису, електронної печатки, електронних документів, послуг електронної доставки та перевірки справжності веб-сайту.

ВСТУП

У 2006–2011 рр. було визнано [1], що в Європейському Союзі (ЄС) не існує всебічних транскордонних та міжрегіональних нормативно-правових та системно-технічних основ для здійснення безпечних, надійних і простих електронних операцій, включаючи електронну ідентифікацію, електронну автентифікацію та деякою мірою електронні цифрові підписи. Водночас стало зрозумілим, що зміцнення довіри в онлайн-середовищі є ключем до економічного розвитку [1] ЄС. У своєму Соціальному звіті 2010 року Комісія ЄС також наголосила на необхідності вирішення основних проблем, які заважають європейським громадянам користуватися перевагами єдиного цифрового ринку і транскордонних цифрових послуг [2]. Європейська Рада закликала Комісію створити єдиний цифровий ринок до 2015 р., щоб домогтися швидкого прогресу у ключових областях цифрової економіки та розвивати повністю інтегрований єдиний цифровий ринок шляхом полегшення транскордонного використання онлайн-послуг, особливу увагу приділяючи полегшенню безпечної електронної ідентифікації і автентифікації [3, 4]. Також Європейська Рада закликала Комісію зробити свій внесок у єдиний цифровий ринок шляхом створення умов для взаємного визнання ключових компонентів без кордонів, таких як електронна ідентифікація, електронні документи, електронні підписи та електронні послуги доставки, а також для сумісності послуг електронного Уряду на території Європейського Союзу. Європейський парламент підкреслив важливість забезпечення безпеки електронних послуг, особливо електронних підписів, а також необхідність створення інфраструктури відкритих ключів на загальноєвропейському рівні, і закликав Комісію створити європейські органи перевірки для забезпечення транскордонної сумісності електронних підписів і для підвищення безпеки операцій, що здійснюється з використанням Інтернету. Важливим є прийняття Директиви 2006/123/ЄС Європейського парламенту та Ради від 12 грудня 2006 року про послуги на внутрішньому ринку [5], в якій він закликав держави-члени до створення «точок єдиного контакту» (PSC), щоб гарантувати, що всі процедури і формальності, пов'язані з доступом до послуг та їх здійсненням, можуть бути виконані легко, дистанційно та за допомогою електронних засобів через відповідні «точки єдиного контакту» і відповідними органами. Зважаючи на вказане, в ЄС визначено ряд існуючих обмежень відносно електронного (цифрового) розвитку Європи і запропоновано новітнє законодавство про електронні підписи, взаємне визнання електронної ідентифікації та електронної автентифікації, а також необхідність розроблення та прийняття чіткої законодавчої бази, забезпечення сумісності, підвищення використання громадянами електронних систем та суттєвого запобігання кіберзлочинності. Основою цього законодавства є спочатку прийнята Пропозиція, а після і сам проект «Регламент Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку» (в подальшому Регламент) [1]. Він є основним перспективним нормативно-правовим документом, який по суті розроблений на основі досвіду створення, застосування та удосконалення інфраструктури відкритого ключа ЄС і направлений на забезпечення безпечних, цілісних електронних операцій

між підприємствами, громадянами і державними органами. Вважається, що його впровадження дозволить підвищити ефективність державних і приватних онлайн-послуг, електронного бізнесу та електронної торгівлі в ЄС. Також на практиці встановлено, що Директива 1999/93/ЄС про «Загальні основи для електронних підписів», в основному охоплює тільки електронні підписи. Тому визнано, що в ЄС відсутні всебічні можливості для здійснення транскордонних та міжрегіональних безпечних, надійних і простих електронних операцій, що включають електронну ідентифікацію, автентифікацію та електронні підписи. Зрозуміло, що першим кроком вирішення протиріч є покращення існуючого законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявлених електронних схем ідентифікації, електронної автентифікації та інших довірчих послуг (eIAS). *Метою цієї статті є визначення та аналіз основних проблемних питань та вимог, які викладені в пропозиціях Регламенту [1], а також розгляд можливостей застосування певних чи усіх його положень відносно вимог у вигляді пропозицій та рекомендацій для України.*

1. СУТНІСТЬ ПРАВИЛ РЕГЛАМЕНТУ ТА ПРИНЦИП ВНУТРІШНЬОГО РИНКУ

В цілому Регламент призначений встановити правила електронної ідентифікації та електронних довірчих послуг для електронних операцій з метою забезпечення належного функціонування внутрішнього ринку ЄС. Він також визначає та встановлює умови, за яких держави-члени ЄС повинні визнавати і приймати засоби електронної ідентифікації фізичних та юридичних осіб, які підпадають під повідомлені схеми електронної ідентифікації іншої держави-члена. Регламент по суті встановлює законодавчу базу щодо електронного підпису, електронної печатки (штампу), електронних міток часу, електронних документів, послуг електронної доставки та перевірки справжності веб-сайту. Регламент гарантує, що довірчі послуги та продукти, які відповідають йому, можуть вільно циркулювати на внутрішньому ринку. Він може бути застосований до електронної ідентифікації, що надається від імені або під відповідальність держав-членів, і до провайдерів довірчих послуг, що розташовані в ЄС. Регламент не поширюється на надання електронних довірчих послуг, які базуються на добровільних угодах у рамках приватного права суб'єктів. Він також не поширюється на аспекти та сутності, які пов'язані з укладанням і дійсністю договорів або інших правових зобов'язань, де є вимоги до форми, встановлені національним або союзним законом.

Основним принципом внутрішнього ринку в ЄС є те, що не має бути ніяких обмежень на надання довірчих послуг провайдерами довірчих послуг на території держави-члена, розташованими в інших державах-членах з причин, які відносяться до галузей,що охоплені Регламентом. При цьому продукти, які відповідають Регламенту, повинні вільно циркулювати на внутрішньому ринку ЄС.

2. ВИЗНАЧЕННЯ ТА ПОНЯТТЯ, ЯКІ ПРИЙНЯТІ В РЕГЛАМЕНТІ

Розглядаючи Регламент з точки зору розвитку та удосконалення, розширення змісту та сутності довірчих послуг, необхідно було в Регламенті внести пояснення і відносно визначень та понять. Розглянемо та проаналізуємо деякі з них, які необхідні для подальшого викладення вимог Регламенту.

Визначення в частині електронної ідентифікації та автентифікації.

2.1. *«Електронна ідентифікація»* означає процес використання персональних даних для ідентифікації в електронній формі, які однозначно визначають фізичну або юридичну особу.

2.2. *«Засіб електронної ідентифікації»* — це матеріальний або нематеріальний блок даних, який містить персональні дані, і використовується для доступу до онлайн-послуг.

2.3. *«Схема електронної ідентифікації»* — це система електронної ідентифікації, за допомогою якої засоби електронної ідентифікації видаються особам.

2.4. «Автентифікація» — це електронний процес, який дозволяє підтвердити правильність електронної ідентифікації фізичної або юридичної особи, або походження та цілісність електронних даних.

Визначення в частині електронного підпису.

2.5. *«Підписувач»* — це фізична особа, яка створює електронний підпис.

2.6. *«Електронний підпис»* — це дані в електронній формі, які приєднуються або логічно пов'язуються з іншими електронними даними, і використовуються підписувачем як підпис.

2.7. *«Вдосконалений електронний підпис»* — це електронний підпис, що відповідає таким вимогам:

а) він однозначно пов'язаний з підписувачем;

б) він може ідентифікувати підписувача;

в) він виробляється з використанням даних вироблення електронного підпису, які підписувач може, з високим ступенем впевненості, одноосібно контролювати;

г) він пов'язаний з даними, до яких він відноситься, так, що будь-яка наступна зміна даних може бути виявлена.

2.8. *«Кваліфікований електронний підпис»* — це вдосконалений електронний підпис, який створюється пристроєм для створення кваліфікованого електронного підпису, і базується на кваліфікованому сертифікаті для електронних підписів.

2.9. *«Дані вироблення електронного підпису»* — це унікальні дані, які використовуються

підписувачем для створення електронного підпису.

2.10. *«Сертифікат»* — це електронний атестат, що пов'язує дані для перевірки електронного підпису або печатки фізичної чи юридичної особи з відповідним сертифікатом і підтверджує ці дані.

2.11. *«Кваліфікований сертифікат електронного підпису»* — це атестат, який використовується для підтримки електронних підписів, видається провайдером кваліфікованих довірчих послуг і відповідає вимогам, викладених у Додатку I Регламенту [4].

Визначення в частині довірчих послуг.

2.12. *«Довірча послуга»* — це будь-яка електронна послуга, що стосується вироблення, перевірки, підтвердження правильності, обробки та зберігання електронних підписів, електронних печаток, електронних міток часу, електронних документів, послуг електронної доставки, підтвердження справжності сайту та електронних сертифікатів, включаючи сертифікати електронного підпису та електронних печаток.

2.13. *«Кваліфікована довірча послуга»* — це довірча послуга, яка відповідає прикладним вимогам, що передбачені у Регламенті [4].

2.14. *«Провайдер довірчих послуг»* — це фізична або юридична особа, яка надає одну чи кілька довірчих послуг.

2.15. *«Провайдер кваліфікованих довірчих послуг»* — провайдер довірчих послуг, який відповідає вимогам, що викладені в Регламенті [4].

2.16. *«Продукт»* – це апаратне або програмне забезпечення, або їх відповідні компоненти, які призначені для використання при наданні довірчих послуг.

2.17. *«Пристрої для створення електронного підпису»* — налаштоване програмне або апаратне забезпечення для створення електронного підпису.

2.18. *«Пристрій для створення кваліфікованого електронного підпису»* — пристрій для створення електронного підпису, що відповідає вимогам, викладених у Додатку II Регламенту [4].

Визначення в частині електронної печатки.

2.19. *«Власник електронної печатки (штампа)»* — фізична або юридична особа, яка накладає електронну печатку (штамп).

2.20. *«Електронна печатка»* — це дані в електронній формі, які додаються або логічно пов'язані з іншими електронними даними, щоб гарантувати походження і цілісність цих даних.

2.21. *«Вдосконалена електронна печатка»* — електронна печатка, яка відповідає таким вимогам:

а) вона однозначно пов'язана з власником печатки;

б) вона здатна ідентифікувати власника печатки;

в) вона створюється з використанням даних для створення електронної печатки, які власник печатки може з високим рівнем впевненості тримати під власним контролем, а також використовувати для створення електронних печаток;

г) електронна печатка пов'язана з даними, до яких вона відноситься, так, що будь-яка наступна зміна даних може бути виявлена.

2.22. *«Кваліфікована електронна печатка»* — це вдосконалена електронна печатка, яка створюється пристроєм для вироблення кваліфікованих електронних печаток, і базується на кваліфікованому сертифікаті електронної печатки.

2.23. *«Дані для створення електронної печатки»* — це унікальні дані, які використовуються власником електронної печатки для створення електронної печатки.

2.24. *«Кваліфікований сертифікат електронної печатки»* — це атестат, який використовується для підтримки електронної печатки, видається кваліфікованим провайдером довірчих послуг і відповідає вимогам, що викладені у додатку III Регламенту [4].

Визначення в частині електронної мітки часу.

2.25. *«Електронна мітка часу»* – це дані в електронній формі, які пов'язують інші електронні дані з конкретним моментом часу, забезпечуючи доказ того, що ці дані існували в той час.

2.26. *«Кваліфікована електронна мітка часу»* — це електронна мітка часу, яка відповідає вимогам, викладених у статті 33 Регламенту [4].

Визначення в частині електронного документу.

2.27. *«Електронний документ»* — це документ у будь-якому електронному форматі.

2.28. *«Послуга електронної доставки»* — це послуга, яка дозволяє передавати дані за допомогою електронних засобів і надає докази щодо обробки переданих даних, у тому числі докази передачі або прийому даних, і захищає дані, що передані, від ризику втрати, крадіжки, пошкодження або несанкціонованих змін.

2.29. *«Кваліфікована послуга електронної доставки»* — це послуга електронної доставки, яка відповідає вимогам, викладених у статті 36 Регламенту [4].

Визначення в частині перевірки справжності сайту.

2.30. *«Кваліфікований сертифікат для перевірки справжності веб-сайту»* — це атестат, що надає можливість перевірити справжність сайту та пов'язує сайт з особою, якій видано сертифікат, за умови, що він видається кваліфікованим провайдером довірчих послуг і відповідає вимогам, які викладені в Додатку IV Регламенту [4].

2.31. *«Дані для перевірки»* — дані, які використовуються для перевірки електронного підпису або електронної печатки.

3. ОСНОВНІ ПРОБЛЕМНІ ПИТАННЯ ТА НЕДОЛІКИ, ЩО УСКЛАДНЮЮТЬ ВПРОВАДЖЕННЯ ЄДИНОГО ЦИФРОВОГО РИНКУ

Основними проблемними питаннями та недоліками, що ускладнюють впровадження єдиного цифрового ринку, є такі:

3.1. Відсутність довіри змушує споживачів, бізнес і керівництво вагатися при здійсненні операцій в електронному вигляді та приймати нові послуги.

3.2. Недостатній рівень довіри до електронних операцій на внутрішньому ринку, в тому числі в частині забезпечення безпечних і цілісних електронних операцій між підприємствами, громадянами і державними органами.

3.3. Директива 1999/93/ЄС Європейського Парламенту та Ради від 13 грудня 1999 року про загальні основи для електронних підписів охоплює в основному електронні підписи, не надаючи всебічних транскордонних та міжрегіональних основ для безпечних, надійних і простих електронних операцій.

3.4. Відсутність сумісності і зростання кіберзлочинності стали як основні перешкоди на шляху ефективного розвитку цифрової економіки.

3.5. Провайдери послуг іншої держави-члена не можуть використати свою електронну ідентифікацію для доступу до цих послуг, оскільки національні схеми електронної ідентифікації в їх країні не визнані і не приймаються в інших державах-членах. Цей електронний бар'єр не дозволяє провайдерам послуг насолоджуватися усіма перевагами внутрішнього ринку.

3.6. Згідно з Регламентом держави-члени ЄС не зобов'язані повідомляти про свої схеми електронної ідентифікації. Вибір залишається за державою: чи повідомити про всі, деякі або про кожну з електронних схем ідентифікації, що використовуються на національному рівні, для доступу до громадських онлайн-послуг або особливих послуг.

3.7. Доступ до онлайн-послуг та їх кінцеве надання заявникові має бути тісно пов'язане з правом отримання таких послуг на умовах, встановлених національним законодавством.

3.8. Має бути транскордонне використання засобів електронної ідентифікації для повідомленої схеми. Виключаються будь-які конкретні національні технічні правила та національні рішення, наприклад, для отримання конкретного апаратного або програмного забезпечення для перевірки і підтвердження повідомленої електронної ідентифікації. Водночас, неминучими є технічні вимоги до користувачів, які випливають з власних характеристик токена, що використовується, наприклад, смарт-картки чи електронного ключа.

3.9. Регламент не повинен вимагати загальне зобов'язання використовувати засоби ідентифікації. Так, він не повинен охоплювати надання послуг на основі добровільних угод у рамках приватного права. Він також не повинен включати аспекти, що пов'язані з укладанням і дійсністю контрактів або інших правових зобов'язань, для яких діють вимоги до форми, встановлені національним законом або законом Союзу.

3.10. У зв'язку з швидким темпом технологічних змін, Регламент повинен бути відкритим для своєчасних інновацій.

3.11. Через швидкий темп технологічних змін, цей Регламент повинен прийняти підхід, який є відкритим для інновацій.

3.12. З метою підвищення довіри населення до внутрішнього ринку і сприяння використанню довірчих продуктів і послуг, мають бути введені поняття кваліфікованих довірчих послуг і кваліфікованих провайдерів довірчих послуг, їх кваліфікованої довірчої послуги та продукту.

3.13. Відповідно до зобов'язань в рамках Конвенції ООН з прав інвалідів вони повинні мати можливість використовувати довірчі послуги та кінцеву продукцію, що використовується при наданні цих послуг, на рівних правах з іншими споживачами.

3.14. Провайдер довірчих послуг повинен брати на себе зобов'язання, що викладені у Директиві 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року про захист особи під час обробки персональних даних і про вільне розповсюдження таких даних. Зокрема, збір даних має бути зведений до мінімуму з урахуванням цілей наданої послуги.

3.15. Використання псевдонімів у сертифікатах не повинно перешкоджати державам-членам вимагати ідентифікацію осіб, яка має здійснюватися відповідно до союзного або національного законодавства.

3.16. Має здійснюватися нагляд за провайдерами кваліфікованих довірчих послуг навіть тоді, коли провайдер надає свої послуги на території іншої держави-члена ЄС, і не підлягає там нагляду, або коли комп'ютери провайдера знаходяться на території іншої держави-члена, ніж та, якій провайдер належить.

3.17. Для забезпечення взаємного визнання електронних підписів необхідно забезпечувати високий рівень безпеки, але електронні підписи з нижчим рівнем гарантій безпеки також повинні прийматися.

3.18. З метою забезпечення подальшого розвитку транскордонних електронних операцій на внутрішньому ринку ЄС оригінальні електронні документи або їх завірені копії, що видані відповідними компетентними органами держав-членів у рамках свого національного законодавства, мають прийматися і в інших державах-членах. Регламент не повинен впливати на право держав-членів визначати, що є оригіналом, а що копією на національному рівні, але повинен гарантувати, що вони можуть використовуватися так само і за кордоном.

3.19. Для того щоб гарантувати операторам ринку правову визначеність, які вже використовують кваліфіковані сертифікати, видані відповідно до Директиви 1999/93/ЕС, необхідно забезпечити достатній період часу, протягом якого буде здійснено перехід.

3.20. Наймовірніше цілі Регламенту не можуть бути повністю досягнуті державами-членами ЄС однаковою мірою, в силу масштабів необхідних дій, якби вони були б у повному обсязі досягнуті на рівні Союзу, то Союз міг би вжити заходів відповідно до принципу взаємодопомоги, як це передбачено в статті 5 Договору про Європейський Союз.

4. ОСНОВНІ ВИМОГИ, ПРОПОЗИЦІЇ ТА РЕКОМЕНДАЦІЇ ВІДНОСНО НАДАННЯ ДОВІРЧИХ ПОСЛУГ В ЄВРОПЕЙСЬКОМУ СОЮЗІ В ПЕРІОД 2015-2030 рр.

Для прийняття рішень та визначення вимог відносно Регламенту були задіяні Європейський парламент та Рада Європейського парламенту, Європейська комісія, Європейський Економічний і Соціальний Комітети та Європейський наглядовий орган з питань захисту даних [1].

Основними вимогами, рекомендаціями та пропозиціями, які визначені в Регламенті та документах ЄС, є такі [1]:

4.1. Вирішення основних проблем, які заважають європейським громадянам користуватися перевагами єдиного цифрового ринку і транскордонних цифрових послуг.

4.2. Дуже важливим є створення єдиного цифрового ринку до 2015 р., забезпечення швидкого прогресу у ключових областях цифрової економіки та розвиток повністю інтегрованого єдиного цифрового ринку шляхом полегшення транскордонного використання онлайн-послуг, полегшення безпечної електронної ідентифікації і автентифікації.

4.3. Рекомендувати Комісії зробити свій внесок в єдиний цифровий ринок шляхом створення умов для взаємного визнання ключових компонентів транскордонно, в першу чергу таких як електронна ідентифікація, електронні документи, електронні підписи та електронні послуги доставки, а також для сумісності послуг електронного Уряду на території ЄС.

4.4. Європейський парламент підкреслює важливість забезпечення безпеки електронних послуг, особливо електронних підписів, а також необхідність створення інфраструктури відкритих ключів на загальноєвропейському рівні.

4.5. Європейський парламент закликав Комісію створити європейські органи перевірки для забезпечення транскордонної сумісності електронних підписів і для підвищення безпеки операцій, що здійснюється з використанням Інтернету.

4.6. Директива 2006/123/ЕС Європейського парламенту та Ради від 12 грудня 2006 року «Про послуги на внутрішньому ринку» закликає держави-члени до створення «точок єдиного контакту — спеціалізовані центри » (PSC), щоб гарантувати, що всі процедури і формальності, які пов'язані з доступом до послуг та їх здійсненням, мають бути виконані легко, дистанційно та за допомогою електронних засобів через відповідні «точки єдиного контакту» і відповідними органами.

4.7. Ряд онлайн-послуг повинен бути доступним через PSC, їх здійснення може виконуватися з використанням електронної ідентифікації, автентифікації та електронного підпису.

4.8. Взаємно визнані і прийняті електронні засоби ідентифікації повинні полегшити транскордонне надання численних послуг на внутрішньому ринку і дозволити підприємствам вийти за кордон, не стикаючись з перешкодами при взаємодії з органами державної влади.

4.9. Згідно з Директивою 2011/24/EU Європейського Парламенту та Ради від 9 березня 2011 року про захист прав пацієнтів у транскордонній системі охорони здоров'я необхідно встановити мережу національних органів, відповідальних за електронну систему охорони здоров'я. Для підвищення безпеки і безперервності транскордонної системи охорони здоров'я ця мережа має розробити керівні принципи, що стосуються транскордонного доступу до електронних даних про стан здоров'я і послуг, у тому числі шляхом підтримки "загальних заходів ідентифікації і автентифікації для полегшення перенесення даних у транскордонну систему охорони здоров'я".

4.10. Взаємне визнання і прийняття електронної ідентифікації і автентифікації має бути ключем до того, щоб зробити транскордонну охорону здоров'я реальною для громадян Європи. Якщо люди подорожують з метою лікування, їх медичні дані мають бути доступні в країні лікування. Це вимагає твердої, безпечної і надійної електронної ідентифікації.

4.11. Однією з цілей Регламенту має бути усунення існуючих бар'єрів для транскордонного використання електронних засобів ідентифікації, що використовуються в державах-членах для доступу, принаймні до громадських послуг.

4.12. Згідно з Регламентом не повинно бути втручання в системи управління електронною ідентифікацією і пов'язаних з ними інфраструктурами, що функціонують у державах-членах ЄС. Його метою має бути забезпечення можливості доступу до транскордонних онлайн-послуг, що надаються державами-членами, а також надання безпечних послуг у частині електронної ідентифікація та автентифікації.

4.13. Держави-члени повинні залишати за собою право використовувати або вводити засоби для електронної ідентифікації взагалі, і для доступу до онлайн-послуг. Вони також повинні вирішити, чи слід залучати приватний сектор до надання цих засобів.

4.14. У Регламенті мають бути встановлені деякі умови, з урахуванням яких повинні прийматися електронні засоби ідентифікації і повідомлятися схеми їх здійснення. Вони мають допомогти державам-членам створити необхідний

рівень довіри один до одного стосовно схем електронної ідентифікації та взаємно визнати і прийняти засоби електронної ідентифікації, що підпадають під їх повідомлені схеми. Повинен застосовуватися принцип взаємного визнання і прийняття, якщо держава-член, що повідомляє схему, яка відповідає умовам повідомлення, і повідомлення було опубліковано в Офіційному журналі Європейського Союзу. Тим не менш, доступ до цих онлайн-послуг та їх кінцеве надання заявникові має бути тісно пов'язане з правом отримання таких послуг на умовах, встановлених національним законодавством.

4.15. Держави-члени повинні мати можливість залучити приватний сектор до випуску засобів електронної ідентифікації та дозволити приватному сектору використання засобів електронної ідентифікації для повідомленої схеми з метою ідентифікації, коли це необхідно для онлайн-послуг або електронних операцій. Можливість використання таких засобів електронної ідентифікації дозволить приватному сектору покладатися на електронну ідентифікацію та автентифікацію, що вже значною мірою використовуються в багатьох державах-членах, принаймні для громадських послуг, і зробити простішим для підприємств і громадян доступ до транскордонних онлайн-послуг. Для того щоб полегшити використання приватним сектором таких засобів електронної ідентифікації транскордонно, для належних сторін має бути доступна можливість автентифікації, надана державами-членами, без дискримінації між державним або приватним сектором.

4.16. Транскордонне використання засобів електронної ідентифікації для повідомленої схеми вимагає співпраці держав-членів у забезпеченні технічної сумісності. Це виключає будь-які конкретні національні технічні правила та національні рішення, наприклад, для отримання конкретного апаратного або програмного забезпечення для перевірки і підтвердження повідомленої електронної ідентифікації. З іншого боку, неминучими є технічні вимоги до користувачів, які випливають з власних характеристик токена, що використовується, наприклад, смарт-картки чи електронного ключа.

4.17. Співробітництво держав-членів ЄС має сприяти встановленню технічної сумісності повідомлених схем електронної ідентифікації, з тим щоб створити високий рівень довіри і безпеки, відповідний ступеню ризику. Причому, обмін інформацією та передовим досвідом між державами-членами, що здійснюватиметься з метою їх взаємного визнання, має допомогти в забезпеченні сумісності.

4.18. Регламент повинен бути основною законодавчою базою використання електронних довірчих послуг. Тим не менш, він не повинен створювати загальне зобов'язання використовувати їх. Зокрема, він не повинен охоплювати надання послуг на основі добровільних угод у рамках приватного права. Він також не повинен охоплювати аспекти, пов'язані з укладанням і дією контрактів або інших правових зобов'язань, для яких діють вимоги до форми, встановлені національним законом або законом Союзу.

4.19. Для того щоб ввійти в загальне транскордонне використання електронних довірчих послуг, має існувати можливість використовувати їх як докази у судових розглядах у всіх державах-членах.

4.20. На додаток до тих, що входять у закритий перелік довірчих послуг, держави-члени ЄС також повинні мати можливість визначати інші види довірчих послуг, що передбачені Регламентом. Це має дозволити визнавати їх на національному рівні як кваліфіковані довірчі послуги.

4.21. Через швидкий темп технологічних змін, Регламент має бути відкритим для інновацій.

4.22. Регламент має бути технологічно нейтральним, причому його правові наслідки мають досягатися за допомогою наявних будь-яких технічних засобів, що задовольняють вимоги Регламенту.

4.23. З метою визначення вимог і зобов'язань із забезпечення високого рівня безпеки будь-якої кваліфікованої довірчої послуги і продукту, а також з метою підвищення довіри населення до внутрішнього ринку і сприяння використанню довірчих продуктів і послуг, мають бути введені поняття "кваліфіковані довірчі послуги" і "кваліфікований провайдер довірчих послуг".

4.24. Інваліди повинні мати можливість використовувати довірчі послуги та кінцеву продукцію, що використовується при наданні цих послуг, на рівних правах з іншими споживачами.

4.25. Провайдер довірчих послуг повинен бути контролером персональних даних і, отже, повинен брати на себе зобов'язання, що викладені у Директиві 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року про захист особи під час обробки персональних даних і про вільне розповсюдження таких даних. Так, збір даних має бути зведений до мінімуму з урахуванням цілей наданої послуги.

4.26. Для забезпечення належного виконання провайдерами послуг законодавства про захист даних наглядові органи повинні співпрацювати і обмінюватися інформацією з органами захисту. Причому, обмін інформацією повинен включати інформацію про інциденти і порушення щодо персональних даних.

4.27. З тим щоб підвищити довіру користувачів до єдиного ринку, на всіх провайдерів довірчих послуг повинно бути покладено зобов'язання застосовувати передові технології забезпечення безпеки, які відповідали б можливим ризикам, пов'язаних з їх діяльністю.

4.28. Положення про використання псевдонімів у сертифікатах не повинно перешкоджати державам-членам вимагати ідентифікацію осіб відповідно до союзного або національного законодавства.

4.29. Усі без виключення держави-члени ЄС повинні виконувати загальні вимоги нагляду для забезпечення належного рівня безпеки кваліфікованих довірчих послуг. Для того щоб полегшити послідовне виконання цих вимог на всій території ЄС, держави-члени повинні прийняти відповідні процедури і обмінюватися інформацією про свою наглядову діяльність та передовий досвід у цій галузі.

4.30. Повідомлення про порушення безпеки або втрати цілісності повинні оперативно надаватись зацікавленим сторонам.

4.31. У разі виявлення порушення необхідно надати запит до наглядових органів з метою отримання стислої інформації про нього, та надсилати її до Комісії та Європейського агентства мережної та інформаційної безпеки.

4.32. Для оцінки рівнів безпеки необхідно дати Комісії та державам-членам змогу оцінювати ефективність його застосування, у тому числі надавати запити до наглядових органів з метою отримання статистичних даних про використання кваліфікованих довірчих послуг.

4.33. Для того щоб Комісії та державам-членам надати змогу оцінити ефективність удосконаленого механізму нагляду, що може вводитись або існує, наглядові органи повинні звітувати про свою діяльність. Результати звітів можуть бути спрощенням обміну передовим досвідом між наглядовими органами, що забезпечило б перевірку повноти та ефективності реалізації основних вимог щодо нагляду у всіх державах-членах.

4.34. Для забезпечення необхідних рівнів гарантій кваліфікованих довірчих послуг та підвищення впевненості користувачів у безперервності надання кваліфікованих довірчих послуг наглядові органи повинні гарантувати, що дані провайдерів кваліфікованих довірчих послуг зберігаються і залишаються доступними протягом відповідного періоду часу, навіть якщо провайдер кваліфікованих довірчих послуг перестає існувати.

4.35. Для полегшення нагляду за провайдерами кваліфікованих довірчих послуг, наприклад, коли провайдер надає свої послуги на території іншої держави-члена ЄС і не підлягає там нагляду, або коли комп'ютери провайдера знаходяться на території іншої держави-члена, ніж та, якій провайдер належить, має бути створена взаємна система допомоги між наглядовими органами в державах-членах.

4.36. Провайдери довірчих послуг, безумовно, відповідають за виконання вимог до надання довірчих послуг, викладених у Регламенті, зокрема, до кваліфікованих довірчих послуг. Наглядові органи несуть відповідальність за контроль виконання провайдерами вимог відносно безпеки надання довірчих послуг.

4.37. Для забезпечення ефективного процесу ініціації роботи провайдерів кваліфікованих довірчих послуг і включення їх у довірчі списки слід заохочувати до попередньої взаємодії потенційного провайдера кваліфікованих довірчих послуг і компетентного контролюючого органу.

4.38. Довірчі списки є важливими елементами зміцнення довіри між операторами ринку, оскільки вони є показником статусу кваліфікованого провайдера послуг під час проведення контролю.

4.39. Ставши предметом повідомлення, кваліфікована довірча послуга не може бути заборонена для здійснення адміністративних процедур або формальностей відповідними органами державного сектору, через те, що вона не включена в довірчі списки, встановлені державами-членами.

4.40. Для нинішніх цілей орган державного сектору звертається до будь-якої державної установи або іншої організації, що уповноважена здійснювати надання послуг електронного Уряду, наприклад, таких як онлайн-декларування податків, запит свідоцтва про народження, участі в електронних процедурах державних закупівель і т.д.

4.41. Для забезпечення взаємного визнання електронних підписів необхідно забезпечувати високий рівень гарантій безпеки, наприклад, у контексті викладення заходів у Рішенні Комісії 2009/767/ЕС від 16 жовтня 2009, що полегшують використання процедур за рахунок використання електронних засобів через "точки єдиного контакту" (відповідно до Директиви 2006/123/ЕС Європейського Парламенту та Ради про послуги на внутрішньому ринку), але електронні підписи з нижчим рівнем гарантій безпеки також повинні прийматися за певних умов.

4.42. Мають бути відповідні механізми і процедури, щоб гарантувати, що підписувач має одноосібний контроль над використанням своїх електронних даних для створення підпису, причому вимоги до кваліфікаційного підпису могли забезпечуватися засобом використання у підписувача кваліфікованого пристрою підписування.

4.43. Для забезпечення правової перевірки підпису має бути визначено, які компоненти кваліфікованого електронного підпису мають бути оцінені відповідною стороною, що здійснює перевірку підпису. Крім того, визначення вимог до провайдерів кваліфікованих довірчих послуг, які можуть надати кваліфіковану послугу перевірки підпису відповідним сторонам, що не бажають або не в змозі самостійно проводити перевірки кваліфікованого електронного підпису, має стимулювати приватний та державний сектор до інвестування в такі послуги. Вони повинні мати можливість зробити перевірку кваліфікованого електронного підпису перевірки на рівні ЄС, використовуючи прості та зручні механізми.

4.44. Також, коли електронна операція вимагає кваліфікованої електронної печатки юридичної особи, кваліфікований електронний підпис уповноваженого представника юридичної особи повинен прийматися.

4.45. Електронні печатки повинні служити доказом того, що електронний документ був виданий юридичною особою, забезпечуючи справжність походження документа та його цілісність.

4.46. Має бути забезпечене довгострокове збереження підписаної інформації, тобто забезпечувати юридичну силу електронного підпису та електронних печаток протягом тривалого періоду часу, гарантуючи, що вони можуть бути перевірені незалежно від майбутніх технологічних змін.

4.47. З метою розвитку транскордонного використання електронних документів цей Регламент має забезпечувати юридичну силу електронних документів, які повинні розглядатися на рівні з паперовими документами, в залежності від оцінених ризиків і за умови забезпечення автентичності та цілісності документів.

4.48. Враховуючи те, що в державах-членах сьогодні використовують різні формати вдосконалених електронних підписів, необхідно, щоб принаймні декілька форматів вдосконалених електронних підписів технічно підтримувалися державами-членами, якщо вони отримують документи, які підписані в електронному вигляді.

4.49. Якщо в державах-членах використовують вдосконалені електронні печатки, то необхідно забезпечити підтримку принаймні декількох форматів вдосконалених електронних печаток.

4.50. Перевірка справжності електронного документа, що виданий юридичною особою, має виконуватись з використанням електронної печатки, причому вона може використовуватись і для автентифікації будь-яких електронних (цифрових) активів юридичної особи, наприклад, програмного коду, серверів тощо.

4.51. Застосування послуги підтвердження справжності веб-сайту та особи, що ним володіє, має ускладнити задачу спроби фальсифікації веб-сайтів.

4.52. Комісії ЄС мають бути передані повноваження приймати:

– акти, які містять рішення щодо сумісності електронної ідентифікації;

– перелік заходів безпеки, які вимагаються від постачальників довірчих послуг;

– перелік визнаних незалежних органів, що відповідальні за проведення аудиту провайдерів послуг;

– перелік довірених списків;

– перелік вимог, які пов'язані з рівнем гарантій безпеки електронних підписів;

– перелік вимог до кваліфікованих сертифікатів електронного підпису, їх перевірки та збереження;

– перелік органів, відповідальних за сертифікацію пристроїв для створення кваліфікованих електронних підписів;

– перелік вимог до рівня безпеки електронних печаток і кваліфікованих сертифікатів для електронних печаток;

– порядок взаємодії між службами електронної доставки.

4.53. В ході підготовчої роботи Комісія повинна проводити відповідні наради, в тому числі на експертному рівні.

4.54. Комісія в ході підготовки і складання делегованих актів, повинна забезпечити одночасну, своєчасну та належну передачу відповідних документів до Європейського парламенту та Ради.

4.55. Повноваження з виконання вимог Регламенту повинні бути покладені на Комісію, зокрема, для визначення відповідних стандартів, використання яких дасть презумпцію відповідності певним вимогам, викладених у цьому Регламенті або визначених у делегованих актах. Причому повноваження мають здійснюватися відповідно до Регламенту № 182/2011 Європейського парламенту і Ради від 16 лютого 2011 року, що встановлює правила і загальні принципи, які стосуються механізмів контролю з боку Державчленів, які повинні здійснюватися Комісією з виконавчих повноважень [1,4].

4.56. З метою повної правової визначеності і ясності Директива 1999/93/ЕС має бути скасована.

4.57. Для того щоб гарантувати правову визначеність операторам ринку, що вже використовують кваліфіковані сертифікати, які видані відповідно до Директиви 1999/93/ЕС, перехід на виконання вимог Регламенту має бути протягом достатнього періоду часу. Також необхідно надати Комісії засоби для прийняття виконавчих та делегованих актів до цієї дати.

4.58. Зважаючи на те, що цілі Регламенту не можуть бути повністю досягнуті усіма державами-членами ЄС, перш за все внаслідок масштабів дійства, то ЄС рекомендується вжити заходів відповідно до принципу взаємодопомоги, як це передбачено в статті 5 Договору про Європейський Союз.

4.59. Відповідно до принципу пропорційності Регламент не виходить за рамки того, що необхідно для досягнення мети, особливо по відношенню до ролі Комісії як координатора національної діяльності.

5. ОСОБЛИВОСТІ ПРОБЛЕМНИХ ПИТАНЬ ТА ОСНОВНІ ВИМОГИ ДО НАЦІОНАЛЬНОЇ СИСТЕМИ НАДАННЯ ДОВІРЧИХ ПОСЛУГ

5.1. Вище в пунктах 3.1–3.20 викладено проблемні питання відносно створення системи надання довірчих послуг в ЄС. Як показав аналіз, а також на основі [8–10], вони ще більшою мірою стосуються і України. Так, існуюча національна система ЕЦП ще більшою мірою є ізольованою по відношенню до існуючої в ЄС. В ній застосовуються національні стандарти усіх криптографічних перетворень, механізми і протоколи автентифікації, встановлення та узгодження ключів, управління ключами, технічні специфікації форматів даних тощо.

5.2. Дуже актуальними та необхідними є завдання аналізу Регламенту в частині можливого розроблення або гармонізації його як аналогічного національного нормативного документу, в тому числі, можливо, для забезпечення транскордонного застосування в Україні.

5.3. З урахуванням сутності напрямів розвитку електронного ринку ЄС та світових тенденцій важливим для України є теоретичне обґрунтування та аналіз методів і механізмів реалізації електронної ідентифікації та автентифікації, електронної печатки та електронної мітки часу, електронних документів та електронної доставки, електронного підпису та автентифікації веб-сайтів.

5.4. Для України важливою проблемою є забезпечення безпеки довірчих електронних послуг, особливо електронних підписів, а також необхідність створення інфраструктури відкритих ключів, включаючи усі довірчі послуги, які рекомендуються для держав Європейського Союзу.

5.5. Для виконання вимог необхідно створити або покласти на існуючі органи перевірку питання забезпечення транскордонної сумісності електронних підписів і для підвищення безпеки операцій, що здійснюються з використанням мереж, наприклад Інтернету.

5.6. Важливим на перспективу для України є створення елементів служби «точок єдиного контакту — спеціалізованих центрів», щоб гарантувати, що всі процедури і формальності, пов'язані з доступом до послуг та їх здійсненням, мають бути виконані легко, дистанційно та за допомогою електронних засобів через відповідні «точки єдиного контакту» і відповідними органами.

5.7. Закон «Про електронний цифровий підпис» та Правила посиленої сертифікації охоплюють тільки електронні підписи, не надаючи безпечних, надійних і простих довірчих електронних послуг електронної ідентифікації та автентифікації, електронної печатки та електронної мітки часу, електронних документів та електронної доставки, електронного підпису та автентифікації веб-сайтів.

5.8. Зростання кіберзлочинності та в більшості випадків несумісність системи ЕЦП в Україні складають основні перешкоди на шляху ефективного розвитку електронної цифрової економіки.

5.9. Повинно бути державне та транскордонне використання засобів електронної ідентифікації для повідомленої або ухваленої схеми.

5.10. Національний документ, аналогічний Регламенту, має бути відкритим для своєчасних інновацій.

5.11. Для підвищення довіри до внутрішнього ринку і сприяння використанню довірчих продуктів і послуг в Україні повинні надаватись кваліфіковані довірчі послуги та мають бути розроблені і схвалені кваліфіковані провайдери довірчих послуг.

5.12. Після створення в Україні системи надання довірчих послуг має здійснюватися нагляд за провайдерами кваліфікованих довірчих послуг.

5.13. Для того щоб гарантувати операторам ринку правову визначеність, що вже використовують кваліфіковані сертифікати, видані відповідно до закону «Про ЕЦП», необхідно забезпечити достатній період часу, протягом якого буде здійснено перехід.

5.14. Дуже важливим є створення єдиного електронного цифрового ринку в Україні до 2015 р., це може забезпечити швидкий прогрес у ключових областях електронної цифрової економіки та розвитку повністю інтегрованого єдиного цифрового ринку, що може полегшити транскордонне використання онлайн-послуг, а також суттєве полегшення безпечної електронної ідентифікації і автентифікації.

5.15. Взаємно визнані і прийняті електронні засоби ідентифікації України повинні полегшити транскордонне надання численних послуг на внутрішньому ринку, а також дозволити підприємствам вийти за кордон, не стикаючись з перешкодами при взаємодії з органами державної влади.

5.16. У нормативному документі України (регламенті) повинні бути встановлені деякі умови, з урахуванням яких мають прийматися електронні засоби ідентифікації і повідомлятися схеми їх здійснення. Вони повинні допомогти створити необхідний рівень довіри один до одного стосовно схем електронної ідентифікації та взаємно визнати і прийняти засоби електронної ідентифікації, що підпадають під їх повідомлені схеми.

5.17. Повинна бути реалізована можливість залучення приватного сектору до випуску засобів електронної ідентифікації та отримані дозволи приватному сектору у використанні засобів електронної ідентифікації для повідомленої схеми з метою ідентифікації, коли це необхідно для онлайн-послуг або електронних операцій.

5.18. Провайдери довірчих послуг України повинні безумовно відповідати за виконання вимог до надання довірчих послуг.

5.19. Наглядові органи повинні нести повну відповідальність за контроль виконання провайдерами вимог відносно безпеки надання довірчих послуг.

5.20. Важливими елементами зміцнення довіри між операторами ринку є довірчі списки, вони є показником статусу кваліфікованого провайдера послуг під час проведення контролю.

5.21 Електронні печатки, що використовуються в Україні, мають бути доказом того, що електронний документ був виданий юридичною особою, забезпечуючи справжність походження документа та його цілісність.

5.22. Має бути забезпечене довгострокове збереження підписаної інформації протягом тривалого періоду часу, гарантуючи, що вона може бути перевірена незалежно від майбутніх технологічних змін.

5.23. З метою розвитку транскордонного використання електронних документів Україна має забезпечувати юридичну силу електронних документів, які повинні розглядатися на рівні з паперовими документами.

5.24. Перевірка справжності електронного документа, що виданий юридичною особою, має виконуватися з використанням електронної печатки.

5.25. В Україні, зважаючи на важливість, мають бути створені та застосовуватись послуги підтвердження справжності веб-сайту та особи, що ним володіє.

5.26. В ході підготовчої роботи в Україні мають бути створена міжвідомча комісія та визначені провідні фірми, які можуть виконати задачі створення та застосування систем надання довірчих послуг, які відповідають вимогам Регламенту.

5.27. З метою повної правової визначеності та ясності закон України «Про електронний цифровий підпис» після деякого часу повинен бути скасованим.

Література

[1] Brussels, XXX. COM(2012) 238/2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILon electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) {SWD(2012) 135} {SWD(2012) 136}.

[2] Соціальний звіт ЄС 2010: Руйнування перешкод, що перешкоджають правам громадян ЄС, COM (2010) 603 пункт 2.2.2, стор. 13.

[3] Висновки Ради щодо плану дій європейського електронного Уряду 2011-2015 роки, 3093rd, Засідання Ради транспорту, телекомунікацій та енергетики, Брюссель, 27 травня 2011 року.

[4] Резолюция Європейського Парламенту від 21.09.2010 про створення внутрішнього ринку для електронної торгівлі, 21.09.10, P7_TA (2010) 0320, і Резолюція Європейського Парламенту від 15.06.2010 про управління Інтернетом: наступні кроки, P7_TA (2010) 0208.

[5] 20 OJ L 376, 27.12.2006, стор. 36.

[6] Закон України «Про електронний цифровий підпис» . № 852-IX від 22.05.2003.

[7] Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.

[8] Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків: Форт. – 2010. – 593 с.

[9] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. 1 та 2 вид. – Харків: ХНУРЕ. – Форт. – 2012. – 878 с.

[10] Правила посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 3 від 13.01.2005, зареєстрованих у Міністерстві юстиції України 27.01.2005 за № 104/10384 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50).

Надійшла до редколегії 14.03.2013

Горбенко Юрій Іванович, к.т.н., технічний директор АТ «ІІТ». Наукові інтереси: криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

УДК 681.3. 06 (07)

Проблемы и требования к предоставлению доверительных услуг в Европейском Союзе в период 2015–2030 рр. / Ю.И. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 184–193.

Определяются и приводятся результаты анализа основных проблемных вопросов и требований, изложенных в предложениях проекта «Регламент Европейского Парламента и Совета относительно электронной идентификации и трастовых сервисов для электронных операций на внутреннем рынке» ЕС, рассматриваются в виде предложений и рекомендаций возможности использования определенных или всех его положений относительно требований в Украине.

Ключевые слова: трансграничные электронные онлайн-услуги, безопасные электронные услуги относительно электронной подписи, электронной печати, электронных документов, услуг электронной доставки и проверки подлинности веб-сайта.

Библиогр.: 10 назв.

UDC 681.3. 06 (07)

Problems and requirements to the grant of confidential services in European Union in the period of 2015 – 2030 / Yu.I. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 184–193.

The results of analysis of the main issues and requirements that are described in the proposals of the "Regulations of the European Parliament and Council for electronic identification and trust services for electronic transactions in the domestic market" are presented. The proposals and recommendations concerning the use of some or all of its provisions to define requirements for a perspective system for provision of trustee services in Ukraine are considered.

Keywords: transfrontal electronic on-line services, safe electronic services in relation to an electronic signature, electronic seal, electronic documents, services of electronic delivery and verification of authenticity of a web server-site.

Ref.: 10 items.

УДК 004.75:004.05

ХМАРНІ ОБЧИСЛЕННЯ ТА АНАЛІЗ ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРІ

І.Ф. АУЛОВ, І.Д. ГОРБЕНКО

Розглядається сучасний стан застосування та розвитку хмарних обчислень, основні переваги та недоліки їх використання у державах, на підприємствах та в науковій діяльності. Визначаються та аналізуються стандарти, нормативні та керівні документи в галузі інформаційної безпеки хмарних обчислень, що розроблені Cloud Security Alliance (CSA), Європейським агентством мережної та інформаційної безпеки (ENISA) і Національним інститутом стандартів і технологій (NIST), а також наводяться результати детального аналізу питань інформаційної безпеки в хмарі.

Ключові слова: хмарні обчислення, інформаційна безпека, порівняльний аналіз, недоліки та переваги обчислень в хмарах.

ВСТУП

В останні роки ефективного застосування набувають хмарні технології або хмарні обчислення (англ. Cloud computing).

В [1] дається визначення хмарних обчислень як моделі забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера.

До хмарних технологій проявляють зацікавленість як великі компанії, які намагаються оптимізувати свої витрати на IT-інфраструктуру підприємства, так і малі компанії, які не мають можливості відразу розгорнути свою власну інфраструктуру. Також зацікавлені звичайні користувачі, що можуть отримати такі послуги як зберігання даних, використання програм тощо. Зростання інтересу до технології хмарних обчислень пов'язано з економічним ефектом від їх використання. В ході їх використання споживачі можуть істотно знизити капітальні витрати на побудову центрів обробки даних, закупівлю серверного та мережного обладнання, апаратних і програмних рішень, забезпечення безперервності і працездатності, а також час побудови та введення в експлуатацію великих об'єктів інфраструктури інформаційних технологій. Всі ці проблемні питання за даних умов перекладаються з користувачів на провайдерів хмарних послуг, а користувач лише оплачує фактично надані послуги. Також хмарні сервіси надають їх користувачам гнучкість у налаштуванні таких параметрів, як обчислювальна потужність, обсяг файлового сховища, склад програмного забезпечення тощо. Однак, незважаючи на явні переваги, під час використання хмарних обчислень необхідно вирішувати і ряд проблемних питань. Основними з них є довіра до постачальника сервісу, забезпечення конфіденційності, цілісності, справжності та неспростовності інформації на усіх етапах її існування, безперебійність в роботі, захист від несанкціонованого доступу (НСД) та збереження особистих даних користувачів, які передаються та обробляються в хмарі. Метою цієї статті є класифікація та огляд основних технологій хмарних обчислень, а також аналіз сучасного стану застосування та досліджень в галузі безпеки хмарних технологій.

1. ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ

NIST США запропонував модель хмари, яка складається з п'яти основних характеристик, трьох моделей обслуговування і чотирьох моделей розгортання [1].

Основними характеристиками хмари є такі:

– Якість самообслуговування на вимогу (*англ.* on-demand self-service), коли споживач не взаємодіючи безпосередньо з представником постачальника послуг, може самостійно визначати та змінювати такі обчислювальні потреби як серверний час, швидкість доступу та обробки даних, обсяг збережених даних тощо.

– Універсальність доступу з використанням мережі (*англ.* broad network access), коли послуги доступні споживачам через мережі передачі інформації, незалежно від термінального пристрою клієнтських платформ (наприклад, мобільні телефони, планшети, ноутбуки та робочі станції).

– Ступінь об'єднання ресурсів (*англ.* resource pooling), коли постачальник послуг об'єднує ресурси для обслуговування декількох споживачів, використовуючи багатокористувальницьку модель з різними фізичними і віртуальними ресурсами, які динамічно розподіляються та перерозподіляються між користувачами відповідно до попиту. При цьому клієнт не має змоги контролювати розташування ресурсу або не знає точне місце його розташування, але в змозі вказати місце розташування на більш високому рівні абстракції (наприклад, країну, штат або центр обробки даних). Як такі ресурси можуть виступати: сховища даних, обчислювальні потужності, пам'ять та пропускна здатність мережі.

– Достатня еластичність (*англ.* rapid elasticity), коли послуги в будь-який момент часу без додаткових витрат на взаємодію з постачальником можуть бути надані, розширені, звужені, як правило, в автоматичному режимі. Для споживача

такі можливості провайдера з надання послуг здаються необмеженими та можуть бути надані в будь-якій кількості і в будь-який час.

– Облік споживання (*англ.* measured service), коли сервіс хмари автоматично управляє та оптимізує використання ресурсів користувачами за рахунок вимірювань на деякому рівні абстракції (наприклад, обсяг збережених даних, пропускна здатність, кількість користувачів, кількість транзакцій). Контроль над використанням ресурсів, можливість управління ресурсами та формування звіту з споживання забезпечують прозорість як для постачальника, так і для споживача послуг.

В [1] також визначено такі моделі обслуговування за допомогою хмари:

– Програмне забезпечення як послуга (SaaS) – модель, коли споживачу надається можливість використання додатків постачальника, що працюють на хмарній інфраструктурі. Програми є доступними з різних клієнтських пристроїв або через інтерфейс тонкого клієнту, такий як веб-браузер (наприклад, веб-пошта) або інтерфейсу програми. Споживач не контролює та не керує базовою інфраструктурою хмари, в тому числі мережею, серверами, операційною системою, зберіганням, або навіть індивідуальними можливостями додатка, за винятком обмежених користувальницьких параметрів конфігурації додатка. Прикладами такої моделі є сервіси Gmail та Google docs.

– Платформа як послуга (PaaS) – модель, коли споживачу надається можливість розгортання на базі хмарної інфраструктури власних чи придбаних додатків, які створені за допомогою мови програмування, бібліотек, служб та засобів, що підтримуються постачальником. Споживач не контролює та не керує базовою інфраструктурою хмари, в тому числі мережею, серверами, операційною системою, або зберіганням, але має контроль над розгорнутими додатками і, можливо, параметрами конфігурації середовища, в якому працюють додатки. Наприклад, Google Apps надає додатки для бізнесу в режимі онлайн, доступ до яких відбувається за допомогою Інтернет-браузера, тоді як програмне забезпечення та дані зберігаються на серверах Google.

– Інфраструктура як послуга (IaaS) – модель, коли споживачу надається можливість обробки, зберігання, доступ до мережі та інших основних обчислювальних ресурсів, де споживач має можливість розгортання і запуску довільного програмного забезпечення, яке може включати в себе операційні системи та програми. Споживач не контролює та не керує базовою інфраструктурою хмари, але має контроль над операційними системами, зберіганням та розгорнутими додатками, і, можливо, обмежений контроль вибору мережних компонентів (наприклад, мережними екранами). Найбільшими гравцями на ринку інфраструктури як послуги є Amazon, Microsoft, VMWare, Rackspace та Red Hat. Хоча деякі з них пропонують більше, ніж просто інфраструктуру, їх об'єднує мета продавати базові обчислювальні ресурси.

Обчислювальна хмара може бути розгорнута як: приватна, публічна, громадська або гібридна [1].

Приватна хмара (*англ.* private cloud) – це хмарна інфраструктура, яка призначена для використання виключно однією організацією, що включає декількох користувачів (наприклад, підрозділів). Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінація). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Громадська хмара (*англ.* community cloud) – це хмарна інфраструктура, яка призначена для використання конкретною спільнотою споживачів із організацій, що мають спільні цілі (наприклад, місію, вимоги щодо безпеки, політику та відповідність різноманітним вимогам). Громадська хмара може перебувати у спільній власності, керуванні та експлуатації однієї чи більше організацій зі спільноти або третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Публічна хмара (*англ.* public cloud) – це хмарна інфраструктура, яка призначена для вільного використання широким загалом. Публічна хмара може перебувати у власності, керуванні та експлуатації комерційних, академічних (освітніх та наукових) або державних організацій (чи будь-якої їх комбінації). Публічна хмара знаходиться в юрисдикції постачальника хмарних послуг.

Гібридна хмара (*англ.* hybrid cloud) – це хмарна інфраструктура, що складається з двох або більше різних хмарних інфраструктур (приватних, громадських або публічних), які залишаються унікальними сутностями, але з'єднані між собою стандартизованими або приватними технологіями, що дозволяють переносити дані та прикладні програми (наприклад, використання ресурсів публічної хмари для балансування навантаження між хмарами).

2. ОСНОВНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРІ

На сьогодні провідними організаціями, що займаються питаннями безпеки в хмарі, є Альянс безпека в хмарі (Cloud Security Alliance, CSA), що складається з представників IT-індустрії, а також дві державні організації Європи та США: Європейське агентство мережної та інформаційної безпеки (ENISA) і Національний інститут стандартів і технологій (NIST).

Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки(ІБ) в хмарі. Розглянемо їх та проведемо порівняння.

2.1 Таксономія питань ІБ у хмарі CSA

CSA є некомерційною організацією, що створена наприкінці 2008 року організаціями, засновниками якої виступили великі IT-компанії,

зацікавлені у впровадженні хмарних технологій: Google, Microsoft, IBM, Salesforce.com, VMware та інші.

Основним документом, який розглядає проблеми безпеки в хмарі, є «Керівництво з безпеки критичних областей для хмарних обчислень». Перша версія його була опублікована в 2009 році. Нами розглянута остання, 3 версія цього документу, яка доступна на офіційному сайті організації. Основними складовими вимог ІБ у хмарах, що рекомендуються до розгляду та аналізу, є такі [4]:

1 *Організаційні та правові питання ІБ*

1.1 Управління ризиками.

1.1.1 Корпоративне управління ризиками.

1.1.2 Управління ризиками підприємства та постачальника послуг.

1.1.3 Управління інформаційними ризиками

1.2 Правові питання та законодавство.

1.2.1 Стандартизація, міжнародне законодавство, узгодження законодавства держав.

1.2.2 Договір між постачальником та клієнтом.

1.2.3 Право власності на інформацію, що обробляється в хмарі.

1.3 Відповідність вимогам та аудит.

1.3.1 Проведення експертизи; моніторинг, тестування та оновлення програмного та апаратного забезпечення постачальника.

1.3.2 Дотримання існуючих міжнародних та державних законів.

1.3.3 Аудит безпеки постачальника послуг.

1.4 Управління інформацією та безпекою даних.

1.4.1 Безпека даних (запобігання витоку, несанкціонованого доступу, втраті тощо).

1.4.2 Управління життєвим циклом даних (створення, зберігання, використання, обмін, архівування, відновлення, знищення).

1.4.3 Керування розташуванням даних.

1.4.4 Управління авторським правом (DRM).

1.5 Переносимість та інтероперабельність.

1.5.1 Сумісність апаратного, програмного забезпечення, архітектурних рішень постачальників.

1.5.2 Стандартизований інтерфейс взаємодії з постачальником хмарних послуг.

2 Технічні питання ІБ

2.1 Традиційна безпека забезпечення безперервності бізнесу та аварійного відновлення.

2.1.1 Захист від стихійних лих, техногенних катастроф та ін.

2.1.2 Захист від людського фактору та обслуговуючого персоналу.

2.2 Операції центру обробки даних.

2.2.1 Взаємодія між центрами постачальника.

2.2.2 Взаємодія між різними постачальниками.

2.3 Реагування на інциденти, повідомлення про них та відновлення.

2.3.1 Попередження виникнення інцидентів ІБ.

2.3.2 Визначення та аналіз інцидентів ІБ.

2.3.3 Відновлення після інцидентів безпеки.

2.4 Безпеки додатків та програм.

2.4.1 Контроль якості, тестування на відмову, безпечність програмного забезпечення.

2.4.2 Розмежування доступу користувачів до додатків.

2.4.3 Моніторинг активності додатків.

2.4.4 Виявлення небезпечних програм та забезпечення безпеки існуючих.

2.5 Шифрування та управління ключами.

2.5.1 Альтернативні підходи до шифрування даних у хмарі.

2.5.2 Криптографія в хмарі.

2.5.3 Шифрування баз даних.

2.5.4 Управління ключами в хмарі (генерація, використання, зберігання, знищення, відновлення).

2.6 Ідентифікація і управляння доступом.

2.6.1 Моделі ідентифікації в хмарі.

2.6.2 Керування профілями користувачів.

2.6.3 Надання послуг ідентифікації, автентифікації, спільного доступу до інформації в хмарі або ресурсів.

2.6.4 Реалізація ідентифікації користувачів у програмному забезпеченні.

2.6.5 Доступність, цілісність даних, доступ до даних авторизованих користувачів.

2.7 Віртуалізація.

2.7.1 Забезпечення захисту гістьової віртуальної машини від атак.

2.7.2 Механізми захисту від неправомірних дій адміністраторів.

2.7.3 Питання швидкодії, пікового збільшення навантаження, збільшення числа вузлів.

2.7.4 Забезпечення безпеки даних на рівні віртуальної машини.

2.7.5 Забезпечення цілісності образів віртуальних машин.

2.8 Безпека як сервіс.

2.8.1 Продаж послуг безпеки.

2.8.2 Проблеми при реалізації послуги безпеки.

2.8.3 Класифікація послуг безпеки.

Документ окрім питань ІБ розглядає також архітектуру побудови хмари та надає рекомендації та шляхи вирішення цих проблем. У цілому питання ІБ у хмарі поділяються на дві великі групи: питання управління ІБ у хмарі (організаційні питання ІБ) та ІБ у хмарі під час її використання (технічні питання ІБ). Кожна з груп розбита на більш малі, що називаються доменами. Домени, що відносяться до організаційних, у першу чергу розглядаються з метою вироблення рішень правових питань, питань політики ІБ, управління ризиками та стандартизація. В рамках технічних питань розглядаються питання реалізації та впровадження захисту в хмарі.

2.2 Таксономія питань ІБ у хмарі ENISA

Європейське агентство з мережної та інформаційної безпеки (ENISA) є організацією, діяльність якої спрямована на «підвищення здатності Європейського Союзу, держав-членів ЄС та бізнес-спільноти на попередження, ліквідацію

і реагування на проблеми мережної та інформаційної безпеки» [6].

Організацією ENISA було підготовлено і опубліковано документ "Безпека хмарних обчислень та оцінка ризиків" [5], в якому були розглянуті питання інформаційної безпеки в хмарі, їх переваги та недоліки, існуючі ризики, аналіз та шляхи їх зменшення, існуючі загрози в середовищі хмарних обчислень. Згідно з цим документом можна виділити такі ризики ІБ, які існують в хмарі :

1 Організаційні питання ІБ

1.1 Втрата можливості керування користувачем деякими налаштуваннями безпеки в хмарі.

1.2 Замкнутість користувача на одному постачальнику послуг у зв'язку з відсутністю переносимості та інтероперабельності розгорнутої інфраструктури.

1.3 Дотримання вимог стандартів.

1.4 Втрати ділової репутації постачальника.

1.5 Припинення роботи сервісом хмари.

1.6 Відмова в роботі одного з постачальників.

1.7 Придбання провайдера хмарних послуг.

2 Правові питання ІБ

2.1 Судовий розгляд та законодавство в сфері електронних даних.

2.2 Ризик зміни юрисдикції.

2.3 Ризики щодо захисту даних.

2.4 Ризики ліцензування.

2.5 Право власності електронних даних.

3 Технічні питання ІБ

3.1 Порушення ізоляції даних користувачів.

3.2 Часткове або неповне знищення даних користувача.

3.3 Вичерпання ресурсів.

3.4 Загроза інсайдерів в інфраструктурі постачальника послуг.

3.5 Ризики інтерфейсу управління.

3.6 Перехоплення даних зловмисником при передачі.

3.7 Витік даних при завантаженні та скачуванні.

3.8 Розподілена відмова в обслуговуванні (DDoS-атака).

3.9 Економічна відмова в обслуговуванні (EDoS-атака).

3.10 Втрата ключів шифрування.

3.11 Проведення сканування та тестування з метою виявлення вразливостей.

2.3 Таксономія питань ІБ у хмарі NIST

З метою впровадження хмарних обчислень урядом США в організації NIST було замовлено розроблення стандарту з забезпечення безпеки та конфіденційності в громадських хмарах. Тому починаючи з 2011 року NIST опублікував ряд документів, які давали визначення хмарним обчисленням, розглядали питання ІБ у хмарі, пропонували архітектуру безпеки в хмарі, давали рекомендації з оцінки та усунення існуючих ризиків ІБ у хмарі.

Класифікація питання ІБ у хмарі розглядається в таких документах NIST: «Посібник з безпеки та конфіденційності в громадських хмарних обчисленнях» [7] та «Короткий огляд хмарних обчислень та рекомендації» [8]. На відміну від розглянутих таксономій питань ІБ у хмарі CSA та ENISA, в таксономії NIST питання ІБ чітко не поділяють на такі рівні як організаційні питання, правові питання та технічні питання ІБ. Розглянемо їх в натуральному вигляді.

1 Управління

1.1 Контроль і нагляд урядовою організацією за політикою, процедурами та стандартами в ході розробки додатків та інформаційних технологій, одержання послуг, а також проектування, впровадження, тестування, використання та моніторинг розгорнутих хмар.

2 Дотримання законів, правил, стандартів та специфікацій

2.1 Дотримання міжнародних та державних стандартів, законів і правил.

2.2 Дотримання законів та правил держав, та їх застосування до даних хмари, що фізично розташовуються в межах цієї держави.

2.3 Законодавство в сфері електронних даних.

2.4 Підтримка в проведенні експертизи.

3 Довіра до постачальника послуг

3.1 Доступ до конфіденційної інформації осіб (інсайдерів), завдяки своєму службовому становищу.

3.2 Право власності електронних даних.

3.3 Складені сервіси та сервіси, які використовують сервіси хмари, надані третьою стороною.

3.4 Аудит постачальника, моніторинг, тестування та оновлення програмного та апаратного забезпечення постачальника.

3.5 Захист персональних даних користувача.

3.6 Управління ризиками.

4 Архітектура програмного і апаратного забезпечення

4.1 Зовнішні атаки на інфраструктуру.

4.2 Захист віртуальної мережі.

4.3 Захист образів віртуальних машин.

4.4 Клієнтський захист.

4.5 Захист серверів постачальника.

4.6 Моніторинг захисту.

5 Ідентифікація і управління доступом

5.1 Автентифікація.

5.2 Контроль доступу.

5.3 Спільний доступ до інформації в хмарі.

5.4 Управління ключовими даними.

6 Ізоляція програмного забезпечення

6.1 Складність ОС, програмного чи апаратного забезпечення, призначеного для розміщення та роботи віртуальної машини.

6.2 Загрози, пов'язані з іншими користувачами віртуальних машин.

7 Захист даних

7.1 Концентрація даних.

7.2 Ізоляція даних.

7.3 Безпечне зберігання, відновлення, архівування, видалення даних.

8 Доступність ресурсів та даних

8.1 Відключення хмарних сервісів (тимчасове, тривале, постійне).

8.2 Атаки DDoS.

8.3 Загрози, пов'язані з розташуванням даних.

9 Реагування на інциденти

9.1 Моніторинг наявності та доступності даних.

9.2 Аналіз інцидентів та їх розв'язання.

2.4 Порівняння підходів та сутностей класифікацій ІБ організацій CSA, ENISA, NIST

Порівняння здійснено за трьома основними групами складових: правові, організаційні та технічні питання ІБ у хмарі. Засновуючись на розглянутих класифікаціях, було виділено питання ІБ до кожної з груп, що наведені в таблицях 1, 2 та 3. Якщо питання ІБ було розглянуто в класифікації повністю, воно відмічено як «+», якщо частково – «+/-», в разі відсутності – «-».

Аналіз даних таблиць показує, що в основному складові ІБ збігаються в усіх класифікаціях. Найбільш повна та структурована класифікація була надана організацією CSA, але її недоліком є об'єднання правових та організаційних проблем ІБ. Головною перевагою класифікації ENISA є оцінка ймовірності виникнення ризиків, пов'язаних з ІБ, причинами їх виникнення, взаємозв'язки з іншими ризиками, та їх вплив на систему та її елементи. До недоліків класифікації NIST можна віднести відсутність поділу проблем ІБ на три основних групи, як це було зроблено в класифікації ENISA.

3. АНАЛІЗ ПРОБЛЕМНИХ ПИТАНЬ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРІ

Більшість з проблем захисту інформації користувача в хмарі може бути вирішено з використанням існуючих методів криптографічного захисту інформації, адміністративних мір з боку як постачальника хмарних послуг, так і користувача, укладання договорів на надання послуг, які б враховували індивідуальні потреби клієнтів, прийняття міжнародних стандартів у галузі, введення контролю з боку держави та створення незалежних експертів у цій галузі.

Так, наприклад, для забезпечення конфіденційності та цілісності даних, що зберігаються в хмарі, необхідно використовувати алгоритми цифрового підпису та шифрування, які засновані на міжнародних стандартах. Для запобігання несанкціонованого використання профілю користувача можна використовувати існуючі методи двофакторної автентифікації користувача.

Сьогодні більшість постачальників мають свій власний, іноді навіть добре документований інтерфейс для програмування, але це призводить до неможливості переходу користувачів від одного постачальника послуг до іншого. Практика в таких питаннях показує, що лише розробка відкритого єдиного міжнародного стандарту може вирішити це питання.

Головними проблемами, які потребують подальшого детального аналізу та вирішення, є такі:

а) Проблема привілегійованих користувачів. Найбільшу загрозу для безпеки інформації в хмарі становлять користувачі, які мають привілегійований доступ до функцій системи або адміністратори хмарних сервісів, тому для зменшення ризику можливих деструктивних дій з їх боку, доцільно вести незалежний нагляд та контроль за їх діями в хмарі. Як показує статистика саме на внутрішніх користувачів припадає найбільша кількість порушень безпеки.

Таблиця 1

Порівняння правових складових ІБ

№	Правові питання ІБ	Класифікація		
		CSA	ENISA	NIST
1	Дотримання міжнародних та державних стандартів, законів і правил	+	+	+
2	Договір між постачальником та клієнтом	+	+	+
3	Право власності на електронні дані	+	+	+
4	Невідповідність законодавств різних держав у сфері електронних даних	+	+	+
5	Захист авторського права (DRM)	+	-	-
6	Дотримання законів та правил держав до даних у хмарі	+	+	+
7	Зміна постачальника послуг, або його купівля іншим постачальником	+	+	+

Таблиця 2

Порівняння організаційних складових ІБ

№	Організаційні питання ІБ	Класифікація		
		CSA	ENISA	NIST
1	Управління ризиками (корпоративними, підприємства, інформаційними, постачальника послуг)	+	+	+
2	Управління безпекою інформації користувача	+	+	+
3	Довіра до постачальника послуг (проведення аудиту, тестування, оновлення забезпечення, підтримка в проведенні експертизи)	+	+	+
4	Захист від інсайдерів	+	+	+
5	Реагування на інциденти ІБ, їх моніторинг, вирішення	+	+	+
6	Захист персональних даних користувача	-	-	+
7	Управління авторськими правами	+	+	+
8	Відмова сервісів хмари по причині стихійного лиха, збоїв у роботі сервісів хмари, що підтримуються третьою стороною	+	+	+

Таблиця 3

Порівняння технічних складових ІБ

№	Технічні питання ІБ		Класифікація		
			CSA	ENISA	NIST
1	Доступність даних та ресурсів	1.1 Відключення хмарних сервісів	+	+	+
		1.2 Атаки DDoS	-	+	+
		1.3 EDoS-атака	-	+	-
		1.4 Розташування даних	+	+	+
		1.5 Вичерпання ресурсів	+	+	-
2	Переносимість та інтероперабельність забезпечення	2.1 Сумісність забезпечення	+	+	+
		2.2 Стандартизований інтерфейс	+	-	-
3	Безпеки додатків та програм	3.1 Безпечність ПЗ	+	+	+
		3.2 Розмежування доступу	+	+	+
		3.3 Моніторинг активності додатків	+	+	+
		3.4 Виявлення небезпечних програм	+	+	+
		3.5 Захист образів віртуальних машин від модифікації	+	-	+
4	Управління даними та захист	4.1 Ізоляція даних	+	+	+
		4.2 Безпечне зберігання та оброблення даних	+	+	+
		4.3 Шифрування даних	+	+	+
		4.4 Управління ключами	+	+	+
5	Ідентифікація, автентифікація та управляння доступом	5.1 Моделі ідентифікації та автентифікація в хмарі	+	-	-
		5.2 Керування профілями користувачів у хмарі	+	+	+
		5.3 Надання послуг ідентифікації, автентифікації, спільного доступу до інформації в хмарі або ресурсів	+	+	+
		5.4 Реалізація ідентифікації користувачів	+	+/-	+
		5.5 Доступ до даних авторизованих користувачів	+	+	+
6	Віртуалізація	6.1 Забезпечення захисту гістьової віртуальної машини від атак	+	-	+
		6.2 Механізми захисту від неправомірних дій адміністраторів	+	+	+
		6.3 Питання швидкодії, пікового збільшення навантаження, збільшення числа вузлів	+	+	+
		6.4 Забезпечення безпеки даних на рівні віртуальної машини	+	-	+

б) Однією з головних проблем, що гальмує поширення хмарних обчислень, є невідповідність законів у сфері обробки, передачі, збереження та захисту інформації різних держав. Вирішення цієї проблеми є ключовим фактором для можливості фізичного розміщення серверів постачальника хмарних сервісів у різних країнах та регіонах, а також використанням користувачами з різних країн одного постачальника послуг. Ця проблема найбільш істотно торкатиметься транснаціональних корпорацій.

в) Питання довіри до постачальника послуг можуть бути вирішені лише за рахунок проведення аудиту безпеки постачальника хмарних послуг та перевірки відповідності його системи безпеки міжнародним вимогам до захисту інформації, що сформульовані в міжнародних стандартах. Формулювання та обґрунтування вимог є одним з важливих питань.

г) Питання загальних вразливостей у хмарі практично нічим не відрізняються від аналогічних у традиційних системах, за винятком того, що знайдена одна вразливість може бути використана для всієї хмари, але водночас її можна легше виправити за допомогою централізованого оновлення, на відміну від традиційних систем. І в цей час її критичність набагато більша, бо вона може з легкістю уразити всіх користувачів даного постачальника послуг, тому потребує превентивних мір та засобів захисту.

д) Проблеми доступності до сервісів та даних користувачами, відновлення їх роботи після збоїв, чи втрати даних повинні вирішуватися на адміністративному та правовому рівнях. При укладанні договорів з користувачем мають бути чітко визначені обов'язки сторін та міра їх відповідальності в залежності від обставин події, що призвела до цих наслідків, а розслідування повинна проводити третя незалежна сторона. Аналогічна проблема існує і в традиційних системах, але користувач має можливість безпосередньо впливати на рівень резервування в системі, що дає можливість більш гнучко її налаштовувати під конкретні вимоги користувача та його фінансові можливості.

є) Проблема надання доступу, спільного доступу та блокування доступу до ресурсів і даних у хмарі користувачам.

е) Проблема захисту інтелектуальної власності в хмарі, зокрема програмного забезпечення та даних.

4. ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ХМАР

Головною перевагою використання хмарних обчислень, яка покладена в основу технології,

є балансування робочого навантаження, за рахунок чого досягається більш ефективне використання ресурсів обчислювальної системи. До основних переваг технології можна віднести:

– можливість доступу до ресурсів у хмарі, використовуючи Інтернет з'єднання, звичайний браузер та невимогливий до ресурсів термінал кінцевого користувача;

– швидке розгортання власних сервісів та/або збільшення робочого навантаження на існуючі постачальником хмарних послуг;

– підтримка резервування, самовідновлення та масштабування, яке дозволяє підвищувати надійність системи та зменшувати ризики при відмовах програмного та апаратного забезпечення;

– управління робочими навантаженнями в реальному часі, в тому числі пакетними операціями та фоновими програми, що взаємодіють з користувачами;

– моніторинг у реальному часі завантаження та балансу системи, а також виділення ресурсів.

Крім перелічених переваг існують недоліки та проблемні питання, які гальмують впровадження хмарних обчислень, а саме:

– неможливість роботи з сервісами хмари без постійного підключення до Інтернет;

– складний або неможливий процес переходу від одного постачальника хмарних послуг до іншого;

– відсутність єдиного міжнародного правового регулювання у сфері хмарних обчислень та обробки інформації в хмарі;

– довіра до постачальника послуг користувачів;

– питання захисту інформації користувача, що обробляються та зберігаються в хмарі.

Для забезпечення безпеки інформації, хмарні обчислення надають такі переваги:

– спеціалізований персонал: провайдер хмари, як велика організація, для забезпечення безпеки в хмарі наймає спеціалістів у галузі безпеки інформації, що дозволяє співробітникам зосередитися виключно на питанні безпеки, досягти високого рівня безпеки, який не можливо досягти в невеликій організації;

– централізоване керування, конфігурація системи безпеки та її аудит;

– стійкість платформи: апаратний та програмний склад платформи, на якій розгорнуто хмару більш рівномірно, ніж у більшості традиційних обчислювальних центрів, що дозволяє краще автоматизувати діяльність щодо забезпечення безпеки, тестування та виправлення помилок у компонентах платформи;

– наявність ресурсів: можливість динамічного масштабування ресурсів системи, а також резервування та аварійного відновлення, що може бути використано для підвищення стійкості системи проти атак типу «відмова в обслуговуванні», а також швидкого відновлення після серйозних інцидентів;

– резервне копіювання і відновлення: провайдер хмарних послуг може дозволити надання більш високого рівня резервного копіювання і відновлення, ніж той, що забезпечують традиційні центри обробки даних, а також забезпечити зберігання резервних копій за географічною вимогою;

– мобільність кінцевих клієнтів: завдяки архітектурі хмари клієнти можуть використовувати різноманітні портативні пристрої, з невеликою обчислювальною потужністю, виходом до мережі Інтернет, браузером та/або декількома встановленими додатками, щоб отримати доступ до основних обчислювальних ресурсів;

– концентрація даних: використання хмари, як єдиного місця для зберігання та обробки даних, у деяких випадках дозволяє підвищити безпеку, ніж зберігання даних, що розосереджені по портативних комп'ютерах, вбудованих пристроях або зберігаються на знімному носії.

До недоліків використання хмарних обчислень з точки зору безпеки інформації відносять:

– складність системи: загальна хмара є надзвичайно складною порівняно з традиційним центром обробки даних. Велика кількість компонентів, з яких складається хмара, дозволяє проводити атаки на різних рівнях абстракції. Крім компонентів для загальних обчислень, таких як розгортання додатків, віртуальних моніторів машини, гістьових віртуальних машин, зберігання даних є також компоненти, які включають в себе елементи управління: самообслуговування, ресурс обліку, управління квотами, реплікація даних і відновлення, моніторинг рівня сервісу, управління робочим навантаженням.

Загальне багатокористувальницьке середовище: основним недоліком публічних хмар є те, що ресурси та компоненти користувачі поділяють з користувачами, які їм не відомі на логічному рівні, що дозволяє зловмиснику, використовуючи вразливості всередині хмари, подолати механізм розподілу ресурсів між користувачами та отримати несанкціонований доступ до ресурсів.

Однорідність програмного та апаратного складу платформи означає, що єдиний недолік проявлятиметься у всій хмарі та потенційно впливатиме на усіх користувачів послуг

Використання Інтернету: сервіси хмари, а також адміністрування та керування налаштуваннями хмарних сервісів та додатків, використовує незахищену мережу Інтернет. При переході організації на використання хмарних обчислень, для внутрішніх захищених мереж та ресурсів виникають нові інформаційні небезпеки, які слід вирішувати. Також виникає необхідність віддаленого адміністрування з використанням незахищеного каналу передачі інформації.

Втрата контролю: при використанні сервісів хмари, користувач передає контроль над інформацією провайдеру хмари, що несе в собі додаткові ризики для безпеки інформації. Користувач стає залежним від провайдера хмари, та може втратити не тільки логічний контроль над інформацією, але й фізичний.

ВИСНОВКИ

Хмарні обчислення є комбінацією з декількох ключових технологій, які були розроблені протягом багатьох років та розглядаються багатьма дослідниками як наступне покоління IT-архітектури підприємств.

Зі всією сукупністю переваг, які надає використання хмарних обчислень, є багато питань безпеки, які на сьогодні не достатньо добре проаналізовані та знаходяться ще на стадії обговорення.

Як було показано в статті, головною проблемою, що не вирішена в галузі хмарних обчислень на сьогодні, є довіра користувачів до постачальника послуг. Ця проблема гостро стоїть не тільки для компаній та підприємств, що використовують сторонніх постачальників, але й звичайних користувачів, персональні дані яких також потребують захисту та гарантій безпеки. Якщо у випадку великого підприємства воно може захистити себе від загроз проведенням аудиту безпеки провайдера хмарних послуг та аналізом ризиків та загроз інформаційної безпеки, а також застрахувати їх, чи створити свою власну приватну хмару, то невеликі компанії або звичайні користувачі не мають такої можливості. Тому необхідно впроваджувати механізми контролю постачальників хмарних послуг на міжнародному рівні або на рівні держави, з метою проведення аудиту безпеки та перевірки їх відповідності міжнародним або державним стандартам та висунутим до них умов.

У подальших роботах планується розглянути та проаналізувати існуючі архітектури побудови хмар з точки зору їх безпеки.

Література

[1] The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011.

[2] Guidelines on Security and Privacy in Public Cloud Computing , NIST SP800-144, 2011.

[3] Cloud Computing Synopsis and Recommendations DRAFT, NIST, 2011.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0. Technical report, Cloud Security Alliance, 2011. Режим доступу http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] D. Catteddu and G. Hogben. Cloud Computing Security Risk Assessment. Technical report, European Network and Information Security Agency, November 2009. Режим доступу http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[6] D. Catteddu and G. Hogben. Cloud Computing Information Assurance Framework. Technical report, European Network and Information Security Agency, November 2009. Режим доступу http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

[7] Wayne Jansen, Timothy Grance Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, 2011. Режим доступу http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[8] Lee Badger Cloud Computing Synopsis and Recommendations NIST Special Publication 800-146 Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas, 2012. Режим доступу http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

Надійшла до редколегії 19.03.2013

Аулов Іван Федорович, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: дослідження принципів побудови, розгортання і аналіз стійкості асиметричних криптографічних систем, хмарні та мобільні технології.

Горбенко Іван Дмитрович, доктор технічних наук, професор, завідувач кафедри БІТ ХНУРЕ, головний конструктор АТ «Інститут інформаційних технологій». Наукові інтереси: прикладна криптологія, криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

УДК 004.75:004.05

Облачные вычисления и анализ информационной безопасности в облаке / И.Ф. Аулов, И.Д. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 194–201.

В статье рассматривается современное состояние облачных вычислений, преимущества и недостатки их использования для предприятия, государства и научной деятельности. Определяются и анализируются стандарты, нормативные и руководящие документы в области информационной безопасности облачных вычислений, которые разработаны Cloud Security Alliance (CSA), Европейским агентством сетевой и информационной безопасности (ENISA) и Национальным институтом стандартов и технологий (NIST), а также приводятся результаты детального анализа вопросов информационной безопасности в облаке.

Ключевые слова: облачные вычисления, информационная безопасность, сравнительный анализ, преимущества и недостатки вычислений в облаке.

Табл.: 3. Библиогр.: 8 назв.

UDC 004.75:004.05

Cloud computing and analysis of information security in the cloud / I.F. Aulov, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 194–201.

The paper considers the current state of cloud computing, the advantages and disadvantages of using them for business, government and academia, analyzes the standards, regulations and guidelines on information security of cloud computing developed by Cloud Security Alliance (CSA), the European Agency for Network and Information Security (ENISA) and the National Institute of Standards and Technology (NIST), for detailed analysis of information security issues in the cloud.

Keywords: cloud computing, information security, comparative analysis, advantages and disadvantages of cloud computing.

Tab.: 03. Ref.: 08 items.

УДК 681.3.06

АНАЛІЗ БЕЗПЕКИ СЕРВІСІВ ЗБЕРІГАННЯ ДАНИХ У ХМАРІ

К.А. ПОГРЕБНЯК, Д.В. ПОВТАРЄВ

Стаття присвячена аналізу сервісів зберігання інформації у хмарі. Для аналізу сервісів визначаються критерії безпеки, за якими проводиться порівняння. Розглядаються такі сервіси: Dropbox, SkyDrive, GoogleDrive, Wuala та Yandex.Disk. Основна увага приділяється аналізу інтерактивного входу в систему, реєстрації, формуванню захищеного каналу зв'язку та механізмам безпеки зберігання даних.

Ключові слова: хмарні обчислення, сервіс зберігання інформації, безпека зберігання даних.

ВСТУП

За останні роки кількість сервісів зберігання даних, що ґрунтуються на публічних хмарах, помітно збільшилась. Зростання попиту користувачів на такі сервіси обумовлено зручністю користування інформацією, зокрема доступу до неї будь-де та будь-коли. Однак, з іншого боку, зручність користування інформацією досягається за рахунок переміщення її на фізичні носії провайдера, що вимагає певних гарантій безпечного зберігання даних та їх функціонування в інформаційних мережах [1]. Зазначимо, що наразі не існує міжнародних стандартів та технічних специфікацій, які визначали б безпечні протоколи передачі та зберігання даних. Тому, на даному етапі розвитку таких сервісів фактично кожен провайдер пропонує свої рішення з забезпечення безпеки інформації. Це призводить до того, що кінцевий користувач повинен самостійно оцінювати якість послуг з точки зору захисту його особистих даних. Тому **актуальною задачею** є аналіз існуючих широко поширених сервісів зі зберігання інформації в публічній хмарі з точки зору безпеки інформації.

1. ОГЛЯД СЕРВІСІВ ЗБЕРІГАННЯ ДАНИХ

Системою зберігання даних у хмарі вважається мережа розподілених центрів обробки даних, які надаються користувачеві третьою стороною та сприймаються ним як один єдиний віртуальний сервер. Для підвищення доступності даних інформація може додатково зберігатися в різних місцях, а деталі реалізації не відомі користувачеві. Користування системою зберігання даних надається у вигляді Інтернет-сервісу [2].

Проаналізувавши наявні сервіси зберігання інформації можна виділити такі популярні в Україні та світі сервіси: Dropbox, SkyDrive, SugarSync, GoogleDrive, Mozy, CrashPlan, Insync, LogMeInCubby, Bitcasa, Strongspace, DollyDrive, SpiderOak, Wuala, Yandex.Disk, Box.net, AmazonCloudDrive, JungleDisk, GooglePlayMusic, MediaFire, Office365, Zoho, RapidShare, Sendspace, YouSendIt, Carbonite, Flickr, Photobucket, SmugMug, GoogleMusic, AppleiCloud, AmazonCloudPlayer.

Для написання роботи були відібрані такі сервіси: Dropbox, SkyDrive, GoogleDrive, Wuala, Yandex.Disk.

Стислий опис кожного з них та пояснення причин відбору наведені нижче.

Dropbox управляється DropboxInc, яка знаходиться в Сан-Франциско, США. Dropbox був обраний, оскільки він є одним з найпопулярніших у світі провайдерів хмарного зберігання даних. Він отримав широке висвітлення в засобах масової інформації і цілком може становити суть того, як хмарні сервіси зберігання бачать сьогодні.Сервіс дуже простий в установці, зручний у використанні і доступний безкоштовно або за низьку ціну. Він був розроблений як самостійний хмарний сервіс зберігання даних і забезпечує обмежену інтеграцію в популярних операційних систем.

Wuala існує з 2007 року і працює з березня 2009 року як власність компанії LaCie AG111, яка знаходиться в Цюріху.

До переліку обраних сервісів Wuala потрапив через те, що він реалізує максимальний набір функцій, поширених серед хмарних сервісів та позиціонується як такий, що забезпечує високий криптографічний рівень захисту даних. Крім того, цей сервіс має одну з найвищих швидкостей взаємодії, та монтується як диск з кешуванням - це може потенційно привабити велику кількість користувачів.

Yandex.Disk належить російській компанії Яндекс та знаходиться на ринку з 2012 року. Яндекс є найбільшою Інтернет компанією на пострадянському просторі. Пошукова система Яндекс посідає друге місце в Україні станом на березень 2013 року, займаючи майже 30% ринку (за даними liveinternet.ru). Виходячи з цього факту, можна зробити висновок, що велика частина користувачів обере послуги цього сервісу.

MicrosoftSkyDrive (скорочено – SkyDrive) створений у серпні 2007 року і керується компанією Microsoft. Сервіс є частиною набору онлайн послуг Windows Live. Microsoft є найбільшою світовою компанією з розробки програмного забезпечення. Великий ступінь інтеграції різноманітного програмного забезпечення (в тому числі iMicrosoft SkyDrive), з сімейством найпопулярніших операційних систем сучасності безумовно

забезпечить гідний рівень використання цього сервісу серед користувачів та організацій.

GoogleDrive є хмарним сховищем даних, створеним в 2012 році компанією GoogleInc. GoogleDrive замінює собою GoogleDocs після активації. Поширеність додатків Google, високий рівень використання GoogleDocs та очікувань від його наступника є передумовами включення цього сервісу до списку.

В цій роботі проводиться порівняння найбільш популярних сервісів за методологією, що наведена в [3].

Кожний сервіс включає в себе частини як клієнтського,так і серверного програмного забезпечення. Відповідно до підходу аналізу, пропонується розглянути виключно клієнтську частину програмного забезпечення.

Для реалізації високого рівня безпеки сервіси повинні забезпечувати високий рівень як мінімум наступних аспектів безпеки, які можуть суттєво впливати на рівень захищеності інформації, що зберігається:

1) вхід у систему та реєстрація, для захисту від викриття та збору інформації та з метою примусового використання надійних паролів;

2) використання захищеного каналу для забезпечення транспортної безпеки між клієнтом і сервером;

3) безпека зберігання даних для унеможливлювання вивчення даних постачальником послуг.

Існують інші характеристики, які потенційно можуть вплинути на рівень безпеки даних. До них відносяться безпечний обмін файлами, що зберігаються, дедуплікація, безпечне використання декількох пристроїв для доступу, функції оновлення програмного забезпечення тощо. Аналіз цих характеристик не входив до задач цієї роботи і буде виконаний у подальшому.

2. АНАЛІЗ СЕРВІСІВ ЗБЕРІГАННЯ ДАНИХ

Для аналізу сервісів визначимо критерії та показники, за якими проводитиметься порівняння:

- Вхід у систему та реєстрація
  - обмеження на довжину пароля;
  - захист від атаки перебору пароля;
  - двофакторна автентифікація;
  - механізм відновлення пароля.
- Захищений канал зв'язку:
  - протокол формування захищеного каналу зв'язку;
  - алгоритм автентифікації повідомлень;
  - алгоритм узгодження ключів.
- Безпека зберігання даних
  - алгоритм шифрування даних;
  - володіння ключем шифрування даних.

Послідовно проаналізуємо кожний з сервісів нашого списку відносно наведених критеріїв безпеки.

2.1 Аналіз сервісу зберігання даних Dropbox

2.1.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується захищений канал зв'язку (TLS).

Реєстрація може бути здійснена на веб-сайті або під час установки клієнта.

Під час реєстрації на веб-сайті користувач повинен ввести ім'я та прізвище (довільні рядки), адресу електронної пошти та пароль. Одна адреса електронної пошти може бути пов'язана тільки з одним обліковим записом.

Під час реєстрації накладаються обмеження на мінімальну довжину пароля, яка має бути не менше за шість символів, максимальне обмеження не встановлене. Крім того як пароль не повинна використовуватися адреса електронної пошти.

При реєстрації на веб-сторінці Dropbox надає підказку про якість обраного пароля, проте приймає слабкі паролі.

Процес реєстрації під час установки клієнта трохи відрізняється: клієнтський додаток не має індикатора надійності пароля і користувач повинен повторити пароль. При введенні адреси, що вже була використана, відображується відповідне повідомлення. При першому вході через клієнтський додаток користувач вводить адресу електронної пошти та пароль. Після проходження перевірки автентичності маркер безпеки передається на сервер і зберігається на клієнтській частині для подальшої автентифікації користувача.

Dropbox не відправляє активаційного повідомлення на електронну пошту відразу після реєстрації, це відбувається лише після спроби отримати перший URL для загального доступу до файла, тож користувач може використовувати новий обліковий запис одразу після заповнення реєстраційної форми.

У разі невдалої спроби входу в систему, Dropbox повідомляє користувача, що один елемент з пари логін/пароль є неправильним, проте не уточнює який саме.

Якщо користувач втратив свій пароль, Dropbox відправляє повідомлення на зареєстровану електронну пошту користувача. Цей лист містить URL захищеної веб-сторінки для введення нового пароля.

Dropbox запобігає перебору паролів, тимчасово блокуючи обліковий запис після багатьох невдалих спроб входу в заданий період часу.

Dropbox має можливість використання двофакторної автентифікації. Ця опція може бути ввімкнена в налаштуваннях профілю. Використовуються одноразові коди доступу, які можна отримувати на мобільний телефон. Крім того є можливість використовувати баркоди за допомогою TimeBasedOneTimePassword мобільних додатків.

Результати аналізу сервісу Dropbox за критерієм «Вхід у систему та реєстрація» наведено в таблиці 1.

Таблиця 1

«Вхід у систему та реєстрація» для сервісу Dropbox

Мінімальна довжина пароля	6 символів
Захист від атаки перебору пароля	Тимчасове блокування
Двофакторна автентифікація	Пароль та одноразовий код доступу, що передається на мобільний телефон чи за допомогою використання баркодів
Механізм відновлення пароля	Надсилається URL сторінки, на якій користувач може змінити пароль

2.1.2 Захищений канал зв'язку

В ході аналізу сервісу Dropbox був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати якого наведено у таблиці 2.

Таблиця 2

«Захищений канал зв'язку» для сервісу Dropbox

Протокол формування захищеного каналу зв'язку	TLS 1.1
Алгоритм автентифікації повідомлень	AES_256_CBC (SHA1)
Алгоритм узгодження ключів	ECDHE_RSA (2048 біт)

2.1.3 Безпека зберігання даних

Dropbox використовує AES-256 для шифрування даних, що зберігаються на серверах. Ці дані не будуть зашифровані на стороні клієнта, замість цього Dropbox шифрує дані після завантаження на стороні сервера, використовуючи свій власний ключ шифрування. Оскільки Dropbox шифрує дані на стороні сервера, користувач не може бути впевнений в конфіденційності даних. Результати аналізу за критерієм «Безпека зберігання даних» наведено в таблиці 3.

Таблиця 3

«Безпека зберігання даних» для сервісу Dropbox

Алгоритм шифрування даних	AES-256
Володіння ключем шифрування даних	Ключем володіє провайдер

2.2 Аналіз сервісу зберігання даних Wuala

2.2.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені тільки за допомогою додатка Wuala.

Під час реєстрації користувач повинен надати унікальне ім'я, адресу електронної пошти та пароль. Одна адреса електронної пошти може бути пов'язана з кількома обліковими записами.

На пароль накладаються лише обмеження на мінімальну довжину, яка повинна бути як мінімум шість символів, максимальне обмеження не встановлено.

Wuala надає підказку про якість обраного пароля під час реєстрації, проте не відкидає слабкі паролі.

Wuala не відправляє активаційного повідомлення на електронну пошту для підтвердження факту реєстрації.

У разі невдалої спроби входу в систему, Wuala повідомляє користувача, що один чи обидва елементи з пари логін/пароль є неправильним, проте не уточнює який саме.

Паролі не зберігаються на серверах Wuala, тому можливість відновлення втраченого пароля відсутня. Wuala забезпечує опційну функціональність підказки пароля. Підказка пароля може бути використана для одного імені користувача або для адреси електронної пошти і буде відправлена на зареєстровану адресу пошти. Якщо є кілька облікових записів, зареєстрованих за однією адресою електронної пошти – кілька листів буде відправлено, по одному для кожного облікового запису, який має підказку для пароля. Функція підказки пароля дозволяє збір інформації про вже зареєстровані імена користувачів і адреси електронної пошти.

Обмежень на кількість невдалих спроб входу немає.

У Wuala наразі не реалізовано механізм двофакторної автентифікації.

Результати аналізу сервісу Wuala за критерієм «Вхід у систему та реєстрація» наведено в таблиці 4.

Таблиця 4

«Вхід у систему та реєстрація» для сервісу Wuala

Мінімальна довжина пароля	6 символів
Захист від атаки перебору пароля	Відсутній
Двофакторна автентифікація	Відсутня
Механізм відновлення пароля	Відсутній

2.2.2 Захищений канал зв'язку

Wuala використовує власний протокол зв'язку між клієнтом і сервером, а не стандартизовані і добре відомий SSL / TLS. Відповідно до прес-релізів Wuala, використовується перевірка цілісності для захисту даних при передачі, але жодної детальної документації про механізми і протоколи не було опубліковано.

У поєднанні з конвергентними схемами шифрування, що їх використовує Wuala, відсутність шифрування при передачі дозволяє зловмисникам отримати повідомлення, які передаються, і спробувати реалізувати атаки зі збором інформації.

В ході аналізу сервісу Wuala був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 5.

Таблиця 5

«Захищений канал зв'язку» для сервісу Wuala

Протокол формування захищеного каналу зв'язку	Відсутній
Алгоритм автентифікації повідомлень	AES_256 (SHA1)
Алгоритм узгодження ключів	DHE_RSA (2048 біт)

2.2.3 Безпека зберігання даних

Ідея, на якій базуються схеми шифрування Wuala, полягає в наявності ненадійної файлової системи, безпека якої забезпечується криптографічними методами. Використані схеми є реалізацією структури дерева каталогів для криптографічних файлових систем, яка називається Cryptree, що була опублікована в [4]. Довіра ґрунтується на симетричному кореневому ключі, який отримується з пароля користувача. Wuala обчислює окремі ключі для кожного каталогу і окремі ключі для кожного файла. Всі вони виводяться через кореневий ключ. Вони можуть бути надані партнерам з метою обміну даними.

Wuala використовує конвергентні схеми шифрування [5]. Це означає, що ключ для шифрування файла є похідним від його геш-значення.

Найбільш важливими властивостями конвергентних схем шифрування є:

1) ідентичні відкриті тексти зашифровуються в ідентичні криптотексти, незалежно від користувача;

2) сервер не може розшифрувати криптотексти, не маючи копію відкритого тексту.

Перша властивість забезпечує реалізацію функції дедуплікації зашифрованих даних. Друга властивість захищає документи, які є унікальними для користувача, наприклад, власноруч написані твори, неопубліковані технічні звіти тощо. З іншого боку конвергентні схеми шифрування мають важливі недоліки, зокрема існує можливість атак у разі, якщо зловмисник має доступ до серверної сторони.

Згідно з прес-релізами відзначається, що Wuala використовує AES-256 для шифрування метаданих і інформації, що зберігається. Клієнт підписує кожен файл за допомогою пари ключів користувача, з метою виявлення файлів, які були отримані від сторонніх осіб. Підписи створюються і перевіряються за допомогою RSA-2048, в той час як для перевірки цілісності використовується геш-функція SHA-256.

Результати аналізу за критерієм "Безпека зберігання даних" наведено в таблиці 6.

Таблиця 6

«Безпека зберігання даних» для сервісу Wuala

Алгоритм шифрування даних	Конвергентна схема шифрування
Володіння ключем шифрування даних	Ключем зберігається на стороні клієнта

2.3 Аналіз сервісу зберігання даних Yandex. Disk

2.3.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені тільки на сторінці Яндекс. Для користування сервісом треба мати обліковий запис у системі Яндекс, що є єдиним для всіх додатків, у тому числі і Yandex.Disk.

Під час реєстрації користувач повинен обов'язково надати ім'я, інформацію про стать, дату народження, придумати унікальний логін та двічі ввести пароль. Крім того необхідно обрати секретне питання та ввести інформацію з картинки. Використовується поштова скринька Яндекс, яка має бути унікальною для кожного облікового запису.

Існують обмеження на довжину пароля, яка має складатися як мінімум з шести символів і бути не більшим за 20 символів, пароль не може бути введено не на англійській розкладці клавіатури, та не повинен співпадати з логіном, інших обмежень немає.

Яндекс надає підказку про якість обраного пароля під час реєстрації, проте не відкидає слабкі паролі.

Оскільки логін є єдиним для всіх додатків Яндекс – додаткове підтвердження реєстрації не проводиться.

У разі невдалої спроби входу в систему Яндекс повідомляє користувача, що була введена не правильна пара логін/пароль.

Якщо користувач забув свій пароль, на альтернативну адресу електронної пошти надсилається URL сторінка для зміни паролю. Також можна використати секретний код, який висилається на альтернативну адресу пошти, якщо вона не зазначена – код надсилається на номер мобільного телефон, якщо він також не зазначений – використовується секретне питання. Функція входу надає можливості для збору інформації про вже зареєстровані імена.

Яндекс запобігає перебору паролів за допомогою вимоги обов'язкового вводу символів із зображення після серії невдалих спроб входу в систему.

В Yandex.Disk наразі не реалізовано механізму двофакторної автентифікації.

Результати аналізу сервісу Yandex.Disk за критерієм «Вхід у систему та реєстрація» наведено в таблиці 7.

Таблиця 7

«Вхід у систему та реєстрація» для сервісу Yandex.Disk

Мінімальна довжина пароля	6 символів
Захист від атаки перебору пароля	Використання символів із зображення після серії невдалих спроб входу в сервіс
Двофакторна автентифікація	Відсутня
Механізм відновлення пароля	Надсилається URL сторінки, на якій користувач може змінити пароль чи використовує секретний код

2.3.2 Захищений канал зв'язку

В ході аналізу сервісу Yandex.Disk був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 8.

Таблиця 8

«Захищений канал зв'язку» для сервісу Yandex.Disk

Протокол формування захищеного каналу зв'язку	TLS 1.0
Алгоритм автентифікації повідомлень	RC4_128 (SHA1)
Алгоритм узгодження ключів	RSA (1024 біт)

2.3.3 Безпека зберігання даних

Yandex.Disk не використовує шифрування даних на стороні сервера.Результати аналізу за критерієм "Безпека зберігання даних" наведено в таблиці 9.

Таблиця 9

«Безпека зберігання даних» для сервісу Yandex.Disk

Алгоритм шифрування даних	Не використовується

2.4 Аналіз сервісу зберігання даних SkyDrive

2.4.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені на сторінці SkyDrive. Для користування сервісом треба мати обліковий запис Microsoft. Обліковий запис є єдиним для додатків Hotmail,WindowsPhone, Xbox LIVE та SkyDrive.

Під час реєстрації, користувач повинен обов'язково надати ім'я та прізвище, інформацію про стать, дату народження, адресу електронної пошти та двічі ввести пароль. Крім того необхідно вказати, щонайменше, номер телефону чи секретне питання та ввести інформацію з картинки. Одна адреса електронної пошти може бути пов'язана з одним обліковим записом.

Для створення облікового запису Microsoft необхідно обрати пароль, який повинен включати не менше 8 і не більше 16 символів, які відносяться принаймні до двох з таких типів: букви верхнього і нижнього регістрів, цифри та символи. Крім того Microsoft відкидає поширені паролі. Під час створення пароля інформація про його якість не надається до моменту реєстрації.

Таким чином слабкі паролі не приймаються.

URL для підтвердження реєстрації передається на зазначену поштову скриньку, користування сервісом можливо лише після її підтвердження.

У разі невдалої спроби входу в систему Microsoft повідомляє який саме елемент було введено не правильно.

Якщо користувач забув свій пароль, йому надається 3 можливі способи для встановлення нового пароля: (1) на захищеній сторінці для встановлення нового пароля, URL якої відправляється на пошту; (2) за допомогою коду, який надсилається на мобільний телефон; (3) за допомогою заповнення анкети з великою кількістю секретних та особистих запитань.

Microsoft запобігає перебору паролів тимчасово блокуючи обліковий запис після багатьох невдалих спроб входу в заданий період часу.

Таблиця 10

«Вхід у систему та реєстрація» для сервісу SkyDrive

Мінімальна довжина пароля	8 символів
Захист від атаки перебору пароля	Тимчасове блокування
Двофакторна автентифікація	Пароль та одноразовий код доступу, що передається на альтернативну поштову адресу чи на мобільний телефон при вході з не довіреного пристрою
Механізм відновлення пароля	Надсилається URL сторінки, на якій користувач може змінити пароль чи використовує секретний код

Microsoft має можливість використання двофакторної автентифікації при вході з не довіреного пристрою, ця опція може бути включена в налаштуваннях профіля. Використовуються одноразові коди доступу, що їх можна отримувати на альтернативну поштову адресу чи на мобільний телефон.

Результати аналізу сервісу SkyDrive за критерієм «Вхід у систему та реєстрація» наведено в таблиці 10.

2.4.2 Захищений канал зв'язку

В ході аналізу сервісу SkyDrive був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 11.

Таблиця 11

«Захищений канал зв'язку» для сервісу SkyDrive

Протокол формування захищеного каналу зв'язку	TLS 1.0
Алгоритм автентифікації повідомлень	AES_128_CBC (SHA1)
Алгоритм узгодження ключів	RSA (2048 біт)

2.4.3 Безпека зберігання даних

SkyDrive не використовує шифрування даних на стороні сервера. Результати аналізу за критерієм «Безпека зберігання даних» наведено в таблиці 12.

Таблиця 12

«Безпека зберігання даних» для сервісу SkyDrive

Алгоритм шифрування даних	Не використовується

2.5 Аналіз сервісу зберігання даних GoogleDrive

2.5.1 Вхід у систему та реєстрація

Для реєстрації і входу в систему використовується безпечний канал зв'язку.

Нові облікові записи можуть бути створені на сторінці Google. Для користування сервісом треба мати обліковий запис Google, який є єдиним для всіх сервісів і прив'язаний до електронної адреси Gmail.

Під час реєстрації користувач повинен обов'язково надати ім'я та прізвище, інформацію про стать, дату народження, придумати унікальну

адресу електронної пошти та двічі ввести пароль. Крім того необхідно ввести інформацію з картинки. Одна адреса електронної пошти може бути пов'язана з одним обліковим записом.

Для створення облікового запису Google необхідно обрати пароль, який повинен включати не менше 8 і не більше 100 символів. У паролі можна використовувати латинські букви (як великі, так і малі: A-Z, a-z), цифри (0-9) і знаки пунктуації. Пароль може складатися із символів лише однієї групи. Під час створення пароля система надає підказку про якість пароля. Крім того Google відкидає поширені паролі.

Таким чином слабкі паролі не приймаються.

Оскільки логін є єдиним для всіх додатків Google– додаткове підтвердження реєстрації не проводиться.

У разі невдалої спроби входу в систему, Google повідомляє користувача, що один елемент з пари логін/пароль є не правильним, проте не уточнює який саме.

Якщо користувач забув свій пароль, йому надається 2 можливі способи для встановлення нового пароля: (1) на захищеній сторінці для встановлення нового пароля, URL якої відправляється на пошту; (2) за допомогою коду, який надсилається на мобільний телефон коротким повідомленням чи може бути повідомлений протягом телефонного дзвінка.

Google запобігає перебору паролів за допомогою вимоги обов'язкового вводу символів із зображення після серії невдалих спроб входу у сервіс.

Google має можливість використання двофакторної автентифікації, ця опція може бути включена в налаштуваннях профілю. Використовуються одноразові коди доступу, що їх можна отримувати на мобільний телефон.

Результати аналізу сервісу GoogleDrive за критерієм «Вхід у систему та реєстрація» наведено в таблиці 13.

Таблиця 13

«Вхід у систему та реєстрація» для сервісу GoogleDrive

Мінімальна довжина пароля	8 символів
Захист від атаки перебору пароля	Використання символів із зображення після серії невдалих спроб входу в сервіс
Двофакторна автентифікація	Пароль та одноразовий код доступу, що передається на мобільний телефон
Механізм відновлення пароля	Надсилається URL сторінки на якій користувач може змінити пароль чи використовує секретний код

2.5.2 Захищений канал зв'язку

В ході аналізу сервісу GoogleDrive був розглянутий принцип забезпечення захищеного каналу зв'язку між клієнтом та сервером, результати наведено у таблиці 14.

Таблиця 14

«Захищений канал зв'язку» для сервісу GoogleDrive

Протокол формування захищеного каналу зв'язку	TLS 1.1
Алгоритм автентифікації повідомлень	RC4_128 (SHA1)
Алгоритм узгодження ключів	ECDHE_ECDSA (256 біт)

2.5.3 Безпека зберігання даних

GoogleDrive не використовує шифрування даних на стороні сервера.Результати аналізу за критерієм "Безпека зберігання даних" наведено в таблиці 15.

Таблиця 15

«Безпека зберігання даних» для сервісу GoogleDrive

Алгоритм шифрування даних	Не використовується

2.6 Порівняльний аналіз сервісів зберігання даних у хмарі

Проаналізувавши сервіси за визначеними критеріями безпеки можна навести наступну підсумкову таблицю 16.

Таблиця 16

Підсумкова оцінка аспектів безпеки

	Вхід в систему та реєстрація	Захищений канал зв'язку	Безпека зберігання даних
Dropbox	±	++	±
Wuala	--	±	++
Яндекс Диск	-	+	--
SkyDrive	++	+	--
GoogleDrive	++	+	--

Кожен критерій безпеки оцінено з використанням таких візуальних позначок:

«++» означає, що всі вимоги виконано; «+» — всі базові вимоги виконано; «±» — більшість вимог виконано, проте є деякі проблеми; «-» — більшість вимог не виконано, «--» — жодна з умов не виконана.

ВИСНОВКИ

Метою роботи є аналіз існуючих широко поширених сервісів зі зберігання інформації в публічній хмарі з точки зору безпеки інформації. Для проведення були відібрані п'ять сервісів, а саме Dropbox, SkyDrive, GoogleDrive, Wuala та Yandex.Disk. Загально визнано, що сервіси Dropbox, SkyDrive та Google Drive є найбільш популярні у світі. Сервіс Yandex.Disk використовується переважно у країнах пострадянського простору. Сервіс Wuala вважається найбільш безпечним та надійним.

Аналіз сервісів зі зберігання інформації в публічній хмарі проводився за такими критеріями:

– вхід у систему та реєстрація;
– захищений канал зв'язку;
– безпека зберігання даних.

Аналіз показав, що з-поміж обраних рішень найвищий рівень безпеки інформації, дійсно, забезпечує сервіс Wuala, проте має певні обмеження на використання та відновлення пароля, найнижчий рівень захисту забезпечується рішенням від Yandex - Yandex.Disk, а сервіси Dropbox, SkyDrive та GoogleDrive можна назвати компромісними рішенням між безпекою інформації, функціональністю та зручністю застосування.

Література

[1] J. W. Rittinghouse, J. F. Ransome, «Cloud Computing: Implementation, Management,andSecurity», 2009, CRC Press – 340 p.

[2] T. Mather, S.Kumaraswamy, S. Latif, «Cloud Security and Privacy: An Enterprise Perspectiveon Risks and Compliance», O'ReillyMedia, 2009.– 334 p.

[3] M. Borgmann, T. Hahn, M. Herfert, T. Kunz, M.Richter, U. Viebeg, S. Vowe, «On the Security of Cloud Storage Services», Fraunhofer Institute SIT, 2012 – 143p.

[4] D. Grolimund, L. Meisser, S. Schmid, R. Wattenhofer, «Cryptree: A folder trees tructure for cryptographic file systems. In Reliable Distributed Systems», SRDS, 2006.

[5] J. R. Douceur, A.Adya, W. J. Bolosky, D.Simon, M. Theimer, "Reclaiming Space from Duplicate Filesin a Server", Fraunhofer Institute SIT, 2012.

Надійшла до редколегії 26.04.2013

Погребняк Костянтин Анатолійович, кандидат технічних наук, доцент кафедри БІТ ХНУРЕ, начальник відділу КЗІ АТ «ІІТ». Наукові інтереси: застосування методів алгебраїчної геометрії в криптології, асиметричний криптоаналіз.

Повтарєв Дмитро Валерійович, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: дослідження механізмів безпеки хмарних обчислень.

УДК 681.3.06

Анализ безопасности сервисов хранения данных в облаке / К.А. Погребняк, Д.В. Повтарев // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 202–208.

Статья посвящена анализу сервисов хранения информации в облаке. Для анализа сервисов определяются критерии безопасности, по которым проводится сравнение. Рассматриваются следующие сервисы: Dropbox, SkyDrive, GoogleDrive, Wuala и Yandex.Disk. Основное внимание уделяется анализу интерактивного входа в систему, регистрации, формированию защищенного канала связи и механизмам безопасности хранения данных.

Ключевые слова: облачные вычисления, сервис хранения информации, безопасность хранения данных.

Табл.: 16. Библиогр.: 5 назв.

UDC 681.3.06

Analysis of security of cloud data storage services / K.A. Pogrebnyak, D.V. Povtariev // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 202–208.

This paper is devoted to analyzing data storage services in the cloud. The security criteria are defined to analyze the services. The paper covers the following services: Dropbox, SkyDrive, GoogleDrive, Wuala and Yandex.Disk. The focus of the analysis is on an interactive login, registration, formation of a secure communication channel and data security mechanisms.

Keywords: cloud computing, information storage service, data storage security.

Tab.: 16. Ref.: 5 items.

СИНТЕЗ И АНАЛИЗ СИМЕТРИЧНЫХ ПРЕОБРАЗОВАНИЙ

UDC 621.3.06

EXTENDED CRITERION FOR ABSENCE OF FIXED POINTS

O. KAZYMYROV

One of the criteria for selecting substitutions used in block ciphers is the absence of fixed points. This paper shows that this criterion must be extended taking into consideration mixing key function. It is shown that modulo addition has more advantages than XOR operation. It is shown in practice that encryption procedure of AES has a natural isomorphic form when fixed points are reached.

Keywords: fixed points, AES, criterion, s-box.

1. INTRODUCTION

Substitution boxes (*S*-boxes) map an n^{th} bit length input message to an m^{th} bit length output message. They provide confusion in symmetric algorithms. For different tasks *S*-boxes are used in various forms. In stream ciphers a substitution is represented usually as a vectorial Boolean function [1]. Permutations constitute a subclass of substitutions and are commonly used in block ciphers as a lookup table. Regardless of ciphers an *S*-box can be converted from one form to another one.

Substitutions must satisfy various criteria for providing high level of security against different types of attacks [2]. A substitution satisfying all criteria is perfect. However, such substitutions don't exist up to date. Therefore, in practice, substitutions satisfying several important criteria are used. They are called optimal *S*-boxes. Optimality criteria vary from cipher to cipher. Generating permutations with optimal criteria is a quite difficult task, especially for a large n an m. The problem is particularly solved by using *EA*- or *CCZ*-equivalence [3, 4].

One of the criteria is absence of fixed points. It is used in many ciphers for increasing resistance against statistical attacks [5]. Designers of modern ciphers try to get rid of the fixed points. This is achieved by using affine equivalence, which is a particular case of *EA*-equivalence. The *S*-box of advanced encryption standard (AES) was constructed using this technique [5, 6]. But the application of this method does not totally prevent the appearance of fixed points. In this paper we show an isomorphic form of AES when fixed points are reached.

Two ciphers E_i and E_j are isomorphic to each other if there exist invertible maps $\varphi: x^i \mapsto x^j$, $\psi: y^i \mapsto y^j$ and $\chi: k^i \mapsto k^j$ such that $y^i = E_i(x^i, k^i)$ and $y^j = E_j(x^j, k^j)$ are equal for all x^i, k^i, x^j and k^j [7, 8]. Obviously, the cipher could have a lot of isomorphic basic transformations as well as full encryption procedures. The cipher BES is a well-known example of isomorphic AES [9]. In [10] an example of isomorphic AES in which the differential probability is higher than in the original cipher was shown. We show another example, which is a special case of isomorphic AES. The new cipher includes a substitution with a fixed point while almost all transformations are unmodified.

2. PRELIMINARIES

Arbitrary substitution can be represented at least in three different forms: algebraic normal form (ANF), over field $\mathcal{F}_{2^n} = GF(2^n)$ and lookup table. Most of substitutions used in block ciphers have a table representation because of simplicity of description and understanding. Meanwhile arbitrary *S*-box S can be always associated with a vectorial Boolean function F in $\mathcal{F}_{2^n}[x]$. If a substitution is a permutation then F is defined uniquely.

The natural way of representing F as a function from $\mathcal{F}_2^n$ to $\mathcal{F}_2^m$ is by its algebraic normal form:

$$\sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right), \quad a_I \in \mathcal{F}_2^m,$$

(the sum is being calculated in $\mathcal{F}_2^m$) [1]. The algebraic degree of F is the degree of its ANF. F is called affine if it has algebraic degree at most 1 and it is called linear if it is affine and $F(0) = 0$. A vectorial Boolean function in table representation can be easily transformed to AFN form and vice versa.

Two functions $F, G: \mathcal{F}_2^n \mapsto \mathcal{F}_2^m$ are called extended affine equivalent (EA-equivalent) if there exist an affine permutation A_1 of $\mathcal{F}_2^m$, an affine permutation A_2 of $\mathcal{F}_2^n$ and a linear function L_3 from $\mathcal{F}_2^n$ to $\mathcal{F}_2^m$ such that

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x). \qquad (1)$$

Clearly, A_1 and A_2 can be presented as $A_1(x) = L_1(x) + c_1$ and $A_2(x) = L_2(x) + c_2$ for some linear permutations L_1 and L_2 and some $c_1 \in \mathcal{F}_2^m$, $c_2 \in \mathcal{F}_2^n$. Two functions F and G are linear equivalent if equation (1) is correct when $L_3 = 0$, $c_1 = 0$, $c_2 = 0$. If the equation (1) is preserved only for $L_3 = 0$, then functions F and G are called affine equivalent [11].

In matrix form *EA*-equivalence is represented as follows

$$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus M_3 \cdot x \oplus V_1.$$

where elements of $\{M_1, M_2, M_3, V_1, V_2\}$ have dimensions $\{m \times m, n \times n, m \times n, m, n\}$ [3].

An element $a \in \mathcal{F}_2^n$ is a fixed point of $F : \mathcal{F}_2^n \mapsto \mathcal{F}_2^m$ if $F(a) = a$. The absence of fixed points criterion is defined as follows.

Definition 1. A substitution must not have fixed point, i.e.

$$F(a) \neq a, \quad \forall a \in \mathcal{F}_2^n.$$

For any positive integers *n* and *m*, a function *F* from $\mathcal{F}_2^n$ to $\mathcal{F}_2^m$ is called differentially δ-uniform if for every $a \in \mathcal{F}_2^n \setminus \{0\}$ and every $b \in \mathcal{F}_2^m$, the equation $F(x) + F(x+a) = b$ admits at most δ solutions [1]. Vectorial Boolean functions used as *S*-boxes in block ciphers must have low differential uniformity to allow high resistance to differential cryptanalysis [12].

The nonlinearity criterion is closely connected to the notion of Walsh transform, which can be described as a function

$$\lambda(u,v) = \sum_{x \in \mathcal{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x},$$

where " $\cdot$ " denotes inner products in $\mathcal{F}_2^n$ and $\mathcal{F}_2^m$ respectively [1]. A substitution has an optimum resistance to linear cryptanalysis if the maximum absolute value of Walsh coefficients is small [13]. Substitutions with the limit values of $\lambda(u,v)$ exist for odd *n* only.

These two criteria are major while selecting substitutions for new ciphers. However, there are many others criteria like propagation criterion, absolute indicator, correlation immunity, strict avalanche criterion, etc [1, 2, 14]. It has been still not proven the importance of the criteria. For example, the substitution used in AES doesn't satisfy most of them. No practical attacks were proposed on block cipher based on the most of these criteria.

Let $E : \{0,1\}^l \times \{0,1\}^k \mapsto \{0,1\}^l$ be a function taking a key *K* of length *k* bits and input message (plaintext) *M* of length *l* bits to return output message (ciphertext) $E(M,K)$. For each key *K* let $E_K : \{0,1\}^l \times \{0,1\}^l$ be the function defined by $E_K(M) = E(M,K)$. Than *E* is a block cipher if E_K and E_K^{-1} are efficiently computable, and E_K is a permutation for every *K*.

Most of the modern block ciphers are based on an iterative procedure. In Figure 1 the iterative function is depicted as the round function.

A general iterative cipher can be mathematically presented as follows

$$E_K(M) = PW_{k_r+1} \circ \bigcirc_{i=2}^{r} \left(R_{k_i}\right) \circ IW_{k_1}(M),$$

where *R* is a round procedure, *IW* is a prewhitening procedure and *PW* is a postwhitening procedure. In Figure 1 a key schedule is an algorithm that takes the master key (*K*) as input and produces the subkeys $(k_1, k_2, \ldots, k_{r+1})$ for all stages of encryption algorithm.

A mixing key procedure of a block cipher is an algorithm, which injects a round key into an encryption procedure. For the majority of the modern block ciphers, the mixing key function is implemented as exclusive or (XOR) operation because of implementation simplicity.

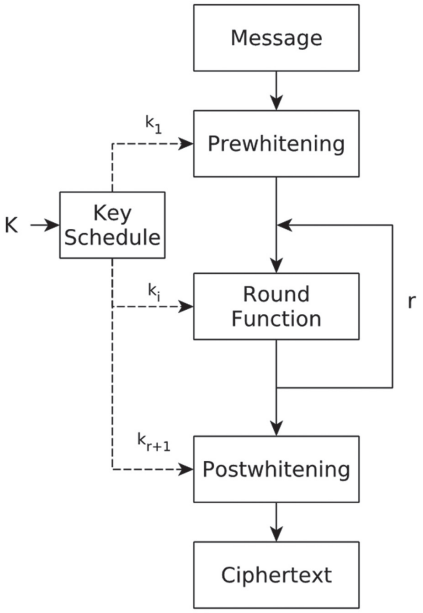


Fig. 1. General structure of an iterative block cipher

3. A BRIEF DESCRIPTION OF AES

AES is a substitution permutation network (SPN) block cipher that supports a fixed block size of 128 bits and a key size of 128, 192 or 256 bits [6]. The number of rounds depends on the key size and is equal to 10, 12 or 14 respectively. The round function consists of four functions: AddRoundKey (σ_k), SubBytes (γ), ShiftRows (π) and MixColumns (θ).

The whole encryption algorithm is described as follows (Figure 2)

$$E_K(M) = \sigma_{k_r+1} \circ \pi \circ \gamma \circ \bigcirc_{i=2}^{r} \left(\sigma_{k_i} \circ \theta \circ \pi \circ \gamma\right) \circ \sigma_{k_1}(M).$$

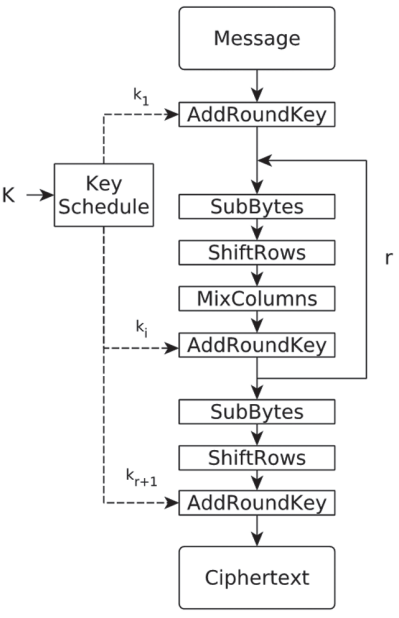


Fig. 2. Encryption algorithm of AES

The SubBytes transformation processes the state of the cipher using a nonlinear byte substitution table that operates on each of the state bytes independently [6]. The *S*-box of AES was generated by finding the inverse element in the field $\mathcal{F}_{2^8}$ followed by applying affine polynomial. In terms of equation (1) the transformation has a form

$$F(x) = A_1(x^{-1}) = L_1(x^{-1}) + c_1.$$

The substitution table generated by vectorial Boolean function $F : \mathcal{F}_{2^8} \mapsto \mathcal{F}_{2^8}$ satisfies the following criteria:

– the maximum value of non-trivial XOR difference transformation probability is 2^{-6};

– the maximum absolute value of linear approximation probability bias is 2^{-4};

– the minimum degree of the component functions is 7 [5, 15].

It should be noticed that the chosen polynomial x^{-1} allows to describe the *S*-box and the whole cipher by overdefined system of equations with degree 2 [16]. But in the same time it is resistant to differential, linear and other statistical methods of cryptanalysis. Additional to general properties the constant of the AES *S*-box has been chosen in such way that it has no fixed points.

The MixColumns transformation takes all of the columns of the state and mixes their data (independently of one another) to produce new columns [6]. This transformation could be represented in different ways. One of them is the matrix multiplication. For 4×4 matrix *m* and input state *x* the output state *y* of the transformation is described as

$$y = M \cdot x.$$

The matrix *M* with maximum distance separable (MDS) property is used in AES. The MDS property associates with a branch number (β)

$$\beta = \min_{x \neq 0}(W(x) + W(M \cdot x)),$$

where $W(z)$ is the Hamming weight of a byte vector z.

From the definition of MDS matrix, it is known that the maximum differential branch number of *m* by *m* MDS matrix is $m+1$ [17]. Hence, MDS matrices have the perfect diffusion property for byte-oriented ciphers.

Multiplication in a filed $\mathcal{F}_{2^n}$ is a linear transformation with respect to XOR, so MixColumns transformation preserves the linear property [9]

$$\theta(x + y) = \theta(x) + \theta(y).$$

The ShiftRows transformation processes the state by cyclically shifting the last three rows of the state by different offsets [6]. More precisely, row *i* is moved to the left by *i* byte positions for $0 \le i \le 3$. The ShiftRows is also a linear function that preserves $\pi(x + y) = \pi(x) + \pi(y)$ property.

Both MixColumns and ShiftRows transformations help to ensure that the number of active *S*-boxes is large even after few rounds [5]. These functions are the basis of the security offered by the AES against differential and linear cryptanalysis.

AddRoundKey transformation is the mixing key function in which a round key is added to the state using XOR operation. The length of a round key equals the size of the state. XOR operation of two *n*-bit length vectors *a* and *b* can be performed bit by bit *n* times. Therefore, AddRoundKey operation of AES can be done independently of each byte.

4. A NEW CIPHER ISOMORPHIC TO AES

There exist several examples of ciphers isomorphic to AES. For example, the big encryption system (BES) describes AES over $\mathcal{F}_{2^8}$ [9]. The cipher AES can be also represented as the system of multivariate equations of the 2nd degree over $\mathcal{F}_2$ [16]. These two examples are based on the algebraic features of the substitution. But there is another approach based on linear properties of the basic functions (i.e. MixColumns and ShiftRows).

The cipher AES is based on Rijndael that was proposed by Daemen and Rijmen to AES process [18]. Authors have used design simplicity principle, which led to performance improvement and code compactness properties of the cipher on a wide range of platforms. For increasing decryption performance of software implementation they use precomputed lookup tables and the linear properties of basic functions.

The original decryption algorithm for arbitrary ciphertext *C* mathematically can be represented as follows (Figure 3) [6]

$$D_K(C) = \sigma_{k_1} \circ \gamma^{-1} \circ \pi^{-1} \circ \bigcirc_{i=2}^{r} \left(\theta^{-1} \circ \sigma_{k_{r-i+2}} \circ \gamma^{-1} \circ \pi^{-1}\right) \circ \sigma_{k_{r+1}}(C).$$

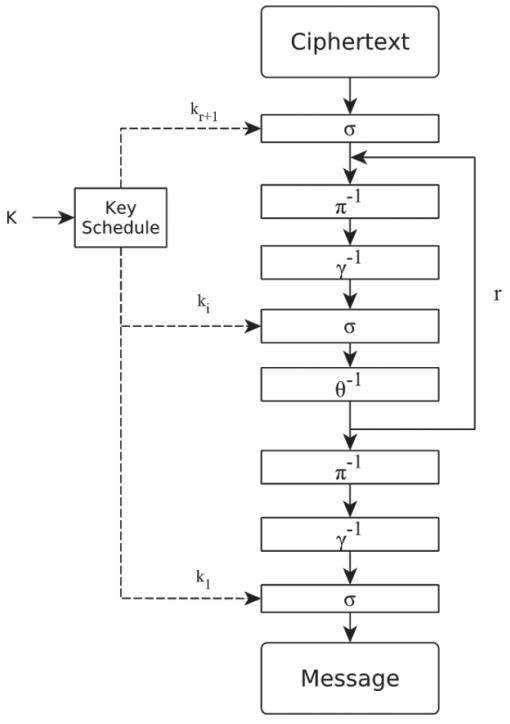


Fig. 3. Decryption algorithm of AES

For using the precomputed tables it is necessary to transform the decryption round function to the similar one of encryption algorithm. Since the functions γ^{-1} and π^{-1} are computed independently they have a commutative property $\gamma^{-1} \circ \pi^{-1} = \pi^{-1} \circ \gamma^{-1}$ [5, 9]. In Section 3 it was stated that the functions θ^{-1} and σ are linear hence

$$\theta^{-1} \circ \sigma_{k_{r-i+2}} = \sigma_{\theta^{-1}(k_{r-i+2})} \circ \theta^{-1}$$

Thus, the whole decryption algorithm has the form (Figure 4)

$$D_K(C) = \sigma_{k_1} \circ \pi^{-1} \circ \gamma^{-1} \circ \bigcirc_{i=2}^{r} \left(\sigma_{\theta^{-1}(k_{r-i+2})} \circ \theta^{-1} \circ \pi^{-1} \circ \right.$$
$$\left. \circ \gamma^{-1} \right) \circ \sigma_{k_{r+1}}(C).$$

The usage of such elementary transformations helps to achieve a significant acceleration of the decryption procedure due to the isomorphic properties of the basic functions [5].

Obviously, the same technique can be applied to the encryption algorithm. However, our task is to find a representation of the cipher in which properties of a new substitution will differ from the original one.

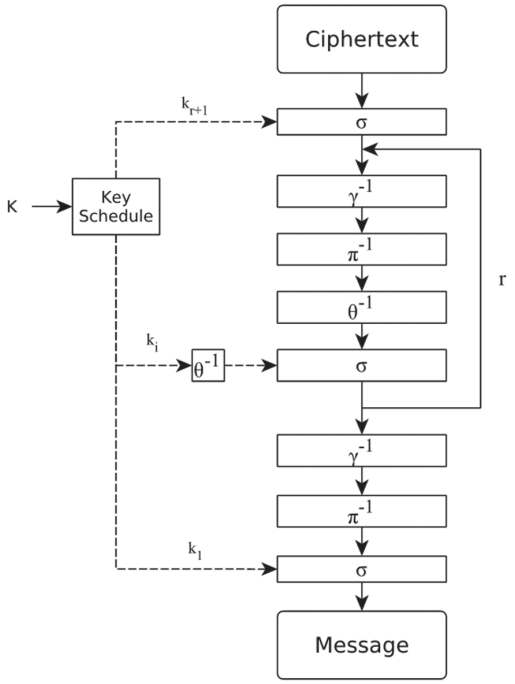


Fig. 4. Algorithm for fast software implementation

For simplicity of description, let us assume that the round keys are independent of each other. Then the encryption procedure takes a form (Figure 5)

$$E_K(M) = \pi \circ \sigma_{\pi^{-1}(k_r+1)} \circ \gamma \circ \bigcirc_{i=2}^{r} \left(\theta \circ \pi \circ \sigma_{\pi^{-1} \circ \theta^{-1}(k_i)} \circ \right.$$
$$\left. \circ \gamma \right) \circ \sigma_{k_1}(M)$$

The equation shows that the last ShiftRows operation is redundant in terms of resistance to attacks. As it was stated above the availability of this function is necessary for fast implementation of the decryption procedure.

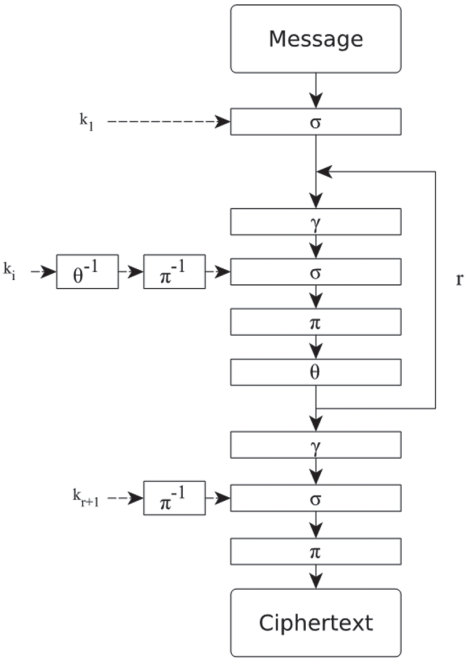


Fig. 5. Modified encryption algorithm

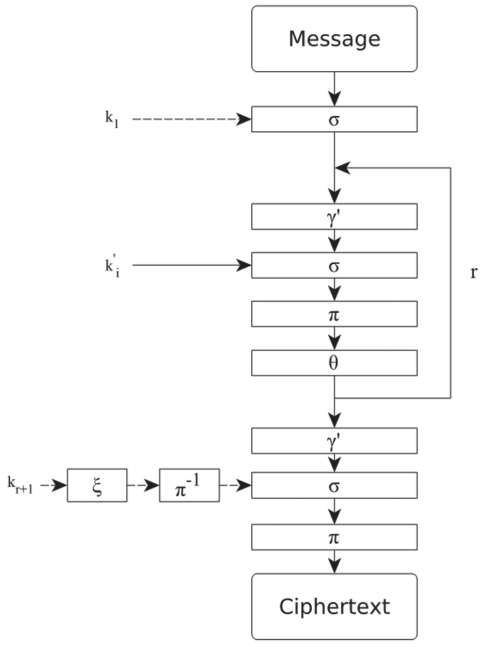


Fig. 6. Isomorphic encryption algorithm with a fixed point

Since arbitrary permutation S can be represented as vectorial Boolean function $F : \mathcal{F}_{2^n} \mapsto \mathcal{F}_{2^n}$ then it can take the form [3]

$$F(x) = F'(x) + F(0).$$

The substitution of AES has more simple form than $F(x) = L(x^{-1}) + c$, where $c = F(0)$. Since the characteristic of the field is 2, the constant can be moved to the round keys. Let ξ be a function in which the constant c is XORed with all bytes of a state. If the round keys $\pi^{-1} \circ \theta^{-1} \circ \xi(k_i)$ are denoted by k_i' than encryption procedure takes the form (Figure 6)

$$E_K(M) = \pi \circ \sigma_{\pi^{-1} \circ \xi(k_r+1)} \circ \gamma' \circ \bigcirc_{i=2}^{r} \left(\theta \circ \pi \circ \sigma_{k_i'} \circ \gamma' \right) \circ \circ \sigma_{k_1}(M),$$

where γ' is the SubBytes function consists of substitutions of the form $F(x) = L(x^{-1})$.

Figure 6 shows that the structure of the cipher remains unchanged. Clearly, if adversary finds a round key for modified cipher she also automatically obtains corresponding round key of the original cipher because of the linear correspondence between the keys k_i and k_i'. However, the new substitution $F(x) = L(x^{-1})$ has the fixed point in $x = 0$. Consequently, the substitution of AES doesn't satisfy the absence of fixed points criterion.

Described feature of the cipher appears from the fact that the operation XOR is linear with respect to MixColumns and ShiftRows. If we replace the mixing key function with some nonlinear function (i.e. addition modulo 2^{32}), then it would be impossible to find an isomorphic cipher of such form. Therefore, a mixed key function based on modulo addition is cryptographically stronger than a function based on XOR operation.

Furthermore, fixed points are directly connected with cyclic properties of substitutions. Inserting an invertible linear function (τ) into the encryption procedure gives a new isomorphic cipher (Figure 7). Herewith, the linearized polynomial can be added to the round key and the inverse function can be part of the new substitution (Figure 8). The cyclic properties of the new substitution will depend on the selected function τ.

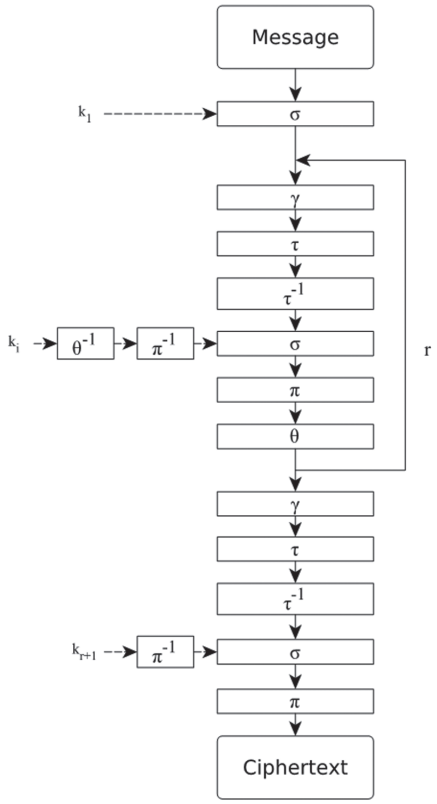


Fig. 7. Modified AES with an invertible linear function

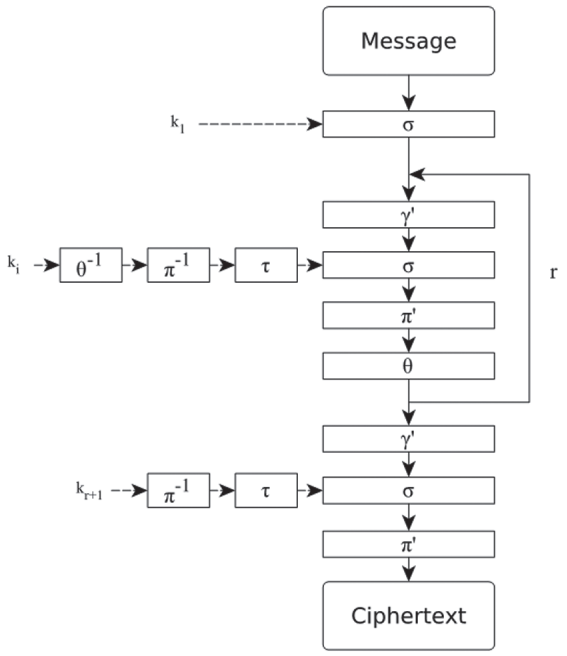


Fig. 8. Isomorphic cipher of modified AES with an invertible linear function

Thereby, adversary in the case of a linear mixing key function can control the cyclic and the absence of fixed points properties of a substitution. Thus, a new criterion for substitutions follows from the description above.

Definition 2. *Substitutions* $S_1, S_2, \ldots, S_n$ *used in diffusion layer must belong to different classes of equivalence.*

Clearly, if substitutions are in the same class (i.e. EA-equivalent) then adversary can find an isomorphic cipher, which consists of one substitution and modified linear layer. So there will be no advantages to use multiple substitutions. The criterion have to be considered both in the design of new ciphers and in the analysis of existing ones [19, 20]. Since CCZ-equivalence is the most general case of known equivalence, it makes sense to check whether substitutions belong to different CCZ-equivalence classes.

5. CONCLUSIONS

It was shown that the absence of fixed points criterion works only in the case if *S*-box is considered as a separate function. There are isomorphic representations of ciphers in which this criterion is not met. This may lead to a weakening of the cipher strength. The method of AES description gives a tool for attacking the cipher, which has been practically secure more than decade.

Since the adversary can add arbitrary invertible linear function to encryption procedure, the cyclic properties also are not important for substitutions. It was shown that mixing key function based on modulo addition is more resistant with respect to the absence of fixed points criterion than function based on XOR operation.

Isomorphism of ciphers adds further restrictions on using multiple substitutions. The proposed

criterion can be used to reduce the number of isomorphic ciphers, thereby reducing the probability of finding the weakest algorithm.

References

[1] Y. Crama and P.L. Hammer. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications v. 2. Cambridge University Press,= 2010. isbn: 9780521847520.

[2] Vincent Rijmen. “Cryptanalysis and design of iterated block ciphers”. Doc- toral thesis. K.U.Leuven, 1997.

[3] Lilya Budaghyan and Oleksandr Kazymyrov. “Verification of Restricted EA-Equivalence for Vectorial Boolean Functions”. In: Arithmetic of Finite Fields. Ed. by Ferruh Ozbudak and Francisco Rodrguez-Henrquez. Vol. 7369. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 108–118. isbn: 978-3-642-31661-6. doi: 10.1007/978-3-642-31662- 3_8.

[4] Claude Carlet, Pascale Charpin, and Victor Zinoviev. “Codes, Bent Func- tions and Permutations Suitable For DES-like Cryptosystems”. In: Des. Codes Cryptography 15.2 (1998), pp. 125–156.

[5. J. Daemen and V. Rijmen. “AES proposal: Rijndael”. In: First Advanced Encryption Standard (AES) Conference. 1998.

[6] National Institute of Standards and Technology. ADVANCED ENCRYP- TION STANDARD (AES). FIPS-197. U.S. DoC/National Institute of Standards and Technology, 2001, pp. 1–47.

[7] Alexander Rostovtsev. Changing probabilities of differentials and linear sums via isomorphisms of ciphers. Cryptology ePrint Archive, Report 2009/117. 2009.

[8] A. Rimoldi. “On algebraic and statistical properties of AES-like ciphers”. PhD thesis. University of Trento, 2009.

[9] Sean Murphy and Matthew J. B. Robshaw. “Essential Algebraic Structure within the AES”. In: Proceedings of the 22nd Annual International Cryp- tology Conference on Advances in Cryptology. CRYPTO ’02. London, UK, UK: Springer-Verlag, 2002, pp. 1–16. isbn: 3-540-44050-X.

[10] Alexander Rostovtsev. Virtual isomorphisms of ciphers: is AES secure against differential/linear attack? Cryptology ePrint Archive, Report 2012/663. 2012.

[11] L. Budaghyan, C. Carlet, and A. Pott. “New classes of almost bent and al- most perfect nonlinear polynomials”. In: Information Theory, IEEE Trans- actions on 52.3 (2006), pp. 1141–1152.

[12] Eli Biham and Adi Shamir. “Differential Cryptanalysis of DES-like Cryp- tosystems”. In: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology. CRYPTO ’90. London, UK, UK: Springer-Verlag, 1991, pp. 2–21. isbn: 3-540-54508-5.

[13] Mitsuru Matsui. “Linear cryptanalysis method for DES cipher”. In: Work- shop on the theory and application of cryptographic techniques on Advances in cryptology. EUROCRYPT ’93. Lofthus, Norway: Springer-Verlag New York, Inc., 1994, pp. 386–397. isbn: 3-540-57600-2.

[14] Linda Dee Burnett. “Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography”. PhD thesis. Queensland University of Technology, 2005.

[15] K. Nyberg. “Perfect nonlinear S-boxes”. In: Advances in CryptologyEU- ROCRYPT91. Springer. 1991, pp. 378–386.

[16] Nicolas Courtois and Josef Pieprzyk. “Cryptanalysis of Block Ciphers with Overdefined Systems of Equations”. In: Proceedings of the 8th Interna- tional Conference on the Theory and Application of Cryptology and Infor- mation Security: Advances in Cryptology. ASIACRYPT ’02. London, UK, UK: Springer-Verlag, 2002, pp. 267–287. isbn: 3-540-00171-9.

[17] Wang Ailan, Li Yunqiang, and Zhang Xiaoyong. “Analysis of Correspond- ing Structure of Differential Branch of MDS Matrixes on Finite Field”. In: Proceedings of the 2010 Third International Conference on Intelligent Net- works and Intelligent Systems. ICINIS ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 381–384. isbn: 978-0-7695-4249-2.

[18] J. Nechvatal et al. Report on the development of the Advanced Encryption Standard (AES). Tech. rep. DTIC Document, 2000.

[19] Daesung Kwon et al. “New Block Cipher: ARIA”. In: Information Security and Cryptology - ICISC 2003. Ed. by Jong-In Lim and Dong-Hoon Lee. Vol. 2971. Lecture Notes in Computer Science. Springer Berlin / Heidel- berg, 2004, pp. 432–445. isbn: 978-3-540-21376-5.

[20] Roman Oliynykov et al. Results of Ukrainian National Public Crypto- graphic Competition. http://www.sav.sk/journals/uploads/0317154006ogdr. pdf. 2012.

Manuscript received March, 5, 2013

Kazymyrov Oleksandr Vladimirovich, post-graduate student of information technologies security department at KNURE. Scientific interests: symmetric cryptography and cryptanalysis, vectorial Boolean functions.

УДК 621.3.06

Расширенный критерий для отсутствия фиксированных точек / О.В. Казимиров // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 209–214.

Одним из критериев для выбора подстановок, используемых в блочных шифрах+, является отсутствие неподвижных точек. В статье показано, что этот критерий необходимо расширить, принимая во внимание функцию смешивания ключа. Показано, что использование модульного сложения более предпочтительно, чем XOR. На практике продемонстрировано, что шифрующее преобразование AES имеет изоморфную форму, в которой присутствуют неподвижные точки.

Ключевые слова: фиксированные точки, AES, критерий, s-бокс.

Ил.: 8. Библиогр.: 20 назв.

УДК 621.3.06

Розширений критерій для відсутності фіксованих точок / О. Казиміров // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 209–214.

Одним із критеріїв для вибору підстановок, що використовуються у блокових шифрах, є відсутність нерухомих точок. У статті показано, що цей критерій треба розширити, приймаючи до уваги схему розгортання ключа. Показано, що використання модульного додавання краще, ніж XOR. На практиці продемонстровано, що шифруюче перетворення AES має ізоморфну форму, в якій присутні нерухомі точки.

Ключові слова: фіксовані точки, AES, критерій, s-бокс.

Іл.: 8. Бібліогр.: 20 найм.

УДК 621. 391:519.2:519.7

О МЕТОДЕ ДОКАЗАТЕЛЬСТВА СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ К АТАКЕ НЕВЫПОЛНИМЫХ ДИФФЕРЕНЦИАЛОВ

В.И. РУЖЕНЦЕВ

Анализируются существующие методы поиска невыполнимых дифференциалов. Предлагается метод, который позволяет обосновать отсутствие невыполнимых дифференциалов. Сложность метода, в отличие от известных, в меньшей степени зависит от размера блока. Метод применяется к Rijndael-подобным SPN шифрам и фейстель-подобным шифрам.

Ключевые слова: блочный шифр, атака невыполнимых дифференциалов, невыполнимый дифференциал, Rijndael-подобные преобразования.

ВВЕДЕНИЕ

Атака невыполнимых дифференциалов (НД) является одним из наиболее эффективных нападений на современные блочные симметричные шифры (БСШ). Этот криптоаналитический метод успешно позволяет атаковать как SPN-шифры [1–3], так и шифры, построенные с использованием цепи фейстеля [4–7] и других структур. Для шифра Rijndael с уменьшенным количеством циклов данную атаку можно считать одной из самых успешных. Подтверждением сказанного является большое количество работ, появившихся за последнее десятилетие и направленных, главным образом, на поиск невыполнимых дифференциалов [1–11]. Целью настоящей работы является рассмотрение существующих подходов к оценке стойкости БСШ к атаке невыполнимых дифференциалов, а также предложение еще одного подхода, который, как будет показано в работе, в ряде случаев является полезным. Например, как будет продемонстрировано, предлагаемый подход позволяет обосновать стойкость группы Rijndael-подобных шифров с 4-мя и более циклами к атаке НД, а также стойкость шифров, использующих цепь фейстеля.

1. ОБЩАЯ ХАРАКТЕРИСТИКА АТАКИ. ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ

Атака НД впервые была предложена Э. Бихамом в [4,5] для шифров SkipJack, IDEA, Khufu. Позже оказалось, что атака НД применима и для других шифров, в том числе и для шифра AES с 5 циклами [1].

Атака НД на блочные симметричные шифры, как большинство криптоаналитических нападений, относится к классу атак на цикловую функцию, и для ее реализации необходимо иметь некоторое количество пар — открытый текст–криптограмма, полученных на одном и том же секретном ключе.

Данная криптоаналитическая методика называется атакой невыполнимых дифференциалов, поскольку в атаке используются дифференциалы специального вида – те, которые не могут выполняться, т. е. имеющие нулевую вероятность. Атака невыполнимых дифференциалов на r-цикловой шифр обычно становится возможной, когда имеется (r-1)-цикловой невыполнимый дифференциал.

При наличии (r-1)-циклового НД с входной разностью $\Delta_{НДвх}$ и выходной разностью $\Delta_{НДвых}$ атака на r-цикловой шифр состоит из следующих шагов. Выполняется поиск пары с выходной разностью $\Delta_{НДвых}$. Если такая пара найдена, то, в соответствии с НД, после первого цикла не могла быть разность $\Delta_{НДвх}$. И все ключи первого цикла, которые будут приводить к этой разности после одноциклового шифрования, являются неверными. Путем отсева всех неверных ключей определяется правильный подключ первого цикла.

Один из вариантов атаки – атака байтовых или усеченных невыполнимых дифференциалов – была предложена в работах [1, 2, 6]. В ходе атаки через преобразования шифра пытаются провести вектора активизации. Каждый бит вектора активизации отражает активность одного байта в обычной разности. Таким образом, вектор активизации содержит столько битов, сколько байтов в блоке, а значение бита определяется активностью байта: «1» – байт активный, «0» – байт пассивный.

В остальной части работы будем, главным образом, обсуждать байтовые НД.

2 АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ПОИСКА НД

2.1 Известные НД для структур, которые используются в БСШ

Для многих структур, которые часто используются при построении БСШ, известны НД. В полной мере это относится к цепи фейстеля. В работе [5] упоминается о том, что если в фейстель-подобном шифре используется биективная шифрующая функция, то всегда существует 5-цикловой НД, который имеет вид (a, 0) $\rightarrow$ (a, 0) для любой ненулевой разности a.

Из работ [1] известно о наличии 4-цикловых НД для Rijndael-подобных БСШ с сокращенным последним циклом. Входная разность в таком НД содержит один активный байт, а выходная – пассивные байты (с нулевой разностью) на позициях, которые соответствуют минимум одной

пассивной колонке (все байты колонки содержат нулевую разность) до преобразования ShiftRow.

Известен также ряд работ, посвященных исследованию НД для различных обобщенных цепей фейстеля [8, 11].

В работе [10] представлены критерии наличия НД для Rijndael-подобных БСШ с различным числом циклов.

В целом, если в шифре используется одна из структур, для которой известно о наличии НД, то НД с аналогичной входной и выходной разностями может существовать и для этого шифра. Однако для таких шифров может существовать и НД для значительно большего количества циклов, следовательно, требуется более подробное исследование. Так, например, для фейстельподобного шифра Camellia, который использует цепь фейстеля, а значит – существует 5-цикловый НД, в процессе анализа были найдены 8-цикловые НД [7].

2.2 Расхождение посередине (miss-in-the-middle)

В работе [5] упоминается о достаточно универсальном подходе к построению НД для БСШ. Подход заключается в поиске двух достоверных дифференциалов (вероятность каждого равна 1), первый из которых определяет движение разности в первой половине шифра в прямом направлении, а второй – во второй половине шифрующих преобразований в обратном направлении. Если конечные разности таких достоверных дифференциалов не равны, то расхождение дифференциалов дает НД.

Используя данный подход построены многие из известных НД, в том числе и все представленные в предыдущем подразделе. Данный подход не редко используется для доказательства стойкости БСШ к атаке НД, хотя о строгом доказательстве невозможности построения НД другими способами не известно.

2.3 Поиск НД полным перебором

Интересный подход к поиску НД был предложен в [5]. Для шифра создавалась уменьшенная модель (уменьшенный размер блока и ключа) и путем перебора всех возможных входных разностей и ключей выполнялся поиск НД. Затем результаты поиска анализировались и выполнялась попытка построения НД для полноразмерного шифра.

Основной недостаток метода заключается в том, что свойства уменьшенной модели и полноразмерного шифра могут существенно отличаться и доказать обратное очень сложно. Поэтому и структура НД для шифров тоже может иметь существенные отличия, а отсутствие или присутствие НД для уменьшенной модели не гарантируют того же для полноразмерного шифра.

2.4 U и UID методы поиска НД

Попытка автоматизировать процесс поиска НД сделана в работах [8, 9]. Методы действуют в соответствии с принципом miss-in-the-middle. Путем полного перебора разностей выполняется поиск достоверных усеченных (байтовых) дифференциалов для обоих половин шифрующих преобразований, а затем проверяется совместимость этих дифференциалов. В случае несовместимости найден НД.

Недостаток методов – значительное увеличение сложности с ростом размера блока и числа циклов в шифре. Для шифров, которые сегодня используются при построении хеш-функций (размер блока 512 или 1024 бита) эти методы не будут работать.

3. ПРЕДЛАГАЕМЫЙ ПОДХОД

В отличие от большинства известных подходов, которые направлены на поиск НД, наш подход направлен на обоснование отсутствия НД. В основе лежит следующая теорема.

Теорема 1. Если для БСШ существует некоторая разность Δ, которая может быть получена из любой ненулевой входной разности за r_1 циклов преобразований и которая может быть получена из любой ненулевой выходной разности за r_2 циклов, выполняемых в направлении дешифрования, то для такого БСШ не существует НД с r_1+r_2 и более циклами.

Доказательство. Справедливость теоремы достаточно очевидна, т. к. если любая входная разность и любая выходная разность могут прийти к промежуточному значению разности Δ, то возможен переход любой входной разности в любую выходную разность, а это значит, что не существует НД. Теорема доказана.

Таким образом, для доказательства отсутствия НД необходимо определить количество циклов r_1 и r_2, за которые любая входная разность и любая выходная могут прийти к некоторому значению разности Δ.

Когда речь идет о байтовой разности, то Δ обычно содержит сразу все активные байты (вектор активизации состоит из всех «1»).

С помощью теоремы 1 можно, например, объяснить отсутствие НД для многих Rijndaelподобных шифров, в том числе для шифра Rijndael со 128 битным блоком. Коротко напомним основные особенности строения таких шифров, а затем продемонстрируем обоснование отсутствия НД.

4. АНАЛИЗ RIJNDAEL-ПОДОБНЫХ ШИФРОВ

В настоящей работе рассматриваются Rijndael-подобные шифры, т. е. алгоритмы шифрования, которые содержат в каждом цикле (даже в последнем) четыре вида преобразований аналоги преобразований шифра Rijndael: ByteSub (BS), ShiftRow(SR), MixColumns (MC) и AddKey. В зависимости от размера блока может меняться количество и размер колонок, из которых состоит блок (рис. 1).

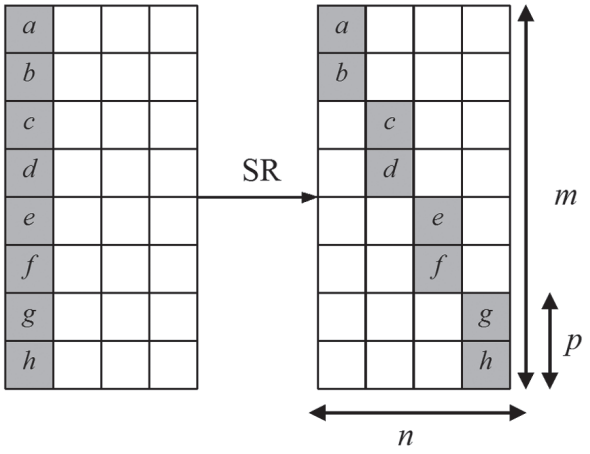


Рис. 1

Когда количество колонок n больше количества строк m, то операция ShiftRow выполняет циклический сдвиг каждой строки на различное количество байтов. В результате операции каждая колонка будет содержать не более одного байта из каждой колонки до преобразования. Для всех вариантов шифра Rijndael [12] выполняется условие $n \geq m$.

Когда $m \geq n$, то количество байтов, которые из одной исходной колонки будут поступать в одну колонку на выходе преобразования ShiftRow, будем обозначать p (см. рис. 1).

В этих случаях всегда выполняется $m = np$.

Такая схема преобразований используется в шифре «Калина» [13].

Прежде чем перейти к рассмотрению стойкости Rijndael к атаке рассмотрим особенности преобразования MixColumns, т. к. именно это преобразование вносит неопределенность в прохождение векторов активизации через циклы шифра. В работе [14] проведен анализ этого преобразования и определены правила определения вероятностей переходов векторов активизации через MixColumns. В табл. 1 и 2 для преобразования MixColumns, которое покрывает 4 и 8 байтов, соответственно, представлены двоичные логарифмы от вероятностей перехода векторов активизации через MixColumns для различного числа активных битов на входе (меняется по столбцам) и выходе (по строкам).

В табл. 1 и 2 переходы, обладающие вероятностью 0, отмечены прочерками.

Справедливо следующее утверждение.

Утверждение 1. Для Rijndael-подобных шифров с блоком, в котором строк не меньше, чем колонок ($m > n$), не существует байтовых НД для 4 и более циклов с полным набором преобразований.

Доказательство. Для доказательства утверждения необходимо показать, что разность с одновременно всеми активными байтами может быть получена при любой начальной разности как после двухциклового зашифрования, так и после двухциклового расшифрования. В этом случае выполняется теорема 1.

Таблица 1

Двоичный логарифм от вероятности перехода вектора активизации через 4-байтный MixColumns

Выход / Вход	0	1	2	3	4
0	0	–	–	–	–
1	–	–	–	–	0
2	–	–	–	–7,99	–0,023
3	–	–	–15,99	–8,017	–0,0226
4	–	–23,983	–16,0115	–8,0171	–0,0226

Таблица 2

Двоичный логарифм от вероятности перехода вектора активизации через 8-байтный MixColumns

Вых. / Вх.	0	1	2	3	4	5	6	7	8
0	0	-	-	-	-	-	-	-	-
1	-	-	-	-	-	-	-	-	0
2	-	-	-	-	-	-	-	-7,99	-0,046
3	-	-	-	-	-	-	-15,9	-8,04	-0,045
4	-	-	-	-	-	-23,9	-16,0	-8,04	-0,045
5	-	-	-	-	-31,9	-24,0	-16,0	-8,04	-0,045
6	-	-	-	-39,9	-32,0	-24,0	-16,0	-8,04	-0,045
7	-	-	-47,9	-40,0	-32,0	-24,0	-16,0	-8,04	-0,045
8	-	-55,9	-48,0	-40,0	-32,0	-24,0	-16,0	-8,04	-0,045

Двухцикловое зашифрование содержит последовательность преобразований: MC, SR, MC; а двухцикловое расшифрование – последовательность тех же обратных преобразований: MC^{-1}, SR^{-1}, MC^{-1}.

Рассмотрим двухцикловое зашифрование. Любая ненулевая усеченная (байтовая) разность имеет по крайней мере одну активную колонку на входе первого преобразования MC. В соответствии с табл. 1 и 2, для любой ненулевой входной разности всегда может быть получена на выходе MC разность со всеми активными байтами. Преобразование SR распространит активные байты этой колонки на все без исключения остальные колонки (поскольку $m > n$). Завершающее преобразование MC всегда может преобразовать такую разность на входе в разность со всеми активными байтами. Аналогичные рассуждения справедливы и для двухциклового расшифрования. Утверждение доказано.

Полученный результат полностью согласуется с известными результатами для шифра Rijndael со 128-битным блоком, т. к. наилучшие НД, которые были найдены или использованы в известных работах, покрывают 3 полных и один (последний) неполный циклы [3].

Для Rijndael-подобных шифров с блоком, в котором строк меньше, чем колонок ($m < n$), для того, чтобы гарантировать отсутствие НД, потребуется, по крайней мере, два дополнительных цикла преобразований (по одному с каждой стороны). То есть, для таких шифров можно говорить об отсутствии НД не менее, чем для 6 полных циклов.

5. АНАЛИЗ ШИФРОВ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЦЕПИ ФЕЙСТЕЛЯ

Схема фейстеля – одна из наиболее распространенных схем современных БСШ. В качестве шифра, стойкость которого будем исследовать, взят алгоритм, который рассматривался в работе [17]. В каждом цикле выполняется SL-преобразование, схема которого представлена на рис. 2.

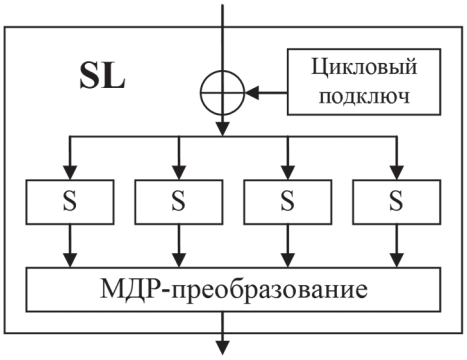


Рис. 2

Важным моментом является то, что МДР-преобразование (аналог MixColumn в Rijndael-подобных шифрах) охватывает весь обрабатываемый полублок. Поэтому за один цикл такое SL-преобразование может любую ненулевую разность на входе трансформировать в разность со всеми активными байтами в полублоке на выходе (см. табл. 1 и 2). Общая схема трех циклов преобразований представлена на рис. 3.

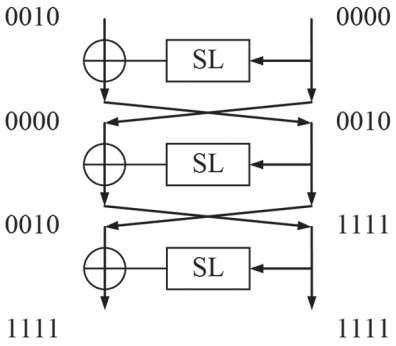


Рис. 3

Используя теорему 1, покажем справедливость следующего утверждения.

Утверждение 2. Для рассматриваемого шифра (схема фейстеля и в цикловом преобразовании МДР-преобразование покрывает весь полублок) не существует НД, покрывающих 6 и более циклов.

Доказательство. Для доказательства утверждения необходимо показать, что за 3 цикла любая начальная разность может быть преобразована в разность с одновременно всеми активными байтами.

Первый цикл может содержать тривиальный переход нулевой разности через первое SL-преобразование (см. рис. 3). Тогда, независимо от вида начальной разности в левом полублоке, на вход SL-преобразования второго цикла поступит ненулевая разность (содержит, по крайней мере, один активный байт). В соответствии с вероятностями переходов из табл. 1, выход такого SL-преобразования всегда может содержать сразу все активные байты для всего полублока независимо от входного значения (для всех ненулевых входных разностей последняя колонка табл. 1 содержит значения вероятности значительно большие, чем 0).

Далее, это значение разности поступит на вход SL-преобразования третьего цикла. Следовательно, на выходе опять может быть получена разность с одновременно всеми активными байтами (см. рис. 3). Таким образом, после 3 циклов всегда есть возможность получения выходной разности с одновременно всеми активными байтами в блоке для любой входной разности.

Так как расшифрование выполняется по такой же схеме, то 3 цикла расшифрования также позволяют для любой начальной разности получить разность с одновременно всеми активными байтами в блоке. Тогда в терминах теоремы 1 для данного шифра $r_1 = r_2 = 3$. Утверждение доказано.

ВЫВОДЫ

В работе рассмотрены существующие методы поиска НД. Проанализированы их слабые и сильные стороны. Предложен метод, который позволяет обосновать отсутствие НД. Сложность метода в меньшей степени зависит от размера блока, в отличие от известных, поэтому он может быть использован для БСШ с большими размерами блока. Продемонстрировано применение метода для Rijndael-подобных шифров и для шифров, которые используют схему фейстеля.

Литература

[1] Biham, E., Keller, N.: Cryptanalysis of Reduced Variants of Rijndael, 3rd AES Conference, New York, USA (2000), http://csrc.nist.gov/encryption/aes/round2/conf3/aes3papers.html.

[2] Cheon, J.H., Kim, M., Kim, K., Lee, J.-Y., Kang, S.: Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 39–49. Springer, Heidelberg (2002).

[3] Jiqiang Lu, Orr Dunkelman, Nathan Keller and Jongsung Kim. New Impossible Differential Attacks on AES. IACR Cryptology ePrint Archive 2008: 540 (2008).

[4] Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials, Technion, CS Dept, Tech Report CS0947 (1998).

[5] Biham, E., Biryukov, A., Shamir, A.: Miss-in-the-Middle Attacks on IDEA, Khufu and Khafre. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 124–138. Springer, Heidelberg (1999).

[6] Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1, Archive available at: http://jiqiang.googlepages.com.

[7] Wenling Wu, Wentao Zhang and Dengguo Feng. Impossible differential cryptanalysis of reduced-round ARIA and Camellia. Journal of Computer Science and Technology, 22(3):449-456, 2007. Springer.

[8] J. Kim, S. Hong, J. Sung, S. Lee and J. Lim: Impossible differential cryptanalysis for block cipher structures, INDOCRYPT 2003, LNCS 2904, pp. 82-96, 2003.

[9] Yiyuan Luo, Zhongming Wu, Xuejia Lai and Guang Gong. A Unified Method for Finding Impossible Differentials of Block Cipher Structures. IACR Cryptology ePrint Archive 2009: 627 (2009).

[10] Ruilin Li, Bing Sun and Chao Li. Impossible Differential Cryptanalysis of SPN Ciphers. IACR Cryptology ePrint Archive 2010: 307 (2010).

[11] H. Yap, Impossible Differential Characteristics of Extended Feistel Networks with Provable Security against Differential Cryptanalysis. SecTech 2008, CCIS 29, pp. 103-121, 2009.

[12] J. Daemen, V. Rijmen. AES Proposal Rijndael, AES Round 1 Technical Evaluation CD1: Documentation, National Institute of Standards and Technology, Aug 1998. See http://www.nist.gov/aes.

[13] Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація / І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 6, №2, 2007. – С. 195-208.

[14] Руженцев В.И. О методах оценки стойкости к атаке усеченных дифференциалов / В. И. Руженцев // Радиоэлектроника и информатика. 2003. – №4. – С. 130-133.

[15] FOX Specifications Version 1.2 appeared on http://crypto.junod.info.

[16] Перспективний блоковий симетричний шифр «Мухомор» - основні положення та специфікація / І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 6, №2, 2007. – С. 168-185.

[17] Руженцев В.И. О стойкости блочных шифров с rijndael-подобными преобразованиями к интегральным атакам. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 11, №2, 2012. – С. 160–164.

Поступила в редколлегию 12.03.2013

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Научные интересы: криптография, криптоанализ блочных симметричных шифров.

УДК 621. 391:519.2:519.7

Про метод доведення стійкості блокових шифрів до атаки нездійснених диференціалів / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 215–219.

Аналізуються відомі методи пошуку нездійснених диференціалів. Пропонується метод, який дозволяє обгрунтувати відсутність нездійснених диференціалів. Складність цього методу, на відміну від відомих, меншою мірою залежить від розміру блоку. Метод застосовується для Rijndael-подібних SPN шифрів та фейстель-подібних шифрів.

Ключові слова: блоковий шифр, атака нездійснених диференціалів, нездійснений диференціал, Rijndael-подібні перетворення.

Табл.: 2. Іл.: 3. Бібліогр.: 12 найм.

UDC 621. 391:519.2:519.7

On the method of proving the resistance of block ciphers to impossible differential attack / V.I. Ruzhentsev // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 215–219.

The known methods of proving the security of block ciphers against impossible differentials attacks are considered. A new method is proposed which allows to validate the absence of impossible differentials. The complexity of the method, unlike the known ones, to a less extent depends on the block size. This method is applied to Rijndael-like SPN ciphers and to ciphers which use the Fiestel scheme.

Keywords: block cipher, impossible differential attack, impossible differential, Rijndael-like transformations.

Tab.: 2. Fig.: 3. Ref.: 12 items.

УДК 681.3.06

СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ

Г.З. ХАЛИМОВ

Представлены результаты строго универсального хеширования на основе методов ортогональных массивов, независимых массивов и слабосмещенных массивов. Получены оценки параметров семейства хеш-функций строго универсального хеширования. Наилучшие результаты универсального хеширования достигаются на слабо смещенных массивах Вейля-Карлитца-Ушиямы.

Ключевые слова: универсальное хеширование.

Задача построения доказуемо секретной аутентификации впервые сформулирована в работе [1]. Решение было предложено в классе универсальных хеш-функции, как аутентификации с максимальной теоретически достижимой секретностью. В методе универсального хеширования на основе скалярного произведения достигается $P_{\text{кол}} = 1/|B|$, при условии что $|K| = |D|$, а в методе полиномиального хеширования $P_{\text{кол}} \sim \log|D|$, $|K| = |B|$, где $|K|, |D|, |B|$ – мощности пространств ключей, сообщений и хеш-кодов. Идеи универсальной аутентификации получили развитие в теории безусловной аутентификации с использованием строго универсального хеширования [2]. Теория построение массивов строго универсальных аутентификаторов определяется ортогональными массивами. Основной результат строго универсального хеширования состоит в том, что вероятность коллизии $P_{\cdot\geq} = 1/|B|$ достигается при условии $|K| \geq |D||B|$. Применение слабосмещенных массивов для построения почти строго универсальных хеш-функций снимает ограничение на размер ключевого пространства $|K| \geq |B|^2$, но увеличивает при этом вероятность коллизии $P_{\text{кол}} > 1/|B|$. Основное противоречие доказуемо стойкой аутентификации состоит в том, что для обеспечения гарантированной вероятности обмана на уровне нижней границы, размер ключа должен быть не меньше размера сообщения, а фиксирование размера ключа на нижней границе определяемой мощностью пространства хешей приводит к пропорциональному росту вероятности коллизии от длины данных.

Целью статьи является решение задачи построения строго универсального хеширования на основе методов ортогональных массивов, независимых массивов и слабосмещенных массивов. В разделе 1 рассмотрены коллизионные свойства MAC кодов универсального хеширования. В разделе 2 получены оценки параметров строго универсального хеширования на основе ортогональных массивов. В разделе 3 представлено строго универсальное хеширование на основе почти независимых массивов. В разделе 4 приводятся свойства универсального хеширования на основе слабосмещенных массивов.

1. КОЛЛИЗИОННЫЕ СВОЙСТВА MAC КОДОВ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

MAC коды универсального хеширования определяются массивами с известными статистическими и комбинаторными свойствами, что позволяет, как правило, получить точные коллизионные границы. Основные положения универсального хеширование приведены в работах [1, 2, 3], уточнения и дополнения в [4].

Определение 1 [1]. $(N;n,m)$ хеш-семейство является ε-универсальным, если для любых двух различных элементов $x_1, x_2 \in A$, существует самое большее εN функций $h \in H$ таких, что $h(x_1) = h(x_2)$. Аббревиатура $\varepsilon - U$ используется для обозначения ε-универсальных хеш-функций.

Утверждение 1 [4]. Пусть h выбирается случайно из заданного $\varepsilon - U(N;n,m)$ хеш-семейства, тогда вероятность коллизии хеш-значений для двух разных входных сообщений $x_1, x_2 \in A$ не превышает ε.

Замечание 1.

1. Первоначальное определение универсальных хеш-функций Картера и Вегмана было предложено для $\varepsilon = 1/m$ [1].

2. Вероятность коллизии для универсальных хеш-функций Картера и Вегмана является наименьшей и определяется мощностью пространства хеш-значений $P_{\text{кол}} = 1/|B|$.

Определение 2 [1]. H является ε – почти универсальным семейством хеш-функций ($\varepsilon - AU(N;n,m)$),если $P_{\text{кол}} = \Pr_{h \in H}\left[h(x_1) = h(x_2)\right] \leq \varepsilon$ для $x_1, x_2 \in A$, $x_1 \neq x_2$, $1/m < \varepsilon \leq 1$.

Замечание 2.

1. Для почти универсальных семейств несколько ослабляются требования к вероятности коллизии.

2. Свойство универсальности (почти универсальности) не связанно с распределением MAC значений по ключевому пространству и, следовательно, не определяет вероятностные характеристики имитационной атаки.

3. Универсальное хеширование определяет доказуемо стойкую аутентификацию со счетчиком в представлении Картера – Вегмана [1].

Дальнейшим развитием универсальных схем являются строго универсальные.

Определение 3 [2]. $(N;n,m)$ хеш-семейство является ε-строго универсальным ($\varepsilon - SU(N;n,m)$),

если для каждого $x \in A$ и $y \in B$ число функций $h \in H$, таких, что $h(x) = y$ равно N / m, а для любых двух различных элементов $x_1, x_2 \in A$, и не обязательно различных $y_1, y_2 \in B$ число функций $h \in H$ таких, что $h(x_1) = y_1$, $h(x_2) = y_2$ не превышает $\nu \le \varepsilon \cdot N / m$. Аббревиатура $\varepsilon - SU$ используется для обозначения ε-строго универсальных хеш-функций.

Замечание 3.

1. Строгая универсальность определена для $\varepsilon = 1/m$.

2. При смягчении требования $\varepsilon > 1/m$ класс функций определяется как почти строго универсальный $\varepsilon - ASU$.

3. Строго (почти строго) универсальное хеширование определяет безусловную аутентификацию и было представлено Стинсоном [2,3].

Коллизионные свойства почти строго универсальных MAC кодов представлены следующими утверждениями.

Утверждение 2. Пусть $(N;n,m)$ семейство хеш-функций является $\varepsilon-$ строго универсальным ($\varepsilon - SU(N;n,m)$). Тогда $N \ge m^2$, $P_{8<} = 1/m$ и $P_{?\searrow 4} = 1/m$.

Доказательство. По определению строгой универсальности число функций $h \in H$ таких, что $h(x_1) = y_1$, $h(x_2) = y_2$ не превышает $\varepsilon \cdot N / m$. Возьмём нижнюю границу $\nu = 1$ и, т. к. $\varepsilon = 1/m$, имеем $N \ge m^2$. Прямое вычисление вероятности имитационной атаки по ключу дает $N \ge m^2$ $P_{\text{им.кл}} = (N/m)/M = 1/m$, что соответствует нижней границе для вероятности имитации по MAC коду, следовательно $P_{\text{им}} = 1/m$. Вероятность подмены определяется условной вероятностью. Так как число h для которых $h(x) = y$ равно N/m, а число h для которых $h(x) = y$, $h(x') = y'$ равно $\nu \le \varepsilon \cdot N/m = N/m^2$, получим $P_{\text{под}} = 1/m$.◊

Утверждение 3. Пусть $\varepsilon - ASU(N;n,m)$ семейство почти строго универсальных хеш-функций. При равновероятном выборе хеш-функции вероятность успеха имитационной атаки равна $P_{\text{им}} = 1/m$ и вероятность подмены $P_{\text{под}} \le \varepsilon$.

Доказательство аналогично предыдущему.

2. СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ ОРТОГОНАЛЬНЫХ МАССИВОВ

Определение 4 [5]. Пусть X, Y являются множествами из k и v элементов, соответственно, и H есть множество функций осуществляющих отображение $f: X \to Y$. *Ортогональным массивом* $OA_\lambda(t,k,v)$ называется массив элементов $y_i \in Y$, со столбцами, соответствующими элементам множества X и строками, определяемыми элементами множества m, в котором для любой выборки из t элементов $y_1, y_2, ..., y_t$ из Y существует только λ функций $f \in m$, для которых справедливо $f(x_i) = y_i$, $i = 1,2,...,t$.

Основная конструкция OA массивов определена теоремой 1.

Теорема 1 [6]. Пусть q простое число, m,n,t — целые числа, $n \ge m$, $2 \le t \le q^n$. Зафиксируем сьюрективное F_q — линейное отображение $\varphi: F_q^n \to F_q^m$. Для каждого t набора $(z, a_1, a_2, ..., a_{t-1})$, где $z \in F_{q^m}$, $a_j \in F_{q^n}$, $i = 1,2,...,t-1$, определим отображение $f = f(z, a_1, a_2, ..., a_{t-1}): F_q^n \to F_q^m$, вида

$$f(x) = \varphi\left(\sum_{j=1}^{t-1} a_j x^j\right) + z. \qquad (1)$$

Тогда массив, составленный из отображений вида (1) является ортогональным с параметрами $OA_{q^{(t-1)(n-m)}}(t, q^n, q^m)$.

Следствие 1. Пусть q — простое число, $n = m$, $t = 2$. Тогда $OA_{\lambda=1}(2, q^m, q^m)$ называется простым, каждая строка повторяется только (точно) один раз и определяется линейным отображением $\varphi: F_q^m \to F_q^m$ с функцией $f(x) = \varphi(ax) + z$, где $a, z \in F_{q^m}$.

Метод ортогональных массивов можно применить для построения строго универсальных хеш-функций. Основной результат представлен в теореме 2.

Теорема 2 [4]. Пусть q — простое число, a, b, k — целые числа, $a > b$. Тогда существует $\frac{k}{q^b} - SU(q^{a+b}, q^{ka}, q^b)$ семейство хеш-функций.

Замечание 4.

1. Если $k = 1$ имеем строго универсальный класс хеш-функций $\frac{1}{q^b} - SU(q^{a+b}, q^a, q^b)$. Размер ключевых данных N определяется произведением пространства аутентификаторов и пространства сообщений, что уточняет ранее полученную границу утверждения 2.

2. Для почти строго универсального хеширования снижаются требования к размеру ключевых данных, которое ограничивается размерами поля вычислений F_{q^a} и F_{q^b}.

Пример 1 [4]. Пусть $q = 2$, $a = 4$, $b = 2$. Построить строго универсальный класс хеш-функций.

Построим простой ортогональный массив $OA_{q^{(a-b)}}(2, q^a, q^b)$ с помощью линейного отображения $\varphi: F_2^4 \to F_2^2$ с функцией $f(x) = \varphi(ax) + z$. Ортогональный массив будет иметь вид матрицы, в которой строки определяются функциями f_j с параметрами $a_i \in F_{2^4}$, $z_i \in F_{2^2}$, столбцы — значениями $x_i \in F_{2^4}$, а элементы — значениями $y_i \in F_{2^2}$. Существует самое большее $\lambda = 4$ функций, для которых справедливо $f(x_1) = y_1$ и $f(x_2) = y_2$. Данный ортогональный массив является семейством строго универсальных хеш-функций. По определению 3 имеем следующие параметры. Общее число функций $N = 64$. Число записей со значением у в каждом столбце матрицы отображения $X \to Y$ встречается $\frac{N}{2^m} = 16$ раз. Число функций $f \in H$ таких, что $f(x_1) = y_1$, $f(x_2) = y_2$ не превышает $v \le 4$, т. к. $\lambda = 4$. Вероятность коллизии ε будет равна

$\varepsilon \cdot \frac{N}{2^b} = \lambda$, $\varepsilon = \frac{1}{4}$ и имеем $\frac{1}{4} - SU(64,16,4)$ семейство хеш-функций.

Утверждение 5. Линейное отображение $\varphi: F_{q_1} \to F_{q_2}$ с функцией $f(x) = \varphi(ax) + z$, где q_1 и q_2 — простые числа, $q_1 > q_2$, $a \in F_{q_1}$, $z \in F_{q_2}$ приводит к почти строго универсальному хешированию $\frac{2}{q_2} - ASU(q_1 q_2, q_1, q_2)$.

Действительно, пусть q_1 и q_2 — простые числа, $q_1 > q_2$, $t = 2$. Тогда $OA_{\lambda=\lceil q_1/q_2 \rceil}(2, q_1, q_2)$ — массив, каждая строка которого повторяется самое большее $\lambda = \lceil q_1 / q_2 \rceil$ раза, где $\lceil q_1 / q_2 \rceil$ определяет округление к большему целому. Вероятность коллизии ε по определению строгой универсальности будет равна $\varepsilon \cdot \frac{N}{q_2} = \lambda$, $N = q_1 q_2$, $\varepsilon = \lambda / q_1 = \lceil q_1 / q_2 \rceil / q_1 \le 2 / q_2$ и получим почти строго универсальное хеширование $\frac{2}{q_2} - ASU(q_1 q_2, q_1, q_2)$. ◊

Замечание 5.

1. Теорема 2 определяет строго универсальное хеширование $\frac{1}{q^m} - SU(q^{n+m}, q^n, q^m)$ над расширенным полем (см. утверждение 3 [4]).

2. Линейное отображение $\varphi: F_q^n \to F_q^m$ определяет умножение элементов в F_{q^n}, проектирование m координат $F_{q^n} \to F_{q^m}$ и сложение в F_{q^m} (см. пример 1).

3. Линейное отображение $\varphi: F_{q_1} \to F_{q_2}$, где q_1 и q_2 — простые числа, определяет отображение простого конечного поля на простое поле меньшей размерности.

3. СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ ПОЧТИ НЕЗАВИСИМЫХ МАССИВОВ

Обобщением ортогональных массивов являются почти независимые массивы (almost independent arrays). Теория почти независимых массивов снимает ограничение на равновероятное распределение наборов хешей по столбцам массива. Почти независимые массивы были рассмотрены Стинсоном [2,3] и в рамках этой теории были определены многократные или t связные коды аутентификации.

Определение 5 [7]. Пусть $0 \le \varepsilon \le 1$. Массив $(n,k)_p$ является t — связным, ε — зависимым (ε — dependent), если для любого набора U из $s \le t$ столбцов и каждого вектора $a \in F_p^s$ частота $v_U(a)$ появления в столбцах значения a удовлетворяет условию $\left| \frac{v_U(a)}{n} - \frac{1}{p^s} \right| \le \varepsilon$.

Замечание 6. Если массив $(n,k)_p$ является t-связным, независимым (0-зависимым), тогда по определению имеем $v_U(a)/n = 1/p^t$. В этом случае $(n,k)_p$ является ортогональным массивом силы t и образует t-строго универсальное семейство хеш-функций [7, 8].

Утверждение 6 [8]. Пусть $(n,k)_p$ — массив, содержащий n строк, k столбцов и записи из набора p элементов. Для $\forall a \in F_p$ частота $v_a(u)$ появления значения a в столбцах массива $u = (u_1, u_2, ..., u_n) \in F_p^n$ удовлетворяет условию $\left| v_a(u)/n - 1/p \right| \le \varepsilon_1$ и для любых пар столбцов u, u' частота $v_{a,a'}(u,u')$ появления в столбцах значений a и a' удовлетворяет условию $\left| v_{a,a'}(u,u')/n - 1/p^2 \right| \le \varepsilon_2$. Тогда $(n,k)_p$-массив есть семейство $\varepsilon - ASU(n,k,p)$ хеш-функций и $\varepsilon = (p^{-2} + \varepsilon_2)/(p^{-1} - \varepsilon_1)$.

Доказательство. Параметр ε определяется условной вероятностью появления любых записей a, a' для различных столбцов u, u' при равновероятном выборе i строки $\varepsilon = \Pr(u'_i = a' / u_i = a)$. По формуле полной вероятности имеем

$$\Pr(u'_i = a' / u_i = a) = \Pr(u_i = a, u'_i = a') / \Pr(u_i = a).$$

Вероятность появления в произвольно выбранном столбце значения a определяется, как $\Pr(u_i = a) = v_a(u)/n$ и с условием ограничения $\left| v_a(u)/n - 1/p \right| \le \varepsilon_1$ удовлетворяет неравенству

$$p^{-1} - \varepsilon_1 \le \Pr(u_i = a) \le p^{-1} + \varepsilon_1.$$

Аналогично для вероятности

$$\Pr(u_i = a, u'_i = a') = v_{(a,a')}(u,u')/n$$

имеем $p^{-2} - \varepsilon_2 \le \Pr(u_i = a, u'_i = a') \le p^{-2} + \varepsilon_2$.

Максимальное значение условной вероятности $\Pr(u'_i = a' / u_i = a) = (p^{-2} + \varepsilon_2)/(p^{-1} - \varepsilon_1)$ получим, подставляя выражение для полной вероятности

$$\Pr(u_i = a) = p^{-1} - \varepsilon_1 \text{ и } \Pr(u_i = a, u'_i = a') = p^{-2} + \varepsilon_2. \text{ ◊}$$

Замечание 7.

1. Параметр ε-зависимость характеризует отклонение от равномерного распределения совместных вероятностей появления кодовых комбинаций в t произвольных столбцах случайно выбранной строки $(n,k)_p$ массива. В теории безусловной аутентификации Стинсона $t = 2$ и рассматривается ASU_2 аутентификация.

2. Как следует из утверждения 6, значение параметра зависимости ε определяет вероятность коллизии MAC кодов и в общем случае, как показано в [9], коллизионные свойства t-кратных кодов аутентификации. Практическое построение почти независимых массивов является проблематичным, т. к. нужны методы, которые позволяют формировать массивы хешей с заданными распределениями по столбцам. В этом отношении для построения строго универсальных хеш-функций более продуктивным является применение слабо смещенных массивов.

4. СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ СЛАБОСМЕЩЕННЫХ МАССИВОВ

Слабо смещённые массивы впервые были введены в работах [10, 11] для массивов дискретных значений большой размерности с распределением незначительно отличающимся от равномерного.

Слабо смещённые массивы определяют свойства распределений хешей в столбцах массива [8].

Определение 6. Пусть p - — простое число, $u=(u_1,u_2,...,u_n)\in F_p^n$. Для $\forall i\in F_p$, $v_i(u)$ есть частота появления элемента i в последовательности u $v_i(u)=\frac{n}{p}+\delta_i(u)$, где $\delta_i(u)$ — отклонение частоты $v_i(u)$ от среднего значения и $\sum_{i\in F_p}\delta_i(u)=0$.

Пусть ξ — комплексный корень p-степени из единицы, тогда смещение вектора u определяется как

$$bias(u)=\frac{1}{n}\left|\sum_{i\in F_p}\delta_i(u)\xi^i\right|=\frac{1}{n}\left|\sum_{i\in F_p}v_i(u)\xi^i\right|.$$

Смещение $bias(u)$ имеет следующие свойства.

Утверждение 7 [8]. Для произвольного вектора u $0\le bias(u)\le 1$ и $bias(u)=1$ только тогда, когда $u=const$.

Определение 7. Пусть $(n,k)_p$ — массив, содержащий n строк, k столбцов и записи из набора p элементов и $0\le\varepsilon\le 1$. Массив $(n,k)_p$ является ε-смещённым (ε-biased), если любая нетривиальная линейная комбинация столбцов имеет смещение $bias\le\varepsilon$.

Замечание 7.

1. Смещение массива является свойством F_p — линейного кода, построенного с помощью столбцов порождающей матрицы.

2. Для двоичных массивов параметр ε смещения прямо связывается с вероятностями появления 0 и 1 в столбцах массива.

3. Для строго универсального класса, массив хеш-значений определяется $(n,k)_p$ массивом со смещением равным нулю [8].

Утверждение 1.11 [8]. Пусть (n,k) двоичный ε-смещённый массив, содержащий n строк, k столбцов, тогда вес Хемминга ω любой нетривиальной линейной комбинации столбцов удовлетворяет неравенству

$$\frac{1-\varepsilon}{2}\le\frac{\omega}{n}\le\frac{1+\varepsilon}{2}.$$

Пусть ω_i вес Хемминга нетривиальной линейной комбинации u_i столбцов двоичной матрицы (n,k). Тогда $v_1(u)=\omega_i$, $v_0(u)=n-\omega_i$ и по определению 6 получим

$$\frac{1}{n}\left|\sum_{i\in F_p}v_i(u)\xi^i\right|=\frac{1}{n}\left|v_0\xi^0+v_1\xi^1\right|=$$

$$=\frac{1}{n}\left|n-2\omega_i\right|\le\varepsilon \text{ или } \frac{1-\varepsilon}{2}\le\frac{\omega_i}{n}\le\frac{1+\varepsilon}{2}. \qquad \Diamond$$

В общем случае, когда $p\ne 2$ прямого соответствия между смещением и вероятностью появления символов в столбцах массива нет.

Практическим методом построения слабосмещенных массивов является метод сумм экспонент Вейля- Карлитца- Ушиямы (ВКУ).

Определение 8 [12]. Метод сумм экспонент ВКУ определяет массив $(p^f,f\cdot(n-n/p))_p$ со смещением $bias\le(n-1)p^{-f/2}$, с записями вида $Tr(a_j\alpha^i)$, где a_j — базис поля $F_{p^f}\left|F_p\right.$, $i\le n$ и i не кратно p, $Tr;F_{p^f}\to F_p$ — след элемента $a_j\alpha^i$.

Пример 2 [8]. Построить массив ВКУ $(p^f,f\cdot(n-n/p))_p$ со смещением $bias\le(n-1)p^{-f/2}$ при $p=2,f=4,n=1$. Базисные элементы поля имеют вид $a_j:1,\alpha,\alpha^2,\alpha^3$. Так как $n=1$, следует взять только одну экспоненту $\varphi:X$. Строки массива индексируются элементами $\alpha\in F_{2^4}$, столбцы — функциями: $X,\alpha X,\alpha^2X,\alpha^3X$, а записи — $Tr(\beta)=\beta+\beta^2+\beta^4+\beta^8$. Получим $(2^4,4)$ массив со смещением $bias=(1-1)2^{-2}=0$.

Пример 3. Построить массив ВКУ $(p^f,f\cdot(n-n/p))_p$ со смещением $bias\le(n-1)p^{-f/2}$ при $p=3,f=2,n=2$. Тогда $a_j:1,\alpha$, $\varphi:X,X^2$ и $Tr(\beta)=\beta+\beta^3$. Строки массива индексируются элементами $\alpha\in F_{3^2}$ (порождающий многочлен поля z^2+z+2), столбцы — функциями: $X,\alpha X,\alpha X^2,X^2=\alpha^4X+1 \pmod{X^2+X+2}$. Массив $(3^2,4)_3$ имеет вид, представленный в табл. 1.

Таблица 1

Слабосмещенный массив ВКУ $(3^2,4)_3$

α^i	X	αX	X^2	αX^2
0	0	0	0	0
α^0	α^4	α^4	α^4	α^4
α^1	α^4	0	0	α^4
α^2	0	α^4	α^0	α^0
α^3	α^4	α^0	0	α^0
α^4	α^0	α^0	α^4	α^4
α^5	α^0	0	0	α^4
α^6	0	α^0	α^0	α^0
α^7	α^0	α^4	0	α^0

Зададим произвольную линейную комбинацию столбцов $Y=\sum_{j=1}^{4}\gamma^jY_j$, $\gamma^j\in F_3$, например, $Y=Y_1+\alpha^4Y_2+\alpha^4Y_4$. Получим результирующий вектор

$$Y_p=(0,\alpha^0,0,0,0,\alpha^0,\alpha^4,\alpha^0,\alpha^0).$$

Значения частот элементов $0,\alpha^0,\alpha^4$ равны: $v_0=4$, $\delta_0=+1$, $v_{\alpha^0}=4$, $\delta_{\alpha^0}=+1$, $v_{\alpha^4}=1$, $\delta_{\alpha^4}=-2$, а смещение

$$bias(v_Y)=\frac{1}{9}\left|1\cdot e^{j\frac{2\pi}{3}\cdot 0}+1\cdot e^{j\frac{2\pi}{3}\cdot 1}+(-2)\cdot e^{j\frac{2\pi}{3}\cdot 2}\right|=$$

$$=\frac{1}{9}\left|1-\frac{1}{2}+\frac{\sqrt{3}}{2}j+1+\sqrt{3}j\right|=\frac{1}{3}.$$

Для всех нетривиальных линейных комбинаций столбцов значение $bias\le\frac{1}{3}$ и $bias\le p^{-1}$.

Замечание 9.

1. Пусть $f=2$, $n=1$, тогда имеем $(p^2,2)_p$. Строки массива индексируются элементами $\alpha\in F_{p^2}$, столбцы — функциями: $X,\alpha X$, записи — $Tr(\beta)=\beta+\beta^p$. Значение смещения столбца $bias\le(n-1)p^{-f/2}$ будет равно 0. Можно показать,

что если $f\cdot(n-n/p)$ чуть меньше 2, верхняя граница смещения массива $(p^2,2)_p$ $bias\le p^{-1}$.

2. Линейная комбинация столбцов массива $(p^2,2)_p$ $Y=\sum_{j=1}^{2}\gamma^j Y_j$, $\gamma^j\in F_p$ имеет смещение $bias=0$ и значение $Y+\eta$ в строке индексированной α, η, $\alpha\in F_{p^2}$, $\eta\in F_p$ определяет строго универсальный класс $\frac{1}{p}-SU(p^3,p^2,p)$. Это совпадает с результатами теоремы 2.

3. Пусть $f=2$, $n=2$, тогда имеем $(p^2,4)_p$. Строки массива индексируются элементами $\alpha\in F_{p^2}$, столбцы – функциями: $X,\alpha X,X^2,\alpha X^2$, записи – $Tr(\beta)=\beta+\beta^p$. Если $f\cdot(n-n/p)$ строго равняется 4, значение смещения будет точно равно $bias=p^{-1}$. Можно показать, что если $f\cdot(n-n/p)$ чуть меньше 4, верхняя граница смещения массива $(p^2,4)_p$ $bias\le 2/p$. Линейная комбинация столбцов массива $(p^2,4)_p$ $Y=\sum_{j=1}^{4}\gamma^j Y_j$, $\gamma^j\in F_p$, имеет смещение $bias\le 1/p$ и значение $Y+\eta$ в строке индексированной α, η, $\alpha\in F_{p^2}$, $\eta\in F_p$ определяет почти строго универсальный класс $\frac{1}{p}-ASU(p^3,p^4,p)$.

4. В случае $f=1$, $n=1$, имеем простой ортогональный массив $(q,1)_q$ с линейным отображением $\varphi: F_q\to F_q$ и функцией $f(x)=\varphi(ax)+z$, где $a,z\in F_q$.

Теорема 3 [9]. Если массив является t-связным и ε-смещенным, он является также и t-связным и ε'-зависимым, причём, $\varepsilon'<\varepsilon$.

Фундаментальное значение этой теоремы заключается в том, что она определяет возможность применения слабо смещённых массивов в схемах аутентификации.

Теорема 4 [7]. Пусть $(n,k)_p$ – массив со смещением ε_0 и $t\le k$. Тогда существует $\varepsilon-ASU_2(p^t n,p^k,p^t)$ универсальное хеширование, где $\varepsilon=p^{-t}+\varepsilon_0$.

Отличие схемы ASU_2 по теореме 4 состоит в том, что используется специальное индексирование строк массива аутентификаторов и записей, что увеличивает пространство ключей и записей, и приводит к лучшим оценкам параметров аутентификации.

ВЫВОДЫ

1. Практическим методом построения строго универсального семейства хеш-функция на основе слабосмещенных массивов является метод сумм экспонент Вейля — Карлитца — Ушиямы.

2. Универсальное хеширование по теореме 4 определяется через слабосмещённые массивы, является обобщением конструкций линейных кодов, ВКУ массивов.

Литература

[1] Carter J. L. Universal classes of hash functions /J. L.Carter, M.N.Wegman // Journal of Computer and Systems Science. – 1979. – V.18. – P. 143-154.

[2] Stinson D.R. Combinatorial techniques for universal hashing / D.R.Stinson //Journal of Computer and Systems Science. – 1994. – V.48. – P.337-346.

[3] Stinson D.R. Universal hashing and authentication codes. / D.R.Stinson // Designs, Codes and Cryptography. –1994. – N. 4. – P.369–380.

[4] Халимов Г.З. Аутентификация и универсальное хеширование / Г.З.Халимов, А.А.Кузнецов // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2001. – Вып. 119. – С. 88-94.

[5] Mukhopadhyay A.L. Construction of some series of ortogonal array / A.L. Mukhopadhyay //Sankya B43. – 1981. – P. 81-92.

[6] Bierbrauer J. Bounds on orthogonal arrays and resilient functions / J.Bierbrauer //Journal of Combinatorial Designs. – 1995. – N. 3. –P. 179–183.

[7] Bierbrauer J. Weakly biased arrays, almost independent arrays and error-correcting codes / J.Bierbrauer, H.Schellwat //Publication in Proceedings of AMS-DIMACS. – 2000. – P.33.

[8] Халимов Г.З. Безусловная аутентификация с использованием слабосмещенных массивов / Г.З. Халимов // Радиотехника. Всеукр. межвед. науч.-техн. сб. Тем. выпуск «Информационная безопасность». – 2003. – № 134. – С. 165–171 .

[9] Kurosawa K. Almost k-wise independent sample spaces and their cryptologic applications / K.Kurosawa, T.Johansson, D.Stinson // Lecture Notes in Computer Science. – 1997. – N. 1233. – P. 409–421.

[10] Alon N. Simple constructions of almost k-wise independent random variables / N.Alon, O.Goldreich, J.Hastad, R.Peralta //Random Structures and Algorithms. – 1992. – N. 3. – P. 289–304.

[11] Naor J. Small-bias probability spaces: efficient constructions and applications / J.Naor, M.Naor //SIAM Journal on Computing. – 1993. – N. 22. – P. 838–856.

[12] Carlitz L. Bounds for exponential sums / L.Carlitz, S.Uchiyama // Duke Mathematical Journal. – 1957. – N. 24. – P. 37–41.

Поступила в редколлегию 15.03.2013

Халимов Геннадий Зайдулович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Научные интересы: методы и средства аутентификации данных.

УДК 681.3.06

Суворо універсальне гешування / Г.З. Халімов// Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 220–224.

Наведено результати суворо універсального гешування на основі методів ортогональних масивів, незалежних масивів і слабко зміщених масивів. Отримано оцінки параметрів сімейства геш-функцій суворо універсального гешування. Найкращі результати універсального гешування досягаються на слабко зміщених масивах Вейля-Карлітца-Ушіями.

Ключові слова: універсальне гешування.

Табл.: 01. Бібліогр.: 12 найм.

UDC 681.3.06

Strongly universal hashing / G.Z. Khalimov // Applied Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 220–224.

This paper presents the results of strongly universal hashing based on the methods of orthogonal arrays, independent arrays and weakly biased arrays. Estimates of parameters of a hash functions family of strongly universal hashing are obtained. The best results of universal hashing are achieved on Weil-Carlitz-Uchiyama weakly biased arrays.

Keywords: universal hashing.

Tab.: 01. Ref.: 12 items.

УДК 681.3.06

ОЦЕНКИ СЛОЖНОСТИ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО АЛГЕБРАИЧЕСКИМ КРИВЫМ

Г.З. ХАЛИМОВ

Представлены результаты универсального хеширования по алгебраическим кривым. Получены решения для вычисления точек наилучших кривых по ключевым данным, оценки сложности вычислений, практические рекомендации применения алгебраических кривых для универсального хеширования.

Ключевые слова: универсальное хеширование, максимальные кривые.

Универсальное хеширование по алгебраическим кривым предложено в работе [1]. Наилучший результат по коллизионным оценкам достигается на максимальных кривых [2, 3]. Проблематика практической реализации универсального хеширования на основе скалярного произведения по рациональным функциям алгебраических кривых определяется сложностью построения точек алгебраических кривых по ключевым данным. Вычислительные затраты на хеширование зависят от размерности функционального поля рациональных функций. Основное противоречие универсального хеширования по алгебраическим кривым состоит в том, что для обеспечения гарантированной вероятности обмана на нижнем уровне, необходимо построить вычисления по рациональным функциям алгебраических кривых с как можно меньшим отношением значения максимального полюса рациональных функций к числу точек кривой для фиксированной длины данных. Применение максимальных кривых большого рода приводит к увеличению размерности функционального поля ассоциированного с кривой и росту сложности вычислений.

Целью статьи является оценка сложности универсального хеширования по алгебраическим кривым. В разделе 1 представлено универсальное хеширование по алгебраическим кривым. В разделе 2 приводятся наилучшие результаты универсального хеширования по максимальным кривым. В разделе 3 получены оценки сложности вычисления точек алгебраических кривых по ключевым даням.

1. УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ В ПОЛЕ РАЦИОНАЛЬНЫХ ФУНКЦИЙ

Универсальное хеширование в поле рациональных функций по точкам алгебраической кривой впервые обосновано Биербрауэром [1]. Интерпретация алгеброгеометрического подхода представлена в работах [4, 5].

Определение 1[6]. Пусть

χ — абсолютно неразложимая, несингулярная проективная кривая над полем F_q;

$P_1, P_2, ..., P_n$ — точки кривой χ;

P_∞ — точка на бесконечности или особая точка кривой χ;

$f_i \in F_q(\chi) \setminus \{0\}$ — рациональные функции поля рациональных функций кривой χ;

$div_\infty(f_i) = \rho_i$ значение дивизора или порядок полюса рациональной функции f_i в точке P_∞;

$f_i(P_j)$ — значение рациональной функции в точке P_j.

Хеш-функция $h_{P_j}(m) \in F_q$ для сообщения $m = (m_1, ..., m_k)$, $m_i \in F_q$ в точке P_j определяется выражением

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i ,$$

где $f_i \in F_q(\chi)$ с упорядоченными порядками полюсов $0 < \rho_1 < \rho_2 < ... < \rho_k$.

Свойства универсального хеширования по рациональным функциям алгебраических кривых определяются утверждением 1.

Утверждение 1[4]. Хеш-функция $h_{P_j}(m)$ определяет универсальный хеш-класс $\varepsilon - U(N, q^k, q)$, где N — число точек алгебраической кривой, q^k — объём пространства сообщений, q — объём пространства хеш-кодов и вероятность коллизии определяется выражением

$$\varepsilon = \rho_k / N ,$$

где ρ_k — значение полюса рациональной функций f_k.

Замечание 1.

1. Параметры универсального хеш-класса $\varepsilon - U(N, q^k, q)$ на основе хеширования по рациональным функциям определяются свойствами алгебраической кривой. Подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < ...\}$ определяется полюсами рациональных функций в особой точке кривой и рациональные функции, упорядоченные по значениям полюсов, образуют векторное линейное пространство размерности $\dim(L(G) = \nu_\ell := \{(i, j) \in N^2 : \rho_i + \rho_j = \rho_{\ell+1}\}$.

2. Ключевой параметр хеш-функции $h_{P_j}(m)$ определяется вычислением в точке алгебраической кривой.

Интерес представляют алгебраические кривые с как можно большим отношением числа точек кривой к её роду, определенные над конечным полем F_q.

Пусть $N_q(g)$ обозначает максимальное число F_q рациональных точек, которое кривая рода

g может иметь. Кривая C рода g является оптимальной над F_q, если её число F_q рациональных точек $\#C(F_q)$ равно $N_q(g)$. Главный результат для теории определяется теоремой Хассе-Вейля.

Теорема 1 [7]. Пусть C — проективная и несингулярная, абсолютно неразложимая кривая, определенная над конечным полем F_q с q элементами. Тогда число F_q рациональных точек кривой определяется неравенством

$$N_q(g) \le 1 + q + 2\sqrt{q}g(C).$$

Для максимальных кривых над конечным полем достигается максимальное отношение числа точек кривой к роду. Основные асимптотические результаты для кривых следующие.

Пусть $N_q(g) = \max_C \#C(F_q)$ — число точек кривой C над F_q, где C пробегает все кривые рода $g(C) = g$. Асимптотическая оценка имеет вид

$$A(q) = \limsup_{g\to\infty} N_q(g)/g.$$

Используя верхнюю границу для $N_q(g) \le q + 1 + \frac{1}{2}\sqrt{(8q+1)g + 4(q^2-q)g} - g$, граница для $A(q)$ впервые была получена Ihara Y. [8]

$$A(q) \le \frac{1}{2}(\sqrt{8q+1} - 1).$$

Отметим, что из границы Хассе-Вейля прямо следует

$$A(q) \le 2\sqrt{q}.$$

Если $g > \sqrt{q}(\sqrt{q}-1)/2$, $N_q(g)$ лежит ниже границы Хассе-Вейля.

Основываясь на идее Ihara Y., Дринфельд и Влэдуц показали [9], что

$$A(q) \le \sqrt{q} - 1$$

и в случае $q = l^2$ на модулярных кривых следует равенство $A(l^2) = l - 1$.

Известна также нижняя граница Цинка для оценки $A(q^3) \ge \frac{2(q^2-1)}{q+2}$ [10].

Замечание 2. Для криптографических применений интерес представляют алгебраические кривые, определенные над конечным полем F_q с как можно большим отношением числа точек кривой к её роду.

Наилучший результат универсального хеширования достигается на максимальных кривых.

2. УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНЫМ КРИВЫМ

Главный результат для максимальных кривых представлен в теоремах 2 и 3. В таблице 1 представлены максимальные кривые над полем F_{l^2}.

Теорема 2 [11]. Пусть C кривая над F_q рода g и удовлетворяются следующие условия

1. $g > (\sqrt{q}-1)^2/4$;

2. $\#C(F_q) = q + 2g\sqrt{q} + 1$, ($C$ является максимальной над F_q).

Тогда X является F_q изоморфной кривой Эрмита над F_q и её род $g = \sqrt{q}(\sqrt{q}-1)/2$.

Теорема 3 [12]. Для положительного целого s заданы $q = 2q_0^2$ и $q_0 = 2^s$. Пусть X кривая над F_q рода g и удовлетворяются следующие условия:

1. $g = q_0(q-1)$;

2. $\#X(F_q) = q^2 + 1$.

Тогда X является F_q изоморфной кривой Дэлигнэ-Лустига, ассоциированной с группой Судзуки $Sz(q)$.

Размерность функционального поля кривой Эрмита определяется леммой 1.

Лемма 1. Пусть P — рациональная точка на кривой Эрмита над полем F_q, $q = l^2$. Тогда подгруппа Вейерштрасса $H(P) = \langle l, l+1\rangle$. Кривая Эрмита является максимальной и определяется линейной серией размерности $\dim = 2$.

Результаты по максимальным плоским кривым в конечном поле F_q, $q = l^2$ представлены в табл. 1.

Замечание 3.

1. Алгебраические кривые:

$$y^l + y = x^{l+1},$$
$$y^l + y = x^{(l+1)/2},$$
$$\sum_{i=1}^{t} y^{l/2^i} = x^{l+1},\ l = 2^t$$

являются максимальными кривыми первого и второго рода, имеют подгруппу Вейерштрасса $H(P_\infty) = \langle \rho_1, \rho_2\rangle$ размерности $\dim = 2$ и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

2. Алгебраические кривые:

$$y^l + y = x^{(l+1)/3},\ l \equiv 2 (\mathrm{mod}\, 3),$$
$$\sum_{i=0}^{t-1} y^{3^i} = \omega x^{l+1},\ l = 3^t,\ \omega \in F_{l^2}\ \ \omega^{l-1} = -1$$

являются максимальными кривыми третьего рода, имеют подгруппу Вейерштрасса $H(P_\infty) = \langle \rho_1, \rho_2\rangle$ размерности $\dim = 2$ и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

3. Максимальные кривые вида:

$$x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0,\ l \equiv 2 (\mathrm{mod}\, 3),$$
$$\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0,$$
$$l \equiv 1 (\mathrm{mod}\, 3),\ \omega \in F_{l^2},\ \omega^{l-1} = -1,$$
$$y^l + y = \left(\sum_i^t x^{l/3^i}\right)^2,\ l = 3^t$$

имеют подгруппу Вейерштрасса $H(P_\infty)$ размерности $\dim = 3$ и функциональное поле определяется рациональными функциями вида $\{x^i \cdot y^j \cdot v^t\}$.

4. Кривая Дэлигнэ-Лустига, ассоциированная с группой Судзуки, определяется полной линейной серией $D = |(q + 2q_0 + 1)P_0|$ размерности $\dim = 4$ и степени $q + 2q_0 + 1$, которая выводится из энумератора зета функции. Кривая

Таблица 1

Максимальные кривые над квадратичным полем F_{l^2}

Уравнение кривой $C(F_{l^2})$	Значение рода кривой	Ограничения на коэффициенты кривой	Значение подгруппы Вейерштрасса
$y^l + y = x^{l+1}$	$g_1 = l(l-1)/2$		$\langle l, l+1\rangle$
$y^l + y = x^{(l+1)/2}$	$g_2 = (l-1)^2/4$	l нечетное	$\langle (l+1)/2, l\rangle$
$\sum_{i=1}^{t} y^{l/2^i} = x^{l+1}$	$g'_2 = l(l-2)/4$	$l = 2^t$	$\langle l/2, l+1\rangle$
$y^l + y = x^{(l+1)/3}$	$g'_3 = (l^2 - 3l + 2)/6$	$l \equiv 2 \pmod 3$	$\langle (l+1)/3, l\rangle$
$\sum_{i=0}^{t-1} y^{3^i} = \omega x^{l+1}$	$g_3'' = l(l-3)/6$	$l = 3^t$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$	$\langle l/3, l+1\rangle$
$x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0$	$g_3 = (l^2 - l + 4)/6$	$l \equiv 2 \pmod 3$	$\langle 2(l+1)/3, l, l+1\rangle$
$\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0$	$g_3''' = l(l-1)/6$	$l \equiv 1 \pmod 3$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$	$\langle (2l-1)/3, l, l+1\rangle$
$y^l + y = \left(\sum_i^t x^{l/3^i}\right)^2$	$g_3''' = l(l-1)/6$	$l = 3^t$	$\langle 2l/3, l, l+1\rangle$
$x^{2(l+1)/3} y^{(l+1)/3} + y^{2(l+1)/3} + x^{(l+1)/3} = 0$	$g_3 = (l^2 - l + 4)/6$	$l \equiv 2 \pmod 3$	$\langle (2l+1)/3, l, l+1\rangle$

Судзуки имеет отображение на проективное пространство P^4 и подгруппу Вейерштрасса $H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$,

$$P \in X(F_q).$$ [8].

Кривая Судзуки имеет представление

$$y^q - y = x^{q_0}(x^q - x),$$

определена над полем F_q, $q = 2q_0^2$, $q_0 = 2^s$, рода $g = q_0(q-1)$ и имеет число точек $N = q^2 + 1$.

Точками кривой являются особая точка на бесконечности $P_0 = (0:1:0)$ кратности q_0 и рациональные точки $P_{a,b} = (a:b:1)$, где $a, b \in F_q$ и $b^q - b = a^{q_0}(a^q - a)$.

Базис пространства $L(\rho_\ell P_0)$, задается функциями вида

$$\{w^j \cdot v^i \cdot y^t \cdot x^r : i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + r \cdot q \le \rho_\ell\},$$

что следует из подгруппы Вейерштрасса $H(P_0)$, представленной порядками полюсов функций $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Порядки полюсов равны

$$div_\infty(x) = qP_0,\ div_\infty(y) = (q+q_0)P_0,$$
$$div_\infty(v) = (q+2q_0)P_0,\ div_\infty(w) = (q+2q_0+1)P_0.$$

Кривая Судзуки представляется в P^4 множеством точек вида

$$P(a,b) := (1:a:b:f(a,b):af(a,b)+b^2)$$
$$\cup\pi(P_0) = (0:0:0:0:1),$$

где $a, b \in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$.

5. Кривая Ферма вида

$$x^{(q-1)/3} + y^{(q-1)/3} + z^{(q-1)/3} = 0$$

над F_q, $q \equiv 1 \pmod 3$, является одной из лучших плоских кривых с большим числом точек

$$N = 2(q-1)^2/9.$$

3. ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЯ ТОЧЕК АЛГЕБРАИЧЕСКИХ КРИВЫХ ПО КЛЮЧЕВЫМ ДАННЫМ

Важный фактор практической реализации хеширования по точкам кривой состоит в вычислении точек кривой по ключевым данным.

Оценки сложности вычисления точек алгебраических кривых над полем F_q представлены в табл. 2.

Замечание 4.

1. Для хеширования над конечным полем F_q по проективной прямой значение ключа может быть прямо отождествлено с элементом поля $\alpha \in F_q$.

2. При хешировании по кривой Сузуки, как следует из уравнения $b^q - b = a^{q_0}(a^q - a)$ значения точки $P_{a,b} = (a:b:1)$, $a, b \in F_q$, могут быть выбраны независимо. Ограничения на выбор a и b определяются тем, что по алгоритму хеширования рациональные функции функционального поля кривой не должны равняться 0, т.е. $a \ne 0$, $b \ne 0$, $a^{2q_0+1} + b^{2q_0} \ne 0$, $ab^{2q_0} + a^{2q+2q_0} + b^{2q_0} \ne 0$, что уменьшает ключевое пространство до $q^2 - 4q$. Назначение $a \ne 0$, $b \ne 0$ по ключу потребует проверок $a^{2q_0+1} + b^{2q_0} \ne 0$, $ab^{2q_0} + a^{2q+2q_0} + b^{2q_0} \ne 0$. Вероятность успеха при случайном задании a и b, $a, b \in F_q$ будет определяться соотношением

$$\Pr = \left|\left\{P(a:b:1), a^{2q_0+1} + b^{2q_0} \ne 0, ab^{2q_0} + a^{2q_0+2} + b^{2q} \ne 0\right\}\right| / \left|\left\{P(a:b:1), a \ne 0, b \ne 0\right\}\right| =$$
$$(q^2 - 4q)/(q-1)^2 \approx 1 - 4/q.$$

3. Кривая Ферма $x^{(q-1)/3} + y^{(q-1)/3} + z^{(q-1)/3} = 0$ имеет большое число точек $N = 2(q-1)^2/9$ и

Таблица 2

Оценки сложности вычисления точек алгебраических кривых над полем F_q

Уравнение кривой	Число точек кривой N над полем F_q	Вычисление точек кривой $P_{a,b}=(a:b:1)$, $a,b\in F_q$	Вероятность успеха определения точки кривой
Проективная прямая	q	$a\neq 0$	1
Кривая Эрмита $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$	$q\sqrt{q}$	$b^{\sqrt{q}}+b=a^{\sqrt{q}+1}$, $a\neq 0$, $b\neq 0$, $b=\alpha^{i\cdot(q-1)+j}$, $a=\alpha^{s+t(q-1)}$, $i=\overline{0,\sqrt{q}}$, $j=\overline{0,\sqrt{q}-2}$ $t=\overline{0,\sqrt{q}}$, $\alpha^{s\cdot(\sqrt{q}+1)}=tr(b)$, $\alpha\in F_q$	$1/\sqrt{q}$
Максимальные кривые второго рода $y^{\sqrt{q}}+y=x^{(\sqrt{q}+1)/2}$	$(q-1)\sqrt{q}/2+\sqrt{q}+1$	$b^{\sqrt{q}}+b=a^{(\sqrt{q}+1)/2}$, $a\neq 0$, $b\neq 0$ $b=\alpha^{i\cdot(\sqrt{q}-1)+j}$, $a=\alpha^{2s+2t(\sqrt{q}-1)}$, $i=\overline{0,\sqrt{q}}$, $j=\overline{0,\sqrt{q}-2}$, $t=\overline{0,(\sqrt{q}+1)/2-1}$, $\alpha^{s(\sqrt{q}+1)}=tr(b)$, $\alpha\in F_q$	$1/2\sqrt{q}$
Максимальные кривые третьего рода $y^{\sqrt{q}}+y=x^{(\sqrt{q}+1)/3}$	$(q-1)\sqrt{q}/3+\sqrt{q}+1$	$b^{\sqrt{q}}+b=a^{(\sqrt{q}+1)/3}$, $a\neq 0$, $b\neq 0$ $b=\alpha^{i\cdot(\sqrt{q}-1)+j}$, $a=\alpha^{3s+3t(\sqrt{q}-1)}$, $i=\overline{0,\sqrt{q}}$, $j=\overline{0,\sqrt{q}-2}$, $t=\overline{0,(\sqrt{q}+1)/3-1}$, $\alpha^{s\cdot(\sqrt{q}+1)}=tr(b)$, $\alpha\in F_q$	$1/3\sqrt{q}$
Кривая Ферма $x^{(q-1)/3}+y^{(q-1)/3}+1=0$	$2(q-1)^2/9$	$a^{(q-1)/3}+b^{(q-1)/3}+1=0$, $a\neq 0$, $b\neq 0$,	2/9
Кривая Сузуки $y^q-y=x^{q_0}(x^q-x)$	q^2-4q	$b^q-b=a^{q_0}(a^q-a)$, $a\neq 0$, $b\neq 0$, $a^{2q_0+1}+b^{2q_0}\neq 0$, $ab^{2q_0}+a^{2q+2q_0}+b^{2q}\neq 0$	$1-4/q$

значения координат $P_{a,b}(a:b:1)$ могут быть выбраны независимо. Ограничения на выбор $a\neq 0$ и $b\neq 0$ определяются алгоритмом хеширования по рациональным функциям функционального поля кривой. Вероятность успеха при случайном выборе a и b, $a,b\in F_q$ по ключевому слову будет определяться выражением

$$\Pr=(2(q^2-1)/9-2(q-1)/3))/$$
$$(q-1)^2\approx 2/9-2/(3(q-1))\approx 2/9.$$

4. Кривая Гурвица

$$x^{2(q-1)/3}y^{(q-1)/3}+y^{2(q-1)/3}+x^{(q-1)/3}=0$$

имеет большее число точек $N=2(q-1)^2/3$. Вероятность успеха выбора точки $P_{a,b}(a:b:1)$ по ключу будет выше и равна $\Pr\approx 2/3$.

5. Точка хеширования $P_{a,b}(a:b:1)$ по кривой Эрмита определяется решением уравнения $b^{\sqrt{q}}+b=a^{\sqrt{q}+1}$, $a\neq 0$, $b\neq 0$.

Утверждение 2. Вычисление точки хеширования по кривой Эрмита определяется задачей дискретного логарифма.

Действительно $b^{\sqrt{q}}+b=tr(b)=c$, $b\in F_q$ и $c\in F_{\sqrt{q}}$. Пусть α — образующий элемент F_q и $\gamma=\alpha^{\sqrt{q}+1}$ является образующим элементом $F_{\sqrt{q}}$. Тогда $c=\gamma^s$ и $a=\alpha^s$. Решение уравнения $c=\gamma^s$ относительно показателя s имеет сложность задачи дискретного логарифма. Для переборного метода вероятность нахождения решения имеет оценку $\Pr\approx 1/\sqrt{q}$.

6. Максимальные кривые второго и третьего рода имеют в 2 и 3 раза меньше точек по сравнению с кривой Эрмита. Вычисление точек хеширования $P_{a,b}(a:b:1)$ по ключевым данным определяется задачей дискретного логарифма. Просто показать, что оценки для вероятности нахождения решения имеют значения $1/(2\sqrt{q})$ и $1/(3\sqrt{q})$ соответственно.

ВЫВОДЫ

1. Построение хеширования по алгебраическим кривым определяется вычислением точки кривой по ключевым данным. Наилучший результат достигается на плоских кривых Ферма и Гурвица с большим числом точек. Применение кривых Ферма и Гурвица снимает практическое ограничение на поле вычисления точек кривых, число точек кривых практически равняется размерности конечного поля и назначение по ключевым данным точки кривой реализуется с вероятностью близкой к единице.

2. Назначение точек кривой Судзуки по ключу имеет наибольшую вероятность успеха, требует дополнительных проверок и имеет ограничение на поле вычислений. Кривые Судзуки имеют представление в поле характеристики 2 с нечетной степенью расширения.

3. Максимальные кривые Эрмита, кривые второго и третьего рода имеют определение над квадратичным полем, наилучшие оценки вероятности коллизии для плоских алгебраических кривых, но задача вычисления значений точек кривых по ключевым данным имеет сложность решения задачи дискретного логарифма.

Литература

[1] Bierbrauer J. Authentication via algebraic-geometric codes. / Bierbrauer J. // URL http://www.math.mtu.edu/~jbierbra/ potpap.ps.

[2] Халимов Г.З. Аутентификация с применением Эрмитовых кодов. / Халимов Г.З., Иохов А.Ю. // Вестник ХПИ. – Х.: Вып. 9. – 2005. – С. 26–32.

[3] Халимов Г.З. Универсальное хеширование по максимальным кривым / Г.З.Халимов //XIII Международная научно-практическая конференция ”Безопасность информации в информационно-телекомуникационных системах”, Киев, 18-21 мая: тез. докл., 2010. – С.53.

[4] Халимов Г.З. Оценка параметров кривых Гурвица для целей универсального хеширования. Сб. трудов Первой международной научно-технической конференции “Компьютерные науки и технологии”. Белгород, Россия. 8-10 октября. Ч. 2. – 2009. – С. 118–121.

[5] Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 144–146.

[6] Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица / Халимов Г.З. // Журнал “Прикладная радиоэлектроника”. Харьков: ХНУРЭ. — 2010. — Т. 9, № 3. — С. 365–370.

[7] Weil A. Courbes algrebriques et variretres abeliennes / A.Weil // Hermann, Paris, 1971. – P.301.

[8] Ihara Y. Some remarks on the number of rational points of algebraic curves over finite fields / Y. Ihara // J. Fac. Science. Tokio. — 1981. – N. 28. – P. 721–724.

[9] Vladut S.G. Number of points of an algebraic curve / S.G. Vladut ё V.G. Drinfeld // Function Analysis. – 1983. – N. 17 (1). – P. 68–69.

[10] Giulietti M. A new family of Fq2-maximal curves / Giulietti M., Korchmaros G. // prep., 2007.

[11] Ruck H.G. A characterization of Hermitian function fields over finite fields / H.G.Ruck, H.Stichtenoth // J. reine angew. **Mathematics**. – 1994. – V. 457. – P.185–188.

[12] Torres f. The Deligne-Lusztig curve associated to the Suzuki group [Электронный ресурс]/ F.Torres // arXiv:alg-geom/9706012v1 26Jun 1997.

Поступила в редколлегию 18.03.2013

Халимов Геннадий Зайдулович, сведения об авторе см. на стр. 224.

УДК 681.3.06

Оцінки складності універсального гешування за алгебричними кривими/ Г.З. Халімов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 225–229.

Наведено результати універсального гешування за алгебричними кривими. Отримано рішення для обчислення точок найкращих кривих за ключовими даними, оцінки складності обчислень, практичні рекомендації щодо застосування алгебричних кривих для універсального гешування.

Ключові слова: універсальне гешування, максимальні криві.

Табл.: 02. Бібліогр.: 12 найм.

UDC 681.3.06

Estimates of complexity of universal hashing by algebraic curves / G.Z. Khalimov // Applied Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 225–229.

This paper presents the results of universal hashing by algebraic curves. Solutions for computing the best points of curves by key data, estimates of the computational complexity, practical recommendations of using algebraic curves for universal hashing are obtained.

Keywords: universal hashing, maximal curves.

Tab.: 02. Ref.: 12 items.

УДК 621. 3.06

О ПРИХОДЕ ИТЕРАТИВНЫХ ШИФРОВ К СТАЦИОНАРНОМУ СОСТОЯНИЮ, СВОЙСТВЕННОМУ СЛУЧАЙНОЙ ПОДСТАНОВКЕ

И.В. ЛИСИЦКАЯ, К.Е. ЛИСИЦКИЙ

В статье обосновывается положение о том, что произведение цикловых шифрующих преобразований с ростом их числа приходит к случайной подстановке.

Ключевые слова: случайная подстановка, произведение подстановочных преобразований, механизм случайного перемешивания.

ВВЕДЕНИЕ

Одним из ключевых моментов развиваемой новой идеологии оценки показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа является положение, в соответствии с которым практически все известные итеративные шифры после небольшого начального числа циклов шифрования приходят к стационарному состоянию, свойственному случайной подстановке соответствующей степени [1]. Заметим, что для Фейстель-подобных шифров DES, ГОСТ и некоторых других переход к стационарному состоянию оказывается более затянутым по сравнению с другими итеративными шифрами.

Сегодня эти результаты подтверждены уже большим числом экспериментов, как с малыми, так и большими версиями современных шифров и опубликованы нами в ряде работ [2–5 и мн. др.].

До сих пор мы не смогли найти теоретического обоснования этому свойству. Удалось лишь показать [1], что после достижения стационарного распределения на выходе итеративного шифра при дальнейшем наращивании числа его циклов это стационарное распределение сохраняется. В этой работе мы представляем дополнительные результаты исследований по обоснованию правомерности приведенного утверждения.

В первой части работы изучаются свойства произведений подстановочных преобразований. Во второй её части представляются соображения по теоретическому обоснованию показателей случайности произведения подстановок. В заключении приводится обсуждение полученных теоретических и экспериментальных результатов.

1. СВОЙСТВА ПРОИЗВЕДЕНИЯ ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

Напомним, что в работе [6] было показано, что все известные итеративные шифры являются Марковскими шифрами (первого или второго порядка). Воспользуемся результатом из работы [3], в соответствии с которым для Марковского шифра первого порядка формирование матрицы переходных вероятностей всего шифра (здесь под матрицей переходных вероятностей понимается дифференциальная таблица, связывающая разности текстов на входе шифра с соответствующими разностями на его выходе) сводится к последовательному выполнению r однотипных (одноцикловых) преобразований входного блока данных.

По результатам экспериментов в работе [6] сделан вывод о том, что *произведение одноцикловых преобразований после небольшого начального числа их повторений приобретает свойства случайной подстановки соответствующей степени независимо от показателей случайности исходного одноциклового преобразования.*

Для подтверждения этих слов в [6] были приведены результаты вычислительного эксперимента с подстановками 256-й степени ($n = 8$). В таблице 1 мы воспроизводим результаты вычислительного эксперимента по определению максимумов XOR таблиц последовательности подстановочных преобразований для двух байтовых подстановок. Одна подстановка взята с показателем δ-равномерности равным 4-м, а вторая с показателем δ-равномерности равным 8-ми. Видно, что обе подстановки (их произведение) уже на втором цикле приходят к максимуму дифференциала равному 10–12, характерному для случайной подстановки степени 2^8 [7].

Интересно отметить, что результат не зависит от ключевых значений, если их ввести после каждого подстановочного преобразования.

Конечно, по законам комбинаторики этот процесс должен быть периодическим, но для интересующих нас значений мы, как правило, оказываемся очень далеко от циклового периода подстановки.

Таблица 1

Распределение максимумов XOR таблиц последовательности подстановочных преобразований байтовой подстановки

Число циклов (повторов)	1	2	3	4	5	6	7	8	9	10	11
Значение максимума XOR таблицы для AES S-блока	4	12	12	10	12	12	10	12	12	12	12
Значение максимума XOR таблицы для S-блока шифра Мухомор	8	10	10	12	10	14	12	12	10	12	10

В этой работе нас будет интересовать сам процесс формирования значений переходов произведения подстановочных преобразований.

Рассмотрим две подстановки (не обязательно разные), для которых заданы (определены) их таблицы дифференциальных разностей, которые будем представлять в виде матриц $A=\{a_{ij}\}$ и $B=\{b_{lk}\}$.

Произведение матриц $C=AB$ мы бы выполняли по правилам $c_{ik}=\sum_{l=1}^{2^n} a_{il}b_{lk}$, где 2^n – степень подстановки (размер таблицы дифференциальных разностей по строкам или столбцам). Но умножение подстановок есть последовательное их выполнение одна за другой, т.е. для произведения подстановочных преобразований мы будем иметь для каждой ячейки результата сумму, но не произведений переходов, а значений последовательной реализации переходов для первой и второй подстановок, которые, как мы убедимся, формируются случайным образом.

Поясним это на примере. Пусть мы рассматриваем произведение самого на себя подстановочного преобразования (10 2 0 6 15 1 12 4 14 11 7 13 9 5 3 8) (произведение одинаковых полубайтовых подстановочных преобразований). Здесь для упрощения рассуждений мы взяли подстановку степени 16 ($n=4$) Очевидно, что

$$(10\ 2\ 0\ 6\ 15\ 1\ 12\ 4\ 14\ 11\ 7\ 13\ 9\ 5\ 3\ 8)\times$$
$$\times(10\ 2\ 0\ 6\ 15\ 1\ 12\ 4\ 14\ 11\ 7\ 13\ 9\ 5\ 3\ 8)=$$
$$=(7\ 0\ 10\ 12\ 8\ 2\ 9\ 15\ 3\ 13\ 4\ 5\ 11\ 1\ 6\ 14).$$

Дифференциальная таблица для подстановки (10 2 0 6 15 1 12 4 14 11 7 13 9 5 3 8) имеет вид (это одна из подстановок, сконструированных регулярными методами [8]):

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0
0	2	2	2	0	0	2	0	0	0	**0**	2	4	2	0	0
0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
0	**0**	0	2	0	0	4	2	2	0	0	0	0	2	2	2
0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
0	4	0	0	2	0	0	2	2	0	2	**0**	2	2	0	0
0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0
0	2	**0**	4	0	0	0	2	0	2	2	2	0	0	2	0
0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
0	2	4	0	0	2	2	2	0	0	2	0	**0**	0	0	2

Произведение рассматриваемой подстановки саму на себя будет иметь дифференциальную таблицу:

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2	0	0	0	**0**	0	4	2	2	0	4	0	0	0	2	0
0	2	0	0	0	0	0	2	2	0	0	0	2	6	0	2
0	0	0	0	0	2	2	4	0	2	2	4	0	0	0	0
0	0	4	4	0	0	0	0	2	0	0	2	2	0	0	**2**
0	0	2	2	0	6	2	0	2	0	2	0	0	0	0	0
0	0	2	2	2	2	0	0	0	0	0	0	0	0	4	4
0	0	0	0	2	2	0	**0**	4	2	0	2	0	2	2	0
0	2	0	4	2	0	0	0	0	2	0	0	0	2	2	2
0	0	0	2	0	0	0	2	2	6	2	0	0	0	0	2
0	2	2	2	0	2	0	0	0	2	0	0	2	0	4	0
0	0	2	0	6	0	2	2	2	0	0	0	0	0	0	2
0	2	2	0	0	0	0	0	0	0	0	2	2	4	2	0	2
0	2	0	0	2	2	2	0	0	0	**2**	4	2	0	0	0
0	4	2	0	0	0	0	2	0	0	2	0	2	2	2	0
0	0	0	0	2	0	4	2	0	2	0	2	2	2	0	0

Когда строится таблица произведения подстановок, необходимо для фиксированного входа исходной подстановки рассматривать все возможные пары входов с фиксированной разностью. Для всего этого набора входов получаются входы во вторую подстановку как весь набор значений выходов (строки дифференциальной таблицы) для соответствующей фиксированной разности входа. В результате для заданного значения разности на выходе произведения подстановок необходимо просмотреть и просуммировать все значения переходов, которые формируются каждым из входов во вторую подстановку (значениями пар, формирующих выходные разности строки таблицы дифференциальных разностей первой подстановки), в заданную выходную разность, определяемую элементами соответствующего столбца дифференциальной таблицы второй подстановки. Действительно получается, что в формировании интересующего нас перехода участвуют элементы дифференциальных таблиц, фигурирующих в произведении матриц. Но в нашем случае результат взаимодействия переходов, фигурирующих в «произведении», определяется возможностью реализации перехода произведения подстановок, а именно согласованием пар текстов, формирующих выходные разности первой подстановки с допустимыми парами входов, формирующих заданную выходную разность второй подстановки, а этот процесс оказывается случайным.

Рассмотрим, например, процесс формирования переходов $c_{ik}=\Lambda_\pi(\Delta X=1,\Delta Z=6)=4$ и $c_{ik}=\Lambda_\pi(\Delta X=1,\Delta Z=2)=0$ для дифференциальной таблицы произведения подстановок.

Выпишем значения строки и столбца таблицы разностей, участвующих в формировании этих переходов, в две колонки:

$c_{ik} = \Lambda_\pi(\Delta X = 1, \Delta Z = 6) = 4$ $c_{ik} = \Lambda_\pi(\Delta X = 1, \Delta Z = 2) = 0$

0	0	0	0
0	4	0	0
0	0	0	0
0	2	0	2
0	0	0	2
2	2	2	2
2	0	2	0
0	0	0	2
4	0	4	0
0	0	0	0
2	0	2	0
2	2	2	2
2	0	2	0
0	2	0	0
2	0	2	2
0	4	0	4

Видно, что в первом случае в формировании интересующего нас перехода произведения участвуют два перехода исходной подстановки, причём первый переход $\Delta X = 1 \to \Delta Y = 6$ равный 2-м формируется одной и той же разностью входов (одной и той же парой входов) и далее при проходе второй подстановки $\Delta Y = 6 \to \Delta Z = 6$ пара выходов первой подстановки повторила пару текстов (входов во вторую подстановку), формирующих выходную разность $\Delta Y = 6$. Совершенно аналогичная ситуация состоялась и для второго перехода. В результате эти два перехода дали результирующее значение ячейки дифференциальной таблицы произведения подстановок равное 4-м.

Во втором случае из трёх ненулевых пар переходов, входящих в сумму ни один не оказался согласованным по парам текстов, формирующих разности на выходе первой подстановки с парами текстов, формирующих переход во второй подстановке в выходную разность $\Delta Z = 2$. Здесь результатом (значением ячейки дифференциальной таблицы произведения подстановок) является 0.

Как мы видим процесс формирования переходов действительно оказывается случайным. Чтобы состоялся ненулевой переход входной разности $\Delta X \neq 0$ в выходную разность произведения подстановок $\Delta Z \neq 0$ необходимо:

1) чтобы состоялись ненулевые переходы исходной входной разности ΔX в промежуточные ненулевые выходные разности ΔY первой подстановки, для которых имеются ненулевые переходы в выходную разность ΔZ второй подстановки;

2) чтобы промежуточные выходные разности первой подстановки оказались бы согласованными с входами во вторую подстановку (совпадали бы пары выходов первой подстановки с ненулевыми парами входов во вторую подстановку, имеющими выбранную выходную разность).

В результате мы приходим к случайному механизму формирования переходов подстановки-произведения (даже для подстановки, построенной с помощью регулярных методов, результирующая подстановка получается случайной).

Далее мы будем представлять процедуру формирования значений переходов произведения подстановок в виде

$$c^*_{ik} = \sum_{l=1}^{2^n} a_{il} \circ b_{lk}, \quad (1)$$

$$i,k = 1,2,\ldots,2^n.$$

В этой формуле символ $\circ$ будет обозначать результат осуществления операции последовательного перехода (прохода) a_{il} -го элемента дифференциальной таблицы первой подстановки «через» b_{lk} -й элемент второй.

Отметим, что при увеличении степени подстановок число случайных слагаемых в суммах (1) быстро увеличивается. Для байтовой подстановки это число для ненулевых переходов подстановок, входящих в произведения, будет уже достигать значения близкого к 25.

Таким образом, представленные результаты свидетельствуют о том, что при умножении подстановок связь входов с выходами этого преобразования формируется на основе механизма случайного взаимодействия полного набора выходов первой подстановки с соответствующим набором входов второй подстановки. Поэтому подстановку-произведение можно действительно рассматривать как случайное преобразование (случайную булеву векторную функцию). Далее в связи с отмеченным обстоятельством предлагается краткая подборка материалов, связанных с математическим описанием свойств случайных булевых векторных функций, одним из известных представлений которых являются подстановки.

2. ЭЛЕМЕНТЫ ТЕОРИИ СЛУЧАЙНЫХ ПОДСТАНОВОК. ПРОИЗВЕДЕНИЕ ПОДСТАНОВОК — СЛУЧАЙНАЯ ПОДСТАНОВКА

Напомним некоторые математические факты, изложенные в работе [9], имеющие отношение к случайным преобразованиям. В этой работе рассматриваются дифференциальные свойства n-разрядных m-битных векторных булевых функций.

Мы здесь воспользуемся более общепринятым определением дифференциальной вероятности, отличающимся от соответствующего определения, приведенного в работе [9] тем, что здесь учитывается удвоение значений дифференциального перехода для каждой разности, возникающего при побитном сложении (XOR) входов для одной и той же пары текстов, взятых в разном порядке и то, что множество из 2^n входов для заданной разности образует 2^n пар.

В соответствии с [9] дифференциал над векторной булевой функцией α состоит из входной разности a и выходной разности b и обозначается (a,b). Дифференциальная вероятность (DP)

дифференциала (a,b) определяется числом пар, которые имеют входную разность a и выходную разность b, поделенным на общее число пар с входной разностью a:

$$DP(a,b) = \#\{\{v,u\} \mid v \oplus u = a \;\&\; \alpha(v) \oplus \alpha(u) = b\} / 2^n$$

(в [9] понятие дифференциала связывается с половинным значением ячеек дифференциальной таблицы и соответственно нормировка выполняется по 2^{n-1} ненулевым значениям входной разности). В [9] далее доказывается теорема:

Теорема 1. *Для случайной n-разрядной m-битной векторной булевой функции, мощность $N(a,b)$ данного дифференциала (a,b) является стохастической переменной с биномиальным распределением:*

$$\Pr\big(N(a,b) = 2i\big) = (2^{-m})^i (1-2^{-m})^{2^{n-1}-i} \cdot \binom{2^{n-1}}{i}.$$

Мы здесь опять при записи формулы тоже внесли поправку (учли то, что заполнениями ячеек дифференциальной таблицы являются чётные числа).

Доказательство очень простое: случайная векторная булева функция отображает 2^n различных входных значений v в независимые выходные значения $\alpha(v)$ и, следовательно, она отображает переходы разности пар входов $\{v, u\}$, в независимые выходные разности. Данный дифференциал (a,b), принимающий пару с входной разностью a, является исходом случайного эксперимента, который считается успешным, если выходная разность равна b. Число экспериментов (число различных пар входов преобразования) равно 2^{n-1} и вероятность успеха есть 2^m. Пусть из общего числа 2^{n-1} возможных различных входных пар i пар имеют заданный переход (являются успешными исходами) в выходную разность, а остальные $2^{n-1} - i$ не дают заданного перехода. Тогда число успехов при независимых исходах имеет биномиальное распределение представленного выше вида.

Приведём также следствие из теоремы 1, приведенное в [9] (с нашей коррекцией).

Следствие 1. При $n \geq 5$ и небольшом значении $n - m$, мы имеем:

$$\Pr\big(N(a,b) = 2i\big) \approx e^{-2^{n-m-1}} \frac{2^{(n-m-1)i}}{i!} = \\ = Puasson(i, 2^{n-m-1}).$$

Справедливость следствия вытекает из того, что при $n \geq 5$ и малом значении разности $n - m$, биномиальное распределение близко (хорошо) аппроксимируется распределением Пуассона с параметром $\lambda = 2^{n-m-1}$ [9]. И ещё одно следствие из этой работы.

Следствие 2. *Для случайного векторного Булева преобразования мы имеем*

$$\Pr\big(N(a,b) = 2i\big) \approx Puasson\left(i, \frac{1}{2}\right) = \frac{e^{-\frac{1}{2}}}{i! \cdot 2^i}. \qquad (2)$$

Приведенный результат следует из следствия 1 при $m = n$ и тогда $\lambda = 1/2$ (в работе [9] следствия 1 и 2 представлены под номерами 2 и 4, а теорема 1 представлена под номером 2).

Далее полученные результаты переносятся на случайную подстановку. Отмечается, что в случайной подстановке, входы в определении её таблицы не являются независимыми друг от друга.

Так, для суммы элементов дифференциальной таблицы подстановки-произведения справедливы очевидные соотношения:

$$\sum_{i=1}^{2^n} c^*_{ik} = \sum_{i=1}^{2^n} \sum_{l=1}^{2^n} a_{il} \circ b_{lk} = 2^n,$$

а также

$$\sum_{k=1}^{2^n} c^*_{ik} = \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} a_{il} \circ b_{lk} = 2^n.$$

В серии из 2^{n-1} экспериментов применения пар с заданной входной разностью и наблюдаемой выходной разностью видно, что пары выходов для всех 2^n возможных значений появляются точно один раз. Это ограничение сильно усложняет анализ. К счастью, как отмечается в работе [9], случай подстановок был подробно изучен и описан в работах [10, 11]. За исключением того, что дифференциалы вида (a, 0) с $a \neq 0$ невозможны, получается, что рассмотренная выше вероятность того, что пара с заданной входной разностью отображается в данную выходную разность, заметно не меняется от того факта, что преобразование является подстановкой. Отсюда следует, что при расчете распределения достаточно заменить вероятность успеха в полученном выше соотношении на $1/(2^n - 1)$ для ненулевого выходного различия b и 0 для $b = 0$. При больших n эта замена оказывает незначительное влияние на мощность дифференциалов (a,b) с $b \neq 0$ и, следовательно, следствие 4 для случайных преобразований справедливо и для случайных подстановок.

Мы здесь можем напомнить и результаты нашей работы [12], в которой доказано, что для закона распределения переходов дифференциальной таблицы случайной подстановки действительно справедлива аппроксимация (2).

Так, для рассмотренного выше примера с байтовыми подстановками ($n = 2^8$) из соотношения для определения заполнений XOR таблицы $(2^n - 1)^2 \cdot \Pr\big(N(a,b) = 2i\big)$, следующего из закона распределения вероятностей (2), получим для $i = 5$ результат 10,24, в то время как для $i = 6$ имеем 0,854, т.е. значения максимумов дифференциалов для случайной подстановки степени 2^8 как раз получаются равными 10-ти или 8-ми, как в нашем эксперименте.

В заключение отметим, что совершенно аналогичные выводы в отношении показателей случайности произведения подстановок будут справедливы и для линейных характеристик этого преобразования. И в этом случае значения

переходов, связывающие маски входов и выходов произведения подстановок, будут формироваться с использованием отмеченного случайного механизма взаимодействия переходов подстановок-сомножителей. Только теперь необходимо будет рассматривать взаимодействие элементов строк и столбцов линейных аппроксимационных таблиц подстановок. Как и в случае дифференциальных переходов произведения подстановок и в этом случае значения слагаемых соотношения вида (1) для каждого из переходов произведения не могут быть больше меньшего из значений переходов подстановок-сомножителей.

Для линейных аппроксимационных таблиц в формуле (1) a_{il} (i,l)-й элемент таблицы первой подстановки для пары масок входа и выхода (α_i,β_l), а b_{lk} – (l,k)-й элемент таблицы второй подстановки для пары масок входа и выхода (ξ_l,θ_k), участвующих в рассматриваемом переходе. Символ $\circ$ теперь будет обозначать результат осуществления операции последовательного перехода (прохода) a_{il}-го элемента линейной таблицы первой подстановки «через» b_{lk}-й элемент второй. В этом случае должны сшиваться наборы выходных равенств четности первой подстановки с соответствующими наборами равенств четности второй.

Таким образом, действительно *произведение* (*последовательность*) *подстановочных преобразований нетривиального типа* (*а не только шифров*) *является с большой вероятностью случайной подстановкой, независимо от свойств подстановок, участвующих в формировании этого преобразования*.

Мы посчитали, что это утверждение является неким «законом природы», который выполняется независимо от нашего желания.

Конечно, здесь речь идёт не о вырожденных подстановках, к которым мы отнесли подстановки с дифференциальными и линейными показателями, выходящими далеко за рамки среднестатистических показателей случайных подстановок [13].

Одновременно становится понятным, что использование разных (отличающихся) S-блоков в шифрах не будет приносить сколько-нибудь ощутимых преимуществ.

ВЫВОДЫ

В работе представлено обоснование замечательного свойства произведения подстановочных преобразований, которое заключается в том, что результатом произведения является подстановка случайного типа.

Итеративные шифры являются произведением подстановочных преобразований. Даже без введения в циклы случайных подключей шифр после некоторого числа начальных цикловых преобразований становится случайной подстановкой. Для шифров с сильным линейным преобразованием (с байтовыми подстановками) этот процесс является достаточно кратковременным (до трёх–четырёх циклов). Для шифров со слабым линейным преобразованием (с полубайтовыми подстановками) этот процесс перехода шифра к случайной подстановке может затягиваться до 7–10 и более циклов. Переходный период прихода к случайной подстановке, характерный для шифров, связан с тем, что при малом числе циклов шифрования булевы векторные функции, описывающие цикловые преобразования, ещё не связаны со всеми битами входа в цикловое преобразование. Необходимо, чтобы сработал механизм перемешивания выходных битов подстановок, входящих в шифр, реализуемый с помощью соответствующих линейных преобразований.

Одновременно представленные результаты подтверждают новую точку зрения по вопросу оценки безопасности блочных шифров к атакам дифференциального и линейного криптоанализа [14, 15], состоящую в том, что максимумы средних вероятностей дифференциалов и линейных корпусов полноцикловых версий шифров от свойств используемых в них S-блоков (исключая вырожденные их конструкции) не зависят (за исключением шифра DES, допускающего построение итеративных характеристик обнуляющего типа).

Конечно, изложенные выше соображения не могут претендовать на высокую математическую строгость, но приведенные аргументы и примеры, на наш взгляд, можно рассматривать как достаточно убедительное свидетельство правомерности положения, лежащего в основе новой методологии оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1], в соответствии с которым итеративные шифры в результате применения последовательности подстановочных преобразований становятся случайными подстановками.

Литература

[1] Лисицкая И.В. Методология оценки стойкости блочных симметричных шифров. / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123–133.

[2] Долгов В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. / В.И. Долгов, А.А. Кузнецов, С.А. Исаев. // Электронное моделирование. – 2011.– Т 33, № 6. – С. 81–99.

[3] Кузнецов А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2 – С. 135–140.

[4] Лисицкая И.В. Большие шифры – случайные подстановки. Сравнение показателей статистической безопасности блочных симметричных шифров, представленных на украинский конкурс / И.В. Ли-

сицкая, А.А. Настенко, К.Е. Лисицкий // Східно-Європейський журнал передових технологій. – 2012. – Т. 6, № 9 (60). – С. 11–21.

[5] Лисицкая И.В. Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс и их уменьшенных моделей. / И.В. Лисицкая, А.А. Настенко, К.Е. Лисицкий // Автоматизированные системы управления и приборы автоматики. – 2012. – Вып. 159. – С. 31–39.

[6] Лисицкая И.В. Оценки максимальных значений дифференциалов и линейных корпусов Марковских шифров. / И.В. Лисицкая., В.И. Долгов, А.А. Настенко // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2 – С. 144–151.

[7] Олейников Р.В. Дифференциальные свойства подстановок. / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333.

[8] A Description of Baby Rijndael, ISU CprE/Math 533; NTU ST765-U, February 19, 2003.

[9] Joan Daemen, Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers. / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38.

[10] L. O'Connor, "On the Distribution of Characteristics in Bijective Mappings," Advances in Cryptology, Proceedings of Eurocrypt '93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1993, pp. 360–370.

[11] P. Hawkes and L O'Connor, "XOR and Non-XOR Differential Probabilities," Advances in Cryptology, Proceedings of Eurocrypt '99, LNCS 1592, J. Stern, Ed., Springer-Verlag, 1999, pp. 272–285.

[12] Лисицкая И.В. Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок. / И.В. Лисицкая // Вісник Харківського національного університету імені В.Н. Каразіна. – 2011. – № 960. Вип.16. – С. 196–206.

[13] Лисицкая И.В. Вырожденные подстановки. / И.В. Лисицкая // Радиотехника. – 2012. – Вып. 171. – С. 41–49.

[14] Лисицкая И.В. Об участии S-блоков в формировании максимальных значений дифференциальных и линейных вероятностей блочных симметричных шифров / И.В. Лисицкая // Спеціальні телекомунікаційні системи та захист інформації. Вип. 7 (21) – Київ.– 2012. – С. 71–84.

[15] Lisitskaya I.V. Importance of S-Blocks in Modern Block Ciphers. / I.V. Lisitskaya, E.D. Melnychuk, K.E. Lysytskiy // Computer Network and Information Security, 2012, 10, 1-12 ISSN: 2074-9104.

Поступила в редколлегию 19.03.2013

Лисицкая Ирина Викторовна, доктор технических наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники. Научные интересы: криптография, методы криптоанализа.

Лисицкий Константин Евгеньевич, студент Харьковского национального университета радиоэлектроники. Научные интересы: криптография, методы криптоанализа.

УДК 621. 3.06

Про прихід ітеративних шифрів до стаціонарного стану, властивому випадковій підстановці / І.В. Лисицька, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. № 2. – С. 230–235.

У статті обгрунтовується положення про те, що добуток циклових шифруючих перетворень із зростанням їх числа приходить до випадкової підстановки.

Ключові слова: випадкова підстановка, добуток підстановних перетворень, механізм випадкового перемішування.

Таб. 1. Бібліогр.: 15 найм.

UDC 621. 3.06

On the reaching by iterative ciphers of a steady state characteristic of a random permutation / I.V. Lisitskaya, K.E. Lisitsky // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 230–235.

The paper substantiates the thesis that the product of cycle encrypting transformations with the growth of their number results in a random substitution.

Keywords: random substitution, product of substitution transformations, mechanism of accidental mixing.

Tab.: 4. Ref.: 15 items.

УДК 621. 391: 519. 2: 519.7

БЛОЧНЫЕ СИММЕТРИЧНЫЕ ШИФРЫ — СЛУЧАЙНЫЕ ПОДСТАНОВКИ. КОМБИНАТОРНЫЕ ПОКАЗАТЕЛИ

В.И. ДОЛГОВ, М.Ю. РОДИНКО

Доказывается, что подстановки, порождаемые блочными шифрами, имеют асимптотически (на полноцикловой длине) законы распределения возрастаний и инверсий, свойственные случайным подстановкам.

Ключевые слова: малая модель шифра, комбинаторные свойства, инверсии, возрастания.

ВВЕДЕНИЕ

Одним из ключевых моментов развиваемой новой идеологии оценки показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1] является положение, состоящее в том, что все итеративные шифры асимптотически (при полноцикловой длине) являются случайными подстановками.

В частности это означает, что их комбинаторные показатели (инверсии, возрастания и циклы) подчиняются законам распределения инверсий, возрастаний и циклов, найденным для случайных подстановок.

Естественно, что проверить эти свойства на полномасштабных моделях шифров не представляется возможным. Однако эти свойства можно проверить на уменьшенных моделях, полагая, что с ростом степени подстановки (размером битового входа в шифр) его свойства случайности могут лишь усиливаться.

Здесь мы развиваем подход, предложенный в работе [2], в которой были изучены циклические свойства уменьшенной модели шифра Rijndael, и было установлено, что эта малая модель показывает числовые характеристики (математическое ожидание и дисперсию), характерные для асимптотического нормального закона распределения циклов случайной подстановки. Позднее в работе [3] путем сопоставления законов распределения циклов в подстановках, сгенерированных случайным образом и подстановках, сформированных мини-шифром было показано, что по критерию согласия Колмогорова эти законы практически совпадают. Было отмечено, что следует ожидать и повторения шифрами законов распределения инверсий и возрастаний случайных подстановок. Однако это предположение не было подтверждено вычислительными экспериментами.

Теперь мы хотим в полном объёме обосновать это положение.

1. ЭЛЕМЕНТЫ ТЕОРИИ СЛУЧАЙНЫХ ПОДСТАНОВОК

Свойства подстановок случайного типа изучались многими авторами, например [4, 5]. Здесь мы кратко изложим наиболее принципиальные результаты, на которые будем опираться в дальнейшем. Приведём здесь определения и теоремы, доказанные в работе [4]. Напомним кратко и сопровождающий понятийный аппарат.

Инверсии случайных подстановок

На множестве $n!$ перестановок (подстановок) множества $X = \{1, 2, ..., n\}$ зададим вероятное распределение путем приписывания любой перестановке вероятности $1/n!$.

Будем говорить, что элемент $i_k . \in X$, $1 \le k \le n$ образует r инверсий в перестановке $(i_1, i_2, ..., i_n)$, если он расположен впереди r элементов, имеющих меньшие значения.

Первая теорема, связанная со случайными подстановками, касается числа инверсий η_n случайной равновероятной подстановки:

$$\eta_n = \eta_{1n} + \eta_{2n} + ... + \eta_{nn},$$

где η_{kn} — число инверсий в подстановках n-й степени, образуемых i_k-м элементом.

Теорема 1. Если η_n — число инверсий в случайной равновероятной подстановке степени n, при этом $(\eta_n = \eta_{1n} + \eta_2 + ... + \eta_{nn})$, то случайная величина

$$\eta_n' = \left(\eta_n - n^2/4\right) \Big/ \left(n^{\frac{3}{2}}/6\right) \qquad (1)$$

имеет асимптотически нормальное распределение с параметрами (0,1)

Для нас важными будут еще два результата [3].

Циклы случайных подстановок

Для числа циклов случайной равновероятной подстановки справедлива теорема 2.

Теорема 2. Если ξ_n — число циклов случайно равновероятно выбранной подстановки степени n, то случайная величина

$$\xi_n' = \frac{\xi_n - \ln n}{\sqrt{\ln n}} \qquad (2)$$

имеет в пределе нормальное распределение с параметрами (0,1).

Возрастания случайных подстановок

Элементы a_i и a_{i+1} перестановки $(a_1, a_2, ..., a_n)$ чисел 1, 2, ..., n образуют возрастание, если $a_i < a_{i+1}$, $1 \le i \le n-1$.

Теорема 3. Если θ_n — число возрастаний в случайной перестановке (подстановке) степени n, то при $n \to \infty$ случайная величина

$$\theta_n' = \frac{\theta_n - n/2}{\sqrt{n/12}} \qquad (3)$$

в пределе имеет нормальное распределение с параметрами (0,1).

Этих теоретических сведений уже достаточно, чтобы вернуться к решению поставленной задачи.

Нас в дальнейшем будут интересовать возрастания и инверсии.

2. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ВОЗРАСТАНИЙ МИНИ-ВЕРСИЙ ШИФРОВ

Изложим методику построения закона распределения числа возрастаний для малой версии шифра, в которой длина ключа (блока) равна 16 бит. В этом случае для каждого ключа зашифрования из полного множества всех ключей путем последовательных зашифрований (на одном и том же ключе) создаётся массив всех возможных вариантов зашифрованных блоков данных, начиная с зашифрования нулевого значения блока данных, и так последовательно до последнего значения входного блока данных (равного 2^{16}–1). Тем самым в массиве данных запоминается вторая строка нормализованного представления подстановки (шифрующего преобразования). Число возрастаний в подстановке, как известно, равно сумме числа возрастаний для каждого элемента, представляющего собой количество элементов массива, каждый из которых больше предыдущего элемента. Число возрастаний, полученное для каждой подстановки, записывается в специально созданный для этого файл. Таким образом, мы получаем закон распределения плотности вероятности числа возрастаний для сформированных подстановок. В процессе вычислительных экспериментов для шифра Baby-Rijndael был получен закон распределения возрастаний для 65535 подстановок.

В качестве теоретического закона распределения числа инверсий предлагается рассматривать нормальное распределение с параметрами, определяемыми предельной теоремой 3 ($n/2$– математическое ожидание, $\sqrt{n/12}$ – среднеквадратическое отклонение). Соответственно для $n = 65535$ математическое ожидание равно 32767,5; среднеквадратическое отклонение – 73,9.

Для проверки выдвигаемой гипотезы о соответствии эмпирического распределения теоретическому используем критерий Колмогорова-Смирнова, предусматривающий нахождение максимума разности двух интегральных функций распределения:

$$D_n = \max \left| F_{шифра}(x_k) - F_{теорет}(x_k) \right|.$$

В табл. 1 приведены результаты, полученные для мини-версии шифра Rijndael. В силу значительной вариации диапазона значений возрастаний ([32461;33071]) привести полную таблицу со значениями полученных интегральных законов и их разностей не представляется возможным, поэтому мы приводим лишь значения чисел подстановок для выбранных диапазонов.

Таблица 1

Значения количества возрастаний для шифра Baby-Rijndael

Диапазон возрастаний	Количество подстановок
32461-32512	21
32513-32564	168
32565-32616	1131
32617-32668	4581
32669-32720	11209
32721-32772	17437
32773-32824	16619
32825-32876	9781
32877-32928	3593
32929-32980	852
32981-33032	128
33033-33084	15

На рис. 1 представлены функции распределения плотности вероятности для двух законов (более извилистая кривая соответствует экспериментально полученному закону распределения числа возрастаний для подстановок шифра Baby-Rijndael, гладкая кривая соответствует теоретическому закону (асимптотически нормальному закону распределения для диапазона возрастаний с асимптотически предельными параметрами)).В соответствии с методикой, изложенной в [2], максимальная разность двух интегральных законов получилась равной 0,005045. Для уровня значимости $\alpha = 0{,}05$ из таблицы распределения Колмогорова-Смирнова [3] находим $Q(\lambda_0) = 1 - \alpha = 1 - 0{,}5 = 0{,}95 \to \lambda_0 = 1{,}36$. Тогда для $n = 2^{16}$ выходит $\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}36}{256} = 0{,}00531$. Следовательно, $D_n < \frac{\lambda_0}{\sqrt{n}}$. Гипотеза о том, что значения возрастаний в подстановках, формируемых мини-БСШ, распределены по нормальному закону, подтверждается.

Нами также была предпринята попытка доказать соответствие закона распределения возрастаний в Baby-Rijndael и закона распределения случайных подстановок соответствующей степени, как это было сделано в работе [2] для значений циклов. Однако разность полученных законов составила 0,005747. Это значение хоть и незначительно, но превышает пороговое значение 0,00531, что не позволяет нам принять гипотезу о соответствии закона распределения возрастаний в подстановках Baby-Rijndael закону распределения возрастаний в экспериментально полученных случайных подстановках. Это связано с тем, что

генерация случайных подстановок имеет вероятностный характер, и закон, полученный в одном эксперименте, может удовлетворить гипотезе, а закон, полученный в другом эксперименте – нет. Сравнение, осуществляемое с теоретическим нормальным законом, свойственным случайным подстановкам, является более строгим и не оставляет места сомнениям.

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ИНВЕРСИЙ МИНИ-ШИФРОВ

Как и при подсчете возрастаний создаётся массив всех возможных вариантов зашифрованных текстов (строится вторая строка нормализованного представления подстановки). Затем на основе последовательного просмотра и сравнения значений элементов массива с текущим, выбранным для анализа, выполняется подсчет числа инверсий, соответствующего рассматриваемому элементу массива (числа превышений значения текущего рассматриваемого элемента множества значений элементов, стоящих в массиве правее рассматриваемого). Результаты подсчетов числа инверсий для каждого из последовательно выбранных элементов массива нижней строки подстановки суммируется, и, как и в случае с возрастаниями, записывается в файл. Закон распределения инверсий был получен для 65520 подстановок.

Полученные значения инверсий для шифра Baby-Rijndael находятся в диапазоне [1063485006; 1083885006]. В табл. 2 представлены интегральные законы, полученные для ширины интервала дискретности взятия отсчётов числа инверсий, равного 1001000.

Согласно предельной теореме 1 в соответствии с (1) математическое ожидание числа инверсий равно $n(n–1)/4$, среднеквадратическое отклонение – $\sqrt{n^3}/6$. Значения данных параметров при $n = 65520$ равны 1073201220 и 2795178 соответственно.

Из таблицы следует, что максимальная разность двух интегральных законов получилась равной 0,002017. Для уровня значимости $\alpha = 0,05$ из

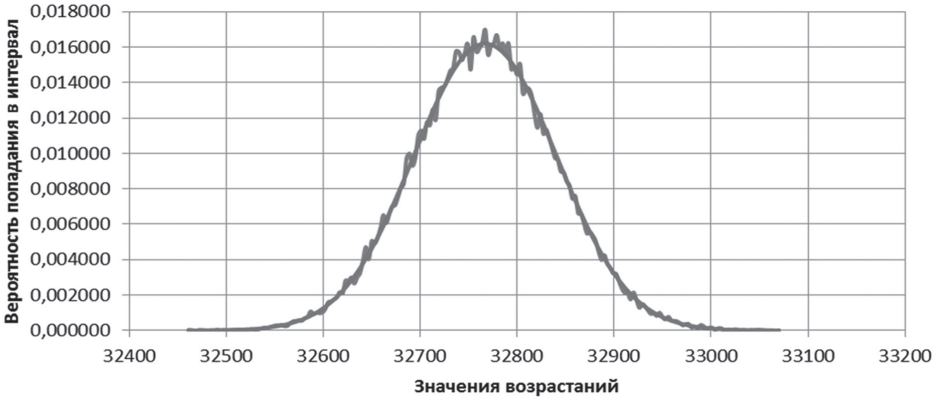


Рис. 1. Экспериментальный и теоретический законы распределения плотности вероятности для числа возрастаний

Таблица 2

Проверка гипотезы о совпадении законов распределения инверсий для шифра и асимптотического нормального закона случайной подстановки

Диапазон инверсий	Количество подстановок	Экспериментальный закон	Теоретический закон	Разность законов
1063606006-1064607006	29	0,000443	0,000569	0,000126
1064607006-1065608006	71	0,001527	0,001889	0,000362
1065608006-1066609006	246	0,005281	0,005568	0,000287
1066609006-1067610006	597	0,014393	0,014606	0,000213
1067610006-1068611006	1289	0,034066	0,034162	0,000096
1068611006-1069612006	2317	0,069430	0,071447	0,002017
1069612006-1070613006	4123	0,132357	0,134073	0,001716
1070613006-1071614006	6061	0,224863	0,226753	0,001890
1071614006-1072615006	7955	0,346276	0,347595	0,001318
1072615006-1073616006	9198	0,486661	0,486413	0,000248
1073616006-1074617006	9167	0,626572	0,626916	0,000343
1074617006-1075618006	8219	0,752015	0,752208	0,000193
1075618006-1076619006	6372	0,849268	0,850647	0,001379
1076619006-1077620006	4464	0,917400	0,918789	0,001389
1077620006-1078621006	2743	0,959265	0,960347	0,001083
1078621006-1079622006	1466	0,981640	0,982678	0,001038
1079622006-1080623006	720	0,992629	0,993249	0,000620
1080623006-1081624006	325	0,997589	0,997658	0,000069
1081624006-1082625006	109	0,999253	0,999278	0,000026
1082625006-1083626006	47	0,999970	0,999803	0,000167
1083626006-1084627006	2	1,000000	0,999952	0,000048

Рис. 2. Закон распределения числа инверсий для шифра мини-Калина

таблицы распределения Колмогорова-Смирнова [6] находим $Q(\lambda_0) = 1 - \alpha = 1 - 0{,}5 = 0{,}95 \rightarrow \lambda_0 = 1{,}36$. Тогда для $n = 2^{16}$ выходит $\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}36}{256} = 0{,}00531$. Следовательно, $D_n < \frac{\lambda_0}{\sqrt{n}}$. Гипотеза о том, что значения инверсий в подстановках, формируемых мини-БСШ, распределены по нормальному закону — подтверждается.

На рис. 2 представлены также результаты построения закона распределения инверсий для шифра Калина, заимствованные из работы [7].

ЗАКЛЮЧЕНИЕ

Таким образом, нами в полной мере обоснован вывод, что блочные шифры на уровне малых моделей по комбинаторным показателям асимптотически являются случайными подстановками. Представляется, что этот вывод полностью переносится и на полномасштабные шифры. Это позволяет в соответствии с методикой, развитой в [1], воспользовавшись формулами, полученными для случайных подстановок, выполнить оценку стойкости полномасштабных БСШ.

Литература

[1] Лисицкая И.В. Методология оценки стойкости-блочных симметричных шифров / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123–133.

[2] Долгов В.И. Анализ циклических свойств блочных шифров. / В.И. Долгов, И.В. Лисицкая, В.И. Руженцев // Прикладная радиоэлектроника. – 2007. – Т.6, №2. – С. 257–263.

[3] Родинко М.Ю., Лисицкий К.Е. Циклические свойства блочных симметричных шифров // Материалы 16-го международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». – 2012. – Т.5. – С. 142–144.

[4] Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982 – 384 с.

[5] Сачков В.Н. Комбинаторные методы дискретной математики. – М.: Наука, 1977. – 319 с.

[6] Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся Втузов. – М.: Наука, 1980. – 976 с.

[7] Долгов В.И.Криптографические свойства уменьшенной версии шифра – Калина / В.И. Долгов, Р.В. Олейников, А.Ю. Большаков, А.В. Григорьев, Е.В. Дробатько // Прикладная радиоэлектроника, 2010. – Т. 9. – № 3. – С. 349–354.

Поступила в редколлегию 22.03.2013

Долгов Виктор Иванович, доктор технических наук, профессор кафедры «Безопасность информационных технологий» ХНУРЭ. Научные интересы: математические методы защиты информации.

Родинко Мария Юрьевна, студентка кафедры БИТ ХНУРЭ. Научные интересы: технологии блочного симметричного шифрования.

УДК 621. 391: 519. 2: 519.7

Блокові симетричні шифри – випадкові підстановки. Комбінаторні показники / В.І. Долгов, М.Ю. Родінко // Прикладна радіоелектроніка: наук. техн. журнал. — 2013. — Том 12. — № 2. — С. 236–239.

Доводиться, що підстановки, які породжуються блоковими шифрами, мають асимптотично (на повноцикловій довжині) закони розподілу зростань та інверсій, властиві випадковим підстановкам.

Ключові слова: мала модель шифру, комбінаторні показники, інверсії, зростання.

Табл.: 2. Іл.: 2. Бібліогр. 6 найм.

UDC 621.391: 519. 2: 519.7

BBlock symmetric ciphers – random substitutions. Combinatorial indicators / V.I. Dolgov, M.Yu. Rodinko // Applied Radio Electronics: Sci. Journ. —2013. — Vol. 12. — № 2. — P. 236–239.

It is proved that substitutions generated by block ciphers asymptotically have (at monocyclelength) distributions of increases and inversions immanent to random substitutions.

Keywords: small cipher model, combinatorial properties, inversions, increases.

Tab.: 2. Fig.: 2. Ref.: 6 items.

УДК 621. 3.06

ИССЛЕДОВАНИЕ СООТВЕТСТВИЯ НОВЫМ КРИТЕРИЯМ ОТБОРА ПОДСТАНОВОЧНЫХ КОНСТРУКЦИЙ СОВРЕМЕННЫХ БСШ

Е.Д. МЕЛЬНИЧУК

Рассматриваются показатели случайности S-блоков ряда современных шифров.

Ключевые слова: подстановка, линейные показатели стойкости, дифференциальные показатели стойкости.

ВВЕДЕНИЕ

Многочисленными экспериментами [1, 3, 4] показано, что все современные шифры после небольшого начального числа циклов зашифрования становятся случайными подстановками (для шифра DES требуется 16 циклов, для остальных 3–4). Здесь имеются в виду повторение шифрами законов распределения вероятностей для числа циклов, инверсий, возрастаний, а также законов распределения вероятностей переходов XOR таблиц и смещения таблиц линейных аппроксимаций соответствующих законов распределения вероятностей случайных подстановок.

Этот факт вызвал интерес к изучению случайных подстановок и исследованию методов их генерации [1, 10] не только как шифрующих преобразований, но и как подстановочных (нелинейных) преобразований, используемых при построении шифров. Выполнен ряд работ по математическому описанию законов распределения вероятностей случайных подстановок [1] и их использованию для построения дополнительных критериев отбора подстановок.

Возникли закономерные вопросы о криптографической значимости подстановок случайного вида: насколько применимы в шифрах подстановки, отобранные по критериям случайности; позволяют ли они улучшить криптографические показатели шифров? Целью этой статьи является изучение ответов на первый вопрос.

В первой части статьи мы кратко излагаем методику оценки показателей случайности подстановок, а во второй мы приводим результаты анализа S-блоков ряда современных шифров на предмет оценки близости их показателей случайности показателям случайных подстановок.

Оценке криптографической пригодности случайных подстановок посвящена наша отдельная работа [1].

1. МЕТОДИКА ОЦЕНКИ ПОКАЗАТЕЛЕЙ СЛУЧАЙНОСТИ ПОДСТАНОВОК

В этой работе мы изучим показатели случайности S-блоков ряда современных шифров. Все S-блоки имеют размер 8×8 (байтовые входы и байтовые выходы). Нас будут интересовать следующие показатели случайности:

- показатели комбинаторной группы критериев (число инверсий, число циклов, число возрастаний);
- линейные и дифференциальные показатели;
- закон распределения переходов таблиц дифференциальных разностей;
- закон распределения переходов таблиц линейных аппроксимаций;
- максимальное расхождение интегральных законов распределения переходов таблиц дифференциальных разностей и таблиц линейных аппроксимаций.
- значение максимума XOR таблицы и число таких максимумов (δ -равномерность);
- значение максимума таблицы ЛАТ и число таких максимумов.

2. КРИТЕРИИ СЛУЧАЙНОСТИ ПОДСТАНОВКИ

Начнем с определения случайной подстановки и критериев случайности подстановки. В частности, в работе [1] введено новое определение случайной подстановки, которое сформулировано в следующем виде:

Подстановка является *случайной*, если вместе с выполнением критериев случайности 1–3 для заполнений ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей (критерий случайности 4 и критерий случайности 5).

Критерий 1. Число инверсий η_n в подстановке степени n приблизительно равно числу “антиинверсий”, а практически, если

$$\left|\eta_n - \frac{n(n-1)}{4}\right| \le a\sigma_\eta,\ \sigma_\eta = \frac{n^{3/2}}{6}.$$

Критерий 2. Число циклов ξ_n в подстановке степени n близко к $\ln n$, а практически, если

$$\left|\xi_n - \ln n\right| \le a\sigma_\xi,\quad \sigma_\xi = \sqrt{\ln n}\,.$$

Критерий 3. Подстановка удовлетворяет критерию случайности 3, если число возрастаний θ_n в подстановке степени n приблизительно равно числу убываний, а практически, если

$$\left|\theta_n - \frac{n}{2}\right| \le a\sigma_\theta,\ \ \sigma_\theta = \sqrt{n/12}\,.$$

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений (по крайней мере, из условия, что множество допустимых подстановок не станет меньше некоторого заданного числа).

Критерий 4. Подстановка удовлетворяет критерию случайности 4, если закон распределения однотипных переходов

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right),\ k=0,1,\ldots,k^*$$

её таблицы XOR разностей для входов, приписываемых к ненулевым характеристикам, соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов (3.2), т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_T(x_k)-F(x_k)|\le b$.

Критерий 5. Подстановка удовлетворяет критерию случайности 5, если закон распределения однотипных переходов $Pr(\lambda^*(\alpha,\beta)=2k)$, $k=0,1,\ldots,k^*$ её таблицы линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения (3.6), т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_T(x_k)-F(x_k)|\le c$.

Утверждение 1. Для любых ненулевых фиксированных ΔX, $\Delta Y\in Z_2^m$ в предположении, что подстановка ϖ выбрана равновероятно из множества S_2^m и $0\le k\le 2^{m-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=\binom{2^{m-1}}{k}^2\cdot\frac{k!\cdot 2^k\cdot\Phi(2^{m-1}-k)}{2^m!},$$

где функция $\Phi(d)$ определяется выражением

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i\cdot\binom{d}{i}^2\cdot 2^i\cdot i!\cdot(2d-2i)!$$

Но тогда становится понятным, что выражение для числа $\Lambda_{m,2k}$ переходов таблицы дифференциальных разностей подстановки порядка 2^m обусловленного типа, – а именно для среднего значения числа ненулевых характеристик $\Delta X\to\Delta Y$, таких, что $\Lambda_\pi(\Delta X,\Delta Y)=2k$, – может быть получено путем умножения выражения (3.2) на число ячеек подматрицы $A_\pi=|a_{i,j}|$ таблицы XOR_π равное $(2^m-1)^2$:

$$\Lambda_{m,2k}=\frac{(2^m-1)^2}{2^m!}\cdot\binom{2^{m-1}}{k}^2\cdot k!\cdot 2^k\cdot\Phi(2^{m-1}-k).$$

Утверждение 5. Пусть $\lambda^*(\alpha,\beta)$ будет случайным значением смещения линейной аппроксимационной таблицы $LAT_\pi^*(\alpha,\beta)$ для пары её входов α и β, когда подстановка ϖ выбрана равновероятно из множества 2^n и α,β не нулевые. Тогда смещения $\lambda^*(\alpha,\beta)$ принимают только четные значения и для $|k|\le 2^{n-2}$

$$Pr\left(\lambda^*(\alpha,\beta)=|2k|\right)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}-|k|}^2.$$

В результате мы можем получить выражение для вычисления $E[\lambda(\pi,2k)]$ как простое умножение формулы (3.10) на общее число ячеек таблицы подстановки, исключая первую строку и первый столбец

$$E[\lambda(\pi,2k)]=\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k|}^2.$$

3. РЕЗУЛЬТАТЫ АНАЛИЗА S-БЛОКОВ ДЛЯ РЯДА СОВРЕМЕННЫХ ШИФРОВ

Для выполнения такого рода исследований на кафедре БИТ ХНУРЭ был разработан программный комплекс, позволяющий получить все интересующие нас оценки.

Результаты вычислительных экспериментов иллюстрируют таблица 1 – таблица 4. На каждой из таких таблиц представлен сам S-блок в общепринятой в литературе системе представлений (вход в таблицу состоит из двух полубайтов – один является входом по строкам, а другой – входом по столбцам, а на пересечении соответствующей строки и столбца читается значение байта в шестнадцатеричном представлении на выходе S-блока).

Как следует из содержания таблиц, на них представлены показатели случайности S-блоков шифров Rijndael, Лабиринт, Мухомор (Калина), Iceberg, ADE, Камелия, GrandCry и Anubis (Khazad).

Таблица 1

S-блок шифра ADE (один из набора)

63	E3	B8	0E	15	AA	D5	41	58	7D	1C	A7	A3	EB	E9	24
65	A1	F7	7F	DC	1D	01	1B	98	79	BC	96	BD	CD	5B	A2
FB	31	99	8D	29	7C	F6	14	27	51	5C	87	C9	CF	C4	A6
9E	4F	6E	30	8C	7A	02	CC	0C	4B	AF	B1	E4	11	18	B6
B4	3D	4A	82	1E	49	8F	B2	46	03	77	84	A9	2D	D8	D0
DA	9A	E1	95	FC	AD	8A	13	36	F9	AE	0D	2B	5A	81	86
06	9B	75	40	7E	C6	CA	4C	0F	4E	EF	71	48	EE	2F	7B
D4	20	EC	8B	05	21	91	F8	A0	67	C1	60	45	3F	89	08
88	57	D7	09	6C	E6	93	A8	DD	5F	ED	72	8E	62	10	C7
F1	33	C8	B0	F2	3B	0B	66	9D	07	DF	3A	BE	F0	BA	5D
BF	56	9F	26	B9	90	83	FE	AC	94	04	FF	97	E8	C0	00
52	6B	B5	DB	85	E5	54	E7	47	39	64	78	12	92	0A	28
D1	9C	1F	44	F3	C3	69	D3	76	2C	2A	61	B7	3C	F4	68
55	E0	F5	80	25	73	6A	59	6D	BB	A5	43	DE	3E	6F	B3
23	D2	C2	D9	A4	53	17	74	50	FD	42	EA	1A	AB	35	22
19	2E	FA	CB	32	CE	E2	38	70	5E	D6	C5	16	37	4D	34

Таблица 2

Показатели случайности S-блока ADE (один из набора)

Количество циклов	3
Количество инверсий	16179
Количество возрастаний	130
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0, 0757866

Таблица 3

Закон распределения элементов таблиц XOR и таблицы LAT S-блока ADE (один из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

Таблица 4

S-блок шифра ADE (второй из набора)

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Таблица 5

Показатели случайности S-блока ADE (второй из набора)

Количество циклов	9
Количество инверсий	15821
Количество возрастаний	125
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0, 0757866

Таблица 6

Закон распределения элементов таблиц XOR и таблицы LAT S-блока ADE (второй из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

Таблица 7

S-блок шифра AES, GrandCru

63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	B	DB
E0	32	3A	A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	3	F6	E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	D	BF	E6	42	68	41	99	2D	F	B0	54	BB	16

Таблица 8

Показатели случайности S-блока AES, GrandCru

Количество циклов	5
Количество инверсий	16753
Количество возрастаний	126
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0, 0757866

Таблица 9

Закон распределения элементов таблиц XOR и таблицы LAT S-блока AES, GrandCru

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

Таблица 10

S-блок шифра Fox

5D	DE	0	B7	D3	CA	3C	D	C3	F8	CB	8D	76	89	AA	12
88	22	4F	DB	6D	47	E4	4C	78	9A	49	93	C4	C0	86	13
A9	20	53	1C	4E	CF	35	39	B4	A1	54	64	3	C7	85	5C
5B	CD	D8	72	96	42	B8	E1	A2	60	EF	BD	2	AF	8C	73
7C	7F	5E	F9	65	E6	EB	AD	5A	A5	79	8E	15	30	EC	A4
C2	3E	E0	74	51	FB	2D	6E	94	4D	55	34	AE	52	7E	9D
4A	F7	80	F0	D0	90	A7	E8	9F	50	D5	D1	98	CC	A0	17
F4	B6	C1	28	5F	26	1	AB	25	38	82	7D	48	FC	1B	CE
3F	6B	E2	67	66	43	59	19	84	3D	F5	2F	C9	BC	D9	95
29	41	DA	1A	B0	E9	69	D2	7B	D7	11	9B	33	8A	23	9
D4	71	44	68	6F	F2	E	DF	87	DC	83	18	6A	EE	99	81
62	36	2E	7A	FE	45	9C	75	91	C	F	E7	F6	14	63	1D
B	8B	B3	F3	B2	3B	8	4B	10	A6	32	B9	A8	92	F1	56
DD	21	BF	4	BE	D6	FD	77	EA	3A	C8	8F	57	1E	FA	2B
58	C5	27	AC	E3	ED	97	BB	46	5	40	31	E5	37	2C	9E
A	B1	B5	6	6C	1F	A3	2A	70	FF	BA	7	24	16	C6	61

Таблица 11

Показатели случайности S-блока Fox

Количество циклов	8
Количество инверсий	17056
Количество возрастаний	126
Максимум таблицы XOR	16
Количество максимумов XOR	70
Максимальное отклонение XOR	0,046105
Максимум таблицы LAT	32
Количество максимумов LAT	219
Максимальное отклонение LAT	0,187922

Таблица 12

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Fox

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	42361	18686
2	15377	18171
4	5758	15888
6	680	6405
8	754	4280
10	19	983
12	6	352
14	0	41
16	70	219

Таблица 13

S-блок шифра Мухомор (один из набора)

F9	CA	14	61	E4	1C	43	20	4E	54	58	A0	FC	DB	C0	72
22	74	FE	B5	65	A8	25	ED	69	33	F1	B1	36	9	6	9A
8E	90	CF	F6	EA	27	BC	7	7F	D7	3C	7C	44	45	21	6B
1A	52	62	29	13	9B	CC	99	4B	42	B6	1D	C7	91	76	16
92	4F	47	70	98	66	C2	48	96	B	2F	C9	C6	38	8C	63
10	F2	A9	37	A7	D3	55	3D	2C	7A	AF	EE	3E	F5	67	C
77	84	C1	C5	DE	A4	DD	B4	E3	B3	EF	49	E2	71	4C	AD
DF	3	12	19	9C	D9	D2	78	50	DC	AA	15	4	39	9D	D1
2D	11	24	2E	F7	59	FA	1E	68	3A	7E	CB	AE	D6	A5	FD
5F	5	F	6A	A6	E7	EC	30	5C	6F	83	CD	B2	BB	EB	2
28	73	4D	18	A3	86	9F	5B	3F	81	AB	75	1B	6C	E	53
64	FB	26	40	7D	E1	95	34	BF	A	BD	31	2B	B0	F4	8D
E0	1	87	56	CE	FF	5D	6D	A2	6E	88	9E	94	89	46	35
4A	B9	DA	C3	F3	5E	8F	97	B7	D4	51	60	D5	23	57	D0
79	3B	17	C4	B8	C8	7B	2A	D	8B	D8	0	E8	BA	E6	F8
41	85	32	F0	80	93	8	E5	82	BE	E9	1F	A1	8A	AC	5A

Таблица 14

Показатели случайности S-блока Мухомор (один из набора)

Количество циклов	5
Количество инверсий	15601
Количество возрастаний	135
Максимум таблицы XOR	8
Количество максимумов XOR	90
Максимальное отклонение XOR	0, 0045059
Максимум таблицы LAT	30
Количество максимумов LAT	8
Максимальное отклонение LAT	0,0034077

Таблица 15

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Мухомор (один из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	39070	6434
2	20244	12644
4	4827	11330
6	794	9667
8	90	7786
10	0	6067
12	0	4321
14	0	2859
16	0	1785
18	0	1033
20	0	564
22	0	303
24	0	146
26	0	59
28	0	17
30	0	8

Таблица 16

S-блок шифра Мухомор (второй из набора)

C	68	DE	9F	42	C0	AA	55	CC	1B	24	16	27	C9	21	AC
97	A9	A5	7C	FC	4	D7	E1	BC	C3	51	D9	F1	B6	D1	74
2F	A	6A	3E	83	71	9A	6D	D0	DB	25	2	A6	8A	DC	B3
FB	9D	E4	4A	69	89	7F	E0	B9	F2	A0	A8	D3	77	10	57
AD	54	6C	C7	11	C5	86	B5	36	0	14	E3	BF	5C	52	18
92	33	D2	8C	E5	1A	34	50	56	87	F3	78	29	22	9E	D8
FA	2E	75	2D	E9	C1	B2	AB	C2	DF	D5	7D	FD	A1	CD	31
AF	F	D6	F7	88	BE	5F	4E	5A	7B	C6	67	6E	5	1E	40
70	B0	F4	60	98	76	7	E	19	F5	8D	28	95	2A	44	32
23	1C	2C	D4	E8	6	91	6B	ED	66	94	93	BD	20	BB	BA
1F	E7	82	3C	EB	FE	CA	30	80	EE	5B	46	8E	9B	7A	F9
17	61	DA	E2	A3	EA	58	9C	B7	99	3A	73	35	FF	CE	B4
8F	CB	90	4C	5D	A7	62	DD	64	F6	37	8B	E6	15	D	4D
2B	AE	53	1D	3B	85	F0	39	81	48	84	F8	45	59	13	38
8	63	6F	EF	1	A2	96	B8	43	79	A4	C8	B	C4	5E	4F
3D	3F	EC	12	7E	49	4B	47	9	72	3	41	B1	26	65	CF

Таблица 17

Показатели случайности S-блока Мухомор (второй из набора)

Количество циклов	5
Количество инверсий	17467
Количество возрастаний	134
Максимум таблицы XOR	8
Количество максимумов XOR	80
Максимальное отклонение XOR	0,004090
Максимум таблицы LAT	30
Количество максимумов LAT	6
Максимальное отклонение LAT	0,002807

Таблица 18

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Мухомор (второй из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	39097	6420
2	20140	12438
4	4944	11420
6	754	9811
8	80	7811
10	0	6141
12	0	4228
14	0	2524
16	0	1763
18	0	1052
20	0	585
22	0	319
24	0	125
26	0	49
28	0	31
30	0	6

Таблица 19

S-блок шифра Iceberg

24	C1	38	30	E7	57	DF	20	3E	99	1A	34	CA	D6	52	FD
40	6C	D3	3D	4A	59	F8	77	FB	61	A	56	B9	D2	FC	F1
7	F5	93	CD	0	B6	62	A7	63	FE	44	BD	5F	92	6B	68
3	4E	A2	97	B	60	83	A3	2	E5	45	67	F4	13	8	8B
10	CE	BE	B4	2A	3A	96	84	C8	9F	14	C0	C4	6F	31	D9
AB	AE	E	64	7C	DA	1B	5	A8	15	A5	90	94	85	71	2C
35	19	26	28	53	E2	7F	3B	2F	A9	CC	2E	11	76	ED	4D
87	5E	C2	C7	80	B0	6D	17	B2	FF	E4	B7	54	9D	B8	66
74	9C	DB	36	47	5D	DE	70	D5	91	AA	3F	C9	D8	F3	F2
5B	89	2D	22	5C	E1	46	33	E6	9	BC	E8	81	7D	E9	49
E0	B1	32	37	EA	5A	F6	27	58	69	8A	50	BA	DD	51	F9
75	A1	78	D0	43	F7	25	7B	7E	1C	AC	D4	9A	2B	42	E3
4B	1	72	D7	4C	FA	EB	73	48	8C	C	F0	6A	23	41	EC
B3	EF	1D	12	BB	88	D	C3	8D	4F	55	82	EE	AD	86	6
A0	95	65	BF	7A	39	98	4	9B	9E	A4	C6	CF	6E	DC	D1
CB	1F	8F	8E	3C	21	A6	B5	16	AF	C5	18	1E	F	29	79

Таблица 20

Показатели случайности S-блока Iceberg (близкие показатели у шифра Anubis (Khazad))

Количество циклов	128
Количество инверсий	16108
Количество возрастаний	133
Максимум таблицы XOR	8
Количество максимумов XOR	102
Максимальное отклонение XOR	0,001353
Максимум таблицы LAT	32
Количество максимумов LAT	5
Максимальное отклонение LAT	0,001934

Таблица 21

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Iceberg (близкие показатели у шифра Anubis (Khazad))

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	39275	6419
2	19875	12610
4	4962	11291
6	811	9774
8	102	7881
10	0	6060
12	0	4166
14	0	2892
16	0	1887
18	0	940
20	0	566
22	0	288
24	0	137
26	0	62
28	0	33
30	0	14
32	0	5

Таблица 22

S-блок шифра Лабиринт

E6	F4	73	BE	7	6A	42	F7	41	4C	5	EA	DC	76	D8	6C
74	87	A5	8B	1A	9C	4E	6B	B	24	91	34	4A	2E	F3	E8
DA	64	7A	8F	EF	D4	93	AF	66	13	CF	82	59	D7	31	4F
C4	65	3	BF	D9	68	C5	E2	84	A6	23	99	C7	B0	5B	62
A0	12	83	ED	8C	0	57	DD	22	FF	9A	A4	F5	F9	3D	6D
FA	5C	49	39	43	5E	86	F	B7	67	52	CA	14	38	DB	25
3A	70	E4	1E	4	55	72	DE	56	47	CD	B6	8D	85	88	D6
A9	F0	5F	AE	9	8A	81	53	21	B5	F6	4B	4D	5D	44	2F
2B	F8	D2	D5	35	A2	3F	C6	BB	C2	A3	F1	9F	6F	1D	E1
60	7E	E0	7F	2D	AC	E3	D	BC	9D	C0	FE	3B	D1	1B	C3
80	63	C9	46	79	E7	89	E9	1C	AB	17	97	5A	20	30	EC
71	B8	B2	2	6	F2	E5	FD	28	D3	3E	3C	D0	BA	CE	29
10	B9	50	8	A1	A8	7D	40	1	15	7C	78	33	69	EB	E
6E	7B	77	54	92	58	95	C1	98	EE	1F	9B	96	51	26	61
2A	CC	B4	C	DF	A7	27	9E	32	37	B3	FC	A	AD	2C	19
B1	11	C8	AA	90	18	45	36	75	94	8E	CB	16	BD	FB	48

Таблица 23

Показатели случайности S-блока Лабиринт

Количество циклов	5
Количество инверсий	17043
Количество возрастаний	127
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0,075786

Таблица 24

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Лабиринт

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

В таблице 25 и таблице 26 представлены для сравнения показатели совершенных по рассматриваемым критериям подстановок.

Таблица 25

Распределение парных разностей для XOR таблицы подстановки порядка 2^8 (расчёты с округлением в сторону ближайшего целого)

$2k$	Число ячеек	Вероятность
0	39363	0,605345
2	19758	0,303855
4	4959	0,0762627
6	830	0,0127609
8	104	0,00160149
10	10	0,000160795
12	1	0,000013454

В работе [9] для проверки соответствия эмпирического распределения теоретическому распределению предлагается воспользоваться критерием согласия Колмогорова [10], который позволяет решить поставленные задачи путем сравнения теоретического интегрального закона распределения вероятностей $F(x)$ (с известными параметрами) с эмпирическим законом распределения вероятностей $F_n(x)$, полученным на входе вычислительного эксперимента.

Статистический критерий согласия Колмогорова, как известно, применяется для проверки простой и параметризованной гипотезы H_0, соответственно которой одинаково распределенные случайные величины X_1, X_2, ..., X_n имеют заданную непрерывную функцию распределения $F(x)$, причем альтернативная гипотеза H_1 предполагается двухсторонней:

$$| EF_n(x) - F(x) | > 0,$$

где EF_n – математическое ожидание функции эмпирического распределения $F_n(x)$. Критическое множество критерия Колмогорова выражается неравенством:

$$D_n = \underset{|x|<\infty}{Sup} |F_n(x) - F(x)| > \lambda_n .$$

В случае справедливости гипотезы H_0 распределение статистики D_n не зависит от функции $F(x)$, причем, если $n \to \infty$, то

$$P\{\sqrt{n} D_n < \lambda\} \to K(\lambda), \quad \lambda > 0.$$

Здесь $K(x)$ – функция распределения Колмогорова, табличная.

Соответственно критерию Колмогорова гипотезу H_0 с уровнем значимости α, $0 < \alpha < 0{,}5$ стоит отбросить, если $D_n \ge \lambda_n(\alpha)$, где $\lambda_n(\alpha)$ – критическое значение критерия Колмогорова, которое соответствует заданному уровню значимости α и есть корнем уравнения $\{D_n \ge \lambda\} = \alpha$.

Для подстановок порядка 2^8 (параметр критерия Колмогорова $n = 255^2$) имеем

$$\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}23}{255} = 0{,}00482 .$$

Таблица 26

Распределение переходов таблицы LAT для подстановки порядка 2^8

$\lvert 2k \rvert$	Число ячеек	Вероятность
0	6502	0,100097
2	12508	0,192818
4	11196	0,1756863
6	9982	0,1535101
8	7872	0,121061
10	5952	0,091534
12	4228	0,065021
14	2822	0,0433987
16	1768	0,0271895
18	1040	0,0159938
20	574	0,00882737
22	298	0,00229178
24	146	0,00458285
26	66	0,00101499
28	28	0,00043060
30	10	0,00015378
32	4	0,00006151
34	2	0,000030757

ВЫВОДЫ

Представленные в таблицах 2–25 результаты свидетельствуют, что практически все рассмотренные S-блоки, используемые в современных шифрах, не укладываются в рамки S-блоков случайного типа.

S-блоки шифров AES (GrandCru), ADE, Fox и Лабиринт не входят даже в допустимые границы (3.8). В эти границы укладываются показатели только S-блоки шифров Мухомор, Iceberg и близкие к ним по показателям S-блоки шифра Anubis (Khazad). Мы уже не говорим здесь о других показателях, которые получаются далекими от показателей совершенных подстановок. В результате удается ввести намного более жесткие, и вместе с тем практически реализуемые критерии отбора случайных подстановок, которые мы посчитали сначала полезными при поиске подстановок с высокими криптографическими показателями. Подстановки, удовлетворяющие самым жестким критериям случайности (и по комбинаторным показателям и по дифференциальным и линейным) предложено называть совершенными.

Мы надеялись, что с помощью таких подстановок удастся реализовать предельные показатели по скорости перехода шифрующих преобразований к асимптотическому режиму, определяемому с точки (момента), когда шифрующее преобразование приобретает свойства случайной подстановки.

Однако проверка степени соответствия новым критериям отбора подстановочных конструкций некоторых известных современных шифров [5–7] показала, что практически все рассмотренные S-блоки, используемые в современных шифрах (S-блоки шифров Rijndael, Лабиринт, Мухомор (Калина), Iceberg, ADE, Камелия, GrandCry и Anubis (Khazad)и др.), не укладываются в рамки S-блоков случайного типа. S-блоки шифров AES (GrandCru), ADE, Fox и Лабиринт не входят даже в допустимые границы. В эти границы укладываются показатели только S-блоки шифров Мухомор, Iceberg и близкие к ним по показателям S-блоки шифра Anubis (Khazad). Мы уже не говорим здесь о других показателях, которые получаются далекими от показателей совершенных подстановок. Более того оказалось, что для обеспечения высоких криптографических показателей шифров совсем не требуются S-блоки со специальными свойствами.

С другой стороны, как показали исследования, свойства подстановок, совершенных по комбинаторным показателям и одновременно совершенным по дифференциальным и линейным показателям, оказались выполненными асимптотически практически для всех известных итеративных шифров.

Литература

[1] Долгов В.И. S-блоки для современных шифров / В.И. Долгов, Е.Д. Мельничук // Науково-технічний журнал «Радіоелектронні та комп'ютерні системи». – Х., 2012. – Вип. 171. – С. 121-133.

[2] Спецификация алгоритма шифрования «Калина-2», версия от 17.08.2012.

[3] Lisitskaya I.V. Importance of S-Blocks in Modern Block Ciphers / I.V. Lisitskaya, E.D. Melnichuk, K.E. Lisitsky // Internet Journal «Computer Network and Information Securuty». – Delhi., – 2012., – Vol. 10, P. 1–12.

[4] Лисицкая И.В. Большие шифры – случайные подстановки / И.В. Лисицкая, А.А. Настенко // Межведомственный научн. технический сборник. Радиотехника. – 2011. – Вып. 166. – С. 50–55.

[5] Лисицкая И.В. Дифференциальные свойства шифра FOX. / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 122–126.

[6] Горбенко І.Д. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації. / І.Д. Горбенко, В.І. Долгов, и др.// Прикладна радіоелектроніка. – 2007. – Т.6. – № 2. – С. 195–208.

[7] Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов, и др. // Прикладная радиоэлектроника. – 2007. – Том. 6, №2. – С. 147–157.

[8] Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том. 6, №2. – С. 230–240.

[9] Олейников Р.В. Результаты анализа алгоритма шифрования ADE. /Р.В. Олейников, В.И. Руженцев, М.С. Михайленко, А.Б. Небывайлов // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2008. – Том. 7, № 3. – С. 210–214.

[10] Долгов В.И. Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радиоэлектронные и компьютерные системы. – Харьков, НАУ ХАИ, 2010. – № 5(46). – С. 79–84 .

[11] Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся вузов. – М.: Наука, 1980. – 976 с.

Поступила в редколлегию 28.03.2013

Мельничук Евгений Дмитриевич, аспирант кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники. Научные интересы: криптография, методы криптоанализа.

УДК 621.3.06

Дослідження відповідності новим критеріям відбору підставних конструкцій сучасних БСШ / Є.Д. Мельничук // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 240–246.

Метою статті є вивчення питання про криптографічні значущості підстановок випадкового виду: наскільки застосовні в шифрах підстановки, відібрані за критеріями випадковості; чи дозволяють вони поліпшити криптографічні показники шифрів. Стисло викладається методика оцінки показників випадковості підстановок, наводяться результати аналізу S-блоків ряду сучасних шифрів на предмет оцінки близькості їх показників випадковості показниками випадкових підстановок.

Ключові слова: підстановка, лінійні показники стійкості, диференціальні показники.

Табл.: 26. Бібліогр.: 10 найм.

UDC 621.3.06

Research of correlation between the new selection criteria and substitutions of modern block ciphers / E.D. Melnichuk // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 240–246.

The purpose of this paper is to study the question of the significance of cryptographic random permutations of a new type: to what extent substitutions selected by randomness criteria are applicable to ciphers; whether the said substitutions allow to improve the performance of cryptographic ciphers. The paper briefly presents the methodology of performance assessment of random permutations and provides the results of analyzing S-blocks of a number of modern ciphers with respect to assessing the similarity of their performance randomness and the corresponding indicators of random permutations.

Keywords: substitution, linear stability indicators, differential resistance indices.

Tab.: 26. Ref: 10 items.

УДК 621. 3.06

АНАЛІЗ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ МІЖНАРОДНОГО СТАНДАРТУ ISO/IEC 29192-2

І.Д. ГОРБЕНКО, А.В. САМОЙЛОВА

Виконується оцінка та порівняльний аналіз блокових симетричних шифрів перспективного міжнародного стандарту ISO/IEC 29192-2. Метою порівняння є оцінка стійкості та швидкодії за умови їх застосування в спрощених застосуваннях (смарт-картках).

Ключові слова: блоковий симетричний шифр, спрощені застосування, міжнародний стандарт, диференційний та лінійний криптоаналіз.

Сьогодні розроблено, стандартизовано та використовуються блокові симетричні шифри (БСШ), які забезпечують високий (гарантований) рівень стійкості та знайшли широке розповсюдження та застосування [1]. В процесі їх впровадження на практиці виявилось, що для деяких додатків вони є складними в реалізації і не забезпечують психологічного сприйняття під час застосування користувачами, наприклад, у ході використання в смарт-картках. Зважаючи на це, розроблено та стандартизовано новітні версії БСШ, які отримали назву полегшених. Зміст полегшеності в тому, що в них зменшена складність криптографічних перетворень. Водночас, це полегшення викликає в свою чергу сумніви відносно рівнів стійкості таких шифрів та їх швидкодії. Метою цієї статті є вивчення сутностей та порівняльний аналіз криптографічної стійкості і швидкодії перспективних БСШ згідно з ISO/IEC 29192-2 [2].

У міжнародному стандарті ISO/IEC 29192-2 представлені два БСШ – PRESENT та CLEFIA. Вони, на наш погляд, складають серйозну конкуренцію вже перевіреним міжнародним стандартам БСШ – AES, Camellia та SEED [1] для використання у смарт картках.

БСШ PRESENT – це симетричний БСШ з 64-ма бітами блока даних та 80 або 128-ма бітами ключа. Він є ітераційним і базується на схемі підстановки-перестановки та складається з 31 раунду.

БСШ CLEFIA має довжину блоків даних у 128 біт та довжину ключа 128, 192 або 256 бітів. Алгоритм шифру побудовано на основі узагальненої структури ланцюга Фейстеля та вимагає виконання 18, 22, 26 раундів відповідно для 128, 192, 256 бітних ключів. Раундова функція CLEFIA ґрунтується на двох різних функціях – F_0 та F_1. N-раунд CLEFIA повторює раундову функцію N разів, причому в першому та останньому раундах використовуються 4 забілені байти ключа. Функції F_0 та F_1 мають SP-структуру.

1. ОЦІНКА СТІЙКОСТІ

Оцінка стійкості БСШ здійснювалась на основі, по-перше, аналізу існуючих джерел та стандартів, відносно цих БСШ, по-друге, на основі самостійних досліджень з використанням програмних моделей.

З'ясовано, що на БСШ PRESENT існують такі види атак: «груба сила», диференційний та лінійний криптоаналіз, алгебраїчна атака, структурна атака та атака на розгортання ключів. Результати аналізу стійкості цього БСШ PRESENT зведено в таблиці 1 [3].

Відносно БСШ CLEFIA існують такі види атак: лінійний та диференційний криптоаналіз, атака нездійсненних диференціалів, та square - атака, з яких атака нездійсненних диференціалів є найбільш ефективною. В таблиці 2 наведено дані щодо стійкості БСШ CLEFIA до певних атак [4].

Результати порівняння БСШ PRESENT та CLEFIA зводяться до наступного. Відносно них не було виявлено криптоаналітичних атак, складність яких була б менше, ніж атака «груба сила». В цілому можна зробити висновок, що БСШ PRESENT та CLEFIA відповідають як мінімум мінімальним вимогам, і можуть бути рекомендованими до застосування для шифрування інформації з використанням малопотужних засобів (смарт-карток). Водночас, на наш погляд, необхідно також провести аналіз стійкості цих шифрів відносно структурної та атаки на схему розгортання ключів, а також square-атаки.

Таблиця 1

Аналіз стійкості шифру PRESENT

Атака	Кількість раундів	Складність реалізації
Атака «груба сила»	Полягає в переборі ключів	На пошук ключів у просторі з 2^{80} ключів знадобиться приблизно $1.596*10^6$ років
Диференційний криптоаналіз	15 раундів	$2^{35,6}$ пар «відкритий текст – шифр - текст»
Лінійний криптоаналіз	26 раундів	2^{64} пар «відкритий текст – шифр - текст»
Алгебраїчна атака	Полягає у вирішенні квадратичних рівнянь	Вирішення 11067 квадратичних рівнянь з 4216 перемінними

Таблиця 2

Аналіз стійкості шифру CLEFIA

Атака	Кількість раундів	Обсяг даних	Час	Сутність атаки
Інтегральна атака на CLEFIA-128/192/256	12	2^{113}	$2^{116.7}$	Метою цієї атаки є прогнозування значень в сумах від обраного байта після певної кількості раундів шифрування
Інтегральна атака на CLEFIA-192/256	13	2^{113}	$2^{180.5}$	
Інтегральна атака на CLEFIA-256	14	2^{113}	$2^{244.5}$	
Атака нездійсненних диференціалів на CLEFIA-128	12	$2^{118,9}$	2^{119}	Атака, реалізована з використанням 9-раундового нездійсненного диференціала
Атака нездійсненних диференціалів на CLEFIA-192	13	$2^{119,8}$	2^{147}	
Атака нездійсненних диференціалів на CLEFIA-256	14	$2^{120,3}$	2^{211}	

2. ОЦІНКА ШВИДКОДІЇ

Оцінка швидкодії здійснювалась на основі програмного моделювання процедур зашифрування та розшифрування для БСШ PRESENT та CLEFIA. Сутність методики порівняння в тому, що алгоритм зашифрування та розшифрування реалізується програмно мовою C++. Далі блоки інформації з довжиною для PRESENT 64 біти, та для CLEFIA 128 бітів зашифровуються багаторазово, і вимірюється число тактів (час зашифрування на блок). Були використані програмні моделі зашифрування – розшифрування: Для БСШ PRESENT з довжинами ключів 80 та 128 бітів, та для БСШ CLEFIA з довжиною ключа 128 бітів.

Результати оцінки швидкодії порівнювались з БСШ міжнародного стандарту ISO/IEC 18033-3 [1].

На основі аналізу даних таблиць 3 та 4, можна зробити висновок, що показники найвищої швидкодії мають БСШ стандарту ISO/IEC 29192-2.

Додатково, аналіз швидкодії здійснюють за вхідною ефективністю. При цьому ефективність устаткування визначається як відношення пропускної здатності до розмірів входу. На рис. 1 зображена площа, яка вказує на більш високу продуктивність, що призводить до більш низького споживання енергії [5]. На рис. 1 БСШ CLEFIA порівнюється з БСШ AES (FIPS197), Camellia (RFC3713), та SEED (RFC4269). Із аналізу графіків можна зробити висновок, що перевагу серед останніх у продуктивності відносно апаратного входу, має БСШ CLEFIA. Отже, можна зазначити, що БСШ стандарту ISO/IEC 29192-2, через свою властивість полегшеності, мають вищі показники швидкодії відносно інших міжнародних стандартів шифрування, та можуть використовуватись ефективно в малопотужних засобах (смарт-картках).

Вказані БСШ можуть використовуватися у вбудованих та безконтактних системах, для конструкцій яких необхідні лише невелика площа кристалу та низьке споживання енергії. Стосовно питань швидкодії та стійкості шифри

Таблиця 3

Аналіз реалізації БСШ (оптимізація площі)

	Режим	Розмір блоку (біти)	Розмір ключа (біти)	Цикл	Площа (GE)	Частота (МГц)	Пропускна здатність (Мбіт/с)	Технологія (μm)
PRESENT	enc	64	80	547	1075	0.1	0.0117	0.18
PRESENT	enc	64	128	559	1391	0.1	0.0115	0.18
CLEFIA	enc	128	128	176	2893	67	49	0.13
CLEFIA	enc/dec	128	128	176	2996	61	44	0.13
AES	enc	128	128	177	3100	152	110	0.13
AES	enc/dec	128	128	1032	3400	80	10	0.35

Таблиця 4

Аналіз реалізації БСШ(оптимізація продуктивності)

	Режим	Розмір блоку (біти)	Розмір ключа (біти)	Цикл	Площа (GE)	Частота (МГц)	Пропускна здатність (Мбіт/с)	Технологія (μm)
PRESENT	enc	64	80	32	1570	0,1	0,20	0,18
PRESENT	enc	64	128	32	1884	0,1	0,20	0,18
CLEFIA	enc/dec	128	128	36	4950	201,3	716,69	0,09
CLEFIA	enc/dec	128	128	18	5979	225,8	1605,94	0,09
AES	enc/dec	128	128	11	12454	145,4	1691,35	0,13
AES	enc/dec	128	128	54	5398	131,2	311,09	0,13

міжнародного стандарту ISO/IEC 29192-2 не поступаються БСШ AES, Camellia, SEED.

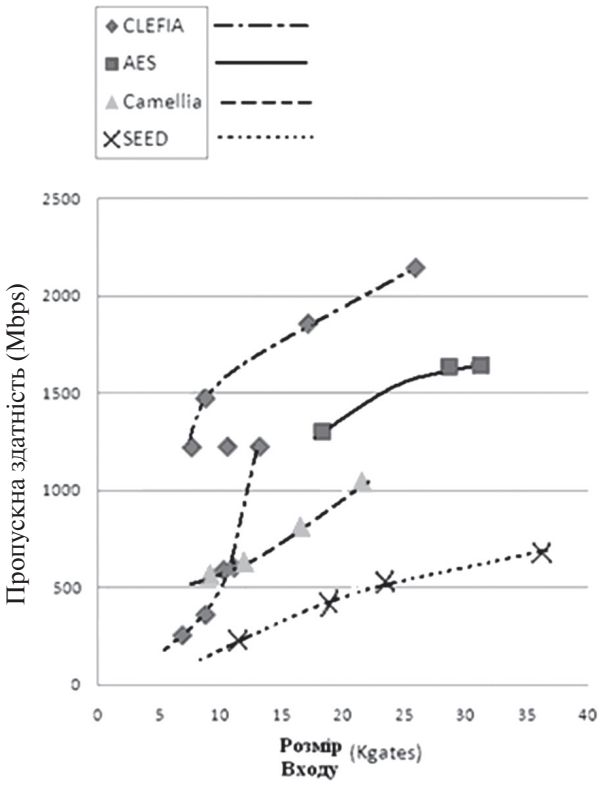


Рис. 1. Графік залежності пропускної здатності від розміру входу

Література

[1] ISO/IEC 18033-3:2005, Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers.

[2] ISO/IEC 29192-2, Information technology — Security techniques — Lightweight cryptography, Part 2: Block ciphers.

[3] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher.

[4] Yukiyasu Tsunoo, Impossible Differential Cryptanalysis of CLEFIA.

[5] Masanobu Katagi, Lightweight Cryptography for the Internet of Things.

Надійшла до редколегії 4.04.2013

Горбенко Іван Дмитрович, фото та відомості про автора див. на с. 201.

Самойлова Аліна Вадимівна, студентка 4-го курсу спеціальності БІКС ХНУРЕ. Наукові інтереси: аналіз стійкості блокових симетричних шифрів, симетрична криптографія.

УДК 621. 3.06

Анализ блочных симметричных шифров международного стандарта ISO/IEC 29192-2 / И.Д. Горбенко, А.В. Самойлова // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 247–249.

Выполняется оценка и сравнительный анализ блочных симметричных шифров перспективного международного стандарта ISO / IEC 29192-2. Целью сравнения является оценка устойчивости и быстродействия при условии их применения в упрощенных приложениях (смарт-картах).

Ключевые слова: блочный симметричний шифр, упрощенные применения, международный стандарт, дифференциальный и линейный криптоанализ.

Табл.: 4. Ил.: 1. Библиогр.: 5 назв.

UDC 621. 3.06

Analysis of block symmetric ciphers of international standard ISO/IEC 29192-2 / I.D. Gorbenko, A.V. Samoilova // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. –№ 2. – P. 247–249.

This paper gives assessment and comparative analysis of block symmetric ciphers of the perspective standard ISO/IEC 29192-2. The aim of comparison is assessing security and speed of response under conditions of their use in simplified applications (smart cards).

Keywords: block symmetric cipher, lightweight application, international standard, differential and linear cryptanalysis.

Tab.: 4. Fig.: 1. Ref.: 5 items.

УДК 681.324.067

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ТЕСТУВАННЯ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ NIST 800-22 ТА NIST 800-90B

Р.І. МОРДВІНОВ

Проаналізовано вимоги, які висуваються у стандарті NIST 800-90B до джерела ентропії та генераторів випадкових біт. Наводиться порівняльний аналіз методик тестування, що описані у стандартах NIST 800-22 та NIST 800-90B. Описано методику тестування та їх порівняння.

Ключові слова: випадкова послідовність, псевдовипадкова послідовність, генератори випадкових послідовностей, детерміновані генератори псевдовипадкових послідовностей.

ВСТУП

У криптології безумовно визнано, що стійкість криптографічних систем суттєво залежить від якісних ключових даних, що використовуються в них. Первинною ознакою, що визначає якість ключових даних, є ентропія джерела ключів. По суті, вона визначає невизначеність початкового стану генератора ключових даних. Усі подальші властивості ключових даних, що генеруються таким генератором, залежать якраз від вказаної початкової ентропії.

У серпні 2012 року запропоновано стандарт NIST DRAFT Special publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation [1]. У ньому описано рекомендації для джерел ентропії, які використовуються для генераторів випадкових бітів. Цей стандарт висуває ряд вимог до фізичних та детермінованих генераторів, пропонує ряд оцінок та тестів для послідовностей. Також наводяться методики для визначення мінімальної ентропії джерела. Розглянемо більш детально та зробимо порівняльний аналіз стандартів NIST 800-22 та NIST 800-90B. *Метою цієї статі є аналіз основних положень NIST DRAFT Special publication 800-90B, дослідження впливу початкової ентропії на криптографічні властивості ключових даних та розробка рекомендацій з його використання у перспективі.*

1. ОСОБЛИВОСТІ АНАЛІЗУ ВЛАСТИВОСТЕЙ ВИПАДКОВИХ ТА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Статистичні властивості ключових даних мають бути нерозрізнювані від випадкових послідовностей. Для визначення таких властивостей використовуються методики статистичного тестування. На сьогодні найбільш практичними та поширеними є FIPS-PUB 140-2 [2], AIS 20 [3], AIS 31 [4] та NIST STS [5].

Методика FIPS-PUB 140-2 має високу швидкість тестування, завдяки чому використовується в основному для оперативного контролю даних генератора під час його функціонування.

Методика AIS 20 використовується для даних з детермінованих генераторів випадкових послідовностей (ДГВБ). Має високу швидкість, через що може використовуватися для тестування в реальному часі.

Методика AIS 31 може використовуватися для тестування випадкових (фізичних) генераторів. Є надійною методикою та забезпечує результати, що і NIST STS. Має високу швидкість, тому може використовуватися для тестування генераторів у режимі реального часу.

NIST STS на сьогодні є одним з найпотужніших та найпоширеніших методик для тестування статистичних властивостей послідовностей. Відповідно останнього видання, до методики NIST STS входять 15 тестів, які, в ході використання всіх параметрів, на виході дають 188 результатів. Ця методика з великою ймовірністю дозволяє відбракувати псевдовипадкові дані, що не відповідають вимогам випадковим. Через велику складність в ході використання усіх тестів зі всіма параметрами, методика NIST STS не дає можливості використовувати тестування генераторів у реальному часі.

Порядок тестування послідовності згідно з NIST STS має такий вигляд:

1. Висувається нульова гіпотеза H_0 – припущення про те, що тестова двійкова послідовність є випадковою.

2. За послідовністю розраховується статистика тесту.

3. Із використанням спеціальної функції і статистики тесту розраховується значення імовірності $P \in [0,1]$.

4. Значення імовірності P порівнюється із рівнем значущості α, $\alpha \in [0,001; 0,01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В іншому випадку приймається альтернативна гіпотеза.

Таким чином, у результаті тестування псевдовипадкових бітів формується вектор значень імовірності $P = \{P_1, P_2, ..., P_{188}\}$. Аналіз складових P_i даного вектора дозволяє вказати на конкретні дефекти псевдовипадкових бітів, що тестуються. У стандарті рекомендованою довжиною є вхідний блок даних 10^6 біт; в одному тестуванні використовується 100 блоків такої довжини. Таким чином довжина вхідних даних для одного тестування складає 10^8 біт. Далі кожний з цих 100 блоків проходить тестування. Результати тестування зводяться до таблиці і мають вигляд 97/100, де 97 – кількість блоків, що пройшли тестування за конкретним тестом, а 100 – загальна кількість тестів. Для зручності використовується

раціональний вид, тобто 0.97. В NIST STS використовуються 2 пороги для результатів тестування – це 0.96 та 0.99, тобто для різних рівнів значущості дозволяється, що зі 100 блоків може не пройти 4 та 1 відповідно.

2. ОСОБЛИВОСТІ ТА РЕЗУЛЬТАТИ ЗАСТОСУВАННЯ СТАНДАРТУ NIST 800-90B

У стандарті NIST 800-90B описана велика кількість тестів. Для виявлення відхилень джерела шуму чи компонентів стану від розподілу при незалежному та стабільному поводженні використовується наступна процедура.

Набір даних довжини N поділяється на 10 підмножин, що не перекриваються та мають довжину $\left\lfloor \frac{N}{10} \right\rfloor$. Кожна з цих підмножин тестується та отримує бали за такою схемою:

- оцінка стиснення – один бал за підмножину даних;
- оцінка великих/малих серій – два бали за підмножину даних;
- оцінка «відвідувань» – один бал за підмножину даних;
- оцінка направлених серій – три бали за підмножину даних;
- оцінка коваріацій – один бал за підмножину даних;
- оцінка колізій – три бали за підмножину даних;
- тест хі-квадрат – прийняття/відбракування послідовності;

У даному стандарті тест з хі-квадрат має два тести – тест на незалежність даних та тест стабільності розподілу даних. Кожен з цих тестів повертає значення ok/fail у випадках проходження/відбракування послідовності.

Першою тестується оригінальна послідовність. Після цього проводиться ще 1000 тестувань з цією ж послідовністю, але після використання перемішування Фішера-Ейтса на кожному кроці. Таким чином формується вектор оцінок. Після цього цей вектор сортується по балах і виявляється положення оригінальних даних. Якщо оцінки оригінальної множини S даних співпадають з іншими, то положення оригінальної множини береться ближче до середини, тобто якщо оцінки множин Rank [482] = 34, Rank [483] = 34, Rank [484] = 35, а Rank [S] оригінальної множини дорівнює 34, тоді її положення Rank (S) = 483, та, якщо Rank [586] = 45, Rank [587] = 46, Rank [588] = 46, Rank [589] = 47, а Rank оригінальної множини дорівнює 46, то її положення Rank (S) = 587 відповідно.

Позиція оригінальної підмножини S повинна бути в інтервалі $50 \le \text{Rank (S)} \le 950$. Таким чином, якщо $\text{Rank (S)} \le 50$ чи $\text{Rank (S)} \ge 950$, то підмножина не проходить тест. Якщо 8 чи більше підмножин оригінальної множини не проходять тести, то джерело ентропії не проходить тести. Ця серія тестів направлена на виявлення недоліків та відхилень джерела ентропії від заданого розподілу. Якщо 8 або більше підмножин не проходять тестування – джерело відкидається.

Для порівняння результатів тестування як джерело ентропії було взято детермінований генератор випадкових послідовностей, заснований на БСШ ГОСТ 28147. Для тестування використовувалися послідовності довжиною 10^8 біт. Тестові дані генерувалися на при одних і тих же ключах та вхідних даних, але на різній кількості циклів шифрування. Всі послідовності були протестовані через обидві методики тестування. Вхідні дані для генератора створювалися за допомогою лічильника та мали велику збитковість «0» бітів.

Результати тестування занесені у таблиці 1–4. У лівій колонці зазначені тести, що були використані, у правій колонці результати у такому вигляді:

– для NIST STS 130/188 (69%), де 130 – кількість пройдених тестів для відповідного рівня значущості (0.96 чи 0.99), 188 – загальна кількість тестів, 69% – відсоток пройдених тестів;

– для NIST 800-90B 8/10, де 8 – кількість оцінок, для яких $50 \le \text{Rank (S)} \le 950$, 10 – загальна кількість результатів тесту.

Перша вхідна послідовність була взята на другому циклі шифрування. Результати тестування наведені у табл. 1.

Таблиця 1

Результати тестування 1-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	0/188 (0%)
Рівень значущості 0.96	0/188 (0%)
NIST 800-90B	
оцінка стиснення	(9/10)
оцінка великих/малих серій	(4/10) (6/10)
оцінка «відвідувань»	(4/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(3/10)
оцінка колізій	(1/10) (5/10) (8/10)
тест хі-квадрат (незалежність даних)	FAIL
тест хі-квадрат (стабільності розподілу даних)	FAIL

Друга вхідна послідовність була взята на шостому циклі шифрування. Результати тестування наведені у табл. 2.

Таблиця 2

Результати тестування 2-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	34/188 (18%)
Рівень значущості 0.96	89/188 (47%)
NIST 800-90B	
оцінка стиснення	(10/10)
оцінка великих/малих серій	(3/10) (7/10)
оцінка «відвідувань»	(8/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(4/10)
оцінка колізій	(9/10) (10/10) (9/10)
тест хі-квадрат (незалежність даних)	OK
тест хі-квадрат (стабільності розподілу даних)	FAIL

Третя вхідна послідовність була взята на сьомому циклі шифрування. Результати тестування наведені у табл. 3.

Таблиця 3

Результати тестування 3-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	108/188 (57%)
Рівень значущості 0.96	174/188 (93%)
NIST 800-90B	
оцінка стиснення	(10/10)
оцінка великих/малих серій	(10/10) (10/10)
оцінка «відвідувань»	(10/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(7/10)
оцінка колізій	(10/10) (10/10) (10/10)
тест хі-квадрат (незалежність даних)	OK
тест хі-квадрат (стабільності розподілу даних)	FAIL

Четверта вхідна послідовність була взята з повноциклової версії шифру. Результати тестування наведені у таблиці 4.

Таблиця 4

Результати тестування 4-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	145/188 (77%)
Рівень значущості 0.96	188/188 (100%)
NIST 800-90B	
оцінка стиснення	(10/10)
оцінка великих/малих серій	(10/10), (10/10)
оцінка «відвідувань»	(10/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(10/10)
оцінка колізій	(10/10) (10/10) (10/10)
тест хі-квадрат (незалежність даних)	OK
тест хі-квадрат (стабільності розподілу даних)	OK

ВИСНОВКИ ТА ПРОПОЗИЦІЇ ВІДНОСНО NIST 800-90B

– Деякі тести з NIST 800-90B не відображують дійсну картину статистичних властивостей вхідної послідовності. Це зумовлено тим, що результати тестування оригінальної послідовності порівнюються не з еталонними значеннями чи межами, а з тією ж самою послідовністю, у якій переставлені значення. Для послідовності, у якій кількість «0» та «1» бітів приблизно рівна, ця методика працюватиме, але при тестуванні послідовностей зі збитковістю тих чи інших – результати оригінальної послідовності не виділяються на фоні «перемішаних» послідовностей.

– Тести великих та малих серій, відвідувань та коваріацій дають більш чітку картину відносно статистичних властивостей послідовності. Перші 2 також є у методиці NIST STS.

– Згідно з алгоритмом в NIST 800-90B тест направлених серій виконується для всієї множини вхідних даних, без розбиття на 10 блоків, як робиться в інших тестах. Через це для відкидання джерела ентропії достатньо, щоб лише один з критеріїв не входив до заданого інтервалу.

– Тести для оцінки колізій виявили відхилення лише у послідовності з великою збитковістю «0» бітів. Коли кількість «0» та «1» бітів ставала приблизно рівною, оцінки тестування майже нічого не показували.

– Тести з використанням хі-квадрат критерію єдині, що порівнюються за еталонними результатами, через що лише вони вказували на статистичні властивості послідовності, а не порівнюють її з результатами цієї ж послідовності, в якій переставлені значення. Тести, що використовують критерій хі-квадрат, також використовуються методикою NIST STS.

– Методика тестування NIST 800-90B підходить для генераторів, в яких розподіл «0» та «1» бітів рівноймовірний. В іншому випадку деякі тести показують не зовсім правильну картину статистичних даних. Більш того, в стандарті написано, що ймовірність вийти за межі заданого інтервалу дорівнює 10%, а в деяких тестах, через те, що значення Rank (S) береться ближче до середини, будуть ще менші. Для відбракування джерела ентропії необхідно, щоб 8 або більше підмножин не пройшли тестування. Через це можна сказати, що, використовуючи лише оцінки, можна відбракувати тільки неякісні джерела ентропії, а послідовності 2 та 3 були відбраковані лише завдяки тестам з використанням критерію хі-квадрат.

Література

[1] NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.

[2] FIPS-PUB-140-2 security requirements for cryptographic modules, 1999.

[3] AIS20 Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, BSI, 1999.

[4] AIS31 Functionality classes and evaluation methodology for true (physical) random number generators, BSI, 2001.

[5] NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Надійшла до редколегії 23.04.2013

Мордвінов Руслан Ігорович, аспірант кафедри БІТ Харківського національного університету радіоелектроніки. Наукові інтереси: розробка та застосування методів генерації випадкових послідовностей.

УДК 681.324.067

Сравнительный анализ методов и средств тестирования случайных последовательностей NIST 800-22 и NIST 800-90B / Р.И. Мордвинов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 250–253.

Проанализированы требования, описанные в стандарте NIST 800-90B к источнику энтропии и генераторам случайных бит. Приводится сравнительный анализ методик тестирования, которые описаны в стандартах NIST 800-22 и NIST 800-90B. Описана методика тестирования и сравнение.

Ключевые слова: случайная последовательность, псевдослучайная последовательность, генератор случайной последовательности, детерминированный генератор случайной последовательности.

Табл.: 4. Библиогр.: 5 назв.

UDC 681.324.067

Comparative analysis of methods and tools for testing random sequences NIST 800-22 and NIST 800-90B / R.I. Mordvinov // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. –№ 2. – P. 250–253.

The paper analyzes requirements of the standard NIST 800-90B to an entropy source and random bit generators. A comparative analysis of the testing techniques which are described in the standards NIST 800-22 and NIST 800-90B is conducted. The methodology of testing and comparison of testing methods is described.

Keywords: random sequence, pseudo-random sequence, random sequence generator, deterministic random sequence generator.

Tab.: 4. Ref.: 5 items.

АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ СВОЙСТВА

УДК 004.056.55

ИССЛЕДОВАНИЕ МЕТОДОВ ВЫЧИСЛЕНИЯ ИНВЕРСИИ В АЛГОРИТМЕ NTRU

Е.Г. КАЧКО, Д.С. БАЛАГУРА, К.А. ПОГРЕБНЯК, Ю.И. ГОРБЕНКО

Проводится анализ и сравнение методов вычисления инверсии в алгоритме NTRU. Проводится экспериментальное исследование влияния свойств кеша и параллелизации вычислений. Даётся оценка производительности некоторых методов вычисления инверсии.

Ключевые слова: методы вычисления инверсии, параллелизация вычислений, оптимизация вычислений, алгоритм NTRU.

Операция инверсии используется для генерации личных ключей шифрования и цифровой подписи и является вычислительно сложной операцией. Целью данной работы является исследование различных методов вычисления инверсии, их оптимизация с учетом возможностей параллельных вычислений. В работе исследуются алгоритмы [1]–[3] с точки зрения их возможной параллелизации. Выполняется сравнение этих алгоритмов по вычислительной сложности.

В алгоритме NTRU используется кольцо усеченных полиномов [1] $Z(X)/(X^N-1)$, которые содержат не более чем N целочисленных элементов. Значения коэффициентов полинома обычно ограничены. Кольцо полиномов, коэффициенты которых меньше p, обозначается как: $(Z/pZ)[X]/(X^N-1)$. Принято обозначать полиномы, принадлежащие такому кольцу, как $a(X), b(X), \ldots$ Инверсия полинома $a(X)$ в кольце $(Z/pZ)[X]/(X^N-1)$ — операция определения полинома $b(X)$, такого что $a(X)*b(X)=1$ в этом же кольце.

Рассмотрим алгоритм инверсии, предложенный в [1].

Алгоритм 1 (A1). Вычисление инверсии.

Вход. Полином $a(X)$, порядок полинома N, модуль q [1].

Выход. Статус (Успех или ошибка), обратный элемент $b(X)$ (в случае успешного статуса).

1. Приведение $a(X)$ в элемент кольца $(Z/2Z)[X]/(X^N-1)$ (все коэффициенты полинома приводятся по модулю $p=2$, отрицательные значения заменяются положительными $(2+a[i]\%2)$.

2. Используя расширенную теорему Эвклида для полиномов $a(X)$ и X^N-1, находим наибольший общий делитель $d(X)$ и коэффициенты $u(X)$, $v(X)$ Диофантового уравнения $u(X)*a(X)+v(X)*(X^N-1)=d(X)$ для модуля $p=2$.

3. Если наибольший общий делитель $d(X)$ не равен 1 ($d[0]\neq\pm1$ или $d[1],d[2],\ldots,d[N-1]\neq0$) – обратного элемента нет, статус равен *Ошибка* и *Выход*.

4. Вычислить

$$b(X)=(d(X)^{-1}(\mathrm{mod}\ p)*u(X))\bmod p.$$

5. Для всех модулей p = 4, 16, 256, 65536 ($p=p^2$).

5.1 Приводим $a(X)$ по модулю p (отрицательные значения заменяем значениями $p+a[i]$).

5.2 Вычисляем новое значение

$$b(X)=(2*b(X)-a(X)*b(X)^2)\bmod p.$$

6. Значение *b(x)* приводим по модулю $q=2048$.

7. Статус равен *Успешно*.

8. Выход.

Алгоритмы, рассмотренные далее (A2, A3, A4), предназначены для вычисления инверсии для модуля 2 (пункты 2–4 алгоритма A1).

Алгоритм 2 (A2)

Вход. Порядок p^2, полиномы $a(X)$, $c(X)$[3].

Выход. Полиномы $d(X), u(X), v(X)$, удовлетворяющие уравнению:

$a(X)*u(X)+c(X)*v(X)=d(X)$ в кольце.

1. Если $c(X)$, то $u(X)=1$, $v(X)=0$, $d(X)=a(X)$.

2. $u(X); d(X)=a(X); v_1(X)=0$; $v_3(X)=c(X)$.

3. Пока ($v_3(X)\neq0$) выполнить

3.1 $q(X)=d(X)\%v_3(X)$[4]; $t_3(X)=d(X)\%v_3(X)$[5]

3.2 $t_1(X)=u(X)-q(X)*v_1(X)$

3.3 $u(X)=v_1(X)$

3.4 $d(X)=v_3(X)$

3.5 $v_1(X)=t_1(X)$

3.6 $v_3(X)=t_3(X)$.

4. $v(X)=(d(X)-a(X)*u(X))/b(X)$.

Рассмотрим оптимизацию A2, как составной части A1.

1. Полином $c(X)=X^N-1$ не может быть равным 0, поэтому первый пункт алгоритма можно опустить.

[1] Для всех полиномов в [1] $q=2048$

[2] Значение p=2

[3] Последнему полиному соответствует полином x^N-1

[4] Деление нацело, дробная часть отбрасывается

[5] Вычисление остатка от деления

2. При выполнении первой итерации цикла в операции деления $a(X)/c(X)$ отметим, что порядок $a(X)$ меньше порядка $c(X)$, следовательно, на первом шаге $q(X)=0$, $t_3(X)=a(X)$. Таким образом, первую итерацию можно опустить целиком. Для второй итерации использовать деление $c(X)/a(X)$, а в качестве начального значения $d(X)$ использовать значение $a(X)$.

3. При вычислении $t_1(X)$ после очередного деления $u(X)=0$, а $v_1(X)=1$ т.е. $t_1(X)=-q(X)$, а с учетом модуля 2 $t_1(X)=q(X)$.

4. Так как все коэффициенты и результат вычисления по модулю 2, операцию умножения (шаг 3.2) следует заменить операциями сложения по модулю 2.

5. Значение $v(X)$ не используется далее, его вычисление можем опустить (пункт 4 алгоритма 2)

6. Везде, где возможно, следует использовать SSE операции.

Алгоритм 2 после оптимизации (A2')

1. $d(X)=a(X); u(X)=1;$
   $q(X)=c(X)/a(X); v_3(X)=c(X)\%a(X)$
2. $v_1(X)=q(X)$
3. Пока ($v_3(X)\neq 0$) выполнить

3.1 $q(X)=d(X)/v_3(X);\ \ t_3(X)=d(X)\%_3(X)$

3.2 $t_1(X)=u(X)\hat{}\,q(X)*v_1(X);\ u(X)=v_1(X);$
$d(X)=v_3(X)$

3.4 $v_1(X)=t_1(X);\ v_3(X)=t_3(X)$

В одной строчке задаются операторы, которые можно выполнять параллельно.

Результаты, полученные после предложенной оптимизации, приведены в табл. 1.

Таблица 1

Оптимизация расширенного алгоритма Эвклида для NTRU[6]

Порядок Полинома N	Время (мс)		Ускорение, S=t1/t2
	A2, t1	A2', t2	
401	4,04	0,826	4,89
449	5,17	0,997	5,19
677	11,56	2,18	5,30
1087	22,99	4,75	4,84
541	5,82	1,38	4,22
613	6,75	1,51	4,47
887	14,49	3,03	4,78
1171	25,76	5,41	4,76
659	8,08	1,99	4,06
761	10,71	2,46	4,35
1087	21,21	4,71	4,50
1499	39,25	8,85	4,44

Как видно из таблицы, оптимизация алгоритма A2 позволила ускорить его не менее, чем в 4 раза.

Продолжим оптимизацию Алгоритма 1. Шаг 3 проверяет, что наибольший общий делитель равен 1 (–1). Заметим, что полином x^N-1. Он имеет корень $X=1$, который не может быть корнем полинома $f(X)$, используемого для вычисления личного ключа. Действительно, $f(X)=3*F(X)+1$, полином $F(X)$ имеет одинаковое число коэффициентов равных 1 и –1, следовательно, $X=1$ — корень полинома $F(X)$, т.е. не является корнем $f(X)$. Второй множитель x^N-1 имеет порядок N, как и полином $f(X)$, но не совпадает с ним, т. к. все его коэффициенты равны 1. Для полинома $g(X)$ количество 1 и -1 отличается на 1, что обеспечивает отсутствие корня $X=1$. Следовательно, проверка наибольшего общего делителя не имеет смысла и может быть опущена. Шаг 4, в котором выполняется вычисление по формуле $b(X)=(d(X)^{-1}(\bmod p)*u(X))\bmod p$, фактически также может быть опущен, т. к. $d(X)=1$, обратный элемент для единичного элемента равен 1, а вычисления $u(X)$ изначально выполняются по модулю 2.

Таким образом, алгоритм 2 в улучшенном варианте можно рассматривать не только как реализацию расширенного алгоритма Эвклида, но и как вычисление обратного элемента по модулю 2.

Использование almost inverses (почти инверсий) [2]

При вычислении инверсии по модулю 2 предыдущим алгоритмом использовалась операция деления, в результате которой порядок полинома на каждом шаге уменьшался. Вместо обнуления старших коэффициентов полинома при вычислении инверсии предложено обнуление младших коэффициентов [2] и вычисление общего числа таких коэффициентов *k*. В этом случае фактически решается уравнение $a(X)*u(X)+c(X)*v(X)=X^k$ Значение $u(X)$ авторы [2] называют Almost Inverses (почти инверсия) и предлагают использовать этот алгоритм для вычисления инверсии для эллиптических кривых. Для получения значения инверсии результат достаточно разделить на X^k.

В работе [3] показана применимость этого метода для вычисления инверсии по модулю 2 в алгоритме NTRU. В качестве необходимых условий возможности применения этого алгоритма используются условия:

$$\gcd(a(X),c(X))=1;\ c(0)=1.$$

Как показано выше, данные условия выполняются.

Алгоритм 3 (A3)[3]

Вход. Порядок $p=2$, полиномы $a(X)$; $c(X)=X^N-1$.

Выход. Полином $b(X)$, такой что $b(X)=a(X)^{-1}$ в кольце $(Z/2Z)/[X]/(X^N-1)$.

1. $k=0;\ \ b(X)=1;\ \ c(X)=0;\ \ f(X)=a(X);$ $g(X)=x^N-1$
2. Выполнить цикл

2.1 Определение количества младших нулевых коэффициентов (r) в $f(X)$

2.2 Сдвиг $f(X)$ вправо на r элементов

[6] Результаты приведены для порядков полинома, рекомендованных [1]

2.3 Сдвиг $c(X)$ влево на r элементов

2.4 $k+=r$

2.5 Если $f(X)==1$, то Выход из цикла

2.6 Если порядок $f(X)$ меньше порядка $g(X)$, то поменять местами $f(X)$ и $g(X)$, $b(X)$ и $c(X)$

2.7 $f(X)=f(X)\hat{}\,g(X); b(X)=b(X)\hat{}\,c(X)$

3. $b(X)=b(X)*X^{(N-k)\%N}$

Оптимизация алгоритма А3.

1. Вместо замены местами полиномов использовать замену местами адресов этих полиномов.

2. Для выполнения этапа 3 использовать циклический сдвиг полинома.

3. Везде, где возможно, использовать SSE команды.

Результаты сравнения алгоритмов А2' и оптимизированного А3 будут приведены ниже после рассмотрения очередного алгоритма.

Использование улучшенного алгоритма вычисления GCD и обратного элемента [5]

Этот алгоритм отличается от алгоритма А2 тем, что вычисление выполняется с помощью прямого и обратного преобразований. При прямом преобразовании выполняется последовательное вычисление частного и остатка, как в алгоритме вычисления GCD. При этом все частные запоминаются в стеке. При обратном преобразовании выполняется фактическое вычисление обратного элемента, если GCD == 1. В противном случае делается вывод об отсутствии обратного элемента.

Алгоритм вычисления обратного элемента с учетом идеи автора [5], в применении к полиномам:

Алгоритм А4.

Прямой ход:

1. $d(X)=c(X); v_3(x)=a(x); r=0$

2. Пока ($v_3(X)\neq 1$) выполнить

2.1 $q(X)=d(X)/v_3(X)$; $t_3(X)=d(X)\%v_3(X)$

2.2 push ($q(x)$) r++;

2.3 $d(x)=v_3(x)$

2.4 $v_3(x)=t_3(x)$

Обратный ход

1 $S(x)=0$;

2 Для $i=1, 2,..., r$ выполнить

2.1 $q(x)=pop()$;

2.2 $b(x)=S(X)+q(x)*v_3(x)$;

2.3 $S(x)=v_3(x)$;

2.4 $v_3(x)=b(x)$

Теоретический анализ производительности алгоритма, проведенный автором [5], обещал улучшение производительности приблизительно на 54%, но при этом не учитывались свойства кеша. В случае полинома, элемент кеша – это полином, число элементов кеша приблизительно равно N/2. Таким образом весь стек во внутреннем кеше не помещается, это приводит к существенным потерям производительности. Более того, для N = 1499 необходимо вместо выделения памяти в стеке использовать выделение динамической памяти, что также замедляет выполнение функции. В табл. 2 приведены результаты сравнения трех оптимизированных алгоритмов вычисления обратного элемента для модуля, равного 2^7.

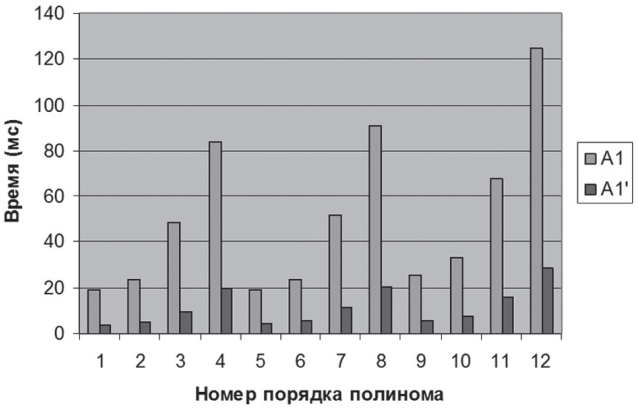


Рис. 1

Таким образом, использование алгоритма А3 вместо оптимизированного алгоритма А2' позволяет увеличить производительность еще примерно в 3 раза, общее увеличение производительности не менее, чем в 12 раз. Использование же усовершенствованного алгоритма вычисления инверсии (А4) по сравнению с обычным (А2), если и дает выигрыш, то максимум на 9 процентов, а вот алгоритм вычисления Almost Invers (А3) существенно выигрывает.

Заметим, что полученные нами результаты противоречат результатам из [4] и [5]. Это связано с тем, что в указанных работах определялось только общее число необходимых итераций и не учитывались возможности их параллельного выполнения, а также свойства кеша.

Вернемся к оптимизации алгоритма А1.

[7] Значение N=1499 для алгоритма А4 не используется

Таблица 2

Сравнение всех алгоритмов вычисления инверсии по модулю 2

Порядок полинома N	Время (мс)			Ускорение, S1=t2/t3	Ускорение, S1=t2/t4	Ускорение, S3=t4/t3
	A2' (t2)	A3 (t3)	A4 (t4)			
401	0,826	0,25	0,80	3,30	1,03	3,20
449	0,997	0,32	0,96	3,12	1,04	3,00
677	2,18	0,63	1,9987	3,46	1,09	3,17
1087	4,75	1,62	4,63	2,93	1,03	2,86
541	1,38	0,41	1,38	3,37	1,00	3,37
613	1,51	0,53	1,47	2,85	1,03	2,77
887	3,03	1,04	3,00	2,91	1,01	2,88
1171	5,41	1,96	5,44	2,76	0,99	2,78
659	1,99	0,61	1,83	3,26	1,09	3,00
761	2,46	0,82	2,43	3,00	1,01	2,96
1087	4,71	1,61	5,12	2,93	0,92	3,18
1499	8,85	3,19	–	2,77	–	–

При вычислении по формуле

$$b(X) = (2 * b(X) - a(X) * b(X)^2) \bmod p$$

для вычисления $b(x)^2$ используется формула сокращенного умножения, а операции сложения, вычитания и приведения по модулю выполняются с помощью SSE команд.

В табл. 3 приведены окончательные результаты, полученные после оптимизации алгоритма A1 (алгоритм A1'), а на рис. 1 – диаграмма с полученными результатами

Таблица 3

Вычисление инверсии по модулю $p = 2048$

Порядок полинома N	Время (мс)		Ускорение, S=t1/t2
	A1, t1	Улучшенный A1, t2	
401	19,42	3,89	4,99
449	23,89	5,07	4,71
677	48,60	9,73	4,99
1087	83,56	20,10	4,16
541	19,06	4,37	4,36
613	23,70	5,52	4,29
887	51,95	11,56	4,49
1171	90,78	20,29	4,47
659	25,75	5,75	4,48
761	33,26	7,53	4,42
1087	67,96	15,76	4,31
1499	124,85	28,99	4,31

В алгоритме A' для вычисления инверсии по модулю 2 используется алгоритм A3. Для параллелизации вычислений используются SIMD команды. Потоки не используются.

Заметим, что ускорение распределено практически равномерно, это связано с тем, что системные погрешности оказывают на этот алгоритм меньше влияние, чем на предыдущие алгоритмы, т. к. время выполнения этого алгоритма больше.

Таким образом, оптимизация алгоритма вычисления инверсии привело к более, чем 4-кратному увеличению скорости.

Литература

[1] American National Standard for Financial Services ANSI X9.98 – 2010. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry.

[2] R. Schroeppel, H. Orman, S. O'Malley and O. Spatscheck, "Fast key exchange with elliptic curve systems," Advances in Cryptology, Proc. Crypto'95, LNCS 963.

[3] NTRU Cryptosystems Technical Report.. http://www.securityinnovation.com/uploads/Crypto/NTRUTech014.pdf.

[4] Kyle Wilhelm. Aspects of Hardware Methodologies for the NTRU Public-Key Cryptosystem. https://ritdml.rit.edu/bitstream/handle/1850/7774/KWillaimsThesis02-2008.pdf?sequence= 1.

[5] Boris S. Verkhovsky. Enhanced Euclid Algorithm for Modular Multiplicative Inverse and Its Application in Cryptographic Protocols. Int. J. Communications, Network and System Sciences, 2010, 3, 901-906.

Поступила в редколлегию 6.03.2013

Качко Елена Григорьевна, кандидат технических наук, профессор кафедры ПО ЭВМ ХНУРЭ. Научные интересы: программные средства криптографических систем.

Балагура Дмитрий Сергеевич, кандидат технических наук, доцент кафедры Безопасности информационных технологий ХНУРЭ. Научные интересы: защита информации, криптографические протоколы выработки и согласования ключей.

Погребняк Константин Анатолиевич, доцент каф. БИТ ХНУРЭ, начальник отдела КЗИ АО «ИИТ». Научные интересы: применение методов алгебраической геометрии в криптологии, асимметричный криптоанализ.

Горбенко Юрий Иванович, фото и сведения об авторе см. на стр. 193.

УДК 004.056.55

Дослідження методів обчислення інверсії в алгоритмі NTRU / О.Г. Качко, Д.С. Балагура, К.А. Погребняк, Ю.І. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 254–257.

Здійснюється аналіз та порівняння методів обчислення інверсії в алгоритмі NTRU. Здійснюється експериментальне дослідження впливу властивостей кеша паралелізації обчислень. Надається оцінка швидкості деяких методів обчислення інверсії.

Ключові слова: методи обчислення інверсії, паралелізація обчислень, оптимізація обчислень, алгоритм NTRU.

Іл.: 1. Бібліогр.: 5 найм.

UDC 004.056.55

Research of methods of calculating of inversion in NTRU algorithm / Kachko E.G., Balagura D.S., Pogrebnyak K.A., Gorbenko Yu.I. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 254–257.

The analysis and comparison of methods of calculating inversion in the NTRU algorithm is carried out. The experimental research of influence of cache properties and parallelization of calculations is conducted. The assessment of productivity of some methods of calculation of inversion is given.

Keywords: methods of calculating inversion, parallelization of calculations, optimization of calculations, NTRU algorithm.

Fig.: 1. Ref.: 5 items.

УДК 004.056.55

ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ ОСНОВНИХ ЗАДАЧ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ

М.Ф. БОНДАРЕНКО, Л.В. МАКУТОНІНА

Наводяться огляд та результати порівняльного аналізу основних обчислювальних задач, що використовують алгебраїчні решітки.

Ключові слова: алгебраїчні решітки, обчислювальна складність, базис решітки, найкоротший вектор у решітці.

ВСТУП

Криптографічні перетворення на алгебраїчних решітках належать до досить нової галузі в криптографії, але є найперспективнішою галуззю, що швидко та потужно розвивається. Першою потенціальною стійкою криптосистемою з відкритим ключем на алгебраїчних решітках вважається криптосистема NTRU, яка була вперше представлена в 1996 році, та яка була запатентована 24 липня 2000 року. З тих пір було запропоновано безліч криптосистем та криптопримітивів, що використовують алгебраїчні решітки [1–6], в тому числі, і на ідентифікаційних даних [7–10].

Одним із найважливіших питань, для криптосистем на алгебраїчних решітках, є визначення стійкості задачі, що лежить в основі конкретної криптографічної схеми. Тому, метою даної статті є визначення та порівняльний аналіз стійкості обчислювальних задач на решітках.

1. ОСНОВНІ ВІДОМОСТІ, ЩО СТОСУЮТЬСЯ АЛГЕБРАЇЧНИХ РЕШІТОК

Решітка – це множина n-лінійно незалежних векторів, тобто решітка з розмірністю n – це набір лінійних комбінацій b_i з цілими коефіцієнтами a_i, тоді решітку L можна подати так:

$$L=\{a_1b_1+\ldots+a_nb_n \mid a_i\in Z^k\}, \qquad (1)$$

де k – ранг решітки. Базисом решітки називають набір лінійно незалежних k-векторів виду: $b_1,\ldots,b_n$, де $b_i\in R^n$. Параметр n є параметром безпеки, і, зазвичай, інші параметри залежать від нього.

Розглянемо основні положення, які є необхідними для подальшого аналізу криптографічної стійкості задач на алгебраїчних решітках.

Довжина вектора x у решітці вимірюється його нормою $\|x\|$. Найчастіше для решіток використовується норма Евкліда, що визначається як:

$$\|x\|=\sqrt{\sum_{i=1}^{n}x_i^2}. \qquad (2)$$

Мінімальна відстань $\lambda_1(L)$ решітки L визначається, як $\min_{x\neq y}\|x-y\|$, де x,y – елементи решітки L. Мінімальна відстань еквівалентна довжині найкоротшого ненульового елемента, тобто $\lambda_1(L)=\min_{x\in L,x\neq 0}\|x\|$. Для даного набору точок S на решітці, $\|S\|$ визначається, як $\max\|s\|$, де максимум береться над усіма елементами $s\in S$.

Нехай q – просте. Тоді, нехай $A\in Z_q^{n\times m}$, тобто A – матриця елементи якої належать до Z_p. Найчастіше, зустрічаються такі два види алгебраїчних решіток [11]:

$$L(A,q)=\{y\in Z^m : y=A^T s \bmod q, \text{ для деякого } s\in Z^n\}; \qquad (3)$$

$$L^{\perp}(A,q)=\{e\in Z^m : Ae=0 \bmod q\}. \qquad (4)$$

Тут, A^T означає транспоновану матрицю A, що породжує решітку $L(A,q)$, A – матриця перевірки парності для решітки $L^{\perp}(A,q)$. Решітку, визначену над Z_q, називають модулярною решіткою.

2. КЛАСИФІКАЦІЯ ТА ЗАГАЛЬНИЙ ОПИС ОСНОВНИХ ОБЧИСЛЮВАЛЬНИХ ЗАДАЧ, ЯКІ ЗАСНОВАНІ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ

Однією із статей, в якій вперше було надано оцінку та вимоги до обчислювальних задач на решітках, є стаття Айтаі [12]. Так, у 1996 році Айтаі сформулював три базові задачі на алгебраїчних решітках, які лягли в основу більшості подальших задач, на алгебраїчних решітках:

1. Знайти довжину найкоротшого ненульового вектора в n-вимірній решітці, з точністю до поліноміального фактору.

2. Знайти найкоротший ненульовий вектор v у n-вимірній решітці L, для якої найкоротший вектор v є унікальним, тобто, будь-який інший вектор, з довжиною не більш за $n^c\|v\|$, є паралельним до вектора v, де, c – достатньо велика абсолютна константа.

3. Знайти базис $b_1,\ldots,b_n$, в n-вимірній решітці L, з довжиною, що визначена, як $\max_{i=1}^{n}\|b_i\|$, і, що є найменшою з можливих, з точністю до поліноміального фактору.

Основні обчислювальні задачі на алгебраїчних решітках можна умовно класифікувати так:

1. Задачі, що засновані на пошуку найкоротшого вектора. До цього класу відносяться задачі, що базуються на пошуку першого послідовного мінімуму в решітці L, що дорівнює довжині найкоротшого ненульового вектора решітки (мінімальній відстані між двома точками в решітці L), тобто, $\lambda_1(L) = \min\{\|x\| \mid x \in L, x \neq 0\}$. Першою очевидною задачею в теорії решіток є пошук ненульового вектора, який би досягав цього мінімуму. Зазначимо також, що такий вектор ніколи не є унікальним, оскільки $\|-x\| = \|x\|$, для усіх векторів решітки $x \in L$ (в решітці існують інші точки з цією ж нормою).

2. Задачі, що засновані на пошуку найближчого вектора. До цього класу відносяться задачі, які базуються на пошуку, для даної точки $t \in R^n$, найближчої точки в решітці L, причому, припускається, що $t \notin L$. Така точка може бути не унікальною, але в багатьох випадках вона є такою.

3. Задачі, що засновані на пошуку найкоротшого набору векторів. До цього класу відносяться задачі, що базуються на прямому зведенні задачі про знаходження найкоротшого вектора в решітці L, тобто поданні, для якого перший послідовний мінімум подається як пряме узагальнення повної послідовності послідовних мінімумів. Такі мінімуми визначаються так: $\lambda_i(L) = \min\{\max\{\|x_1\|,\ldots,\|x_i\|\} \mid x_1,\ldots,x_i \in L,$ лінійно незалежні$\}$.

4. Задачі, що засновані на модулярних решітках. Решітка $L \subset Z^m$ називається модулярною за модулем q, або q-нарною, якщо $qZ^m \subset L$. Зазвичай, використовуються решітки, для яких $q << \mathrm{vol}(L)$, де $\mathrm{vol}(L)$ – потужність решітки L. У даній статті розглядатимуться модулярні решітки виду $L_{A,q} = \{x \in Z^m \mid Ax \equiv 0 (\mathrm{mod}\, q)\}$, де A – матриця розмірністю $n \times m$, з цілими коефіцієнтами взятими за модулем q.

5. Задачі, що засновані на ідеальних решітках. Для даного типу задач $R = Z[x]/\langle f \rangle$ – кільце цілочисельних поліномів за модулем деякого нормованого полінома f ступеня n. Оскільки R ізоморфно до Z^n, тоді адитивна група та ідеали в кільці R, що визначені підгрупами, відповідають решітці. Решітку такого виду називають ідеальною решіткою по відношенню до f.

6. Задачі, що засновані на пошуку радіусу покриття. Радіусом покриття для даної, можливо нескінченої, множини точок P решітки L у Евклідовому просторі, є найменше число r таке, що сфера з радіусом r навколо всіх точок P покриває весь простір.

3. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ПОШУКУ НАЙКОРОТШОГО ВЕКТОРА

Задача пошуку найкоротшого вектора в решітці (SVP- задача) є класичною задачею в теорії чисел. Найкращі алгоритми, які існують на сьогодні, розв'язують дану задачу за експоненціальний час. Айтай у роботі [12] показав, що SVP-задача є NP-повною задачею.

1) SVP-задача (The Shortest Vector Problem)

Вхідні дані: Базис решітки L.

Завдання: Знайти $y \in L$, такий, що $\|y\| = \lambda_1(L)$.

2) SVP γ-задача (The Approximate Shortest Vector Problem)

Вхідні дані: Базис решітки L, апроксимаційний фактор $\gamma \geq 1$.

Завдання: Знайти $y \in L$, такий, що $0 < \|y\| \leq \gamma\lambda_1(L)$.

Відомо, що SVP γ-задача є NP- складною [13], для $\gamma = 2^{\log^{1/2-\varepsilon}(n)} \approx \sqrt{n}$.

Для двох наведених вище задач значення $\lambda_1(L)$ не є відомим, але, замість цього значення може бути використано значення $\mathrm{vol}(L)$, що є відомим, задачу такого типу називають Ермітовим варіантом апроксимації SVP- задачі (див. наступну задачу).

3) HSVP γ-задача (The Hermite Shortest Vector Problem)

Вхідні дані: Базис решітки L, апроксимаційний фактор $\gamma > 0$.

Завдання: Знайти $y \in L$, такий, що $0 < \|y\| \leq \gamma \mathrm{vol}(L)^{1/n}$.

У роботі [13] показано, що алгоритм Ленстри-Ленстри-Ловаса (далі – LLL) [14] розв'язує останню задачу за поліноміальний час для $\gamma = (\sqrt{4/3} + \varepsilon)^{(n-1)/2}$, на практиці це значення приблизно дорівнює $\gamma = 1{,}02^n$.

4) DSVP- задача (The Decision Shortest Vector Problem)

Вхідні дані: Базис решітки L, радіус $r > 0$.

Завдання: Визначити, чи існує $y \in L$, такий, що $0 < \|y\| \leq r$.

Наступна задача основується на припущенні, про можливість знаходження першого послідовного мінімуму, без знання найкоротшого ненульового вектора в решітці.

5) SLP γ-задача (The Approximate Shortest Length Problem)

Вхідні дані: Базис решітки L, апроксимаційний фактор $\gamma > 1$.

Завдання: Знайти λ, таке, що

$$\lambda_1(L) \leq \lambda \leq \gamma\lambda_1(L),$$

де $\lambda_1(L)$ – перший послідовний мінімум.

Говорять, що $L' \subset L$, з рангом $n' < n$, таким, що $\mathrm{vol}(L')^{1/n'}$, є істотно меншою за решітку з $\mathrm{vol}(L)^{1/n'}$. Інакше кажучи, існують вектори решітки L, такі, що є коротшими ніж очікувалося у випадковій решітці. Такий розрив між першими двома послідовними мінімумами отримав назву наступної апроксимації SVP-задачі.

6) USVP γ-задача (The Unique Shortest Vector Problem)

Вхідні дані: Базис решітки L, фактор лакуни $\gamma \geq 1$.

Завдання: Знайти, якщо такий існує, унікальний ненульовий вектор $y \in L$, такий, що для будь-якого $v \in L$ з $\|v\| \leq \gamma\|y\|$ є кратним y.

7) GapSVP γ-задача (The Gap Shortest Vector Problem)

Вхідні дані: Базис решітки L, раціональне число $r>0$, апроксимаційний фактор $\gamma>1$.

Завдання: Якщо $\lambda_1(L)\le r$, повернути відповідь «Так»; якщо $\lambda_1(L)>\gamma r$, повернути «Ні».

Хот у роботі [15] показав, що GapSVP γ - задача є NP-складною для деякого константного значення γ.

Хот і Вішной у роботі [16] сформулювали визначення ще двох апроксимацій SVP- задачі, які залежать від l_p - норми, що наведені нижче. Також, у роботі [16] було показано, що наступні дві задачі є NP-складними для деякого $p\ge 1$. Для будь-якого $p\ge 1$ визначена l_p - норма вектора $x=(x_1,x_2,\ldots,x_n)\in R^n$ так: $\|x\|_p:=(\sum_{i=1}^n|x_i|^p)^{1/p}$.

8) USVP p - задача (Unique Shortest Vector Problem in l_p norm)

Вхідні дані: Базис $\{b_1,\ldots,b_n\}\in Z^n$ решітки L, раціональне число $r>0$.

Завдання: Якщо в решітці L існує рівно два ненульових вектора $(v,-v)$ з нормою l_p меншою, ніж r, повернути відповідь «Так»; якщо в решітці L не існує ненульовий вектор з нормою l_p меншою, ніж r, повернути відповідь «Ні».

9) PSVP p - задача (Unique Shortest Vector Problem in l_p norm)

Вхідні дані: Базис $\{b_1,\ldots,b_n\}\in Z^n$ – набір лінійно-незалежних ненульових векторів, з довжиною щонайменше за одиницю з нормою l_p.

Завдання: Якщо в решітці L існує ненульовий вектор з довжиною меншою, ніж ς, повернути відповідь «Так»; якщо в решітці L усі ненульові вектори мають довжину меншу, ніж ς, повернути відповідь «Ні».

4. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ПОШУКУ НАЙБЛИЖЧОГО ВЕКТОРА

Задача пошуку найближчого вектора в решітці (CVP- задача) є однією з найголовніших задач в теорії алгебраїчних решіток. Найкращі алгоритми, які існують на сьогодні, розв'язують дану задачу за експоненціальний час, але існує алгоритм, який запропонував Бабаі [17], що вирішує апроксимацію даної задачі за поліноміальний час. Даний алгоритм використовує метод форсування нуля (обнуління) з послідовним усуненням перешкод (Zero Forcing with Successive Interference Cancellation) [18].

1) CVP- задача (The Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$.

Завдання: Знайти ненульовий вектор $y\in L$, такий, що $\|t-y\|=n(t,L)$.

2) CVP γ - задача (The Approximate Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$, апроксимаційний фактор $\gamma\ge 1$.

Завдання: Знайти ненульовий вектор $y\in L$, такий, що $\|t-y\|=\gamma n(t,L)$.

Санджив Арора та ін. [19] показали, що CVP γ - задача є NP- складною для деякого константного значення γ, та, імовірно, що дана задача є NP- складною для $\gamma=2^{\log^{1-\varepsilon}n}\approx n$. Алгоритм Бабаі вирішує CVP γ - задачу за поліноміальний час для $\gamma=2(\sqrt{4/3})^n$ [13,17].

3) DCVP- задача (The Decision Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$, радіус $r>0$.

Завдання: Визначити, чи існує $y\in L$, такий, що $\|y-t\|\le r$.

Існують криптосистеми, які нібито засновані на CVP- задачі, але, при цьому, не відомо чи є відстань між решіткою і цільовою точкою обмеженою. Тому, зазвичай, використовують таку апроксимацію CVP- задачі, що є простішою.

4) BDD α -задача (Bounded Distance Decoding)

Вхідні дані: Базис решітки L, параметр відстані $\alpha>0$, цільовий вектор $t\in R^n$, такий, що $n(t,L)<\alpha\lambda_1(L)$.

Завдання: Знайти таке $y\in L$, що $n(y,t)=n(L,t)$.

Стійкість BDD α - задачі залежить від значення α, і BDD α - задача є NP- складною для $\alpha>1/2\sqrt{2}$ [20].

5) GapCVP γ - задача (The Gap Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$, дійсні числа $\gamma,r>0$.

Завдання: Якщо $\|y-t\|\le r$, повернути відповідь «Так»; якщо $\|y-t\|>\gamma r$, повернути «Ні».

5. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ПОШУКУ НАЙКОРОТШОГО НАБОРУ ВЕКТОРІВ

Вперше задачу, що заснована на пошуку базису мінімальної довжини в алгебраїчній решітці, запропонував Айтаі у 1996 році [12], яка в даній статті наведена під назвою SBP.

1) SBP- задача (The Shortest Basis Problem)

Вхідні дані: Решітка L, n -вимірна, з довжиною, визначеною, як $\max_{i=1}^n\|b_i\|$.

Завдання: Знайти найменший базис даної решітки $\{b_1,\ldots,b_n\}$, з точністю до поліноміального фактору.

В роботі [12] Айтаі довів, що $\max_{i=1}^n\|b_i\|\le n^c\,\mathrm{bl}(L)$, для деякої абсолютної константи c, з імовірністю $1-2^{-\sigma}$.

2) SBP γ - задача (The Approximate Shortest Basis Problem)

Вхідні дані: Базис $\{a_1,\ldots,a_n\}$ решітки L, апроксимаційний фактор $\gamma\ge 1$.

Завдання: Знайти такий базис $\{b_1,\ldots,b_n\}$ решітки L, що $\max_i\|b_i\|\le\gamma\min\{max_i\|a_i\|\,|\{a_1,\ldots,a_n\}\in L\}$.

3) SMP γ - задача (The Successive Minima Problem)

Вхідні дані: Базис $\{b_1,\ldots,b_n\}$ решітки L.

Завдання: Знайти лінійно незалежний набір $\{y_1,\ldots,y_n\}$ такий, що $\|y_i\|=\lambda_i(L)$, для $i=1,\ldots,n$.

Також існує SMP γ - задача з апроксимаційним фактором $\gamma > 1$, що визначається аналогічно з SMP- задачею, з точністю до γ.

4) SIVP- задача (The Shortest Independent Vector Problem)

Вхідні дані: Базис $\{b_1,...,b_n\}$ решітки L.

Завдання: Знайти лінійно незалежний набір $\{y_1,...,y_n\}$, такий, що $\max_i \|y_i\| \le \lambda_n(L)$.

5) SIVP γ - задача (The Approximate Shortest Independent Vector Problem)

Вхідні дані: Базис $\{b_1,...,b_n\}$ решітки L, апроксимаційний фактор $\gamma \ge 1$.

Завдання: Знайти лінійно незалежний набір $\{y_1,...,y_n\}$, такий, що $\max_i \|y_i\| \le \gamma\lambda_n(L)$.

Блумер і Сейферт у роботі [21] показали, що SIVP γ - задача є NP-складною для $\gamma = n^{1/\log\log n}$.

6) GapSIVP γ - задача (The Gap Shortest Independent Vector Problem)

Вхідні дані: Решітка L, m -вимірна, з базисом $\{b_1,...,b_n\} \in Z^n$ таким, що $m \ge n$, в Евклідовому просторі, апроксимаційний фактор $\gamma \ge 1$, пара (B,d), де B – ранг, d – раціональне число.

Завдання: Якщо $\lambda_n(B) \le d$, повернути відповідь «Так»; якщо $\lambda_n(B) > \gamma(n)\cdot d$, повернути відповідь «Ні».

Далі розглянемо загальний випадок SIVP- задачі, тобто дещо спрощений випадок SIVP- задачі, який було сформульовано в роботі [22].

7) GIVP $_{\gamma}^{\phi}$ - задача (Generalized Independent Vectors Problem)

Вхідні дані: Базис $B = \{b_1,...,b_n\}$ n -вимірної решітки L.

Завдання: Знайти такий набір лінійно незалежних векторів $S = \{s_1,...,s_n\} \subset L(B)$, що $\|S\| \le \gamma(n)\cdot\phi(B)$.

Зазвичай ϕ означає деяку довільну функцію решітки. Якщо обрати $\phi = \lambda_n$, тоді в результаті отримаємо) SIVP- задачу. В роботі [22] ϕ означає параметр згладжування, який пов'язаний з розподілом Гауса.

6. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА МОДУЛЯРНИХ РЕШІТКАХ

Вперше задачу вирішення малих цілих (SIS- задача) було запропоновано в [22].

1) SIS- задача (Small Integer Solutions Problem)

Вхідні дані: Решітка $L_{A,q}$, модуль q, матриця $A \pmod q$, $v < q$.

Завдання: Знайти таке $y \in Z^m$, що $Ay \equiv 0 \pmod q$ і $\|y\| \le v$.

2) ISIS- задача (Inhomogeneous Small Integer Solutions Problem)

Вхідні дані: Решітка $L_{A,q}$, $x \in Z^n$, модуль q, матриця $A \pmod q$, $v < q$.

Завдання: Знайти таке $y \in Z^m$, що $Ay \equiv x \pmod q$ і $\|y\| \le v$.

Задача навчання з помилками (LWE-задача) була запропонована Регевом у [23]. Нехай q – модуль. Для $s \in Z_q^n$ і ймовірнісного розподілу χ над Z_q нехай $A_{s,\chi}$ – ймовірнісний розподіл над $Z_q^n \times Z_q$ з вибіркою такого виду: $a \in Z_q^n$ обирається рівномірно, $e \in Z_q$ обирається відповідно до χ, далі повертається $(a, \langle a,s\rangle + e) \pmod q$.

3) LWE- задача (Learning With Errors Problem)

Вхідні дані: Решітка $L_{A,q}$, n, розподіл χ (бажано дискретний Гауса), модуль q, будь-яке число незалежних вибірок з $A_{s,\chi}$.

Завдання: Знайти s.

4) DLWE- задача (Decision Learning With Errors Problem)

Вхідні дані: Решітка $L_{A,q}$, n, розподіл χ (бажано дискретний Гауса), модуль q, будь-яке число незалежних вибірок з $A_{s,\chi}$.

Завдання: Якщо були обрані елементи вибірки з $A_{s,\chi}$, повернути відповідь «Так»; якщо були обрані елементи з нормального розподілу повернути відповідь «Ні».

7. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ІДЕАЛЬНИХ РЕШІТКАХ

Перші дві задачі, які наведені нижче, були запропоновані Любашевським і Міссіансіо в роботі [24]. На сьогодні не відомо, чи є наступні задачі NP- складними. Для наступних двох задач, визначимо: для будь-якого ідеалу I над $Z[x]/\langle f\rangle$, де f – це незвідний цілочисельний поліном ступеня n, $\lambda_i^p(I)$ дорівнює $\lambda_i^p(L(I))$.

1) IdealSPP γ - задача (Approximate Shortest Polynomial Problem)

Вхідні дані: Ідеал I решітки L в $Z[x]/\langle f\rangle$.

Завдання: Знайти поліном $g \in I \setminus \{0\}$, такий, що $\|g\|_f \le \gamma\lambda_1^{\infty}(I)$.

Для того щоб сформулювати наступну задачу, дамо визначення фактору розширення (Expansion Factor), який відноситься до властивостей f: $EF(f,k) = \max_{g \in Z[x], \deg(g) \le k(\deg(f)-1)} \|g\|_f / \|g\|_{\infty}$.

2) IdealISPP γ - задача (Approximate Incremental Shortest Polynomial Problem)

Вхідні дані: Ідеал I решітки L в $Z[x]/\langle f\rangle$, поліном $g \in I$, такий, що $\|g\|_f > \gamma\lambda_1^{\infty}(I)$.

Завдання: Знайти $h \in I$, таке, що $\|h\|_f \ne 0$.

Задача IdealSPP γ зводиться за поліноміальний час до IdealISPP γ - задачі [24].

Штеле та ін. у роботі [5] сформулювали дві задачі на решітках IdealSIS$_{q,m}^{f}$ і IdealLWE$_{q,m}^{\chi}$, що засновані на задачах найгіршого випадку IdealSIS і IdealLWE, запропонованих в [22,25]. Спочатку сформулюємо найгірший випадок задачі IdealSIS.

3) IdealSIS $_{q,m,\beta}^{f,p}$ - задача (Ideal Small Integer Solution Problem), найгірший випадок.

Вхідні дані: Поліноми m і n, $g_1,...,g_m$ обрані рівномірно і випадково з $Z_q[x]/\langle f\rangle$.

Завдання: Знайти $e_1,...,e_m$ в $Z[x]$, такі, що $\sum_{i \prec m} e_i g_i = 0 \pmod q$ і $\|e\|_p \le \beta$, де e – це вектор, обчислений шляхом конкатенації всіх коефіцієнтів e_i's.

4) IdealSIS $_{q,m}^{f}$ - задача (Approximate Ideal Small Integer Solution Problem)

Вхідні дані: Решітка L, m-вимірна.

Завдання: Знайти невеликий ненульовий елемент $M^{\perp}(g)=\{b\in(Z[x]/f)^m,\langle b,g\rangle=0 \bmod q\}$ з $Z[x]/\langle f\rangle$, де $g=(g_1,\ldots,g_m)$.

5) IdealLWE$^{\chi}_{q,m}$ - задача (Ideal Learning With Errors Problem).

Вхідні дані: Параметр n, матриця $G\in Z^{m(n)\times n}_{q(n)}$ обрана рівномірно і випадково, і $Gs+e\in(R/[1,q(n)])^n$, де $s\in Z^n_{q(n)}$ обране рівномірно і випадково, координати $e\in(R/q(n))^{m(n)}$ незалежно обраного з $\chi(n)$.

Завдання: Знайти s.

8. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА РАДІУСІ ПОКРИТТЯ

Одед Регев та ін. у роботах [26,27] сформулювали та надали аналіз стійкості задачі покриття радіусу в алгебраїчній решітці (CRP- задача).

1) CRP- задача (Covering Radius Problem)

Вхідні дані: Решітка L, n-вимірна, з множиною точок P.

Завдання: Знайти раціональне число r, таке, щоб сфера з радіусом r навколо всіх точок P покрила весь простір.

Для того щоб сформулювати наступну задачу, дамо визначення радіусу покриття. Радіус покриття $\rho(B)$ решітки

$$L=\{x\in\text{span}(L):\forall y\in L,\langle x,y\rangle\in Z\}$$

з максимальною відстанню $dist(x,\rho(B))$, визначається так: $\rho(B)=\max\limits_{x\in span(B)}\{dist(x,\rho(B))\}$. Наступна задача також визначена для лінійних кодів [27].

2) GapCRPγ-задача (The Gap Covering Radius Problem)

Вхідні дані: Решітка L, m-вимірна, з базисом $\{b_1,\ldots,b_n\}\in Z^n$ таким, що $m\geq n$, в Евклідовому просторі, апроксимаційний фактор $\gamma\geq 1$, пара (B,r), де B – ранг, r – раціональне число.

Завдання: Якщо $\rho(B)\leq r$, повернути відповідь «Так»; якщо $\rho(B)>\gamma(n)\cdot r$, повернути відповідь «Ні».

В роботі [27] була проаналізована складність даної задачі і доказано, що задача радіуса покриття для n-вимірної решітки з апроксимаційним фактором $\gamma(n)$ задовольняє такі властивості:

– для будь-якої константи $\gamma(n)>1$ задача може бути ймовірносно розв'язана за час $2^{O(n)}$;

– для $\gamma(n)=\sqrt{n}$, задача є NP∩coNP- стійкою;

– для $\gamma(n)=2^{\Omega(n\log\log n/\log n)}$, задача може бути розв'язана за випадковий поліноміальний час;

– для $\gamma(n)=2^{\Omega(n(\log\log n)^2/\log n)}$, задача може бути розв'язана за детермінований поліноміальний час.

Пізніше, у роботі [26] було доведено, що для будь-якого достатньо великого $p\leq\infty$, існує константа $c_p>1$, така, що CRP^p - задача є Π_2 - стійкою, відносно апроксимаційного фактору c_p.

Наступна задача наведена в роботі [22]. Зазвичай параметр ϕ, який раніше було описано в задачі GIVP$^{\phi}_{\gamma}$, для наступної задачі означає радіус покриття решітки.

3) GDD$^{\phi}_{\gamma}$- задача (Guaranteed Distance Decoding Problem)

Вхідні дані: Базис $B=\{b_1,\ldots,b_n\}$ n-вимірної решітки L, цільова точка t.

Завдання: Знайти точку $x\in L(B)$ в решітці L, таку, що $\text{dist}(t,x)\leq\gamma(n)\cdot\phi(B)$.

Зазначимо, що для будь-якого базису B у решітці і цільової точки $t\in R^n$ завжди існує точка в решітці з відстанню $\phi(B)$ від t, де $\phi(B)$ – це радіус покриття.

9. ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ ОСНОВНИХ ЗАДАЧ НА РЕШІТКАХ

Результати порівняльного аналізу складності основних обчислювальних задач на алгебраїчних решітках були зведені до табл. 1.

Задачі, що засновані на ідеальних решітках, а також HSVPγ, DSVP, DCVP, GapCVPγ, SBPγ, SMPγ, SIVP, GapSIVPγ, GIVP$^{\phi}_{\gamma}$, SIS, ISIS, LWE, DLWE, CRP і GDD$^{\phi}_{\gamma}$ не були включені до табл. 1, оскільки на сьогодні не відомо, чи є вони NP- складними, та поки що не надано будь-яких оцінок їхньої стійкості.

ВИСНОВОК

У роботі наведено огляд досягнень галузі криптографії, що динамічно розвивається, а саме алгебраїчних решіток. Робота містить необхідні базові визначення, опис основних задач теорії решіток, а також наведені існуючі на сьогодні результати аналізу стійкості основних задач на решітках.

Найважливішими із задач у теорії решіток є SVP і CVP, саме ці задачі породжують майже всі існуючі апроксимації задач на алгебраїчних решітках. Якщо проаналізувати існуючі результати стійкості даних задач, можна сказати, що на сьогодні відкрито питання доказу стійкості більшості з цих задач. Але, тим не менш, існуючі криптосистеми на алгебраїчних решітках мають відносно високу швидкодію, і є стійкими до квантових атак, тому, дане питання є перспективним напрямом вивчення і досліджень у криптографії та прикладній криптології.

Література

[1] *Daniele Micciancio.* Improving lattice based cryptosystems using the Hermite normal form / In Joseph H. Silverman, edit. – Proceedings of the 1st international conference held in Providence. – Lecture Notes in Computer Science «Cryptography and lattices». – Vol.2146. – Springer. – 2001. – P.126–145.

[2] *Oded Regev.* New lattice-based cryptographic constructions / Journal of the ACM. – Vol.51. – 2004. – P.899–942.

Таблиця 1

Результати порівняльного аналізу складності основних задач на решітках

№	Задача	Обчислювальна складність	Результати, стосовно розв'язання даної задачі
1.	SVP	NP- повна задача [12]	Усі існуючі алгоритми вирішують не менш ніж за експоненціальний час
2.	SVP γ	NP- складна [13], для деякого $\gamma = 2^{\log^{1/2-\epsilon}(n)} \approx \sqrt{n}$ [13]	Не існує поліноміальних алгоритмів, для l_p - норми, з константним фактором, та над $\mathrm{NP} \not\subseteq \mathrm{RTIME}(2^{poly(\log n)})$, для деякого $2^{(\log n)^{1/2-\epsilon}}$ [15]
3.	HSVP γ	-	LLL- алгоритм [14] вирішує за поліноміальний час, для $\gamma = (\sqrt{4/3}+\varepsilon)^{(n-1)/2}$ [13]
4.	SLP γ	Вважається, що є NP- складною в найгіршому випадку[12]	-
5.	GapSVP γ	NP-складна для деякого константного значення γ [15]	-
6.	USVP p	NP-складна для деякого $p \geq 1$ з l_p - нормою [16]	-
7.	PSVP p	NP-складна для деякого $p \geq 1$ з l_p - нормою [16]	-
8.	CVP	CVP = CVP_1 є NP- складною [29]	Усі існуючі алгоритми вирішують не менш ніж за експоненціальний час
9.	CVP γ	NP- складна для деякого константного значення γ, та, імовірно, є NP- складною для $\gamma = 2^{\log^{1-\epsilon} n} \approx n$ [19]	Алгоритм Бабаї вирішує за поліноміальний час для $\gamma = 2(\sqrt{4/3})^n$ [13,17]
10.	BDD α	Залежить від α [20], є NP- складною для $\alpha > 1/2\sqrt{2}$	-
11.	SBP	Вважається, що є NP- складною в найгіршому випадку[12]	-
12.	SIVP γ	NP- складна [21], для деякого $\gamma = n^{1/\log\log n}$	-
13.	GapCRP γ	Для деякого $\gamma(n) = \sqrt{n}$, є NP∩coNP- складною[27]	Для будь-якої константи $\gamma(n) > 1$ може бути ймовірнісно вирішена за час $2^{O(n)}$

[3] *O. Regev.* Lattice-based cryptography / In Advances in cryptology (CRYPTO). – 2006. – P.131–141.

[4] *Akinori Kawachi, Keisuke Tanaka, Keita Xagawa.* Multi-bit cryptosystems based on lattice problems / In Tatsuaki Okamoto, Xiaoyun Wang edit. – Lecture Notes in Computer Science «Public key cryptography—PKC 2007». – Vol.4450. – Springer. – 2007. – P.315–329.

[5] *Damien Stehlй, Ron Steinfeld, Keisuke Tanaka, Keita Xagawa. Efficient* Public Key Encryption Based on Ideal Lattices / In Mitsuru Matsui, edit. – Lecture Notes in Computer Science «Advances in Cryptology». – Vol.5912. – Springer. – 2009. – P.617–635.

[6] *Yi Ding, Lei Fan.* Efficient Password-Based Authenticated Key Exchange from Lattices / In Yuping Wang, Yiu-ming Cheung, Ping Guo, Yingbin Wei, edit. – Seventh International Conference on Computational Intelligence and Security. – 2011. – P.934–938.

[7] *Shweta Agrawal, Dan Boneh, Xavier Boyen.* Efficient Lattice (H)IBE in the Standard Model / Lecture Notes in Computer Science «Advances in Cryptology – EUROCRYPT 2010». – Vol.6110. – Springer-Verlag. – 2010. – P.553–572.

[8] *Jin Wang, Jingguo Bi.* Lattice-based Identity-Based Broadcast Encryption Scheme [Електронний ресурс] / Cryptology ePrint Archive. – Report 2010/288.– Режим доступу: http://eprint.iacr.org/2010/288.

[9] *Shweta Agrawal, Xavier Boyen.* Identity-based encryption from lattices in the standard model. [Електронний ресурс] / Manuscript. – Режим доступу: http://www.cs.stanford.edu/~xb/ab09/.

[10] *Amit Sahai, Brent Waters.* Fuzzy identity-based encryption / In Ronald Cramer, edit. – Lecture Notes in Computer Science «Advances in Cryptology - EUROCRYPT 2005». – Vol.3494. – Springer. – 2005. – P. 457–473.

[11] *Sanjit Chatterjee, Palash Sarkar.* Identity-Based Encryption / Springer Science + Business Media, LLC. – 2011. – P.125–135.

[12] *Miklys Ajtai.* Generating Hard Instances of Lattice Problems (Extended Abstract) / In Gary L. Miller, edit. – Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing. – STOC. – Vol.28. – 1996. – P. 99–108.

[13] *Thijs Laarhoven, Joop van de Pol, Benne de Weger.* Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems [Електронний ресурс] / Cryptology ePrint Archive. – Report 2012/533.– Режим доступу: http://eprint.iacr.org/2012/533.

[14] *A.K. Lenstra, H.W. Lenstra, L. Lovasz.* Factoring polynomials with rational coefficients / Mathematische Annalen. – Vol.261(4). – Springer-Verlag. – 1982. – P. 515–534.

[15] *Subhash Khot.* Hardness of approximating the shortest vector problem in lattices / Journal of the ACM. – Vol.52(5). – 2005. – P. 789–808.

[16] *Subhash Khot, Nisheeth K. Vishnoi.* Hardness of Lattice Problems in lp Norm [Електронний ресурс] / Microsoft Research. – Режим доступу: http://research.microsoft.com/en-us/um/people/nvishno/webpapers/kv03svpusvp.pdf.

[17] *Lőszly Babai.* On Lovбsz' lattice reduction and the nearest lattice point problem / Combinatorica. – Vol.6(1). – Springer. – 1986. – P. 1–13.

[18] *H. Yao, G. W. Wornell.* Lattice-reduction-aided detectors for MIMO communication systems / IEEE Global Telecommunications Conference (GLOBECOM 2002). – 2002. – P. 17–21.

[19] *Sanjeev Arora, Lőszly Babai, Jacques Stern, Z. Sweedyk.* The Hardness of Approximate Optimia in Lattices, Codes, and Systems of Linear Equations / Proc. of the 34th Annual Symposium on Foundations of Computer Science IEEE. – Computer Society Press. – 1993. – P. 724–733.

[20] *Y.K. Liu, V. Lyubashevsky, D. Micciancio.* On bounded distance decoding for general lattices / In Josep Diaz, Klaus Jansen, Jose D.P. Rolim, Uri Zwick, edit. – Lecture Notes in Computer Science «Approximation, Randomization, and Combinatorial Optimization, Algorithms and Techniques». – Vol.4110. – Springer. – 2006. – P. 450–461.

[21] *J. Blomer, J.P. Seifert.* On the complexity of computing short linearly independent vectors and short bases in a lattice / Proc. of the 31st annual ACM symposium on Theory of Computing (STOC '99). – 1999. – P. 711–720.

[22] *Daniele Micciancio, Oded Regev.* Worst-Case To Average-Case Reductions Based On Gaussian Measures / SIAM Journal on Computing. – Vol.37(1). – 2007. – P. 267–302.

[23] *Oded Regev.* The Learning with Errors Problem (Invited Survey) / Proc. of the 25th Annual IEEE Conference on Computational Complexity (CCC 2010). – IEEE Computer Society. – 2010. – P. 191–204.

[24] *Vadim Lyubashevsky, Daniele Micciancio.* Generalized compact knapsacks are collision resistant / In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, Ingo Wegener, edit. – Lecture Notes in Computer Science. – Part II. – Vol.4052. – Springer. – 2006. – P. 144–155.

[25] *Craig Gentry, Chris Peikert, Vinod Vaikuntanathan.* Trapdoors for hard lattices and new cryptographic constructions / In Richard E. Ladner, Cynthia Dwork edit. – STOC. – ACM. – 2008. – P. 197–206.

[26] *Ishay Haviv, Oded Regev.* Hardness of the Covering Radius Problem on Lattices. Proc. of the 21st Annual IEEE Conference on Computational Complexity (CCC 2006). – IEEE Computer Society. – 2006. – P. 145–158.

[27] *Venkatesan Guruswami, Daniele Micciancio, Oded Regev.* The Complexity of the Covering Radius Problem on Lattices and Codes / Proc. of the 19th Annual IEEE Conference on Computational Complexity (CCC 2004). – IEEE Computer Society. – 2004. – P.161-173.

[28] J.H. van de Pol. Lattice-based cryptography. – Eindhoven University of Technology. – Eindhoven. – 2011. – 106p. [Докторська дисертація].

[29] P van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice / Technical Report. – Vol.81-04. – Mathematisch Instituut. – 1981.

Надійшла до редколегії 13.03.2013

Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного університету радіоелектроніки.

Макутоніна Лідія Вікторівна, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: асиметричні системи шифрування, криптографічні системи та протоколи, що засновані на ідентифікаторах та алгебраїчних решітках.

УДК 004.056.55

Вычислительная сложность основных задач на алгебраических решетках / М.Ф. Бондаренко, Л.В. Макутонина // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 258–264.

Приводятся обзор и результаты сравнительного анализа основных вычислительных задач, использующих алгебраические решетки..

Ключевые слова: алгебраическая решетка, вычислительная сложность, базис решетки, кратчайший вектор в решетке.

Табл.: 1. Библиогр.: 29 назв.

UDK 004.056.55

Computational complexity of algebraic lattice basic problems / M.F. Bondarenko, L.V. Makutonina // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 258–264.

A review and comparative analysis of basic computational problems using algebraic lattices are provided.

Keywords: algebraic lattice, computational complexity, lattice base, shortest vector in the lattice.

Tab.: 1. Ref.: 29 items.

УДК 621.3.06

ОПТИМИЗАЦИЯ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ОТНОСИТЕЛЬНО УСЛОВИЙ ТЕОРЕТИЧЕСКОЙ НЕДЕШИФРУЕМОСТИ

В.В. КОТЕНКО, С.В. КОТЕНКО, К.Е. РУМЯНЦЕВ, И.Д. ГОРБЕНКО

Приводится фундаментальное решение задачи оптимизации процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Применение предложенного подхода открывает принципиально новую область возможностей для комплексного решения проблем повышения стойкости защиты информации.

Ключевые слова: ансамбль ключевых данных, комплексное решения проблем повышения стойкости, оптимизация процессов защиты информации, условия теоретической недешифруемости, энтропия ансамбля ключа.

ВВЕДЕНИЕ

До настоящего времени стратегия обеспечения теоретической недешифруемости (ТНДШ) информации по ряду причин считается практически нереализуемой. Этим во многом объясняется общепринятое отношение к ней как к некоему недостижимому ориентиру, не заслуживающему внимания в практических приложениях. Возможность решения этой проблемы открывает применение подхода, состоящего в виртуализации процессов защиты информации [1, 2, 3, 4]. Виртуализация, согласно отмеченного подхода, – это реализация возможного в установленных условиях при отсутствии ограничений на выбор условий.

1. ВИРТУАЛИЗАЦИЯ ПРОЦЕССОВ ЗАЩИТЫ ДИСКРЕТНОЙ ИНФОРМАЦИИ

Следуя предложенной в [1, 2] методике виртуализации, установим основное условие теоретической недешифруемости и определим теоретические основы защиты дискретной информации (шифрования) для установленного условия.

Условие 1.1. Защита дискретной информации при определенной статистической зависимости сообщений и ключей должна сопровождаться соответствующим увеличением средней неопределенности ключей.

Теорема 1.1. Пусть шифрование Ф определяется ансамблями сообщений U^*, ключей K^* и криптограмм E^*. Тогда, если при шифровании Ф формирование криптограмм сопровождается увеличением средней неопределенности ключей при их статистической зависимости от сообщений, причем

$$H[K^*/U^*E^*] - H[K^*/U^*] = I[U^*;E^*], \quad (1)$$

то существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Доказательство. Запишем выражение для среднего количества взаимной информации в виде

$$I[U^*K^*;E^*] = I[U^*;E^*] + I[K^*;\ U^*/E^*], \quad (2)$$

где

$$I[K^*;\ U^*/E^*] = I[K^*;U^*E^*] - I[K^*;U^*] = H[K^*/U^*E^*] - H[K^*/U^*]. \quad (3)$$

Из теоремы шифрования следует, что существование теоретически недешифруемого шифра Φ_0 возможно тогда, когда среднее количество взаимной информации $I[U^*K^*;E^*]$ будет равно нулю. Исходя из этого, на основании (2), с учетом (3) имеем

$$I[U^*;E^*] - (H[K^*/U^*E^*] - H[K^*/U^*]) = 0.$$

Откуда окончательно получаем

$$I[U^*K^*;E^*] = I[U^*;E^*] + I[K^*;\ U^*/E^*]. \quad (4)$$

Что и требовалось доказать.

Правую часть выражения (4) в приведенном доказательстве можно трактовать как изменение условной энтропии ключа при формировании криптограмм. Таким образом, из (4) и (1) следует довольно неординарный вывод о том, что теоретическая недешифруемость возможна и при статической зависимости ансамблей сообщений, ключей и криптограмм, если шифрование сопровождается изменением условной энтропии ключа и если данное изменение будет компенсировать среднее количество взаимной информации о сообщениях в криптограммах. Неординарность этого вывода состоит в том, что он расширяет границы общепринятого *классического представления теоретической недешифруемости*, устанавливающего обязательную статистическую независимость сообщений и ключей от криптограмм, т. е.

$$H[U^*/E^*] = H[U^*] \quad (5)$$

$$H[K^*/E^*] = H[K^*] \quad (6)$$

откуда

$$I[U^*;E^*] = H[U^*] - H[U^*/E^*] = 0, \quad (5)$$

$$I[K^*;E^*] = H[K^*] - H[K^*/E^*] = 0. \quad (6)$$

Физический смысл этих условий вполне понятен. Он состоит в исключении какой-либо информации о сообщениях и ключах из криптограмм, формируемых при шифровании. Кроме

того, в основной массе практических приложений обычно постулируется статистическая независимость сообщений и ключей, что объясняется, по-видимому, стремлением обеспечить дополнительные гарантии теоретической недешифруемости. Это стремление, а также попытки максимально приблизиться к (5)–(8), на практике не только приводит к достаточно громоздким и неоптимальным решениям, но и существенно усложняет решение такой важной задачи, как обеспечение имитостойкости.

Теорема1 объясняет возможность существования теоретически недешифруемых шифров при статистической зависимости сообщений и криптограмм, когда равенства (5)–(8) не выполняются. При этом изначально допускается, что ансамбли U^* и K^* статистически связаны и отсутствие этой статистической зависимости рассматривается лишь как частный случай, при котором (1) принимает вид

$$H[K^*/E^*] - H[K^*] = I[U^*;E^*]. \qquad (7)$$

Откуда с учетом того, что

$$I[K^*;E^*] = H[K^*] - H[K^*/E^*] \qquad (8)$$

следует

$$I[K^*;E^*] = -I[U^*;E^*]. \qquad (9)$$

В свою очередь, если в выражении (1) учесть, что

$$H[K^*/U^*] - H[K^*/U^*E^*] = I[K^*;U^*/E^*] \qquad (10)$$

и в соответствии с этим привести его к виду

$$-I[K^*;U^*/E^*] = I[U^*;E^*], \qquad (11)$$

то становится понятным и общий физический смысл Теоремы 1. Оказывается, что теоретически недешифруемые шифры могут существовать и при статистической зависимости ансамблей сообщений, ключей и криптограмм, если шифрование предполагает увеличение средней условной неопределенности ключей. Причем это увеличение должно обеспечиваться введением ложной информации о сообщениях в формируемые криптограммы.

Из доказанной теоремы следует принципиально новый подход к решению задач защиты дискретной информации, состоящий в допущении возможности существования теоретически недешифруемых шифров при статистической зависимости ансамблей сообщений, криптограмм и ключей. Введение регулируемой неопределенности изменения энтропии ансамбля ключа, соответствующей среднему количеству взаимной информации $I[U^*; E^*]$ в процессе шифрования, можно трактовать как виртуализацию алгоритма формирования ключей относительно условия 1.

Таким образом, установленное условие 1 и доказанная применительно к этому условию теорема 1 определяют обобщенную модель виртуализации защиты дискретной информации с позиций теоретической недешифруемости (рис. 1).

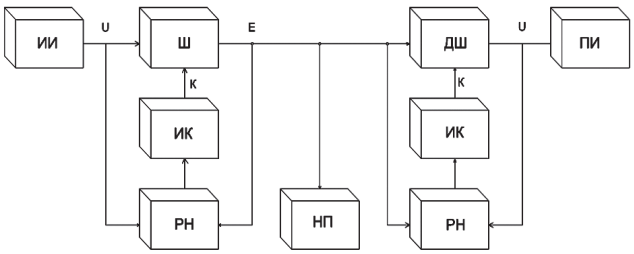


Рис. 1. Обобщенная модель виртуализации процесса защиты дискретной информации с позиций условий теоретической недешифруемости

Особенностью полученной модели является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности (РН) состояний источника ключа (ИК) по правилам, базирующимся на теоретической основе, установленной Теоремой1.

2. ВИРТУАЛИЗАЦИЯ ПРОЦЕССОВ ЗАЩИТЫ НЕПРЕРЫВНОЙ ИНФОРМАЦИИ

Виртуализация процесса защиты непрерывной информации заключается в установлении условий виртуализации, оптимизирующих этот процесс, и определении решений, соответствующих данным условиям.

В общем виде процесс защиты непрерывной информации представляет собой процесс преобразования непрерывных сообщений в криптограммы по секретному закону, определенному ключом. Обычно этот процесс называют *скремблированием*, а обратный ему процесс преобразования криптограмм в сообщения — *дескремблированием*. В зависимости от вида ансамбля формируемых криптограмм существует *два* основных варианта защиты непрерывной информации:

– аналоговое скремблирование, когда ансамбль формируемых криптограмм является непрерывным;

– цифровое скремблирование, когда ансамбль формируемых криптограмм дискретный.

Отличительной особенностью процесса защиты непрерывной информации является высокая избыточность непрерывных сообщений, которую, как правило, не удается в полной мере устранить в формируемых криптограммах. Решение этой проблемы определяет целесообразность виртуализации источников непрерывной информации относительно условий, устанавливающих достижение минимально возможного значения избыточности сообщений. При этом, возможно два варианта виртуализации источников непрерывной информации:

– виртуализация непрерывного источника при условии реализации виртуального непрерывного источника с минимально возможной избыточностью;

– виртуализация непрерывного источника при условии реализации виртуального дискретного источника с минимально возможной избыточностью.

Первый вариант виртуализации источников непрерывной информации применяется при аналоговом скремблировании, второй – при цифровом скремблировании. Исходя из этого, обобщенная модель процесса защиты непрерывной информации имеет два вида представления:

1) представление для аналогового скремблирования (рис. 2);

2) представление для цифрового скремблирования (рис. 3).

При аналоговом скремблировании непрерывные сообщения s(t) источника информации (ИИ) обычно подвергаются компандированию. Чаще всего это частотная компрессия непрерывных сообщений на выходе ИИ, означающая сжатие частотного диапазона спектра случайного процесса, представляющего ансамбль S источника. Формируемый таким образом процесс можно представить, как выборочное пространство некоторого *виртуального непрерывного источника* $\hat{S}$, обладающего меньшей избыточностью. Преобразование непрерывного ансамбля S в непрерывный ансамбль $\hat{S}$, применительно к условию минимизации избыточности, определяется как *непрерывная виртуализация источника*. Сообщения $s(t)$ этого источника путем преобразований аналогового скремблирования (ПАС) по закону, заданному элементами дискретного ансамбля K источника ключа (ИК), преобразуются в криптограммы $e(t)$ ансамбля криптограмм E. Ансамбль криптограмм в данном случае является непрерывным.

При дескремблировании производятся обратные преобразования аналогового скремблирования (ОПАС) криптограмм в сообщения $s(t)$, которые после экспандирования (декомпрессии) поступают к получателю информации. Закон обратных преобразований аналогового скремблирования задается ключами ансамбля K. При этом к криптограммам может получать доступ несанкционированный пользователь (НП). Основная задача защиты непрерывной информации в данном случае состоит в установлении аналогового скремблирования источника, обеспечивающего невозможность дескремблирования криптограмм при несанкционированном доступе к ним.

Нетрудно заметить, что основу решения данной задачи составляет выбор методов преобразований аналогового скремблирования. К используемым для этих целей методам ПАС принято относить: 1) методы коммутируемой инверсии; 2) методы частотных перестановок; 3) методы временных перестановок; 4) методы амплитудного скремблирования. Часто в целях повышения эффективности аналогового скремблирования применяют различные комбинации отмеченных методов в виде так называемых комбинированных методов ПАС. Однако, как показала практика, все это не позволяет обеспечить решение отмеченной основной задачи. Исходной причиной данной проблемы является высокая избыточность непрерывных сообщений, которую не удается устранить при формировании криптограмм. Так, например, для речевых сообщений характерна почти двадцатикратная избыточность, которая в значительной мере сохраняется и после скремблирования. Следствием этого является принятая в настоящее время *стратегия аналогового скремблирования*, основными направлениями которой выступают:

1) обеспечение временной стойкости защиты информации;

2) выполнение условий однозначности дескремблирования.

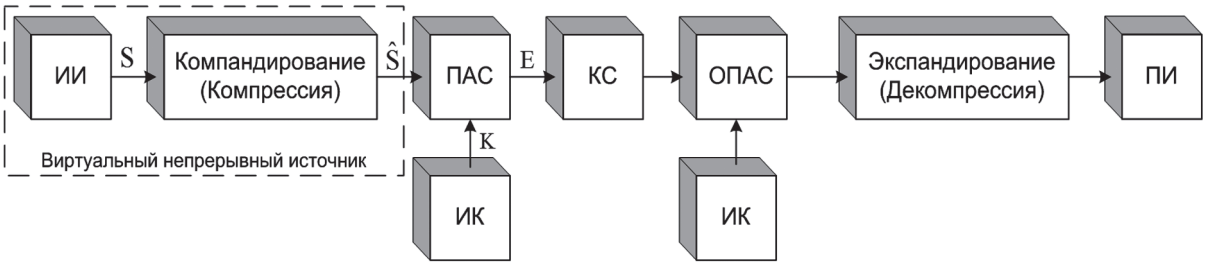


Рис. 2. Обобщенная модель аналогового скремблирования с позиций условия реализации виртуального непрерывного источника

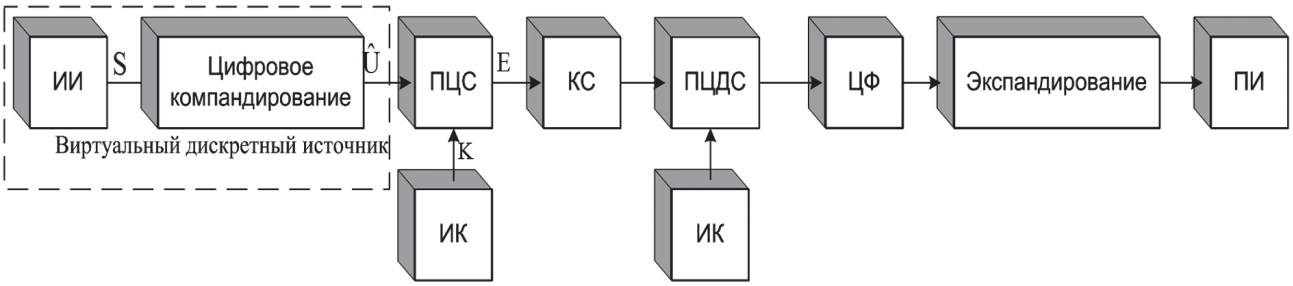


Рис. 3. Обобщенная модель цифрового скремблирования с позиций условия реализации виртуального дискретного источника

Условия однозначного дескремблирования обеспечиваются идентичностью ключевых последовательностей, используемых при скремблировании и дескремблировании, а также полной идентичностью прямых и обратных частотно-временных преобразований.

Цифровое скремблирование, в отличие от аналогового, обеспечивает более эффективное решение проблемы высокой избыточности непрерывных источников. Это достигается путем цифрового компандирования непрерывных сообщений $s(t)$ источника информации (ИИ). Полученные таким образом кодовые последовательности можно рассматривать, как элементы ансамбля $\hat{U}$, соответствующего некоторому *виртуальному дискретному источнику*. Преобразование непрерывного ансамбля S в дискретный ансамбль $\hat{U}$, применительно к условию минимизации избыточности, определяется как *дискретная виртуализация источника*. С этих позиций последующие преобразования цифрового скремблирования (ПЦС) и цифрового дескремблирования (ПЦДС) выступают аналогами шифрования и дешифрования при защите дискретной информации. Это во многом объясняет преимущественное применение в задачах цифрового скремблирования подходов, используемых при шифровании. При этом требуется учитывать *особенности, свойственные цифровому скремблированию*. Во-первых, на эффективность цифрового скремблирования существенное влияние могут оказывать потери информации, вызванные цифровым представлением. Во-вторых, применение в нем компандирования открывает дополнительные возможности для повышения качества защиты информации. Первая особенность обычно учитывается путем оптимальной цифровой фильтрации (ЦФ) результатов дескремблирования, вторая – путем подбора методов компрессии и экспандирования, обеспечивающих максимальное уменьшение избыточности для заданной точности восстановления непрерывной информации у получателя (ПИ).

Таким образом, принятая в настоящее время *стратегия цифрового скремблирования* включает следующие основные направления:

1) обеспечение гарантированной стойкости защиты информации;

2) выполнение условий однозначности дескремблирования;

3) обеспечение требуемой точности восстановления сообщений.

Следует обратить внимание, что данная стратегия, за исключением третьего направления, аналогична принятой в настоящее время стратегии защиты дискретной информации. Таким образом, цифровому скремблированию в принципе свойственны те же проблемы, что и шифрованию. Однако особенности цифрового скремблирования в значительной мере усиливают эти проблемы, требуя специфичных подходов к решению о*сновной задачи* защиты информации, состоящей в данном случае в установлении цифрового скремблирования, обеспечивающего невозможность дескремблирования криптограмм при несанкционированном доступе к ним. Прежде всего, это относится к проблеме абсолютной недешифруемости, которая при цифровом скремблировании приобретает специфику. Следует отметить, что при аналоговом скремблировании эта специфика значительно усиливается, делая решение проблемы абсолютной недешифруемости практически невозможным.

С позиций теории виртуализации стратегия решения проблемы абсолютной недешифруемости защиты непрерывной информации определяется как:

– установление условий виртуализации непрерывных источников информации;

– установление условий теоретической недешифруемости защиты непрерывной информации;

– установление условий, при которых любой продуктивный прогноз ключа является невозможным;

– определение теоретических основ защиты непрерывной информации (скремблирования) в установленных (заданных) условиях.

Согласно принятой стратегии, установим основные условия теоретической недешифруемости и определим теоретические основы защиты непрерывной информации (скремблирования) для установленных условий. По аналогии с шифрованием основу определения условий обеспечения абсолютной недешифруемости при защите непрерывной информации составляет определение теорем скремблирования.

Теорема 2.1. Теорема аналогового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений S, непрерывным ансамблем криптограмм E и дискретным ансамблем ключей K. Тогда, если среднее количество взаимной информации равно

$$I[SK;E] = 0, \qquad (12)$$

то существует аналоговое скремблирование Φ_{CA}, обеспечивающее теоретическую недешифруемость.

Доказательство. Теоретическая недешифруемость дескремблирования криптограмм при несанкционированном доступе означает, что

$$J[s_i(t)k(i);e_i(t)] = 0 \text{ , для всех } i \text{ ,}$$

т. е. количество информации о сообщении $s_i(t)$ и соответствующем ему i -м ключе $k(i)$, содержащееся в криптограмме $e_i(t)$, должно быть равным нулю.

Среднее количество взаимной информации о сообщениях и ключах в криптограммах определяется как

$$I[SK;E]=M\left[J[s_i(t)k(i);e_i(t)]\right], \qquad (13)$$

где $M\left[J[s_i(t)k(i);e_i(t)]\right]$ – функция математического ожидания.

Так как количество информации всегда неотрицательная величина, т. е. $J[s_i(t)k(i);e_i(t)] \geq 0$, то равенство (12) всегда будет однозначно свидетельствовать о выполнении (13). Что и требовалось доказать.

Криптограммы при аналоговом скремблировании с физической точки зрения можно рассматривать как результат искажения непрерывных сообщений источника некоторым гипотетическим непрерывным шумом скремблирования, характеристики которого определяются элементами дискретного ансамбля ключа. Исходя из этого, доказанная теорема позволяет определить условия, при которых исключается возможность дескремблирования криптограмм при несанкционированном доступе, т. е. когда среднее количество информации о сообщениях в криптограммах будет стремиться к нулю.

Теорема 2.2. Пусть скремблирование определяется непрерывным ансамблем сообщений *S*, непрерывным ансамблем криптограмм *E* и дискретным ансамблем ключей *K*. Пусть s_i и e_i – случайные величины, представляющие выборки реализаций непрерывных выборочных пространств ансамблей сообщений и криптограмм, соответственно, и пусть σ_i^2 – дисперсия искажающего воздействия на сообщение в процессе скремблирования, заданного составляющими выборочного пространства ансамбля ключа. Тогда среднее количество информации о сообщениях в криптограммах при аналоговом скремблировании будет стремиться к нулю, если дисперсия σ_i^2 будет стремиться к бесконечности, т. е. $\sigma_i^2 \to \infty$.

Доказательство. Введем ряд упрощений, не влияющих на общность доказательства. Будем считать, что сообщения источника имеют гауссовский закон распределения, а также, что сообщения и криптограммы статистически не связаны с элементами дискретного ансамбля ключа. Таким образом, с учетом гауссовской аппроксимации сообщения можно представить как гауссовскую случайную величину с нулевым средним значением, дисперсией σ_s^2 и плотностью вероятности вида:

$$P(s_i) = \frac{1}{\sqrt{2\pi\sigma_s^2}} \exp\left(-\frac{s_i^2}{2\sigma_s^2}\right). \qquad (14)$$

Исходя из статистической независимости сообщений и криптограмм от элементов дискретного ансамбля ключа, искажающее воздействие на сообщение в процессе скремблирования, можно считать аддитивным вид гауссовской случайной величины с нулевым средним значением и дисперсией σ_i^2. Тогда условная плотность вероятности криптограмм при условии, что заданы сообщения, имеет вид

$$P(e_i / s_i) = \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp\left[-\frac{(e_i - s_i)^2}{2\sigma_i^2}\right]. \qquad (15)$$

Так как криптограммы в данном случае представляются как сумма двух гауссовских случайных величин, их также можно считать гауссовской случайной величиной с дисперсией $\sigma_s^2 + \sigma_i^2$ и плотностью вероятности

$$P(e_i) = \frac{1}{\sqrt{2\pi(\sigma_s^2 + \sigma_i^2)}} \exp\left[-\frac{e_i^2}{2(\sigma_s^2 + \sigma_i^2)}\right].$$

Выражения (14) и (15) позволяют определить дифференциальную условную энтропию для ансамблей *S* и *E*:

$$h[E/S] = -\int P(s_i) \int P(e_i / s_i) \log P(e_i / s_i)\, de_i ds_i =$$

$$= \int P(s_i) \int P(e_i / s_i) \left[\log\sqrt{2\pi\sigma_i^2} + \frac{(e_i - s_i)^2}{2\sigma_i^2} - \log e\right] de_i ds_i.$$

Учитывая, что $\int P(e_i / s_i)\left(e_i^2 - s_i^2\right) de_i$ равен дисперсии условного распределения σ_i^2, получаем

$$h[E/S] = \int P(s_i)\left[\log\sqrt{2\pi\sigma_i^2} + \frac{1}{2}\log e\right] ds_i =$$

$$= \frac{1}{2}\log\left(2\pi e\sigma_i^2\right).$$

Аналогично можно определить выражение для дифференциальной энтропии криптограмм:

$$h[E] = \frac{1}{2}\log\left[2\pi e\left(\sigma_s^2 + \sigma_i^2\right)\right].$$

Откуда окончательно получаем выражение для средней взаимной информации:

$$I[S;E] = h[E] - h[E/S] = \frac{1}{2}\log\left(1 + \frac{\sigma_s^2}{\sigma_i^2}\right). \qquad (16)$$

Из (16) следует, что среднее количество информации о сообщениях в криптограммах стремится к нулю, когда дисперсия σ_i^2 стремится к бесконечности. Что и требовалось доказать.

Полученный результат может быть обобщен для случая, когда выборочные пространства сообщений и криптограмм задаются случайными процессами. С учетом этого доказанная теорема имеет принципиально важное практическое значение. Она *показывает невозможность обеспечения условий ТНДШ при аналоговом скремблировании* и во многом объясняет непродуктивность поиска подходов, практически исключающих возможность дескремблирования криптограмм при несанкционированном доступе.

Теорема 2.3. Теорема цифрового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений *S*, дискретным ансамблем криптограмм *E* и дискретным ансамблем ключей *K*. Пусть дискретный ансамбль $\hat{U}$ является ансамблем виртуальных сообщений, полученным в результате виртуализации непрерывного ансамбля *S*. Тогда, если среднее количество взаимной информации равно

$$I[\hat{U}\,K;E] = 0,$$

то всегда существует цифровое скремблирование Φ_{CD}, обеспечивающее теоретическую недешифруемость.

Доказательство. Теоретическая недешифруемость дескремблирования криптограмм при несанкционированном доступе для рассматриваемого случая означает, что

$$J[u(i)k(i);e(i)]=0, \qquad (17)$$

т. е. количество информации о сообщении $s_i(t)$, представленное в $u(i)$, и ключе $k(i)$, содержащееся в криптограмме $e(i)$, должно быть равным нулю.

Среднее количество взаимной информации о сообщениях и ключах в криптограммах для рассматриваемого случая определяется как

$$I[UK;E]=M\left[J[u(i)k(i);e(i)]\right], \qquad (18)$$

где $M\left[J[u(i)k(i);e(i)]\right]$ — функция математического ожидания.

Так как количество информации всегда неотрицательная величина, т. е. $J[u(i)k(i);e(i)]\geq 0$, то равенство (17) всегда будет однозначно свидетельствовать о выполнении (18). Что и требовалось доказать.

Теорема 2.4. Теорема виртуализации цифрового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений *S*, дискретным ансамблем криптограмм *E* и дискретным ансамблем ключей *K*. Пусть дискретный ансамбль $\hat{U}$ является ансамблем виртуальных сообщений, полученным в результате виртуализации непрерывного ансамбля *S*. Пусть элементы выборочного пространства ансамбля $\hat{U}$ формируются в результате цифрового компандирования сообщений выборочного пространства ансамбля *S*. Тогда, если при цифровом скремблировании, заданном дискретными ансамблями ключей *K* и криптограмм *E*, средняя взаимная информация $I[\hat{U}\,K;E]=0$, то всегда и только всегда будет справедливо равенство $I[SK;E]=0$.

Доказательство. Как уже отмечалось, к особенности цифрового скремблирования относится то, что преобразованиям цифрового скремблирования подвергаются не сами непрерывные сообщения ансамбля *S* источника, а результаты их цифрового компандирования, составляющие ансамбль $\hat{U}$. Исходя из этого, выражение для средней взаимной информации $I[S\,K;\,E]$ может быть представлено в виде

$$I[SK;E]=I\left[S\hat{U}\,K;E\right]=$$
$$=I\left[\hat{U};E\right]+I\left[K;E/\hat{U}\right]+I\left[S;E/K\hat{U}\right].$$

Отметим, что сумма двух первых членов правой части соответствует средней взаимной информации $I[\hat{U}\,K;E]=0$. Исходя из этого, выражение может быть приведено к виду

$$I[SK;E]=I\left[\hat{U}\,K;E\right]+I\left[S;E/K\hat{U}\right]. \qquad (12)$$

Запишем выражение для второго члена правой части:

$$I\left[S;E/K\hat{U}\right]=I\left[S;K\hat{U}\,E\right]-I\left[S;K\hat{U}\right]. \qquad (13)$$

Вследствие отмеченной особенности цифрового скремблирования средняя взаимная информация о сообщениях ансамбля *S* источника в элементах ансамблей $\hat{U}$, *K* и *E* будет однозначно определяться средней взаимной информацией о сообщениях ансамбля *S* в результатах их цифрового компандирования, составляющих ансамбль $\hat{U}$, т. е.

$$I\left[S;K\hat{U}\,E\right]=I\left[S;K\hat{U}\right]=I\left[S;\hat{U}\right].$$

Откуда окончательно получаем

$$I[SK;E]=I\left[\hat{U}\,K;E\right]. \qquad (19)$$

Таким образом, для выполнения равенства $I[SK;E]=0$ необходимо и достаточно выполнение равенства $I[\hat{U}\,K;E]=0$. Что и требовалось доказать.

Доказательство теоремы устанавливают взаимосвязь цифрового скремблирования и шифрования. Так, выражение (19) дает основание считать, что условия теоретической недешифруемости защиты дискретной информации, применимые для виртуального дискретного ансамбля сообщений $\hat{U}$, будут применимы и для соответствующего ему исходного непрерывного ансамбля *S*. При этом теоремы 2.1 – 2.4 и будут определять теоретические основы реализации этих условий и, как следствие, обобщенную модель виртуализации защиты непрерывной информации с позиций условий теоретической недешифруемости (рис. 4).

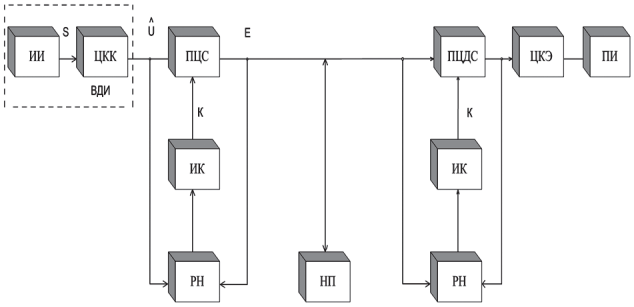


Рис. 4. Обобщенная модель виртуализации процесса защиты непрерывной информации с позиций условий теоретической недешифруемости

Особенностью полученной модели является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности (РН) состояний источника ключа. Ансамбль $\hat{U}$ является результатом виртуализации ансамбля *S* непрерывного источника информации. Таким образом, эффективность обобщенной модели процесса защиты непрерывной информации, с позиций условий теоретической недешифруемости (рис. 4), зависит от

установленных условий виртуализации непрерывного источника информации.

Основу виртуализации непрерывных источников при цифровом скремблировании составляет цифровое компандирование, предусматривающее компрессию (ЦКК) при скремблировании и экспандирование (ЦКЭ) при дескремблировании (рис. 4). С этих позиций к основным *условиям виртуализации непрерывных источников при цифровом скремблировании* относятся:

1. Минимизация информационных потерь.

2. Обеспечение минимальной избыточности.

Обеспечение установленных условий целесообразно рассматривать относительно к цифровому скремблированию, т. к. из доказательства теоремы 2.2 следует невозможность обеспечения условий ТНДШ при аналоговом скремблировании. Поэтому виртуализация непрерывных источников при цифровом скремблировании определяется как цифровая виртуализация.

ВЫВОДЫ

1. При теоретически недешифруемой защите дискретной информации ансамбль ключевых данных не оказывает влияния на стойкость шифрования, что позволяет использовать ключевые данные, открытые для несанкционированного доступа.

2. Защита дискретной информации при определенной статистической зависимости сообщений и ключей должна сопровождаться соответствующим увеличением средней неопределенности ключей.

3. Теоретическая недешифруемость возможна при статической зависимости ансамблей сообщений и криптограмм, если шифрование сопровождается изменением условной энтропии ключа и если данное изменение будет соответствовать среднему количеству взаимной информации о сообщениях в криптограммах.

4. Теоретически недешифруемая защита дискретной информации может обеспечиваться при статистической зависимости ансамблей сообщений, ключей и криптограмм, если предполагается увеличение средней условной неопределенности ключей. Причем это увеличение должно обеспечиваться введением ложной информации о сообщениях в формируемые криптограммы.

5. Введение регулируемой неопределенности изменения энтропии ансамбля ключа, в процессе шифрования, можно трактовать как изменение алгоритма формирования ключей соответственно установленным условиям теоретической недешифруемости, т.е. как виртуализацию алгоритма формирования ключей.

6. При цифровом скремблировании условия теоретической недешифруемости защиты дискретной информации, применимые для виртуального дискретного ансамбля сообщений, будут применимы и для соответствующего ему исходного непрерывного ансамбля сообщений.

7. Особенностью обобщенной модели процесса защиты непрерывной информации с позиций условий теоретической недешифруемости является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности состояний источника ключа.

8. Непрерывное сообщение, полученное в результате цифрового дескремблирования (оценка) и ошибка цифрового компандирования должны быть независимыми.

Литература

[1] *Котенко В.В.* Теория информации и защита телекоммуникаций: монография / В.В. Котенко, К.Е. Румянцев. – Ростов н/Д: Изд-во ЮФУ, 2009. – 369 с.

[2] *Величкин А.И.* Передача аналоговых сообщений по цифровым каналам. – М.: Радио и связь. – 1983. – 240 с.

[3] *Kotenko V., Rumjantsev K., Kotenko S.* "New Approach to Evaluate the Effectiveness of the Audio Information Protection for Determining the Identity of Virtual Speech Images". Proc. of the Second International Conference on Security of Information and Networks. The Association for Computing Machinery (ACM). New York. Publications Dept., ACM, Inc. 2009, pp. 235–239.

[4] *Котенко В.В.* Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177–183.

[5] *Котенко В.В.* Теоретические основы виртуализации представления объектов, явлений и процессов // Информационное противодействие угрозам терроризма: науч.-практ. журн., 2011, № 17. – С. 32–48

[6] *Котенко В.В.* Теоретические основы виртуализации информационных потоков // Информационное противодействие угрозам терроризма: науч.-практ. журн., 2011, № 17. – С. 69–80.

[7] *Котенко В.В.* Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа. // Информационное противодействие угрозам терроризма: науч.-практ. журн., 2011, № 17. – С. 96–104.

Поступила в редколлегию 19.03.2013

Котенко Владимир Владимирович, профессор кафедры информационной безопасности телекоммуникационных систем факультета информационной безопасности Южного федерального университета. Научные интересы: защита информации в информационно-телекомуникационных системах, информационное противодействие угрозам терроризма.

Котенко Станислав Владимирович, аспирант Южного федерального университета. Научные интересы: защита информации в информационно-телекомуникационных системах, информационное противодействие угрозам терроризма.

Румянцев Константин Евгеньевич, заведующий кафедрой информационно безопасности телекоммуникационных систем факультета информационной безопасности Южного федерального университета. Научные интересы: защита информации в информационно-телекомуникационных системах, информационное противодействие угрозам терроризма.

Горбенко Иван Дмитриевич, фото и сведения об авторе см. на стр. 201.

УДК 621.3.06

Оптимізація процесів захисту інформації з позицій віртуалізації щодо умов теоретичної недешифрувальності / В.В. Котенко, С.В. Котенко, К.Є. Румянцев, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 265–272.

Наводиться фундаментальне розв'язання задачі оптимізації процесів захисту інформації з позицій віртуалізації щодо умов теоретичної недешифрувальності. Застосування запропонованого підходу відкриває принципово нову область можливостей для комплексного вирішення проблем підвищення стійкості захисту інформації.

Ключові слова: ансамбль ключових даних, комплексне вирішення проблем підвищення стійкості, оптимізація процесів захисту інформації, умови теоретичної недешифрувальності, ентропія ансамблю ключа.

Іл.: 4. Бібліогр.: 7 найм.

UDC 621.3.06

Optimization of information security processes in terms of virtualization relative to conditions of theoretical indecipherability / V.V. Kotenko, S.V. Kotenko, K.E. Rumyantsev, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 265–272.

The fundamental solution of the problem of optimization of information security processes from virtualization positions concerning conditions of theoretical indecipherability is provided. Application of the offered approach opens a brand new area of opportunities for the complex solution of problems of improving information security.

Keywords: ensemble of key data, complex solution of problems of improving security, optimization of processes of information security, conditions of theoretical indecipherability, entropy of a key ensemble.

Fig.: 4. Ref.: 7 items.

УДК 681.3.06

ПАРАМЕТРИ КРИПТОСИСТЕМИ НА КРИВІЙ ЕДВАРДСА НАД РОЗШИРЕННЯМИ МАЛИХ ПРОСТИХ ПОЛІВ

А.В. БЕССАЛОВ, А.А. ДІХТЕНКО, О.І. ЯЦЕНКО

Розглянуто можливість удосконалення криптографічних систем на еліптичних кривих на базі кривих у формі Едвардса. Описаний підхід для обчислення загальносистемних параметрів криптосистеми на кривій Едвардса над розширеннями полів F_5 та F_7. Отримано 28 наборів параметрів, що відповідають стандартним криптографічним вимогам та можуть бути рекомендовані у майбутніх стандартах.

Ключові слова: еліптична крива, форма Едвардса, розширене поле, порядок кривої.

ВСТУП

Криптосистеми на еліптичних кривих є основою більшості сучасних стандартів та протоколів шифрування. Паралельно із дослідженнями щодо можливих атак на еліптичні криптосистеми не менш інтенсивно відбувається процес пошуку шляхів можливого вдосконалення таких систем. Роботи [2–6] присвячені дослідженню та аналізу властивостей нормальної форми (або форми Едвардса) еліптичної кривої, які можуть бути цікаві з точки зору криптографії. Аналіз складності групової операції для кривих у формі Едвардса дозволяє стверджувати, що на сьогоднішній день вони є найбільш продуктивними, порівняно з іншими відомими формами еліптичних кривих [2, 3]. У роботі [4] розглянуто перетворення канонічної еліптичної кривої в ізоморфну криву Едвардса, наведено умови, за яких порядок кривої Едвардса має найменший кофактор 4. Оскільки криві Едвардса не стандартизовані, відкритою залишається задача пошуку кривих, прийнятних до криптографії. В роботі [5] запропонований один із можливих шляхів розв'язання цієї задачі, а саме пошук кривих Едвардса над розширеннями полів малої характеристики, а в [6] наданий аналіз щодо складності задачі дискретного логарифмування на кривій Едвардса над розширенням малих полів.

Базуючись на результатах [2–6], у даній роботі наведений набір параметрів для реалізації криптографічної системи на кривій Едвардса над розширеннями поля малої характеристики. В результаті отримано набори з 28 примітивних поліномів та відповідних до них генераторів групи точок кривої Едвардса над полями F_5^{181}, F_5^{277} та F_7^{127}.

1. ПОРЯДКИ КРИВИХ ЕДВАРДСА НАД РОЗШИРЕННЯМИ ПОЛІВ МАЛОЇ ХАРАКТЕРИСТИКИ, ПРИЙНЯТНІ ДЛЯ КРИПТОГРАФІЇ

Крива Едвардса над кінцевим полем F_p^m характеристики $p > 3$ в афінній системі координат визначається рівнянням [1, 2]:

$$x^2 + y^2 = 1 + dx^2y^2,$$

де $d(1 - d) \neq 0$,

$$d \neq A^2. \qquad (1)$$

З точністю до ізоморфізму [2–4] можна вважати різними криві, що задаються різними значеннями параметру d у рівнянні (1), причому d має бути квадратичним нелишком в полі F_p^m. Будь-яка така крива має 4 обов'язкові точки:

$O = (0, 1]$ – нуль адитивної групи точок,

$D = (0, -1)$ – єдину точку другого порядку,

$\pm P = (\pm 1, 0)$ – точки четвертого порядку.

Отже, характерною властивістю кривих вигляду (1) є те, що їх порядок кратний 4. Формули додавання двох точок кривої Едвардса мають вигляд [1, 2]:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right). \qquad (2)$$

Закон додавання є повним і визначений для будь-яких двох точок (x_1, y_1), (x_2, y_2), якщо d – квадратичний нелишок у полі F_p^m [2].

У роботі [5] детально розглянуто один із можливих способів знаходження кривих Едвардса вигляду (1), в межах прийнятних криптографічних значень параметрів. Ідея полягає у знаходженні кривої Едвардса мінімального порядку 4 над полем F_p малої характеристики та подальшому розширенні поля з метою відбору простих степенів розширення m, за яких знайдена крива над полем F_p^m має майже просте значення порядку $N_{Em} = 4n$ (де n – просте). В [5] отримано три розширених поля характеристики $p = 5$ або $p = 7$, для яких крива $x^2 + y^2 = 1 + 3x^2y^2$ має псевдопросте значення порядку, що відповідає стандартним вимогам до порядку генератора криптосистеми. Отримані поля наведені в таблиці 1 відповідно до величини поля в бітах та значення $n = N_{Em}/4$.

Слід зауважити, що арифметичні операції в полях малої характеристики та їх розширеннях, як правило, виконуються більш ефективно порівняно з простими полями великої характеристики [5]. Крім того, криві з малим значенням параметру $d = 3$ дають можливість зменшити складність операції додавання різних точок на 1U – одну польову операцію множення на параметр кривої [2, 4], оскільки множення на 3 замінюється триразовим додаванням у полі (тобто практично безкоштовною операцією).

Таблиця 1

Розширення полів характеристики $p = 5$ та $p = 7$ та відповідні прості порядки підгрупи точок кривої $x^2 + y^2 = 1 + 3x^2y^2$

F_p^m	m_b	$n = N_{Em}/4$
F_5^{181}	420	4D1E1043D31FB1CC9B562A717B3C43259476330974981C14F25E03EACA14C7378C72BEB6F54DB 72B8180B352DF12BA34CC023C219
F_5^{227}	527	21C529DD78FA571E196B3EBB0D20429C476A1848CAB5E0E8A121378DE187888F99D299F404EE 4F9B-C974D5035A62AC9F5E1E0DA29A510B4012E23ECD15909A4B1065
F_7^{127}	356	5CAC4104D859A6DF582D5731211D9947A4AE9CFD1F4E3648997D050DCE03624B891381F19AA 1824CF98DE5637

2. ОБЧИСЛЕННЯ ПАРАМЕТРІВ КРИПТОСИСТЕМИ НА КРИВІЙ ЕДВАРДСА НАД РОЗШИРЕННЯМИ МАЛИХ ПОЛІВ

Подальша реалізація рекомендованих у [5] кривих Едвардса над розширеннями полів F_5 та F_7 становить два послідовних етапи:

– пошук примітивних поліномів $P(z)$ для полів F_5^{181}, F_5^{277}, F_7^{127} та побудова відповідної арифметики цих полів;

– обчислення генератора абелевої групи точок кривої згідно з визначеною арифметикою полів F_5^{181}, F_5^{277} та F_7^{127}.

Таким чином, за допомогою прикладної програми був отриманий ряд примітивних поліномів вказаних полів, серед яких ми обрали поліноми найменшої ваги. (Слід зазначити, що для випадку поля F_7^{127} існують примітивні поліноми найменшої можливої ваги – тобто триноми). У загальному випадку точками кривої будуть пари (x, y) елементів поля F_p^m, для яких виконується рівність (1). Щоб отримати генератори підгруп точок досліджуваної кривої Едвардса $x^2 + y^2 = 1 + 3x^2y^2$, вибираємо випадкову координату x з елементів відповідного поля та обчислюємо значення $a = \dfrac{1 - x^2}{1 - 3x^2}$. Визначення квадратного кореня з елементу a в розширеному полі робиться за допомогою експоненціювання [4].

У випадку полів характеристики 5:

$$q = 5^{181} \equiv 5 \bmod 8$$

або

$$q = 5^{227} \equiv 5 \bmod 8.$$

У мультиплікативній групі поля F_q, якщо $a = y^2$ – квадратичний лишок, маємо елементи підгрупи F_5^*:

$$a^{\frac{q-1}{2}} = 1,$$

$$a^{\frac{q-1}{4}} = \pm 1 = \delta,\ \delta^{\frac{1}{2}} = \pm 2.$$

Тоді

$$a = \delta a \cdot a^{\frac{q-1}{4}} = \delta \cdot a^{\frac{q+3}{4}} \Rightarrow y = \delta^{\frac{1}{2}} \cdot a^{\frac{q+3}{8}}.$$

Для поля характеристики 7: $q = 7^{127} \equiv 3 \bmod 4$.

Аналогічно, оскільки $a = y^2$ – квадратичний лишок, маємо:

$$a^{\frac{q-1}{2}} = 1,\ a^{\frac{q-1}{2}} a = a^{\frac{q+1}{2}} = a,\ \Rightarrow\ y = a^{\frac{q+1}{4}}.$$

Таким чином отримаємо пару (x, y), що задовольняє рівності $x^2 + y^2 = 1 + 3x^2y^2$, значить точка $Q = (x, y)$ належить до кривої Едвардса. Помноживши Q на величину n з таблиці1, можемо отримати точку нуль $O = (0, 1)$, точку $D = (0, -1)$ другого порядку або точки $\pm P$ четвертого порядку. В першому випадку генератором G підгрупи точок кривої Едвардса буде власне точка $G = Q = (x, y)$, в інших – генератор G визначається як $G = 2Q$ або $G = 4Q$ відповідно. Результати обчислень, а саме, примітивні поліноми та генератори підгрупи точок кривої $x^2 + y^2 = 1 + 3x^2y^2$ для відповідних полів, наведені в таблицях 2–4 (молодші степені векторів – зліва).

ВИСНОВКИ

З практичної точки зору питання щодо реальних оцінок швидкодії криптосистеми на кривій Едвардса над розширеннями малих полів залишається відкритим. Однак теоретичні дослідження дозволяють стверджувати, що параметри, надані в таблицях 2–4, забезпечать максимальну продуктивність криптосистеми при заданій стійкості.

Отримані параметри можна розглядати як еквівалентні відносно продуктивності при однаковому рівні стійкості системи. Виключення складає випадок поля F_7^{127}: для цього поля знайдено два примітивних поліноми ваги 3,тому відповідна арифметика поля є більш прийнятною порівняно з арифметикою, що побудована відповідно до поліномів більшої ваги. Незначна втрата стійкості [6] криптосистеми на кривій Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полями F_5^{181}, F_5^{227} та F_7^{127}, складає 4 біта в кожному з трьох випадків та є незначною порівняно з величинами відповідних полів у бітах.

У цілому вважаємо, що отримані параметри можна рекомендувати в ході побудови продуктивних криптосистем та розробки проектів майбутніх стандартів та протоколів.

Література

[1] Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.

[2] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1–20.

Таблиця 2

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_5^{181}

P(z) = $z^{181} + z^3 + z^2 + 3z + 3$ *x*=[020142034310022224101012221304140301432203243032241124434204012141101011240333421403412430442412314131110013401212233320143114004323232130032424012224444043224043044333224012421344 3] *y*=[332430012113102123101022332221434201344433301244110443241322234411431010032114420334344112412432431021014432304242413441103201032141100413114111433042433133303044101341124422443002304]
P(z) = $z^{181} + z^3 + 4z^2 + 3z + 2$ *x*=[003221341120100121431033232411403230122241311323210244242401303214311143302311010034314220313344043333222032223222444424114233140304204112240344421344401313430043340203404013033302433] *y*=[030430204201141033440121201004420123233110441401320234130413132430332314112324002304112100120314202043203010241004311331222434423031243233323200023131134221110113111233041334110303]
P(z) = $z^{181} + 2z^4 + z^3 + 2z^2 + 2$ *x*=[220040230041043404420133412422133002214421300102100213000014342404203433130301411043301443334133403430243214003433214402340413103210401232142442030124341024334330424232440120113002] *y*=[324300134424422004304443143011323210214220110204230003303304332200424212313420321244233112204111100321304111301221304220240310204210400144112114132110343442043222324113020213312223 2]
P(z) = $z^{181} + 3z^4 + z^3 + 3z^2 + 3$ *x*=[011433204102241024431323333143404030230302121104140032234130212203213312414310110320022334001221240441441134200322420423343020343343324131140104122114122431314220110124242443242042] *y*=[311413314004400102434442214401411431222410402332322421104120144303241334020333042402231213312011432423300213000033211313020000223144030224120300414144421111040002243104234311144333 1]
P(z) = $z^{181} + z^5 + z^3 + 2z + 2$ *x*=[230131240411444014004331023430112230122412200032422443331243043210341234231422340233444040231120021144303304300324121313201024243440011311440201424314041042203010202041413442203 44] *y*=[033434123041431141422433401103404123342044233133442343442443223324403133423141434011003012441433334023221141034212344144400334121032240203210003304242103013330244110134334240110411 2]
P(z) = $z^{181} + z^5 + z^3 + 2z + 3$ *x*=[033331143444211324403301130103313221202030422040211300031102241223241112323041432130114324303210400034023343134041203141411102033013423121332040144331022011214142131032100202332 33] *y*=[224433021012423102133424420211322011420114010032223220143234001020013040323402413104011423002000431000143241344412311141324132443100130433141322430110132124031133311233110111321222 2]
P(z) = $z^{181} + z^5 + 2z^4 + 3z^3 + 2$ x=[401313203242141100414140341402132031340204211010304301304433000241303202204322333210310143001114430042433302110323403441142111010403133420102301120222303041212423022004240014014144 2] y=[233004302440242400114114043112223221431440010340210110330414113414342233432443313200244201210031432134431420414013303432040211000102400144423003012304204124411022242214442113402104 2]
P(z) = $z^{181} + z^5 + 3z^4 + 3z^3 + 3$ *x*=[430231143030042104122442004211031442233231212331100100323003341201344433331120310002101312011223223204122134310412131024210020010344000212342212231041402210200331004344113222024213] *y*=[220214013224431013231414442230343012344044044401130023141411412230431411443324442143420222112422320020233343333111224420014110214141313101211024203211233332014432024110101244422032]
P(z) = $z^{181} + 2z^5 + 2z^3 + 4z + 2$ *x*=[213303120043101410430241413000223042401423430440104441233234204013241021021410012212131113130013010300034431014044244234032001424420410222124313100214302032044141310412102201011224] *y*=[333342223403012114404422142010023210021141130430442302023204431414313444410321233000203120022141222334233342304003212003112104210341331403421343332031320420414242343223111134313142 4]
P(z) = $z^{181} + 2z^5 + 2z^3 + 4z + 3$ *x*=[041004310220124400010323000323444403432134210112041043030341412422420242102402133113211112200032214301020314430023124230400401241320121003143044221313232340414001111113200242424002 4] *y*=[103300132311434420343104341031424340043124401420403234203202244214313030440040144030112014201104040324134020031111201004020110110010132221100403014044244244444304122341310121023030 02]

Таблиця 3

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем F_5^{277}

P(z) = $z^{227} + z^3 + 2z^2 + z + 2$ *x*=[200434204200342242421132330113311033122431404333242244010231330340440143341310142343240422122201214402222123002202403002134144100032233014232144123313204242302143241432122113134024422102010113012333310234243412410301100 10244112] *y*=[143314021300210304111310442344114031131013143133441204112044300113411410202331023320443333224142334442403242311333313133304320431140021013242301132431231300041404210042241140132201331324024442100212031201421440342020413 00112124]
P(z) = $z^{227} + z^3 + 3z^2 + z + 3$ *x*=[320221201114411222324310314021323031404042223141002332301313302110244332031130143141303444041130332024410412 2112124013232240022103421404113442144044230413324232024103443241442331014202303401043230341031433334412311032413 3014444] *y*=[001120210000330303040420144233441044014422043244201001232342113432204102340213022403420240434030113014040240 1133341212021323300414322143310300223222304313024443401212311042303131101220244224230313201403111311112343424220 20044441]

$P(z) = z^{227} + z^4 + 2z^2 + z + 2$ x=[00130341131312012421212040140240313014202340431420010044200313404102301334141242324123210333142033414113314031314413000113222221440212004022430131433321234031143331414443402413000302044033411121214340141423243302210011112410233] y=[00314323301034220420433200330304332423230043240411103020101034122314222141341104433434122243404422030404334223334303034040424401041124242344400104324232112301300142220320443040141332230222013431233200332300420214144122220040011]
$P(z) = z^{227} + 2z^4 + 4z^3 + 2z + 3$ x=[04143040131323211331302033023204443224124423021343210341003414444033213324434332221104012340233034200120441212232122404211210033411123013102023002023120343430143204313011133221134001430444231340213300421434310222012014001304312] y=[42230343300243410212030123020242100011302124303210440141002443241020441144112034004242310442233112340411042343130421314112244031221111113214212420111422144013404042341302424143014134400303140332312122304404124120142141042421121]
$P(z) = z^{227} + 3z^4 + 4z^3 + 2z + 2$ x=[42431120100132410101402123140402300013433034141124410421142232234430434120401121023214001134341202002213410434423032400123012013430200241103103223122442420240324142044104100240004233131420424303114010414324324130040420431221312] y=[23232102342014112231203433413112230330443100403233204023040124003030212110124431223141434223110141130003014112014223414410344240443220114242140311242030003020022043303103223344013230202242002334432013101442113041341131031430241]
$P(z) = z^{227} + 4z^4 + 3z^2 + z + 3$ x=[24303342131044231204240342011032222001302212422341124300210304133423242121230234243044432440011442411134133222320440240412311313044320002023232102241443012142241224120334231443021114444001103101414044000330333300223133121322424401] y=[40102210133011344034021002421020034141420303101421331324144221410320010321143014134030033032023410234330304043201320120331223210303032224341221323003143110234311212444143243044203323123423114230014324124313042224402203031310 1]
$P(z) = z^{227} + z^6 + 2z^3 + 3z + 2$ x=[41343412343120121333342000313130332230423131402141143200010243111304221133241011324424303433302322122022133330013424344010021424442231123133242042124241242443220044410131214232130224333204101014144141323112113143340440320304] y=[42341340241244422300440440242221330212001312412041114221331204134443000440111002000141312344244104034224311222404020431110333441012014033401031100020212130201021122122401244121014312434301430040141131032043411000444241002004334]
$P(z) = z^{227} + z^6 + 3z^3 + z + 3$ x=[13400344332022344142410331300231134012343032440040214210314334144342412302243033102032000413012112033000441311241321003432332023102404143423331401224000000004034103413012121121022041011430241031402142103120443432423412343041442 2] y=[02103340414110114412303311341210031003243303104322111303243324030244003103023104232420221234332223111020343134121220432022130433000121203432010320110330301331233132010120324403142341310220200300141314144212422121234042041232021]
$P(z) = z^{227} + 2z^6 + z^4 + 2z^2 + 2$ x=[32430432204441144130401211141034021102003130444001114011304301313433441123000142403411000400241433323230400134043303013343004030211413131231430001030022322410141340242404322113122423244222040423221042213312140403221123420220143] y=[10420433333004020211302010113111131024121232430033304242243030003102014401040010430212034430124413432331321310232423322241243123140220131422102112422100014203040212131300001014434224221141411234112422113200341203313003133043313]
$P(z) = z^{227} + 2z^6 + 3z^4 + 4z^2 + 3$ x=[02124203121121324411200224140411102320211132444243110341144403332421234003140123120411042423013102433344041411420133023011103223400200431141020403033114412130332424342132443301332100234223114013114320024111430010043412323030441] y=[43424210212234423234101402131204120131221240003311022232424130102024343134034323320333441003124123322112410 2012302120210033344401142332300004344211034012233004204031041232212044304430023011210422224300313433044030201434202140 2]

Таблиця 4

Крива Едвардса $x^2 + y^2 = 1 + 3x^2y^2$ над полем $F_7{}^{127}$

$P(z) = z^{127} + 3z^2 + 2$ x=[46044006603145305201405123204222530031016222516201005661204244422522523363324113266525222005454623240563146654441612464210212622] y=[13151463044055366051631435240114440055064050055036454015644623565455240161623205625064212024436215201514620643652053153153046 04]
$P(z) = z^{127} + 5z^2 + 4$ x=[03655433365210564341154620351326454535151161013652330566553051162552456414405421111444536306551655040562536036133666510226532136] y=[13205354620266042601015444262135612041153411156022203232033334332456261531212132660656611400600631511244133355062142313264524 65]
$P(z) = z^{127} + 2z^2 + 2z + 4$ x=[64663156522464360424613322621061264325155146612546650340165526460656260605330601001241524365532112242546361653423243663533105 33]
y=[05423004534624634645144346564106464142151303115465555340552214514542542415513632050154600544522051154153431552254401341 6]

$P(z) = z^{127} + 4z^2 + 2z + 2$ x=[156036134334532014564403432461341616623261162625645626110654136116401500643545203224414354302031524052223361061603162304503464 6] y=[225651365154041032143546141001026204244326102044342215055265206316101201033041310341355324424250211600206356043453306053213245]
$P(z) = z^{127} + 2z^3 + 6z^2 + 2$ x=[510232400251512003015131465556251123335143134253126154046246333635444641124021432311045466445624116331516646433452526221032242 2] y=[314546003640022304353165222000356536306533263361055343302601643622336405351324050122611535522560114361501505141233060455355555305]
$P(z) = z^{127} + 4z^3 + 3z^2 + 4$ x=[032104460221551530616360444453465435545665322340211542662646430065534316213363304523543423304163211302330065104135163465126042 1] y=[643004566234311166623635400353406535235400160150044555651513462330355264665540264160105564053203333363313136064113103645665611 3]
$P(z) = z^{127} + 3z^5 + 2z^2 + 4$ x=[360554063253063002002062140020353366635121004451151221431264632043325236211316313312131064046010503011264510662402135401436311 6] y=[502334232404301404025500036021355020350553350330566212632040005330062002331604551532526031661063104051361050150236622362112661 6]
$P(z) = z^{127} + 6z^5 + 4z^2 + 2$ x=[263536326365544262432531352065003352434164663011216645330110565464143210235525622154142303024501161450602100416105443561563056 2] y=[406432032231634653246024514250335146034624533454121205465461245335003004365653411544013653656556131646645012205146262300316223 3]

[3] Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, № 4, 2011. – С. 33–36.

[4] Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника, вып. 167, 2011. – С. 203–208.

[5] Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей // Прикладная радиоэлектроника, 2012, Том 11, № 2. – С. 225–227.

[6] Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Оценка реальной стойкости криптосистемы на кривой Едвардса нарасширениями малых полей. Сучасний захист інформації, №2, 2012. – С. 17–20.

[7] Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб.пособие. – К.: ІВЦ «Політехніка», 2004. – 224 с.

Надійшла до редколегії 29.03.2013

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри ММЗІ ФТІ НТУУ «КПІ». Наукові інтереси: криптографія, теорія коригуючого кодування.

Діхтенко Аліса Анатоліївна, аспірант кафедри теорії пружності та обчислювальної математики Донецького національного університету. Наукові інтереси: асиметрична криптографія.

Яценко Олександр Іванович, консорціум ЄДАПС, КП ОТІ, системний програміст відділу криптографічного захисту інформації. Наукові інтереси: криптографія, теорія алгоритмів, програмування.

УДК 681.3.06

Параметры криптосистемы на кривой Едвардса над расширениями малых простых полей / А.В. Бессалов, А.А. Дихтенко, О.И. Яценко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 273–277.

Рассмотрена возможность совершенствования криптосистем на эллиптических кривых на базе кривых, представленных в форме Эдвардса. Описан подход для вычисления общесистемных параметров криптосистемы на кривой Эдвардса над расширениями полей F_5 и F_7. Получено 28 наборов параметров, которые удовлетворяют стандартным криптографическим требованиям и могут быть рекомендованы в будущих стандартах.

Ключевые слова: эллиптическая кривая, форма Эдвардса, расширеное поле, порядок кривой.

Табл.: 4. Библиогр.: 7 назв.

UDC 681.3.06

Parameters of cryptosystems on the Edwards curve above expansions of small simple fields / A.V. Bessalov, A.A. Dihtenko, O.I. Yatsenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 273–277.

The improvement possibility of elliptic curve cryptosystems on the basis of the Edwards curves is considered. An approach for evaluating Edwards's curve system-wide-parametres over F_5 and F_7 ffield expansions is described. 28 sets of parametres which satisfy standard cryptographic requirements are obtained. They can be recommended in future standards.

Keywords: elliptic curve, Edwards form, field extension, curve order.

Tab.: 4. Ref.:7 items.

УДК 681.3.06

ДЕЛЕНИЕ ТОЧКИ НА ДВА ДЛЯ КРИВОЙ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

А.В. БЕССАЛОВ

Дано решение обратной удвоению задачи деления точки на два для эллиптических кривых, представленных в форме Эдвардса. Получены оценки сложности операции деления на два в сравнении с удвоением точки. Рассмотрено одно из приложений свойств делимости точки на два для определения порядка точки в криптосистеме.

Ключевые слова: эллиптическая кривая, форма Эдвардса, удвоение точки, деление точки на два.

ВВЕДЕНИЕ

Наряду с классической групповой операцией удвоения точки эллиптической кривой в задачах криптоанализа и экспоненцирования точек может бать полезным решение обратной задачи: при известных координатах точки 2P найти координаты точки P. Для несуперсингулярных кривых над полями характеристики 2 такая задача рассматривалась в [1]. Замечательным свойством операции деления здесь оказалась предельная простота групповой операции, сводящаяся в одном из приложений к одной операции умножения в поле. Последовательное выполнение операции деления на два практически на порядок ускоряет вычисления.

В данной статье приведено решение обратной удвоению задачи для перспективного класса кривых Эдвардса [2, 3] над простым полем $\mathbf{F}_p$ порядка $p > 2$. Определены условия существования и координаты двух точек деления на два, даны оценки сложности групповой операции в сравнении с операцией удвоения. Рассмотрены приложения операции деления для нахождения порядка случайной точки кривой.

1. ВЫЧИСЛЕНИЕ КООРДИНАТ ТОЧЕК ДЕЛЕНИЯ НА ДВА

Пусть $P = (x_1, y_1)$ и $2P = (a,b)$. Согласно закону удвоения точки кривой Эдвардса

$$E_{ED} : x^2 + y^2 = 1 + dx^2y^2 \qquad (1)$$

с параметром $d \neq c^2$ [2, 3] имеем

$$2P = 2(x_1, y_1) = \left(\frac{2x_1y_1}{1 + \tilde{d}x_1^{\,2}y_1^{\,2}}, \frac{y_1^{\,2} - x_1^{\,2}}{1 - \tilde{d}x_1^{\,2}y_1^{\,2}} \right) = (a,b). \qquad (2)$$

Обозначим $X = x_1^{\,2}$, $Y = y_1^{\,2}$, $Z = X + Y$. Заменим знаменатели в (2) на $X + Y$ и $2 - X - Y$ соответственно. Возводя первую координату в (2) в квадрат и умножая результат на d, можно получить квадратное уравнение

$$z^2 - \frac{4}{da^2}z + \frac{4}{da^2} = 0$$

с двумя решениями

$$z_{1,2} = \frac{2}{da^2}\left(1 \pm \sqrt{1 - da^2}\right). \qquad (3)$$

Необходимым условием существования точек деления на 2 является то, что дискриминант $1\text{-}da^2 = A^2$ является квадратичным вычетом поля F_p. В противном случае для некоторой случайной точки точек деления на 2 не существует.

Из равенства для второй координаты в (2) с учетом введенных обозначений получим систему уравнений

$$(b\text{-}1)X + (b+1)Y = 2b, \qquad (4)$$
$$X + Y = z_{1,2}.$$

Отсюда

$$X(b) = \frac{1+b}{2}z_{1,2} - b,$$
$$Y(b) = \frac{1-b}{2}z_{1,2} + b = X(-b). \qquad (5)$$

Здесь выбор одного из решений z_1 или z_2 определяется тем, что значения (5) должны быть квадратами в поле F_p. Значения координат точек деления на два вычисляются извлечением квадратных корней из (5).

При выполнении условия существования точек деления получим две точки $P = (x_1, y_1)$ и $P^* = (-x_1, -y_1)$, которые связаны как $P^* = P + D$, где $D = (0, -1)$ – точка 2-го порядка. При этом, очевидно, $2P = 2P^*$, т. к. $2D = O = (0, 1)$ – нуль группы точек кривой Эдвардса. Заметим также, что порядки точек P^* и P отличаются в 2 раза.

В качестве примера рассмотрим кривую $x^2 + y^2 = 1 + 8x^2y^2 \bmod 13$, которая имеет порядок $N_E = 12$. Пусть $P = (3, 6)$, тогда согласно (2) $2P = (6, 3)$, т.е. $a = 6$, $b = 3$. Ясно, что дискриминант в (3) $1 - da^2 = 12 = 25 \bmod 13$, является квадратичным вычетом, так что $z_{1,2} = 1 \pm 5 = \{6, 9\}$. Из (5) при выборе $z_1 = 6$ получим квадратичные вычеты $X = 9$, $Y = 10$ (выбор $z_2 = 9$ дает невычеты). Извлекая квадратные корни, получаем две точки деления на 2: $P = (3, 6)$ и $P^* = (-3, -6) = P + D$. Другие две точки $(-3, 6)$ и $(3, -6)$, обратные точкам P и P^*, не проходят проверку удвоением, которая дает точку $-2P$. Для этого достаточно вычислить лишь первую координату точки $-2P$, равную $-a$.

2. ОЦЕНКА СЛОЖНОСТИ УДВОЕНИЯ И ДЕЛЕНИЯ ТОЧКИ НА ДВА В АФФИННЫХ КООРДИНАТАХ

Пусть M, S, I, R – полевые операции умножения, возведения в квадрат, инверсии и

извлечения квадратного корня. Игнорируя простые операции сложения и вычитания, из (2) после замены знаменателей на $x_1^2 + y_1^2$ и $2 - x_1^2 - y_1^2$ соответственно получим оценку сложности удвоения точки

$$\mathrm{DUBBL} = 2I + M + 2S.$$

Процедура вычисления двух точек деления на 2 согласно (3) – (5) имеет трудоемкость не менее

$$\mathrm{DIV} = I + 4M + S + 3R.$$

Если принять I = 10M, S = 0.7M, R = 4M, DUBBL = 22.4M, DIV = 26.7M, т.е следует ожидать более высоких вычислительных затрат при делении точки на два по сравнению с удвоением. При вычислении скалярного произведения точки эта операция, скорее всего, не дает положительного эффекта (как это имеет место для полей характеристики 2). Вместе с тем эта операция может оказаться полезной при нахождении порядка случайной точки и генератора криптосистемы. Это обсуждается в следующем параграфе.

3. УСЛОВИЕ ДЕЛЕНИЯ ТОЧКИ НА ДВА ДЛЯ ОПРЕДЕЛЕНИЯ ПОРЯДКА СЛУЧАЙНОЙ ТОЧКИ КРИВОЙ ЭДВАРДСА

В криптографических приложениях наиболее приемлемыми являются кривые Эдвардса с минимальным кофактором 4 порядка кривой $N_E = 4n$, где n – достаточно большое простое число. Если порядок генератора P кривой E_{ED} равен $\mathrm{Ord}P = 4n$, то генератор криптосистемы $G = 4P$ имеет порядок $\mathrm{Ord}G = n$. Любая кривая содержит нуль группы O = (0, 1), точку $D = (0, -1)$ второго порядка и точки $\pm Q = (\pm 1, 0)$ четвертого порядка. Точки 8-го порядка отсутствуют, поэтому $(1 - d)$ – квадратичный невычет [3].

Утверждение 1. На кривой Эдвардса порядка $4n$ не существует точек деления на 2 для точек $< P >$ максимального порядка и точек Q четвертого порядка, и существуют – для всех других точек кривой.

Доказательство. Каждой точке kP кривой отвечает скалярный множитель k как элемент кольца целых чисел Z_N операциями по модулю $N_E = 4n$. Все нечетные элементы кольца, которым соответствуют точки кривой максимального порядка $4n$ и порядка 4, не делятся на 2 в кольце Z_N. С другой стороны, все четные элементы $k = 2s$ при делении на два по модулю N_E дают два значения s и $s + N_E/2$, удвоение которых дает вновь $k = 2s$. Возвращаясь к точкам kP кривой, заключаем, что утверждение 1 доказано.

На кривой E_{ED} приблизительно половина всех точек имеет максимальный порядок $4n$, четверть точек – порядок $2n$, и четверть точек – порядок n. При выборе случайной точки как точки $T = (a, b)$ максимального порядка получим в результате тестирования, что $(1 - da^2)$ является невычетом в поле $\mathbf{F}_p$, после чего генератор криптосистемы определяется как $G = 4T$. Если же $(1 - da^2)$ является квадратичным вычетом в поле $\mathbf{F}_p$, то порядок точки T равен $2n$ или n. Удвоение любой из таких точек даст точку G порядка n.

Литература

[1] Бессалов А.В. Метод решения проблемы дискретного логарифмирования на эллиптических кривых путем деления точек на два // Кибернетика и системный анализ, №6, 2001. – С. 50–53.

[2] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007. – PP. 1–20.

[3] Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. – С. 203–208.

Поступила в редколлегию 09.04.2013

Бессалов Анатолий Владимирович, фото и сведения об авторе см. на стр. 277.

УДК 681.3.06

Ділення точки на два для кривої Едвардса над простим полем / Бессалов А.В. // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 278–279.

Дано розв'язок оберненої до здвоєння задачі ділення точки на два для еліптичних кривих, які подані у формі Едвардса. Отримано оцінки складності операції ділення на два в порівнянні зі здвоєнням точки. Розглянуто один з додатків властивостей ділення точки на два для визначення порядку точки у криптосистемі.

Ключові слова: еліптична крива, форма Едвардса, здвоєння точки, ділення точки на два.

Бібліогр.: 3 найм.

UDC 681.3.06

Dividing a point by two for the Edwards curve over a simple field / Bessalov A.V. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 278–279.

The solution of an inverse to doubling point-halving problem for elliptic Edwards curves is given. Estimations of complexity of a point-halving operation in comparison with point-doubling are obtained. One of the applications of properties of a point-halving divisibility to define a point order in a cryptosystem is considered.

Keywords: elliptic curve, Edwards form, point doubling, point halving.

Ref.: 3 items.

УДК 004.056.55

АНАЛІЗ СКЛАДНОСТІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК ЕК ЗАЛЕЖНО ВІД ОБРАНОГО БАЗИСУ

М.В. ЄСІНА, І.Д. ГОРБЕНКО

Розглядаються існуючі базиси представлень еліптичних кривих та їх використання під час виконання операцій у групах точок еліптичних кривих, а також швидкісні характеристики. Формуються пропозиції щодо використання базисів перетворень.

Ключові слова: базис, координати, криптографічні перетворення, складність.

Точки в групах точок ЕК можуть бути подані у декількох координатних базисах. Основними з них є: афінні координати, проективні координати, якобіанові координати, координати Чудновського (Chudnovsky Jacobian) та модифіковані якобіанові координати [6].

Рівняння ЕК над полем F_p дозволяє використовувати 5 найбільш відомих базисів, відомо також 3 базиси подання точок на ЕК над розширеним полем.

Змішані координати мають перевагу, яку легше побачити за наявності великої кількості базисів подання точок на ЕК. Тому з метою проведення подальшого порівняльного аналізу та вибору найбільш привабливих розглядатимемо більш детально базиси подання точок на ЕК над полем F_q.

Для подальшого порівняння складності операцій додавання та подвоєння визначимо змінні, які позначатимуть відповідні дії під час виконання операцій додавання та подвоєння точок: $t(B+B)$ та $t(2B)$ – додавання та подвоєння точок відповідно, B – координатний базис [5,6]; складність операцій додавання та подвоєння точок на кривій зазвичай виражається у:

– кількості множень – (M)
– піднесеннях до квадрата – (S)
– інверсіях – (I)

Операція додавання може ігноруватися в силу незначної складності [1, 2].

1. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В АФІННОМУ ПОДАННІ

Нехай рівняння еліптичної кривої E над F_p має вигляд (1).

$$E: y^2 = x^3 + ax + b\left(a,b \in F_p, 4a^3 + 27b^2 \neq 0\right). \quad (1)$$

Нехай також є точки $P_1 = (x_1, y_1) \in E\left(F_p\right)$ та $P_2 = (x_2, y_2) \in E\left(F_p\right)$. Тоді сумою двох точок P_1 та P_2 називається точка $P_3 \in E\left(F_p\right)$, така що $P_3 = P_1 + P_2 = (x_3, y_3)$. Якщо $P_1 \neq P_2$, то координати точки $P_3 = (x_3, y_3) = P_1 + P_2 = (x_1, y_1) + (x_2, y_2)$ визначаються з використанням формули (2) [4]

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \pmod p, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \pmod p, \end{aligned} \quad (2)$$

де $\lambda = (y_2 - y_1)/(x_2 - x_1) \pmod p$.

Якщо $P_1 = P_2$, то операцію $P_1 + P_2$ називають подвоєнням і вона обчислюється як $P_3 = (x_3, y_3) = 2P_1 = 2(x_1, y_1)$, причому [4]

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \pmod p, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \pmod p, \end{aligned} \quad (3)$$

де $\lambda = \left(3x_1^2 + a\right)/(2y_1) \pmod p$.

2. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ПРОЕКТИВНОМУ ПОДАННІ

Для проективних координат $x = X/Z$ та $y = Y/Z$, тому рівняння ЕК над F_p має вигляд (4).

$$E_P: Y^2 Z = X^3 + aXZ^2 + bZ^3 \pmod p. \quad (4)$$

Нехай є точки $P_1 = (X_1, Y_1, Z_1) \in E_P\left(F_p\right)$ та $P_2 = (X_2, Y_2, Z_2) \in E_P\left(F_p\right)$, тоді сумою двох точок P_1 та P_2 називається точка $P_3 \in E_P\left(F_p\right)$ така, що $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3)$. Якщо $P_1 \neq P_2$, то координати точки $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2 = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$ обчислюються як в [6]

$$\begin{aligned} X_3 &= vA \pmod p, \\ Y_3 &= u\left(v^2 X_1 Z_2 - A\right) - v^3 Y_1 Z_2 \pmod p, \\ Z_3 &= v^3 Z_1 Z_2 \pmod p \end{aligned} \quad (5)$$

де $u = Y_2 Z_1 - Y_1 Z_2 \pmod p$; $v = X_2 Z_1 - X_1 Z_2 \pmod p$; $A = u^2 Z_1 Z_2 - v^3 - 2v^2 X_1 Z_2 \pmod p$.

Якщо $P_1 = P_2$, то операцію $P_1 + P_2$ називають подвоєнням $P_3 = (X_3, Y_3, Z_3) = 2P_1 = 2(X_1, Y_1, Z_1)$, причому [5]

$$\begin{aligned} X_3 &= 2hs \pmod p, \\ Y_3 &= w(4B - h) - 8Y_1^2 s^2 \pmod p, \\ Z_3 &= 8s^3 \pmod p \end{aligned} \quad (6)$$

де $w = aZ_1^2 + 3X_1^2 \pmod p$; $s = Y_1 Z_1 \pmod p$; $B = X_1 Y_1 s \pmod p$; $h = w^2 - 8B \pmod p$.

3. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ЯКОБІАНОВИХ КООРДИНАТАХ

Для якобіанових координат $x = X/Z^2$ та $y = Y/Z^3$, тому рівняння ЕК над F_p має вигляд:

$$E_J: Y^2 = X^3 + aXZ^4 + bZ^6 \pmod p. \quad (7)$$

Нехай є точки $P_1=(X_1,Y_1,Z_1)\in E_J(F_p)$ та $P_2=(X_2,Y_2,Z_2)\in E_J(F_p)$, тоді сумою двох точок P_1 та P_2 називається точка $P_3\in E_J(F_p)$ така, що $P_3=P_1+P_2=(X_3,Y_3,Z_3)$. Якщо $P_1\neq P_2$, то координати точки $P_3=(X_3,Y_3,Z_3)=P_1+P_2=(X_1,Y_1,Z_1)+(X_2,Y_2,Z_2)$ обчислюються за правилом [5].

$$\begin{aligned}&X_3=-H^3-2U_1H^2+r^2\,(\mathrm{mod}\,p),\\&Y_3=-S_1H^3+r\left(U_1H^2-X_3\right)(\mathrm{mod}\,p),\\&Z_3=Z_1Z_2H\,(\mathrm{mod}\,p)\end{aligned}\qquad(8)$$

де $U_1=X_1Z_2^2\,(\mathrm{mod}\,p)$, $U_2=X_2Z_1^2\,(\mathrm{mod}\,p)$, $S_1=Y_1Z_2^3\,(\mathrm{mod}\,p)$, $S_2=Y_2Z_1^3\,(\mathrm{mod}\,p)$, $H=U_2-U_1\,(\mathrm{mod}\,p)$, $r=S_2-S_1\,(\mathrm{mod}\,p)$.

Якщо $P_1=P_2$, то операцію P_1+P_2 називають подвоєнням і $P_3=(X_3,Y_3,Z_3)=2P_1=2(X_1,Y_1,Z_1)$, причому

$$\begin{aligned}&X_3=T\,(\mathrm{mod}\,p),\\&Y_3=-8Y_1^4+M(S-T)(\mathrm{mod}\,p),\\&Z_3=2Y_1Z_1\,(\mathrm{mod}\,p)\end{aligned}\qquad(9)$$

де $S=4X_1Y_1^2\,(\mathrm{mod}\,p)$; $M=3X_1^2+aZ_1^4\,(\mathrm{mod}\,p)$; $T=-2S+M^2\,(\mathrm{mod}\,p)$.

4. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В КООРДИНАТАХ ЧУДНОВСЬКОГО

Для координат Чудновського $x=X/Z^2$ та $y=Y/Z^3$, тому рівняння ЕК над F_p має вигляд

$$E_{J^c}:Y^2=X^3+aXZ^4+bZ^6\,(\mathrm{mod}\,p),\qquad(10)$$

тобто співпадає з (7).

Нехай є точки $P_1=\left(X_1,Y_1,Z_1,Z_1^2,Z_1^3\right)\in E_{J^c}(F_p)$ та $P_2=\left(X_2,Y_2,Z_2,Z_2^2,Z_2^3\right)\in E_{J^c}(F_p)$, тоді сумою двох точок P_1 та P_2, називається точка $P_3\in E_{J^c}(F_p)$ така, що $P_3=P_1+P_2=\left(X_3,Y_3,Z_3,Z_3^2,Z_3^3\right)$. Якщо $P_1\neq P_2$, то координати точки

$$\begin{aligned}&P_3=\left(X_3,Y_3,Z_3,Z_3^2,Z_3^3\right)=P_1+P_2=\\&=\left(X_1,Y_1,Z_1,Z_1^2,Z_1^3\right)+\left(X_2,Y_2,Z_2,Z_2^2,Z_2^3\right)\end{aligned}$$

формуються так [6]:

$$\begin{aligned}&X_3=-H^3-2U_1H^2+r^2\,(\mathrm{mod}\,p),\\&Y_3=-S_1H^3+r\left(U_1H^2-X_3\right)(\mathrm{mod}\,p),\\&Z_3=Z_1Z_2H\,(\mathrm{mod}\,p),\\&Z_3^2=Z_3^2\,(\mathrm{mod}\,p),\\&Z_3^3=Z_3^3\,(\mathrm{mod}\,p),\end{aligned}\qquad(11)$$

де $U_1=X_1\left(Z_2^2\right)(\mathrm{mod}\,p)$; $U_2=X_2\left(Z_1^2\right)(\mathrm{mod}\,p)$; $S_1=Y_1\left(Z_2^3\right)(\mathrm{mod}\,p)$; $S_2=Y_2\left(Z_1^3\right)(\mathrm{mod}\,p)$; $H=U_2-U_1\,(\mathrm{mod}\,p)$; $r=S_2-S_1\,(\mathrm{mod}\,p)$.

Якщо $P_1=P_2$, то операцію P_1+P_2 називають подвоєнням і $P_3=\left(X_3,Y_3,Z_3,Z_3^2,Z_3^3\right)=2P_1=2\left(X_1,Y_1,Z_1,Z_1^2,Z_1^3\right)$, причому:

$$\begin{aligned}&X_3=T\,(\mathrm{mod}\,p),Y_3=-8Y_1^4+M(S-T)(\mathrm{mod}\,p),\\&Z_3=2Y_1Z_1\,(\mathrm{mod}\,p),Z_3^2=Z_3^2\,(\mathrm{mod}\,p),\\&Z_3^3=Z_3^3\,(\mathrm{mod}\,p),\end{aligned}\qquad(12)$$

де $S=4X_1Y_1^2\,(\mathrm{mod}\,p)$; $M=3X_1^2+a\left(Z_1^2\right)^2\,(\mathrm{mod}\,p)$; $T=-2S+M^2\,(\mathrm{mod}\,p)$.

5. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ У МОДИФІКОВАНИХ ЯКОБІАНОВИХ КООРДИНАТАХ

Для модифікованих якобіанових координат $x=X/Z^2$ та $y=Y/Z^3$, рівняння ЕК має вигляд

$$E_{J^m}:Y^2=X^3+aXZ^4+bZ^6\,(\mathrm{mod}\,p),\qquad(13)$$

тобто співпадає з (7, 10).

Нехай є дві точки $P_1=\left(X_1,Y_1,Z_1,aZ_1^4\right)\in E_{J^m}(F_p)$ та $P_2=\left(X_2,Y_2,Z_2,aZ_2^4\right)\in E_{J^m}(F_p)$, тоді сумою двох точок P_1 та P_2 називається точка $P_3\in E_{J^m}(F_p)$ така, що $P_3=P_1+P_2=\left(X_3,Y_3,Z_3,aZ_3^4\right)$.
Якщо $P_1\neq P_2$, то координати точки

$$\begin{aligned}&P_3=\left(X_3,Y_3,Z_3,aZ_3^4\right)=P_1+P_2=\\&=\left(X_1,Y_1,Z_1,aZ_1^4\right)+\left(X_2,Y_2,Z_2,aZ_2^4\right)\end{aligned}$$

формуються так [3]:

$$\begin{aligned}&X_3=-H^3-2U_1H^2+r^2\,(\mathrm{mod}\,p),\\&Y_3=-S_1H^3+r(U_1H^2-X_3)(\mathrm{mod}\,p),\\&Z_3=Z_1Z_2H\,(\mathrm{mod}\,p),aZ_3^4=aZ_3^4\,(\mathrm{mod}\,p),\end{aligned}\qquad(14)$$

де $U_1=X_1Z_2^2\,(\mathrm{mod}\,p)$; $U_2=X_2Z_1^2\,(\mathrm{mod}\,p)$; $S_1=Y_1Z_2^3\,(\mathrm{mod}\,p)$; $S_2=Y_2Z_1^3\,(\mathrm{mod}\,p)$; $H=U_2-U_1\,(\mathrm{mod}\,p)$; $r=S_2-S_1\,(\mathrm{mod}\,p)$.

Якщо $P_1=P_2$, то операцію P_1+P_2 називають подвоєнням та $P_3=\left(X_3,Y_3,Z_3,aZ_3^4\right)=2P_1=2\left(X_1,Y_1,Z_1,aZ_1^4\right)$, причому:

$$\begin{aligned}&X_3=T\,(\mathrm{mod}\,p),\\&Y_3=M(S-T)-U\,(\mathrm{mod}\,p),\\&Z_3=2Y_1Z_1\,(\mathrm{mod}\,p),\\&aZ_3^4=2U\left(aZ_1^4\right)(\mathrm{mod}\,p),\end{aligned}\qquad(15)$$

де $S=4X_1Y_1^2\,(\mathrm{mod}\,p)$, $U=8Y_1^4\,(\mathrm{mod}\,p)$, $M=3X_1^2+\left(aZ_1^4\right)(\mathrm{mod}\,p)$, $T=-2S+M^2\,(\mathrm{mod}\,p)$.

У таблиці 1 наведено основні співвідношення, які визначають складність перетворень у різних базисах.

Таблиця 1

Складність перетворення у різних базисах

Базис	Додавання
Афінний A	$t(A+A)=I+2M+S$
Проективний P	$t(P+P)=12M+2S$
Якобіанів J	$t(J+J)=12M+4S$
Чудновського J^C	$t(J^c+J^c)=11M+3S$
Модифікований Якобіанів J^m	$t(J^m+J^m)=13M+6S$
Базис	Подвоєння
Афінний A	$t(2A)=I+2M+2S$
Проективний P	$t(2P)=7M+5S$
Якобіанів J	$t(2J)=4M+6S$
Чудновського J^C	$t(2J^c)=5M+6S$
Модифікований Якобіанів J^m	$t(2J^m)=4M+4S$

У таблиці 2 наведено час, який затрачається на операцію складання та подвоєння у кожній системі координат.

Таблиця 2

Час, необхідний для виконання операції складання та подвоєння

Базис	$t(B+B)$	$t(2B)$
Афінний A	0.198 мс	0.209 мс
Проективний P	0.468 мс	0.245 мс
Якобіанів J	0.339 мс	0.186 мс
Чудновського J^C	0.260 мс	0.172 мс
Модифікований Якобіанів J^m	0.423 мс	0.137 мс

Як бачимо, на складання менше витрачається часу в афінному базисі, а на подвоєння – у модифікованому Якобіановому базисі. Найбільше часу на складання точок, а також на їх подвоєння потребує проективний базис. Тобто, якщо керуватися критерієм часу виконання операцій, то проективний базис можна відкинути як такий, що не задовольняє умову швидкодії.

У таблиці 3 наведено оцінку обчислювальної складності $t(X \to Y)$, необхідної для перетворення точки еліптичної кривої з однієї системи координат (X) до іншої (Y).

6. АНАЛІЗ СКЛАДНОСТІ КРИПТОПЕРЕТВОРЕНЬ ТА МОЖЛИВОСТІ ЇХ ЗМЕНШЕННЯ ЗА РАХУНОК КОМБІНАЦІЇ ПЕРЕТВОРЕНЬ У РІЗНИХ БАЗИСАХ

Просторова та часова складності криптоперетворень у групі точок еліптичних кривих залежать від базисів, що застосовуються при криптоперетвореннях, а також від конкретності реалізації криптопримітивів. Для кращої реалізації криптосистем необхідно мінімізувати складність перетворень за рахунок використання найкращого (можливо оптимального) базису.

Графіки складності додавання та подвоєння у групі точок ЕК в афінних та проективних координатах (в залежності від порядку розширеного поля m) наведені на рис. 1, 2 відповідно.

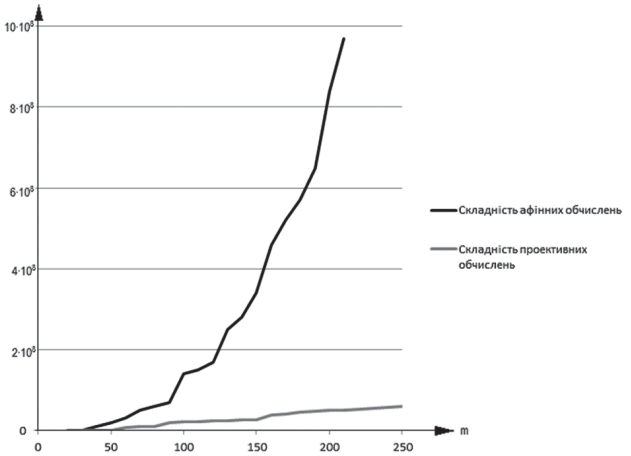


Рис. 1. Складність додавання у групі точок ЕК в афінних та проективних координатах

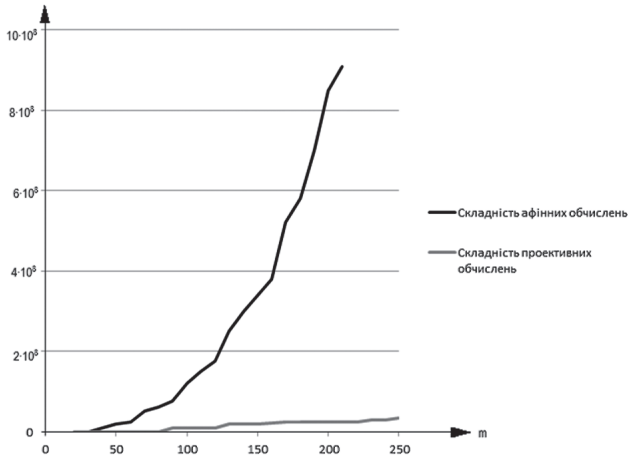


Рис. 2. Складність подвоєння у групі точок ЕК в афінних та проективних координатах

Таблиця 3

Оцінка обчислювальної складності

З/до	A	P	J	J^C	J^m
Афінний A	0	$2M$	$3M+S$	$3M+S$	$4M+2S$
Проективний P	$2M+I$	0	$2M+S$	$3M+S$	$3M+2S$
Якобіанів J	$3M+S+I$	$M+S+I$	0	$M+S$	$M+2S$
Чудновського J^C	$3M+S+I$	$M+S+I$	0	0	$M+S$
Модифікований Якобіанів J^m	$3M+S+I$	$M+S+I$	0	$M+S$	0

Складність додавання та подвоєння точок обчислена у числі тактів, необхідних для виконання операцій з довжиною чисел у m біт. Знаючи число тактів виконання операцій додавання та подвоєння, можна визначити час виконання кожної з операцій.

При додаванні та при подвоєнні складність обчислень більша в афінних координатах, а в проективних значно менше. Але водночас, проективні координати потребують більше часу на виконання операцій складання та подвоєння точок, ніж афінні, які взагалі є найшвидшими серед усіх інших базисів.

Зрештою, після різних перетворень приходять до афінних координат: наприклад, для максимального зменшення складності криптографічних перетворень у групі точок ЕК необхідно використовувати криптографічні перетворення в змішаних координатах з подальшим перетворенням в афінний базис. Це ще раз доводить швидкодію афінного базису.

Для побудови криптосистем на основі ЕК кращим є використання подання точок у модифікованих якобіанових координатах, оскільки вони забезпечують мінімізацію складності операції подвоєння точки на ЕК. Але при великій кількості одиниць у бінарному поданні множника необхідно використовувати більш збалансоване подання координат – якобіанове подання [6].

Використання одного координатного базису не завжди дозволяє досягнути максимальної продуктивності. Перспективним напрямком є використання змішаних координат.

У таблиці 4 наведено складності операцій додавання та подвоєння у випадку використання змішаних координат.

Таблиця 4

Складність операцій додавання та подвоєння під час використання змішаних координат

Подвоєння	
Операція	Часові витрати
$t(2P)$	$7M+5S$
$t(2J^c)$	$5M+6S$
$t(2J)$	$4M+6S$
$t(2J^m=J^c)$	$4M+5S$
$t(2J^m)$	$4M+4S$
$t(2A=J^c)$	$3M+5S$
$t(2J^m=J)$	$3M+4S$
$t(2A=J^m)$	$3M+4S$
$t(2A=J)$	$2M+4S$
$t(2A)$	$2M+2S+I$
Додавання	
Операція	Часові витрати
$t(J^m+J^m)$	$13M+6S$
$t(J^m+J^c=J^m)$	$12M+5S$
$t(J+J^c=J^m)$	$12M+5S$
$t(J+J)$	$12M+4S$
$t(P+P)$	$12M+2S$
$t(J^c+J^c=J^m)$	$11M+4S$
$t(J^c+J^c)$	$11M+3S$
$t(J^c+J=J)$	$11M+3S$
$t(J^c+J^c=J)$	$10M+2S$
$t(J+A=J^m)$	$9M+5S$
$t(J^m+A=J^m)$	$9M+5S$
$t(J^c+A=J^m)$	$8M+4S$
$t(J^c+A=J^c)$	$8M+3S$
$t(J+A=J)$	$8M+3S$
$t(J^m+A=J)$	$8M+3S$
$t(A+A=J^m)$	$5M+4S$
$t(A+A=J^c)$	$5M+3S$
$t(A+A)$	$2M+S+I$

ВИСНОВКИ

Аналіз таблиці 4 дозволяє визначити таке: для максимального зменшення складності криптографічних перетворень у групі точок ЕК необхідно використовувати криптографічні перетворення в змішаних координатах з подальшим перетворенням в афінний базис. Причому, вибір змішаних координат напряму залежить від алгоритму скалярного множення.

Література.

[1] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты та языке Си. Москва: «Триумф», 2002. – 797 с.

[2] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves. Part 2. Digital signatures.

[3] *Cohen H., Miyaji A., Ono T.* "Efficient elliptic curve exponentiation using mixed coordinates", Advanced in Cryptology, 1998.

[4] *Бондаренко М.Ф., Горбенко И.Д., Качко Е.Г., Свинарев А.В., Гриненко Т.А.* Сущность и результаты исследования свойств перспективных стандартов цифровой подписи X9.62-1998 и распределение ключей X9.63-199X на эллиптических кривых. // Радиотехника 114/2000. – С.15–24.

[5] *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Сложность операций в группах точек эллиптических кривых для криптограффических операций. // Радиотехника: Всеукр. межвед. науч-тех. сб 2001. Вып. 119. – С. 51–55.

[6] *Збитнев С.И.* Проективная геометрия – не все так гладко // Радиотехника: Всеукр. межвед. науч-тех. сб 2002. – Вып. 126. – С. 123–131.

Надійшла до редколегії 17.04.2013

Горбенко Іван Дмитрович, фото та відомості про автора див. на с. 201.

Єсіна Марина Віталіївна, студентка факультету комп'ютерних наук, кафедри Безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: криптографія, криптоаналіз та їх застосування з метою захисту інформації.

УДК 004.056.55

Анализ сложности криптографических преобразований в группе точек ЭК в зависимости от выбранного базиса / Есина М.В., Горбенко И.Д. // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 280–284.

Рассматриваются существующие базисы представлений эллиптических кривых и их использование при выполнении операций в группах точек эллиптических кривых, а также скоростные характеристики. Формулируются предложения, касающиеся базисов преобразований.

Ключевые слова: базис, координаты, криптографические преобразования, сложность.

Ил.: 2. Библиогр.: 6 назв.

UDC 004.056.55

Analyzing the complexity of cryptographic transformations in a group of points of elliptic curves according to a basis chosen / M.V. Yesina, I.D. Gorbenko / / Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 280–284.

Existing elliptic curves representation bases and their using in carrying out operations in groups of elliptic curves points are considered. Proposals for using transformation bases are formulated.

Keywords: basis, coordinates, cryptographic transformations, complexity.

Fig.: 2. Ref.: 6 items.

УДК 681.3.06

КРИПТОСТОЙКИЕ КРИВЫЕ ЭДВАРДСА НАД ПРОСТЫМИ ПОЛЯМИ

А.В. БЕССАЛОВ, А.А. ДИХТЕНКО

Рассмотрена форма Эдвардса эллиптической кривой. Приведены явные формулы изоморфного преобразования канонической эллиптической кривой в кривую Эдвардса и обратно. Найдено 40 кривых в форме Эдвардса над простыми полями, приемлемых для криптографии, получены координаты генераторов криптосистем.

Ключевые слова: эллиптическая кривая, форма Эдвардса, простое поле, порядок кривой.

ВВЕДЕНИЕ

Среди различных форм представления эллиптических кривых особое место занимает кривая в форме Эдвардса, появившаяся в современной научной литературе сравнительно недавно [1, 2]. Обладая рядом замечательных свойств, кривые Эдвардса над конечными полями весьма перспективны в криптографии. Закон сложения для точек кривой Эдвардса обладает свойствами универсальности и полноты [2]. Более того, скалярное произведение для точек кривой Эдвардса вычисляется минимальным числом операций в поле по сравнению с другими известными представлениями эллиптических кривых [2, 4]. Несомненно, что кривые Эдвардса вызывают интерес при проектировании криптографических протоколов и будущих стандартов асимметричного шифрования.

Поиск кривых Эдвардса, приемлемых для криптографии, представляет собой нетривиальную задачу. Ключевым моментом в ней является расчет порядка кривой, заданной над конечным полем. В [6] для поиска кривых Эдвардса почти простого порядка предложен подход, в котором для найденных кривых над полями $\mathbf{F}_5$ и $\mathbf{F}_7$ с минимальным порядком 4 найдены кривые приемлемого порядка $4n$ в расширениях этих полей [6, 7]. В данной работе поставлена задача поиска кривых в форме Эдвардса с почти простым значением порядка над большими простыми полями. В первом разделе мы приводим общие сведения о кривых в форме Эдвардса над конечным полем. Второй раздел обозначает проблему определения порядка кривой в форме Эдвардса и кратко описывает возможные пути ее решения. В третьем разделе мы приводим 40 кривых Эдвардса над простыми полями $\mathbf{F}_p$ с модулями p длиной 192, 224, 256 и 384 бит [8]. Порядок $4n$ предложенных кривых содержит простой сомножитель n, сравнимый по величине с величиной соответствующего поля. Таким образом, найденные кривые удовлетворяют современным требованиям к порядку генератора криптосистемы и с успехом могут применяться на практике.

1. КРИВЫЕ В ФОРМЕ ЭДВАРДСА. ЗАКОН СЛОЖЕНИЯ ТОЧЕК КРИВОЙ

Пусть k – конечное поле ($char(k) \neq 2$). Кривая в форме Эдвардса над полем k задается уравнением в аффинных координатах [1–6]:

$$E: \quad x^2 + y^2 = 1 + dx^2y^2 . \qquad (1)$$

Далее будем рассматривать кривые Эдвардса с учетом ограничения на параметр кривой $d \neq A^2$ в поле k. Это гарантирует полноту закона сложения, заданного над точками кривой (1). Сумма двух точек с координатами (x_1, y_1), (x_2, y_2) определяется формулой

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right). \qquad (2)$$

Таким образом, если $d \neq A^2$ в поле k, то закон (2) корректен для произвольных точек (x_1, y_1), (x_2, y_2), включая совпадающие, обратные точки и точку $O = (0,1)$. Доказано [2], что знаменатели $1 + dx_1x_2y_1y_2 \neq 0$ и $1 - dx_1x_2y_1y_2 \neq 0$ при $\forall x_1, x_2, y_1, y_2 \in k$.

Легко видеть, что кривая (1) содержит как минимум четыре точки: нуль аддитивной группы точек O = (0, 1), точку 2-го порядка $D = (0, -1)$, точки 4-го порядка $\pm P = (\pm 1, 0)$. Отсюда следует, что любая кривая в форме Эдвардса имеет порядок, кратный четырем. В работе [2] доказано, что для любой кривой, записанной в форме (1), найдется изоморфная эллиптическая кривая в канонической форме над полем k. Однако, в известных стандартах шифрования на эллиптических кривых [8] не содержится кривых над простыми полями с кофактором 4 порядка. Это не позволяет преобразовать рекомендуемые современными стандартами кривые непосредственно в форму (1). В этой связи для криптографических приложений следует провести поиск кривых Эдвардса над простыми полями с приемлемым значением порядка $4n$.

2. ИЗОМОРФИЗМ МЕЖДУ КРИВОЙ В ФОРМЕ ЭДВАРДСА И КАНОНИЧЕСКОЙ КРИВОЙ. РАСЧЕТ ПОРЯДКА КРИВОЙ В ФОРМЕ ЭДВАРДСА

Для каждой кривой (1) в форме Эдвардса E найдется изоморфная ей кривая в форме Вейерштрасса W вида

$$W: \quad v^2 = u^3 + Au + B . \qquad (3)$$

Соответствующий изоморфизм между точками кривых E и W задается правилами [3]:

$$u=\frac{(5-d)+(1-5d)y}{12(1-y)},\ v=\frac{(1-d)+(1+y)}{4x(1-y)}, \quad (4)$$

при $x(y-1)\neq 0$.

Четыре точки пересечения с осями координат преобразуются следующим образом:

$$(x,y)=(0,1)\to(u,v)=O,$$

$$(x,y)=(0,-1)\to(u,v)=\left(\frac{1+d}{6},0\right) \text{ при } x=0. \quad (5)$$

$$(x,y)=(\pm 1,0)\to(u,v)=\left(\frac{5-d}{12},\pm\frac{1-d}{4}\right) \text{ при } y=\pm 1.$$

Коэффициенты кривой W выражаются через параметр кривой E следующим образом [3]:

$$A=-\frac{(1+14d+d^2)}{48},$$

$$B=-\frac{(1-33d-33d^2+d^3)}{864}. \quad (6)$$

Для обратного преобразования справедливо:

$$x=\frac{6u-(1+d)}{6v},\ y=\frac{12u+d-5}{12u+1-5d},$$

$$\text{при } 6v(12u+1-5d)\neq 0,$$

$$(u,v)=\left(\frac{1+d}{6},0\right)\to(x,y)=(0,-1), \text{ при } v=0, \quad (7)$$

$$(u,v)=O\to(x,y)=(0,1).$$

Одним из способов расчета порядка кривой Эдвардса является адаптация соответствующих методов нахождения порядка канонических эллиптических кривых (таких как алгоритмы Скуфа, SEA, Satoh). Используя соотношения (4)–(7), для кривых в форме Эдвардса, определяется последовательность полиномов деления [3], посредством которых может быть вычислен порядок рассматриваемой кривой Эдвардса. С другой стороны, подсчитать порядок кривой Эдвардса можно посредством изоморфного перехода к канонической форме с последующим нахождением порядка кривой по известным алгоритмам.

Второй сценарий был использован для поиска кривых над простыми полями, приведенных в разделе 3. Выбрав произвольно параметр $d\neq A^2$ в поле k и, используя формулы (6), получим изоморфную эллиптическую кривую в форме Вейерштрасса. Заметим, что при заданном ограничении на параметр d кривой, дискриминант изоморфной эллиптической кривой будет отрицательным и в кубик правой части уравнения (3) будет иметь единственный корень. Подсчитать порядок эллиптической кривой можно, например, по алгоритму SEA. Порядок N_E рассматриваемой кривой считаем приемлемым, если число $n=N_E/4$ простое, лежащее приблизительно в пределах 180–600 бит. Такая кривая может быть рекомендована к применению в криптопротоколах.

Для построения криптографической системы на полученной кривой Эдвардса необходимо определить генерирующую точку порядка n. Задавая произвольно координату x и вычисляя из уравнения кривой (1) значение y, получим произвольную точку Q кривой Эдвардса. Если $x\neq 0$ и $x\neq\pm 1$ (вероятность этого события ничтожно мала), порядок точки Q может быть равен $n=N_E/4$, $2n$ или $4n$. Тогда генератором криптосистемы будет точка Q, $2Q$ или $4Q$ соответственно.

3. КРИВЫЕ ЭДВАРДСА ПОЧТИ ПРОСТОГО ПОРЯДКА НАД ПРОСТЫМИ ПОЛЯМИ

В данном разделе мы рассматриваем простые поля с модулями

$$p_{192}=2^{192}-2^{64}-1,$$

$$p_{224}=2^{224}-2^{96}+1,$$

$$p_{256}=2^{256}-2^{224}+2^{192}+2^{96}-1,$$

$$p_{384}=2^{384}-2^{128}-2^{96}+2^{32}-1,$$

рекомендуемые стандартом FIPS – 186 – 2 – 2000 [8], и приводим перечень кривых в форме Эдвардса почти простого порядка $N_E=4n$ (n – простое) над каждым из полей. Данные изложены в таблицах 1–4. Наряду с этим, в таблицах также содержатся общесистемные параметры для реализации шифрования с помощью кривой Эдвардса, а именно, порядок $n=N_E/4$ и координаты (x_G,y_G) генератора криптосистемы для каждой кривой.

В каждой из приведенных ниже таблиц содержится по 10 кривых Эдвардса над соответствующим полем с параметрами d различной битовой длины. Порядок кривых сравним по длине с длиной рассматриваемого поля. Расчеты производились посредством прикладных программ, основанных на использовании функций библиотеки MIRACL.

ЗАКЛЮЧЕНИЕ

На сегодняшний день открытой остается задача адаптации алгоритмов вычисления порядка кривой для кривых в форме Эдвардса. Однако приемлемые кривые Эдвардса над простыми полями можно получить посредством трансформации кривой Эдвардса в изоморфную кривую в форме Вейерштрасса с последующим определением порядка кривой в форме Вейерштрасса.

Таким способом в данной работе получено 40 кривых Эдвардса над простыми полями с модулями p_{192}, p_{224}, p_{256}, p_{384}. Порядок кривых, приведенных в разделе 3, имеет минимально возможный кофактор, равный 4, и простой кофактор, сравнимый по длине с длиной соответствующего поля. Это делает возможным применение полученных кривых в практических приложениях. Благодаря выигрышу в быстродействии (в среднем в 1.5 раза [4]) и удобству программирования

Таблица 1

Кривые Эдвардса почти простого порядка над полем с модулем p_{192}

$p=$	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF
$d=$	28453E
$n=$	40000000000000000000000001AEAD1229D137F564D7FF6D5
$x_G=$	AE709D07B2D112CECD4A7AE103757F2C101D054ACB1A0F17
$y_G=$	8BDF8D5A994AAB1E1455889D28E29CA3EC68548D3F7CA32F
$d=$	6DBA6A
$n=$	3FFFFFFFFFFFFFFFFFFFFFFFEA75D4027230DD4DFFDB0455
$x_G=$	44F083BB00E51AD91A2743284D31F57EE5C84826FCC91F4B
$y_G=$	15FC16E5870524E0DBBE9EC8BB9F066C02A02B1978D4E029
$d=$	CE37DC
$n=$	400000000000000000000000002618428A483A133570834389
$x_G=$	508AEB91AB9A230C377BD82BDDBE5B75CD38CDF1DA407A3C
$y_G=$	6E12D78C595D0ECC1614BFD04616CE45D6BB7D8607BB2ED7
$d=$	111DB4A
$n=$	400000000000000000000000004F2EA0DD45656E7E6066E8C9
$x_G=$	1603A0943674DA7D8476608E764BA7A63DBEBE4D8E549165
$y_G=$	148D5DA4654152C9196699074374EE091FE789A0CC7EC60
$d=$	12CCB98
$n=$	400000000000000000000000006AF187D9A93890273705F7E9
$x_G=$	6AC4FE0FEF645CA5754BFB0BD05967A418FCCAAF20E473A9
$y_G=$	B2F122E8816B142765B0FABCD7834CDC2D1AAC7EA779750B
$d=$	BFFAB4397C01049E12A46027E7E14D7A666240E6831D926
$n=$	400000000000000000000000022F2FB1AD838D6680571D7BB
$x_G=$	B46D3402D2A7F4CE30C5AA7839B0CE8D957240684824C726
$y_G=$	F0B24C20880DE704123ADF2A44189480DDFFDEEAF002B238
$d=$	CAE5B27FA36F62C6EC5EEC6ABE086C2BFF6A9F029CE42C88
$n=$	3FFFFFFFFFFFFFFFFFFFFFFFBD410EA5F77DD3ECCBD0FC45
$x_G=$	72F6A4BADEB19F876258926630ECA22F1D9FEF34CE53440C
$y_G=$	852D88019C7A20987BEE784A9EC09FF213639E59A3C3A51E
$d=$	2FDE6BF890C01A5FEB8B8D976676DDAC8C3349FE0C89959A
$n=$	3FFFFFFFFFFFFFFFFFFFFFFFC9B03E26E57C1A34245E23ED
$x_G=$	F2FA1F9E30FDF9C5CD1E84D287CE5F2DE9283B077C2C83FA
$y_G=$	419A50AF660CBF77699FBECBF7181F7F15C0DCF31523171F
$d=$	83E48CF4C49FDDEF6E5D812D3FBD06054835C85D6DD283BC
$n=$	400000000000000000000000002640829409C3B60282409D8B
$x_G=$	5BCFE7F1248E5A43CDF179D95334FE45061F0ECB599020B2
$y_G=$	FDEB479483DB5D1743AE7496B9A32B5CF774B8D8CD13272F
$d=$	CFC522DAB7BE9E92FA78DDA10CE941CC7108A299FB4A79C9
$n=$	400000000000000000000000006B362B3138DB79B9866A5BD7
$x_G=$	BE321DFF94A4E7DA940394E9C9EC1F2BC4B29F93302BDA3B
$y_G=$	B5E1CE7F685CEFE82284E5027404FE6E8D3C11E7D37092F3

Таблица 2

Кривые Эдвардса почти простого порядка над полем с модулем p_{224}.

$p =$	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF000000000000000000000001
$d =$	3608425
$n =$	400000000000000000000000020BBEC47CEDB34DD05BCB6B7E619
$x_G =$	C448CA02660F57204FF1BDE2B5CC3E25606A7460399FEA3DA9A06383
$y_G =$	319117770D6FC7FE35F6A02905FE1F363156BD2E5B75BB89A64CAFAB
$d =$	42E5CF5
$n =$	400000000000000000000000070D1AD037FD1F2585B37C3CD8E75
$x_G =$	74E8DA9676A0AA64C73460EFBA56F04A5D69FB39DC03A0D53B9E99A9
$y_G =$	A70D758DE2B7CADCEED9D6315F44987AF89B9D1D3BB62B54574971D5
$d =$	148CD57
$n =$	400000000000000000000000001BE5276AAC300270278233024CF9
$x_G =$	EEA0CBD1BFB937E1C83C12E90200429DD3F74854256DA5E249B04A2B
$y_G =$	512F075B98B7281E07BDABF68CE2BF4A30200DB1A9029ABDAAAEDEEA
$d =$	2C4C61C
$n =$	400000000000000000000000000054547A5F0105F649731ECC684CF
$x_G =$	142954F6B9702D136634AD2F6574ED5CF24E2D7D8AEB0B855105451A
$y_G =$	6EB430B9BE6B0A78D41BCBCFC3A207D0A813C8AB052BFD23529D23E9
$d =$	2DD96A9
$n =$	400000000000000000000000000024E3FE6372F8DB77945FFF06024D
$x_G =$	C62E8C8EB908FFC6DAE6D79D335618D62855B9A14F49DF1DEE0A414E
$y_G =$	6955A4D991CFE25E6EE21B64FC61763C16634CA234222A0E752F4E85
$d =$	1968A1D7A81AF44243D0F60F186A519FB95BF7C2FE2C037798D70FE9
$n =$	400000000000000000000000000003FCA1753F6F54C2A869DC8C5DBD9
$x_G =$	6F39E721F18128534C6C0339A982011683D9676565CAFD942F8C7761
$y_G =$	2E5ECC135081FE6FF9E0F7020BBC7EFD9DFB18A47B81DB825FC26817
$d =$	60B4BE2A9399C390AA051FC8B4706856E1CE2A03791C1B5A2C88DD40
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFF5722B78ED1CA9B003572246F325
$x_G =$	60D6B139288C1B171E8FE28EC068130CABDA0A1A48C1DF7280A14211
$y_G =$	198E5F9E549D6C080CCCA7886E6BC880623B5AB1070CB62A81377BC0
$d =$	E3850F8A3D93759F172493E9339B29DB7D345BE57CFCDCE545EEB1DC
$n =$	400000000000000000000000000005B3B3E37B9EDE0A1B45BEC627F5B
$x_G =$	DB921A45CBF9979A3425F0556165DEF73ED6792034A9D9A5DC180FC9
$y_G =$	A3A87DA7A0307AD196B2CEC840C3E17147C570EBE9CC432DBF941CD7
$d =$	6E6607C2DCE3392468455ED0DBFBA5442AD87C7B8CE484C1B85D592
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFE623254CA68DF10B09B50D57327B
$x_G =$	96C7C00D85C8BB5B53F74E6EF38EFEEB458FE9434290046114E0E906
$y_G =$	A2410947B7C669193EC0B39001FC786B0558C3DBB6B64BC9677A7016
$d =$	2BFE721565BE78DE5DABD588BCE5E62C7127A0BEC33A2FF844E0B79D
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFCCA2B4C227A60815F6A6359225E9
$x_G =$	DA2B86A81DBF8B887D3A3552A26CF3679DC73C300998BD82EEC1F49C
$y_G =$	D817BCDA64B37A31B2A15975F472A18F8D226446D1473CB3FB38D7C

Таблица 3

Кривые Эдвардса почти простого порядка над полем с модулем p_{256}.

$p =$	FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
$d =$	72A38
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFBA76FA29C30CC3AA4954B53EDBE54D75
$x_G =$	894F8283626AEE6848515DDDC3B8DBB3D5302DEE0EE75080D6753E4D39BA5AB2
$y_G =$	EA612346223F6480CBBAFA39DB95D54D21469DD3074A957EFDA4FD79FEB630B5
$d =$	2EBFA9
$n =$	3FFFFFFFC0000000400000000000000005EFF905BA96F95CE79513CBE0CC53D1F
$x_G =$	363D655BF3F221256F032FC791B06149C14ACFFD92B59C84D1D3B817A9E622D2
$y_G =$	A52438C53DDCA661685B1F235EF0F1D280A493C33153AD691097AEC67A62C564
$d =$	805294
$n =$	3FFFFFFFC000000040000000000000051814C8E8360B7C96A8419F38B8039F1
$x_G =$	EEBABE42482F67FECF7F9D2D49A4430372D7678CF7EDAB4B9184D42BD93F390C
$y_G =$	E2A059E8C776F46028BA9265E20C09A785ECEEFB162562DA2AF78BC412D2D3CC
$d =$	9855C9
$n =$	3FFFFFFFC000000040000000000000002C1564946E895DAE0EB7EB501C62C62F
$x_G =$	D139CE35F84CFA17E8ED28E083F07C708303AE788477118C5AFE86D313D443BD
$y_G =$	F5F4A5309EEA75820AEE714A8D99CD22CE2539E73D2C6688B8480E18F1D384D
$d =$	BE957B
$n =$	3FFFFFFFC000000040000000000000005DACD9D621DE8444CB5625A8193E1D81
$x_G =$	B1550150B88C76AEC1CD0B0EC2008D1D73D086A0FD63103A0875EF574F0FF113
$y_G =$	306021DA97347B1DA05C98CE858B5C69ED901187DB03F68C399B694003FACA96
$d =$	4A5084ABF5DFFAC393E29A8BF045F4AA94C80F55414AFDAB8517CE769130DC82
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFF9B91248CDD0CAF813BD0F8B9F32C892B
$x_G =$	96540A02F26ED385B606A7956E5BA33B8D5A9E47FCE718C752562E2F2A6891E2
$y_G =$	ACDE96C64793B77B72DC71EB12508AAC629C4CCAA281BF164B73030EF382D9DE
$d =$	340B9C82867CD106FA7E1B11E9415A1099BB48C9A28F3B21A77E70C20E528839
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFFBE08C2E4E3DDB90FBAB306B69633071
$x_G =$	490659C09655C82EECDC109AC5F29E85DC94882E30916E9F21273AFE9D1B01AC
$y_G =$	9BB0A4609F48A8029AD9014BE7184E36A120B5789799DE52F4E7D8D90386F786
$d =$	32BBA52848792541A79779B4CFFF035903D2112814334C1BE3556A670A9D73D1
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFFC0285F94E407693E8624559A0D329309
$x_G =$	9D39DB8088196DE49C37D787D64EEB9ECA6A762BE77D0FCBD0430DCCBB057C2E
$y_G =$	62ABD075DA7C26034514079E7B5000D4493BC4318C5A3E3856FAAB8724C5C0F5
$d =$	8884FA14412BC9B62B0C467262DA6BD8F529C01AAD09545B2A294D479B254B2F
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFC7D37AFE15BFD6994B8E6427BA368D27
$x_G =$	D5D245310DD89B88DFF59C2CAEC8DBE62000E53D0BB4051247B97DDF420158C
$y_G =$	444B435A604729B76A17E8F4B93A47DC62D7777C1B056DB727675D627CF749F1
$d =$	E49478138FFE7946F81C3AC55BBBE4D41B4DF660A3B118B0075676506425D9FA
$n =$	3FFFFFFFC000000040000000000000000300FC8D622E987518514DFF16654AAFB
$x_G =$	92967B57C8CAB56FBDE3C3B0568C336BE2FBBB875F3983281D38B173C80971B9
$y_G =$	F3270D7C8A827B913A0B10079555D7D2E3A1C64578A49A77A9C1E6B45C186E90

Таблица 4

Кривые Эдвардса почти простого порядка над полем с модулем p_{384}

$p =$	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFF0000000000000000FFFFFFFF
$d =$	12593A
$n =$	40000000000000000000000000000000000000000000000005063576B5A9A0C3A23E9510EA680650B4884E63A2968DD71
$x_G =$	1FC0E8E61F599813E376D11F7510D77F177C2F1CDE19FD14D63A2EC5EAD4D0DED1BD06676CCF365243BF3C0675A31B62
$y_G =$	F52B4FA352B257D7A102FA45C56A50CCBDB3DEC053D5610EDBD0188C11F321F28A43E2FC50395E4A8BD0029AE71D51AA
$d =$	46959A
$n =$	40000000000000000000000000000000000000000000000000C06E6B5CE557E3DDEC6844B3470B819A9E1C0ED5F348517
$x_G =$	4567EA938DECB2BC17F9ABDEDBD77AD188FEFD6E244FD8A12C95A365F9C241E13888506D9D1FB4F8F9B8AA49098C3DF0
$y_G =$	121D587D9CEDEB34DD331E150D9FB2A23B314A354411C4F4A5AFF18685F6EDA1D557EC99F830785420A4DAD15897814E
$d =$	5FD247
$n =$	4000000000000000000000000000000000000000000000000A6A021C752BB157244080A30D578824A05A3BFFF4E67575
$x_G =$	8947F1251392317F3C0E127F7D337B1EE67A120BC69B5E1D91B6C7DC004904C1D42013DE9F12176B6EB34AD5CAC2D485
$y_G =$	B934A355EC5F900123E5EFFDB74502E084A94E59BFDF80E2B0979D02F971F0FE93A4ECE5FFC82C34724A2063836DA847
$d =$	7B35A8
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF96861B6F4CC029EE5B29F5BE0649FA4B3A605D3EC2CFD8F
$x_G =$	712160E70ED57AEC69A66E55A3A285DBFA712F9ACF9B334AC881E5066E55A415BE5935881C7DF7AF90EF6558C380037
$y_G =$	F1FF700AB04A2CA0F40FD94F1E32F61A3D4638570A28EB07AD1D281DAAC0293B946205098F71AC9BEBC8616F1B1DD3E8
$d =$	9302CE
$n =$	400000000000000000000000000000000000000000000000422338834D697FC3149FC70C79239975452EA01F75E2B699
$x_G =$	E9FDD336AC467447D6DB0627563C181663797C6D87F8E66A3E61BE69E53F66CCC4847DF28A19235D9377F4A33FEE0F69
$y_G =$	CF9AC7F9EEB6528DF53C80BF02E3A83D07614F2708148B4F7F1907398DE79019256D32E535219D71F173DEAE9621716B
$d =$	4CCEDF781B3680122FCFC696374F2ACA57E8F7514293BDD81F5040F0858023ECD295E6835FC14021B1AFFAF8065139C9
$n =$	400000000000000000000000000000000000000000000000046824B5EE5BADD70EB246617456AD087BADECDA7CD2A6E81
$x_G =$	36AFEDFF2308CF4C2F2052B0BF3068F0B4EE9759729A40491EF5D5E75F23E74A6F8528D276E6C528F487DE35E71454CB
$y_G =$	94D6B53F630A6D41E4DD65CD195839CC24DE7B6A71C3DC0A814E379445C67C6604B8034F7C5580AC0FBE771FBA1E9E36
$d =$	3462B5F8DD2744C13ED8618BAFC853F60F83134B936F3DD2867562D1CEEA866E590D702CE8C11262193F077A798918DE
$n =$	400000000000000000000000000000000000000000000000339419162A90FA9A9CA9C0C12B231CF5D95CC5E241D18C0F
$x_G =$	387CCD92DDCF7203D579EC6D158AD3A4DBAB83BBA4E153FB130F380425FD9F73AABEE0F2BE3BCA53D9E1D798DB016F3C
$y_G =$	50E827613BC65DEC52FD123387279D4E9E27102CE6B9119DC656632ED043D3961C72EB7C67D690D970CC65DD2F7C5702
$d =$	941F6CCE649868BD59F335D3293FBB201E3C811ADE19779EEFD8FB21AC1A466377365A8763793A3B3BB2B6575D9893D1
$n =$	400000000000000000000000000000000000000000000000002E0E36DDDDC5D4EA80D339D03926CA39AE3A4739EF81A1C9
$x_G =$	647D270CE4CB1F9038EEE75ED9570A3360AC68DE443BE52D23A734966F813D690615BE4284BDD78CF89B4ED2D02BE08A
$y_G =$	32247232CFA0A712AE3B029B1DDF8C5FE86A78E5728CB4D4386026C21A92297C271C81294C7B9DC18E245F6D87706865
$d =$	584D94FEA391957947760106F180D57CFE8E85109656E4B0BF6FCBF69D62F9A649AEF53CDA9B9F3B2BB247DEB6AB0C70
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8C7F4A394F5C92E8C6FB2FD97B1657DF603DB9677EEE6DD9
$x_G =$	4CAFBA0D62C538B7CC74F8274978AF35C43E2360BA6606FD379086367898EFD57040629FD9AC9721D65BCB511603BA00
$y_G =$	E2C024B79576CC47776562F9203B166E1C8300AD5C7F4D0B04FE0DBAF92FEC3DD0E5CE1F93288308D2C5CFF5B24DEC9A
$d =$	A01FD8E4FCE20AF1A99E214FDFB6AB3CAB8FEBF45F18DA66000E104265E11B82D8499835148459978BB-8003DB7E1F5B6
$n =$	4000000000000000000000000000000000000000000000000025DABC64D5F4783A6399E3A6701B920E95AA760041BFFAD
$x_G =$	144C701104F4122AC3D09B9B212CD428F8B61993E202C74A02CC95EFAAE257E1FF7DCA3592A60A37E76BA94D-50213C7C
$y_G =$	1BF38FDE630B35DA3EEA40138E94574CF9BD4AF60779D792360252752EBAAAD36D1C31DD-9294586633178062BAA5AF0F

криптосистем кривые Эдвардса могут стать эффективной альтернативой каноническим эллиптическим кривым.

Литература

[1] Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.

[2] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[3] Moloney R., McGuire G. Two kinds of division polynomials for twisted Edwards curves. Applicable Algebrain Engineering, Communication and Computing, 2011. – PP. 321–345.

[4] Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, №4, 2011. – С. 33–36.

[5] Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника, вып. 167, 2011. – С. 203–208.

[6] Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей // Прикладная радиоэлектроника, том 11, №2, 2012. –С. 225–227.

[7] Бессалов А.В., Дихтенко А.А., Яценко А.И. Параметры криптосистемы на кривой Эдвардса над расширениями малых простых полей // Прикладная радиоэлектроника, том 12, № 2, 2013. – С. 93–97.

[8] Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224 с.

Поступила в редколлегию 25.04.2013

Бессалов Анатолий Владимирович, фото и сведения об авторе см. на стр. 277.

Дихтенко Алиса Анатольевна, фото и сведения об авторе см. на стр. 277.

УДК 681.3.06

Криптостійкі криві Едвардса над простими полями / Бессалов А.В. // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 285–291.

Розглянуто форму Едвардса еліптичної кривої. Наведено формули явного ізоморфного перетворення канонічної еліптичної кривої у криву Едвардса і навпаки. Знайдено 40 кривих у формі Едвардса, які прийнятні для криптографії, отримано координати генераторів криптосистем.

Ключові слова: еліптична крива, форма Едвардса, просте поле, порядок кривої.

Бібліогр.: 8 найм.

UDC 681.3.06

Cryptographically resistant Edwards curves over prime fields / Bessalov A.V., Dihtenko A.A. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 285–291.

The Edwards form of an elliptic curve is considered. Explicit formulas of isomorphic transformation of a canonical elliptic curve into Edwards's curve and inverse are given. 40 curves in the Edwards form over prime fields suitable to cryptography are discovered, coordinates of cryptosystem generators are obtained.

Keywords: elliptic curve, Edwards form, prime field, curve order.

Ref.: 8 items.

УДК 621. 391:519.2:519.7

МЕТОДИ ПРОТИДІЇ АТАКАМ НА РЕАЛІЗАЦІЇ, ЯКІ БАЗУЮТЬСЯ НА АНАЛІЗІ ЕНЕРГОСПОЖИВАННЯ, СХЕМИ НАПРАВЛЕНОГО ШИФРУВАННЯ У КІЛЬЦЯХ ЗРІЗАНИХ ПОЛІНОМІВ

Д.В. ІВАНЕНКО

Аналіз існуючих методів протидії атакам спеціального виду. Досліджуються недоліки та переваги методів протидії атакам: CPA, SPA, DPA, які реалізуються на криптосистеми у кільцях зрізаних поліномів.

Ключові слова: методи протидії, атаки спеціального виду, CPA, DPA, SPA.

ВСТУП

Відсутність нових відкритих публікацій про переваги та недоліки математичної моделі сучасних асиметричних криптосистем, при існуванні відомих успішних реалізації на схеми направленого шифрування, наводить на думку науковий світ, що зловмисники звернули увагу безпосередньо на програмну та апаратну реалізацію. Тобто завдання зловмисника зводиться до дослідження реалізованої криптосистеми з метою пошуку залежностей, переваг та недоліків; гонка за швидкістю, великою продуктивністю за рахунок оптимізації, використання сучасних технологій – веде до складностей при апаратній реалізації, людського фактору – помилок у реалізації, все це веде до імовірності реалізації атак [3] на реалізацію.

Такі атаки отримали назву атаки спеціального виду, існування таких атак формулює завдання аналізу існуючих та можливих методів протидії атакам спеціального виду. В цій роботі будуть проаналізовані методи боротьби з атаками, які базуються на аналізі енергоспоживання, та зроблено спробу запропонувати універсальний метод.

1. ІСНУЮЧІ МЕТОДИ ПРОТИДІЇ АТАКАМ НА РЕАЛІЗАЦІЇ

З появою атак спеціального виду виникла задача створити методи та засоби протидії цим атакам. Наведемо класифікацію та дамо визначення таким методам протидії:

1) Використання фіксованих схем операції для кожної моделі операції:

а) Метод Монтгомері [6–9]. Цей метод дозволяє прискорити операцію множення та піднесення до квадрата;

б) Доповнення до операцій [10–13]. До основної групи операції додаються змішані додавання, фіксовані додавання, єдині додавання, подвоєння;

в) Атомарність [14]. Це властивість операцій, під якою розуміють, що операція виконується як єдине ціле або не виконується взагалі. Тобто, внаслідок порушення процедури виконання операції, процедура виконання відкочується до початку операції і всі операнди операції генеруються спочатку.

2) Рандомізація даних [5];

3) Засліплення даних [15–17]. Засліплення служить для зміни вхідних даних у деякий непередбачуваний стан. Залежно від характеристик функції засліплення, вона може виключити деякі або всі витоки корисної інформації.

Складність вибору методу протидії ускладнюється ще тим, що атака спеціального виду є атакою окремого випадку. Тобто успішна реалізація на одному пристрої може бути неефективною для іншого пристрою.

Також з впровадженням методу протидії потрібно враховувати особливість системи, для того щоб реалізація методу протидії не впливала на ефективність та на властивості, за якими було обрано криптоперетворення.

2. КРИПТОСИСТЕМА З ВІДКРИТИМ КЛЮЧЕМ NTRU

Для аналізу методів протидії атакам спеціального виду обрали схему направленого шифрування у кільцях зрізаних поліномів, NTRU. Тому що саме в NTRU бачать світле майбутнє у постквантовій криптографії.

Алгоритм включає в себе три відкритих параметри (N, q, p), де N, q, p – цілі, та q, p – взаємно прості при тому, що p значно менше від q. Процедура генерації ключа починається з вибору випадкового $F \in R$ та вирахування $f:=1+pF$. У випадку, якщо f не має зворотного елемента за *mod q*, то потрібно обрати інший F та повторити процедуру. Далі необхідно вибрати другий поліном $g \in R$, який буде зворотний за *mod q*. Таким чином, f – це секретний ключ, а h – відкритий ключ, який потрібно обчислити з такого виразу: $h:=pf^{-1} *g \bmod q$. Повідомлення позначається через m. При шифруванні відправник випадково вибирає поліном $r \in R$, потім обчислює значення шифр-тексту $e:=r*h+m \bmod q$. Для розшифрування e отримувач обчислює $a:=f*e \bmod A\ q$, де *modA q* означає, що коефіцієнти зсуваються на інтервал $[A, A+q-1]$ після приведення за *mod q*. Потім отримувач відновлює текст за формулою – $m:=a \bmod p$.

Домінуючою операцією в шифруванні та розшифруванні NTRU вважається обчислення $r*h \bmod q$ та $f*e \bmod q$. Коефіцієнти поліномів h та

e розподілені майже випадково, один вибирає *r* та *F* так, що результат операції згортання *r*h* та *F*e* може бути мати більш низьку обчислювальну складність. В алгоритмі використовуються бінарні або тернарні коефіцієнти, r_i, $F_i \in \{0,1\}$ або {-1,0,1}, і фіксується число ненульових коефіцієнтів у *r* та *F*[18,19]. Потім обчислення операції згортання може бути обчислено за *dN*-операцією, де N – загальне число коефіцієнтів поліномів та d – число ненульових коефіцієнтів.

Алгоритм 1 є оптимізованим алгоритмом обчислення $t=a*c \bmod q$, де зниження за модулем $\bmod N$ пересуває в індексі обчислення по масиву t за рахунок додаткової пам'яті (t_N, ..., t_{2N-1}). У цьому алгоритмі, $a \in R$ є бінарним поліномом з d ненульовими коефіцієнтами та $c \in R$ – загальним поліномом. Бінарний поліном a є масивом b, у якому позначено ненульові положення d. Наприклад, $a(X)=1+x3+x6=[1,0,0,1,0,0,1,0]$ для $N=8$ матиме такий вигляд $b=[0,3,6]$.

Наприклад: розглянемо ситуацію, де зловмисник намагається відновити секретний ключ (a(x)), при тому що він контролює вхідні дані (поліном c(x)) та знає результат операції згортки (t(x)). Припущення відносно знання секретного ключа зловмисник робить за допомогою аналізу спектра енергоспоживання під час виконання операції згортки на пристрої.

Алгоритм 1 – Обчислення операції згортання [4]

Вхідне: масив b, який є не нульовим значенням бінарного поліному $a(X)$, що є секретним ключем); поліном $c(X)$.

Вихідне: $t(x)$ тимчасовий буфер, у якому зберігається результат.

1. for $0 \le j < 2N$ do
2. $t_j \leftarrow 0$ //з t_N до t_{2N-1} : тимчасовий буфер
3. end for
4. for $0 \le j < d$ do
5. for $0 \le k < N$ do
6. $t_{k+b[j]} \leftarrow t_{k+b[j]} + c_k$
7. end for
8. end for
9. for $0 \le j < N$ do
10. $t_j \leftarrow (t_j + t_{j+N}) \bmod q$
11. end for

3.ЗАПРОПОНОВАНІ МЕТОДИ ПРОТИДІЇ АТАКАМ СПЕЦІАЛЬНОГО ВИДУ НА ЕНЕРГОСПОЖИВАННЯ

Аналіз алгоритму NTRU показує, що головною математичною операцією під час зашифрування та розшифрування у алгоритмі NTRU є добуток двох поліномів $a(X)$ і $b(X)$, та операція згортання $t(X)=c(X)+a(X)$, де $a(X)$ поданий у вигляді множини b. Тому було б ефективно запропонувати методи протидії, пов'язані саме з цими операціями:

1. Рандомізація тимчасових даних, які зберігаються у t.
2. Засліплення відкритих даних c.
3. Рандомізація секретних даних b.

Мета цієї статі полягає не тільки в аналізі запропонованих методів протидії атакам спеціального виду, а ще й у знаходженні таких методів, реалізація яких не впливала б на ефективність самого алгоритму, тобто щоб алгоритм не втрачав своєї початкової швидкості, стійкості, ефективності.

Загальним принципом впровадження методів є рандомізація та складність вияву залежності операції над значенням секретних даних, важливим аспектом реалізації кожного методу протидії є необхідність підтримувати початкові властивості алгоритму: швидкість, стійкість, ефективність.

Використовуючи класифікацію атак спеціального виду на енергоспоживання[3], проаналізуємо запропоновані методи протидії для криптосистеми NTRU.

4.РАНДОМІЗАЦІЯ ТИМЧАСОВИХ ДАНИХ, ЯКІ ЗБЕРІГАЮТЬСЯ У *t*

Першим методом протидії є ініціалізація t з випадковими цілими числами, а не нулями. Ця протидія направлена як на SPA, так і на CPA(включаючи DPA). Ініціалізація t з невідомими значеннями ускладнює для зловмисника реалізацію SPA та робить складнішим пошук кореляції між енергоспоживанням та основним додаванням, тому що один з двох операндів має випадкове значення. Тобто імовірність знаходження максимумів, в ході аналізу спектра енергоспоживання зловмисником, йде до нуля, що і потрібно було зробити.

На рис. 1 показано максимальне значення коефіцієнта кореляції після використання першого заходу протидії, з цього можна зробити висновок, що пошук максимального піку для визначення значення $b[l]$-$b[l$-1] є досить складним.

Для того щоб реалізація алгоритму не втратила необхідну ефективність, необхідно щоб $t_{\max} \le d \times \max_{0 \le k < N} c_k$, де t_{max} – є максимумом серед t при $0 \le j \le 2N$.

Таким чином впровадження цього заходу тільки обмежить стійкість алгоритму до CPA, оскільки обмежується вибір r_j. Наприклад, шукаючи вихідне значення $b[1]$-$b[0]=3$ (див. рис.1), зловмисник має $HD(c_3, c_3+c_0)$ та це значення зміниться на $HD(r_4+c_3, r_4+c_3+c_0)$, у випадку реалізації першої протидії. Тоді буде безглуздо використовувати r_4, який набагато більший, ніж c_3+c_0, тому що з високою імовірністю положення старшого біту в r_4 майже не сприяє знаходженню відстані Хеммінга, для цього c_3+c_0. Тому розумно припустити, що r_4 знаходитиметься в інтервалі $[0, c_3+c_0]$. Просте узагальнення цього спостереження для інших значень $b[l]$-$b[l$-1] призводить до рішення, що розумно припустити, що $r_j \le t_{\max}$. Якщо $\max_{0 \le k < N} c_k$ у звичайному шифр-тексті, то $r_j < dq$.

Після цього зловмисник може зробити припущення щодо деякого фіксованого значення

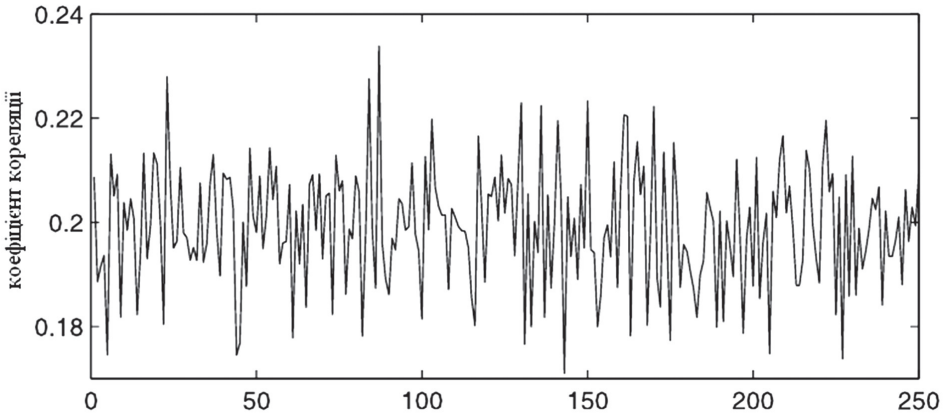


Рис. 1. Максимальна кореляція для кожного можливого припущення після впровадження протидії №1

всіх r_j при $r < dq$ та спробувати розпочати схожу атаку до оригінального CPA. Такий вид атаки може бути визначений як потенційний, тому що у випадку, коли зловмисник накопичив достатнє число слідів енергоспоживання, він матиме багато випадків, де $r_{b[l]} = r$ і випадок, коли всі інші стани відіграватимуть роль шуму. Однак, виникає проблема, що кожне r_J впливатиме тільки на одне t_j протягом виконання алгоритму. Таким чином, якщо наведена вище атака успішна для розкриття $b[1]$-$b[0]$, то вона також може бути використана для знаходження усіх значень $b[l]$-$b[l\text{-}1]$, без істотного збільшення числа потрібних слідів енергоспоживання.

5. ЗАСЛІПЛЕННЯ ВІДКРИТИХ ДАНИХ *c*

Розглядаючи цей метод, можна запропонувати два варіанта цього методу: рандомізація цілих чисел та рандомізація поліному. Перший реалізує рандомізацію цілого *r* та неодноразово використовується для засліплення всіх $c_к$. Цей захід протидії маскує кореляцію між поліномом $c(X)$ та енергоспоживанням рандомізованого $c(X)$. Насправді, ця процедура має такий вигляд $(c(X)+R(x))*a(X)-R(X)*a(X)$, де $R(X)=[r,r,..,r]$. Оскільки $R(X)*a(X)=[dr \mod q, dr \mod q,...,dr \mod q]$, то можемо ліквідувати $R(X)*a(X)$ шляхом віднімання dr від кожного t_j.

Цей метод можна назвати досить прийнятним за рахунок незначних накладних витрат. Однак, потрібно бути обережними при використані засліплення у ситуації, коли енергоспоживання обчислюється за допомогою коду Хеммінга, тому що інший вид атаки CPA теоретично буде можливим у цьому випадку. Наприклад, вважатимемо, що енергоспоживання змінюється від найменш значущого біта кожного t_j. Спочатку пояснимо атаку CPA проти алгоритму без використання протидій. Як зазначалося вище, завдання зловмисника полягає у знаходженні вихідного відносного зсуву індексу *t*, яке показує $b[1]$- $b[0]$, $b[2]$-$b[1]$ і т. д. Тому візьмемо поліном $c^1,...,c^S$ та його сліди енергоспоживання $P^1,...,P^S$ зробимо припущення, що $b[1]$-$b[0]=w$ при $w \geq 1$, та перевіримо на наявність помітних кореляцій між $LSB(c_w^l + c_0^l)$ та P^l, де $LSB(x)$ – значення найменш значущого біта *x*. Цікавий факт те, що ця атака буде реалізована навіть якщо *r* додане до кожного $c_к$, $LSB((c_w^l + r)+(c_0^l + r)) = LSB(c_w^l + c_0^l)$. На рис. 2 показано, що пік з'являється серед коефіцієнтів кореляції, хоча це важко зробити на рис. 3, тому що енергоспоживання нашого процесору впливає більш швидше на відстань Хеммінга, ніж на код Хеммінга.

Решта завдання атаки, відновлення $b[2]$-$b[1]$, $b[3]$-$b[2]$ і т. д., ускладнюється в результаті втрати залежності *r* на *LSB*. Ця проблема може буде легко вирішена припущенням двох відносних зсувів водночас. Вважатимемо, що зловмисник

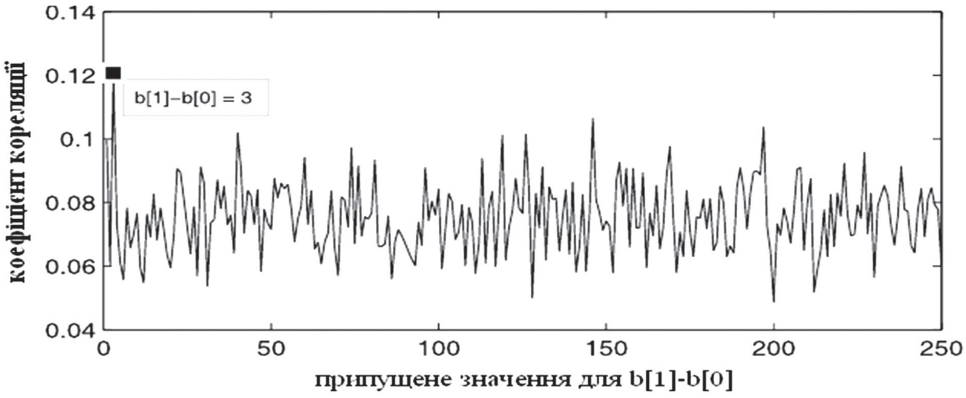


Рис. 2. Максимальна кореляція для кожного можливого припущення при моделі коду Хеммінга з *c*, який засліплений випадковим цілим числом

відновив $b[1]$-$b[0]=v$, використовуючи вищезазначений метод. Після чого зловмисник робить припущення $b[3]$-$b[1]=w_1$ та $b[3]$-$b[1]=w_2$ та знаходить кореляцію, використовуючи $LSB(c_{w_1+v}+c_{w1}+c_{w2}+c_0)$. Наприклад, v=3, w_1=3, w_2=2, див. рис. 2 [3]. Цей метод успішно ліквідовує ефект засліплення для r, тому що значення, з яким зловмисник має справу, складається з парного числа r. Хоча простір пошуку (w_1, w_2) буде більшим, ніж просте w, він все ще знаходиться у практичному діапазоні. Тому, розглядаючи перший метод з простим цілим r, можна вважати потенційним рішенням для розв'язання задачі рандомізації відкритих даних.

Розв'язати цю задачу може і наступний метод, він оснований на використані загального поліному $R(X)$, який безпосередньо і буде засліплюватиме $c(X)$. Вирахуємо $(c(X)+R(X))*a(X)$-$R(X)*a(X)=c(X)*a(X)$, використовуючи випадковий поліном $R(X)$. Для зменшення навантаження обчислення $R(X)*a(X)$ взяли за ідею [5] та [6]. Тобто спочатку обирається випадкове $R(X)$, обчислюється $S(X)=R(X)*a(X)$, та зберігається $R(X)$ та $S(X)$. Коли згортання $(c(X)+R(X))*a(X)$- $S(X)$ буде зроблено, $R(X)$ та $S(X)$ оновлюється шляхом обчислення $R(X) \leftarrow kR(x)$ та $S(X) \leftarrow kS(x)$ для випадкового κ. Тому можна використовувати другий метод як ефективну протидію проти CPA. На рисунку 3 показано максимальне значення коефіцієнта кореляції після застосування цієї протидії. Але все одно знаємо, що засліплення c не перешкодить реалізації SPA атаки.

6. ВИСНОВКИ ВІДНОСНО АТАКИ ДРУГОГО РОДУ

Проаналізувавши запропонований захід протидії, а саме рандомізацію вектора r_k, зловмисник може зробити висновок про ймовірність реалізації атаки CPA. Тобто є ймовірність того, що рандомізацію вектора r_k можна відокремити від сигналу енергоспоживання для отримання корисної інформації.

Спочатку розглянемо сутність атаки CPA. Завдання зловмисника полягає у відновленні $b[1]$-$b[0]$ для отримання множини b. Для цього зловмисник описує вираз енергоспоживання, використовуючи модель відстані Хеммінга(1), робить припущення P відносно значення енергоспоживання, тобто значення регістра, що змінюється під час виконання операції згортання поліномів.

$$P(y \to z) \approx mHD(y,z)+n = mHW(y \oplus z)+n, \quad (1)$$

де m – скалярний коефіцієнт посилення між відстанню Хеммінга та енергоспоживанням і n – незалежна зміна шуму.

Повернемося до рисунка 1 [3], де розглянуто приклад, за яким зловмисник робить припущення w відносно значення $b[1]$–$b[0]$. Його припущення будується на відстежуванні відмінностей кореляції між $P(r_k \to r_k + c_w)$ та $HD(r_k, r_k + c_w)$ при j=0 та кореляції між $P(r_k + c_w \to r_k + c_w + c_0)$ та $HD(r_k + c_w, r_k + c_w + c_0)$ при j=1. Усі припущення зловмисника можна подати у вигляді

$$HW(x \oplus (x+y)) \quad (2)$$

та звести до

$$HW(x \oplus (x+y)) = HW(y)+\epsilon, \quad (3)$$

де ϵ – імовірнісна залежність зсувів при операції згортання поліномів з використанням рандомізації вектора r_k.

Таким чином, у випадку, коли зловмисник отримав достатньо статистичних даних про операції згортання на деякій множині поліномів, він, проаналізувавши енергоспоживання отриманих операцій згортання та використовуючи вирази (1) та (2), може припустити, що можна знайти залежність зсувів при використанні рандомізованого вектора r_k. Це припущення сформоване на підставі складності вибору r_k та переповненні або переносі регістра зсуву при додаванні r_k до добутку поліномів. Потім зловмисник відфільтровує шум, маючи на увазі корисну інформацію про рандомізований вектор r_k, та отримує сигнал даних енергоспоживання операції згортання без реалізації заходів протидії атакам на енергоспоживання, проводить атаку спеціального виду [3], тим самим відновлюючи секретний ключ.

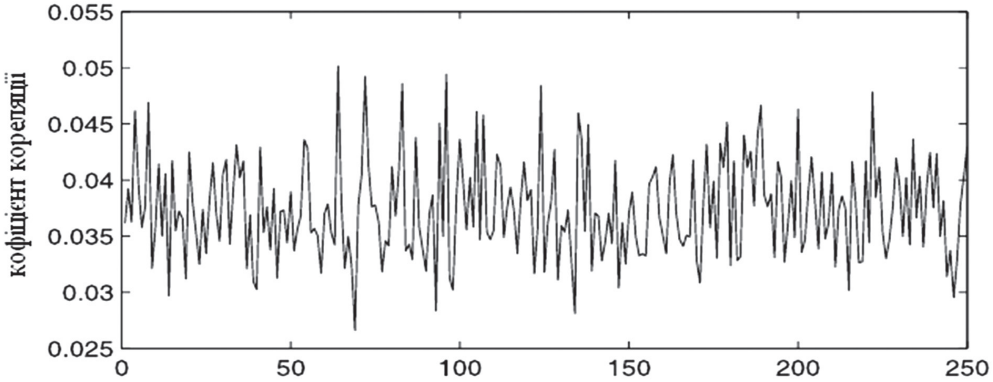


Рис. 3. Максимальна кореляція для кожного можливого припущення з c, який засліплений випадковим поліномом

7. РАНДОМІЗАЦІЯ *b*

Під час спостережень за поведінкою алгоритму 1 виявився цікавий факт, що зміна порядку елементів множини *b* не впливає на результат операції згортання. Цей факт відкриває ефективність використання рандомізації *b*, як міри протидії атаці CPA. Ця протидія може ефективно запобігти CPA, тому що CPA використовує позиції відносних зсувів, які додаються до c_0 між двома послідовними операціями в головному циклі, але мета порівняння та значення цих зсувів змінюється цією протидією при кожному виконанні. Наприклад, при ітерації $j = 0$ та $j = 1$, відносний зсув більше не дорівнює $b[1] - b[0]$, крім того він більше немає фіксованого значення. На рисунку 4 показано максимальне значення коефіцієнтів кореляції після застосування рандомізації *b*.

Проте необхідно відмітити, що рандомізація *b* може мати потенційну слабкість до SPA атаки, якщо зловмисник зробить декілька успішних припущень.

Нехай множина $b'[j]$ є елементом в *j* позиції *b* після перестановки. Тоді легко помітити, що пара ($b'[1]$, $b'[0]$) може мати $d(d–1)$ варіантів, тобто 2^{256} варіантів при $d = 48$. Якщо зловмисник зібрав достатнє число слідів енергоспоживання, то всі $d(d–1)$ варіанти також мають бути включені до зібраних даних.

Потім зловмисник представляє атаку SPA незалежно для кожного з слідів енергоспоживання, відновлюючи упорядковану множину *B* усіх можливих значень при відносному зсуві $b'[1] – b'[0]$. Хоча ця множина *b* не явно показує оригінальну множину *b*, але може показати деяку частину інформації про *b*, якщо *b* буде вибрано не обережно. Наприклад, вважатимемо, що при N=251 та d=48 останні елементи множини *B* матимуть вигляд [239,242,244,245,246,249]. Потім останній елемент 249 інформує зловмисника, що ($b[0]$,$b[47]$)=(0,249) або (1,250), тому що максимальний зсув має відбутися між $b[1]$ та $b[d\text{-}1]$. Це означає, що зловмисник відновить два вихідних елемента з 48-ми з імовірністю 0,5, та ця процедура може бути продовжена для визначення інших елементів, сконструювавши дерево пошуку(див. рис. 5). Для простоти пояснимо тільки першу гілку, тому що інша буде симетричною. Другий останній елемент у *B,* 246, породжує 3 дочірні гілки у дереві пошуку. Тобто ($b[0]$,$b[1]$,$b[46]$, $b[47]$)=(0,3,246,249); ($b[0]$,$b[1]$,$b[47]$)=(0,3,249) та $b[46] \neq 246$ ($b[0]$,$b[1]$,$b[46]$)=(0,3,246) та $b[1] \neq 3$. Але перша гілка може бути скорочена, тому що перша гілка не входить до множини *B* у точці, в якій зловмисник не може знайти відносний зсув $b[46]$-$b[1]$=243 у *B.* Виходячи з цього на наступному рівні, зловмисник отримує 4 секретних елемента з 12 варіантів, що істотно знижує пошук у просторі *b*. Хоча такий вид атаки буде корисний тільки при невеликій глибині дерева, тому що утворюється велика кількість гілок після певного рівня і обрізка практично неможлива, тому потрібно бути обережним при використанні такої протидії проти атак SPA.

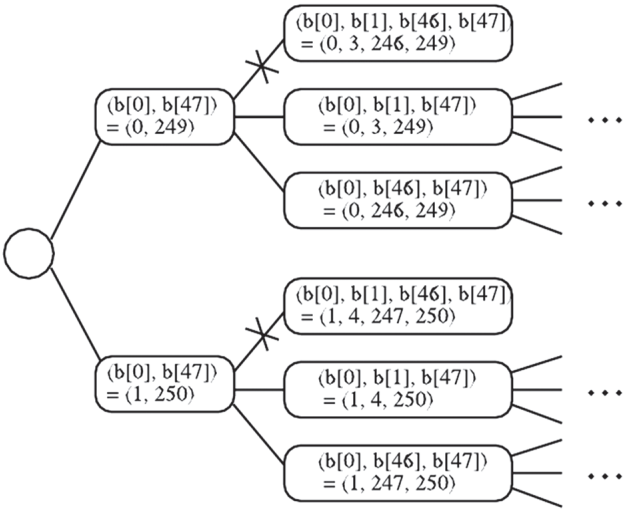


Рис. 5. Приклад дерева пошуку при B = [...,239,242,244,245,246,249]

8. АНАЛІЗ ПРОДУКТИВНОСТІ

Аналізуючи методи протидії, доцільно було б порівняти алгоритм [1] та алгоритми з різними методами протидії. На нашу думку ці реалізації можна порівняти, аналізуючи використану пам'ять та швидкість операції обчислення, тобто, доказуючи ефективність протидії до розглянутих атак, потрібно також враховувати вплив реалізації методів на властивості алгоритму.

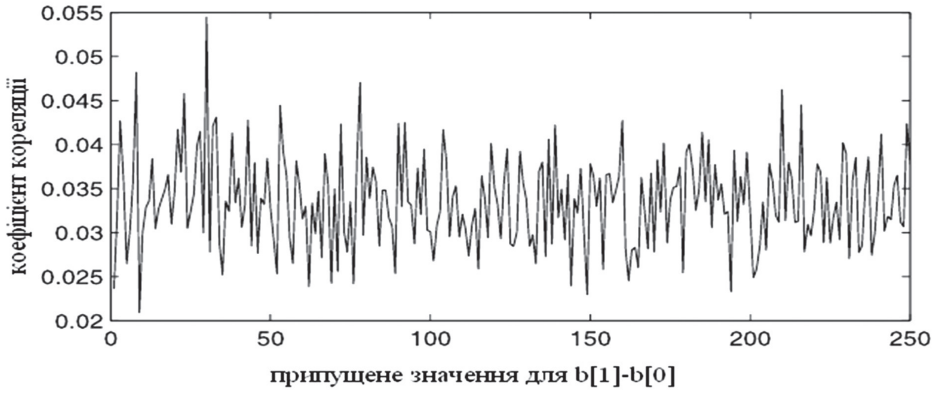


Рис. 4. Максимальна кореляція для кожного можливого припущення з рандомізованим *b*

Розглянувши табл. 1, можна проаналізувати продуктивність різних реалізації щодо виконання операції згортання $t(X)=c(X)*a(X)$, яка є вразливою до атак спеціального виду на енергоспоживання. Як видно з таблиці, що засліплення *c* з випадковим поліномом вимагає занадто багато пам'яті в порівнянні з іншими заходами протидії та більше використовує обчислювальний ресурс ніж інші заходи. Засліплення *c* з випадковим числом показує найвищу швидкість серед усіх заходів, але цей метод вразливий до атак типу CPA. Далі з таблиці видно, що порівнюючи використання пам'яті та швидкості обчислення, можна виділити реалізацію одночасно двох заходів: рандомізація *t* та рандомізація *b,* реалізація яких зведе нанівець можливість CPA та SPA.

Таблиця 1

Алгоритм згортання	ROM	RAM	Затрачений час
Алгоритм 1 (без застосування протидії)	3796	1063	67.383
Рандомізація *t*	3980	1063	71.191
Засліплення *c* з цілим *r*	4022	1064	69.043
Засліплення *c* з поліномом *R(X)*	4194	2067	101.953
Рандомізація *b*	4050	1063	70.117
Рандомізація *t* та рандомізація *b*	4106	1064	73.828

ВИСНОВОК

Таким чином, проаналізувавши методи протидії, виявили, що кожний метод має як переваги, так і недоліки, і назвати універсальний метод протидії, який би протидіяв однаково ефективно атакам спеціального виду, виявилося складно. Насамперед, методи ускладнюють завдання зловмисника з відновлення секретного ключа, але при реалізації методів протидії потрібно значну увагу приділяти впливу цих методів на сам алгоритм.

Рандомізація *t* ускладнює SPA та робить складнішим пошук кореляції, але обмежується вибором r_j, що може призвести до потенційних атак. Засліплення *c* може реалізовуватися двома варіантами, нести незначні накладні витрати, але вразливі до атак, які використовують для аналізу даних код Хеммінга, та при реалізації засліплення *c* за допомогою поліному потрібно більше RAM(вдвічі більше, ніж у інших випадках). Рандомізація *b* ефективна проти CPA, але не ефективна проти SPA, при атаці SPA – контролюючі вхідні дані та використовуючи дерево пошуку, буде досить легко знайти залежності та досягнути мети.

Література

[1] Hoffstein, J. "NTRU: A new high speed public key cryptosystem,"/J. Hoffstein, J. Pipher, J. Silverman Preprint// presented at the rump session of Crypto 96.

[2] Іваненко Д.В. Порівняльний аналіз сучасних асиметричних криптосистем/Д.В. Іваненко, О.В. Сєвєрінов//Системи управління, навігації та зв'язку. – К: ЦНДІ НіУ, 2012. – Вип.2(22).

[3] Іваненко Д.В. Класифікація атак спеціального виду на енергоспоживання/Д.В. Іваненко//Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 5 (103).

[4] Hoffstein J. "Optimizations for NTRU,"/ J. Hofftein, J. Silverman,// Proc.Public-Key Cryptography and Computational Number Theory,2000.

[5] Coron, J.S. "Resistance against differential power analysis for elliptic curve cryptosystems," / J.S.Coron, // Cryptographic Hardware and Embedded Systems — CHES'99, LNCS, vol.1717, pp.292–302, Springer, 1999.

[6] Okeya K., "Power analysis breaks elliptic curve cryptosystems even secure against the timing attack,"/ K.Okeya, K. Sakurai // Indocrypt 2000, LNCS, vol.1977, pp.178–190, Springer, 2000.

[7] Brier E. "WeierstraЯ elliptic curves and side-channel attacks,"/ E. Brier, M. Joye // Public Key Cryptography — PKC 2002, LNCS, vol.2274, pp.335–345, Springer, 2002.

[8] Fischer W., "Parallel scalar multiplication on general elliptic curves over Fp hedged against non-differential side-channel attacks,"/ W. Fischer, C. Giraud, E. Knudsen, J. Seifert // 2002. International Association for Cryptologic Research (IACR) Cryptology ePrint Archive 2002/007, http://eprint.iacr.org/2002/007.

[9] Izu T., "A fast parallel elliptic curve multiplication resistant against side channel attacks,"/ T. Izu, T.Takagi // Public Key Cryptography — PKC 2002, LNCS, vol.2274, pp.280–296, Springer, 2002.

[10] Okeya, K., "Elliptic curves with the montgomery-form and their cryptographic applications,"/ K. Okeya, H. Kurumatani, K. Sakurai,// Public Key Cryptography — PKC 2000, LNCS, vol.1751, pp.238–257, Springer, 2000.

[11] Liardet P. "Preventing SPA/DPA in ECC systems using the Jacobi form,"/ P. Liardet, N. Smart // Cryptographic Hardware and Embedded Systems — CHES 2001, LNCS, vol.2162, pp.391–401, Springer, 2001.

[12] Joye M. "Hessian elliptic curves and side-channel attacks,"/ M. Joye. J. Quisquater // Cryptographic Hardware and Embedded Systems — CHES 2001, LNCS, vol.2162, pp.402–410, Springer, 2001.

[13] Bernstein D., "Faster addition and doubling on elliptic curves," / D.Bernstein, T. Lange //Advances in Cryptology — Asiacrypt 2007, LNCS, vol.4833, pp.402–410, Springer, 2007.

[14] Chevallier-Mames B. "Low-cost solutions for preventing simple side-channel analysis: Side-channel atomicity,"/ B. Chevallier-Mames, M. Ciet, M. Joye,// IEEE Trans. Comput., vol.53, no.6, pp.760–768, 2004.

[15] Oswald E., "Randomized addition-subtraction chains as a countermeasure against power attacks,"/ E. Oswald, M. Aigner, // Cryptographic Hardware and Embedded Systems — CHES 2001, LNCS, vol.2162, pp.39–50, Springer, 2001.

[16] Moeller B., "Securing elliptic curve point multiplication against side-channel attacks,"/ B. Moeller // Information Security — ISC 2001, LNCS, vol.2200, pp.324–334, Springer, 2001.

[17] Hasan M., "Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems,"/ M. Hasan // IEEE Trans. Comput., vol.50, no.10, pp.1071–1083, 2001.

[18] Lee, M.K., "Sliding window mothod for NTRU,"/ M.K. Lee, J.W. Kim, J.E. Song, K. Park // Applied Cryptography and Network Security — ACNS 2007, LNCS, vol.4521, pp.432–442, Springer, 2007.

[19] Gama N., "Symplectic lattice reduction and NTRU,"/ N. Gama, N. Howgrave-Graham, P. Nguyen // Eurocrypt 2006, LNCS, vol.4004, pp.233–253, Springer, 2006.

Надійшла до редколегії 26.04.2013

Іваненко Дмитро Вікторович, аспірант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Наукові інтереси: криптографія, криптоаналіз.

УДК 621. 391:519.2:519.7

Методы противодействия атакам специального вида на криптопреобразования NTRU, которые основываются на анализе энергопотребления / Д.В. Иваненко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 292–298.

Анализируются существующие методы противодействия атакам специального вида, которые основываются на анализе энергопотребления. Рассматривается реализация атак специального вида на криптопреобразования NTRU, учитывая реализованные методы противодействия, такие как рандомизация и заслепление. Проведен анализ недостатков и преимуществ методов противодействия относительно таких атак специального вида как SPA, DPA и CPA, которые были направлены на криптопреобразования NTRU.

Ключевые слова: методы противодействия, атаки специального вида, CPA, DPA, SPA.

Табл.: 1. Ил.: 5. Библиогр.: 19 назв.

UDC 621. 391:519.2:519.7

Methods to counteract side channel attacks on the NTRU cryptotransformations, based on energy consumption analysis / D.V. Ivanenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 292–298.

The paper analyzes methods of counteracting side channel attacks which are based on energy consumption analysis. Implementing side channel attacks on NTRU cryptotransformation is considered taking into account the realized methods of counteracting such as randomization and blinding. Analyzing advantages and disadvantages of the methods of countracting such side channel attacks as CPA, SPA and DPA which were aimed at NTRU transformations is performed.

Keywords: methods of counteract, side channel attacks, CPA, SPA, DPA.

Tab.: 1. Fig.: 5. Ref.: 19 items.

УДК 004 056 55

ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОСИСТЕМ NTRU

Д.С. БАЛАГУРА, И.А. БАГЛАЕВ

Проводится исследование функционала инфраструктур открытых ключей в части использования криптографических протоколов. Определяется возможность использования криптосистем NTRU в инфраструктурах открытых ключей.

Ключевые слова: инфраструктуры открытых ключей, несимметричные криптосистемы, криптосистема NTRU, сертификат, личный ключ.

Инфраструктуры открытых ключей предназначены для управления ключевыми данными в различных, зачастую открытых информационных структурах. В таких случаях необходимо использовать несимметрические алгоритмы, кроме того, эти же алгоритмы зачастую используются и в элементах управления инфраструктурами открытых ключей. Таким образом, можно сказать, что функционирование инфраструктур открытых ключей напрямую зависит от выбора алгоритмов цифровой подписи и направленного шифрования. В данной работе представлен перспективный алгоритм шифрования и цифровой подписи NTRU, основанный на преобразования в кольцах усечённых полиномов, который может заменить действующие алгоритмы RSA, DSA, ECDSA и им подобные. Подробное описание всех этих алгоритмов и криптосистем можно найти в большом количестве различных источников [1, 2].

1. ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ NTRU В ИНФРАСТРУКТУРАХ ОТКРЫТЫХ КЛЮЧЕЙ

Основываясь на описании, анализе, требованиях, которые предъявляются к инфраструктурам открытых ключей в мире в целом и в Украине в частности, рассмотрим возможность использования в них NTRU криптосистем.

Как известно, инфраструктуры открытых ключей строятся и эксплуатируются для обеспечения конечных пользователей аутентичными и целостными копиями открытых ключей других пользователей (сертификатами открытых ключей). Исходя из назначения и задач инфраструктуры открытых ключей, в ней формируются центры сертификации ключей (ЦСК). Основными криптографическими операциями, использующимися ЦСК, являются операции цифровой подписи, а также направленного шифрования и симметрического шифрования. Естественно, использование симметрических алгоритмов и хеш-функций не зависит от используемых алгоритмов ЭЦП и направленного шифрования (кроме аспектов, связанных с общей стойкостью системы). Рассмотрим основные протоколы (действия) инфраструктур открытых ключей и алгоритмы, применяемые в них.

а) протокол отправки ключа на сертификацию/получения сертификата. В зависимости от класса системы и требований, предъявляемых к её защищённости, возможно использование ЭЦП и направленного шифрования;

б) сертификация открытого ключа ЦСК, серверов ЦСК, открытых ключей пользователей. Используется ЭЦП;

в) формирование списков отозванных сертификатов. Используется ЭЦП;

г) формирование меток времени. Используется ЭЦП;

д) формирование ответов на запросы по протоколу OCSP. Используется ЭЦП;

е) использование ключей и сертификатов конечными пользователями:

– цифровая подпись;

– направленное шифрование.

Таким образом, в протоколах инфраструктур открытых ключей из несимметричных алгоритмов используются алгоритмы электронной цифровой подписи и направленного шифрования. Учитывая тот факт, что криптосистемы на базе NTRU позволяют реализовывать как направленное шифрование, так и электронную цифровую подпись, то существует возможность построения инфраструктуры открытых ключей, которая будет полностью основываться на криптосистеме NTRU.

В последующих разделах рассматриваются различные аспекты построения инфраструктур открытых ключей с использованием NTRU, а также проводится сравнение протоколов ИОК, основывающихся на RSA, эллиптических кривых и NTRU [3, 4].

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОТОКОЛОВ ИНФРАСТРУКТУР ОТКРЫТЫХ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ NTRU

Протоколы управления сертификатами инфраструктуры открытых ключей требуются для обеспечения целостности, конфиденциальности, неотказуемости, подтверждения авторства, а также поддержки on-line взаимодействия между компонентами PKI.

Рассматриваемые протоколы должны удовлетворять следующим требованиям к управлению PKI[2]:

Управление PKI должно соответствовать стандарту ISO 9594-8 и связанным с ним расширениям сертификата.

Управление PKI должно соответствовать стандарту X.509 v3.

Должна быть возможность регулярного изменения любой пары ключей без влияния на какую-либо другую пару ключей.

Использование сервисов, обеспечивающих конфиденциальность, в протоколах управления PKI должно быть сведено к минимуму, чтобы уменьшить связанные с этим проблемы.

Протоколы управления PKI должны допускать использование различных криптографических алгоритмов, являющихся промышленными стандартами (специально включая только RSA, DSA, MD5, SHA-1). Это означает, что центры регистрации/сертификации или конечный пользователь PKI могут использовать для своей пары ключей любой набор алгоритмов.

Протоколы управления PKI должны поддерживать опубликование сертификатов, относящихся к конечным пользователям, центрам сертификации/регистрации.

Протоколы управления PKI должны поддерживать создание списков отозванных сертификатов, позволяя сертифицированным конечным пользователям посылать запросы на отмену сертификатов – это должно быть организовано так, чтобы невозможно было предпринять DoS-атаку.

Протоколы управления PKI должны использоваться поверх различных транспортных механизмов, включая LDAP, SMTP, HTTP, TCP/IP и FTP.

При запросе конечным пользователем сертификата, содержащего данное значение открытого ключа, конечный пользователь должен быть готов продемонстрировать обладание соответствующим значением закрытого ключа. Это можно организовать по-разному, в зависимости от типа алгоритма открытого ключа.

В зависимости от топологии ИОК, а также использования алгоритмов NTRU, возможны некоторые изменения в выдвигаемых требованиях. В табл. 1 приведены основные протоколы, использующие NTRU шифрование и цифровую подпись.

3. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ PKI, С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ КРИПТОСИСТЕМ

Как отмечалось ранее, криптосистема NTRU имеет некоторые преимущества, по сравнению с такими криптосистемами как RSA, DSA, EGSA, ECDSA и им подобным:

1. Процедура направленного зашифрования/расшифрования и подписи более эффективна как на программной, так и на аппаратной реализации.

Таблица 1

Основные протоколы ИОК, с использованием NTRU

Протоколы (действия)	NTRUEncrypt	NTRUSign
Отправка ключа на сертификацию Получение сертификата	+	+
Сертификация ключа ЦСК Сертификация конечных пользователей	+/-	+
Формирование CAC	-	+
Формирование меток времени	+/-	+
Формирование ответов на запросы (OCSP)	-	+
Использование ключей и сертификатов конечных пользователей	+	+

2. Процедура генерации ключа происходит гораздо быстрее, что позволяет использовать сеансовые ключи.

При равных длинах ключа, стойкость NTRU выше, чем стойкость RSA.

Сравнение стойкости основных ассиметричных систем.

Предварительная безопасность и временные сравнения NTRU и RSA представлены в табл. 2. RSA и NTRU работают в единицу времени на блок сообщения. Таким образом, в таблице 2 представлены значения времени зашифрования/расшифрования единичного блока сообщения [3].

Таблица 2

Сравнение RSA и NTRU

Система	Безопасность (MIPS за год)	Длина ключа (бит)	Генерация ключа (мс)	Шифрование (блок/с)	Расшифрование (блок/с)
RSA 512	$4{,}00 \cdot 10^{5}$	512	360	2441	122
NTRU 167	$2{,}08 \cdot 10^{6}$	1169	4.0	5941	2818
RSA 1024	$3{,}00 \cdot 10^{12}$	1024	1280	932	22
NTRU 263	$4{,}61 \cdot 10^{14}$	1841	7.5	3676	1619
RSA 2048	$3{,}00 \cdot 10^{21}$	2048	4195	310	3
RSA 4096	$2{,}00 \cdot 10^{33}$	4096	-	-	-
NTRU 503	$3{,}38 \cdot 10^{35}$	4024	17.3	1471	608

Однако NTRU имеет недостатки, связанные с выбором параметров и проверкой подписи:

1. Необходимость использования только рекомендованных параметров (табл. 3).

2. Вероятность возникновения ошибки при проверке подписи. Даже верно сформированная подпись не всегда пройдёт проверку.

3. Размер подписи варьируется.

Таблица 3

Рекомендуемые параметры NTRU

	N	p	q	d_f	d_g	d_r
NTRU167:3	167	3	128	61	20	18
NTRU251:3	251	3	128	50	24	16
NTRU503:3	503	3	256	216	72	55
NTRU167:2	167	2	127	45	35	18
NTRU251:2	251	2	127	35	35	22
NTRU503:2	503	2	253	155	100	65

Сравнение производительности ассиметричных алгоритмов

Табл. 4 содержит набор параметров с соответствующим для них уровнем безопасности, производительность (с точки зрения подписания/проверки подписи за секунду) для каждого из рекомендованного набора параметров.

Для уровня безопасности больше чем 80 бит, длина подписи NTRU меньше чем соответствующая RSA подпись, однако больше чем ECDSA. Секретный ключ NTRUSign содержит в себе полиномы f и g, а так же полиномы f_i, g_i и h_i. Для хранения полиномов f и g необходимо $2N$ бит, а для полинома h необходимо $N\log_2(q)$ бит. Таким образом, для параметров размером 80–128 бит необходимо $16N$ бит для хранения ключевых данных и $17N$ бит для параметров размером в 160–256 бит, что примерно в два раза больше чем длина открытого ключа.[4]

ВЫВОДЫ

Функционирующие инфраструктуры открытых ключей могут использовать различные несимметричные алгоритмы направленного шифрования и цифровой подписи. В зависимости от масштаба и топологии ИОК, выбирают те или иные алгоритмы, исходя из требований стойкости, скорости работы и т.д. В проделанной работе была рассмотрена перспективная несимметричная криптосистема NTRU, которая имеет как преимущества, так и недостатки.

В первую очередь, стоит отметить, что криптосистема NTRU отличается от остальных криптосистем математическим аппаратом и основана на алгебраической структуре полиномиального кольца, что позволяет выполнять процедуры шифрования, подписи и проверки подписи гораздо быстрее, чем алгоритм RSA. В то время как RSA с длиной ключа в 512 бит шифрует примерно 2441 блоков/с и создаёт 824 подписи/с, NTRU:167 шифрует 5941 блок/с и создаёт 13841 подпись/с. Эти данные свидетельствуют о высокой скорости работы алгоритма. При определённых наборах параметров NTRU и ECDSA, обеспечивающих примерно равную стойкость, криптосистема NTRU работает немного быстрее, чем криптосистема на эллиптических кривых. Вдобавок к этому, процедура генерации ключа происходит гораздо быстрее, чем в других криптосистемах, что позволяет использовать «одноразовые» ключи.

Важным моментом является относительно большая размерность ключа и общесистемных параметров, что, безусловно, приведёт к увеличению размера цифрового сертификата в целом.

В данный момент не существует инфраструктур открытых ключей, функционирующих с использованием криптосистемы NTRU. Одной из причин этому является проблема при подписании сообщения и соответственно при проверке подписи. Данные нюансы ставят под сомнение использование криптосистемы NTRU в инфраструктурах большого масштаба. Однако, дальнейшие исследования по нахождению определённых константных значений, исключающих или уменьшающих вероятность появления ошибки при проверке подписи, позволяют предположить, что криптосистема NTRU найдёт широкое применение в инфраструктурах открытых ключей.

Литература

[1] Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика *Ю.І. Горбенко, І.Д. Горбенко.* – Харків «Форт», 2010. – 608 с.

[2] Основы технологии PKI. *В.С. Горбатов, О.Ю. Полянская.* – М.:Горячая линия – Телеком, 2004. – 248 с.

[3] NTRU: A public key cryptosystem *J. Hoffstein, D. Lieman, J. Pipher, Joseph H. Silverman.* – M., 2004 – 17 с.

[4] Practical lattice-based cryptography: NTRUEncrypt and NTRUSign *J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte.* – M., 2005. – 42 с.

Поступила в редколлегию 14.05.2013

Таблица 4

Производительность NTRUSign для различных наборов параметров

Параметры				Открытый ключ и размер подписи				Подписей/с			Проверок/с		
k	N	d	q	NTRU	ECDSA ключ	ECDSA подпись	RSA	NTRU	ECDSA		NTRU	ECDSA	
80	157	29	256	1256	192	384	1024	4560	5140	0.89	15955	1349	11.83
112	197	28	256	1576	224	448	~2048	3466	3327	1.04	10133	883	11.48
128	223	32	256	1784	256	512	3072	2691	2093	1.28	7908	547	14.46
160	263	45	512	2367	320	640	4096	1722	-	-	5686	-	-
192	313	50	512	2817	384	768	7680	1276	752	1.69	4014	170	23.61
256	349	75	512	3141	512	1024	15360	833	436	1.91	3229	100	32.29

Балагура Дмитрий Сергеевич, фото и сведения об авторе см. на стр. 257.

Баглаев Игорь Алексеевич, студент кафедры Безопасности информационных технологий ХНУРЭ. Научные интересы: защита информации, инфраструктуры открытых ключей.

УДК 004 056 55

Інфраструктури відкритих ключів з використанням криптосистем NTRU / Д.С. Балагура, І.О. Баглаєв // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 299–302.

Здійснюється дослідження функціоналу інфраструктур відкритих ключів у частині використання криптографічних протоколів. Визначається можливість використання криптосистем NTRU в інфраструктурах відкритих ключів.

Ключові слова: інфраструктури відкритих ключів, несиметричні криптосистеми, криптосистема NTRU, сертифікат, особистий ключ.

Табл.: 4. Бібліогр.: 4 найм.

UDC 004 056 55

Public key infrastructures with the use of NTRU cryptosystems / Balagura D.S., Baglaev I.A. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 299–302.

Research of the functional of public key infrastructures regarding the use of cryptographic protocols is conducted. A possibility of using NTRU cryptosystems in public key infrastructures is defined.

Keywords: public key infrastructures, asymmetrical cryptosystems, NTRU cryptosystem, certificate, personal key.

Tab.: 4. Ref.: 4 items.

УДК 378.22

АНАЛІЗ СТАНУ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ «ІНФОРМАЦІЙНА БЕЗПЕКА»

Р.В. ПРОСКУРОВСЬКИЙ

Проведено огляд стану підготовки фахівців із захисту інформації в Україні. Аналіз галузевих стандартів вищої освіти України в галузі "Інформаційна безпека" показав, що є потреба у їх доопрацюванні та у другій редакції. Проведено короткий аналіз стану підготовки фахівців із захисту інформації в Казахстані та Росії.

Ключові слова: стандарти вищої освіти України в галузі "Інформаційна безпека", галузь знань 1701 "Інформаційна безпека", захист інформації, локальні і регіональні обчислювальні мережі, світовий інформаційний простір, фахівці із захисту інформації.

Сьогодні, в Україні, у зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені сотовим зв'язком, Інтернет став доступний для широкого кола користувачів, системи електронного документообігу в державних органах, система електронних платежів вже стали часткою повсякденного життя суспільства [1]. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Тривалий час методи захисту інформації розроблялися і використовувалися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн. Унаслідок цього процесу значно зросла потреба у фахівцях із захисту інформації [2].

Підготовкою спеціалістів із захисту інформації в радянські часи займалися виключно військові та спеціальні навчальні заклади, які територіально розташовувалися переважно на території Росії. Більшість випускників цих закладів були інженерами-програмістами, радіоінженерами, математиками, що займалися: забезпеченням безпеки системи урядового зв'язку, технічним та криптографічним захистом інформації, протидією іноземним технічним розвідкам. У СРСР займалися виключно захистом інформації, що є власністю держави.

Після розпаду СРСР, Україна, як і більшість республік Союзу, опинилася в кризовому стані в області підготовки фахівців із захисту інформації. Але з часом, починаються формуватися наукові школи та центри з підготовки фахівців із захисту інформації в Києві, Харкові та Львові. Основним кадровим потенціалом цих навчальних закладів стають військові вчені, та науковці, які за часи Союзу працювали на органи державної безпеки чи міністерство оборони, а також підключаються до роботи фахівці із суміжних, не закритих, у минулому напрямків досліджень.

Спеціалістів з інформаційної безпеки у навчальних закладах готували за тими галузями знань, напрямами та спеціальностями, які більш-менш підходили для цього. Згодом, для забезпечення підготовки спеціалістів із захисту інформації було відкрито галузь знань 1701 "Інформаційна безпека", яка включає три напрями та п'ять спеціальностей, що наведені у табл. 1 [3]. Значним кроком для якості та стандартизації підготовки фахівців із захисту інформації було зроблено створенням Галузевих стандартів вищої освіти для напрямів підготовки 6.170102 "Системи технічного захисту інформації" (СТЗІ) та 6.170103 "Управління інформаційною безпекою"

Таблиця 1

Бакалавр	Спеціаліст	Магістр
6.170101 Безпека інформаційних і комунікаційних систем	7.17010101 Безпека інформаційних і комунікаційних систем	8.17010101 Безпека інформаційних і комунікаційних систем
	7.17010102 Безпека державних інформаційних ресурсів	8.17010102 Безпека державних інформаційних ресурсів
6.170102 Системи технічного захисту інформації	7.17010201 Системи технічного захисту інформації, автоматизація її обробки	8.17010201 Системи технічного захисту інформації, автоматизація її обробки
6.170103 Управління інформаційною безпекою	7.17010301 Управління інформаційною безпекою	8.17010301 Управління інформаційною безпекою
	7.17010302 Адміністративний менеджмент у сфері захисту інформації	8.17010302 Адміністративний менеджмент у сфері захисту інформації

(УІБ) в 2009 році, і стандарт для напряму підготовки 6.170101 "Безпека інформаційних і комунікаційних систем" (БІКС) в 2010 році [4].

У цілому, в Україні, за даними на 2011 рік, підготовкою спеціалістів за напрямом підготовки: 6.170101 "Безпека інформаційних і комунікаційних систем" займається більше 15 ВНЗ; 6.170102 "Системи технічного захисту інформації" займається більше 15 ВНЗ; 6.170103 "Управління інформаційною безпекою" займається більше 10 ВНЗ [5].

Великим здобутком для України є те що, в переліку спеціальностей, за якими проводиться захист дисертацій на здобуття наукових ступенів кандидата наук і доктора наук, є спеціальності із захисту інформації (див. табл. 2). Основні наукові школи з підготовки наукових кадрів у галузі інформаційної безпеки, на сьогодні, знаходяться в Києві та Харкові.

Як показують результати 2010, 2011 років Всеукраїнської студентської олімпіади з напряму "Інформаційна безпека" високу підготовку фахівців підтримує: Харківський національний університет радіоелектроніки, Фізико-технічний інститут НТУУ "КПІ", Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ" [6].

У цілому, в Україні, зроблено основні та важливі кроки з побудови системи підготовки фахівців в області захисту інформації, але на жаль, є і недоліки, які потрібно усувати.

Досить болючою темою є неузгодженість та протиріччя використаних у зазначених галузевих стандартах термінів, хоча посилання на відповідні нормативно-правові акти присутні. Так термін "інформаційна безпека" має декілька тлумачень, викликають і ряд запитань терміни "комунікаційні системи", "інформаційно-комунікаційні системи", "управління (керування, менеджмент) інформаційною безпекою" тощо. Зазначимо, що в Україні, згідно з діючим законодавством, визначено такі терміни в:

– Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" [7] (інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів; інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле; телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб);

– Законі України "Про телекомунікації" [8] (інформаційна система загального доступу – сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних; інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації; телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням);

– Законі України "Про Концепцію Національної програми інформатизації" [9] (інформаційно-телекомунікаційна система органів державної влади включає високошвидкісні і звичайні канали зв'язку, розподілені і локальні мережі різного рівня та призначення);

– Указі Президента України "Про Положення про технічний захист інформації в

Таблиця 2

Шифр	Галузь науки, група спеціальностей, спеціальність	Галузь науки, за якою присуджується науковий ступінь
05.13.21	Системи захисту інформації	технічні
21.05.01	Інформаційна безпека держави	технічні

Таблиця 3

Бакалавр	Кваліфікація	Первинні посади
6.170101 Безпека інформаційних і комунікаційних систем	3439 Фахівець із захисту інформації в інформаційних і комунікаційних системах	– інспектор; – спеціаліст державної служби;
6.170102 Системи технічного захисту інформації	3439 Фахівець із технічного захисту інформації	– інженер; – спеціаліст державної служби; – фахівець; – фахівець з технічної експертизи; – оператор радіочастотного контролю; – інспектор електрозв'язку;
6.170103 Управління інформаційною безпекою	3439 Фахівець із організації інформаційної безпеки	– фахівець із організації захисту інформації з обмеженим доступом; – фахівець із режиму секретності; – фахівець з нагляду, охорони та інших видів захисту; – фахівець із організації інформаційної безпеки.

Україні" [10] (інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку).

Тому, використовувати в назві напряму підготовки та назвах дисциплін галузевого стандарту термін "комунікаційні системи" чи "інформаційно-комунікаційні системи" є не доречним.

В існуючих галузевих стандартах відсутній єдиний підхід щодо визначення первинних посад, які можуть займати фахівці (див. табл. 3), так у БІКС це посади інспектора та спеціаліста, але не інженера, в СТЗІ додається ще інженер, фахівець та оператор. Виходить "бакалавр" може займати посади оператора, інспектора, спеціаліста, інженера, фахівця, а які ж тоді посади займатиме "спеціаліст" та "магістр", підготовлений на базі даних освітньо-кваліфікаційних рівнів бакалавра.

Недоліки виявились і в наявному переліку видів діяльності за ДК 009-2005 (див. табл. 4) [11]. Найбільше питань виникає з напряму підготовки 6.170103 "Управління інформаційною безпекою", в якому згідно з кодом діяльності (див. табл. 4) технічних наук там немає взагалі, хоча згідно з "Переліком природничо-математичних та інженерно-технічних напрямів підготовки (спеціальностей) МОНмолодьспорту" [12], зазначений напрямок підготовки відноситься до інженерно-технічних напрямів. Так, у стандарті 6.170103 "Управління інформаційною безпекою" визначено, що випускники займатимуться діяльністю, пов'язаною з дослідженням і розробкою в галузі гуманітарних та суспільних наук, проводити наукові дослідження та розробки у галузі національної безпеки (мається на увазі інформаційно-психологічної безпеки), державного управління, фізичного виховання та спорту, соціологічних, політичних, філософських, економічних, юридичних, педагогічних, психологічних наук. 90 зі 146 кредитів, у стандарті, займають гуманітарні дисципліни, тобто більше 60%, фундаментальні дисципліни займають 35 кредитів – 25%, тобто тільки 21 кредит, а це тільки 15% стандарту є технічними дисциплінами. Отже, займатися діяльністю в технічній галузі, згідно з галузевим стандартом, не передбачено.

З 01.01.2012 року набрав чинності новий класифікатор видів економічної діяльності ДК 009-2010 [13] (зазначені галузеві стандарти, розроблені згідно з ДК 009-2005), згідно з яким кодам 73, 73.2, 73.20, 73.20.2 відповідає "Рекламна діяльність і дослідження кон'юнктури ринку", а не "Дослідження і розробки в галузі гуманітарних та суспільних наук" для стандарту 6.170103 "Управління інформаційною безпекою". Для стандарту 6.170102 "Системи технічного захисту інформації" є невідповідність в кодах, так кодам 30.02, 32.20 відповідає "Виробництво залізничних локомотивів і рухомого транспорту", коду 43.31 відповідає "Штукатурні роботи" тощо.

Як видно з табл. 5, ряд навчальних дисциплін є в наявності в усіх трьох стандартах, але з різними назвами та кредитами ECTS. Було б доречним, назви дисциплін привести до спільного знаменника (наприклад, у всіх трьох стандартах існують дисципліни за змістом однакові, але із різною назвою, наприклад «Захист інформації в інформаціно-комунікаційних системах», «Безпека інформаційних та комунікаційних систем», «Безпека інформаціно-комунікаційних систем»), а також і їх години, це було б дуже доречним для ВНЗ, які готують фахівців за двома, трьома напрямами підготовки, і які могли б читати ряд дисципліни потоком. У зв'язку з цим, у кожному із стандартів, за можливості було б доречно виділити біля 30 – 50% кредитів для дисциплін базових, спільних для галузі "Інформаційна безпека", назвати їх однаково і з рівними кредитами.

Таблиця 4

Бакалавр	Код діяльності за ДК 009-2005
6.170101 Безпека інформаційних і комунікаційних систем	72 Діяльність у сфері інформатизації 72.1 Консультування з питань інформатизації 72.2 Розроблення програмного забезпечення та консультування в цій сфері 72.4 Діяльність пов'язана з банками даних 72.6 Інша діяльність у сфері інформатизації 74.6 Проведення розслідувань та забезпечення безпеки
6.170102 Системи технічного захисту інформації	30.02 Виробництво ЕОМ та іншого устаткування для оброблення інформації 32.20 Виробництво передавальної апаратури 32.30 Виробництво апаратури для приймання, запису та відтворення звуку і зображення 33.20.1–3 Виробництво, монтаж, установлення, ремонт та технічний контроль вимірювальних приладів 43.31 Електромонтажні роботи 64.20 Діяльність зв'язку 74.60 Проведення розслідувань та забезпечення безпеки
6.170103 Управління інформаційною безпекою	73 Дослідження і розробки 73.2, 73.20, 73.20.2 Дослідження і розробки в галузі гуманітарних та суспільних наук Системне вивчення та творчі зусилля у трьох зазначених видах (73.2, 73.20, 73.20.2) наукових досліджень та розробок у галузі національної безпеки, державного управління, фізичного виховання та спорту, соціологічних, політичних, філософських, економічних, юридичних, педагогічних, психологічних наук

Таблиця 5

6.170101 Безпека інформаційних і комунікаційних систем	ECTS	6.170102 Системи технічного захисту інформації	ECTS	6.170103 Управління інформаційною безпекою	ECTS
Вища математика	19	Вища математика	19	Вища математика	19
Фізика	10	Фізика	12	Фізика	7
Інформаційні технології/ Операційні системи/ Архітектура комп'ютерних систем	4 4,5 3	Інформаційні технології	6,8	Інформатика	9
Прикладна криптологія	8,5	Криптографія та стеганографія	3,5	Основи криптографічного захисту інформації	4
Системи технічного захисту інформації	4,5	Методи та засоби захисту інформації/ Організаційне забезпечення технічного захисту інформації/ Технічні засоби охорони об'єктів/	10 4 4	Основи технічного захисту інформації	4
Основи теорії кіл, сигнали та процеси в електроніці	4	Основи теорії кіл, сигналів та процесів у системах ТЗІ	9,5		
Управління інформаційною безпекою	3,5	Управління інформаційною безпекою	2	Менеджмент інформаційної безпеки /Інформаційна безпека держави/ Забезпечення інформаційної безпеки держави/	4,5 8 7
Захист інформації в інформаціно-комунікаційних системах	12,5	Безпека інформаційних та комунікаційних систем	3,5	Безпека інформаційно-комунікаційних систем	4,5
Технології програмування	13			Технології програмування	3
Комплексні системи захисту інформації: проектування, впровадження, супровід	11	Проектування систем захисту інформації/ Організаційне забезпечення технічного захисту інформації	4,5 4	Комплексні системи захисту інформації	4
Теорія інформації та кодування	5	Теорія інформації та кодування	2,5		

У стандарті 6.170102 "Системи технічного захисту інформації" майже відсутні дисципліни, що відповідають за комп'ютерну підготовку, програмування та за питання несанкціонованого доступу до інформації в комп'ютерних системах та мережах (3,5 кредитів у дисципліні "Безпека інформаційних та комунікаційних систем" не достатньо), тобто стандарт вийшов якимось однобоким: акцент робиться тільки на один бік технічного захисту інформації: на канали витоку інформації, експлуатацію і проектування систем, пристроїв технічного захисту інформації та засобів зв'язку. На вивчення дисциплін "Проектування систем захисту інформації" та "Організаційне забезпечення технічного захисту інформації" виділено менше часу ніж на аналогічні в стандарті «Безпека інформаціно-комунікаційних систем».

Крім напрямків підготовки фахівців із захисту інформації в галузі "Інформаційна безпека", в Україні є ще напрям 6.040301 "Прикладна математика", на основі якого готуються спеціалісти та магістри за спеціальністю 7.04030104 (8.04030104) "Криптологія" (в Росії є "закритою" спеціальністю). Програма бакалаврської підготовки майбутніх "криптографів" насичена математичними дисциплінами, які для майбутніх фахівців не є актуальними, а дисципліни які, обов'язково необхідні в ході підготовки "криптографів" – відсутні в стандарті. Вважаю, що було б доречним перенести підготовку "криптографів" у галузь знань "Інформаційна безпека" та створити новий напрям підготовки з можливими назвами: "Прикладна криптологія", "Криптографія" або "Криптографічний захист інформації", і на цій базі готувати в подальшому спеціалістів та магістрів.

Стан системи підготовки фахівців із захисту інформації в країнах СНД різний. Як зазначається в [14], у Казахстані відсутня концепція підготовки кадрів у галузі інформаційної безпеки, відсутні спеціалізовані вчені ради із захисту кандидатських та докторських дисертацій в галузі захисту інформації. Спецслужби Казахстану, Білорусії частково готують фахівців з інформаційної безпеки в РФ ("Академия ФСО России", "ИКСИ Академии ФСБ России") та Україні (ІСЗЗІ НТУУ "КПІ").

У РФ є такі напрями підготовки фахівців: 090101 "Криптография", 090102 "Компьютерная безопасность", 090103 "Организация и технология защиты информации", 090104 "Комплексная защита объектов информатизации", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность

телекоммуникационных систем", 090107 "Противодействие техническим разведкам", 090900 "Информационная безопасность" та ін.

Як зазначає С.В. Карпенко в [15] у РФ існує достатньо багато концептуальних питань, пов'язаних із стандартизацією і системою підготовки фахівців з інформаційної безпеки, кваліфікація випускників за всіма напрямами не має системного стандартного підходу. Також, не зрозумілим є присутність в переліку спеціальностей РФ назв спеціальностей, які за своєю семантикою практично ідентичні, а також практично ідентичні і плани підготовки фахівців, однак спеціалісти мають різну кваліфікацію. На сьогодні час в освіті РФ проходить реорганізація напрямів підготовки, зокрема і за напрямом інформаційної безпеки. В РФ діють численні спеціалізовані вчені ради із захисту інформації, що гарантує підготовку нових вчених.

У цілому слід зазначити, що як в Україні, так і в РФ зроблено значні кроки для покращення стану підготовки фахівців в галузі інформаційної безпеки. Наявність галузевих стандартів вищої освіти є суттєвим здобутком для справи підготовки фахівців у галузі "Інформаційна безпека", разом з тим дані стандарти потребують ще деяких коректив та доопрацювань. Крім того було б добре усунути нестачу практично-прикладної підготовки з використання сучасних інформаційно-телекомунікаційних засобів, систем та технології.

Література

[1] Юдин О.К. Концепция подготовки специалистов в области информационной безопасности (часть 1) / http://itiss.info/publishing/experts-articles/48-yudin/127-koncepciya-podgotovki-specialistov-v-oblasti-informacionnoi-bezopasnosti-chast-1.

[2] Конспект лекцій до дисципліни Захист інформації для студентів спеціальностей 7.090701, 8.090701 "Радіотехніка", 7.090703, 8.090701 "Апаратура радіозв'язку, радіомовлення та телебачення" очної і безвідривної форм підготовки бакалаврів. / Укл.: Ю.С.Ямпольський, І.І.Маракова. – Одеса: ОНПУ, 2002. – 47 с.

[3] Постанова Кабінету міністрів України № 787 від 27.08.2010 р. "Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра".

[4] Освітні стандарти України / http://itiss.nau.edu.ua/standards-of-higher-education.

[5] Вступна кампанія 2011 "Галузі знань і напрями підготовки" 1701 Інформаційна безпека / http://vstup.info/2011/i2011b1701.html.

[6] Всеукраїнські олімпіади з напряму "Інформаційна безпека" / http://pti.kpi.ua/2010-11-04-12-51-34/-qi-q.

[7] Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" / http://zakon1.rada.gov.ua/laws/show/80/94-вр.

[8] Закон України "Про телекомунікації" / http://zakon2.rada.gov.ua/laws/show/1280-15.

[9] Законі України "Про Концепцію Національної програми інформатизації" / http://zakon2.rada.gov.ua/laws/show/75/98-вр.

[10] Указ Президента України "Про Положення про технічний захист інформації в Україні" / http://zakon2.rada.gov.ua/laws/show/1229/99.

[11] Національний класифікатор України. Класифікація видів економічної діяльності. ДК 009:2005 / http://zakon.nau.ua/doc/?code=va375202-05.

[12] Щодо переліку природничо-математичних та інженерно-технічних напрямів підготовки (спеціальностей) / http://osvita.ua/legislation/Vishya_osvita/28787/.

[13] Національний класифікатор України. Класифікація видів економічної діяльності. ДК 009:2010 / http://zakon.nau.ua/doc/?code=vb457609-10.

[14] Жангисина Г.Д., Аманжолова С.Т. Проблемы подготовки специалистов в области защиты информации республики казахстан / http://www.kazntu.kz/ru/publication/view/1899/93.

[15] Карпенко С.В. Концепция подготовки специалистов в области информационной безопасности / http://www.trn.ua/articles/2097/.

Надійшла до редколегії 17.05.2013

Проскуровський Роман Васильович, кандидат технічних наук, заступник завідувача кафедри БГІР ІСЗЗІ НТУУ «КПІ». Наукові інтереси: криптографічний захист інформації, захист інформації в інформаційно-телекомунікаційних системах.

УДК 378.22

Анализ состояния подготовки специалистов в области «Информационная безопасность» / Р.В. Проскуровский // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 303–307.

Проведен обзор состояния подготовки специалистов по защите информации в Украине. Анализ отраслевых стандартов высшего образования Украины в области «Информационная безопасность» показал, что существует потребность в их доработке и переиздании. Проведен анализ состояния подготовки специалистов и научных кадров по информационной безопасности в Казахстане и России.

Ключевые слова: стандарты высшего образования Украины в области «Информационная безопасность», отрасль знаний 1701 «Информационная безопасность», защита информации, локальные и региональные вычислительные сети, мировое информационное пространство, специалисты по защите информации.

Табл.: 5. Библиогр.: 15 назв.

УДК 378.22

Analyzing the state of training specialists in the information security field / R.V. Proskurovskyi // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 303–307.

The paper provides a review of the state of training specialists in the information security field in Ukraine. Analysis of the branch standards for higher education in Ukraine has shown a need for their improvement and reissuing. Specialists and scientific manpower training state analysis in the information security field in Kazakhstan and Russia is carried out.

Keywords: standards for higher education in Ukraine in the information security field, knowledge branch 1701 "Information security", information security, local area and regional computational networks, world information space, specialists in information security.

Tab.: 5. Ref.: 15 items.

СИСТЕМЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 621.3.06

СТРАТЕГИЯ ЗАЩИТЫ НЕПРЕРЫВНОЙ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ АНСАМБЛЯ КЛЮЧЕЙ НА ФОРМАЛЬНЫЕ ОТНОШЕНИЯ АНСАМБЛЕЙ

В.В. КОТЕНКО, С.В. КОТЕНКО, К.Е. РУМЯНЦЕВ, Ю.И. ГОРБЕНКО

Приводится фундаментальное обоснование стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей. Устанавливается, что применение стратегии впервые открывает возможность трехуровневой защиты непрерывной информации. Оценка эффективности защиты от криптоанализа на первом (начальном) уровне защиты показывает потенциальную возможность выполнения условий абсолютной недешифруемости путем соответствующего увеличения дисперсии ансамбля виртуальных ключей.

Ключевые слова: ансамбль ключей, виртуализация процесса защиты непрерывной информации, объём выборочного пространства ансамбля ключевых данных, трехуровневая защита непрерывной информации, энтропия виртуального ансамбля ключей.

ВВЕДЕНИЕ

Особенностью виртуализации процесса защиты непрерывной информации является возможность использования исходного ансамбля источника сообщений в качестве непрерывного ансамбля виртуализации [1]. Отображение модели защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей, следующее из условия реализации отмеченной возможности, приведено на рис. 1.

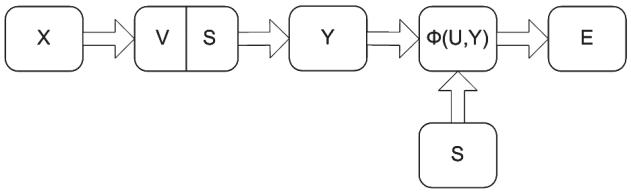


Рис. 1. Отображение модели защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей

Приведенное отображение показывает формальные функциональные отношения ансамблей, определяющих защиту непрерывной информации, при условии использования в качестве непрерывной составляющей ансамбля виртуализации исходного ансамбля источника сообщений *S*. Выборочное пространство ансамбля *V*, являющееся отображением ансамбля ключевых данных *X*, представляет дискретную составляющую ансамбля виртуализации *VS*. Дискретное выборочное пространство ансамбля *V* определяет функциональную форму изменения непрерывного выборочного пространства ансамбля *S*, которая отображается в дискретную форму выборочного пространства ансамбля ключевых последовательностей *Y*. Выборочное пространство ансамбля ключевых последовательностей *Y* используется для представления Φ_{CD} ансамбля сообщений виртуального дискретного источника $\hat{U}$, полученного в результате цифровой виртуализации непрерывного источника *S*, ансамблем криптограмм *E*.

Анализ отображения рис. 1 показывает, что разработка стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей невозможна без ответа на два основных вопроса:

1. Насколько включение исходного ансамбля сообщений *S* в состав ансамбля виртуализации способно влиять на стремление к бесконечности энтропии виртуального ансамбля ключей?
2. Какие ограничения на объём выборочного пространства ансамбля ключевых данных *X* накладывает включение в состав ансамбля виртуализации непрерывного ансамбля *S*?

1. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ

Теорема 1. Пусть скремблирование Φ_{CD} определяется ансамблем сообщений виртуального дискретного источника $\hat{U}^*$, ансамблем криптограмм E и виртуальным ансамблем ключей *K*, представленным совместным ансамблем *XYVZ*, где *VZ* – совместный дискретно-непрерывный ансамбль виртуализации. Тогда, если в совместный ансамбль виртуализации в качестве непрерывного ансамбля *Z* включить исходный ансамбль сообщений, то энтропия дискретно-непрерывного ансамбля виртуализации и энтропия виртуального ансамбля ключей будут стремиться к бесконечности, а вероятность продуктивного анализа ключа будет стремиться к нулю.

Доказательство. Энтропию дискретно-непрерывного ансамбля виртуализации согласно постановочной части теоремы можно представить как:

$$H[VZ] = H[VS] = H[S] + H[V/S]. \quad (1)$$

Из (1) следует, что при установленном стремлении абсолютной энтропии непрерывного ансамбля S к бесконечности, энтропия дискретно-непрерывного совместного ансамбля VS так же стремится к бесконечности.

Выражение для энтропии ансамбля ключей при включении в соответствующий ему совместный ансамбль непрерывного ансамбля S можно представить в виде:

$$H[K] = H[XYVS] = H[S] + H[XYV/S]. \quad (2)$$

Энтропия $H[S]$ в (2) представляет собой абсолютную энтропию непрерывного ансамбля, которая всегда стремится к бесконечности. Отсюда, согласно (2) энтропия виртуального ансамбля ключей $H[K]$ будет стремиться к бесконечности, а вероятность продуктивного анализа ключа будет стремиться к нулю. Что и требовалось доказать.

Теорема 2. Пусть скремблирование Φ_{CD} определяется ансамблем сообщений виртуального дискретного источника $\hat{U}^*$, ансамблем криптограмм E и виртуальным ансамблем ключей K, представленным совместным ансамблем $XYVZ$, где VZ – совместный дискретно-непрерывный ансамбль виртуализации. Тогда, включение в совместный ансамбль виртуализации в качестве непрерывного ансамбля Z исходного ансамбля сообщений S не устанавливает ограничений на объём выборочного пространства ансамбля ключевых данных X.

Доказательство. Так как ансамбль S непрерывный, то формирование виртуальных выборочных пространств совместного ансамбля ключей $XVSY$ обеспечивает абсолютную недешифруемость. Пусть выборочное пространство ансамбля X содержит N точек. Тогда выражение для средней взаимной условной вероятности $I[XV;Y/S]$ можно представить двумя способами:

$$I[XV;Y/S] = I[X;Y/S] + I[V;Y/SX], \quad (3)$$

$$I[XV;Y/S] = I[X;Y/SV] + I[V;Y/S]. \quad (4)$$

Последнее слагаемое в (3) и последнее слагаемое в (4) неотрицательны и ограничены сверху величиной $\max H[V] \le \log_2 N_V$. Отсюда, приравнивая правые части в (66) и (67), можно получить

$$\left| I[X;Y/SV] - I[X;Y/S] \right| \le \log_2 N_V. \quad (5)$$

Статистическая независимость X и Y определяет справедливость равенства

$$I[X;Y/S] = 0. \quad (6)$$

С учётом (6), неравенство (5) принимает вид:

$$\log_2 N_V \ge I[X;Y/SV]. \quad (7)$$

Так как среднее количество информации всегда положительно, знак модуля при переходе от (5) к (7) опускается.

Запишем выражение для $I[X;Y/SV]$ в виде

$$I[X;Y/SV] = H[X/SV] - H[X/YSV], \quad (8)$$

где

$$H[X/YSV] = \sum_x \sum_y \sum_v \int_s P(x,y,s,v) \log \frac{1}{P(x/y,s,v)} ds =$$

$$= \sum_x \sum_y \sum_v \int_s P(x,y,s,v) \log \frac{P(x,y,s)}{P(x,y,s,v)} ds.$$

Применяя цепную формулу для вероятности, имеем

$$H[X/YSV] =$$

$$= \sum_x \sum_y \sum_v \int_s P(x,y,s,v) \log \frac{P(y/sv)}{P(x/sv)\, p(y/xsv)} ds, \quad (9)$$

откуда, учитывая статистическую независимость X и Y

$P(v) = P(y/sv)$ для всех x, y, s, v при $P(xsv) > 0$, получаем

$$H[X/YSV] = \sum_x \sum_v \int_s P(xsv) \log \frac{1}{P(x/sv)} ds =$$

$$= H[X/SV].$$

С учётом этого неравенство (7) основании (8) приводится к виду:

$$\log_2 N_V \ge 0. \quad (10)$$

Принимая во внимание, что выборочное пространство ансамбля V является однозначной дискретной проекцией выборочного пространства ансамбля ключевых данных X, можно записать:

$$\log N_V = \log N,$$

откуда с учетом (10) следует:

$$N \ge 1. \quad (11)$$

Из (11) следует, что минимально возможное число точек выборочного пространства ансамбля V^*, обеспечивающее абсолютную недешифруемость, равно 1. Это значение можно рассматривать как предел сжатия виртуальной дискретной проекции выборочного пространства ансамбля ключевых данных X. Учитывая однозначную взаимосвязь элементов этой проекции с ключевыми данными, этот предел может быть отнесен и к выборочному пространству ансамбля ключевых данных. Это означает, что при виртуализации ансамбля ключей путем включения в состав совместного ансамбля виртуализации исходного ансамбля сообщений S абсолютная недешифруемость сохраняется при сокращении (сжатии) множества исходных ключей до одного ключа. Это означает, что включение в совместный ансамбль виртуализации в качестве непрерывного ансамбля Z исходного ансамбля сообщений S не устанавливает ограничений на объём выборочного пространства ансамбля ключевых данных X. Что и требовалось доказать.

2. ЭФФЕКТИВНОСТЬ СТРАТЕГИИ

На основании теорем 1–2 обобщенная модель реализации стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей может быть приведена к виду рис. 2.

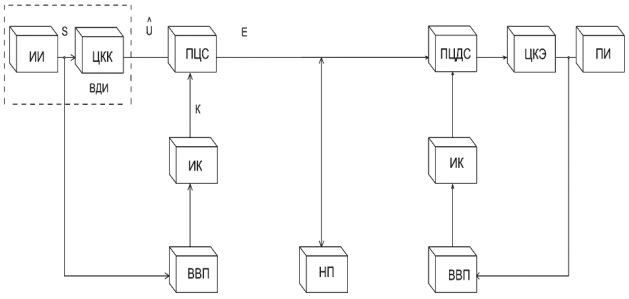


Рис. 2. Обобщенная модель реализации стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей

Нетрудно заметить, что полученная в [2] обобщенная схема адаптивного цифрового скремблирования является частным случаем реализации модели, приведенной на рис. 2.

Возможности обеспечения абсолютной недешифруемости, которые открывает реализация полученной модели (рис. 2), определяют актуальность поиска подходов к оценке стойкости и эффективности виртуального скремблирования, с позиций виртуализации ансамбля ключей. Проблема в данном случае состоит в специфике определения условной энтропии, определяющей стойкость защиты непрерывной информации $C\left(\Phi_{CD_X},S\right)$, входящей в состав выражения для эффективности защиты $D\left(\Phi_{CD_X},S\right)$:

$$D\left(\Phi_{CD_X},S\right)=D\left(\Phi_{CD_X},\hat{U}\right)=C\left(\Phi_{CD_X},\hat{U}\right)-H\left[Y_p\right],$$

$$C\left(\Phi_{CD_X},\hat{U}\right)=H\left[Y_p/E\right],$$

где Φ_{CD_X} – используемый шифр; U,E,Y_p – ансамбли сообщений, криптограмм и развернутых ключевых последовательностей, соответственно; X – ансамбль ключевых данных.

Условная энтропия $H[Y_p/E]$ характеризует среднюю неопределенность значения развернутого ключа $y_{i.}$ возникающую при несанкционированном перехвате соответствующего значения криптограммы $e_{i.}$. С физической точки зрения ее можно интерпретировать как среднее количество информации, которого не хватает для принятия однозначного правильного решения об y_i при криптоанализе $e_{i.}$. При этом особенностью виртуального скремблирования является то, что элементы дискретного ансамбля Y_p являются выборками реализаций $k_B(t)$ непрерывного выборочного пространства Z ансамбля виртуализации. Выборочное пространство Z, определяется дискретным выборочным пространством V ансамбля виртуализации, элементы которого, в свою очередь, однозначно определяются исходными ключами $k_И$ выборочного пространства ансамбля ключевых данных. Таким образом, криптоанализ виртуального скремблирования должен быть многоэтапным, включая:

– определение реализации виртуального ключа $k_B(t)$ по известным значениям криптограмм e_i;

– определение и вычисление значений параметров, задающих $k_B(t)$;

– определение исходного ключа по известным значениям задающих $k_B(t)$ параметров.

Последовательная реализация этих этапов в полном объеме являются необходимым условием успешного криптографического анализа при виртуализации процесса защиты непрерывной информации. В данном случае каждый этап может рассматриваться как уровень защиты. С этих позиций для успешного криптоанализа виртуального скремблирования необходимо преодолеть *трехуровневую защиту*, в отличие от одноуровневой, присущей для известных подходов. При этом значение $D_1\left(\Phi_{CD_X},S\right)$ и $C_1\left(\Phi_{CD_X},S\right)$ на первом уровне можно рассматривать как нижние границы диапазона изменения эффективности и стойкости виртуального скремблирования:

$$D_1\left(\Phi_{CD_X},S\right)=C_1\left(\Phi_{CD_X},S\right)-H[Y_p], \qquad (12)$$

$$C_1\left(\Phi_{CD_X},S\right)=H[\ \ _B/E]=$$

$$=\sum_i\int_{-\infty}^{\infty}p(e_i)P(k_{Bi}/e_i)\log\frac{1}{P(k_{Bi}/e_i)}dk_{Bi}. \qquad (13)$$

Здесь $P(k_{Bi}/e_i)$ является условной плотностью вероятности того, что при формировании значения e_i использовалось значение k_{Bi}. С позиций криптоанализа виртуального скремблирования, где на первом этапе стоит задача определения k_{Bi} по значениям e_i, виртуальный ключ можно рассматривать как результат искажения e_i некоторым гипотетическим случайным шумом, заданным процедурой скремблирования. С этих позиций задача криптоанализа сводится к оценке данного искажения. Если представить это искажение как аддитивное, то при гауссовской аппроксимации выражение для условной вероятности в (13) может быть определено как

$$P(k_{Bi}/e_i)=\frac{1}{\sqrt{2\pi\sigma_i^2}}\exp\left(-\frac{(k_{Bi}-e_i)^2}{\sigma_i^2}\right), \qquad (14)$$

где σ_i^2 — дисперсия условного распределения на i-м шаге криптоанализа.

Подставив (14) в (13), получаем

$$C_1\left(\Phi_{CD_X},S\right)=\sum_i p(e_i)\times$$

$$\times\left[\int_{-\infty}^{\infty}P(k_{Bi}/e_i)\log\sqrt{2\pi\sigma_i^2}dk_{Bi}+\right.$$

$$\left.\int_{-\infty}^{\infty}P(k_{Bi}/e_i)\frac{k_{Bi}-e_i}{2\sigma_i^2}\log e dk_{Bi}\right].$$

Откуда с учетом того, что

$$\int P(k_{Bi}/e_i)(k_{Bi}-e_i)dk_{Bi}=\sigma_i^2$$

имеем

$$C_1\left(\Phi_{CD_X},S\right)=\sum_i P(e_i)\left[\log\sqrt{2\pi\sigma_i^2}+\frac{1}{2}\log e\right]=$$

$$=\frac{1}{2}\log(2\pi e\sigma^2).$$

Принимаем во внимание, что дисперсия условного распределения при криптоанализе σ^2 с позиций введенных выше допущений может быть представлена как $\sigma^2=\sigma_K^2-\sigma_E^2$, где σ_K^2 — дисперсия виртуального ключа, а σ_E^2 — дисперсия значений криптограмм. Тогда выражение (13) можно привести к виду

$$C_1\left(\Phi_{CD_X},S\right)=\frac{1}{2}\log(2\pi e\,[\sigma_K^2-\sigma_E^2]). \qquad (15)$$

Подставив (14) в (12), получим выражение эффективности виртуальной защиты для первого уровня криптоанализа виртуального скремблирования

$$D_1\left(\Phi_{CD_X},S\right)=\frac{1}{2}\log(2\pi e\,[\sigma_K^2-\sigma_E^2])-H[Y_p]. \quad (16)$$

Выражения (15) и (16) определяют нижнюю границу стойкости и эффективности защиты непрерывной информации при виртуальном скремблировании. Их анализ позволяет прийти к ряду практически важных выводов.

Во-первых, виртуальное скремблирование способно обеспечить значения стойкости и эффективности защиты непрерывной информации, соответствующие области теоретической недешифруемости. Причем для этого достаточно выполнить практически просто реализуемое условие:

$$\frac{1}{2}\log\left(2\pi e\left(\sigma_K^2-\sigma_E^2\right)\right)\geq H[Y_p].$$

Во-вторых, дисперсия виртуального ключа может иметь определяющее значение при решении задач повышения эффективности виртуального скремблирования. Так, приближение значений σ_K^2 к бесконечно большим величинам, $\sigma_K^2\to\infty$, вызывает соответствующее увеличение эффективности скремблирования $D_1\left(\Phi_{CD_X},S\right)\to\infty$. Это свидетельствует о потенциальной возможности выполнения условий абсолютной недешифруемости при виртуальном скремблировании путем соответствующего увеличения дисперсии ансамбля виртуальных ключей.

Необходимо подчеркнуть, что данные выводы относятся только к первому уровню защиты от криптоанализа, которую обеспечивает виртуальное скремблирование. При этом из них следует, что даже на этом уровне виртуальное скремблирование способно обеспечивать эффективность скремблирования, значительно превышающую эффективность известных подходов к защите непрерывной информации.

ВЫВОДЫ

1. Особенностью виртуализации процесса защиты непрерывной информации является возможность использования в качестве непрерывного ансамбля виртуализации исходного ансамбля источника сообщений.

2. При виртуализации ансамбля ключей путем включения в состав совместного ансамбля виртуализации исходного ансамбля сообщений абсолютная недешифруемость сохраняется при сокращении (сжатии) множества исходных ключей до одного ключа.

3. Включение в совместный ансамбль виртуализации в качестве непрерывного ансамбля исходного ансамбля сообщений не устанавливает ограничений на объём выборочного пространства ансамбля ключевых данных.

4. Виртуализация процесса защиты непрерывной информации обеспечивает трехуровневую защиту с позиций криптоанализа ключа в отличие от одноуровневой, присущей для известных подходов.

5. Виртуальное скремблирование способно обеспечить значения стойкости и эффективности защиты непрерывной информации, соответствующие области теоретической недешифруемости.

Литература

[1] *Котенко В.В.* Теория виртуализации и защита телекоммуникаций: – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 244 с.

[2] *Котенко В.В., Румянцев К.Е.* Теория информации и защита телекоммуникаций: монография / Котенко В.В., Румянцев К.Е. – Ростов н/Д: Изд-во ЮФУ, 2009. – 369 с.

[3] *Величкин А.И.* Передача аналоговых сообщений по цифровым каналам. – М.: Радио и связь. – 1983. – 240 с.

[4] *Kotenko V., Rumjantsev K., Kotenko S.* "New Approach to Evaluate the Effectiveness of the Audio Information Protection for Determining the Identity of Virtual Speech Images". Proc. of the Second International Conference on Security of Information and Networks. The Association for Computing Machinery (ACM). New York. Publications Dept., ACM, Inc. 2009, pp. 235 –239.

[5] *Котенко В.В.* Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177–183.

[6] *Котенко В.В.* Теоретические основы виртуализации представления объектов, явлений и процессов // Информационное противодействие угрозам терроризма.: науч.-практ. журн., 2011, №17. – С. 32–48.

[7] *Котенко В.В.* Теоретические основы виртуализации информационных потоков // Информационное противодействие угрозам терроризма.: науч.-практ. журн., 2011, № 17. –С. 69–80.

[8] *Котенко В.В.* Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа // Информационное противодействие угрозам терроризма.: науч.-практ. журн., 2011, № 17. – С. 96–104.

Поступила в редколлегию 12.03.2013

Котенко Владимир Владимирович, фото и сведения об авторе см. на стр. 271.

Котенко Станислав Владимирович, фото и сведения об авторе см. на стр. 271.

Румянцев Константин Евгеньевич, фото и сведения об авторе см. на стр. 272.

Горбенко Юрий Иванович, фото и сведения об авторе см. на стр. 193.

УДК 621.3.06

Стратегія захисту безперервної інформації з позицій віртуалізації ансамблю ключів на формальні відносини ансамблів / В.В. Котенко, С.В. Котенко, К.Є. Румянцев, Ю.І. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 308–312.

Наводиться фундаментальне обґрунтування стратегії захисту безперервної інформації з позицій віртуалізації ансамблю ключів на формальні відносини ансамблів. Встановлюється, що застосування стратегії вперше відкриває можливість трирівневого захисту безперервної інформації. Оцінка ефективності захисту від криптоаналізу на першому (початковому) рівні захисту показує потенційну можливість виконання умов абсолютної недешифрувальності шляхом відповідного збільшення дисперсії ансамблю віртуальних ключів.

Ключові слова: ансамбль ключів, віртуалізація процесу захисту безперервної інформації, обсяг вибіркового простору ансамблю ключових даних, трирівневий захист безперервної інформації, ентропія віртуального ансамблю ключів.

Іл.: 2. Бібліогр.: 8 найм.

UDC 621.3.06

Continuous data protection strategy from the standpoint of virtualization of ensemble of keys on a formal relationship of ensembles / V.V. Kotenko, S.V. Kotenko, K.E. Rumyantsev, Yu.I. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 308–312.

Fundamental justification of continuous information protection strategy from the positions of virtualization of an ensemble of keys on of ensembles is given. It is found that the strategy application opens for the first time a formal relations possibility of three-level protection of continuous information. The assessment of efficiency of protection against cryptanalysis at the first (initial) level of protection shows a potential possibility of satisfying the conditions of an absolute indecipherability by the corresponding increase of dispersion of an ensemble of virtual keys.

Keywords: : ensemble of key data, virtualization of continuous information protection process, amount of sample space of key data ensemble, three-level protection of continuous information, entropy of a virtual key ensemble.

Fig.: 2. Ref.: 8 items.

УДК 621.391:519.2

МЕТОД ВОССТАНОВЛЕНИЯ СИСТЕМАТИЧЕСКИХ ЛИНЕЙНЫХ КОДОВ ПО НАБОРАМ ИСКАЖЕННЫХ КОДОВЫХ СЛОВ

А.Н. АЛЕКСЕЙЧУК, А.Ю. ГРЯЗНУХИН

Показано, что задача восстановления систематического линейного кода по набору искаженных кодовых слов, наблюдаемых на выходе двоичного симметричного канала связи, сводится к решению ряда систем линейных уравнений с искаженными правыми частями. Получены оценки сложности решения указанных систем уравнений. Представлены результаты вычислительных экспериментов по восстановлению кодов с малой плотностью проверок на четность.

Ключевые слова: восстановление линейных кодов, система уравнений с искаженными правыми частями, коды с малой плотностью проверок на четность.

ВВЕДЕНИЕ

Одной из практически важных задач в области информационной безопасности является разработка методов восстановления дискретных отображений по наблюдениям за их значениями. Как правило, в реальных условиях такие наблюдения производятся под воздействием шумов (случайных искажений, преднамеренных помех, внутренних сбоев и т.п.), что приводит к специфическим по своей постановке задачам. К их числу относится задача восстановления неизвестных систематических линейных кодов по наборам искаженных кодовых слов, наблюдаемых на выходе двоичного симметричного канала связи. Несмотря на то, что эта задача является естественной как с теоретической, так и с прикладной точек зрения, авторам не удалось найти упоминаний о ней в научных публикациях.

В настоящей статье показано, что эта задача сводится к решению ряда систем линейных уравнений (СЛУ) с искаженными правыми частями (с основами теории таких систем уравнений можно ознакомиться по работам [1, 2]). Показано также, что вероятности искажений в правых частях полученных систем зависят от максимальной плотности проверочных соотношений искомого кода, так что сложность его восстановления растет экспоненциально с ростом указанного параметра.

Проведенные вычислительные эксперименты свидетельствуют о том, что предложенный метод может быть эффективно применен на практике для восстановления линейных кодов с малой плотностью проверок на четность [3], длина и размерность которых не превышают нескольких сотен бит. В частности, если вероятности искажений в канале не превосходят 0,1, то для восстановления одного из таких кодов длины 128 и размерности 80 требуется примерно 15 секунд работы стандартной ЭВМ и не более 385 искаженных кодовых слов.

ПОСТАНОВКА ЗАДАЧИ И ОСНОВНЫЕ ТЕРЕТИЧЕСКИЕ РЕЗУЛЬТАТЫ

Пусть C – неизвестный двоичный линейный (n,k) – код с порождающей матрицей $G=(E_k,X)$, где E_k – единичная матрица порядка k, X – матрица размера $k\times(n-k)$, не содержащая нулевых столбцов. Наблюдается последовательность векторов

$$Y_i = U_i G \oplus \eta_i\ ,\ i\in\overline{1,m}\ , \qquad (1)$$

где U_i – независимые случайные равновероятные двоичные векторы длины k (информационные сообщения), $\eta_i=(\eta_{i,1},\dots,\eta_{i,n})$ – векторы искажений, координаты которых являются независимыми в совокупности и не зависящими от $U_1,\dots,U_m$ случайными величинами, распределенными по законам

$$\mathbf{P}\{\eta_{i,s}=0\}=1-\mathbf{P}\{\eta_{i,s}=1\}=1/2\cdot\left(1+\theta_{i,s}\right), \qquad (2)$$

где

$$\theta_{i,s}\ge\theta>0\ ,\ i\in\overline{1,m}\ ,\ s\in\overline{1,n}\ . \qquad (3)$$

Требуется восстановить матрицу X по известным значениям n,k,θ и последовательности (1).

Предлагаемый метод решения поставленной задачи заключается в построении систем линейных уравнений с искаженными правыми частями относительно столбцов матрицы X и решении этих систем с использованием известных алгоритмов. Для изложения метода введем ряд дополнительных обозначений.

Для любого натурального l обозначим V_l множество двоичных векторов длины l. Обозначим $Y_i^{(1)}$ и $Y_i^{(2)}$ подвекторы вектора Y_i, состоящие из его первых k и последних $n-k$ координат соответственно. Аналогичные обозначения введем для случайного вектора η_i, $i\in\overline{1,m}$. Положим $A_i=U_i\oplus\eta_i^{(1)}$, $\xi_i=\eta_i^{(1)}X\oplus\eta_i^{(2)}$, $i\in\overline{1,m}$.

Из формулы $G=(E_k,X)$ вытекает, что равенства (1) равносильны соотношениям

$$(Y_i^{(1)},Y_i^{(2)})=(U_i\oplus\eta_i^{(1)},\ U_iX\oplus\eta_i^{(2)})\ ,\ i\in\overline{1,m}\ ,$$

которые могут быть записаны в виде:

$$A_i=Y_i^{(1)}\ ,\ A_iX\oplus\xi_i=Y_i^{(2)}\ ,\ i\in\overline{1,m}\ . \qquad (4)$$

При этом в силу сделанных выше предположений о распределениях случайных векторов U_i, η_i, $i\in\overline{1,m}$, векторы $A_1,\dots,A_m$ независимы в совокупности и равномерно распределены на

множестве V_k, а векторы $\xi_1, \ldots, \xi_m$ независимы в совокупности и не зависят от $A_1, \ldots, A_m$.

Для того, чтобы придать соотношениям (4) более естественный вид, обозначим A матрицу, составленную из строк $A_1, \ldots, A_m$, x_j – j-й столбец матрицы X; положим

$$b^{(j)} = (Y_{1,j}^{(2)}, \ldots, Y_{m,j}^{(2)})^T, \ \xi^{(j)} = (\xi_{1,j}, \ldots, \xi_{m,j})^T,$$

где $Y_{i,j}^{(2)}$ и $\xi_{i,j}$ – j-е координаты векторов $Y_i^{(2)}$ и ξ_i соответственно, $i \in \overline{1,m}$, $j \in \overline{1,n-k}$. На основании вышеизложенного вектор x_j совпадает с истинным решением $x_j^{(0)}$ СЛУ с искаженными правыми частями

$$Ax = b^{(j)} = Ax_j^{(0)} \oplus \xi^{(j)}, \qquad (5)$$

где матрица A и вектор $b^{(j)}$ определяются непосредственно по набору слов вида (1):

$$A_i = Y_i^{(1)}, \ b^{(j)} = (Y_{1,j}^{(2)}, \ldots, Y_{m,j}^{(2)})^T, \ i \in \overline{1,m}, \ j \in \overline{1,n-k}. \qquad (6)$$

Далее, обозначим $\| x_j \|$ вес (число ненулевых координат) вектора x_j, $\rho_C = \max\limits_{1 \le j \le n-k} \| x_j \|$ и предположим, что код C удовлетворяет следующему условию:

$$\rho_C \le \rho, \qquad (7)$$

где $\rho \in \overline{2,k}$. Из равенства $\xi_i = \eta_i^{(1)} X \oplus \eta_i^{(2)}$ и условия (7) вытекает, что случайная величина $\xi_{i,j}$, $j \in \overline{1,n-k}$, является суммой не более $\rho+1$ независимых случайных величин $\eta_{i,s}$, $i \in \overline{1,m}$, $s \in \overline{1,n}$. Отсюда на основании формул (2), (3) следует, что для любых $i \in \overline{1,m}$, $j \in \overline{1,n-k}$ выполняется соотношение

$$\mathbf{P}\{\xi_{i,j} = 0\} = 1 - \mathbf{P}\{\xi_{i,j} = 1\} \ge 1/2 \cdot \left(1 + \theta^{1+\rho}\right). \qquad (8)$$

Итак, доказано следующее утверждение.

Утверждение 1. Пусть выполняются равенства (1), где случайные векторы U_i, η_i, $i \in \overline{1,m}$, удовлетворяют перечисленным выше условиям. Тогда для любого $j \in \overline{1,n-k}$ j-й столбец матрицы X является решением системы уравнений (5), где матрица A и вектор $b^{(j)}$ определяются по формулам (6). При этом A является случайной равновероятной двоичной матрицей размера $m \times k$, а координаты случайного вектора $\xi^{(j)}$ – независимы в совокупности и не зависят от матрицы A, $j \in \overline{1,n-k}$. Кроме того, при выполнении условия (7) справедлива формула (8).

Следствие. Пусть столбцы x_1, ..., x_{n-k} матрицы X удовлетворяют условию $\| x_j \| = \rho \ge 2$, $j \in \overline{1,n-k}$. Тогда восстановление этой матрицы по набору, состоящему из m слов кода C, искаженных в двоичном симметричном канале с вероятностью ошибки $p \in (0, 1/2)$, сводится к решению $n-k$ СЛУ с искаженными правыми частями (5), где $\xi^{(j)} = (\xi_{1,j}, \ldots, \xi_{m,j})^T$ – случайный вектор с независимыми в совокупности координатами, распределенными по закону

$$\mathbf{P}\{\xi_{i,j} = 1\} = 1 - \mathbf{P}\{\xi_{i,j} = 0\} = 1/2 \cdot (1 - (1-2p)^{\rho+1}),$$

$$i \in \overline{1,m}, \ j \in \overline{1,n-k}.$$

Таким образом, для нахождения по наблюдаемой последовательности (1) неизвестной матрицы X следует составить СЛУ с искаженными правыми частями (5) и решить их одним из известных методов. Отметим, что эти методы и алгоритмы можно разделить на универсальные (применимые к любым системам уравнений, независимо от вида их левых и правых частей) и алгоритмы, использующие особенности строения матриц коэффициентов и/или множеств искомых решений рассматриваемых СЛУ. К универсальным относятся метод максимума правдоподобия [1], алгоритмы "декодирования по информационным совокупностям" [4 – 6], трудоемкость которых зависит экспоненциально от числа неизвестных системы, а также ряд субэкспоненциальных алгоритмов [7 – 12], лучшие из которых требуют порядка $2^{O(k/\log k)}$ операций при том же количестве уравнений, где k – число неизвестных в системе. Если параметр ρ_C искомого кода удовлетворяет условию (7), где ρ – небольшая константа, то для решения систем уравнений (5) можно использовать метод максимума правдоподобия (трудоемкость которого в этом случае полиномиально зависит от k и экспоненциально от ρ) или один из недавно разработанных алгоритмов [13, 14], предназначенных для нахождения истинных решений СЛУ с искаженными правыми во множестве векторов заданного (малого) веса.

Остановимся подробнее на модификации метода максимума правдоподобия, состоящей в применении процедуры декодирования в ближайшее кодовое слово [1].

Рассмотрим СЛУ с искаженными правыми частями

$$Ax = b = Ax^{(0)} \oplus \xi, \qquad (9)$$

где A – случайная равновероятная двоичная матрица размера $m \times k$, $x^{(0)}$ – фиксированный неизвестный вектор, принадлежащий множеству $M \subseteq V_k$, а $\xi = (\xi_1, \ldots, \xi_m)^T$ – случайный вектор с независимыми в совокупности координатами, распределенными по закону $\mathbf{P}\{\xi_i = 0\} = 1 - \mathbf{P}\{\xi_i = 1\} = p_i = 1/2 \cdot (1 + \theta_i)$, где $\theta_i \ge \tilde{\theta} > 0$ для любого $i \in \overline{1,m}$. Докажем следующее вспомогательное утверждение.

Лемма. Пусть $\hat{x} \in M$ – вектор, удовлетворяющий условию

$$\nu_m(\hat{x}) = \min_{x \in M} \nu_m(x),$$

где $\nu_m(x) = \| Ax \oplus b \|$ для любого $x \in M$. Тогда при указанных выше предположениях относительно системы уравнений (9) справедливо неравенство

$$\mathbf{P}\{\hat{x} \ne x_0\} \le |M| \exp\{-1/8 \cdot \tilde{\theta}^2 m\}. \qquad (10)$$

Доказательство. Проводится по схеме, аналогичной доказательству теоремы 5.1 в [1]. Заметим, что для любого $C > 0$

$$\{\hat{x} \neq x^{(0)}\} \subseteq \{\nu_m(x^{(0)}) \geq C\} \cup \bigcup_{x \in M: x \neq x^{(0)}} \{\nu_m(x) < C\},$$

откуда следует, что

$$\mathbf{P}\{\hat{x} \neq x^{(0)}\} \leq \mathbf{P}\{\nu_m(x^{(0)}) \geq C\} + \\ + (|M|-1) \max_{x \in M: x \neq x^{(0)}} \mathbf{P}\{\nu_m(x) < C\}. \quad (11)$$

Далее, по условию леммы $\nu_m(x^{(0)})$ является суммой независимых случайных величин $\xi_1, \ldots, \xi_m$. Следовательно, полагая

$$C = 1/4 \cdot m\left(2 - \tilde{\theta}\right), \quad (12)$$

на основании неравенства Гефдинга [15] получим следующие соотношения:

$$\mathbf{P}\{\nu_m(x^{(0)}) \geq C\} = \mathbf{P}\{\sum_{i=1}^{m} \xi_i - \sum_{i=1}^{m} \mathbf{E}\xi_i \geq C - \sum_{i=1}^{m} p_i\} \leq \\ \leq \mathbf{P}\{\sum_{i=1}^{m} \xi_i - \sum_{i=1}^{m} \mathbf{E}\xi_i \geq 1/4 \cdot m\tilde{\theta}\} \leq \exp\{-1/8 \cdot m\tilde{\theta}^2\}. \quad (13)$$

Пусть теперь $x \in M$, $x \neq x^{(0)}$; тогда по условию леммы $\nu_m(x)$ является суммой независимых случайных величин $\eta_1, \ldots, \eta_m$, равномерно распределенных на множестве $\{0,1\}$. Следовательно, на основании формулы (12) и неравенства Гефдинга

$$\mathbf{P}\{\nu_m(x) < C\} = \mathbf{P}\{\sum_{i=1}^{m} \eta_i - \sum_{i=1}^{m} \mathbf{E}\eta_i < C - 1/2 \cdot m\} = \\ = \mathbf{P}\{\sum_{i=1}^{m} \eta_i - \sum_{i=1}^{m} \mathbf{E}\eta_i < -1/4 \cdot m\tilde{\theta}\} \leq \exp\{-1/8 \cdot m\tilde{\theta}^2\}. \quad (14)$$

Подставляя оценки (13), (14) в формулу (11), получим неравенство (10). Лемма доказана.

Предположим теперь, что столбцы $x_1, \ldots, x_{n-k}$ порождающей матрицы кода C принадлежат известному множеству $M \subseteq \{x \in V_k : 1 \leq \| x \| \leq \rho\}$, где $\rho \in \overline{2,k}$, и требуется восстановить их, решая СЛУ с искаженными правыми частями (5).

Алгоритм решения указанных СЛУ путем декодирования в ближайшее кодовое слово [1] состоит в вычислении для каждого $j \in \overline{1,n-k}$ всех значений $\| Ax \oplus b^{(j)} \|$, где $x \in M$, и нахождении вектора $\hat{x}_j \in M$ такого, что $\| A\hat{x}_j \oplus b^{(j)} \| = \min_{x \in M} \| Ax \oplus b^{(j)} \|$.

Следующее утверждение позволяет оценить эффективность этого алгоритма.

Утверждение 2. Пусть выполнено условие утверждения 1, $\delta \in (0,1)$ и

$$m = \left\lceil 8 \cdot \theta^{-2(1+\rho)} \ln\left((n-k)\,\delta^{-1}\,|M|\right)\right\rceil. \quad (15)$$

Тогда описанный алгоритм восстанавливает все столбцы матрицы X с вероятностью не менее $1-\delta$, используя $O\left(m(n-k)(\rho+1)|M|\right)$ двоичных операций. В частности, если $\| x_j \| = \rho$ для любого $j \in \overline{1,n-k}$, то двоичная временная сложность алгоритма равна

$$T = O\left(m(n-k)(\rho+1)\binom{k}{\rho}\right). \quad (16)$$

Доказательство. Положим $\tilde{\theta} = \theta^{1+\rho}$; тогда на основании леммы и соотношений (8)

$$\mathbf{P}\left(\bigcup_{j=1}^{n-k} \{\hat{x}_j \neq x_j\}\right) \leq \sum_{j=1}^{n-k} \mathbf{P}\{\hat{x}_j \neq x_j\} \leq \\ \leq (n-k)\,|M| \exp\{-1/8 \cdot \tilde{\theta}^2 m\} \leq \delta,$$

где последнее неравенство следует непосредственно из формулы (15). Таким образом, вероятность ошибки алгоритма не превосходит δ. Далее, для нахождения вектора $\hat{x}_j$, $j \in \overline{1,n-k}$, необходимо вычислить векторы $Ax \oplus b^{(j)}$ для всех $x \in M$ (что потребует не более $\rho m |M|$ двоичных операций) и найти их веса (что займет еще $O(m|M|)$ операций). Следовательно, суммарная трудоемкость алгоритма составляет $O\left(m(n-k)(\rho+1)|M|\right)$ двоичных операций, что и требовалось доказать.

Ниже, в табл. 1, 2 приведены численные значения (двоичного) логарифма трудоемкости алгоритма и объема материала, достаточного для восстановления с вероятностью не менее $1-\delta$ систематического линейного кода с параметрами n, k, ρ по набору кодовых слов, искаженных в двоичном симметричном канале с вероятностью ошибки $p = 1/2 \cdot (1-\theta)$.

Как видно из таблиц, количество слов, достаточное для восстановления кодов с указанными параметрами, во многих случаях заметно меньше их размерности k. Это объясняется высокой избыточностью описания класса рассматриваемых кодов, каждый из которых задается некоторой $k \times (n-k)$-матрицей X с малым числом ρ единиц в каждом столбце. Согласно табл. 2, для надежного (с вероятностью не менее 0,9) восстановления кода с параметрами $n = 4000$, $k = 2000$, $\rho = 3$ требуется выполнить не более 2^{53} двоичных операций, что находится в пределах возможностей современных супер-ЭВМ. При $n = 500$, $k = 300$, $\rho = 3$ трудоемкость изложенного алгоритма составляет не более 2^{41} операций, что позволяет говорить о возможности восстановления кодов с такими параметрами в реальном времени с помощью стандартных вычислительных средств.

РЕЗУЛЬТАТЫ ВЫЧИСЛИТЕЛЬНЫХ ЭКСПЕРИМЕНТОВ

Для проверки изложенных выше теоретических выводов были проведены вычислительные эксперименты по восстановлению ряда случайно сгенерированных кодов с малой плотностью проверок на четность. Эксперименты проводились с различными источниками сообщений, обладающими естественной (малой) избыточностью, и различными кодами, параметры которых удовлетворяют условиям $n \leq 256$, $k \leq 100$, $\rho \leq 5$.

В табл. 3, 4 показаны типичные результаты экспериментальных исследований, полученные для двух таких кодов C и C' с порождающими матрицами (E_{80}, X) и (E_{80}, X') соответственно, где X' и X'' – случайно сгенерированные 80×48 -матрицы, содержащие, соответственно, $\rho=3$ и $\rho=5$ единиц в каждом столбце.

Для каждой пары значений (p, m'), указанных в табл. 3, 225 раз выполнялась следующая процедура: m' независимых случайных сообщений источника кодировались кодом C; координаты полученных кодовых слов искажались независимо друг от друга с вероятностью p; полученный список из m' искаженных слов подавался на вход алгоритма, описанного в предыдущем пункте.

В результате выполнения алгоритма восстанавливались столбцы матрицы X. В последних трех колонках табл. 3 указаны средние значения (по всем 225 запускам) числа правильно

Таблица 1

Численные значения параметров (15), (16) ($n=500$, $k=300$, $\delta=0{,}1$)

p	ρ					
	3		4		5	
	m	$\log T$	m	$\log T$	m	$\log T$
0,100	1093	40,84	2029	47,95	3646	54,69
0,050	426	39,48	625	46,25	888	52,65
0,030	301	38,98	405	45,63	527	51,90
0,010	216	38,50	267	45,03	320	51,18
0,001	187	38,30	223	44,77	257	50,87

Таблица 2

Численные значения параметров (15), (16) ($n=4000$, $k=2000$, $\delta=0{,}1$)

p	ρ					
	3		4		5	
	m	$\log T$	m	$\log T$	m	$\log T$
0,100	1475	52,81	2767	62,68	5020	72,18
0,050	575	51,45	852	60,98	1222	70,14
0,030	406	50,95	552	60,35	725	69,39
0,010	291	50,47	364	59,75	440	68,67
0,001	252	50,26	304	59,49	354	68,35

Таблица 3

Результаты вычислительных экспериментов ($n=128$, $k=80$, $\rho=3$, $\delta=0{,}1$)

p	Теория		Эксперимент			
	m	$\log T$	m'	Среднее число восстановленных столбцов (%)	Среднее число восстановленных матриц (%)	Среднее время выполнения алгоритма (сек.)
0,100	836	32,67	304	99,81	92,00	13,96
			376	99,98	99,11	14,98
			384	100	100	15,55
			832	100	100	22,40
0,050	326	31,32	104	99,78	89,33	4,55
			120	99,98	99,11	4,72
			128	100	100	5,05
			320	100	100	10,00
0,030	231	30,82	64	99,70	87,11	3,38
			72	99,93	96,44	4,08
			80	100	100	4,12
			224	100	100	7,60
0,010	165	30,34	40	99,87	49,60	3,04
			48	99,99	93,00	3,11
			56	100	100	3,18
			160	100	100	6,00
0,001	143	30,13	24	99,16	68,89	2,28
			32	99,99	99,56	2,69
			40	100	100	3,75
			136	100	100	6,00

Таблица 4

Результаты вычислительных экспериментов ($n=128$, $k=80$, $\rho=5$, $\delta=0{,}1$)

p	Теория		Эксперимент			
	m	$\log T$	m'	Среднее число восстановленных столбцов (%)	Среднее число восстановленных матриц (%)	Среднее время выполнения алгоритма (сек.)
0,050	659	40,56	656	100	100	741,53
0,030	391	39,81	384	100	100	297,86
0,010	237	39,09	232	100	100	197,97
0,001	191	38,78	184	100	100	155,14

восстановленных столбцов, числа правильных восстановлений всей матрицы X и времени выполнения алгоритма. Для сравнения в левой части табл. 3 приведены значения параметров m и $\log T$, рассчитанные по формулам (15) и (16) соответственно. Вычисления проводились на ЭВМ с процессором Intel Pentium G620 (2,6 ГГц) и объемом оперативной памяти 2 Гб RAM (DDR3) на базе Windows XP (использовалась среда разработки Microsoft Visual C++ Studio 2008).

Отметим, что для моделирования источника использовалась заранее сформированная и протестированная случайная последовательность достаточно высокого качества. Количество запусков (равное 225) выбрано так, чтобы отклонение значений, приведенных в предпоследней колонке табл. 3, от теоретической вероятности правильного восстановления матрицы X не превышало 0,1 с надежностью не менее 0,9973 (см., например, [6], с. 87 – 88). В частности, если все 225 запусков завершены успешно, то при указанном в таблице количестве слов m' вероятность правильного восстановления матрицы X больше либо равна 0,9 с надежностью не менее 99,73 %.

Данные в табл. 4 получены аналогично, лишь с тем отличием, что вместо 225 запусков процедуры (для каждой пары входных значений (p, m')) выполнялось только 10. Последнее обстоятельство обусловлено заметным увеличением времени выполнения алгоритма с ростом параметра ρ .

Как видно из таблиц, для восстановления искомых матриц X' и X'' с заданной надежностью во всех случаях требуется меньше данных по сравнению с теоретической верхней границей (15). При этом время восстановления занимает от нескольких секунд до нескольких минут в зависимости от значений параметров p , ρ и m' .

Таким образом, предложенный метод может быть эффективно применен на практике для восстановления кодов с малой плотностью проверок на четность, длина и размерность которых не превышают нескольких сотен бит. Разработка более эффективных, по сравнению с описанным выше, алгоритмов восстановления кодов является задачей дальнейших исследований.

Литература

[1] Балакин Г.В. Введение в теорию случайных систем уравнений // Труды по дискретной математике. – М.: ТВП. – 1997. – Т. 1. – С. 1–18.

[2] Левитская А.А. Системы случайных уравнений над конечными алгебраическими структурами // Кибернетика и системный анализ. – 2005. – Т. 41, № 1. – С. 82–116.

[3] Галлагер Р.Г. Коды с малой плотностью проверок на четность / Р.Г. Галлагер // Сб. Теория кодирования. Пер. с англ. – М.: Мир, 1964. – С. 139–165.

[4] Евсеев С.Г. О сложности декодирования линейных кодов / С.Г. Евсеев // Проблемы передачи информации. – 1983. – Т. 19. – Вып. 1. – С. 1–8.

[5] Coffey J.T. The complexity of information set decoding / J.T. Coffey, R.M. Goodman // IEEE on Inform. Theory. – 1990. – Vol. 36. – P. 1031–1037.

[6] Becker A. Decoding random binary linear codes in $2^{n/20}$: how 1 + 1 = 0 improves information set decoding / A. Becker, A. Joux, A. May, A. Meurer // Cryptology ePrint Arhive, Report 2012/026, http: // eprint.iacr.org/2012/026.

[7] Коваленко І.М. Про алгоритм суб'експоненційної складності декодування сильно спотворених лінійних кодів / І.М. Коваленко // Доп. АН УРСР. Сер. А. – 1988. – № 10. – С. 16–17.

[8] Blum A. Noise-tolerant learning, the parity problem, and the statistical query model / A. Blum, A. Kalai, H. Wasserman // J. ACM. – 2003. – Vol. 50. – № 3. – P. 506–519.

[9] Wagner D. A generalized birthday problem / D. Wagner // Advances in Cryptology – CRYPTO'02, Proceedings. – Springer Verlag, 2002. – P. 288 – 303.

[10] Lyubashevsky V. The pariry problem in the presence of noise, decoding random linear codes, and the subset sum problem / V. Lyubashevsky // APPROX and RANDOM'05, Proceedings. – Springer Verlag, 2005. – P. 378–389.

[11] Fossorier M.P.C. A novel algorithm for solving the LPN problem and its application to security evaluation of the HB protocol for RFID authentication / M.P.C. Fossorier, M.J. Mihaljević, H. Imai, Y. Cui, K. Matsuura // Cryptology ePrint Arhive, Report 2006/197, http://eprint.iacr.org/2006/197.

[12] Minder L. The extended k-tree algorithm / L. Minder, A. Sinclair // The 19th Annual ACM-SIAM Symposium on Discrete Algorithms, Proceedings, 2009. – P. 586–595.

[13] Grigorescu E. On noise-tolerant learning of sparse parities and related problems / E. Grigorescu, L. Reysin, S. Vempala // The 22nd Internationale Conf. of Algorithmic learning Theory, Proceedings, 2011. – P. 413–424.

[14] Valliant G. Finding correlation in subquadratic time, with applications to learning parities and juntas with

noise / G. Valliant // Electronic Colloquium on Computational Complexity, Report 2012/006, http://eccc.hpi-eb.dc/report/2012/006.

[15] Hoeffding W. Probability inequalities for sums of bounded random variables / W. Hoeffding // J. Amer. Statist. Assoc. – 1963. – Vol. 58. – № 301. – P. 13–30.

[16] Ширяев А.Н. Вероятность: Учеб. пособие для вузов / А.Н. Ширяев. – М.: Наука, 1989. – 640 с.

Поступила в редколлегию 15.03.2013

Алексейчук Антон Николаевич, доктор технических наук, профессор кафедры Института специальной связи и защиты информации Национального технического университета Украины “КПИ”. Научные интересы: теоретическая криптография.

Грязнухин Александр Юрьевич, аспирант Института специальной связи и защиты информации Национального технического университета Украины “КПИ”. Научные интересы: корреляционный криптоанализ.

УДК 621.391:519.2

Метод відновлення систематичних лінійних кодів за наборами систематичних кодових слів / А.М. Олексійчук, О.Ю. Грязнухін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 313–318.

Показано, що задача відновлення систематичного лінійного коду за набором спотворених кодових слів, що спостерігаються на виході двійкового симетричного каналу зв’язку, зводиться до розв’язання ряду систем лінійних рівнянь зі спотвореними правими частинами. Отримано оцінки складності розв’язання зазначених систем рівнянь. Подано результати обчислювальних експериментів щодо відновлення кодів з малою щільністю перевірок на парність.

Ключові слова: відновлення лінійних кодів, система рівнянь зі спотвореними правими частинами, коди з малою щільністю перевірок на парність.

Бібліогр.: 16 найм.

UDC 621.391:519.95

A method of restoring systematic linear codes by samples of noisy code words / A.N. Alekseychuk, A.Yu. Gryaznukhin // Applied Radio Electronics: Sci. Journ. – 2013. Vol. 12. – № 2. – P. 313–318.

It is shown that the problem of restoring a systematic linear code by samples of noisy code words observed at the output of a binary symmetric channel can be reduced to solving of some systems of linear equations with noised right-hand sides. Estimations of comlexity of an algorithm for solving the said systems of equations are obtained. Results of experiments with computer simulation on retrieving codes with low-density parity-checks in the presence of noise are obtained.

Keywords: restoring of linear codes, system of linear equations with noised right-hand sides, low-density parity-check codes.

Ref.: 16 items.

УДК 621.391

МНОГОМЕРНЫЕ СПЕКТРЫ ДЛЯ ОПИСАНИЯ КАСКАДНЫХ КОДОВ В ЧАСТОТНОЙ ОБЛАСТИ

А.А. КУЗНЕЦОВ, С.И. ПРИХОДЬКО, БИЛАЛ ХАМЗЕ

Рассматривается математический аппарат многомерного дискретного преобразования Фурье в конечных полях. Исследуются методы описания линейных блоковых кодов в частотной области. Показано, что, в отличие от итеративных кодов (кодов-произведений) каскадные коды в общем случае не могут быть описаны в частотной области в терминах многомерных спектров. Получены аналитические выражения, устанавливающие взаимно-однозначное функциональное соответствие спектра последовательности над конечным полем и спектров соответствующих слов, полученных ограничением этого слова на подполе. Получено общее решение задачи представления каскадных кодов в частотной области, что позволит, используя выведенные аналитические зависимости компонентов многомерных спектров, строить в частотной области вычислительно эффективные алгоритмы кодирования и декодирования.

Ключевые слова: многомерное дискретное преобразование Фурье, каскадные коды, конечные поля.

1. ПОСТАНОВКА ПРОБЛЕМЫ В ОБЩЕМ ВИДЕ И АНАЛИЗ ЛИТЕРАТУРЫ

Математический аппарат дискретного преобразования Фурье в полях Галуа используется в современной теории помехоустойчивого кодирования как для описания в частотной области наиболее важных в прикладном отношении блоковых кодов, так и для построения новых кодовых конструкций с улучшенными свойствами [1–4]. За счет применения алгоритмов быстрого преобразования Фурье удается существенно сократить вычислительную сложность алгоритмов кодирования и декодирования, а также реализовать некоторые вычислительные процессы параллельно [4, 5].

Преобразования Фурье в конечных полях могут быть обобщены и на многомерный случай. Если кодовые слова блоковых кодов представимы в виде кодовых многочленов от нескольких переменных, а соответствующие кодовые символы записываются некоторой многомерной матрицей, тогда математический аппарат многомерных спектров, как правило, позволяет задавать коды в многомерной частотной области. К кодам, допускающим такое описание, относятся простейшие итеративные коды (коды-произведения), для которых перенос вычислений в многомерную частотную область позволяет повысить вычислительную эффективность алгоритмов кодирования-декодирования и выполнить многие операции параллельно [2, 3]. В то же время кодовые соотношения итеративных кодов далеки от оптимальных, что и объясняет их малое практическое использование [1–3].

Наибольшее распространение в технике помехоустойчивого кодирования получили т.н. каскадные коды, в конструкции которых используются два кода – код внутренней (первой) ступени над конечным полем $GF(q)$ и код внешней (второй) ступени над расширенным полем $GF(q^m)$ [1–3]. Полученный блоковый код определен над полем $GF(q)$, однако при формировании кодовых слов и их декодировании выполняются преобразования как над полем $GF(q)$, так и над его расширением $GF(q^m)$. Кодовые слова каскадного кода также представляют в виде матрицы, однако математический аппарат многомерных спектров к каскадным кодам не применим. Невозможно использовать и быстрые многомерные преобразования Фурье, т.е. получить тот эффект, который дают в технике помехоустойчивого кодирования преобразования в частотной области. Разрешению этого противоречия и посвящена данная работа.

Таким образом, *целью статьи* является развитие математического аппарата многомерных спектров для представления каскадных кодовых конструкций в частотной области и реализации на их основе эффективных алгоритмов кодирования и декодирования.

Работа структурирована следующим образом. В п. 2 приводятся основные положения и аналитические соотношения для дискретного преобразования Фурье в конечных полях, показана их связь с полиномиальным описанием блоковых кодов. В п. 3 преобразования Фурье обобщены на многомерный случай. На примере итеративного кода дается описание многомерных кодов в частотной области. Показано, что для каскадных кодов соответствующее представление получить не удается. П. 4 посвящен решению этой задачи. Через введение взаимно-однозначного функционального соответствия спектров кодовых слов произвольного вектора над конечным полем и спектров его слов-ограничений на произвольное подполе удается получить аналитические выражения, которые дополняют математический аппарат многомерных спектров, что позволяет дать описание каскадных кодов в частотной области. В п. 5 полученные результаты обобщаются, обсуждается их прикладное значение для реализации вычислительно эффективных алгоритмов кодирования и декодирования каскадными кодами. Все

сформулированные утверждения по тексту работы дополняются примерами, которые наглядно демонстрируют справедливость приведенных рассуждений и упрощают их восприятие.

2. ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ В КОНЕЧНЫХ ПОЛЯХ

Преобразование Фурье играет важнейшую роль в развитии современных методов теории обработки и передачи информации. В частности, для обработки и исследования сигналов, непрерывных во времени и принимающих вещественные и комплексные значения, используют интегральное преобразование Фурье [6, 7]. Для цифровой обработки сигналов, дискретных во времени используют дискретное преобразование Фурье [3–7]:

$$X_k = \sum_{j=0}^{n-1} e^{\frac{-2\pi i}{n} jk} x_j, k = 0,...,n-1, \quad (1)$$

$$x_j = \frac{1}{n}\sum_{k=0}^{n-1} e^{\frac{2\pi i}{n} jk} X_k, j = 0,...,n-1, \quad (2)$$

где n — количество значений сигнала и компонент разложения (спектра); $x = \{x_j, j = 0,...,n-1\}$ — значения сигнала в дискретных временных точках с номерами $j = 0,...,n-1$; $X = \{X_k, k = 0,...,n-1\}$ — n комплексных амплитуд синусоидальных сигналов, слагающих исходный сигнал; k —индекс частоты.

Для многих длин последовательностей определено также преобразование Фурье в полях Галуа, которое представляет собой развитый аналитический аппарат, используемый для описания блоковых кодов в частотной области, исследования их корректирующих свойств, построения вычислительно эффективных алгоритмов кодирования и декодирования [3].

Ядром дискретного преобразования Фурье в (1) и (2) является комплексный корень n-й степени из единицы $e^{\frac{-2\pi i}{n}}$. Проводя аналогию с конечным полем, в котором элемент α порядка n является корнем n-й степени из единицы, в работе [3] введено следующее определение дискретного преобразования Фурье над полями Галуа.

Пусть $v = \{v_i, i = 0,...,n-1\}$ — вектор над $GF(q)$, где n делит $q^m - 1$ при некотором m и пусть α — элемент порядка n в поле $GF(q^m)$. Преобразование Фурье в поле Галуа вектора v определяется как вектор $c = \{c_j, j = 0,...,n-1\}$ над $GF(q^m)$, задаваемый равенствами [3]:

$$c_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i, j = 0,...,n-1. \quad (3)$$

Дискретный индекс i в (1) принято назвать временем, а v — временной функцией или сигналом. Соответствующий индекс j принято назвать частотой, а c — частотной функцией или спектром [3].

Порядок элемента $\alpha \in GF(q^m)$ в (3) обязан быть делителем $q^m - 1$, следовательно, в отличие от поля комплексных чисел, в конечном поле преобразование Фурье определено не для любой длины, а только для соответствующих делителей $q^m - 1$. Наиболее важную в прикладном отношении роль играет выбор в качестве $\alpha \in GF(q^m)$ примитивного элемента с максимальным порядком $n = q^m - 1$. В общем случае в качестве длины n может быть выбран произвольный делитель $q^m - 1$ для некоторого положительного целого m и элемента $\alpha \in GF(q^m)$ порядка n в качестве ядра преобразования. Спектр в этом случае будет определен над расширением $GF(q^m)$, хотя и будет содержать лишь элементы порядка n из этого поля.

Таким образом, над полем $GF(q)$ вектор v и его спектр c связаны соотношениями [3]:

$$c_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i, \quad (4)$$

$$v_i = \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{-ij} c_j, \quad (5)$$

где n интерпретируется как элемент поля $GF(q)$, $n \mid (q^m - 1)$, а $c_j \in GF(q^m)$.

Так как сигнал v определен над полем $GF(q)$, а его спектр A определен над расширением $GF(q^m)$, не все векторы над $GF(q^m)$ могут быть спектрами каких либо сигналов над $GF(q)$. Обратное преобразование Фурье сигнала c над $GF(q^m)$ является вектором v с компонентами из $GF(q)$ тогда и только тогда, когда выполняются следующие равенства (ограничения сопряженности):

$$c_j^q = c_{qj \bmod n}, j = 0,...,n-1. \quad (6)$$

Действительно, согласно малой теореме Ферма,

$$c_j^q = \left(\sum_{i=0}^{n-1} \alpha^{ij} v_i\right)^q = \sum_{i=0}^{n-1} \alpha^{i(qj)} v_i = c_{qj \bmod n}, j = 0,...,n-1.$$

Разобьем числа $0,...,n-1$ по $\bmod n$ на подмножества [3]:

$$A_j = \{j, jq, ..., jq^{m_j - 1}\}, \quad (7)$$

где m_j — наименьшее положительное целое, удовлетворяющее равенству $jq^{m_j - 1} = j \bmod n$, в силу конечности поля такое m_j всегда существует.

Множество A_j выделяет в спектре такое множество частот, называемых хордой, что если сигнал принимает значения в поле $GF(q)$, то значение спектра в одной из частот хорды определяет значения спектра при всех частотах этой хорды [3]. Другими словами, для того, чтобы задать сигнал через обратное преобразование Фурье (5) достаточно определить все хорды (7) с учетом ограничений (6). Выбор хорды A_j соответствует определению такого минимального многочлена

$f_{\alpha^j}(x)$, корнями которого являются все элементы α^{jq^s}, $s = 0,...,m_j - 1$:

$$f_{\alpha^j}(x) = \prod_{s=0}^{m_j-1} (x - \alpha^{jq^s}). \quad (8)$$

Рассмотренные преобразования широко используются в теории помехоустойчивого кодирования для описания кодов в частотной области и для исследования их свойств. Например, наиболее важные в прикладном отношении полиномиальные коды задаются в частотной области через определенные нулевые компоненты спектра их кодовых слов.

Если элементы вектора v заданы в виде коэффициентов многочлена $v(x)$:

$$v(x) = v_0 + v_1 x + ... + v_{n-1} x^{n-1},$$

тогда с помощью преобразования Фурье в поле Галуа он может быть преобразован в многочлен

$$c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1},$$

который называется спектральным многочленом или ассоциированным с многочленом $v(x)$ [3].

Свойства спектра тесно связаны с корнями многочленов [3]:

– элемент α^j является корнем многочлена $v(x)$ тогда и только тогда, когда j-я частотная компонента c_j равна нулю.

– элемент α^{-i} является корнем многочлена $c(x)$ тогда и только тогда, когда i-я временная компонента v_i равна нулю.

Действительно, вычисление значения многочлена $v(x)$ в точке α^j дает:

$$v(\alpha^j) = v_0 + v_1\alpha^j + ... + v_{n-1}\alpha^{jn-1} = \sum_{i=0}^{n-1} \alpha^{ij} v_i = c_j,$$

т.е. равенство нулю частотной компоненты c_j означает, что соответствующий элемент α^j — корень многочлена $v(x)$.

Отсюда следует, что полиномиальные коды, задаваемые порождающими и/или проверочными многочленами, определяются в частотной области нулевыми частотными компонентами, непосредственно связанными с корнями этих многочленов. В частности, если код Боуза-Чоудхури-Хоквингема (БЧХ) над $GF(q)$ задан своим порождающим $g(x)$ и/или проверочным $h(x)$ многочленами, т.е. если с учетом (6) – (8):

$$g(x) = \quad . \quad . \quad . \left(\prod_j f_{\alpha^j}(x) \right) = \prod_j (x - \alpha^j),$$

$$h(x) = \quad . \quad . \quad . \left(\prod_{i \neq j} f_{\alpha^i}(x) \right) = \prod_{i \neq j} (x - \alpha^i),$$

тогда спектры всех кодовых слов такого кода обязательно содержат нули в компонентах c_j и могут быть не нулевыми в компонентах c_i.

Это наглядно продемонстрировано на рис. 1, на котором схематично отмечены нулевые компоненты спектра – корни порождающего многочлена $g(x)$ и ненулевые элементы – корни проверочного многочлена $h(x)$.

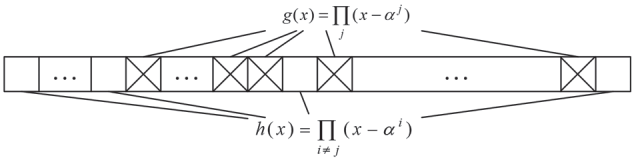


Рис. 1. Структура кодовых слов полиномиальных кодов в спектральной области

Преобразование Фурье для функций, заданных над вещественным пространством, обобщается в виде т.н. многомерных спектров [3]. Соответствующие многомерные обобщения преобразования Фурье могут быть также введены и на дискретных последовательностях из многомерных пространств над конечными полями.

3. МНОГОМЕРНЫЕ СПЕКТРЫ И ИХ ПРИМЕНЕНИЕ В ТЕОРИИ КОДИРОВАНИЯ

Пусть длины $n_1, n_2, ..., n_p$ одновременно являются делителями порядка мультипликативной группы конечного поля $GF(q^m)$ для некоторого положительного целого m, т.е.

$$n_1 \big| (q^m - 1) \wedge n_2 \big| (q^m - 1) \wedge ... \wedge n_p \big| (q^m - 1).$$

Тогда произвольный p-мерный сигнал

$$v = \{v_{i_1,i_2,...,i_p}, i_1 = 0,...,n_1 - 1, i_2 = 0,..., n_2 - 1,..., i_p = 0,..., n_p - 1\}$$

и его p-мерный спектр

$$c = \{c_{j_1,j_2,...,j_p}, j_1 = 0,...,n_1 - 1, j_2 = 0,..., n_2 - 1,..., j_p = 0,..., n_p - 1\}$$

связаны соответствующими преобразованиями:

$$c_{j_1,j_2,...,j_p} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} ... \sum_{i_p=0}^{n_p-1} \alpha_1^{i_1 j_1} \alpha_2^{i_2 j_2} ... \alpha_p^{i_p j_p} v_{i_1,i_2,...,i_p}, \quad (8)$$

$$v_{i_1,i_2,...,i_p} = \frac{1}{n_1}\frac{1}{n_2}...\frac{1}{n_p} \times \times \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} ... \sum_{j_p=0}^{n_p-1} \alpha_1^{-i_1 j_1} \alpha_2^{-i_2 j_2} ... \alpha_p^{-i_p j_p} c_{j_1,j_2,...,j_p}, \quad (9)$$

где α_1, α_2, ..., α_p – элементы конечного поля $GF(q^m)$ порядка n_1, n_2, ..., n_p, соответственно.

По аналогии с ограничениями сопряженности одномерных спектров (6) введем соответствующие условия для многомерного случая:

$$c^q_{j_1,j_2,...,j_p} = c_{q_{j_1} \bmod n, qj_2 \bmod n, ..., qj_p \bmod n}, \quad i_1 = 0,...,n_1 - 1, i_2 = 0,...,n_2 - 1,..., i_p = 0,...,n_p - 1, \quad (10)$$

справедливость которых легко проверяется

$$c^q_{j_1,j_2,\ldots,j_p} = \left(\sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} \ldots \sum_{i_p=0}^{n_p-1} \alpha_1^{i_1 j_1} \alpha_2^{i_2 j_2} \ldots \alpha_p^{i_p j_p} v_{i_1,i_2,\ldots,i_p} \right)^q =$$

$$= \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} \ldots \sum_{i_p=0}^{n_p-1} \alpha_1^{i_1 (qj_1)} \alpha_2^{i_2 (qj_2)} \ldots \alpha_p^{i_p (qj_p)} v_{i_1,i_2,\ldots,i_p} =$$

$$= c_{qj_1 \bmod n,\, qj_2 \bmod n,\, \ldots,\, qj_p \bmod n},$$

$$i_1 = 0,\ldots,n_1-1, i_2 = 0,\ldots,n_2-1,\ldots,i_p = 0,\ldots,n_p-1.$$

Разобьем кортежи чисел

$$i_1 = 0,\ldots,n_1-1, i_2 = 0,\ldots,n_2-1,\ldots,i_p = 0,\ldots,n_p-1$$

на подмножества:

$$A_{j_1,j_2,\ldots,j_p} = \begin{Bmatrix} \{j_1, j_1 q, \ldots, j_1 q^{m_{j_1}-1}\}, \{j_2, j_2 q, \ldots, j_2 q^{m_{j_2}-1}\}, \\ \ldots, \{j_p, j_p q, \ldots, j_p q^{m_{j_p}-1}\} \end{Bmatrix}, \quad (11)$$

где m_{j_s} — наименьшее положительное целое, удовлетворяющее равенству $j_s q^{m_{j_s}} = j_s \bmod n_s$, в силу конечности поля такое m_{j_s} всегда существует.

Множество $A_{j_1,j_2,\ldots,j_p}$ выделяет в многомерном спектре многомерную хорду, причем, если временной сигнал принимает значения в поле $GF(q)$, то значение спектра в одной из частот хорды определяет значения спектра при всех частотах этой хорды [3]. Таким образом, сигнал может быть задан через обратное многомерное преобразование Фурье (9), если определить хорды (11) с учетом ограничений (10).

Многомерные спектры используются в теории помехоустойчивого кодирования для описания т.н. итеративных кодов (или кодов-произведений) в частотной области. Рассмотрим, без потери общности, наиболее простой, двумерный случай.

Информационные символы $I = \{I_1, I_2, \ldots, I_k\}$, подлежащие кодированию двумерным итеративным (n,k,d) кодом над $GF(q)$, разобьем на k_2 подблоков, содержащих по k_1 символов в каждом, т.е. $k = k_1 k_2$. Запишем их в виде матрицы размером $k_1 \times k_2$, у которой каждый столбец является подблоком из k_1 символов. Каждая строка полученной матрицы кодируется линейным блоковым (n_2,k_2,d_2) кодом над $GF(q)$, называемым кодом второй (внешней) ступени. Результат кодирования дает матрицу, содержащую n_2 столбцов по k_1 символов в каждом.

Каждый из n_2 столбцов полученной матрицы кодируется линейным блоковым (n_1,k_1,d_1) кодом над $GF(q)$, называемым кодом первой (внутренней) ступени. В результате выполнения последней операции получаем матрицу размером $n_1 \times n_2$ символов из $GF(q)$, у которой каждый столбец есть кодовое слово кода первой ступени, а каждая строка – кодовое слово кода второй ступени (для последних $r_1 = n_1 - k_1$ строк это является следствием линейности кодов первой и второй ступеней). Полученная матрица является кодовым словом итеративного кода с параметрами: $n = n_1 n_2$, $k = k_1 k_2$, $d = d_1 d_2$.

Для исследования спектральных свойств итеративного кода в работе [3] использован математический аппарат многомерных спектров. Кодовое слово $v = \{v_{i_1,i_2}, i_1 = 0,\ldots,n_1-1, i_2 = 0,\ldots,n_2-1\}$ двумерного кода-произведения можно записать в виде многочлена от двух переменных:

$$v(x,y) = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} v_{i_1,i_2} x^{i_1} y^{i_2}, \quad (12)$$

где v_{i_1,i_2} — символы из $GF(q)$ (компоненты сигнала).

Используя (8) и (9) для $p = 2$ по заданному сигналу — двумерной матрице v во временной области можно вычислить все компоненты спектра $A = \{A_{j_1,j_2}, j_1 = 0,\ldots,n_1-1, j_2 = 0,\ldots,n_2-1\}$ и наоборот. Таким образом, с многочленом (12) можно ассоциировать его спектральный многочлен

$$c(x,y) = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} c_{j_1,j_2} x^{j_1} y^{j_2}, \quad (13)$$

где c_{j_1,j_2} — символы из $GF(q^m)$ являются компонентами спектра.

Представление кодовых слов итеративного кода в виде многочлена (12) и ассоциированного с ним спектрального многочлена (13) особенно полезно при использовании на первом и втором каскаде полиномиальных кодов, в первую очередь, кодов БЧХ. Корни порождающих многочленов таких кодов соответствуют нулевым значениям спектральных компонент, что для двумерного случая может быть схематично представлено в виде рис. 2.

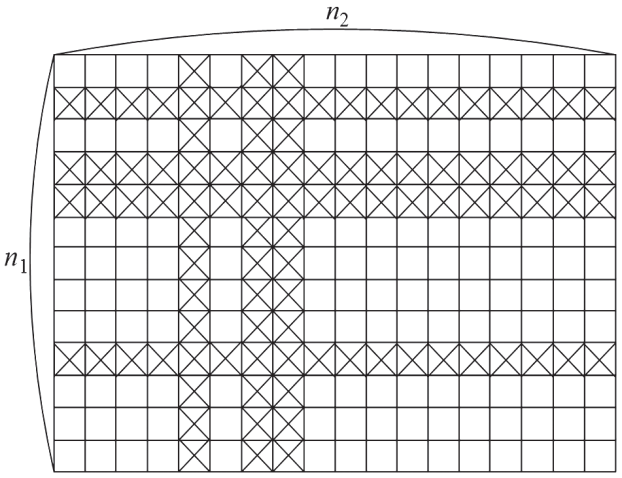


Рис. 2. Структура кодовых слов двумерного кода-произведения в частотной области (по аналогии с рис. 1)

Определение итеративного кода (многомерного кода-произведения) в частотной области позволяет использовать развитый аппарат быстрого преобразования Фурье для снижения вычислительной сложности алгоритмов кодирования и декодирования, а также выполнять некоторые вычислительные процессы параллельно [3]. Например, для рассмотренного выше двумерного случая вычисление $n_2 - k_2$ последних слов

кода первой ступени во временной области может быть реализовано только после вычисления всех слов кода второй ступени. Используя многомерные преобразования Фурье, вычисление каждого кодового символа v_{i_1,i_2} может быть организовано параллельно и независимо друг от друга посредством вычисления обратного преобразования по формуле (9) с $p=2$.

Следует однако отметить, что кодовые соотношения итеративных кодов далеки от оптимальных и при фиксированных (n,k,d) параметрах они, как правило, проигрывают другим известным конструкциям, например, каскадным кодам.

Рассмотрим каскадный (Nn,Kk,Dd) код над $GF(q)$, образованный из (N,K,D) кода над $GF(q^m)$ на внешней ступени каскада и $(n,k=m,d)$ кода над $GF(q)$ на внутренней ступени каскада.

Схематично структуру кодового слова каскадного кода представим на рис. 3 в виде матрицы из n строк и N столбцов, в ячейках которой записаны кодовые символы, принадлежащие полю $GF(q)$.

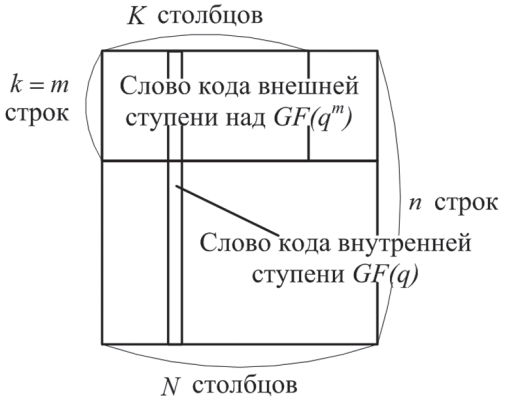


Рис. 3. Структура кодового слова каскадного кода

Левая верхняя область, состоящая из $k=m$ строк и K столбцов, соответствует информационным символам из $GF(q)$. Каждый столбец в этой области, состоящий из m символов из $GF(q)$ представляется как один символ из $GF(q^m)$:

$$V_i \Rightarrow \begin{pmatrix} v_{0,i} \\ v_{1,i} \\ \dots \\ v_{m-1,i} \end{pmatrix},\ i=0,\dots,K-1, \qquad (14)$$

т.е. для полиномиального представления элементов поля имеем:

$$V_i(z)=v_{0,i}+v_{1,i}z+\dots+v_{m-1,i}z^{m-1},\ V_i(z)\in GF(q^m).$$

Все K столбцов, таким образом, представляются как K символов из $GF(q^m)$, которые обрабатываются как информационная последовательность

$$I=(V_0,\ V_1,\dots,\ V_{K-1})$$

(N,K,D) кода внешней ступени. Кодовое слово такого кода представляется в виде последовательности

$$V=(V_0,\ V_1,\dots,\ V_{K-1},\ V_K,\ V_{K+1},\dots,\ V_N), \qquad (15)$$

где проверочные символы V_K, V_{K+1}, ..., V_N формируются в процессе кодирования (N,K,D) кодом внешней ступени и записываются в матрицу в виде соответствующих векторов-столбцов в верхней правой области (см. рис. 3).

Таким образом, первые m строк в матричном представлении кодового слова каскадного кода соответствуют N символам из $GF(q^m)$ кодового слова кода внешней ступени. Каждый такой символ, представленный вектором из m символов

$$I_i=(v_{0,i},\ v_{1,i},\dots,\ v_{m-1,i}),\ i=0,\dots,N-1$$

обрабатывается как i-я информационная последовательность кода внутренней ступени. Соответствующее кодовое слово представляется в виде последовательности

$$v_i=(v_{0,i},\ v_{1,i},\dots,\ v_{m-1,i},\ v_{m,i},\ v_{m+1,i},\dots,\ v_{n-1,i}), \qquad (16)$$

где проверочные символы $v_{m,i}$, $v_{m+1,i}$,..., $v_{n-1,i}$ формируются в процессе кодирования $(n,k=m,d)$ кодом внутренней ступени и записываются по столбцам матрицы (см. рис. 3).

Таким образом, кодовое слово (сигнал) каскадного кода представляется в виде следующего массива символов из $GF(q)$:

$$v=\begin{pmatrix} v_{0,0} & v_{0,1} & \dots & v_{0,K-1} & v_{0,K} & v_{0,K+1} & \dots & v_{0,N-1} \\ v_{1,0} & v_{1,1} & \dots & v_{1,K-1} & v_{1,K} & v_{1,K+1} & \dots & v_{1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ v_{m-1,0} & v_{m-1,1} & \dots & v_{m-1,K-1} & v_{m-1,K} & v_{m-1,K+1} & \dots & v_{m-1,N-1} \\ v_{m,0} & v_{m,1} & \dots & v_{m,K-1} & v_{m,K} & v_{m,K+1} & \dots & v_{m,N-1} \\ v_{m+1,0} & v_{m+1,1} & \dots & v_{m+1,K-1} & v_{m+1,K} & v_{m+1,K+1} & \dots & v_{m+1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ v_{n-1,0} & v_{n-1,1} & \dots & v_{n-1,K-1} & v_{n-1,K} & v_{n-1,K+1} & \dots & v_{n-1,N-1} \end{pmatrix}. \qquad (17)$$

Очевидно, что выполняя двумерное преобразование Фурье матрицы (17) по выражению (9) с $p=2$, получим соответствующий двумерный спектр

$$c=\begin{pmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,K-1} & c_{0,K} & c_{0,K+1} & \dots & c_{0,N-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,K-1} & c_{1,K} & c_{1,K+1} & \dots & c_{1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{m-1,0} & c_{m-1,1} & \dots & c_{m-1,K-1} & c_{m-1,K} & c_{m-1,K+1} & \dots & c_{m-1,N-1} \\ c_{m,0} & c_{m,1} & \dots & c_{m,K-1} & c_{m,K} & c_{m,K+1} & \dots & c_{m,N-1} \\ c_{m+1,0} & c_{m+1,1} & \dots & c_{m+1,K-1} & c_{m+1,K} & c_{m+1,K+1} & \dots & c_{m+1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{n-1,0} & c_{n-1,1} & \dots & c_{n-1,K-1} & c_{n-1,K} & c_{n-1,K+1} & \dots & c_{n-1,N-1} \end{pmatrix}, \qquad (18)$$

который, хотя и будет взаимно-однозначно соответствовать временному сигналу (17) над $GF(q)$,

однако не будет соответствовать слову (15) с символами из $GF(q^m)$.

Другими словами, вычисленный спектр (18) будет соответствовать такому временному сигналу (17), который является кодовым словом некоторого итеративного кода, в котором код второй ступени образован посредством ограничения слова (15) с символами из $GF(q^m)$ на подполе $GF(q)$. Под ограничением здесь и далее понимается формирование слов

$$\begin{gathered} v_0 = (v_{0,0}, v_{0,1}, v_{0,2}, ..., v_{0,N-1}), \\ v_1 = (v_{1,0}, v_{1,1}, v_{1,2}, ..., v_{1,N-1}), \\ ... \\ v_{m-1} = (v_{m-1,0}, v_{m-1,1}, v_{m-1,2}, ..., v_{m-1,N-1}), \end{gathered} \quad (19)$$

из слова (15) с помощью правила (14).

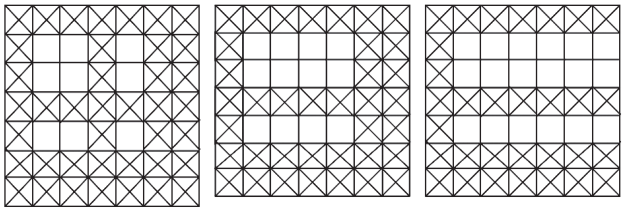
Практически это означает, что прямое двумерное преобразование Фурье матрицы (17) будет давать такие сигналы-матрицы (18), которые *не будут* соответствовать словам каскадного (Nn, Kk, Dd) кода над $GF(q)$.

Для наглядности приведенных выше рассуждений рассмотрим пример.

Пример 1. Вначале рассмотрим итеративный двоичный (49,9,16) код, образованный произведением двух двоичных (7,3,4) кодов БЧХ с порождающим многочленом

$$g(x) = f_{\alpha^0}(x) f_{\alpha^3}(x) =$$
$$= (x-\alpha^0)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) = 1 + x + x^2 + x^4.$$

Двумерный спектр кодовых слов заданного таким образом итеративного кода схематично представим на рис. 4, *а*.



а *б* *в*

Рис. 4. Структура кодовых слов двумерного кода-произведения в частотной области

Как видно на рис. 4, *а* в двумерном спектре всего имеется девять не обязательно нулевых спектральных компонент. Используя выражение (11) для этих компонент, сформируем три двумерных множества

$$A_{1,1} = \{\{1,2,4\},\{1,2,4\}\};\ A_{1,2} = \{\{1,2,4\},\{2,4,1\}\};$$
$$A_{1,4} = \{\{1,2,4\},\{4,1,2\}\},$$

которые реализуют ограничения сопряженности (10) и выделяют в двумерном спектре три двумерные хорды

$$c_{1,1}^2 = c_{2,2},\ c_{2,2}^2 = c_{4,4},\ c_{4,4}^2 = c_{1,1};$$
$$c_{1,2}^2 = c_{2,4},\ c_{2,4}^2 = c_{4,1},\ c_{4,1}^2 = c_{1,2};$$
$$c_{1,4}^2 = c_{2,1},\ c_{2,1}^2 = c_{4,2},\ c_{4,2}^2 = c_{1,4}.$$

Задав по одному (произвольному) представителю каждой хорды, вычислим остальные спектральные компоненты этих хорд по правилу сопряженности. Соответствующий двумерный сигнал получим через обратное двумерное преобразование Фурье сформированного спектра. Справедливо и обратное: сформировав сигнал по правилу кодирования БЧХ кодами с порождающим многочленом

$$g(x) = (x-\alpha^0)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6)$$

и выполнив над ним прямое двумерное преобразование Фурье, получим спектр с нулевыми компонентами c_{j_1,j_2} для $j_1, j_2 \in \{0,3,5,6\}$ и не обязательно нулевыми спектральными компонентами c_{j_1,j_2} для $j_1, j_2 \in \{1,2,4\}$.

Рассмотрим теперь двоичный каскадный (49,12,16) код, образованный из кода Рида-Соломона (РС) над $GF(2^3)$ с параметрами (7,4,4) на внешней ступени и двоичного кода БЧХ с параметрами (7,3,4) на внутренней ступени.

Зададим РС код порождающим многочленом

$$G(X) = (X-\alpha^0)(X-\alpha^5)(X-\alpha^6) =$$
$$= \alpha^4 + \alpha^2 x + \alpha^3 x^2 + x^3.$$

На внутренней ступени каскада будем использовать тот же двоичный код БЧХ, заданный порождающим многочленом

$$g(x) = (x-\alpha^0)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) =$$
$$= 1 + x + x^2 + x^4.$$

Прежде всего отметим, что все слова рассмотренного выше итеративного (49,9,16) кода содержатся среди слов каскадного (49,12,16) кода, т.е. итеративный код является в данном случае подкодом каскадного кода. При этом, только за счет изменения правила кодирования для фиксированного кодового расстояния, удалось на треть повысить относительную скорость кода.

Исходя из значения корней многочлена

$$G(X) = (X-\alpha^0)(X-\alpha^5)(X-\alpha^6),$$

логичной структурой спектра кодовых слов каскадного кода была бы изображенная на рис. 4, *б* схема, т.е. матрица с нулевыми столбцами, соответствующими корням $G(X)$. Однако применение к кодовым словам каскадного кода двумерного преобразования Фурье приведет к представлению слов РС кода в виде соответствующих ограничений на двоичное подполе. С учетом ограничений сопряженности (6) полученные по правилу (18) двоичные слова образуют двоичный (7,6,2) код БЧХ с проверочным многочленом

$$h(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) =$$
$$= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

и порождающим многочленом

$g(x) = (x-\alpha^0) = 1 + x$, соответственно.

Другими словами, ненулевые спектральные компоненты $c_{i,3}$ двумерного спектра могут привести к ненулевым значениям всех спектральных компонент внутри соответствующих хорд:

$$c_{1,3}^2 = c_{2,6},\ c_{2,6}^2 = c_{4,5},\ c_{4,5}^2 = c_{1,3};$$
$$c_{2,3}^2 = c_{4,6},\ c_{4,6}^2 = c_{1,5},\ c_{1,5}^2 = c_{2,3};$$
$$c_{4,3}^2 = c_{1,6},\ c_{1,6}^2 = c_{2,5},\ c_{2,5}^2 = c_{4,3}$$

и спектр кодового слова в общем виде будет иметь вид, схематично представленный на рис. 4, *в*.

Задавая кодовые слова через обратное двумерное преобразование Фурье спектра, соответствующего рис. 4, *в*, получим не каскадный (49,12,16) код, а некоторый итеративный (49,18,8), как код-произведение двоичных (7,3,4) и (7,6,2) кодов БЧХ.

Таким образом, математический аппарат многомерных спектров *не позволяет* дать описание кодовых слов каскадных кодов в частотной области. Соответственно для этих кодов *невозможно* получить и тот полезный эффект, который дают в технике помехоустойчивого кодирования быстрые многомерные преобразования Фурье. Разрешению этого противоречия и посвящен следующий раздел данной работы.

4. ОПИСАНИЕ КАСКАДНЫХ КОДОВ В ЧАСТОТНОЙ ОБЛАСТИ

Для решения задачи описания каскадных кодов в частотной области необходимо аналитически связать значения спектральных компонент кода внешней ступени с соответствующими спектральными компонентами его ограничения на подполе. Тогда математический аппарат многомерных спектров, с учетом этой введенной аналитической связи, очевидно, позволит вычислить кодовое слово каскадного кода в частотной области.

Таким образом, необходимо решить следующие ***частные задачи***:

1. Аналитически выразить спектр вектора (15) по заданным спектрам произвольных последовательностей (19).
2. Аналитически выразить спектр последовательностей (19) по заданному спектру произвольного вектора (15).
3. Аналитически выразить многомерный спектр вида (18) по заданным спектрам последовательностей (19) и/или (15).

Решение задачи 1.

Обозначим в общем виде спектр последовательности (15) в виде

$$C = (C_0, C_1, C_2, ..., C_{N-1}), \qquad (20)$$

причем $V_i, C_j \in GF(q^m)$, т.е. поле символов сигнала и его спектра совпадают.

Для каждого вектора из (19) найдем спектр, получим

$$c_0 = (c_{0,0}, c_{0,1}, c_{0,2}, ..., c_{0,N-1}),$$
$$c_1 = (c_{1,0}, c_{1,1}, c_{1,2}, ..., c_{1,N-1}), \qquad (21)$$
$$...$$
$$c_{m-1} = (c_{m-1,0}, c_{m-1,1}, c_{m-1,2}, ..., c_{m-1,N-1}),$$

где спектральные компоненты $c_{i,j}$ для всех m спектров c_0, c_1,..., c_{m-1} принадлежат, как и компоненты спектра C, расширенному полю $GF(q^m)$.

Утверждение 1. Спектр произвольного временного вектора есть линейная комбинация спектров его векторов-ограничений на произвольное подполе.

Доказательство. Найдем спектр сигнала V над $GF(q^m)$. Ядром преобразования Фурье в поле Галуа выступает элемент α порядка n, равный корню степени n из единицы. Выберем этот элемент, например, в виде $\alpha = z$. Тогда

$$V_i = v_{0,i} + v_{1,i} z + ... + v_{m-1,i} z^{m-1} =$$
$$= v_{0,i} + \alpha v_{1,i} + ... + \alpha^{m-1} v_{m-1,i}$$

и, соответственно,

$$V = v_0 + \alpha v_1 + ... + \alpha^{m-1} v_{m-1}.$$

То есть вектор V может быть записан как линейная комбинация векторов v_0, v_1, ..., v_{m-1} из (19) (выбор другого элемента $\alpha \in GF(q^m)$ порядка n приведет к изоморфному представлению элемента V, т.е. изменит лишь вид этой линейной комбинации).

Преобразование Фурье, по определению, является линейным и для конечных полей может быть записано в виде матричного умножения сигнала V на матрицу Вандермонда W, составленную из всех степеней элемента α (ядра преобразования), т.е.:

$$C = VW,\ c_i = v_i W,\ i = 0,..,m-1,$$

где

$$W^T = \begin{pmatrix} \alpha^0 & \alpha^0 & \alpha^0 & ... & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^2 & ... & \alpha^{N-1} \\ \alpha^0 & \alpha^2 & \alpha^4 & ... & \alpha^{N-2} \\ ... & ... & ... & ... & ... \\ \alpha^0 & \alpha^{N-1} & \alpha^{N-2} & ... & \alpha^1 \end{pmatrix},\ n = N = q^m - 1.$$

Для обратного преобразования следует использовать обратную матрицу:

$$(W^{-1})^T == \begin{pmatrix} \alpha^0 & \alpha^0 & \alpha^0 & ... & \alpha^0 \\ \alpha^0 & \alpha^{N-1} & \alpha^{N-2} & ... & \alpha^1 \\ \alpha^0 & \alpha^{N-2} & \alpha^{N-3} & ... & \alpha^2 \\ ... & ... & ... & ... & ... \\ \alpha^0 & \alpha^1 & \alpha^2 & ... & \alpha^{N-1} \end{pmatrix}.$$

Используя последние выражения, т.е. свойство линейности преобразования Фурье, получим:

$$C = VW = v_0 W + \alpha v_1 W + ... + \alpha^{m-1} v_{m-1} W =$$
$$= c_0 + \alpha c_1 + ... + \alpha^{m-1} c_{m-1}, \qquad (22)$$

следовательно, *спектр C произвольного временного вектора V над $GF(q^m)$ есть линейная комбинация спектров c_0, c_1, ..., c_{m-1} векторов v_0, v_1, ..., v_{m-1} — ограничений V на подполе $GF(q) \subseteq GF(q^m)$*. Конкретный вид этой линейной комбинации определяется, очевидно, выбором элемента α –ядра преобразования Фурье.

Доказанное утверждение позволяет вычислить спектр кодового слова РС кода по известным спектрам его ограничения на подполе, т.е. по известным спектрам соответствующих кодовых слов некоторого БЧХ кода.

Пример 2. Рассмотрим произвольное кодовое слово (7,4,4) РС кода над $GF(2^3)$ из примера 1. Пусть, например,

$$V = (\alpha^6, \alpha^4, \alpha^2, 0, 0, \alpha^4, \alpha^0).$$

Ограничением (14) на двоичное подполе получим три кодовых слова v_0, v_1 и v_2 двоичного (7,6,2) кода БЧХ (см. пример 1). Конкретный вид этих векторов зависит от способа представления элементов поля $GF(2^3)$. Пусть, например, поле $GF(2^3)$ построено по кольцу многочленов с операциями по модулю неприводимого многочлена $f(z) = 1 + z + z^3$ и примитивный элемент $\alpha = z$ поля $GF(2^3)$ является корнем этого многочлена. Тогда слова v_0, v_1 и v_2 примут вид:

$$v_0 = (1,0,0,0,0,0,1),$$
$$v_1 = (0,1,0,0,0,1,0),$$
$$v_2 = (1,1,1,0,0,1,0).$$

Найдем спектр векторов v_0, v_1 и v_2, для чего используем преобразование Фурье вида (4) с ядром $\alpha = z$, получим:

$$c_0 = (0, \alpha^2, \alpha^4, \alpha^5, \alpha^1, \alpha^6, \alpha^3),$$
$$c_1 = (0, \alpha^6, \alpha^5, \alpha^0, \alpha^3, \alpha^0, \alpha^0),$$
$$c_2 = (0,0,0, \alpha^6, 0, \alpha^3, \alpha^5).$$

Используя (22), найдем спектр C вектора V:

$$C = c_0 + \alpha c_1 + \alpha^2 c_2 = = \begin{pmatrix} 0+0+0 \\ \alpha^2+\alpha^0+0 \\ \alpha^4+\alpha^6+0 \\ \alpha^5+\alpha^1+\alpha^1 \\ \alpha^1+\alpha^4+0 \\ \alpha^6+\alpha^1+\alpha^5 \\ \alpha^3+\alpha^1+\alpha^0 \end{pmatrix}^T = \begin{pmatrix} 0 \\ \alpha^6 \\ \alpha^3 \\ \alpha^5 \\ \alpha^2 \\ 0 \\ 0 \end{pmatrix}^T.$$

Непосредственная проверка показывает, что спектр вектора

$$V = (\alpha^6, \alpha^4, \alpha^2, 0, 0, \alpha^4, \alpha^0),$$

вычисленный по правилу (4), действительно равен

$$C = (0, \alpha^6, \alpha^3, \alpha^5, \alpha^2, 0, 0).$$

Решение задачи 2.

Решим теперь обратную задачу, т.е. нахождение спектров (21) по известному спектру (20). Воспользуемся введенными выше обозначениями. Справедливо следующее утверждение.

Утверждение 2. Компоненты спектров векторов-ограничений произвольного временного вектора на произвольное подполе есть линейная комбинация результатов степенных отображений компонентов спектра этого вектора.

Доказательство. Используя (22), запишем

$$\begin{aligned} C_0 &= c_{0,0} + \alpha c_{1,0} + \ldots + \alpha^{m-1} c_{m-1,0}, \\ C_1 &= c_{0,1} + \alpha c_{1,1} + \ldots + \alpha^{m-1} c_{m-1,1}, \\ C_2 &= c_{0,2} + \alpha c_{1,2} + \ldots + \alpha^{m-1} c_{m-1,2}, \\ &\ldots \\ C_{n-1} &= c_{0,n-1} + \alpha c_{1,n-1} + \ldots + \alpha^{m-1} c_{m-1,n-1}, \end{aligned} \qquad (23)$$

т.е. нахождение компонентов спектров (21) сводится к решению недоопределенной системы из n линейных уравнений от nm неизвестных.

Недоопределенная система в общем виде либо имеет бесконечное число решений, либо не имеет их вовсе, однако в данном случае систему уравнений можно несколько упростить.

Действительно, первое уравнение при $\alpha = z$ примет вид

$$C_0 = c_{0,0} + c_{1,0} z + \ldots + c_{m-1,0} z^{m-1},$$

что с учетом $C_0 \in GF(q^m)$ и $c_{i,0} \in GF(q)$ для $i = 0,1,\ldots,m-1$ означает, что элементы ($c_{0,0}$, $c_{1,0}$, ..., $c_{m-1,0}$) определяются как q-ичное представление C_0.

Для остальных уравнений используем ограничения сопряженности (10), которые, для двумерного случая ($p = 2$), перепишем следующим образом: $(c_{i,j})^q = c_{i,jq \bmod (q^m-1)}$.

Ограничения сопряженности преобразуют недоопределенную систему линейных уравнений (23) в множество из u определенных подсистем по u_s нелинейных уравнений (и по u_s неизвестных) в каждой подсистеме, соответственно:

$$\begin{aligned} C_s &= c_{0,s} + \alpha c_{1,s} + \ldots + \alpha^{m-1} c_{m-1,s}, \\ C_{sq \bmod N} &= (c_{0,s})^q + \alpha (c_{1,s})^q + \ldots + \alpha^{m-1} (c_{m-1,s})^q, \\ &\ldots \\ C_{sq^{u_s-1} \bmod N} &= (c_{0,s})^{q^{u_s-1}} + \alpha (c_{1,s})^{q^{u_s-1}} + \ldots + \alpha^{m-1} (c_{m-1,s})^{q^{u_s-1}}, \end{aligned} \qquad (24)$$

где u — число нетривиальных классов сопряженных элементов поля $GF(q^m)$ (или, что эквивалентно, число различных нетривиальных хорд A_s в спектре одномерных сигналов длины N над $GF(q)$), u_s — число элементов в s-м классе (или, что эквивалентно, число элементов в хорде A_s), s — положительное целое, пробегающее все степени примитивного элемента из разложения поля $GF(q^m)$ на классы $\{\alpha^s, \alpha^{sq}, \ldots, \alpha^{sq^{u_s}}\}$ так, что

$$\sum_s u_s = q^m - 2\,,\ \#s = u\,.$$

Найдем решение для произвольной подсистемы нелинейных уравнений (24), т.е. для произвольного s. Для этого используем следующее свойство конечных полей [3–5]:

$$(\alpha+\beta)^{q^b} = \alpha^{q^b} + \beta^{q^b}\,,$$

справедливое для любых $\alpha,\beta \in GF(q^m)$ и любого положительного целого b.

Возведем w-е уравнение подсистемы (24)

$$C_{sq^w \bmod N} = (c_{0,s})^{q^w} + \alpha(c_{1,s})^{q^w} + \ldots + \alpha^{m-1}(c_{m-1,s})^{q^w},$$
$$w = 0,1,..,u_s - 1$$

в степень q^{m-w}, получим:

$$\left(C_{sq^w \bmod N}\right)^{q^{m-w}} =$$
$$= (c_{0,s})^{q^m} + \alpha^{q^{m-w}}(c_{1,s})^{q^m} + \ldots + \alpha^{(m-1)q^{m-w}}(c_{m-1,s})^{q^m},$$

что, согласно малой теореме Ферма, дает линейное уравнение:

$$\left(C_{sq^w \bmod N}\right)^{q^{m-w}} = c_{0,s} + \alpha^{q^{m-w}} c_{1,s} + \ldots + \alpha^{(m-1)q^{m-w}} c_{m-1,s}.$$

Обозначим множество свободных членов в левой части системы (24) через

$$C^s = \{C_s, C_{sq \bmod N}, \ldots, C_{sq^{u_s-1} \bmod N}\}.$$

Тогда функциональное соответствие

$$\left(C_{sq^w \bmod N}\right)^{q^{m-w}} = \varphi\left(C_{sq^w \bmod N}\right),\ w = 0,\ldots,u_s - 1 \quad (25)$$

реализует *степенное отображение* $\varphi: C^s \to \overline{C^s}$ множества C^s в множество

$$\overline{C^s} = \left\{(C_s)^{q^m}, \left(C_{sq \bmod N}\right)^{q^{m-1}}, \ldots, \left(C_{sq^{u_s-1} \bmod N}\right)^{q^{m-u_s+1}}\right\}.$$

Записав поэлементно результат отображения φ, т.е. найдя $\left(C_{sq^w \bmod N}\right)^{q^{m-w}}$ для всех $w = 0,\ldots,u_s - 1$, получим систему линейных уравнений

$$(C_s)^{q^m} = c_{0,s} + \alpha^{q^m} c_{1,s} + \ldots + \alpha^{(m-1)q^m} c_{m-1,s},$$

$$\left(C_{sq \bmod N}\right)^{q^{m-1}} = c_{0,s} + \alpha^{q^{m-1}} c_{1,s} + \ldots + \alpha^{(m-1)q^{m-1}} c_{m-1,s},$$

$$\ldots \quad (26)$$

$$\left(C_{sq^{u_s-1} \bmod N}\right)^{q^{m-u_s+1}} = c_{0,s} + \alpha^{q^{m-u_s+1}} c_{1,s} + \ldots + \alpha^{(m-1)q^{m-u_s+1}} c_{m-1,s},$$

решение которой и дает искомые компоненты спектра для s-й подсистемы.

Найденное решение будет выражаться линейной комбинацией от свободных членов в левой части системы, т.е. от элементов множества $\overline{C^s}$ — результатов степенного отображения компонентов спектра C вектора V.

Выполнив аналогичные преобразования для всех u определенных подсистем, получим, с учетом ограничений сопряженности (10), решения для всех неизвестных компонентов спектров векторов-ограничений временного вектора V на произвольное подполе. Очевидно, что найденные таким образом *компоненты спектров векторов-ограничений произвольного временного вектора на произвольное подполе также будут выражаться линейной комбинацией результатов степенных отображений компонентов спектра этого вектора.*

Сформулированное и доказанное утверждение позволяет аналитически связать спектр векторов-ограничений произвольного кодового слова со спектром этого кодового слова. Для наглядности приведем пример вычисления спектра кодовых слов БЧХ кода по известному спектру кодового слова РС кода из примера 2.

Пример 3. Рассмотрим произвольное кодовое слово $V = (V_0, V_1, V_2, V_3, V_4, V_5, V_6)$ РС кода над $GF(2^3)$ из предыдущего примера.

Запишем его спектр C с компонентами из $GF(2^3)$ в общем виде: $C = (C_0, C_1, C_2, C_3, C_4, C_5, C_6)$. Спектр соответствующих кодовых слов БЧХ кода (или, что эквивалентно, спектр векторов-ограничений v_0, v_1, v_2 слова V на двоичное подполе) запишем в виде:

$$c_0 = (c_{0,0}, c_{0,1}, c_{0,2}, c_{0,3}, c_{0,4}, c_{0,5}, c_{0,6}),$$
$$c_1 = (c_{1,0}, c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5}, c_{1,6}),$$
$$c_2 = (c_{2,0}, c_{2,1}, c_{2,2}, c_{2,3}, c_{2,4}, c_{2,5}, c_{2,6}).$$

Используя выражение (22), получим

$$C = c_0 + \alpha c_1 + \alpha^2 c_2\,,$$

что в поэлементной записи (23) дает следующую недоопределенную систему из 6 уравнений и 18 неизвестных

$$C_0 = c_{0,0} + \alpha c_{1,0} + \alpha^2 c_{2,0}\,,$$
$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1}\,,$$
$$C_2 = c_{0,2} + \alpha c_{1,2} + \alpha^2 c_{2,2}\,,$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3}\,,$$
$$C_4 = c_{0,4} + \alpha c_{1,4} + \alpha^2 c_{2,4}\,,$$
$$C_5 = c_{0,5} + \alpha c_{1,5} + \alpha^2 c_{2,5}\,,$$
$$C_6 = c_{0,6} + \alpha c_{1,6} + \alpha^2 c_{2,6}\,.$$

Рассмотрим первое уравнение, заметим, что $C_0 \in GF(2^3)$ и все $c_{i,0} \in GF(2)$. Тогда для $\alpha = z$ имеем $C_0 = c_{0,0} + c_{1,0} z + c_{2,0} z^2$, т.е. элементы

$$(c_{0,0},\ c_{1,0},\ c_{2,0})$$

определяются как двоичное представление C_0.

Используя ограничения сопряженности

$$(c_{i,j})^2 = c_{i,2j \bmod(7)}\,,$$

перепишем оставшиеся уравнения в виде:

$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1},$$
$$C_2 = (c_{0,1})^2 + \alpha (c_{1,1})^2 + \alpha^2 (c_{2,1})^2,$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3},$$
$$C_4 = (c_{0,1})^4 + \alpha (c_{1,1})^4 + \alpha^2 (c_{2,1})^4,$$
$$C_5 = (c_{0,3})^4 + \alpha (c_{1,3})^4 + \alpha^2 (c_{2,3})^4,$$
$$C_6 = (c_{0,3})^2 + \alpha (c_{1,3})^2 + \alpha^2 (c_{2,3})^2.$$

Элементы поля $GF(2^3)$ образуют $u = 2$ нетривиальных класса сопряженных элементов $\{\alpha^1, \alpha^2, \alpha^4\}$ и $\{\alpha^3, \alpha^6, \alpha^5\}$, т.е. по (24) для $s = 1$ и для $s = 3$ имеем две подсистемы из $u_1 = u_3 = 3$ нелинейных уравнений (и по столько же неизвестных) в каждой подсистеме:

$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1},$$
$$C_2 = (c_{0,1})^2 + \alpha (c_{1,1})^2 + \alpha^2 (c_{2,1})^2,$$
$$C_4 = (c_{0,1})^4 + \alpha (c_{1,1})^4 + \alpha^2 (c_{2,1})^4;$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3},$$
$$C_5 = (c_{0,3})^4 + \alpha (c_{1,3})^4 + \alpha^2 (c_{2,3})^4,$$
$$C_6 = (c_{0,3})^2 + \alpha (c_{1,3})^2 + \alpha^2 (c_{2,3})^2.$$

Для каждого $s = 1,3$, используя функциональное соответствие (25)

$$\left(C_{s2^w \bmod 7}\right)^{2^{3-w}} = \varphi\left(C_{s2^w \bmod 7}\right),\ w = 0,...,2,$$

реализуем степенные отображения $\varphi : C^s \to \overline{C^s}$ множеств $C^s = \{C_s, C_{s2 \bmod 7}, C_{s4 \bmod 7}\}$ в множества

$$\overline{C^s} = \left\{C_s, \left(C_{s2 \bmod 7}\right)^4, \left(C_{s4 \bmod 7}\right)^2\right\},$$

результат запишем поэлементно в форме (26).

Получим две системы линейных уравнений:

$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1},$$
$$(C_2)^4 = c_{0,1} + \alpha^4 c_{1,1} + \alpha c_{2,1},$$
$$(C_4)^2 = c_{0,1} + \alpha^2 c_{1,1} + \alpha^4 c_{2,1};$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3},$$
$$(C_5)^2 = c_{0,3} + \alpha^2 c_{1,3} + \alpha^4 c_{2,3},$$
$$(C_6)^4 = c_{0,3} + \alpha^4 c_{1,3} + \alpha c_{2,3},$$

решение которых имеет вид линейных комбинаций:

$$c_{0,1} = C_1 + (C_2)^4 + (C_4)^2,$$
$$c_{1,1} = \alpha^2 C_1 + \alpha (C_2)^4 + \alpha^4 (C_4)^2,$$
$$c_{2,1} = \alpha C_1 + \alpha^4 (C_2)^4 + \alpha^2 (C_4)^2;$$
$$c_{0,3} = C_3 + (C_5)^4 + (C_6)^2,$$
$$c_{1,3} = \alpha^2 C_3 + \alpha (C_5)^4 + \alpha^4 (C_6)^2,$$
$$c_{2,3} = \alpha C_3 + \alpha^4 (C_5)^4 + \alpha^2 (C_6)^2.$$

Остальные компоненты спектра получим из условий сопряженности (10):

$$c_{0,2} = (c_{0,1})^2 = (C_1)^2 + C_2 + (C_4)^4,$$
$$c_{0,4} = (c_{0,1})^4 = (C_1)^4 + (C_2)^2 + C_4,$$
$$c_{1,2} = (c_{1,1})^2 = \alpha^4 (C_1)^2 + \alpha^2 C_2 + \alpha (C_4)^4,$$
$$c_{1,4} = (c_{1,1})^4 = \alpha (C_1)^4 + \alpha^4 (C_2)^2 + \alpha^2 C_4,$$
$$c_{2,2} = (c_{2,1})^2 = \alpha^2 (C_1)^2 + \alpha C_2 + \alpha^4 (C_4)^4,$$
$$c_{2,4} = (c_{2,1})^4 = \alpha^4 (C_1)^4 + \alpha^2 (C_2)^2 + \alpha C_4,$$
$$c_{0,6} = (c_{0,3})^2 = (C_3)^2 + C_6 + (C_5)^4,$$
$$c_{0,5} = (c_{0,3})^4 = (C_3)^4 + (C_6)^2 + C_5,$$
$$c_{1,6} = (c_{1,3})^2 = \alpha^4 (C_3)^2 + \alpha^2 C_6 + \alpha (C_5)^4,$$
$$c_{1,5} = (c_{1,3})^4 = \alpha (C_3)^4 + \alpha^4 (C_6)^2 + \alpha^2 C_5,$$
$$c_{2,6} = (c_{2,3})^2 = \alpha^2 (C_3)^2 + \alpha C_6 + \alpha^4 (C_5)^4,$$
$$c_{2,5} = (c_{2,3})^4 = \alpha^4 (C_3)^4 + \alpha^2 (C_6)^2 + \alpha C_5.$$

Таким образом, в общем виде решение системы уравнений для $0 < j \le 6$ запишем как *линейную комбинацию результатов степенных отображений компонентов спектра* C:

$$c_{0,j} = C_j + (C_{2j \bmod 7})^4 + (C_{4j \bmod 7})^2,$$
$$c_{1,j} = \alpha^2 C_j + \alpha (C_{2j \bmod 7})^4 + \alpha^4 (C_{4j \bmod 7})^2,$$
$$c_{2,j} = \alpha C_j + \alpha^4 (C_{2j \bmod 7})^4 + \alpha^2 (C_{4j \bmod 7})^2.$$

Проверка для спектра

$$C = (0, \alpha^6, \alpha^3, \alpha^5, \alpha^2, 0, 0)$$

дает

$$c_0 = (0, \alpha^2, \alpha^4, \alpha^5, \alpha^1, \alpha^6, \alpha^3),$$
$$c_1 = (0, \alpha^6, \alpha^5, \alpha^0, \alpha^3, \alpha^0, \alpha^0),$$
$$c_2 = (0, 0, 0, \alpha^6, 0, \alpha^3, \alpha^5),$$

что полностью совпадает с данными из примера 2.

Полученные аналитические решения первых двух задач, связанных с поиском взаимно-однозначного функционального соответствия спектра вектора (15) и спектров произвольных последовательностей (19), позволяют в общем виде решить задачу аналитического представления многомерного спектра вида (18) по заданным спектрам последовательностей (19) и/или (15).

Решение задачи 3.

Вернемся к рассмотрению кодового слова каскадного кода над $GF(q)$ в форме (17) и соответствующего ему спектра (18) с компонентами из $GF(q^m)$. Если первые m строк матрицы (17) являются векторами-ограничениями (19) кодового слова (15) на подполе $GF(q) \subseteq GF(q^m)$, тогда спектр слов (19) взаимно-однозначно функционально связан со спектром слова (15), что и доказывают предыдущие утверждения. Рассмотрим теперь оставшиеся $n - m$ строк матрицы (17).

Утверждение 3. Кодовое слово каскадного кода есть линейная комбинация векторов-ограничений кодового слова внешней ступени.

Доказательство. Структура каскадного кода (см. рис. 3) такова, что после кодирования кодом внешней ступени (формирование первых m строк матрицы (17)) каждый полученный столбец рассматривается как информационная последовательность $(n,k=m,d)$ кода внутренней ступени. Соответствующие ему кодовые слова записываются по столбцам матрицы (17). Для линейного кода это эквивалентно умножению $v_i=(v_{0,i},v_{1,i},...,v_{m-1,i})g$, где v_i – кодовое слово (16) кода внутренней степени, записываемое в i-й столбец матрицы (17).

Другими словами, процесс формирования всего кодового слова (17) может быть представлен как умножение $N\times k$ матрицы ($k=m$), образованной элементами векторов (19), на порождающую $k\times n$ матрицу g кода первой ступени:

$$v=\begin{pmatrix} v_{0,0} & v_{1,0} & \dots & v_{m-1,0} \\ v_{0,1} & v_{1,1} & \dots & v_{m-1,1} \\ \dots & \dots & \dots & \dots \\ v_{0,N-1} & v_{1,N-1} & \dots & v_{m-1,N-1} \end{pmatrix} g .$$

Это эквивалентно формированию строк матрицы v, как линейной комбинации векторов:

$$v_0=(v_{0,0},v_{0,1},v_{0,2},...,v_{0,N-1}),$$
$$v_1=(v_{1,0},v_{1,1},v_{1,2},...,v_{1,N-1}),$$
$$\dots$$
$$v_{m-1}=(v_{m-1,0},v_{m-1,1},v_{m-1,2},...,v_{m-1,N-1}),$$

т.е. *линейной комбинации векторов-ограничений (19) кодового слова внешней ступени на произвольное подполе*.

Рассмотрим теперь спектр двумерного слова v. Вначале отметим, что для общего случая вычисления многомерных спектров (8) справедливо следующее утверждение.

Утверждение 4. Многомерный спектр многомерного слова есть результат многократного вычисления одномерного спектра ко всем одномерным представлениям этого слова.

Доказательство. Многомерное преобразование Фурье (8) является линейным и может быть записано посредством многократного (p раз, т.е. по каждому измерению матрицы v с учетом транспонирования) умножения матрицы v на матрицу Вандермонда W из утверждения 1:

$$A=\underbrace{\left(\left((vW)^TW\right)^T\dots W\right)^T}_{p\text{ раз}} .$$

Однако результат вычисления vW в построчной записи дает множество спектров, соответствующих строкам матрицы v, т.е. ее одномерному представлению. Другими словами, *многомерный спектр многомерного слова v есть результат многократного вычисления одномерного спектра ко всем одномерным представлениям слова v*.

Объединив предыдущие два утверждения, получим следующее.

Утверждение 5. Спектр кодового слова каскадного кода является, в построчной записи, множеством результатов двукратного вычисления одномерного спектра ко всем линейным комбинациям векторов-ограничений кодового слова внешней ступени.

Доказательство. Применение утверждения 4 к каскадному коду дает следующее выражение

$$A=(vW)^TW , \qquad (27)$$

т.е. спектр кодового слова каскадного кода является, в построчной записи, множеством спектров, соответствующих спектрам строк (v_0, v_1, ..., v_{N-1}) матрицы v.

Однако, как показано в утверждении 3, строки матрицы v являются линейными комбинациями векторов-ограничений v_0, v_1, ..., v_{m-1} из (19) кодового слова внешней ступени. Преобразование Фурье, по определению, линейно, следовательно, спектр линейной комбинации векторов (v_0, v_1, ..., v_{m-1}) из (19) дает линейную комбинацию соответствующих спектров (c_0, c_1, ..., c_{m-1}) из (21). Тогда спектр кодового слова каскадного кода является, в построчной записи, множеством спектров линейных комбинаций спектров (21), или, что эквивалентно, *множеством результатов двукратного вычисления одномерного спектра ко всем линейным комбинациям векторов-ограничений кодового слова внешней ступени*.

Аналитическую связь спектра кодового слова каскадного кода со спектром слов кода внешней ступени дает применение утверждения 2 к последнему результату.

Утверждение 6. Компоненты спектра произвольного кодового слова каскадного кода определяются линейной комбинацией результатов степенных отображений компонентов спектра кодового слова кода внешней ступени.

Доказательство. Действительно, если, согласно утверждению 2, компоненты спектров векторов-ограничений произвольного временного вектора на произвольное подполе есть линейная комбинация результатов степенных отображений компонентов спектра этого вектора, тогда, из утверждения 5 следует, что и *компоненты спектра кодового слова каскадного кода определяются линейной комбинацией результатов этих отображений*.

Приведем пример, наглядно демонстрирующий справедливость приведенных соображений. В качестве исходных данных будем использовать пример 1. Напомним, что использование двумерных спектров в примере 1 *не позволило* дать описание каскадных кодов в частотной области. Покажем теперь как, используя полученные аналитические закономерности, можно решить эту задачу и реализовать кодирование каскадными кодами в частотной области.

Пример 4. Рассмотрим двоичный каскадный (49,12,16) код, образованный из кода РС над $GF(2^3)$ с параметрами (7,4,4) на внешней

ступени и двоичного кода БЧХ с параметрами $(7,3,4)$ на внутренней ступени (см. пример 1).

Спектр векторов-ограничений кодового слова РС кода внешней ступени в общем виде дает результат утверждения 2. Для данного случая (см. пример 2) соответствующие аналитические выражения имеют вид:

$$c_{0,j} = C_j + (C_{2j \bmod 7})^4 + (C_{4j \bmod 7})^2,$$
$$c_{1,j} = \alpha^2 C_j + \alpha(C_{2j \bmod 7})^4 + \alpha^4 (C_{4j \bmod 7})^2,$$
$$c_{2,j} = \alpha C_j + \alpha^4 (C_{2j \bmod 7})^4 + \alpha^2 (C_{4j \bmod 7})^2,$$

справедливые для всех $j = 0,\ldots,N-1$.

Предположим, что на внутренней ступени каскада правило кодирования кодом БЧХ с $g(x) = 1 + x + x^2 + x^4$ задано в систематическом виде через умножение на порождающую матрицу g (см. утверждение 3):

$$g = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Тогда промежуточный результат vW в (27) в построчной записи будет определяться линейными комбинациями векторов $c_{0,j}$, $c_{1,j}$, $c_{2,j}$ по правилу, задаваемому матрицей g, т.е. для всех $j = 0,\ldots,6$ имеем:

$$c_{3,j} = c_{0,j} + c_{2,j} = \alpha^3 C_j + \alpha^5 (C_{2j \bmod 7})^4 + \alpha^6 (C_{4j \bmod 7})^2,$$

$$c_{4,j} = c_{0,j} + c_{1,j} + c_{2,j} =$$
$$= \alpha^5 C_j + \alpha^6 (C_{2j \bmod 7})^4 + \alpha^3 (C_{4j \bmod 7})^2,$$
$$c_{5,j} = c_{0,j} + c_{1,j} =$$
$$= \alpha^6 C_j + \alpha^3 (C_{2j \bmod 7})^4 + \alpha^5 (C_{4j \bmod 7})^2,$$
$$c_{6,j} = c_{1,j} + c_{2,j} =$$
$$= \alpha^4 C_j + \alpha^2 (C_{2j \bmod 7})^4 + \alpha^1 (C_{4j \bmod 7})^2.$$

Вычисление одномерного преобразования Фурье вектора $c_j = (c_{0,j}, c_{1,j}, c_{2,j}, c_{3,j}, c_{4,j}, c_{5,j}, c_{6,j})$ для всех $j = 0,\ldots,6$ даст все строки спектра кодового слова каскадного кода. То есть общее решение запишем в следующем виде:

$$c_{0,j} = c_j\left(\alpha^i\right)^0 = 0;\ c_{j,0} = c_0\left(\alpha^i\right)^j = 0;$$
$$c_{1,1} = \alpha^6 C_1 + \alpha^0 (C_2)^4 + \alpha^5 (C_4)^2,$$
$$c_{2,2} = (c_{1,1})^2 = \alpha^5 (C_1)^2 + \alpha^0 (C_2)^1 + \alpha^3 (C_4)^4,$$
$$c_{4,4} = (c_{2,2})^2 = \alpha^6 (C_1)^4 + \alpha^0 (C_2)^2 + \alpha^6 (C_4)^1,$$
$$c_{1,2} = \alpha^6 C_2 + \alpha^0 (C_4)^4 + \alpha^5 (C_1)^2,$$
$$c_{2,4} = (c_{1,2})^2 = \alpha^5 (C_2)^2 + \alpha^0 (C_4)^1 + \alpha^3 (C_1)^4,$$
$$c_{4,1} = (c_{2,4})^2 = \alpha^6 (C_2)^4 + \alpha^0 (C_4)^2 + \alpha^6 (C_1),$$
$$c_{1,3} = \alpha^6 C_3 + \alpha^0 (C_6)^4 + \alpha^5 (C_5)^2,$$
$$c_{2,6} = (c_{1,3})^2 = \alpha^5 (C_3)^2 + \alpha^0 (C_6)^1 + \alpha^3 (C_5)^4,$$
$$c_{4,5} = (c_{2,6})^2 = \alpha^6 (C_3)^4 + \alpha^0 (C_6)^2 + \alpha^6 (C_5),$$
$$c_{1,4} = \alpha^6 C_4 + \alpha^0 (C_1)^4 + \alpha^5 (C_2)^2,$$
$$c_{2,1} = (c_{1,4})^2 = \alpha^5 (C_4)^2 + \alpha^0 (C_1)^1 + \alpha^3 (C_2)^4,$$
$$c_{4,2} = (c_{2,1})^2 = \alpha^6 (C_4)^4 + \alpha^0 (C_1)^2 + \alpha^6 (C_2),$$
$$c_{1,5} = \alpha^6 C_5 + \alpha^0 (C_3)^4 + \alpha^5 (C_6)^2,$$
$$c_{2,3} = (c_{1,5})^2 = \alpha^5 (C_5)^2 + \alpha^0 (C_3)^1 + \alpha^3 (C_6)^4,$$
$$c_{4,6} = (c_{2,3})^2 = \alpha^6 (C_5)^4 + \alpha^0 (C_3)^2 + \alpha^6 (C_6),$$
$$c_{1,6} = \alpha^6 C_6 + \alpha^0 (C_5)^4 + \alpha^5 (C_3)^2,$$
$$c_{2,5} = (c_{1,6})^2 = \alpha^5 (C_6)^2 + \alpha^0 (C_5)^1 + \alpha^3 (C_3)^4,$$
$$c_{4,3} = (c_{2,5})^2 = \alpha^6 (C_6)^4 + \alpha^0 (C_5)^2 + \alpha^6 (C_3),$$
$$c_{3,j} = 0,\ c_{5,j} = 0,\ c_{6,j} = 0.$$

Для проверки зададим спектр кодового слова РС кода как в примере 3: $C = (0, \alpha^6, \alpha^3, \alpha^5, \alpha^2, 0, 0)$, что дает

$$c_0 = (0, \alpha^2, \alpha^4, \alpha^5, \alpha^1, \alpha^6, \alpha^3),$$
$$c_1 = (0, \alpha^6, \alpha^5, \alpha^0, \alpha^3, \alpha^0, \alpha^0),$$
$$c_2 = (0, 0, 0, \alpha^6, 0, \alpha^3, \alpha^5)$$

и соответствующий спектр кодового слова каскадного кода, вычисленный по выведенным аналитическим выражениям, примет вид:

$$c = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^1 \\ 0 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^5 & \alpha^2 & \alpha^1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^3 & \alpha^6 & \alpha^4 & \alpha^1 & \alpha^2 & \alpha^3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Не трудно убедиться, что обратное двумерное преобразование Фурье матрицы c дает матрицу

$$v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad (28)$$

которая действительно является кодовым словом каскадного $(49,12,16)$ кода.

Таким образом, пример 4 наглядно демонстрирует реализацию кодирования каскадным кодом через преобразования в частотной области. Этот результат, по мнению автора, получен *впервые*.

В заключение приведем выражения для получения компонентов сигнала v над $GF(q)$ по задаваемым в частотной области компонентам спектра кодовых слов кода внешней ступени над

$GF(q^m)$. Для этого сформулируем и докажем следующее утверждение.

Утверждение 7. Компоненты произвольного кодового слова каскадного кода (во временной области) определяются линейной комбинацией результатов степенных отображений компонентов спектра кодового слова кода внешней ступени.

Доказательство. Из (27) следует, что для нахождения вектора v необходимо выполнить двукратное обратное одномерное преобразование Фурье над строками матрицы c с учетом транспонирования. При этом промежуточный результат vW уже известен из утверждения (5). В построчной записи vW представляет собой линейные комбинации спектров (21), которые, по утверждению 2, определяются линейными комбинациями результатов степенных отображений (25) компонентов спектра (20). Таким образом, для вычисления кодового слова v достаточно выполнить обратное преобразование Фурье всех линейных комбинаций векторов (21), т.е., с учетом линейности преобразования, *кодовое слово v определяется линейной комбинацией результатов степенных отображений компонентов спектра кодового слова кода внешней ступени.*

Покажем вид этих линейных комбинаций для рассмотренного в примере 4 случая.

Пример 5. Вычисляя обратное преобразование Фурье для всех векторов c_j, $j=0,...,6$ (см. пример 4), получим:

$$v_{0,0}=\sum_{j=0}^{6}\left(C_j+(C_{2j \bmod 6})^4+(C_{4j \bmod 6})^2\right),$$

$$v_{1,0}=\sum_{j=0}^{6}(\alpha^j)^{-1}\left(C_j+(C_{2j \bmod 6})^4+(C_{4j \bmod 6})^2\right),$$

$$\ldots$$

$$v_{6,0}=\sum_{j=0}^{6}(\alpha^j)^{-6}\left(C_j+(C_{2j \bmod 6})^4+(C_{4j \bmod 6})^2\right),$$

$$v_{0,1}=\sum_{j=0}^{6}\left(\alpha^2 C_j+\alpha(C_{2j \bmod 7})^4+\alpha^4(C_{4j \bmod 7})^2\right),$$

$$v_{1,1}=\sum_{j=0}^{6}(\alpha^j)^{-1}\left(\alpha^2 C_j+\alpha(C_{2j \bmod 7})^4+\alpha^4(C_{4j \bmod 7})^2\right),$$

$$\ldots$$

$$v_{6,1}=\sum_{j=0}^{6}(\alpha^j)^{-6}\left(\alpha^2 C_j+\alpha(C_{2j \bmod 7})^4+\alpha^4(C_{4j \bmod 7})^2\right),$$

$$\ldots$$

$$v_{6,6}=\sum_{j=0}^{6}(\alpha^j)^{-6}\left(\alpha^4 C_j+\alpha^2(C_{2j \bmod 7})^4+\alpha^1(C_{4j \bmod 7})^2\right).$$

Непосредственная проверка со спектром $C=(0,\alpha^6,\alpha^3,\alpha^5,\alpha^2,0,0)$ из примера 4 дает кодовое слово (28), что подтверждает справедливость и адекватность приведенных рассуждений.

ВЫВОДЫ

Таким образом, в результате проведенных исследований получено общее решение задачи представления каскадных кодов в частотной области, что позволит, используя выведенные аналитические зависимости компонентов многомерных спектров, строить в частотной области вычислительно эффективные алгоритмы кодирования и декодирования. Наиболее перспективным в этом смысле является использование быстрых многомерных преобразований Фурье.

Решение задачи описания каскадных кодов в частотной области потребовало нетривиальных абстрактных представлений соответствующих кодовых слов и их ограничений на подполе. Тем не менее, полученный результат связывает спектр кодового слова внешней ступени с кодовым словом каскадного кода (и/или его спектром) в виде простых аналитических выражений (см. примеры 4 и 5). Прикладное значение этого результата состоит в возможности построения кодовых слов каскадного кода в частотной области через соответствующие компоненты спектра кодового слова внешней ступени. Анализируя полученные результаты, следует также отметить специфическую структуру конечных выражений. Действительно, переменные в правой части уравнений (см. примеры 4 и 5) сгруппированы по классам сопряженных элементов, что указывает на непосредственное влияние групповых свойств конечного поля. Это наблюдение, очевидно, также может служить предметом дальнейших исследований с целью сокращения вычислительной сложности соответствующих преобразований.

Литература

[1] Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2007. – 1104 с.

[2] Кларк Дж. – мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: пер. с англ. / под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.

[3] Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.

[4] Федоренко С.В. Методы быстрого декодирования линейных блоковых кодов. – СПб.: ГУАП, 2008. – 199 с.

[5] Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

[6] Сергиенко А. Б. Цифровая обработка сигналов. - 2-е. – СПб: Питер, 2006. – С. 751.

[7] Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов: пер. с англ. / Р. Блейхут. – М.: Мир, 1989. – 448 с.

Поступила в редколлегию 20.03.2013

Кузнецов Александр Александрович, доктор технических наук, профессор, профессор кафедры БИТ ХНУРЭ. Научные интересы: теория кодирования и аутентификации.

Приходько Сергей Иванович, заведующий кафедрой транспортной связи Украинской академии железнодорожного транспорта. Научные интересы: теория помехоустойчивого кодирования, передача и обработка информации.

Билал Хамзе, аспирант кафедры транспортной связи Украинской академии железнодорожного транспорта. Научные интересы: теория помехоустойчивого кодирования, передача и обработка информации.

УДК 621.391

Багатовимірні спектри для опису каскадних кодів у частотній області // О.О. Кузнецов, С.І. Приходько, Білал Хамзе // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 319–332.

Розглядається математичний апарат багатовимірного дискретного перетворення Фур'є в кінцевих полях. Досліджуються методи опису лінійних блокових кодів у частотній області. Показано, що, на відміну від ітеративних кодів (кодів-добутків) каскадні коди в загальному випадку не можуть бути описані в частотній області в термінах багатовимірних спектрів. Отримано аналітичні вирази, що встановлюють взаємно-однозначну функціональну відповідність спектру послідовності над кінцевим полем і спектрів відповідних слів, отриманих обмеженням цього слова на підполе. Отримано загальне розв'язання задачі подання каскадних кодів у частотній області, що дозволить, використовуючи виведені аналітичні залежності компонентів багатовимірних спектрів, будувати в частотній області обчислювально ефективні алгоритми кодування і декодування.

Ключові слова: багатовимірне дискретне перетворення Фур'є, каскадні коди, кінцеві поля.

Іл.: 4. Бібліогр.: 7 найм.

UDC 621.391

Multidimensional spectra for describing cascade codes in the frequency domain // A.A. Kuznetsov, S.I.Prihod'ko, Bilal Hamse // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 319–332.

Mathematical tools of multidimensional discrete Fourier transformation over finite fields are considered. Methods for describing linear block codes in the frequency domain are researched. It is shown that unlike iterative codes (product codes) in the general case cascade codes cannot be described in the frequency domain in terms of multidimensional spectra. Analytical expressions establishing one-to-one functional correspondence of a spectrum of sequence over a finite field and spectra of relevant words derived by restriction of the word to the subfield are obtained. A general solution of the problem of cascade code representation in the frequency domain is obtained which makes it possible to construct computationally efficient algorithms for encoding and decoding using the derived analytical relations of multidimensional spectra.

Keywords: multidimensional discrete Fourier transformation, cascade codes, finite fields.

Fig.: 4. Ref.: 7 items.

УДК 621.396.253

ПРОГРАММНАЯ МОДЕЛЬ УСТРОЙСТВА ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ С ОСОБЫМИ КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

А.А. СМИРНОВ

Исследуется алгебраический подход к формированию больших ансамблей дискретных сигналов с многоуровневой функцией корреляции, который основан на сечении циклических орбит групповых кодов. Число и величина уровней боковых лепестков функции корреляции формируемых последовательностей, а также мощность ансамбля сигналов определяются дистанционными и структурными свойствами колец многочленов над конечными полями. Разрабатываются предложения по программной реализации устройств формирования дискретных сигналов с многоуровневой функцией корреляции.

Ключевые слова: программная модель, дискретные сигналы, особые корреляционные свойства, многоуровневая функция корреляции.

ВВЕДЕНИЕ

Перспективным направлением в развитии алгебраических методов теории дискретных сигналов является использование развитого математического аппарата теории конечных полей и, в частности, теории колец многочленов, что позволяет связать корреляционные свойства формируемых последовательностей с групповыми и структурными свойствами кодовых последовательностей [1 – 4]. Проведенные в этих работах исследования показали, что развиваемый алгебраический подход к синтезу дискретных сигналов на основе сечения циклических орбит группового кода позволяет формировать большие ансамбли последовательностей, корреляционные свойства которых обладают многоуровневой структурой. Наибольший практический интерес синтезированные сигналы представляют в радиосистемах управления со множественным доступом [5–7]. Использование больших ансамблей дискретных сигналов с улучшенными свойствами позволит существенно повысить абонентскую емкость радиосистем управления с кодовым разделением каналов.

В данной работе разрабатываются предложения по программной реализации устройств формирования дискретных сигналов с многоуровневой функцией корреляции. Показано, что разработанные предложения позволяют формировать последовательности с улучшенными корреляционными и ансамблевыми свойствами и практически реализуют разработанный в [1–4] метод формирования дискретных сигналов.

1. АЛГЕБРАИЧЕСКИЙ ПОДХОД К ФОРМИРОВАНИЮ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С МНОГОУРОВНЕВОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Предложенный в работах [1 – 4] алгебраический подход к формированию больших ансамблей дискретных сигналов с многоуровневой функцией корреляции основан на сечении циклических орбит групповых кодов. Число и величина уровней боковых лепестков функции корреляции формируемых последовательностей, а также мощность ансамбля сигналов определяются дистанционными и структурными свойствами колец многочленов над конечными полями. Кратко рассмотрим эти положения, составляющие теоретическую основу формирования дискретных сигналов.

Групповой код однозначно задается лидерами (представителями) составляющих его циклических орбит. Под орбитой здесь и далее понимается множество кодовых слов эквивалентных друг другу относительно операции циклического сдвига. Под сечением орбит группового кода будем понимать выбор одного представителя (лидера) каждой орбиты. Дистанционные (корреляционные) свойства образованного таким образом множества лидеров определяются дистанционными свойствами групповых кодов, при этом эквивалентность относительно операции циклического сдвига отсутствует по определению сечения орбит. Это свойство положим в основу формирования ансамбля дискретных сигналов.

Векторное пространство $GF^n(q)$ расклады-вается на множество непересекающихся орбит V_ξ, $\xi = 0,...,L$. При этом групповой код V представляется через объединение конечного числа орбит. Предлагается следующая схема выбора лидеров орбит – по одному произвольному представителю из каждого циклического подмножества V_ξ, $\xi = 0,...,M$ (для удобства обозначения кодовые слова $C_{v,u} = \left(c_0^{v,u}, c_1^{v,u}, ...c_{n-1}^{v,u}\right)$ обозначены двумя индексами: v – номер орбиты V_v кода V, $v = 1,...,M$; u – номер кодового слова в орбите, $u = 1,...,z_v$, где z_v – число кодовых слов в орбите V_v, $z_v \le n-1$).

Из отобранных представителей орбит сформируем множество $S = \left(S_1, S_2, ..., S_M\right)$, где $S_v = C_{v,u}$, $v = 1,...,M$, а выбор индекса u при соответствующем $C_{v,u}$ определяется правилом сечения v-й циклической орбиты группового кода.

Рассмотрим двоичный случай, т.е. ограничимся исследованием свойств множества $S = \left(S_1, S_2, ..., S_M\right)$, образованного посредством

сечения циклических орбит двоичного группового кода. Элементы формируемых дискретных последовательностей (дискретных сигналов) $S_v = \left(s_0^v, s_1^v, ...s_{n-1}^v\right)$ зададим по элементам отобранных кодовых слов (лидеров орбит) $C_{v,u} = \left(c_0^{v,u}, c_1^{v,u}, ...c_{n-1}^{v,u}\right)$ следующим образом: $s_i^v = \begin{cases} 1, c_i^{v,u} = 1; \\ -1, c_i^{v,u} = 0. \end{cases}$

Предположим, что рассматриваемый (n, k, d) код V имеет весовой спектр вида:

$$\begin{cases} A(0) = 1; \\ A(1) = 0; \\ A(2) = 0; \\ \quad ... \\ A(d-1) = 0; \\ A(d); \\ A(d+1); \\ \quad ... \\ A(n). \end{cases} \qquad (1)$$

$w = 0,...,n$, где $A(w)$ – число кодовых слов кода V с весом w.

Тогда образованное сечением циклических орбит кода V множество двоичных дискретных сигналов $S = (S_1, S_2, ..., S_M)$ обладает корреляционными и ансамблевыми свойствами, определяемыми следующим утверждением [1 – 4].

Утверждение.

1. Боковые лепестки периодической функции авто- (ПФАК) и взаимной (ПФВК) корреляции ансамбля сигналов $S = (S_1, S_2, ..., S_M)$ принимают следующие значения:

$$\text{ПФВК, ПФАК} = \frac{n-2w}{n}, \qquad (2)$$

для таких $w = d, d+1, ..., n$, что $A(w) \neq 0$.

2. Для всех таких $w = d, d+1, ..., n$, что $A(w) = 0$ боковые лепестки ПФАК и ПФВК никогда не принимают значений $\frac{n-2w}{n}$.

3. Мощность M ансамбля $S = (S_1, S_2, ..., S_M)$ определяется числом ненулевых орбит кода V и ограничена снизу выражением:

$$M \geq \frac{2^k - 1}{n}. \qquad (3)$$

Равенство выполняется в случае максимального периода последовательностей всех орбит, образующих код, т.е. если код V состоит из набора орбит, образованных последовательностями максимальной длины (m-последовательностями).

Рассмотрим наиболее общий случай, когда двоичный групповой (n,k,d) код над $GF(2)$ задан через проверочный многочлен вида:

$$h(x) = f_{i1}(x) f_{i_2}(x) ... f_{i_u}(x) = \\ = \prod_{s=1}^{m-1} \left(x - \alpha^{i_1(2^s)}\right)\left(x - \alpha^{i_2(2^s)}\right)...\left(x - \alpha^{i_u(2^s)}\right), \qquad (4)$$

где $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x) - u$ произвольных подряд следующих минимальных многочлена элементов $\alpha^{i_1} \in GF\left(2^m\right)$, $\alpha^{i_2} \in GF\left(2^m\right)$, ..., $\alpha^{i_u} \in GF\left(2^m\right)$ соответственно, где порядок элементов α^{i_1}, α^{i_2}, ..., α^{i_u} равен порядку мультипликативной группы конечного поля $GF\left(2^m\right)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF\left(2^m\right)$, $n = 2^m - 1$.

Положим без потери общности, что $i_1 = 1$. Определим проверочный и порождающий многочлен следующим образом:

$$h(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{(2^s)}\right)\left(x - \alpha^{i_2(2^s)}\right)...\left(x - \alpha^{i_u(2^s)}\right),$$

$$g(x) = \frac{x^n - 1}{h(x)} = \prod_{j \neq 1, i_2, ..., i_u} \prod_{s=0}^{m_j}\left(x - \alpha^{j(2^s)}\right).$$

Схематично процесс формирования проверочного и порождающего многочлена представлен на рис. 1. Символом v обозначено число классов сопряженных элементов, составляющих мультипликативную группу конечного поля $GF\left(2^m\right)$. В первом классе (элементы α^1, α^2, ..., $\alpha^{2^{m_1}} = \alpha^{2^{m-1}}$) содержится m сопряженных элементов (что определяет примитивность элемента α). В следующих классах (элементы α^j, α^{2j}, ..., $\alpha^{j2^{m_2}}$) содержится m_j сопряженных элементов (m_j делит нацело m), $j \in [1..v]$. Для каждого $j \in [1..v]$ соответствующее m_j определяется как наименьшее положительное целое, для которого справедливо равенство:

$$j = \left(j2^{m_j}\right) \bmod \left(2^m - 1\right).$$

Если порядок мультипликативной группы есть простое число, т.е. когда:

$$2^m - 1 = \textit{prime number},$$

тогда:

$$\forall j : m_j = m.$$

Единичный элемент поля $\alpha^0 = 1$ образует дополнительный сопряженный класс из одного элементов.

На рис. 2 представлено соответствующее распределение элементов конечного поля по многочленам $h(x)$ и $g(x)$. Элементы конечного поля из первых u классов сопряженных элементов являются корнями проверочного многочлена $h(x)$.

Диапазон элементов конечного поля, в котором лежат корни проверочного многочлена $h(x)$, определяется наибольшим значением z, для которого выполняется условие $\alpha^z = \alpha^{(z) \bmod (2^m - 1)}$, т.е.:

$$z = \max_{s=0,...,m-1} \{\left(2^s\right) \bmod \left(2^m - 1\right), \\ \left(i_2 2^s\right) \bmod \left(2^m - 1\right), \\ ..., \\ \left(i_u 2^s\right) \bmod \left(2^m - 1\right)\}.$$

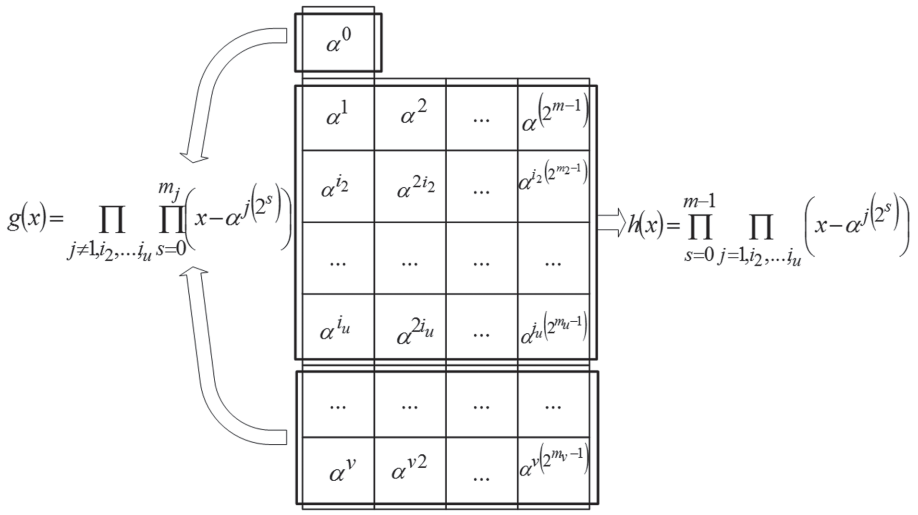


Рис. 1. Схема формирования проверочного и порождающего многочленов группового кода

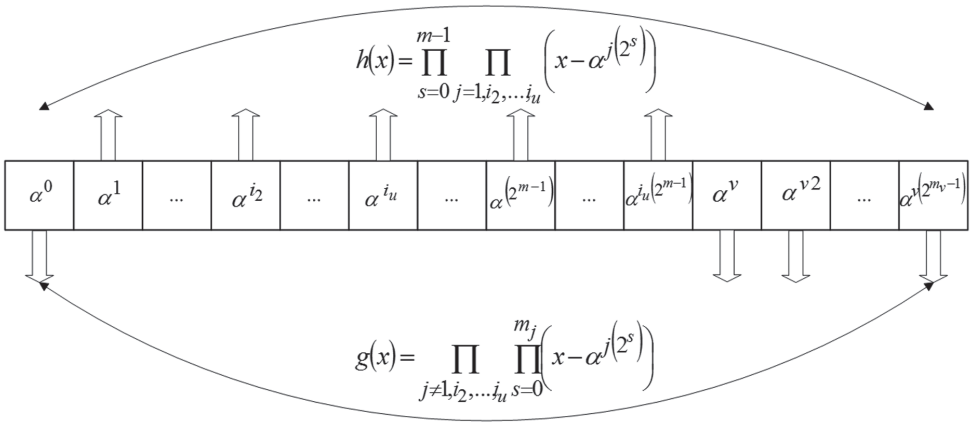


Рис. 2. Распределение элементов конечного поля по проверочному и порождающему многочленам группового кода

В общем случае корни многочленов $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)$ лежат в диапазоне:

$$\underbrace{\alpha^{i_1},\dots,\alpha^{i_1(2^{m-1})},\dots,\alpha^{i_2},\dots,\alpha^{i_2(2^{m-1})},\dots,\alpha^{i_u},\dots,\alpha^{i_u(2^{m-1})}}_{z\text{ значений}},$$

откуда имеем:

$$2t=2^m-z-1,$$

и, соответственно:

$$d=2t+1=2^m-z.$$

Соответствующие кодовые параметры группового кода имеют вид:

$$\left(n=2^m-1,k=zm,d=2^m-z\right). \qquad (5)$$

Оценим весовой спектр кода. Проверочный многочлен кода с параметрами (5) содержит в качестве сомножителя проверочные многочлены всех кодов, с проверочными многочленами $h(x)=f_{i1}(x)f_{i_2}(x)\dots f_{i_y}(x), y\le u$.

Отсюда следует, что все кодовые слова групповых кодов с $h(x)=f_{i1}(x)f_{i_2}(x)\dots f_{i_y}(x), y\le u$ являются кодовыми словами рассматриваемого кода с параметрами (5), т.е. ненулевые компоненты весового спектра образуются поочередным добавлением (в порядке добавления сомножителей в многочлен $h(x)=f_{i1}(x)f_{i_2}(x)\dots f_{i_y}(x), y\le u$) соответствующей пары элементов (для всех $y=2,3,\dots,u$):

$$A(z_y)\neq 0,$$

$$A(2^m-z_y)\neq 0,$$

где:

$$z_y=\max_{s=0,\dots,m-1}\{\left(2^s\right)\bmod\left(2^m-1\right),$$
$$\left(i_2 2^s\right)\bmod\left(2^m-1\right),$$
$$\dots,$$
$$\left(i_y 2^s\right)\bmod\left(2^m-1\right)\}.$$

При $y=1$ имеем один ненулевой компонент весового спектра $A(2^{m-1})\neq 0$, который соответствует $z_y=2^{m-1}$.

Рассмотренные в работах [1 – 4] случаи построения трех и пятиуровневых дискретных сигналов соответствуют:

$$y=2: z_y=2^{m-1}+2^{\frac{m+1}{2}-1},$$

$$A(2^{m-1}+2^{\frac{m+1}{2}-1})\neq 0,\ A(2^{m-1}-2^{\frac{m+1}{2}-1})\neq 0$$

$$y=3: z_y=2^{m-1}+2^{\frac{m+1}{2}},$$

$$A(2^{m-1}+2^{\frac{m+1}{2}})\neq 0,\ A(2^{m-1}-2^{\frac{m+1}{2}})\neq 0.$$

Таким образом, трех и пятиуровневые дискретные сигналы являются частным случаем построения больших ансамблей дискретных сигналов с многоуровневыми функциями корреляции.

Общее выражение для оценки весового спектра группового кода, заданного проверочным многочленом (4) запишем в виде:

$$A(w)=\begin{cases}1, w=0;\\ 0, w=1,\ldots,z_u-1;\\ \neq 0, w=z_u;\\ \ldots\\ \neq 0, w=z_3=2^{m-1}-2^{\frac{m+1}{2}};\\ 0, w=z_3+1,\ldots,z_2-1;\\ \neq 0, w=z_2=2^{m-1}-2^{\frac{m+1}{2}-1};\\ 0, w=z_2+1,\ldots,z_1-1;\\ \neq 0, w=z_1=2^{m-1};\\ 0, w=z_1+1,\ldots,2^m-z_2-1;\\ \neq 0, w=2^m-z_2=2^{m-1}+2^{\frac{m+1}{2}-1};\\ 0, w=2^m-z_2+1,\ldots,2^m-z_3-1;\\ \neq 0, w=2^m-z_3=2^{m-1}+2^{\frac{m+1}{2}};\\ \ldots\\ \neq 0, w=2^m-z_u;\\ 0, w=w=2^m-z_u+1,\ldots,2^m-1.\end{cases}$$

Соответствующее выражение по оценке уровней боковых лепестков периодической функции корреляции в общем случае примет вид:

$$\text{ПФВК, ПФАК}=\begin{cases}\dfrac{2^m-2z_u-1}{2^m-1}, w=z_u=\\ =\max\limits_{s=0,\ldots,m-1}\left\{\left(2^s\right)\bmod\left(2^m-1\right),\left(i_2 2^s\right)\bmod\left(2^m-1\right),\ldots,,\left(i_u 2^s\right)\bmod\left(2^m-1\right)\right\};\\ \ldots\\ \dfrac{2^m-2z_3-1}{2^m-1}=\dfrac{-1-2^{\frac{m+1}{2}+1}}{2^m-1}, w=z_3=2^{m-1}-2^{\frac{m+1}{2}};\\ \dfrac{2^m-2z_2-1}{2^m-1}=\dfrac{-1-2^{\frac{m+1}{2}}}{2^m-1}, w=z_2=2^{m-1}-2^{\frac{m+1}{2}-1};\\ \dfrac{2^m-2z_1-1}{2^m-1}=\dfrac{-1}{2^m-1}, w=z_1=2^{m-1})6(;\\ \dfrac{2^m-2(2^m-z_2)-1}{2^m-1}=\dfrac{-1+2^{\frac{m+1}{2}}}{2^m-1}, w=2^m-z_2=2^{m-1}+2^{\frac{m+1}{2}-1};\\ \dfrac{2^m-2(2^m-z_3)-1}{2^m-1}=\dfrac{-1+2^{\frac{m+1}{2}+1}}{2^m-1}, w=2^m-z_3=2^{m-1}+2^{\frac{m+1}{2}};\\ \ldots\\ \dfrac{2^m-2(2^m-z_u)-1}{2^m-1}, w=2^m-z_u=\\ =2^m-\max\limits_{s=0,\ldots,m-1}\left\{\left(2^s\right)\bmod\left(2^m-1\right),\left(i_2 2^s\right)\bmod\left(2^m-1\right),\ldots,,\left(i_u 2^s\right)\bmod\left(2^m-1\right)\right\}.\end{cases}$$

Таким образом, формируемые предлагаемым методом дискретные сигналы обладают многоуровневыми функциями авто и взаимной корреляции. Величины боковых выбросов принимают конечное число значений, задаваемых весовыми свойствами используемого группового кода.

Оценим мощность ансамбля формируемых дискретных сигналов. Мощность используемого кода $2^k=2^{um}$, всего имеется:

$$2^k-1=2^{um}-1$$

ненулевых кодовых слов.

Если предположить, что каждое кодовое слово обладает максимальным периодом и в каждой циклической орбите содержится ровно 2^m-1 кодовых слов, тогда выражение для оценки мощности ансамбля формируемых сигналов примет вид:

$$M=\frac{2^{um}-1}{2^m-1}=2^{(u-1)m}+2^{(u-2)m}+\ldots+2^m+1.$$

Анализ последнего выражения показывает, что использование групповых кодов позволяет формировать большие ансамбли дискретных сигналов. Добавление минимального многочлена в качестве очередного сомножителя в проверочном многочлене повышает мощность ансамбля на $2^{(u-i)m}$, где $u-i$ — число добавленных минимальных многочленов.

3. АППАРАТНАЯ РЕАЛИЗАЦИЯ УСТРОЙСТВ ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ ПРЕДЛОЖЕННЫМ МЕТОДОМ

Разработанный метод формирования дискретных сигналов позволяет строить большие ансамбли слабокоррелированных двоичных

последовательностей. Рассмотрим возможности практического формирования больших ансамблей слабокоррелированых дискретных сигналов и построения соответствующих аппаратных устройств генерирования двоичных последовательностей.

Формирование дискретных сигналов на случай многоуровневых последовательностей, реализуется с использованием следующей схемы. (рис. 3). Устройство построено через подключение к сумматору выходов *u* регистров сдвига. Схема подключения отводов соответствующих регистру сдвига в кольцо обратной связи задается коэффициентами отобранных примитивных многочленов $h_1(x)$, $h_2(x)$, ..., $h_u(x)$ степени m, соответственно. При этом длина двоичных последовательностей равняется $n = 2^m - 1$ и для их формирования нужно использовать *u* регистров сдвига регистры сдвига с m двоичными разрядами. Начальное состояние регистров сдвига задает вид формируемой последовательности.

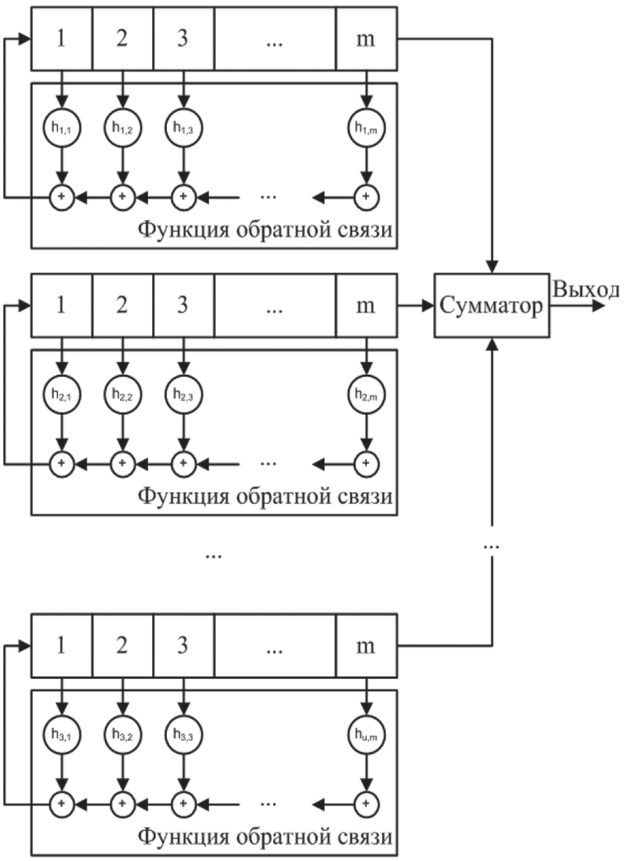


Рис. 3. Структурная схема устройства формирования дискретных сигналов с многоуровневой функцией корреляции

Функции обратной связи регистров сдвига задаются коэффициентами примитивных многочленов степени m:

$$h_1(x) = h_{1,0} + h_{1,1}x + h_{1,2}x^2 + \ldots + h_{1,m}x^m = = f_{i_1}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_1(2^s)}\right),$$

$$h_2(x) = h_{2,0} + h_{2,1}x + h_{2,2}x^2 + \ldots + h_{2,m}x^m = = f_{i_2}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_2(2^s)}\right),$$

...,

$$h_u(x) = h_{u,0} + h_{u,1}x + h_{u,2}x^2 + \ldots + h_{u,m}x^m = = f_{i_u}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_u(2^s)}\right),$$

где $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)$ – минимальные многочлены элементов α^{i_1}, α^{i_2}, ..., α^{i_u}, соответственно, из конечного поля $GF(2^m)$, которые задаются через свои корни $\alpha^{i_1(2^s)}$, $\alpha^{i_2(2^s)}$, ..., $\alpha^{i_u(2^s)}$, $s = 0, 1, \ldots, m-1$.

Порядок элементов α^{i_1}, α^{i_2}, ..., α^{i_u} равняется порядку мультипликативной группы конечного поля $GF(2^m)$, α – примитивный элемент конечного поля $GF(2^m)$.

Устройство работает рассмотренным выше образом, и позволяет формировать:

$$M = \frac{2^{um} - 1}{2^m - 1} = 2^{(u-1)m} + 2^{(u-2)m} + \ldots + 2^m + 1$$

последовательностей длины $n = 2^m - 1$.

4. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ УСТРОЙСТВ ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ ПРЕДЛОЖЕННЫМ МЕТОДОМ

Программа создана для практической проверки алгоритмов формирования дискретных сигналов с многоуровневой функцией корреляции предложенным методом, а также для эмпирического доказательства соответствия значений боковых выбросов функции авто- и взаимной корреляции теоретически предсказанным значениям, путём полного перебора при малых значениях *m* (5, 7, 11).

Алгоритм работы программы состоит в следующем.

Сперва выбирается значение *m*, для которого необходимо сформировать ансамбли дискретных сигналов с одно-, трех- и пятиуровневой функцией корреляции.

Затем задается порождающий полином конечного поля $GF(2^m)$ и рассчитываются значения примитивных элементов $\alpha^{i_1} \in GF(2^m)$, $\alpha^{i_2} \in GF(2^m)$, ..., $\alpha^{i_u} \in GF(2^m)$ соответственно, где порядок элементов α^{i_1}, α^{i_2}, ..., α^{i_u} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF(2^m)$, $n = 2^m - 1$.

После этого для заданного *m* элементы конечного поля распределяются в циклотомические классы (рис. 1).

Следующим шагом является формирование функций обратной связи регистров сдвига

(линейных рекуррентных регистров), которые задаются коэффициентами примитивных многочленов степени m, соответствующих элементов циклотомических классов.

Для формирования m-последовательностей используется один линейный рекуррентный регистр, функция работы которого задается проверочным полиномом $h(x)$. При этом корни минимальных многочленов $f_{i_1}(x)$, являющихся сомножителями, из которых образуется данный полином, принадлежат элементам одного циклотомического класса.

Для формирования сигналов Голда (дискретные сигналы с трехуровневой функцией авто- и взаимной корреляции) используются два линейных рекуррентных регистра, работа которых задается функциями $f_{i_1}(x)$ и $f_{i_2}(x)$ (рис. 3). Где $f_{i_1}(x)$ и $f_{i_2}(x)$ – два произвольных подряд следующих минимальных многочлена элементов $\alpha^{i_1} \in GF(2^m)$ и $\alpha^{i_2} \in GF(2^m)$ соответственно, где порядок элементов α^{i_1} и α^{i_2} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF(2^m)$, $n = 2^m - 1$.

Для формирования дискретных сигналов с пятиуровневой функцией авто- и взаимной корреляции используются три линейных рекуррентных регистра, работа которых задается функциями $f_{i_1}(x)$, $f_{i_2}(x)$ и $f_{i_3}(x)$ (рис. 3). Где $f_{i_1}(x)$, $f_{i_2}(x)$ и $f_{i_3}(x)$ – три произвольных подряд следующих минимальных многочлена элементов $\alpha^{i_1} \in GF(2^m)$ и $\alpha^{i_2} \in GF(2^m)$ соответственно, где порядок элементов α^{i_1} и α^{i_2} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF(2^m)$, $n = 2^m - 1$.

Добавление в дальнейшем еще одного линейного рекуррентного регистра в схему формирования дискретных сигналов, дает добавление еще двух дополнительных боковых выбросов функции авто- и взаимной корреляции (рис. 3).

Следующим этапом работы программы является выбор файла, в который будут записываться ансамбли дискретных сигналов с одно- (m-последовательности), трех- (сигналы Голда) и пятиуровневой функцией авто- и взаимной корреляции (новые классы дискретных сигналов). Кроме того, в данный файл записываются значения боковых выбросов для функции автокорреляции, для каждой сформированной последовательности (рис. 4).

Общий вид окна программы для формирования дискретных сигналов с многоуровневой функцией корреляции показан на рис. 5.

На рис. 5 выделены и пронумерованы области, значение которых следующее:

1 – Поле для выбора степени образующего полинома в $GF(2^m)$.

2 – Вид образующего полинома $GF(2^m)$.

3 – Калькулятор в полученном $GF(2^m)$.

4 – Сформировать дискретные сигналы и рассчитать значения боковых выбросов ПФАК и ПФВК.

5 – Сформировать отчёт в выбранный текстовый файл (m-последовательность, сигналы Голда, дискретные сигналы с пятиуровневой функцией корреляции).

6 – Рассчитанные, для образующего полинома, значения элементов конечного поля $\alpha^{i_1} \in GF(2^m)$, $\alpha^{i_2} \in GF(2^m)$, ..., $\alpha^{i_u} \in GF(2^m)$ соответственно, где порядок элементов α^{i_1}, α^{i_2}, ..., α^{i_u} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF(2^m)$, $n = 2^m - 1$.

7 – Распределение элементов конечного поля в циклотомические классы для заданного m.

8 – Перечень рассчитанных $h_j(x)$.

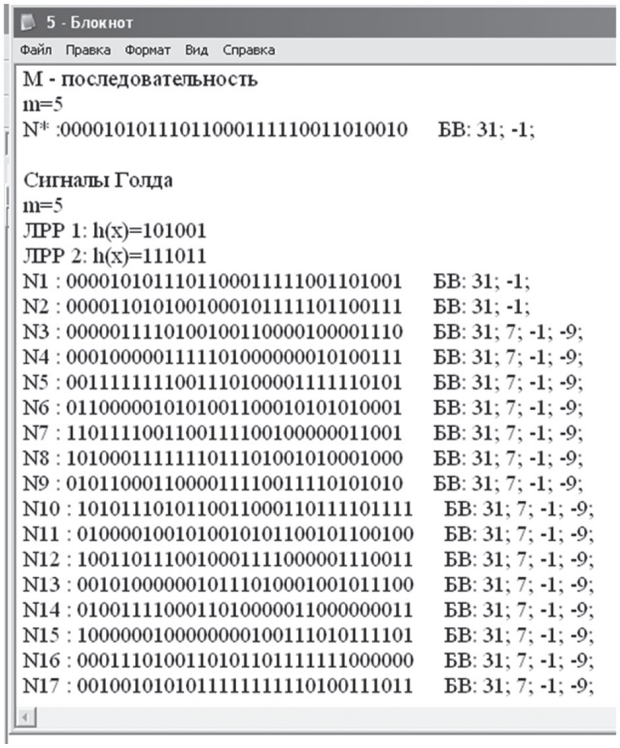


Рис. 4. Пример файла с ансамблями сформированных дискретных сигналов и значений боковых выбросов ПФАК и ПФВК

На рис. 6, 7 отображены, соответственно, вкладка просмотра сгенерированных m-последовательностей, образующих сигналы Голда и дискретные сигналы с многоуровневой функцией корреляции, вкладка просмотра значений функции автокорреляции для m-последовательностей.

Рассмотрим алгоритмическую реализацию формирования элементов конечного поля $GF(2^m)$. На основе выбранного образующего полинома степени m строится циклическое множество полиномов. На алгоритмическом уровне

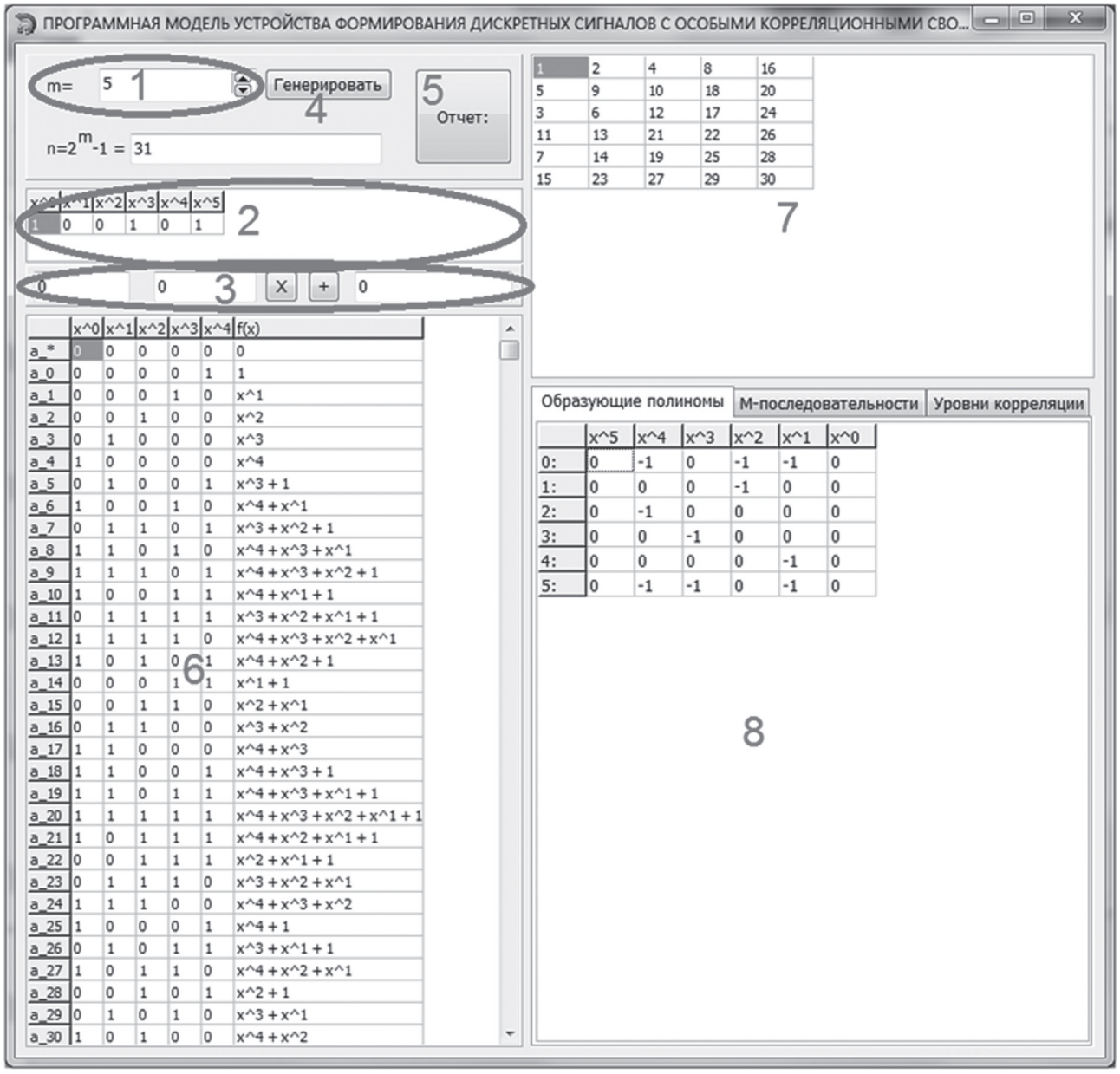


Рис. 5. Общий вид программы формирования дискретных сигналов с многоуровневой функцией корреляции

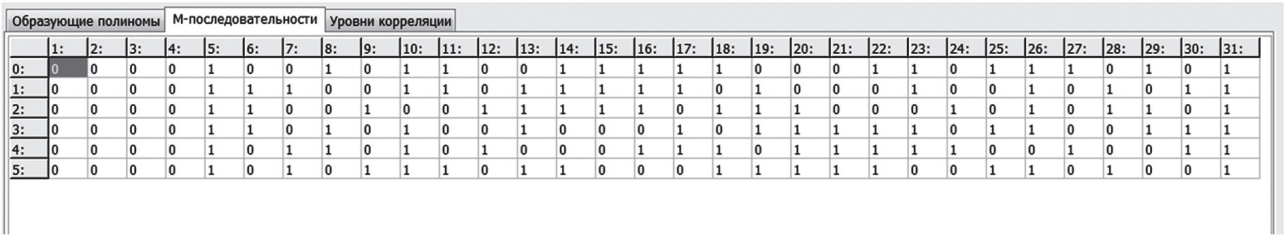


Рис. 6. Вкладка просмотра сгенерированных *m*-последовательностей, образующих сигналы Голда и дискретные сигналы с многоуровневой функцией корреляции

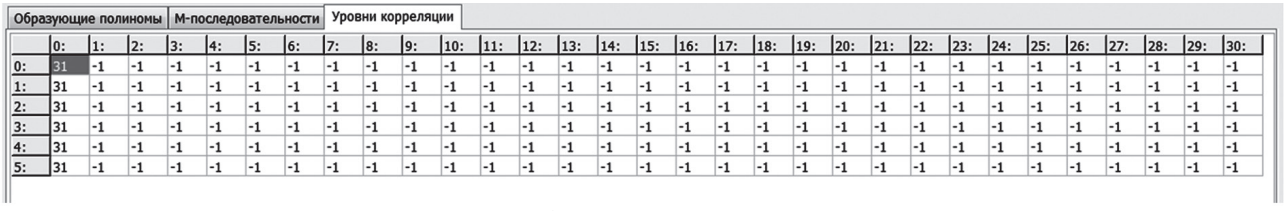


Рис. 7. Вкладка просмотра значений функции автокорреляции для *m*-последовательностей

необходимо, начиная с единичного полинома, перемножать текущий полином на x, после чего дополнить список остатком деления результата умножения на образующий полином. Полином записывается в виде бинарного числа. Описанные действия можно реализовать операцией сдвига влево, и при выталкивании единицы производить сложение по модулю два с образующим полиномом. Реализация процесса показана на следующей схеме (рис. 8).

5. ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ПРОГРАММНОЙ РЕАЛИЗАЦИИ ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ С МНОГОУРОВНЕВОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Оценим сложность алгоритма при формировании m-последовательности (субортогональных сигналов) и реализации функции автокорреляции. Для определения значения автокорреляции необходимо перемножить попарно элементы последовательности со всеми циклическими сдвигами этой последовательности, при этом нулевые значения принимаются как -1. Количество элементов последовательности задаёт количество операций умножения и количество вычислений значений корреляции исходной функции со сдвинутой. Общее количество операций при вычислении автокорреляции одной последовательности будет пропорциональна квадрату длины этой m-последовательности: $O(n^2)$.

Оценим сложность алгоритма при формировании сигналов Голда и реализации функции автокорреляции этих сигналов. Количество сигналов Голда, которые заданы двумя порождающими m-последовательностями, будет равно n. Каждая последовательность Голда получена поэлементным сложением по модулю два, двух m-последовательностей со смещениями от 0 до $n-1$. Для оценки сложности формирования последовательностей Голда необходимо повторить алгоритм формирования функции автокорелляции m-последовательности n раз, что означает возрастание сложности алгоритма до $n \cdot O(n^2)$, или $O(n^3)$.

Оценим сложность алгоритма при формировании нового класса сигналов (с пятиуровневой функцией корреляции) и реализации функции автокорреляции этих сигналов. Формирование нового класса сигналов (с пятиуровневой функцией корреляции) реализуется комбинацией циклических сдвигов поэлементного сложения трёх m-последовательностей, общее количество которых составляет n^2. В этом случае сложность перебора всех вариантов расширенных сигналов будет $O(n^4)$.

Сложность полного перебора последовательностей расширенных сигналов $O((2^m-1)^4)$, где m – степень образующего полинома.

ВЫВОДЫ

Таким образом, в ходе проведенных исследований были разработаны практические предложения, относительно программной реализации формирования дискретных последовательностей с многоуровневой функцией корреляции.

Разработанные схемы реализуются вычислительно эффективными преобразователями,

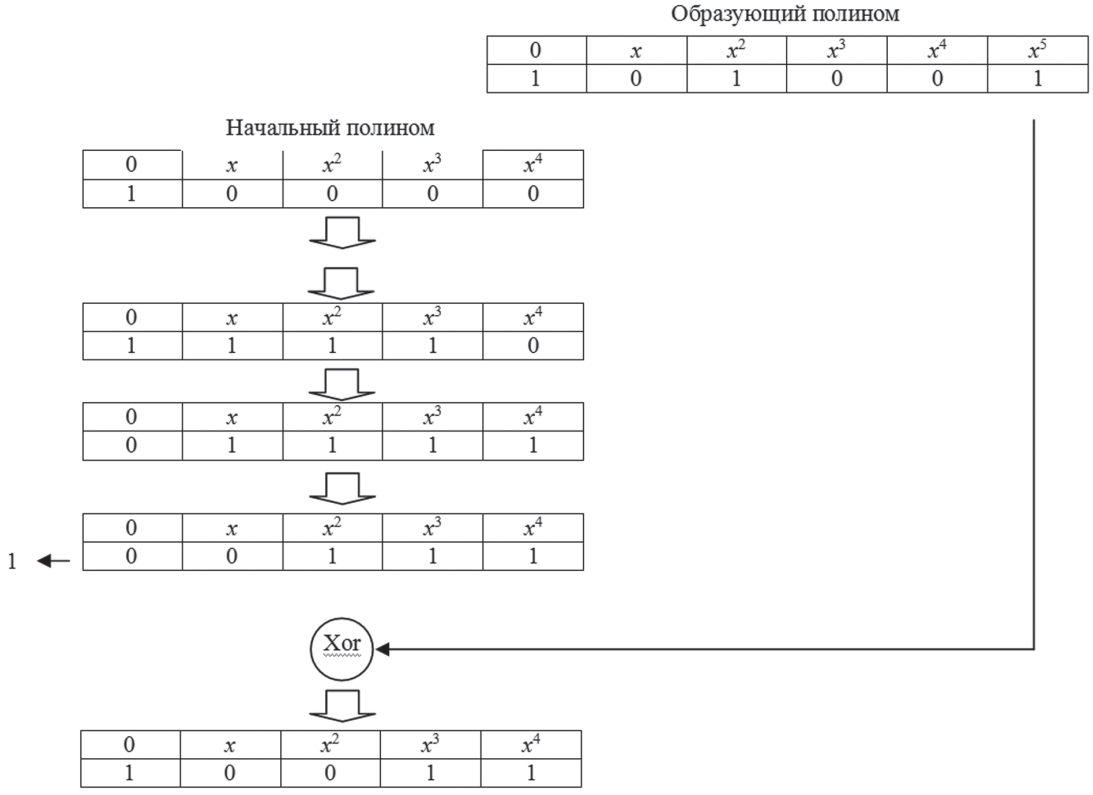


Рис. 8. Схема формирования элементов конечного поля $GF(2^m)$

например, на основе цепей с регистрами сдвига и сумматором (рис. 3). Они позволяют формировать большие ансамбли дискретных сигналов с улучшенными корреляционными и ансамблевыми свойствами. Таким образом, разработанные предложения позволяют практически реализовать разработанный метод формирования дискретных сигналов.

Разработанное программное обеспечение возможно усовершенствовать в направлении оптимизации скорости формирования дискретных сигналов с многоуровневой функцией корреляции.

Кроме того, разработанное программное обеспечение возможно использовать при проведении лабораторных работ по учебным дисциплинам, в которых рассматриваются вопросы кодового разделения каналов радиоуправления и связи, а также вопросы практической реализации алгоритмов стеганографии с использованием сложных дискретных сигналов.

Литература

[1] Кузнецов А.А., Смирнов А.А., Сай В.Н. Дискретные сигналы с многоуровневой функцией корреляции // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЭ. – 2011. – Вып. 166. – С. 142–152.

[2] Кузнецов А.А., Смирнов А.А., Сай В.Н. Формирование дискретных сигналов с многоуровневой функцией корреляции // Системи обробки інформації. – Харків: ХУ ПС. – 2011 – Вып. 5(95). – С. 50–60.

[3] Kuznetsov A.A. Use of Complex Discrete Signals for Steganographic Information Security / A.A. Kuznetsov, A.A. Smirnov // International Journal of Engineering Practical Education. – Volume 1, Issue 1. – USA, Indiana: Science and Engineering Publishing Company. – 2012. – P. 21–25.

[4] Смирнов А.А. Сравнительные исследования методов синтеза дискретных сигналов с особыми корреляционными свойствами / А.А. Смирнов, Е.В. Мелешко // Збірник тез V міжнародного науково-технічного симпозіуму «Новітні технології в телекомунікаціях» (ДУІКТ-Карпати-2012) м. Київ. 17-21 січня 2012 р. – Київ: ДУІКТ. – 2012. – С. 80–81.

[5] Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине. – Мир связи, 1998, № 3. – С. 40–43.

[6] Науменко Н. І., Стасев Ю. В., Кузнецов О.О., Євсєєв С.П. Теорія сигнально-кодових конструкцій. Х.:ХУ ПС, 2008р. – 489.

[7] Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

Поступила в редколлегию 8.04.2013

Смирнов Алексей Анатольевич, кандидат технических наук, доцент, профессор кафедры программного обеспечения Кировоградского национального технического университета. Научные интересы: защита информации, телекоммуникации, компьютерные сети и системы.

УДК 621.396.253

Програмна модель пристрою формування дискретних сигналів з особливими кореляційними властивостями / О.А. Смірнов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. — № 2. – С. 333–341.

Досліджується алгебраїчний підхід до формування великих ансамблів дискретних сигналів з багаторівневою функцією кореляції, що заснований на перетині циклічних орбіт групових кодів. Число й величина рівнів бічних пелюстків функції кореляції формованих послідовностей, а також потужність ансамблю сигналів визначаються дистанційними й структурними властивостями кілець багаточленів над кінцевими полями. Розробляються пропозиції з програмної реалізації пристроїв формування дискретних сигналів з багаторівневою функцією кореляції.

Ключові слова: програмна модель, дискретні сигнали, особливі кореляційні властивості, багаторівнева функція кореляції.

Іл.: 8. Бібліогр.: 7 найм.

UDC 621.396.253

Software model of a device of forming discrete signals with special correlation properties / A.A. Smirnov // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 333–341.

The paper researches an algebraic approach to forming large ensembles of discrete signals with multi-level correlation function, which is based on the section of circular orbits of group codes. The number and value of sidelobe levels of the correlation function of generated sequences as well as power of a signal ensemble are determined by remote and structural properties of polynomial rings over finite fields. Proposals for a software implementation of devices of forming discrete signals with multi-function correlation are being developed.

Keywords: programming model, discrete signals, special correlation properties, multi-level correlation function.

Fig.: 8. Ref.: 7 items.

УДК 681.142

МЕТОД КОНТРОЛЯ ДАННЫХ, ПРЕДСТАВЛЕННЫХ В КЛАССЕ ВЫЧЕТОВ

В. А. КРАСНОБАЕВ, М. А. МАВРИНА, А. А. ЗАМУЛА

В статье предложен метод повышения достоверности контроля данных, представленных в классе вычетов (КВ). Результаты расчетов и сравнительного анализа достоверности контроля данных в КВ показали, что с ростом разрядной сетки обрабатываемых данных эффективность непозиционного кодирования в классе вычетов существенно возрастает.

Ключевые слова: класс вычетов, непозиционная система счисления, достоверность контроля данных.

ВВЕДЕНИЕ

Известно, что непозиционная система счисления в классе вычетов (КВ) весьма удобна при реализации целочисленных арифметических и других модульных операций [1, 2]. Однако значительное время процедуры контроля данных снижает общую эффективность применения непозиционных кодовых структур (НКС) в КВ. Разработанные в последнее время методы оперативного контроля данных в системах обработки данных (СОД) позволяют существенно снизить время контроля, при этом возникает задача повышения достоверности процесса контроля [3–4]. Таким образом, важны исследования, посвященные решению задачи повышения достоверности контроля данных в КВ. Цель данной статьи – разработка метода повышения достоверности контроля данных в СОД, функционирующей в КВ.

ОСНОВНАЯ ЧАСТЬ

Известный метод контроля данных в КВ основан на получении и использовании так называемого позиционного признака непозиционного кода (ППНК), который является одной из характеристик однорядового кода (ОК), получаемого из исходной (контролируемой) НКС $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1})$ данных, представленной в КВ основаниями $(i=\overline{1,n+1})$, с одним контрольным a_{n+1} остатком по контрольному основанию (модулю) m_{n+1}, при этом $M=\prod_{i=1}^{n}m_i$; $M_0=\prod_{i=1}^{n+1}m_i$.

Рассмотрим процедуру получения ППНК на основе контролируемой НКС

$$A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1}).$$

В общем виде ОК

$$K_N^{(n_A)}=\left\{Z_{N-1}^{(A)}\ Z_{N-1}^{(A)}\ ...\ Z_1^{(A)}\ Z_0^{(A)}\right\} \qquad (1)$$

представляет собой последовательность двоичных $Z_K^{(A)}$ $(K=\overline{0,N-1})$ разрядов, состоящую из единиц и только одного нуля, находящегося на nA–м месте (считая справа, от разряда $Z_0^{(A)}$, налево, до разряда $Z_{N-1}^{(A)}$). Параметр n_A является ППНК непозиционной кодовой структуры $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1})$ данных. Математически параметр n_A представляет собой натуральное число, которое указывает на местоположение нулевого двоичного разряда $Z_{n_A}^{(A)}=0$ в записи ОК $K_N^{(n_A)}$. С его помощью, с определенной W точностью, которая зависит от значения величины модуля mi КВ, определяется номер j_i числового $[j_i\cdot m_i,\ (j_i+1)\cdot m_i)$ интервала нахождения числа А, т.е. определяется местоположение исходного числа $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1})$ на числовой оси $0\div M_0$.

Рассмотрим процедуру формирования ОК $K_N^{(n_A)}$, являющееся основой предлагаемого метода контроля данных в КВ. Для выбранного основания m_i КВ по значению остатка a_i числа $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1})$ в блоке констант нулевизации (БКН) СОД определяется константа вида $KH_{m_i}^{(A)}=\left(a_1^{'},a_2^{'}...,a_{i-1}^{'},a_i,a_{i+1}^{'},...,a_{n+1}^{'}\right)$. Далее, посредством выбранной константы $KH_{m_i}^{(A)}$ нулевизации осуществляется операция вычитания

$$A_{m_i}=A-KH_{m_i}^{(A)}=\left(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1}\right)-$$
$$-\left(a_1^{'},a_2^{'},...,a_{i-1}^{'},a_i,a_{i+1}^{'},...,a_n^{'},a_{n+1}^{'}\right)=$$
$$=\left[a_1^{(1)},a_2^{(1)},...,a_{i-1}^{(1)},0,a_{i+1}^{(1)},...,a_n^{(1)},a_{n+1}^{(1)}\right].$$

Эта операция соответствует смещению контролируемого числа

$$A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1})$$

на левый край интервала $[j_i\cdot m_i,\ (j_i+1)\cdot m_i)$ его первоначального (исходного) нахождения. В этом случае $A_{m_i}=j_i\cdot m_i$, т.е. число A_{m_i} кратно значению модуля m_i КВ.

Известно, что правильность числа A в КВ определяется его нахождением в числовом информационном $[0,M)$ интервале. Если число А находится вне этого интервала $(A\geq M)$, то оно считается искаженным (неправильным). В этом случае по значению n_A необходимо произвести контроль правильности исходного числа А путем определения факта попадания или непопадания исходного числа А в интервал $[0,\ M)$.

Чтобы определить факт нахождения числа в информационном $[0,M)$ числовом интервале, необходимо провести совокупность операций вида

$$A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)}. \quad (2)$$

Операция (2) проводится одновременно и параллельно во времени посредством совокупности из N констант $K_A \cdot m_i$ вида $\left(K_A = \overline{0, N-1}\right)$:

$$\begin{cases} A_{m_i} - 0 \cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1 \cdot m_i = Z_1^{(A)}, \\ A_{m_i} - 2 \cdot m_i = Z_2^{(A)}, \\ \quad \dots \\ A_{m_i} - (N_i - 2) \cdot m_i = Z_{N-2}^{(A)}, \\ A_{m_i} - (N_i - 1) \cdot m_i = Z_{N-1}^{(A)}, \end{cases} \quad (3)$$

где $N_i = \prod_{\substack{K=1; \\ K \neq i.}}^{n+1} m_K$.

В совокупности (3) аналитических соотношений существует единственное значение n_A из (2), для которого $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0$ $(K_A = n_A)$, т.е. $A_{m_i} - n_A \cdot m_i = 0$. Остальные значения (2) равны $Z_l^{(A)} = 1$ $(A_{m_i} - l \cdot m_i \neq 0;\ l \neq n_A)$. В общем случае количество двоичных разрядов в записи ОК $K_N^{(n_A)}$ равно значению N. Однако отметим, что для определения только факта искажения числа A нет необходимости иметь и анализировать всю последовательность из N совокупности значений $Z_{K_A}^{(A)}$ ОК $K_N^{(n_A)}$. Для этого достаточно иметь ОК $K_{N_i}^{(n_A)}$ длиною всего $N_i =]M / m_i[$ двоичных разрядов (где значение $]M / m_i[$ обозначает целую часть числа M / m_i, его не меньшую, т.е. производится округление числа M / m_i до ближайшего целого в большую сторону).

Как отмечалось выше, для установления факта правильности числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ нет необходимости анализировать все числовые интервалы $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$, расположенные вне информационного интервала $[0, M)$. Для установления только факта правильности числа A, определение номеров и анализ местоположения этих интервалов $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$ не имеют никакого значения. Для контроля НКС А в КВ достаточно знать местоположение нуля в записи (1) ОК (знать численное значение n_A) только в числовых интервалах $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$, находящихся в информационном числовом интервале $0 \div M$, и в первом, находящимся после значения M, интервале, расположенном на отрезке $0 \div M_0$. Для контроля данных $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ достаточно иметь ОК $K_{N_i}^{(n_A)}$ длиною всего $N_i =]M / m_i[$ двоичных разрядов.

Суть метода контроля данных в КВ состоит в следующем. Для контролируемой НКС $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, представленной в КВ, определяется ППНК n_A путем формирования ОК $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)} \right\}$ в виде последовательности из N_i двоичных разрядов. Выбор основания m_i КВ производится специальным образом, в соответствии с определенными критериями. Исходя из значения остатка a_i числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, выбирается константа нулевизации вида

$$KH_{m_i}^{(A)} = \left(a_1^{'}, a_2^{'}, ..., a_{i-1}^{'}, a_i, a_{i+1}^{'}, ..., a_n^{'}, a_{n+1}^{'}\right).$$

Далее проводиться реализация операции $A_{m_i} = A - KH_{m_i}^{(A)}$. Используя N_i констант $K_A \cdot m_i$ $\left(K_A = \overline{0, N_i - 1}\right)$, одновременно проводятся операции вычитания $A_{m_i} - K_A \cdot m_i$, в результате которых образуется значение двоичных разрядов $Z_{K_A}^{(A)}$, т.е. формируется ОК $K_{N_i}^{(n_A)}$. Значение ППНК n_A определяется из равенства $A_{m_i} - n_A \cdot m_i = 0$.

Рассмотрим пример реализации метода контроля для конкретного КВ, который задан основаниями $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ и $m_k = m_{n+1} = m_5 = 11$. Данный КВ обеспечивает обработку данных в однобайтовой ($l = 1$) разрядной сетке СОД. При этом $M = \prod_{i=1}^{4} m_i = 420$, $M_0 = M \cdot m_{n+1} = 4620$. Кроме этого будем считать, что $m_i = 11$. В этом случае

$$N_i = N_{n+1} =]M / m_i[=]M / m_{n+1}[=$$
$$=]420 / 11[=]38{,}18[= 39.$$

В табл. 1 приведено содержимое БКН СОД относительно основания $m_K = m_{n+1} = 11$.

Таблица 1

Константы $KH_{m_{n+1}}^{(A)}$ нулевизации по основанию $m_k = m_5 = 11$

Остаток $a_к = a_{n+1}$	Константы нулевизации				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_k = m_5 = 11$
	a'_1	a'_2	a'_3	a'_4	a_5
0000	00	00	000	000	0000
0001	01	01	001	001	0001
0010	10	10	010	010	0010
0011	00	11	011	011	0011
0100	01	00	100	100	0100
0101	10	01	000	101	0101
0110	00	10	001	110	0110
0111	01	11	010	000	0111
1000	10	00	011	001	1000
1001	00	01	100	010	1001
1010	01	10	000	011	1010

Пример 1. Провести контроль данных $A = (01, 11, 010, 000, 1001)$. По значению $a_5 = 1001$ в БКН (табл. 1) выбирается константа $KH_{m_{n+1}}^{(A)} = (00, 01, 100, 010, 1001)$. Определим, что $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (01, 10, 011, 101, 0000)$. Так как $A_{m_{n+1}} - n_A \cdot m_{n+1} = 418 - 38 \cdot 11 = 0$, то ОК имеет вид $K_{N_i}^{(n_A)} = K_{39}^{(38)} = \{011...11...11\}$ и $n_A = 38$. Исходя из того, что $n_A = 38 < N_i = 39$, делается вывод: число A правильное (не искажено). Однако проверка показывает, что $A = 427 > M = 420$, т.е. A неправильное число (рис. 1). В этом случае при контроле данных допущена ошибка.

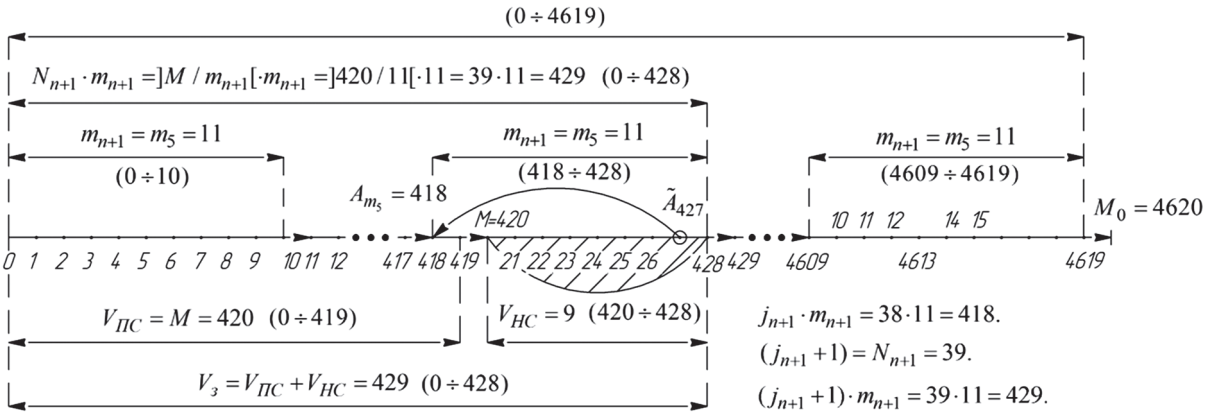


Рис. 1. Схема контроля данных в КВ для $m_i = 11$

Из примера 1 видно, что применение рассмотренного метода контроля данных в КВ не во всех случаях обеспечивает достоверный результат контроля. Действительно, существует совокупность $(j_{n+1}+1)\cdot m_{n+1} - M$ неправильных Γ чисел, которые определяются системой контроля СОД как правильные, что обуславливает низкую достоверность контроля. Для примера 1, таких чисел будет более половины (табл. 2).

Таблица 2

Совокупность кодовых слов в КВ

Числовой диапазон [418, 429)	
Правильные числа A	Совокупность неправильных Γ чисел, которые определяются системой контроля СПОД как правильные
418, 419	420, 421, 422, 423, 424, 425, 426, 427, 428

Таким образом, очевидно, что разработанный метод оперативного контроля данных в КВ и устройства для его реализации имеет весьма низкую достоверность контроля [3, 4].

Низкая достоверность контроля данных обусловлена наличием ненулевого значения α остатка в выражении

$$\alpha = M_{n+1}/m_{n+1} - [M_{n+1}/m_{n+1}] = \\ = M/m_{n+1} - [M/m_{n+1}]. \quad (4)$$

В свою очередь наличие ненулевого $\alpha \neq 0$ остатка определяется фактом не кратности значения M контрольному модулю m_{n+1} КВ, который определяет величину числового интервала $[j_{n+1}\cdot m_{n+1}, (j_{n+1}+1)\cdot m_{n+1})$ возможного нахождения числа A. В этом случае контроль данных $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ осуществляется на основе использования контрольного m_{n+1} основания КВ, путем формирования ОК

$$K_{N_{n+1}}^{(n_A)} = \left\{ Z_{N_{n+1}-1}^{(A)} \; Z_{N_{n+1}-2}^{(A)} \ldots Z_0^{(A)} \right\}. \quad (5)$$

Геометрически низкую достоверность контроля данных можно пояснить следующим образом. Числовой информационный интервал $[0, M = \prod_{i=1}^{n} m_i)$ не вмещает целое число отрезков длинною равных значению $m_i = m_{n+1}$. В этом случае на числовой оси $0 \div M_0$ существует числовой интервал $[j_{n+1}\cdot m_{n+1}, (j_{n+1}+1)\cdot m_{n+1})$ (или $[(N_{n+1}-1)\cdot m_{n+1}, N_{n+1}\cdot m_{n+1})$ внутри которого находится число M. Поэтому в данном интервале одновременно находится совокупность $(j_{n+1}+1)\cdot m_{n+1}) - M$ «неправильных» чисел (или $N_{n+1}\cdot m_{n+1} - M$) и совокупность $M - j_{n+1}\cdot m_{n+1}$ правильных чисел (или $M - (N_{n+1}-1)\cdot m_{n+1}$). В процессе контроля данных A, при проведении процедуры нулевизации, все, как неправильные $(j_{n+1}+1)\cdot m_{n+1}) - M$, так и правильные $M - j_{n+1}\cdot m_{n+1}$ числа, смещаются на левый край (к одному правильному числу $j_{n+1}\cdot m_{n+1}$) интервала $[j_{n+1}\cdot m_{n+1}, (j_{n+1}+1)\cdot m_{n+1})$. В этом случае, системой контроля (СК) СОД, неправильные $[N_{n+1}\cdot m_{n+1}) - M]$ числа будут идентифицироваться (определяться) как правильные.

Под достоверностью контроля данных в классе вычетов будем понимать вероятность получения истинного результата операции контроля данных, представленных в КВ. В качестве показателя для количественной оценки достоверностью контроля данных в классе вычетов может воспользоваться соотношением

$$P_{дк} = V_{ПС}/V_{ОС}, \quad (6)$$

где в общем случае: $V_{ПС} = M$ – количество (от 0 до $M \div 1$) правильных ($A < M$), находящихся в рабочем числовом $[0, M_0)$ диапазоне, кодовых слов для данного КВ; $V_{ОС} = (V_{ПС} + V_{НС})$ – общее количество кодовых слов, которые в результате проведения контроля данных считаются правильными; $V_{НС} = (N_i \cdot m_i - M)$ – количество неправильных ($A \geq M$) кодовых слов, которые в результате проведения контроля данных считаются правильными (отметим, что $N_i =]M/m_i[= j_i + 1$.

С учетом этого показатель достоверности (6) определяется соотношением

$$P_{дк} = \frac{M}{M + N_i \cdot m_i - M} = \frac{M}{N_i \cdot m_i}. \quad (7)$$

Для $m_i = m_{n+1}$ имеем, что

$$V_{НС} = (N_{n+1}\cdot m_{n+1} \quad M).$$

Если $m_i = m_{n+1}$, то выражение (7) примет вид

$$P_{дк} = \frac{M}{M + N_{n+1} \cdot m_{n+1} - M} = \frac{M}{N_{n+1} \cdot m_{n+1}}. \quad (8)$$

Так как заведомо $N_{n+1} \cdot m_{n+1} > M$ (см. (4)), то в этом случае всегда выполняется условие $P_{\text{дк}} < 1$.

Если в качестве основания m_i, определяющего величины числовых $j_i \cdot m_i \div (j_i + 1) \cdot m_i$ интервалов, возьмём информационное основание КВ, например, $m_i = m_1$, тогда $N_i =]M / m_i[= N_1 =]M / m_1[$ и $N_1 = \prod_{i=2}^{n} m_i$. В этом случае, выражение (7) примет вид

$$P_{\text{дк}} = \frac{M}{M + N_1 \cdot m_1 - M} = \frac{M}{N_1 \cdot m_1} = 1. \qquad (9)$$

В этом случае имеем, что (см. выражение (4)) всегда $Д = 1$, т.е., в случае выбора $m_i = m_1$, СК СОД всегда обеспечивает достоверный результат контроля данных в КВ.

Предлагаемый метод повышения достоверности контроля основан на известном методе оперативного контроля информации в КВ, который, в свою очередь, состоит из процедур получения и использования ППНК. Данный признак является одной из характеристик ОК, получаемого из исходной НКС $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ данных, представленной в КВ основаниями $\{m_i\}$, $i = \overline{1,\ n+1}$, с одним контрольным основанием m_{n+1}.

Суть предлагаемого метода повышения достоверности контроля данных в КВ состоит в обеспечении максимальной $P_{\text{дк}} = 1$ достоверности контроля данных, путем обеспечения выполнения условия $\alpha = 0$ (см. выражение (4)). В этом случае для вычисления значения $N_i =]M / m_i[$ выбирается модуль m_i, определяющий номер j_i числового интервала $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$ нахождения числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, только из совокупности n информационных модулей КВ, которые, естественно, кратны значению M. В этом случае $\alpha = M - [M / m_i] \cdot m_i = 0$, что и обеспечивает максимальное значение показателя достоверности контроля $P_{\text{дк}} = 1$ (см. выражение (7)).

Приведем пример применения разработанного метода повышения достоверности контроля данных в КВ.

Пример 2. Из вышеприведенного КВ выбираем, например, информационное основание $m_i = m_1 = 3$. При этом

$$N_i = N_1 = M / m_1 = 4 \cdot 5 \cdot 7 = 140.$$

В этом случае рабочий числовой $[0, M_0)$ диапазон КВ разбивается на интервалы $[j_1 \cdot m_1, (j_1 + 1) \cdot m_1)$. Для значения $m_1 = 3$ информационный числовой интервал $[0, M)$ разбивается точно на $N_1 = M / m_1 = 140$ отрезков длиною три единицы каждый (см. рис. 2). В табл. 3 приведено содержимое БКН относительно основания $m_1 = 3$.

Таблица 3

Содержимое БКН для $m_1 = 3$

a_i	Константы				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_5 = 11$
00	00	00	000	000	0000
01	01	01	001	001	0001
10	10	10	010	010	0010

Пусть необходимо провести контроль числа $A = (01, 11, 010, 000, 1001)$. По значению $a_1 = 01$ в БКН (табл. 3) выбираем константу нулевизации вида $KH_{m_1}^{(A)} = (01, 01, 001, 001, 0001)$. Далее опреде-

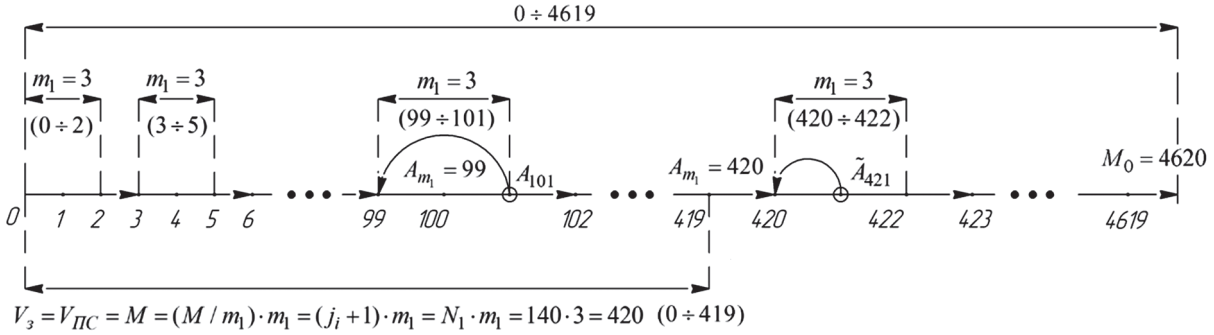


Рис. 2. Схема контроля данных в КВ для $m_i = 3$

Таблица 4

Результат расчёта значений $Д_i$ и $Д_{n+1}$ достоверности контроля в КВ

№ п.п.	m_{n+1}	M	M / m_{n+1}	$]M / m_{n+1}[$	$N_{n+1} =]M / m_{n+1}[\cdot m_{n+1}$	$Д_{n+1}$	$Д_i$, $i = \overline{1,n}$	Выигрыш в [%]
	1	2	3	4	5	6	7	8
1	11	420	38,2	39	429	0,979	1	2,1
2	13	420	32,3	33	429	0,979	1	2,1
3	17	420	24,7	25	425	0,988	1	1,2
4	19	420	22,1	23	437	0,961	1	3,9
5	23	420	18,2	19	437	0,961	1	3,9
6	29	420	14,4	15	435	0,965	1	3,5

ляем $A_{m_1} = A - KH_{m_1}^{(A)} = (00,10,001,110,1000)$. Если $A_{m_1} - n_A \cdot m_1 = 426 - 142 \cdot 3 = 0$, то ОК имеет вид $K_{N_i}^{(n_A)} = K_{140}^{(142)} = \{Z_{139}^{(A)}\ Z_{138}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)}\} = \{11...11...11\}$. Так как $N_i = 140 < n_A = 142$, т. е. ошибка в числе A [5].

Проверка: $A = 427 > M = 420$. Число $A > M$, т.е. оно неправильное (искажено).

В табл. 4 приведены результаты расчета и сравнительного анализа достоверности контроля данных в КВ.

ВЫВОДЫ

В статье предложен метод контроля данных в КВ. Применение данного метода обеспечивает получение достоверного результата контроля данных в КВ. Результат расчетов и сравнительного анализа достоверности контроля данных в КВ показал, что с ростом разрядной сетки обрабатываемых данных в СОД, эффективность непозиционного кодирования в классе вычетов существенно возрастает.

Литература

[1] Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.

[2] Материалы Международной научно-технической конференции “50 лет модулярной арифметике”. МИЭТ, г. Зеленоград. Моск. обл. 23-25 ноября 2005 г.

[3] ДП на корисну модель № 49054 України, МПК (2009.01) G 06 F 11/08. Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І., Дейнеко Ж.В. Пристрій для виявлення помилок у модулярній системі числення. № u 2009 12062. Заявл. 24.11.2009. Опубл. 12.04.2010, Бюл. № 7. – 10 с.

[4] ДП на корисну модель № 49711 України, МПК (2009.01) G 06 F 11/08. Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І. Спосіб виявлення помилок у системі обробки цифрової інформації, що функціонує у модулярній системі числення. № u 2009 11295. Заявл. 06.11.2009. Опубл. 11.05.2010, Бюл. № 9. – 4 с.

[5] ДП на корисну модель № 73375 України, МПК (2006.01) G 06F 11/08. Краснобаєв В. А., Жадан В. О., Мороз С. О,. Тиртишніков О. І., Одарущенко О. М., Горбенко Р. А. Пристрій для контролю помилок даних в інформаційно-телекомунікаційній системі, що функціонує у класі лишків. № u 2012 01854. Заявл. 20.02.2012. Опубл. 25.09.2012, Бюл. № 18.

Поступила в редколлегию 11.04.2013

Краснобаев Виктор Анатольевич, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенко, доктор техн. наук, профессор, Заслуженный изобретатель Украины, Почётный радист СССР. Научные интересы: теоретическое обоснование и практическое создание сверхбыстродействующих и высокоотказоустойчивых вычислительных структур в модулярной арифметике.

Маврина Марина Алексеевна, магистрант кафедры компьютерной инженерии Полтавского национального технического университета им. Юрия Кондратюка. Научные интересы: разработка методов оперативного контроля данных компьютерных устройств коммутационно-коммуникационного узла телекоммуникационной системы, функционирующих в непозиционной системе счисления класса вычетов.

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, кандидат технических наук, доцент. Научные интересы: технологии защиты информации в информационно-телекоммуникационных системах.

УДК 681.142

Метод контролю даних, поданих у класі лишків / В.А. Краснобаєв, М.О. Мавріна, О.А. Замула // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. — № 2. – С. 342–346.

У статті запропоновано метод підвищення достовірності контролю даних, поданих у класі лишків (КВ). Результати розрахунків та порівняльного аналізу достовірності контролю даних у КВ показав, що із зростанням розрядної сітки даних, які обробляються, ефективність непозиційного кодування у класі лишків суттєво зростає.

Ключові слова: непозиційна система, клас лишків, достовірність контролю даних.

Табл.: 4. Іл.: 2. Бібліогр.: 5 найм.

UDC 681.142

Method for controlling data presented in residue classes / V.A. Krasnobaev, M.A. Mavrina, A.A. Zamula // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 342–346.

A method for improving the reliability of monitoring data presented in residue classes (RC). The results of calculations and comparative analysis of the reliability of data monitoring in RCs have shown that as the word length of the data under processing increases, the efficiency of non-positioning encoding in the residue class substantially increases.

Keywords: residue class, non-positional number system, reliability of data control.

Tab.: 4. Fig.: 2. Ref.: 5 items.

УДК 004.056.53+530.145

УСИЛЕНИЕ БЕЗОПАСНОСТИ МЕТОДОМ ГАММИРОВАНИЯ ПРОТОКОЛА КВАНТОВОЙ ПРЯМОЙ БЕЗОПАСНОЙ СВЯЗИ

С.В. НИКОЛАЕНКО

В статье рассматривается классический (не квантовый) способ усиления безопасности пинг-понг протокола с парами перепутанных кубитов. Этот способ заключается в шифровании методом гаммирования блоков сообщений и позволяет обеспечить достаточно высокий уровень безопасности протокола. При этом сами гаммы не являются секретной информацией и передаются открытым каналом только после того, как легитимные пользователи убедились в отсутствии атаки в квантовом канале. Разработана имитационная модель пинг-понг протокола с парами перепутанных кубитов в квантовом канале с использованием шифрования методом гаммирования. Выполнен расчет необходимых для обеспечения заданного уровня безопасности длин блоков сообщения в зависимости от параметров протокола и параметров атакующей операции злоумышленника, а также соответствующий расчет необходимых размеров случайных гамм. Выполнены оценки вычислительной сложности генерации гамм для данного метода усиления безопасности. Показано, что время генерации является приемлемым для гамм размером около 2000 бит при использовании вычислительной техники с невысоким быстродействием.

Ключевые слова: квантовая криптография, пинг-понг протокол, метод усиления безопасности протокола, шифрования методом гаммирования, имитационное моделирование, временные оценки.

ВВЕДЕНИЕ

В современном мире передача конфиденциальных данных между несколькими абонентами в сетях связи может привести не только к потере передаваемой информации, но и к ее компрометации, т.е. разглашению информации, которая становится известной кому-либо, кто не имеет права доступа к ней. В последнее десятилетие активно развивается новое направление защиты информации – квантовая криптография. В отличие от криптографических методов, безопасность которых основывается на недоказанных математических утверждениях, безопасность квантовой криптографии основана на законах квантовой физики, а для переноса информации используются объекты квантовой механики. Такими объектами могут быть фотоны в линиях волоконно-оптической связи. Квантовые явления, используемые в целях криптографической защиты информации, позволяют создать такую систему защиты, при которой любое подслушивания обнаруживается с высокой степенью достоверности. Попытка подслушивания приводит к возмущению исходного состояния квантовой системы, поскольку невозможно измерить хотя бы одну характеристику фотона, не нарушив и не исказив другие.

Одним из направлений квантовой криптографии являются протоколы квантовой прямой безопасной связи (КПБС), которые позволяют передавать конфиденциальные сообщения непосредственно по квантовому каналу, т.е. без использования шифрования. В настоящее время предложено большое количество различных по назначению протоколов КПБС [1-7]. Одним из таких протоколов, который не нуждается в квантовой памяти большого объема, является пинг-понг протокол с парами перепутанных кубитов и без использования квантового сверхплотного кодирования, который позволяет передать один бит классической информации за один цикл протокола [1].

Пинг-понг протокол является одним из простых протоколов КПБС, который может быть реализован с использованием современных технологий квантовой информатики [8]. В настоящее время существуют различные варианты этого протокола [1, 2, 6, 7], но не до конца исследована их стойкость к различным атакам злоумышленника. Поскольку пинг-понг протокол предназначен для безопасной передачи классической информации квантовыми каналами связи, то существует возможность использования классических методов защиты информации для усиления безопасности пинг-понг протокола и других КПБС.

В настоящее время существует большое количество классических методов усиления безопасности протоколов передачи данных [9–12], которые надежно защищают данные от вмешательства и могут быть применены для защиты от злоумышленников информации, передаваемой с помощью квантовых пинг-понг протоколов. Одним из таких актуальных и криптографически гарантированных методов защиты информации является метод гаммирования. Однако, если оценки надежности и скорости метода гаммирования для пинг-понг протокола с парами перепутанными кутритов частично выполнялись ранее [13], то для пинг-понг протоколов с группами перепутанных кубитов таких оценок раньше вообще не проводилось.

Целью настоящей работы является усиление безопасности пинг-понг протокола с парами перепутанных кубитов с помощью метода гаммирования.

1. МЕТОД УСИЛЕНИЯ БЕЗОПАСНОСТИ ПИНГ-ПОНГ ПРОТОКОЛА С ПАРАМИ ПЕРЕПУТАННЫХ КУБИТОВ С ПОМОЩЬЮ ГАММИРОВАНИЯ

Пинг-понг протокол является двусторонним протоколом квантовой безопасной связи – для передачи сообщения от одного абонента (Алисы) к другому абоненту (Бобу) кубит пересылается сначала от Боба к Алисе, а затем обратно от Алисы к Бобу. В пинг-понг протоколе применяются два режима – режим передачи самого сообщения и режим контроля подслушивания, необходимый для обнаружения атаки пассивного перехвата. Алиса и Боб чередуют эти режимы случайным образом. Атака обнаруживается с некоторой вероятностью в режиме контроля подслушивания.

Для усиления безопасности пинг-понг протоколов можно применять метод гаммирования [9]. Идея этого метода состоит в следующем.

Перед передачей Алиса разбивает свое двоичное сообщение на l блоков некоторой фиксированной длины r, обозначим эти блоки через a_i ($i = 1,...l$), затем генерирует для каждого блока отдельно случайную двоичную гамму γ_i размером r и складывает полученные гаммы с соответствующими блоками сообщения: $b_i = a_i + \gamma_i$.

Полученные в результате блоки b_i передаются по квантовому каналу с использованием пинг-понг протокола. Даже если подслушивающему агенту (Еве) удастся перехватить один (или несколько) из этих блоков, оставшись не обнаруженной, то, не зная использованных гамм γ_i, Ева не может восстановить исходные блоки a_i. Для обеспечения достаточного уровня безопасности длина блока r и соответственно размер гамм γ_i должны выбираться так, чтобы вероятность необнаружения Евы после передачи одного блока была пренебрежимо малой величиной.

Гаммы γ_i передаются Бобу по обычному открытому каналу после завершения квантовой передачи, но только в том случае, если Алиса и Боб убедились в отсутствии подслушивания. Затем Боб складывает их с соответствующими блоками b_i и восстанавливает исходное сообщение: $a_i = b_i + \gamma_i$.

В соответствии с вышеизложенным методом усиления безопасности пинг-понг протоколов, для имитационного моделирования протокола с парами перепутанных кубитов разработан алгоритм последовательности действий, который состоит в следующем.

Шаг 1. Сообщение разбивается на l блоков a_i заданной длины r. Длина блока определяется из условия того, что вероятность необнаружения атаки после передачи одного блока не превышает заданную величину 10^{-k} [7]:

$$r \geq I = \frac{-kI_0}{\lg((1-q)/(1-q\cdot(1-d)))}, \qquad (1)$$

где I – количество информации, которое получает Ева при передаче одного блока; I_0 – количество информации, которое получает Ева за один раунд протокола; q – вероятность перехода в режим контроля подслушивания; d – уровень ошибок, вносимый атакой Евы.

Шаг 2. Генерация случайной двоичной гаммы γ_i размером r и сложение гаммы с соответствующим блоком $b_i = a_i + \gamma_i$ (т.е. выполнение *операции XOR* или исключающее ИЛИ).

Шаг 3. Выполнение режима передачи сообщения пинг-понг протокола с парами перепутанных кубитов. Режим контроля подслушивания протокола не моделировался.

Шаг 4. В случае, когда легитимные пользователи убедились в отсутствии подслушивания, моделируется передача гамм обычным открытым каналом связи.

Шаг 5. Восстановление исходного блока данных a_i, т.е. сложение полученного блока b_i с соответствующей гаммой γ_i: $a_i = b_i + \gamma_i$ (т.е. выполнение *операции XOR* или исключающее ИЛИ).

Для моделирования работы режима передачи сообщения пинг-понг протокола с парами перепутанных кубитов с использованием метода гаммирования, согласно вышеизложенному алгоритму, в среде программирования C++ Builder разработано программное обеспечение. Так, например, для передачи сообщения длинной 340 бит его нужно разбить на 5 блоков по 68 бит согласно (1) и для каждого сгенерировать свою гамму (ключ шифрования). Затем нужно передать это закодированное сообщение по квантовому каналу, убедиться в отсутствии прослушивания и передать по открытому каналу соответствующие гаммы для каждого блока зашифрованного сообщения, согласно выше описанному алгоритму. На принимающей стороне нужно сделать расшифровку полученного сообщения.

2. ОЦЕНКИ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ГЕНЕРАЦИИ ДВОИЧНЫХ ГАММ ОПРЕДЕЛЕННОГО РАЗМЕРА

Для алгоритма, который был описан выше, были рассчитаны средние оценки вычислительной сложности генерации случайных двоичных гамм определенного размера r, приведенные в табл. 1. Вычисления проводились на двухъядерном процессоре Intel Pentium Dual-CoreT3200 со следующими параметрами: тактовая частота (MHz): 2000, частота шины (MHz): 667, кэш 2-го уровня (Kb): 1024, поддерживается набор команд MMX, SSE, SSE2, SSE3, SSSE3, EM64T. Соответствующее программное обеспечение для генерации случайных двоичных гамм определенного размера было разработано в среде программирования C++ Builder. С использованием генератора случайных чисел выполнялась генерация 1000 случайных двоичных гамм заданного размера r и вычислялось время, которое требуется для генерации одной такой гаммы. Описанная процедура выполнялась 1000 раз для каждого размера гамм, а затем были вычислены средние значения, которые и приведены в табл. 1.

Для сравнительного анализа данного метода повышения безопасности пинг-понг протокола с методом повышения безопасности, предложенным в [7] и основанном на использовании обратимого хеширования (с использованием обратимых матриц), разработано программное обеспечение для обращения случайных двоичных матриц в среде программирования C++ Builder, в котором используется алгоритм LUP-разложения [14]. С помощью этого программного обеспечения генерировалось по 1000 псевдослучайных двоичных матриц заданного размера r с использованием генератора случайных чисел, с проверкой их на обратимость и расчетом времени, необходимого для генерации одной обратимой матрицы. Для каждого размера матриц описанная процедура выполнялась 1000 раз с вычислением среднего значения, результаты приведены в табл. 1. Согласно результатам работы [15], доля обратимых в двоичном поле Галуа GF (2) матриц составляет 0,289 от полного количества таких матриц (при $r \geq 16$).

Таблица 1

Оценки вычислительной сложности генерации двоичных гамм размера r и генерации случайных обратимых двоичных матриц размера $r \times r$

r	Среднее время генерации одной случайной обратимой двоичной матрицы, с	Среднее время генерации одной случайной двоичной гаммы, с
50	0,0122	0,0009
100	0,0728	0,0046
150	0,2094	0,0095
200	0,4429	0,0169
250	0,9184	0,0254
300	1,6102	0,0371
350	2,5682	0,0502
400	3,8923	0,0671
450	5,3113	0,0836
500	6,6605	0,1057
550	8,5056	0,1314
600	11,395	0,1578
650	14,610	0,1856
700	18,214	0,2145
750	22,385	0,2460
800	28,452	0,2788
850	31,597	0,3113
900	36,741	0,3557
950	44,027	0,3955
1000	55,075	0,4381
1250	99,148	0,6911
1500	186,75	0,9972
1750	323,18	1,3517
20000	438,23	1,7635

Согласно данным в табл. 1, время генерации одной случайной двоичной гаммы незначительно для небольших гамм даже на таком сравнительно слабом процессоре. Так, для двоичных гамм размером 500 бит на генерацию одной гаммы нужно примерно 0,106 секунд, а для гамм размером 2000 бит – 1,763 секунд. Генерация же одной случайной обратимой двоичной матрицы размером 500×500 происходит примерно за 6,6 секунд, а матрицы 1000×1000 – примерно за минуту. Однако это время быстро растет с увеличением размера матриц.

Таким образом, новый предложенный способ усиления безопасности пинг-понг протокола требует значительно меньше времени на подготовительную операцию – генерацию случайных гамм (ключа шифрования) в поле GF (2) заданного размера, чем способ, который использует обратимое хеширование [7]. На приемной стороне процедура восстановления исходных блоков сообщения вообще практически не влияет на эффективность протокола.

Следует подчеркнуть, что предложенный метод усиления безопасности пинг-понг протокола, хотя и использует гаммы для шифрования блоков сообщения, но (как и предложенный ранее метод с использованием обратимого хеширования) не является традиционным шифрованием. Нет необходимости сохранять гаммы в секрете, они передаются по открытому каналу связи после того, как легитимные пользователи пинг-понг протокола убедились, что во время квантовой передачи не было атаки пассивного перехвата, что обеспечивается режимом контроля подслушивания самого протокола. Таким образом, при использовании предложенного метода усиления безопасности пинг-понг протоколов не существует проблемы хранения и передачи секретной информации, и основное преимущество квантовых протоколов безопасной связи, т.е. отсутствие традиционного шифрования, сохраняется при использовании этого метода.

При использовании метода усиления безопасности, который основан на обратимом хешировании [7], выполняются сложные криптографические операции с использованием случайных двоичных обратимых матриц (перемежевание), а при гаммировании выполняется только простая операция XOR. Однако метод гаммирования имеет несколько меньшую безопасность, т.к. для восстановления исходного блока данных при обратимом хешировании злоумышленнику нужно перехватить как весь блок данных при его передаче в квантовом канале, так и всю соответствующую хеш-матрицу, а при гаммировании он имеет возможность сразу восстановить ту часть блока данных, которую он перехватил в квантовом канале, если перехватит также соответствующую часть гаммы. Однако возможность этого может быть сделана как угодно малой, если легитимные пользователи выберут достаточную длину блока для гаммирования так, чтобы вероятность обнаружения атаки в квантовом канале была сколь угодно малой. Если же легитимные пользователи обнаружат атаку, то они не будут передавать гамму по открытому каналу, и злоумышленник не получит никакой информации.

ВЫВОДЫ

Методы симметричного шифрования являются одними из актуальных и криптографически гарантированных методов защиты информации, которые с соответствующей модификацией могут применяться и для усиления безопасности протоколов квантовой прямой безопасной связи, в частности, для пинг-понг протокола с парами перепутанных кубитов. Предложенный в данной статье метод усиления безопасности такого протокола с помощью гаммирования блоков сообщения имеет значительно большую скорость, чем метод усиления безопасности, основанный на использовании случайных обратимых матриц [7]. При этом новый метод также сохраняет основное преимущество пинг-понг протокола – отсутствие необходимости шифрования сообщений с распределением секретных ключей, – гаммы не являются секретными ключами и передаются открыто в случае, если не было подслушивания при передаче сообщения в квантовом канале. Таким образом, предложенный в данной статье метод усиления безопасности пинг-понг протокола предпочтительнее известного ранее и является вполне приемлемым для практического применения.

Литература

[1] Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.

[2] Deng F.-G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block / F.-G. Deng, G.L. Long, X.-S. Liu // Physical Review A. – 2003. – V. 68, № 4. –042317.

[3] Wang Ch. Multi–step quantum secure direct communication using multi-particle Greenberger-Horne-Zeilinger state /Ch. Wang, F.G. Deng, G.L. Long // Optics Communications. – 2005. – V. 253, № 1. – P. 15–20.

[4] Li X.-H. Multiparty Quantum Remote Secret Conference /X.-H. Li,C.-Y. Li, F.-G. Deng et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23–26.

[5] Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X. Ji, Y.-Q. Zhang et al // Physics Letters A. –2006. –V. 354, № 1-2. – P. 67–70.

[6] Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.

[7] Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83–91.

[8] Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, issue 17. – P. 4540–4544.

[9] АграновскийА.В. Практическая криптография (серия «Аспекты защиты») / А.В. Аграновский, Р.А. Хади. – М.: Солон-Пресс, 2002.– 254 с.

[10] Диффи У. Новые направления в криптографии / У. Диффи, М.Э. Хеллман. – М.: ИЛ, 1976. –654 с.

[11] Шеннон К. Э. Работы по теории информации и кибернетике / К. Э. Шеннон. – М.: ИЛ, 1963. –832 с.

[12] Партыка Т.Л. Информационная безопасность/ Т.Л. Партыка, И.И. Попов. – М.: Форум - Инфра, 2007. –368 с.

[13] Кінзерявий В.М. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів / В.М. Кінзерявий, Є.В. Василіу, С.О. Гнатюк, Т.О. Жмурко// Захист інформації. – 2012, №2 (55). – С. 5–13.

[14] Кормен Т. Алгоритмы: построение и анализ = Introduction to Algorithms /Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн.– М.:Вильямс, 2005. – 1296 с. – ISBN 5-8459-0857-4.

[15] Overbey J. On the keyspace of the Hill cipher / J. Overbey, W. Traves, J. Wojdylo // Cryptologia. – 2005. – V. 29, № 1. – P. 59– 72.

Поступила в редколлегию 16.04.2013

Николаенко Сергей Валентинович, ассистент кафедры информационных технологий Одесской национальной академии связи им. А.С. Попова. Научные интересы: криптография, квантовая криптография, Web-программирование, базы данных.

УДК 004.056.53+530.145

Підсилення безпеки методом гамування протоколу квантового прямого безпечного зв'язку/ С.В. Ніколаєнко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 347–350.

У статті розглянуто класичний (не квантовий) спосіб підсилення безпеки пінг-понг протоколу з парами переплутаних кубітів. Цей спосіб використовує шифрування методом гамування блоків повідомлень. При цьому самі гами не є секретною інформацією і передаються відкритим каналом зв'язку тільки після того, як легітимні користувачі переконалися у відсутності атаки у квантовому каналі. Крім того, запропонований спосіб не потребує квантової пам'яті.

Ключові слова: квантова криптографія, пінг-понг протокол, метод підсилення безпеки протоколу, шифрування методом гамування, імітаційне моделювання, часові оцінки.

Табл.: 1. Бібліогр.: 15 найм.

UDC004.056.53+530.145

Improving security of quantum direct secure communication protocol by XOR encryption / S.V. Nikolaenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 347–350.

The paper considers the classical (not quantum) method of improving security of the ping-pong protocol with pairs of entangled qubits. This method uses XOR encryption of message blocks. Keys are not secret information and are transmitted via an open channel only after legitimate users convince in the absence of an attack in the quantum channel. In addition, the suggested method of security improving does not require a quantum memory.

Keywords: quantum cryptography, ping-pong protocol, method of improving protocol security, XOR encryption, simulation, time estimations.

Tab.: 01. Ref.: 15 items.

УДК 621.39:65.012.8

ОБҐРУНТУВАННЯ ВИБОРУ ЗАХОДІВ ЗАХИСТУ ХАРАКТЕРИСТИК ПРОДУКЦІЇ ВІД КОНКУРЕНТНОЇ РОЗВІДКИ

В.І. ЗАБОЛОТНИЙ, Є.В. ЗАДОРОЖНА

Стаття присвячена обґрунтуванню способів захисту інформації від конкурентної розвідки (КР) з урахуванням можливості застосування нею засобів технічних розвідок (ЗТР). Розглянуто організаційні принципи побудови системи КР, інформаційні ресурси для КР, можливі відомості з обмеженим доступом (ВзОД), що потрібно захищати, та їх ознаки, на які потрібно впливати, наведено приклад дослідження певної продукції в умовах КР, зроблено аналіз її характеристик з урахуванням тренду, запропоновані заходи захисту.

Ключові слова: конкурентна розвідка, технічні засоби розвідки, відомості з обмеженим доступом, дезінформація, приховування.

ВСТУП

З 90-х років XX сторіччя в усьому світі конкуренція стала дуже важливим фактором розвитку економіки, модернізації, інновацій. Телекомунікація, транспорт, енергетика та інші галузі економіки слугують яскравими прикладами всієї потужності конкуренції, що створює умови постійних інновацій, та швидкі темпи їх розвитку.

Через посилення конкуренції за останнє двадцятиріччя та прагнення конкурентів мати вигоду і провідне місце на ринку став стрімко розвиватися новий напрямок розвідувальної діяльності – конкурентної розвідки (еквівалентні назви – ділова розвідка, бізнес-розвідка).

Конкурентна розвідка (КР) особливо важлива на етапі підготовки до випуску нового товару. Для отримання вигоди та лідируючого місця на ринку конкурентам важливо отримати відомості про продукцію до її випуску, щоб зробити аналог, який буде кращий за параметрами, з меншими витратами на розробку. Як правило, компанії в конкурентній боротьбі використовують різні методи добування інформації про нові вироби своїх конкурентів: аналіз відкритої інформації, підкуп працівників, промислове шпигунство, зовнішнє спостереження за дослідними зразками продукції та виробничими підрозділами, у тому числі і з застосуванням засобів технічних розвідок (ЗТР).

Зазначене і актуалізує необхідність розробки обґрунтованих заходів захисту від конкурентної розвідки. Сьогодні на провідних підприємствах сформувалися організаційні структури, спрямовані як на добування конкурентної інформації, так і на захист її від розвідок. Провідні ВНЗ, у тому числі і України, готують фахівців і з добування, і з захисту конкурентно-важливої інформації (специфічна категорія підготовки "Консолідована інформація" 8.000012, що відповідає Business Intelligence та три спеціальності у галузі знань "Інформаційна безпека" 1701).

Розробка заходів захисту має дві сторони. По-перше, спрямованість на захист інформації про об'єкт захисту. Тобто стандартні заходи захисту документів, технічного захисту інформації з обмеженим доступом (ІзОД) в ході її обробки інформації на ЕОМ, обговорення вголос, а також проведення активних дезінформаційних заходів [1] у засобах масової інформації (ЗМІ), Інтернеті тощо. Цей вид діяльності з захисту ІзОД, на сьогодні, достатньо повно регламентований і, як правило, не викликає труднощів.

По-друге, захист відомостей обмеженого доступу (ВзОД) шляхом фізичного приховування [2] матеріальних зразків новітніх розробок від стороннього зовнішнього спостереження, у тому числі і від розвідки із застосуванням технічних засобів [3, 4]. Дезінформаційні заходи у ЗМІ, Інтернеті потребують підкріплення заходами технічної дезінформації [2] відносно дійсних характеристик цих розробок. Безперечно, заходи з захисту продукції інженерно-технічними засобами та організаційними заходами від спостереження потребують значних матеріальних витрат і обмежень в ході її розробки, дослідження і, часто, виготовлення.

Метою даної статті є формалізоване обґрунтування комплексу заходів захисту інформації від конкурентної розвідки в умовах її підкріплення застосуванням ЗТР. Тобто йде мова про комлексацію заходів захисту ІзОД та ВзОД. Для цього розглядаються організаційні принципи побудови системи конкурентної розвідки, проаналізовано інформаційні ресурси, що використовуються в КР, розглянено можливі ВзОД, їх ознаки [5], що необхідно захищати.

Об'єктом дослідження виступає методика вибору та обґрунтування комплексу заходів захисту характеристик матеріальної продукції з урахуванням їх покращення та попарної кореляції.

Експериментальна частина роботи полягає в застосуванні стандартного програмного забезпечення для дослідження тренду характеристик матеріальної продукції, їх розкиду та прогнозу на заданий період часу.

Дослідження проілюстроване прикладом щодо обрання та обґрунтування характеристик продукції, що підлягає захисту, запропоновано заходи їх захисту.

КОНКУРЕТНА ІНФОРМАЦІЯ

Отримання конкурентної інформації (CI – competitive intelligence) часто розглядається як відносно нова дисципліна, що з'явилася приблизно в 1980-ті роки. Оскільки обробка інформації про конкурентів є складним процесом, то використовують поняття «конкурентна розвідка», що означає систематичні та системні збір, аналіз та управління інформацією про конкурентів. Конкурентна розвідка проводиться з метою кращого розуміння роботи конкурентів для прийняття рішення та розробки такої стратегії, яка призводить до конкурентної переваги, що, в свою чергу, дозволяє досягти особливих результатів на відміну від конкурентів.

Процес КР є динамічним і циклічним та описується такою послідовністю дій: збір даних, фільтр, аналіз, прийняття рішення. Кожний етап підвищує цінність зібраної та опрацьованої інформації. Тож, конкурентна інформація – це етично багатоетапний процес, який може сильно допомогти організації.

Джерелами інформації на етапі збору інформації можуть виступати різні інформаційні ресурси. Наприклад, Інтернет-ресурси, відділи продаж, бази даних, продуктивні набори, цінові пропозиції, специфікації продуктів, клієнти конкурента, дослідження ринку (вторинна інформація), виставки, семінари, конференції, прес-релізи, корпоративна преса, корпоративна звітність, промислові огляди, аналітичні записки, галузеві звіти. Джерелами інформації на етапі збору даних можуть виступати різні інформаційні ресурси, які є відкритими або «незакритими».

Для отримання об'єктивної інформації досліджують матеріальне середовище. Існують різні методи дослідження середовища, тим самим отримуючи дані. Не виключається і використання засобів технічної розвідки. Технічна розвідка – несанкціоноване здобування конфіденційної інформації за допомогою технічних засобів та її аналіз [3].

Опираючись на літературні джерела з конкурентної розвідки [6, 7], можна сказати, що з посиленням конкуренції на ринку не виключається добування конкурентної інформації засобами технічних розвідок (ЗТР), тобто несанкціонованого здобування закритої інформації за допомогою технічних засобів та її аналіз.

Виробництво конкурентоздатної продукції, розробка споживчих товарів є успішним, коли продукція випускається раптово, першою та найкращою серед конкурентів. Це є одним із визначальних факторів лідерства на ринку, тому з метою отримання даних про продукцію конкуренти проводять дослідження матеріального виробництва. Результатом їх досліджень може бути збір даних про характеристики продукції, термін її випуску, нові технології, подальший аналіз інформації та прийняття рішення. Для забезпечення конкурентоздатності слід захищати характеристики нової продукції від технічних розвідок.

Використовуючи ЗТР існує два шляхи добування даних конкурентами: добування даних про об'єкти в знаковій формі та спостереження за матеріальними об'єктами розвідки [5]. Знакова форма становить сукупність символів, літер, цифр, звуків, які відображують предмети та явища реального світу у віртуальному світі. Предметна форма існування відомостей про об'єкти захисту проявляється самими матеріальними об'єктами реального світу у процесі виробництва й застосування продукції, технологій різного призначення також у вигляді електромагнітних, оптичних, гравітаційних, акустичних та інших полів й випромінювань, хімічних речовин [8]. Розвідка цих ефектів за допомогою ЗТР дозволяє конкурентам синтезувати дані щодо відомостей з обмеженим доступом (ВзОД), які захищають від конкурентів.

ВзОД – електромагнітні, оптичні, гравітаційні, акустичні, гідроакустичні, сейсмічні поля, радіаційні випромінювання, хімічні речовини, які є матеріальними об'єктами у процесі виробництва та застосування [8]. Більш широкий спектр фізичного прояву відрізняє предметну форму прояву даних від знакової. Але обидва види прояву даних потребують захисту від технічних розвідок.

Ознаки, що супроводжують вищеперераховані типи відомостей можуть бути причиною встановлення відомостей з обмеженим доступом технічною розвідкою. Такі ознаки надалі називатимемо «ознаками відомості» або ОВ.

Інформація та відомості з обмеженим доступом може піддатися витоку технічними каналами, модифікації та блокуванням. Це і є задачею технічного захисту інформації (ТЗІ). Але в конкурентній розвідці слід захищати ІзОД та ВзОД саме від витоку ТКВІ, щоб захистити потрібні параметри нової продукції терміново чи постійно для отримання конкурентоспроможності на ринку та вигоди від розробки.

ДОСЛІДЖЕННЯ ВЗОД

Більшість великих підприємств приділяє багато уваги КР. Нижче наведено компанії, які використовують конкурентну розвідку: Xerox, Procter & Gamble, Eastman Kodak, Ford, American Express та ін. Вважається, що єдиний тип компаній, яким не потрібна конкурентна розвідка – це компанії, які не мають конкурентів. Зловмисники або конкуренти можуть отримувати відомості нового виробу та у відповідь покращувати свій продукт, отримуючи лідерство на ринку продажів. З цього випливає необхідність розробки заходів захисту від конкурентної розвідки.

Робота [9] присвячена шляхам обґрунтування плану захисту інформації про матеріальні об'єкти в умовах ведення конкурентної розвідки з урахуванням добування об'єктивних даних засобами технічних розвідок.

Кількісні характеристики продукції, що підлягали захисту, визначались сукупністю моментів

випадкових величин і на цьому оцінювалась спрямованість заходів захисту на приховування або технічну дезінформацію характеристик.

Як видно з наведеного, прийнятий математичний апарат відображав характеристики продукції у статиці, усереднено за певний період часу – без урахування тренду – переважаючої тенденції, загального напрямку удосконалення певної характеристики продукту.

ПРОПОЗИЦІЯ ЩОДО РОЗВ'ЯЗАННЯ ЗАДАЧІ

Суть пропозиції полягає у прогнозній оцінці можливого значення кожної характеристики, що треба захищати на заданий термін часу. Прогноз здійснюється методом часового аналізу [10] тренду та прогнозування, з використанням апарату найменших квадратів. Одночасно оцінюється величина середньоквадратичного відхилення (СКВ) можливого значення оцінюваної характеристики. Якщо реальне значення заявленої характеристики лежить у межах СКВ, то вимоги щодо її захисту не будуть першочерговими. Якщо воно знаходиться за межами СКВ у кращу сторону, то дану характеристику треба захищати обов'язково. Відповідно до рекомендацій, наведених у [10], проводити заходи дезінформації, спрямовуючи фальшиве значення характеристики у межу СКВ, а краще за межу СКВ у гіршу сторону, де захист взагалі непотрібний.

Даний аналіз можна робити, використовуючи стандартне програмне забезпечення, наприклад, Microsoft Office 2010 Excel.

АЛГОРИТМ РОЗВ'ЯЗАННЯ ЗАДАЧІ

1. Складається опис відомих виробів у формі таблиці 1.

2. Окремо формуються: рядок із конкретними характеристиками для нового виробу, які можуть складати як ВзОД, так і відкриті дані та рядок із характеристиками фальшивого об'єкта (об'єкта прикриття), під який дезінформуватиметься новий виріб.

3. Експертна група проводить ранжування конкретних характеристик нового виробу за ступенем важливості щодо їх захисту від конкурентів.

4. Обчислюють тренд часового ряду зміни та прогнозу кожної з характеристик та середньоквадратичне відхилення у часі (рисунки 1 та 2).

5. Порівняльним аналізом виявляється взаємне положення оцінки прогнозної та реальної характеристик.

6. Приймається рішення щодо планування заходів захисту характеристики виробу або із погіршенням характеристик (дезінформація), або відмови здійснення заходів захисту.

У наведеному алгоритмі можна використовувати метод попарного аналізу характеристик виробу, запропонований у [9]. У даному випадку додатково провести:

1) перевірку на узгодженість заходів захисту характеристик низьких рангів заходам захисту характеристик високих рангів за коефіцієнтами парної регресії і відповідним чином їх відкоригувати;

2) скласти сукупний опис відомих виробів і нового виробу, з характеристиками, що пропонується показувати конкурентам, у формі таблиці 1 (змінений останній рядок ВзОД на характеристики, які потрібно висунути конкурентам);

3) визначити ознаки ВзОД, які треба захищати способами дезінформації і приховування. Перевірити можливість реалізації запропонованих заходів в ході виготовлення та випробування нових виробів. За неможливості – повторювати дослідження, до досягнення бажаного результату.

7. Скласти план заходів дезінформації і приховування від конкурентної розвідки за розділами:

– заходи дезінформації у відкритих джерелах інформації, Інтернеті тощо;

– заходи забезпечення контрольованої зони навколо об'єктів з виготовлення та випробування нових виробів;

– заходи захисту від безпосереднього спостереження та ЗТР за виготовленням і випробуванням виробів із-за меж контрольованої зони способами технічної дезінформації та приховування.

Даний алгоритм дає основу для обґрунтованої розробки комплексу захисту нових виробів від конкурентної розвідки.

ПРИКЛАД РОЗВ'ЯЗАННЯ ЗАДАЧІ

Як виріб для прикладу було запропоновано взяти автомобілі представницького класу (класу F) різних років випуску, різних фірм та порівнювати їх за характеристиками. Для обґрунтованого аналізу характеристик визначили вимоги до автомобілів представницького класу відповідно до аудиторії, на яку вони розраховані та цілі, які перед ними ставлять користувачі. На основі визначення та вимог автомобілів класу F, можна сказати, що головними з їх характеристиками є:

1) розмір;
2) швидкість;
3) потужність;
4) комфорт;
5) безпека.

Якщо вищеперераховані характеристики є основними вимогами класу F, та говорячи про виготовлення автомобілів у контексті конкурентної розвідки, то ці характеристики виступають даними предметної форми прояву, тобто відомостями з обмеженим доступом.

Для захисту від конкурентної розвідки часто використовують метод маскування та дезінформації [1]. Дезінформація – це спосіб дії на людину, коли їй надається інформація, що вводить її в оману відносно істинного положення справ, спроба створити хибне враження і, відповідно, підштовхнути до бажаної діяльності та/або бездіяльності. Дезінформація може спрямовуватися до нав'язування конкурентам відомостей про споживчі характеристики виробів: погіршених або завищених. У відповідь на це конкуренти

реагують недовірою до отриманих даних та посиленням розвідки або довірою, якщо дані мають невелике відхилення від середнього значення цього параметру такої продукції різних виробників та відповідають прогнозам розвитку параметрів цієї продукції з часом.

Виникає необхідність зваженості обґрунтування та проведення заходів дезінформації при припустимих заходах приховування. Для забезпечення довіри конкурентів до результатів розвідки в галузі автомобілебудування необхідно створити дані з невеликим відхиленням від очікуваних, типових для даної продукції.

За допомогою методу порівняння було проведено дослідження характеристик автомобілів представницького класу, випущених у період 2003-2013 років різних марок, наприклад: Audi A8, Lexus LS, BMW 7, Mercedes-Benz S, Rolls-Royce Phantom, Maybach 57, Maserati Quattroporte та ін. Для кожного з років цього періоду взято автомобілі, випущені в той рік з їх технічними характеристиками. Після цього було пораховано середнє значення кожної характеристики. Характеристиками послугували відомості згідно з вимогами, перерахованими вище: розмір (споряджена маса, габарити), швидкість (максимальна швидкість, час розгону до швидкості 100 км/год), потужність у кінських силах, об'єм двигуна у куб. см. Оскільки після аналізу даних та порівняння ставилося за мету дослідити тенденцію зміни характеристик автомобілів з часом та створення «правильної» (з результатом довіри конкурентів) дезінформації для випуску нового автомобіля у майбутньому, було порівняно автомобілі різних років випуску. Так, після збору даних визначені середні значення кожної з характеристик за кожний рік та тренд (тенденцію) їх розвитку. Крім того, був розрахований прогноз значень параметрів на наступні 2 роки відповідно до лінійного тренду з апроксимацією методом найменших квадратів. Порівняння існуючих автомобілів класу «люкс» за основними характеристиками та прогноз на 2014–2015 рр. наведено в табл. 1.

Таблиця 1

Значення характеристик

Рік	Максимальна швидкість, км/год	Час розгону до 100, км/год	Об'єм двигуна, куб. см	Довжина, м
2003	250	6,07	4775	5,21
2004	245	6,50	4748	5,00
2005	258	6,26	4846	5,27
2006	253	5,54	5543	5,51
2007	254	6,74	4919	5,33
2008	258	6,58	4880	5,37
2009	257	5,02	4824	5,16
2010	268	5,56	4947	5,26
2011	239	5,05	5156	5,28
2012	247	6,01	4252	5,22
2013	252	5,80	4013	5,18
2014	252	5,45	4474	5,26
2015	251	5,41	4343	5,25

Отримані прогнозні значення характеристик можна використовувати для обрання способу їх захисту шляхом приховування або дезінформації, у тому числі і технічної за підходом, наведеним у п.6 алгоритму. Для даного прикладу конкретні характеристики нового автомобіля авторами не пропонувались.

Для ілюстрації наведено результат аналізу та прогнозу у вигляді графіка тренд характеристики «час розгону до швидкості 100 км/год», наведеного на рис. 1.

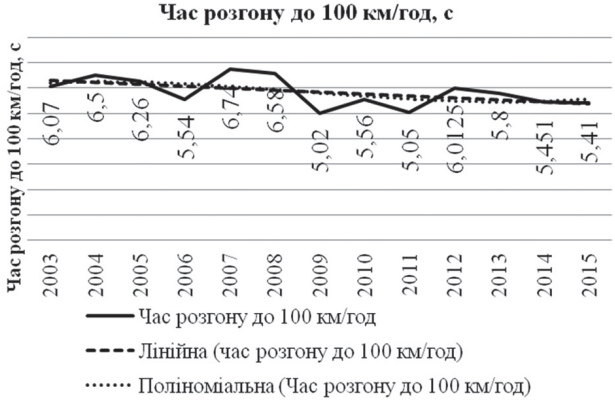


Рис. 1. Тенденція розвитку параметру «час розгону до 100 км/год» за період 2003–2015 роки

На рис. 2 наведено розкид параметру «час розгону до 100 км/год, с», тобто пораховано середньоквадратичне відхилення за кожний з років. За цим графіком видно загальну тенденцію: відхилення зменшується, отже, вимоги щодо відтворення значення характеристик для технічної дезинформації фальшивого об'єкта стають все більш суворими.

Рис. 2. Тенденція розвитку значень середньоквадратичного відхилення параметру

Знаючи таку тенденцію розвитку параметру можна користуватися цим при випуску нової продукції. Із застосуванням дезінформації як методу захисту від конкурентної розвідки з урахуванням можливості підтвердження результатів засобами технічних розвідок слід опиратися на даний прогноз та давати конкурентам відкриту інформацію, яка не є сильно відхиленою від середнього значення для цієї групи продукції з урахуванням тренду.

ВИСНОВКИ

Конкурентна розвідка та захист від неї особливо важливі на етапі підготовки та випуску нового товару.

В роботі наведено організаційні принципи побудови системи конкурентної розвідки на підприємстві, інформаційні ресурси, що використовуються в КР, можливі ВзОД та їх ознаки, що необхідно приховувати, зроблено дослідження певної продукції – автомобілів представницького класу, зробивши аналіз їх характеристик з урахуванням тренду.

В конкурентній розвідці існує два шляхи захисту ВзОД: дезінформація та приховування, причому реакція конкурентів може бути різною в залежності від відомостей розробників продукції: при недовірі конкурентів розвідка посилюється; приховування також посилює розвідку. Розвідка призупиняється через довіру, яка може базуватися на невеликому відхиленні одержаних ВзОД від очікуваних, типових для даної групи продукції.

Розв'язання задач обгрунтованого захисту від КР можна проводити з використанням математичного апарату аналізу часових рядів.

Застосування методу проілюстровано на прикладі.

Література

[1] Кузин А. Дезинформация и активные средства в бизнесе / Кузин А., Нежданов И., Ющук И. – Казань, 2009. – 134 с.

[2] Меньшаков Ю.К. Основы защиты от технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ. ред. М.П.Сычева. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2011. – 478 с.

[3] Меньшаков Ю.К. Виды и средства иностранных технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ. ред. М.П.Сычева. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. – 656 с.

[4] Меньшаков Ю.К. Теоретические основы технических разведок: Учеб. пособие / Ю.К. Меньшаков; под ред. Ю.Н. Лаврухина – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

[5] Заболотний В.І., Класифікація технічних каналів витоку інформації / В.І. Заболотний // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2003. Вип. 134.

[6] Нежданов И.Ю. Технологии разведки для бизнеса / Нежданов И.Ю. –М.: «Ось-89», 2009.

[7] Характерні особливості конкурентної розвідки та промислового шпигунства/ТкачукТ.//Персонал.– 2007. – № 2. – С. 72 – 79.

[8] Захист інформації. Технічний захист інформації. Основні положення.: ДСТУ 3396.0-96. – [Чинний від 01.01.1997 р.]. – К.: Держспоживстандарт України, 1997. – 45 с.

[9] Обгрунтування плану захисту об'єктів від конкурентної розвідки / В.І. Заболотний, А.А. Абузова, Б.В. Волобуєв // Науково-технічний збірник «Радіотехніка».

[10] Мишулина О. А. Статистический анализ и обработка временных рядов. — М.: МИФИ, 2004. — С. 180.

Надійшла до редколегії 18.04.2013

Задорожна Євгенія Вадимівна, студент 4-го курсу спеціальності БІКС ХНУРЕ. Наукові інтереси: технічний захист інформації, конкурентна розвідка та захист від неї.

Заболотний Володимир Ілліч, канд. техн. наук, професор кафедри БІТ ХНУРЕ. Наукові інтереси: технічний захист інформації.

УДК 621.39:65.012.8

Обоснование выбора средств защиты характеристик продукции от конкурентной разведки / В.И. Заболотный, Е.В. Задорожняя // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 351–355.

Статья посвящена обоснованию способов защиты информации от конкурентной разведки (КР) с учетом возможности применения ею средств технических разведок. Рассмотрены организационные принципы построения системы КР, информационные ресурсы для КР, возможные сведения с ограниченным доступом, которые нужно защищать, и их признаки, на которые нужно влиять, приведен пример исследования определенной продукции в условиях КР, сделан анализ ее характеристик с учетом тренда, предложен подход к обоснованию мер защиты.

Ключевые слова: конкуретная разведка, технические средства разведки, сведения с ограниченным доступом, дезинформация, сокрытие.

Табл.: 1. Ил.: 2. Библиогр.: 10 назв.

UDC 621.39:65.012.8

Substantiation of choosing the methods of protection of the production characteristics from competitive intelligence / V.I. Zabolotnyi, E.V. Zadorozhnaya // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 351–355.

The paper is devoted to the substantiation of methods of information protection against competitive intelligence (CI) in view of the fact that CI can apply technical reconnaissance means. Organizing principles of competitive intelligence (CI); information recourses for CI; possible information with restricted access that must be protected and its features should be influenced on are considered. An example of investigating definite production under conditions of CI is given. An analysis of the characteristics of the production including a trend is done and an approach to substantiating protection measures is suggested.

Keywords: competitive intelligence, technical reconnaissance, information with restricted access, misinformation, hiding.

Tab.: 1. Fig.: 2. Ref.: 10 items.

УДК 004.94

КОНТРОЛЬ ТА ВІЗУАЛІЗАЦІЯ СТАНУ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

В.М. ЧИЖ, М.П. КАРПІНСЬКИЙ, С.М. БАЛАБАН

Розглянуто важливість та складність організації ефективних методів контролю за станом надійності поширення інформації у бездротових сенсорних мережах. Запропоновано оригінальні методи контролю за параметрами сигналів окремих або компактно розташованих сенсорів та візуалізації атак на них. Обґрунтовано доцільність використання кластерної моделі зі симплексним покриттям його поля для візуалізації областей трансформації сенсорів, сигнали яких зазнали атак.

Ключові слова: функціональна безпека, інформаційні системи, сенсор, бездротова сенсорна мережа, кластер, візуалізація, трансформація, стаціонарна сигнальна точка, фіктивна сигнальна точка, еталонна сигнальна точка.

ВСТУП

Темпи розвитку та масштаби використання інформаційних систем (ІС), складовими частинами яких є бездротові сенсорні мережі (БСМ), ставлять перед їх розробниками ряд складних завдань. Особливе місце серед них займає забезпечення надійності роботи мережі та її захищеність, а також, безпека інформації. Успішне вирішення вказаних завдань значною мірою забезпечує наявність простих і ефективних методів контролю та візуалізації параметрів, що характеризують роботу ІС. Значну увагу,при цьому, приділяють виявленню і локалізації наслідків атак на сигнали сенсорів, які працюють у мережі. Але сьогодні відсутня інформація про методи контролю та візуалізації, які б дозволяли одночасно відслідковувати атаки на різні параметри сигналів.

Під візуалізацією функціональної безпеки ІС зі застосуванням БСМ розуміють контроль, виявлення і відображення атак на інформацію. Зокрема, в літературних джерелах [1, 2, 3, 4] наведено результати візуалізації атак типу «wormhole», які призводять до зміни сили сигналів у мережі. Така візуалізація дозволяє виявити вплив атаки на окремий сенсор, як який виступає інформаційний вузол (ІВ), або групу компактно розміщених сенсорів.

Для відслідковування атак на параметри сигналів окремих вузлів ІС запропоновано використання симплексно-кластерного моделювання ІС. [5, 6, 7]. При такому моделюванні передбачено створення візуалізованої форми реконструйованої топології мережі ІВ із використанням сітки рівносторонніх трикутників, у вершинах яких розміщені сигнальні точки (СТ), які представляють ІВ.

Створення методів аналізу роботи симплексно-кластерних моделей і візуалізації атак на параметри сигналів ІВ, які входять до даних моделей.

1. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

При стабільній роботі ІВ у «польових умовах» кластер (рис. 1), як це було відмічено в роботі [5], має геометрію двовимірного евклідового простору із функціональними зв'язками (ФЗ) довжиною l. Атака на ІВ сигналом є змінює довжину ФЗ на величину $l_\varepsilon = l(\varepsilon)$ і, здійснює переміщення СТ, положення яких залежить від них.

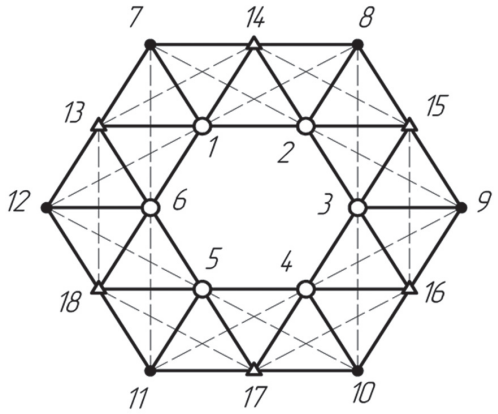


Рис. 1. Кластерна модель зі схемою поділу на симплекси [4С]

1.1. Метод 4-точкових симплексів (метод [4с])

Візуалізація атаки у кластері ґрунтується на можливості переміщення сигнальних точок у залежності від довжини ФЗ [5, 7]. Візуалізація реалізується завдяки покриттю поля кластера 4-точковими симплексами ([4С]). При стабільній роботі ІВ простір кластера заповнений ромбами, в яких п'ять відстаней між сигнальними точками є ФЗ довжиною l, а шоста відстань – друга діагональ ромба – геометричний зв'язок (ГЗ) довжиною $d = \sqrt{3}l$. Геометрія кластера при здійсненні атаки на один або декілька джерел інформації зміниться (відповідні ФЗ отримають видовження).

За даними довжин ФЗ, комп'ютер вибудує нові положення СТ кластера, відобразить трансформацію кластерного поля навколо СТ, і здійснить візуалізацію атакованих сенсорів у конфігураційному просторі комп'ютера.

В роботі [7] проаналізовано утворення областей трансформації при атаці на один і два сенсори.

При атаці на один сенсор утворяться три типи [4С] (рис. 2):

– [4С] з частковою трансформацією (ЧТр), яка визначається двома ФЗ із видовженнями $l_\varepsilon = l(\varepsilon)$ (рис. 2, *б*). В таких [4С] один трикутник знаходиться в області трансформації, а інший — поза нею. Трансформація симплекса призводить до утворення тривимірного геометричного об'єкта з нульовим об'ємом, складеного із двох трикутників, зігнутих вздовж спільної основи – функціонального зв'язку, який не змінюється і залишає нерухомими кінці відрізка (сигнальні точки);

– [4С] з повною трансформацією (ПТр) визначається трьома ФЗ із видовженнями $l_\varepsilon = l(\varepsilon)$ (рис. 2, *в*). Такі [4С] не можуть бути реалізованими у двовимірному просторі кластера. Вони утворять тривимірні геометричні об'єкти у вигляді трикутної піраміди. В основі піраміди знаходяться три нерухомі СТ, з'єднані двома функціональними зв'язками довжиною l і геометричним зв'язком довжиною $d = \sqrt{3}l$. Довжина висоти піраміди здійснює оцінку ступеня атаки на сенсор [5].

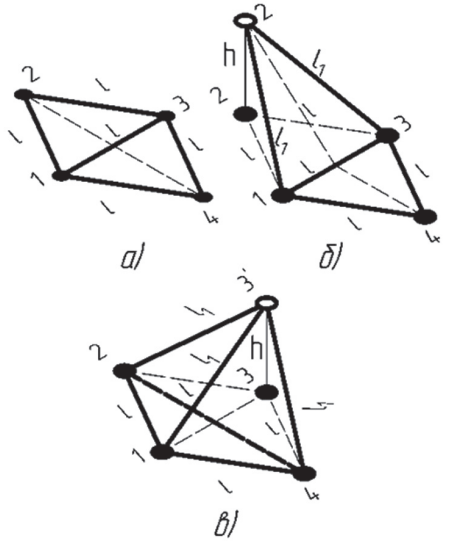


Рис. 2. Типи трансформації симплекса

В залежності від того, якому класу належить сигнальна точка, яка визначає атакований ІВ, отримуємо різні області трансформації у кластері (рис. 3).

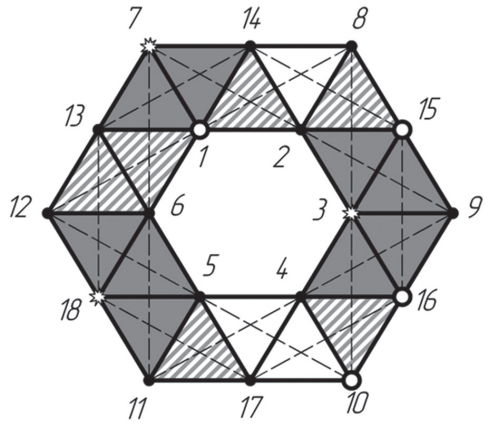


Рис. 3. Області трансформацій при атаці на сенсори, які представлені сигнальними точками різних класів

Якщо атаку здійснено на ІВ, представленими СТ, які є вершинами зовнішнього шестикутника (СТ – c_7, c_8, c_9, c_{10}, c_{11}, c_{12}), то в область трансформації входять три [4С]. При цьому один симплекс отримує ПТр, а два інші, які в перетині із цим симплексом мають його складові, отримують ЧТр. Всі інші 15 [4С] залишаться у вигляді первинних ромбів двовимірного простору кластера (рис. 3).

Якщо атаку здійснено ІВ, які у кластері представлені СТ – серединами сторін зовнішнього шестикутника(СТ – c_{13}, c_{14}, c_{15}, c_{16}, c_{17}, c_{18}), то в область трансформації попадають чотири [4С]. При цьому два симплекси отримують ПТр, а два інші, які в перетині із цими симплексами мають спільні складові, отримують ЧТр. Інші 14 [4С] зберігатимуть форму ромбів.

Якщо атаку здійснено на сенсори, які представлені у кластері СТ – вершинами внутрішнього шестикутника (СТ – c_1, c_2, c_3, c_4, c_5, c_6), то в область трансформації входять п'ять [4С]. При цьому три симплекси отримують ПТр, а два, які в перетині із цими симплексами мають спільні геометричні складові, отримують ЧТр. 13 симплексів кластера не задіяні в трансформаційних процесах і зберігають початкову форму ромба.

Необхідно зазначити, що рис. 3 можна розглядати, як одночасну атаку на три сенсори, які в кластері представлені сигнальними точками c_3, c_7 і c_{18}. Аналіз показує, що в області повної, часткової і нульової трансформації входять по 6 [4С].

На рис. 4 зображено області повної трансформації у кластері при здійсненні атак на ІВ, представлених сигнальними точками різних класів, а на рис. 5, відповідні візуальні зображення областей ПТр

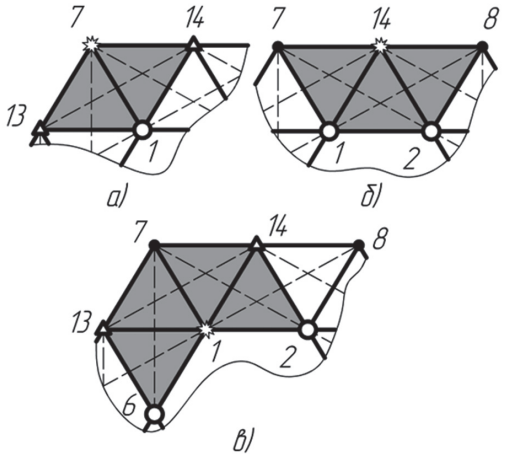


Рис. 4. Області трансформації кластера при атаці на один сенсор

В роботі [7] визначено також області трансформації кластера при одночасній атаці на два ІВ, які належать одному [4С] (рис. 6).

При атаці на два сенсори одного [4С] кластера можливими є випадки переміщення двох СТ (рис. 6), які визначаються: двома ФЗ (рис. 6, *а*); трьома ФЗ при розміщенні СТ на кінцях малої

діагоналі ромба, яка є також ФЗ (рис. 6, *б*); трьома ФЗ для однієї СТ і двома ФЗ для іншої при розміщенні сигнальних точок на кінцях однієї із сторін ромба (рис. 6, *в*).На рис. 7 зображено області ПТр кластера при таких трансформаціях [4С].

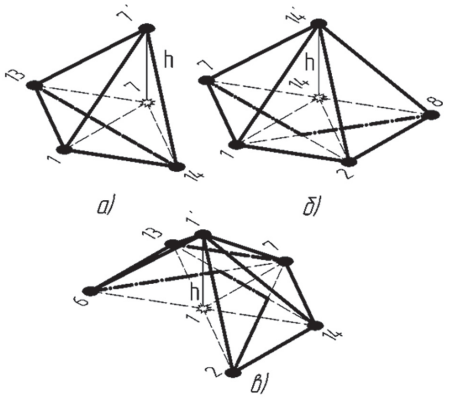


Рис. 5. Візуальне зображення областей трансформації за методом [4С]

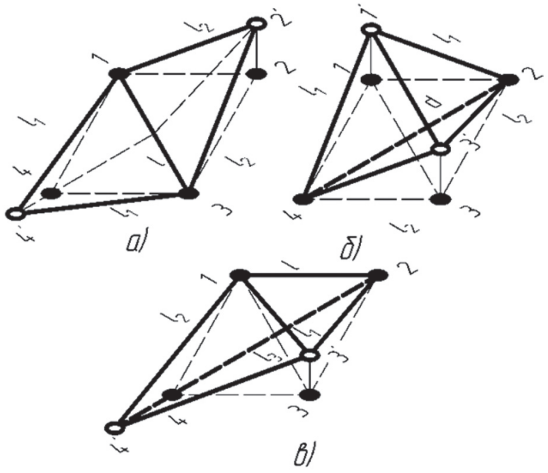


Рис. 6. Типи трансформації [4С] при двох атакованих сенсорах

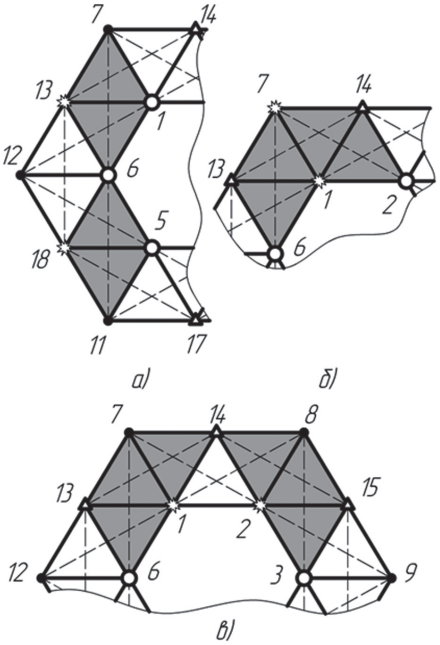


Рис. 7. Області ПТр кластера при атаці на два сенсори в одному [4С]

1.2. Метод фіктивних сигнальних точок (метод ФСТ)

Основним завданням, яке виникає при розгляді методу [4С], є необхідність однозначного визначення області ПТр кластера при здійсненні атак на сенсори. Задача визначення області ПТр вирішується використанням методу фіктивних сигнальних точок (ФСТ). За цим методом у кластері, який здійснює візуалізацію роботи сенсорів, при виникненні нестандартної роботи сенсора,функціональні зв'язки отримують видовження. В кінці видовження утворюється нове фіктивне положення СТ, яка у кластері представляє атакований сенсор. Здійснивши такі ж самі видовження із іншими ФЗ, які з'єднують СТ із сусідніми СТ, ми отримаємо (рис. 8): три ФСТ атакованого сенсора, якщо СТ знаходиться у вершині зовнішнього шестикутника кластера; чотири ФСТ атакованого сенсора, якщо СТ знаходиться на середині сторін зовнішнього шестикутника; п'ять ФСТ атакованого сенсора, якщо сигнальна точка є вершиною внутрішнього шестикутника.

З'єднавши ФСТ між собою і з місцем розміщення СТ при стабільній роботі сенсора, отримуємо плоскі геометричні об'єкти, які із симетрією відносно початкового положення СТ відображують структуру області ПТр у кластері при атаках на сенсори. Спроба з'єднати ФСТ в одну точку призводить до переміщення СТ атакованих сенсорів у третій вимір і створення візуалізації тривимірних геометричних об'єктів, які досліджувались методом [4С].

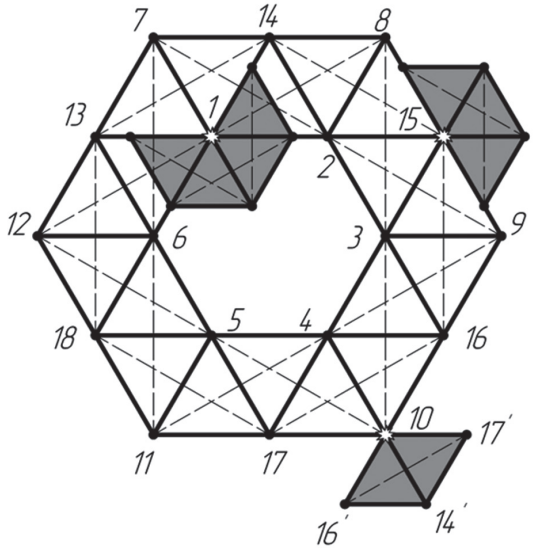


Рис. 8. Одинарний дослідний симплекс

На рис. 9 показано деякі приклади атак на два сенсори одного симплекса: рис. 9, *а* представляє атаку на два сенсори, сигнальні точки яких є вершиною внутрішнього шестикутника і серединою сторони зовнішнього шестикутника; рис. 9, *б* – атаку на сенсори, представлені сигнальними точками, одна з яких є вершиною, а інша – серединою зовнішнього шестикутника; рис. 9, *в* і 9, *г*

представляють атаки на сенсори, якщо СТ є вершинами зовнішнього і внутрішнього шестикутників; рис. 9, *д* – атаку на сенсори, представлені СТ, які є серединами двох сусідніх сторін зовнішнього шестикутника.

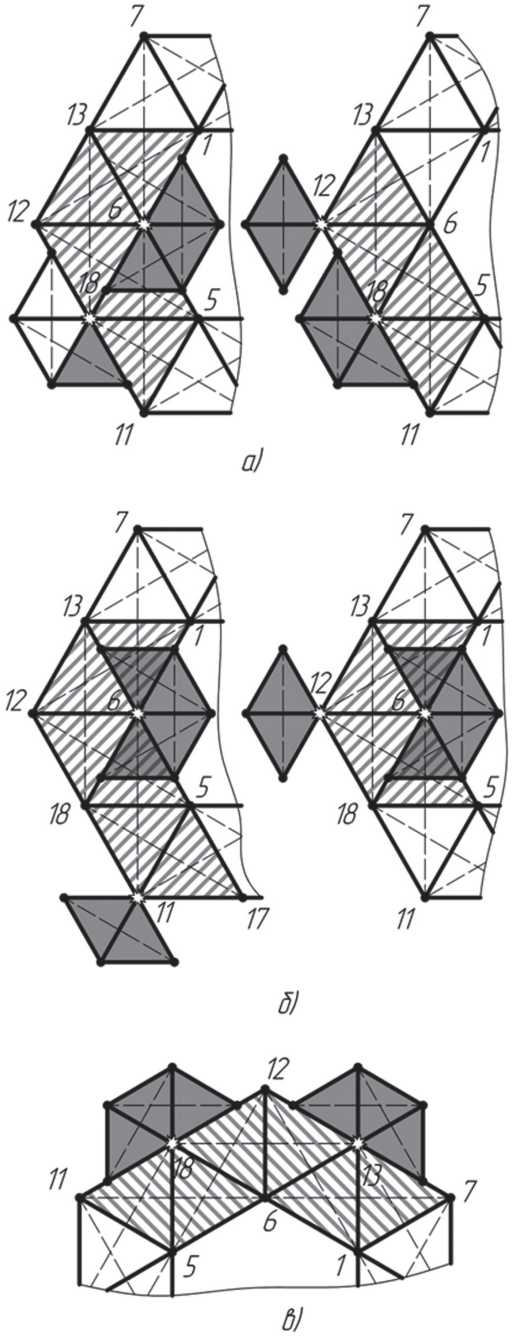


Рис. 9. Приклади атак на два сенсори при використанні методу ФСТ

1.3. Метод еталонних сигнальних точок (метод ЕСТ)

Метод еталонних сигнальних точок полягає в тому, що на першому етапі у 4-точковому симплексі всі ФЗ визначаються одними і тими ж параметрами еталонного сенсора (ЕС). Таким чином утворюється симплекс із п'ятьма рівними ФЗ довжиною l і одним геометричним зв'язком, довжиною $d = \sqrt{3}l$. Такий [4С]має форму ромба. Параметри підозрілого на атакованість сенсора подаються у положення [4С], яке визначається трьома ФЗ(СТ малої діагоналі ромба).

Видовження трьох ФЗ спричинить трансформацію плоского [4С] у тривимірний [4С] у формі трикутної піраміди із вершиною у СТ, що визначає атакований сенсор. Висота піраміди, в цьому випадку, характеризуватиме ступінь атаки на сенсор [5] (рис. 10).

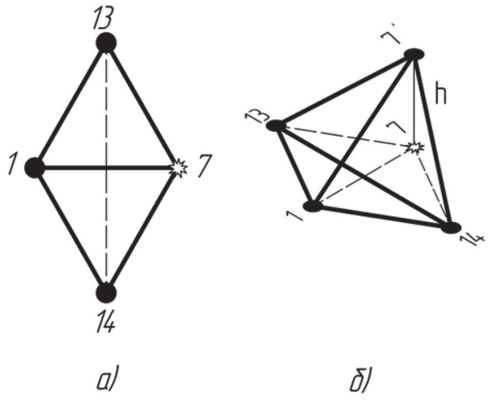


Рис. 10. Одинарний досліджуваний симплекс

Якщо внаслідок атаки на сенсори кластера (на рисунку позначені «*е*») утворюється область ПТр, то доцільно параметри кожного сенсора цієї області дослідити за допомогою такого ЕС. У цьому випадку можна утворити дослідницькі кластери, які складаються із двох, чотирьох, восьми, шістнадцяти [4С], кожний з яких визначається трьома СТ, що перебувають у стані спокою. Четверта СТ кожного [4С] даватиме характеристику атаки на сенсор (рис. 11, 12).

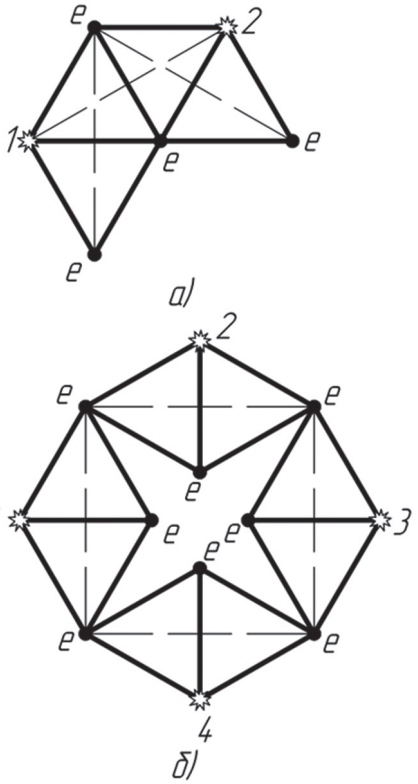


Рис. 11. Досліджувані кластери із двох і чотирьох [4С]

Розглянуті дослідні кластери (рис. 11, 12) характеризуються тим, що в них на один досліджуваний сенсор припадає два ЕС.

З метою зменшення їхньої кількості є можливість утворити інші типи кластерів, у яких крім утворення трикутних пірамід виникають і інші тривимірні симплекси, складові яких стають гранями трикутних пірамід.

На рис. 13 зображено дослідні кластери, які складаються із шести, десяти і 18-ти СТ для дослідження, відповідно, двох; чотирьох та восьми атакованих ІВ.

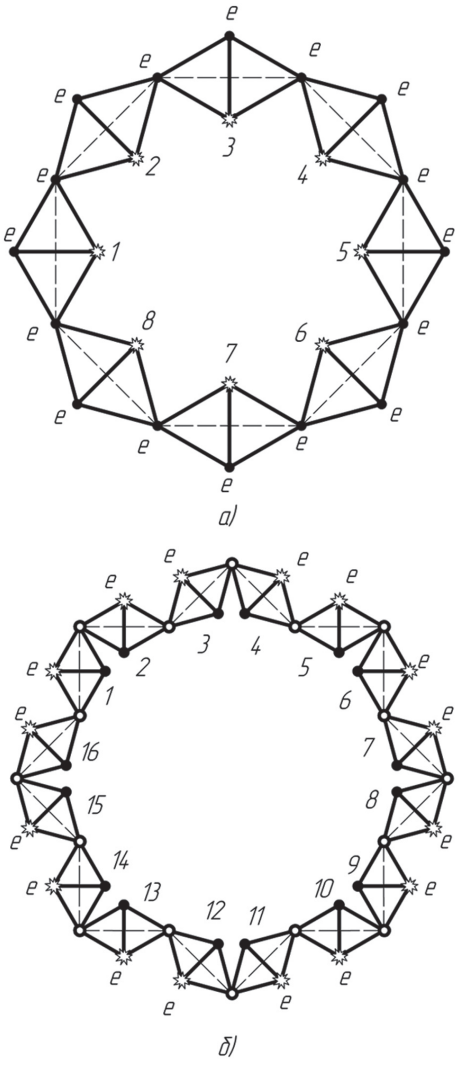


Рис. 12. Досліджувані кластери із восьми і шістнадцяти [4С]

Блок типу (рис. 13, *а*) дає можливість формувати більш складні кластерні структури, в яких відбувається зменшення кількості еталонних сенсорів (рис. 13, *б*, 13, *в*).

Можна скласти послідовність відношень кількості еталонних сенсорів до кількості досліджуваних сенсорів:

$$\frac{4}{2}=2\,,\quad \frac{6}{4}=1{,}5\,,\quad \frac{8}{6}=\frac{4}{3}\approx 1{,}33\,,$$

$$\frac{10}{8}=1{,}25\ldots,\quad \frac{2(n+1)}{2n},\ldots$$

Збільшуючи кількість початкових блоків *n* типу рис. 13, *а*, ми в границі отримаємо одиницю:

$$\lim_{n\to\infty}\frac{2(n+1)}{2n}=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)=1\,.$$

Це означає, що при великій кількості блоків відношення кількості еталонних сенсорів до кількості досліджуваних сенсорів близьке до одиниці.

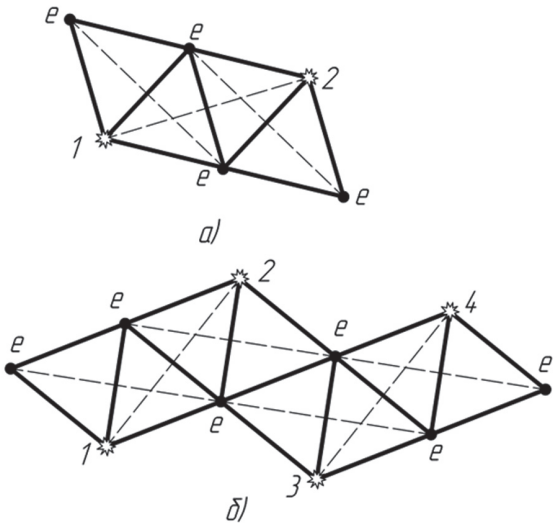


Рис. 13. Кластерні структури більш складних типів

1.4. Метод стаціонарних сигнальних точок (метод ССТ)

Цей метод дозволяє реалізувати інший вид візуалізації атак на ІВ, які моделюються кластером у конфігураційному просторі комп'ютера. Він ґрунтується на тому, що первинне положення СТ фіксується у кластері. Утворена плоска структура кластера із стабільно визначеними положеннями СТ і ФЗ між ними стає жорстким плоским каркасом. Сигнальні точки залишаються нерухомими і при здійсненні атак на ІВ. Зміна характеру роботи ІВ або групи ІВ спричиняє зміну довжин відповідних ФЗ.

Стаціонарність СТ у кластері перетворює ФЗ із відрізків у дуги кіл, які з'єднують сигнальну точку атакованого ІВ із сусідніми СТ. Таким чином, область ПТр кластера складатиметься із групи взаємозв'язаних трикутників, дві сторони кожного з яких перетворюються на дуги, що з'єднують СТ із точкою – представником атакованого ІВ. Сама ж область трансформації отримає локальне викривлення у вигляді, подібному до раковини молюска. Необхідно відмітити, що при використанні такої візуалізації зникає поняття часткової трансформації. Крім цього, якщо необхідно визначити горизонтальний зв'язок, то він знаходитиметься у плоскому полі каркасу кластера і не змінює своєї довжини.

Це нагадує ситуацію, коли на нерухомий каркас натягнути гумову плівку, зафіксовану у 18-ти точках і по периметру, який визначає ФЗ, які не змінюються внаслідок здійснення атаки. Змінені у довжині, внаслідок атаки на ІВ, ФЗ стають

дугами кіл, відділеними хордами, довжиною l. Дуги мають своїм початком зафіксовану СТ – представника атакованого ІВ. Кінці дуг фіксуються у сигнальних точках, які визначають ФЗ у створеному при стабільній роботі ІВ каркасу кластера.

Внаслідок того, що при створенні кластера із стабільною роботою ІВ, положення сигнальних точок визначається функціональними зв'язками довжиною l між точками то, на відміну від попередніх методів цей каркас (поле кластера) достатньо представити заповненим множиною трикутників. Тому визначення геометричних зв'язків потрібне лише при вирішенні конкретних задач, які можуть виникати.

На рис. 14 показано візуалізацію атак на ІВ, для яких представниками у кластері є СТ: вершини (рис. 14, *а*) та середини сторін (рис. 14, *б*) зовнішнього шестикутника; вершини внутрішнього шестикутника (рис. 14, *в*).

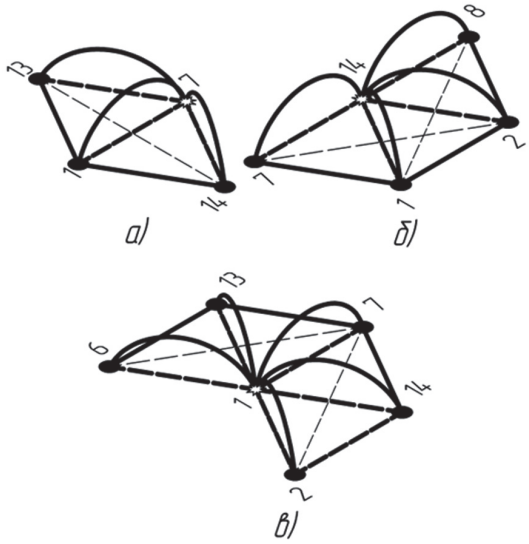


Рис. 14. Візуальне зображення областей повної трансформації за методом ССТ

ВИСНОВКИ

Доведено доцільність у процесі моделювання БСМ розглядати як модель кластер у вигляді плоскої замкнутої шестикутної геометричної структури, складеної із 18 сигнальних точок, з'єднаних за допомогою 36 однакових відрізків. Розглянуто чотири методи виявлення і дослідження областей трансформації кластера при здійсненні атаки на один і два сенсори, які представлені у кластері сигнальними точками одного 4-точкового симплекса.

Література

1. Majid Meghdadi. A Survey of Wormhole-based Attack sand their Counter measures in Wireless Sensor Networks [Електронний ресурс] // Department of Electrical Engineering IndianInstitute of Technology. – New Delhi, 2011. – Volume 28 Режим доступу: http://www.tr.ietejournals.org/ article. asp?issn= 0256-4602; year = 2011; volume=28;issue=2;spage=89;epage=102;aulast=Meghdadi. – Назва з екрану.
2. A. Becher. Tampering with motes: Real-world physical attacks on wireless sensor networks / A. Becher, Z. Benenson, M. Dornseif // volume 3934 of Lecture Notesin Computer Science, In J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, editors, SPC, – 2006. – Pages 104-118.
3. Hyunsang Choi. Fast detection and visualization of network attacks on parallel coordinates / Hyunsang Choi, Heejo Lee, Hyogon Kim // Computers & Security. – July 2009. – Issue 5. – Pages 276–288
4. Пат. на корисну модель 64391 Україна: МПК H04W 12/00 Спосіб візуалізації [Текст] / Карпінський В.М., Євтух П.С., Боровік Б.Л., Карпінський М.П.; власник патенту Тернопільський національний технічний університет ім. І. Пулюя. – № u 2011 03578; заявл. 25.03.11; опубл. 10.11.2011, Бюл. № 21. – 4 с.
5. Демчишин О. Кластерна модель комп'ютерної візуалізації мережі сенсорів [Текст] / О. Демчишин // Вісник Тернопільського національного технічного університету. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2012. – Т. 18, № 2. – С. 120–132.
6. Чиж В. Геометричне моделювання деяких атак на сигнали у бездротових сенсорних мережах / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Матеріали 14-ї міжнародної науково-практичної конференції, "Прикладна геометрія та інженерна графіка". – Мелітополь: ТДАУ, 2012. – Вип. 4. – С. 195–201.
7. Чиж В. Використання кластерної моделі для розрахунку надійності бездротової сенсорної мережі / В. Чиж, О. Демчишин, М. Карпінський, С. Балабан // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ: Видавництво СНУ ім. В. Даля, 2012. – Вип. № 8. – С. 92–96.

Надійшла до редколегії 23.04.2013

Чиж Віталій Михайлович, аспірант кафедри «Комп'ютерні науки» Тернопільського національного технічного університету ім. Івана Пулюя. Наукові інтереси: кластерні системи, безпека інформаційних систем.

Карпінський Микола Петрович, доктор технічних наук, професор, Prof. Dr. sc. nat., Chairman of Computer Science Division of University of Bielsko-Biala, Bielsko-Biała. Наукові інтереси: спеціалізовані комп'ютерні мережі, безпровідні інформаційні технології та системи їх безпеки.

Балабан Степан Миколайович, кандидат технічних наук, доцент, доцент кафедри «графічного моделювання» Тернопільського національного технічного університету імені Івана Пулюя. Наукові інтереси: енергозберігаючі технології, екологічні проблем і проблем геометричного моделювання.

УДК 004.94

Контроль и визуализация состояния функциональной безопасности информационных систем с применением беспроводных сенсорных сетей / В.М. Чиж, М.П. Карпинский, С.М. Балабан // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 356–362.

В статье рассмотрены важность и сложность организации эффективных методов контроля за состоянием надежности распространения информации в беспроводных сенсорных сетях. Предложены оригинальные методы контроля параметров сигналов отдельных или компактно расположенных сенсоров и визуализации атак на них. Обоснована целесообразность использования кластерной модели с симплексным покрытием его поля для визуализации областей трансформации сенсоров, сигналы которых подверглись атакам.

Ключевые слова: функциональная безопасность, информационные системы, сенсор, беспроводная сенсорная сеть, кластер, визуализация, трансформация, стационарная сигнальная точка, фиктивная сигнальная точка, эталонная сигнальная точка.

Ил.: 14. Библиогр.: 06 наим.

UDC 519:616-079.4:616.5

Control and visualization of functional security of information systems using wireless sensor networks / V.M. Chyzh, M.P. Karpinskiy, S.M. Balaban // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 356–362.

The importance and complexity of organizing effective methods of monitoring the status of the reliability of propagating information in wireless sensor networks are examined. Original methods of controlling signal parameters of individual or compactly disposed sensors and visualization methods of attacks on them are proposed. Authors substantiated using a cluster model with simplex coverage of its field to visualize areas of transformation of sensors whose signals were subjected to attacks.

Keywords: functional security, information systems, sensor, wireless sensor network, cluster visualization, transformation, fixed alarm point, dummy alarm point, reference signal point.

Fig.: 14. Ref.: 06 items.

УДК 681.3.06:519.248.681

УДОСКОНАЛЕННЯ ПРОТОКОЛУ НУЛЬОВИХ ЗНАНЬ, ЗАСНОВАНОГО НА ДИСКРЕТНИХ ЛОГАРИФМАХ

І.В. ОЛЕШКО

В роботі запропоновано удосконалену версію протоколу нульових знань, заснованого на дискретних логарифмах – протокол нульових знань з використанням еліптичної кривої. За допомогою методу аналізу ієрархій було проведено порівняльний аналіз двох протоколів: існуючого протоколу на дискретних логарифмах та його удосконаленої версії. Доведено, що кращим протоколом є протокол нульових знань з використанням еліптичної кривої.

Ключові слова: протокол нульових знань, дискретний логарифм, еліптична крива, механізм автентифікації, Пред'явник, сертифікат, метод аналізу ієрархій.

ВСТУП

До механізмів і протоколів нульових знань висуваються суворі вимоги в частині забезпечення їх безпечності з необхідним рівнем гарантій. Сьогодні знайшов застосування протокол нульових знань, що базується на перетвореннях в скінченому полі [1]. Захищеність такого протоколу від атаки "повне розкриття " носить субекспоненційний характер. У зв'язку з цим, відповідно до вимог FIPS 186-3 [2], для забезпечення навіть мінімального рівня захищеності від атаки "повне розкриття", необхідно встановити модуль перетворення не менше 2^{2048} . Таке збільшення модуля викликає зменшення швидкодії і необхідність збільшення потужності засобів обчислення.

Розв'язання цього протиріччя, на наш погляд, можна досягти на основі використання механізму, що розглянутий вище, у групі точок еліптичної кривої. Метою цієї статті є обґрунтування та удосконалення криптографічного протоколу нульових знань на основі його реалізації у групі точок еліптичної кривої. Вказана мета досягається на основі розв'язання таких задач:

1. Аналіз рівня безпечності протоколу нульових знань на дискретному логарифмі, що наведено в стандарті [1].

2. Визначення та вирішення основних етапів та задач з удосконалення протоколу на основі застосування замість дискретного логарифму перетворення у групі точок еліптичної кривої.

3. Обґрунтування та вибір критеріїв, виконання порівняльного аналізу та розробка рекомендацій із застосування удосконаленого протоколу нульових знань.

1. МЕХАНІЗМ, ЗАСНОВАНИЙ НА СЕРТИФІКАТАХ З ВИКОРИСТАННЯМ ДИСКРЕТНИХ ЛОГАРИФМІВ

З метою використання цього механізму групами об'єктів, мають бути виконані такі кроки [1]:

а) кожен об'єкт, який має намір діяти або як пред'явник або як перевіряючий, повинен мати засоби генерації випадкових чисел;

б) усі об'єкти, що входять до складу визначеної групи, мають узгодити три позитивних цілих числа p, q та g. Ціле число p має бути простим числом, q має бути обрано таким способом, щоб воно було простим числом та одночасно було множником $p-1$. А число g має бути обрано так, щоб воно було елементом порядку q за модулем p, таким, що задовольняє вимоги:

$$g^q \bmod p = 1, \quad (1)$$

$$g \neq 1. \quad (2)$$

Значення p та q мають бути такі, що для заданого довільного цілого числа $i(1 \le i \le q)$, знаходження цілого числа j (якщо таке існує) такого, що $g^j \bmod p = i$ має бути обчислювально неможливо;

в) усі об'єкти групи мають дійти до згоди щодо того, яка функція хешування використовуватиметься;

г) кожен об'єкт, який має намір діяти як пред'явник, має бути забезпечений асиметричною ключовою парою;

д) кожен об'єкт, який має намір діяти як перевіряючий, має бути забезпечений засобами обчислення довірених копій відкритих ключів перевірки для об'єктів, чия ідентичність перевіряється.

Кожен об'єкт, який має намір діяти як пред'явник у цьому механізмі, має бути забезпечений асиметричною ключовою парою (y_E, z_x), де z_X (особистий ключ) має бути цілим числом, таким, що задовольняє нерівності $0 \le z_X \le q$. Відповідне значення відкритого ключа перевірки y_X має дорівнювати $g^{z_x} \bmod p$.

Нижче наведено обміни, які необхідно здійснювати в ході виконання односпрямованого механізму автентифікації між Пред'явником А та Перевіряючим В, для того щоб В мав змогу впевнитися в тому, що об'єкт А є тим за кого він себе видає.

Механізм автентифікації наведено на рис. 1. Цифри у дужках позначають відповідні кроки обміну, які описано нижче.

Форма першого маркера ($TokenAB_1$), що надсилається пред'явником перевіряючому або

$TokenAB_1 = W$, або $TokenAB_1 = h(W \| Text)$. W — це доказ, h — функція гешування, а $Text$ це необов'язкове текстове поле. Якщо це текстове поле непусте, то об'єкт B повинен мати засоби для того, щоб отримати це значення; це може потребувати від об'єкта A надіслати все або частину текстового поля разом із маркером $TokenAB_1$.

Форма другого маркера ($TokenAB_2$), що надсилається пред'явником перевіряючому: $TokenAB_2 = D$, де D — це відповідь.

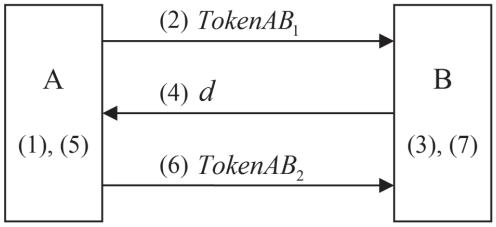


Рис. 1. Механізми, засновані на дискретних логарифмах

1) Об'єкт A обирає випадкове число r, з огляду на те, що r має бути цілим числом, яке задовольняє нерівності $1 \le r \le q$. Це число зберігається в таємниці об'єктом A. Об'єкт A обчислює доказ W:

$$W = g^r \bmod p. \quad (3)$$

2) Об'єкт A надсилає $TokenAB_1$ об'єкту B. Маркер $TokenAB_1$ має бути рівним або W або $h(W \| Text)$.

3) Отримавши маркер $TokenAB_1$, об'єкт B має випадковим чином обрати ціле число d (запит), значення якого має задовольняти нерівності $0 \le d \le q$.

4) Об'єкт B надсилає запит d об'єкту A.

5) Отримавши запит d, об'єкт A повинен обчислити відповідь D з (секретного) значення r та особистого ключа z_A об'єкта A за такою формулою:

$$D = r - dz_A \bmod q. \quad (4)$$

6) Об'єкт A надсилає маркер $TokenAB_2$ об'єкту B.

7) Отримавши відповідь D, об'єкт B має виконати такі розрахунки:

а) об'єкт B перевіряє, що $0 < D < q$. І якщо це не так, то об'єкт B бракує об'єкт A;

б) об'єкт B обчислює значення W' за такою формулою:

$$W' = (y_A)^d g^D \bmod p. \quad (5)$$

г) якщо W було надіслано при першому обміні процедури, то об'єкт B перевіряє, що обчислене значення $W' = W$. Якщо $h(W \| Text)$ було надіслано при першому обміні процедури, то об'єкт B перевіряє, що обчислене значення $h(W' \| Text) = h(W \| Text)$, яке надіслано при першому обміні процедури. Якщо перевірка завершилася успішно, вважається, що уся ця ітерація завершена успішно. В інших випадках об'єкт B бракує об'єкт A.

2. АНАЛІЗ ІСНУЮЧОГО ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ, ЗАСНОВАНОГО НА СЕРТИФІКАТАХ З ВИКОРИСТАННЯМ ДИСКРЕТНИХ ЛОГАРИФМІВ

Проведемо аналіз одного з протоколу нульових знань, заснованого на сертифікатах з використанням дискретних логарифмів. Складність криптографічного алгоритму залежить від довжини ключа, що використовується, а, отже, і від кількості різних, можливих ключів. Складність криптоаналізу алгоритму, заснованого на дискретних логарифмах, обчислюється за формулою [3]:

$$I_{дл} = e^{\delta(\ln p)^{\nu}(\ln\ln p)^{1-\nu}}. \quad (6)$$

Сучасні обчислювальні потужності, а також алгоритм криптоаналізу дозволяють використовувати в цій формулі такі значення для δ і ν: $\delta = 2.06$, $\nu = 1/3$.

Припустимо, що даний протокол заснований на перетвореннях у групі точок еліптичної кривої. Складність криптоаналізу для такого протоколу обчислюватиметься за такою формулою :

$$I_{ек} \approx \sqrt{-2n\ln(1 - P_к)}, \quad (7)$$

де n — порядок базової точки, $P_к$ — імовірність колізії.

У подальших розрахунках приймемо, що $P_к = 0.99$, тоді:

$$I_{ек0,99} \approx \sqrt{-2n\ln 10^{-2}} = \sqrt{4\ln 10 n} \approx 3.03\sqrt{n}. \quad (8)$$

Також проведемо розрахунок безпечного часу $t_б$. Безпечним часом називається кількість часу, необхідне для розкриття алгоритму із заздалегідь заданою ймовірністю успіху. $t_б$ розраховується за формулою [4]:

$$t_б = \frac{N_{кл}}{\gamma \cdot k} P_у, \quad (9)$$

де $N_{кл} = I$; к $\approx 3{,}1 * 10^7$ (с), кількість секунд у році; $P_у$ — імовірність успіху. У подальших розрахунках $P_у = 1$, тобто 100%; γ — кількість операцій в секунду, які виконуються системою криптоаналітика для заданого алгоритму. Для операцій, які виконуються в полях та кільцях $\gamma = 10^{12}$, а для операцій у групі точок еліптичної кривої — $\gamma = 10^{10}$.

Розрахуємо значення стійкості I та безпечного часу $t_б$, для алгоритмів, що базуються на перетвореннях у полях та кільцях та у групі точок еліптичної кривої (ЕК). Розрахуємо ці значення для таких довжин ключа: 2^{128}, 2^{256}, 2^{512}, 2^{1024}.

Таблиця 1

Порівняння I та t_1, в залежності від довжини ключа

Довжина ключа	2^{128}		2^{256}	
	I	$t_б$	I	$t_б$
Поля та кільця	$7.1*10^{10}$	$2.3*10^{-9}$	$1.4*10^{15}$	$0.45*10^{-4}$
Еліптична крива	$5.6*10^{19}$	$1.2*10^{2}$	$1.03*10^{39}$	$3.3*10^{21}$

Таблиця 2

Порівняння I та t_1, в залежності від довжини ключа

Довжина ключа	2^{512}		2^{1024}	
	I	$t_б$	I	$t_б$
Поля та кільця	$4.4*10^{20}$	14	$9.5*10^{27}$	$3.07*10^{8}$
Еліптична крива	$3.5*10^{77}$	$1.1*10^{60}$	$4.06*10^{154}$	$1.3*10^{137}$

При порівнянні цих двох алгоритмів, спостерігається збільшення часу необхідного для розкриття ключа при збереженні його довжини для алгоритму, що базується на перетвореннях у групі точок еліптичної кривої, або з іншого боку, $t_б$ залишається колишнім, а довжина ключа значно зменшується. Тому пропозицією з удосконалення протоколу автентифікації, заснованого на сертифікатах з використанням дискретних логарифмів, буде переклад його на ЕК.

3. УДОСКОНАЛЕННЯ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ НА ДИСКРЕТНИХ ЛОГАРИФМАХ

Для переводу даного протоколу на еліптичні криві за основу був взятий алгоритм електронного цифрового підпису EC-GDSA, описаний в [5]. В результаті, у протоколі нульових знань, заснованому на дискретних логарифмах, описаному вище, необхідно зробити такі зміни:

- замінити випадкове число *r*, яке задовольняє нерівності $1 \le r \le q$ на випадкове ціле число k в інтервалі $\{1,...,n-1\}$;
- замінити доказ W на r, яке обчислюється за формулою $r = \pi(k \cdot G) \bmod n$, де G — це порядок базової точки;
- замінити ціле число d (запит), значення якого має задовольняти нерівності $0 \le d \le q$ на e, яке в свою чергу має задовольняти нерівності $1 \le e \le n$;
- замість асиметричної ключової пари (y_X, z_X), де z_X — таємний ключ, необхідно використовувати іншу ключову пару d_A, Q_A, де d_A — це секретний ключ, а відкритий ключ генерується за формулою $Q_A = d_A^{-1} \cdot G$.

Далі для наочності наведена таблиця порівняння, у першій колонці кроки алгоритму без змін, як у стандарті [1], а в другій — кроки алгоритму після переведення його на еліптичну криву.

Для перевірки нового алгоритму автентифікації нульових знань була розроблена програмна реалізація. Як криптографічна бібліотека була використана бібліотека Crypto + + ® Library 5.2.1. Параметри полів і еліптичної кривої для нового алгоритму були такі:

$$f(x) = x^{191} + x^9 + 1$$

$$y^2 + xy = x^3 + ax^2 + b$$

n: 4000000000000000000000004A20E90C39067C893BBB9A5h

a: 2866537B676752636A68F56554E12640276B649EF7526267h

b: 2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185ECh

G(x, y) = (36B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0Dh, 65BE73433B3F95E332932E70EA245CA2418EA0EF98018FBh)

Таблиця 3

Порівняння алгоритмів автентифікації

Протокол з використанням дискретних логарифмів	Протокол з використанням еліптичної кривої
1) Пред'явник генерує випадкове ціле число r, яке задовольняє нерівності $1 \le r \le q$. Дане число зберігається в таємниці. Пред'явник обчислює W: $W = g^r \bmod p$;	1)) Пред'явник генерує випадкове ціле число k, яке знаходиться в інтервалі $\{1,...,n-1\}$. Дане число зберігається в таємниці. Пред'явник обчислює r: $r = \pi(k \cdot G)$;
2) Пред'явник відсилає Перевіряючому маркер $TokenAB_1 = W$;	2) Пред'явник відсилає Перевіряючому $r = \pi(k \cdot G)$;
3) Перевіряючий генерує число d, $0 \le d \le q$;	3) Перевіряючий генерує число e, значення якого повинно задовольняти нерівності $1 \le e \le n$;
4) Перевіряючий відправляє число d Пред'явнику;	4) Перевіряючий відправляє число e Пред'явнику;
5) Пред'явник повинен обчислити відповідь D на основі r та власного ключа z_A за формулою: $D = r - dz_A \bmod q$;	5) Пред'явник повинен обчислити відповідь S на основі k та власного ключа d_A за формулою: $S = (kr - e)d_A \bmod n$;
6) Пред'явник відправляє маркер $TokenAB_2 = D$ Перевіряючому;	6) Пред'явник відправляє S Перевіряючому;
7) Перевіряючий перевіряє, чи належить D до інтервалу $0 < D < q$, обчислює значення W' за формулою: $W' = (y_A)^d g^D \bmod p$ та перевіряє W=W'. Якщо перевірка закінчилась успішно, то вважається, що вся ітерація завершилась успішно. В іншому випадку Перевіряючий ігнорує Пред'явника.	7) Отримавши відповідь S, Перевіряючий обчислює значення r' за формулою: $r' = \pi((SQ_A + eG)r^{-1})$; та перевіряє $r = r'$. Якщо перевірка закінчилась успішно, то вважається, що вся ітерація завершилась успішно. В іншому випадку Перевіряючий ігнорує Пред'явника.

4. СУТНІСТЬ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

У методі аналізу ієрархій елементи завдання порівнюються попарно відносно їхнього впливу («ваги», або «інтенсивності») на загальну для них характеристику [6]. Парні порівняння елементів призводять до матричної форми таблиці.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Рис. 2. Порівняння елементів методом аналізу ієрархій

Ця матриця має властивість зворотної симетричності, тобто $a_{ji} = 1/a_{ij}$. Вона складається для порівняння відносної важливості критеріїв на другому рівні стосовно загальної мети на першому рівні, на третьому рівні стосовно критеріїв другого рівня і т. д. [7].

Заповнення квадратних матриць парних порівнянь виконується за таким правилом. Якщо елемент E_1 переважає над елементом E_2, то клітинка матриці, що відповідає перетинанню елементу E_1 (рядка) й елементу E_2 (стовпця), заповнюється цілим числом (від 1 до 9), а клітинка, що відповідає перетинанню рядка E_2 й стовпця E_1, заповнюється зворотним йому числом. Якщо елемент E_2 переважає над E_1, то ціле число ставиться в клітинку, що відповідає рядку E_2 й стовпцю E_1, а дріб ставиться в клітинку, що відповідає рядку E_1 й стовпцю E_2. Якщо елементи E_1 й E_2 мають однакову вагу, то в обох позиціях матриці ставляться одиниці.

Наведемо приклад формування матриці парних порівнянь. Нехай $E_1, E_2, ..., E_n$ – множина із n елементів , а $\nu_1, \nu_2, ... \nu_n$ – відповідно їхні ваги, або інтенсивності. Порівняємо попарно ваги, або інтенсивності всіх елементів множини щодо загальної для них властивості або мети. У цьому випадку матриця парних порівнянь $[E]$ матиме вигляд, як наведено на рисунку 3.

$[E] =$

	E_1	E_2	...	E_n
E_1	ν_1 / ν_1	ν_1 / ν_2	...	ν_1 / ν_n
E_2	ν_2 / ν_1	ν_2 / ν_2	...	ν_2 / ν_n
...	...	...	...	...
E_n	ν_n / ν_1	ν_n / ν_2	...	ν_n / ν_n

Рис. 3. Матриця парних порівнянь

При здійсненні попарних порівнянь необхідно відповісти на одне з питань: який із двох елементів, що порівнюються, важливіший, який більше ймовірний та який кращий. Отримані судження виражаються в цілих числах з урахуванням дев'ятибальної шкали (табл. 4) [7].

В ході використання зазначеної шкали, порівнюючи два об'єкти після досягнення мети, розташованої на вищестоящому рівні ієрархії, необхідно поставити у відповідність цьому порівнянню число 1, 3, 5, 7, 9 або зворотне йому значення. Числа 2, 4, 6, 8 і їх зворотні величини використовуються для полегшення компромісів між дещо відмінними від основних чисел судженнями. У тих випадках, коли складно розрізнити скільки проміжних градацій від абсолютного до слабкої переваги або цього не потрібно в конкретному завданні, може використовуватися шкала з меншим числом градацій. Найменше така шкала може мати дві оцінки: 1 — об'єкти рівнозначні; 2 — перевага одного об'єкта над іншим.

Таблиця 4

Шкала відносин (ступені значущості елементів)

Ступінь значущості	Визначення	Пояснення
1	Однакова значущість	Дві дії вносять однаковий вклад у досягнення мети
3	Деяка перевага значущості однієї дії над іншою (слабка значущість)	Існують аргументи на користь переваги однієї з дій, але ці аргументи недостатньо переконливі
5	Істотна або сильна значущість	Існують надійні дані або логічні судження для того, щоб показати перевагу однієї з дій
7	Очевидна або дуже сильна значущість	Переконливе свідчення на користь однієї дії над іншою
9	Абсолютна значущість	Свідчення на користь переваги однієї дії над іншою переконливі в максимальному ступені
2,4,6,8	Проміжні значення між двома сусідніми судженнями	Ситуація, коли необхідне компромісне рішення
Зворотні величини наведених вище величин	Якщо дії *i* при порівнянні з дією *j* приписується одне з вказаних вище ненульових чисел, то дії *j* при порівнянні з дією *i* приписується зворотне значення	Якщо узгодженість була визначена при одержанні N числових значень для створення матриці

Із групи матриць попарних порівнянь ми формуємо набір локальних пріоритетів, які виражають відносний вплив множини елементів нижнього рівня на елемент рівня, що примикає зверху. Для цього необхідно обчислити множину власних векторів для кожної матриці, які після нормалізації стають векторами пріоритетів. Найбільш точним способом для обчислення власного вектора є метод обчислення геометричного середнього шляхом перемножування всіх елементів у кожному рядку з наступним добуванням кореня n-го ступеня, де n — кількість елементів у рядку.

$$q_j^{(r-1)} = \sqrt[n]{(v_j^{(r)} / v_1^{(r)}) \times (v_j^{(r)} / v_2^{(r)}) \times \cdots \times (v_j^{(r)} / v_n^{(r)})}\ , \quad (10)$$

де r — рівень ієрархії, для матриці якого виконується розрахунок, n — кількість елементів у рядку, j — порядковий номер рядка.

Отриманий у такий спосіб стовпець нормалізується діленням кожного числа на суму всіх чисел.

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}}\ . \quad (11)$$

Матриця попарних порівнянь може бути узгодженою і не узгодженою. У загальному випадку, під узгодженістю мається на увазі те, що за наявності основного масиву необроблених даних всі інші дані логічно можуть бути отримані з основного масиву. Для проведення парних порівнянь n об'єктів або дій, які представлені в даних хоча б один раз, потрібно n-1 суджень про парні порівняння. З них можна вивести всі інші судження, використовуючи таке відношення: якщо об'єкт A_1 в 3 рази перевершує об'єкт A_2 і в 6 разів перевершує A_3, то $A_1 = 3A_2$ і $A_1 = 6A_3$. Отже, $3A_2 = 6A_3$, або $A_2 = 2A_3$ і $A_3 = 1/2A_2$. Якщо чисельне значення судження в позиції (2, 3) відрізняється від 2, то матриця буде неузгодженою. Це трапляється часто і не є проблемою.

Відомо, що узгодженість матриці еквівалентна вимозі рівності її максимального власного значення $\lambda_{max} = n$. Можна також оцінити відхилення від узгодженості за формулою $(\lambda_{max} - n) / (n - 1)$. Ця величина називається індексом узгодженості (ІУ). Зауважимо, що нерівність $\lambda_{max} \geq n$ завжди правильна. Наскільки погана узгодженість для певного завдання, можна оцінити шляхом порівняння отриманого нами значення ІУ з її значенням з випадково вибраних суджень і відповідних зворотних величин матриці того ж розміру. Ця величина має назву випадковий індекс (ВІ) [7]. У Національній лабораторії Окриджа згенерували середні ВІ для матриць порядку від 1 до 15 на базі 100 випадкових вибірок. Їх значення наведено в таблиці.

Таблиця 5

Значення ВІ для різних порядків матриці

Розмір матриці	1	2	3	4	5	6	7
ВІ	0	0	0,58	0,9	1,12	1,24	1,32

Продовження таблиці 5

8	9	10	11	12	13	14	15
1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Відношення ІУ до ВІ для матриці того самого порядку називається відношенням узгодженості (ВУ). Значення ВУ, менше, ніж 0,1 вважатимемо прийнятним. Для знаходження λ_{max} необхідно виконати такі кроки:

- Помножити матрицю порівнянь на оцінку вектора рішення. Отримаємо новий вектор.
- Розділити перший компонент цього вектора на першу компоненту оцінки вектора рішення, другу компоненту нового вектора на другу компоненту оцінки вектора рішення і т. д. Визначимо ще один вектор.
- Розділити суму компонент останнього вектора на число компонент. Таким чином знайдемо наближення до числа λ_{max}.

Обчислення значень ІУ та ВУ виконується за формулами, наведеними вище.

5. ПОРІВНЯННЯ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЙ

Протоколи автентифікації оцінюватимемо за такими критеріями [8]:

1. Автентифікація суб'єкта;
2. Автентифікація ключа;
3. Вид автентифікації суб'єкта;
4. Вид автентифікації ключа;
5. Наявність підтвердження ключа;
6. Новизна ключів;
7. Керування ключовими даними;
8. Захист від атак типу «повтор раніше переданого»;
9. Число обмінів повідомленнями;
10. Складність обчислень;
11. Можливість використання попередніх обчислень;
12. Вимоги до третьої сторони;
13. Криптографічна стійкість ключа;
14. Складність реалізації атак «повне розкриття»;
15. Вид неспростовності.

Порівняємо протоколи автентифікації за вище наведеними критеріями (табл. 6).

Таблиця 6

Порівняння протоколів автентифікації

	Протоколи / Критерії	Протокол, заснований на сертифікатах з використанням дискретних логарифмів	Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК
1	Автентифікація суб'єкта	Суб'єкт А для суб'єкта В	Суб'єкт А для суб'єкта В
2	Автентифікація ключа	Явна від А до В	Явна від А до В
3	Вид автентифікації суб'єкта	Однобічна абонента А до В	Однобічна абонента А до В
4	Вид автентифікації ключа	Однобічна автентифікація ключа абонента А	Однобічна автентифікація ключа абонента А
5	Наявність підтвердження ключа	Підтвердження ключа абонента А, Z_A	Підтвердження ключа абонента А, d_A
6	Новизна ключів	Немає новизни ключів	Немає новизни ключів

Продовження таблиці 6

7	Керування ключовими даними	На розсуд сторін протоколу	На розсуд сторін протоколу
8	Захист від атак типу «повтор раніше переданого повідомлення»	Здійснюється за рахунок випадкового числа r й випадкового цілого числа d	Здійснюється за рахунок випадкового числа r й випадкового цілого числа d
9	Число обмінів повідомленнями	3	3
10	Складність обчислень	1 операція секретного перетворення, 1 операція відкритого перетворення	1 операція секретного перетворення, 1 операція відкритого перетворення
11	Можливість використання попередніх обчислень	Немає	Немає
12	Вимоги до 3-ї сторони	Сторони протоколу самі вирішують, хто виготовляє пару ключів і якщо це третя сторона, то вона генерує відкритий та секретний ключ	Сторони протоколу самі вирішують, хто виготовляє пару ключів і якщо це третя сторона, то вона генерує відкритий та секретний ключ
13	Криптостійкість ключа	Забезпечується криптостійкість Y_A за відсутності компрометації секретної інформації акредитації Z_A	Забезпечується криптостійкість Y_A за відсутності компрометації секретної інформації акредитації d_A
14	Складність реалізації атак «повне розкриття»	Субекспоненційна	Експоненційна
15	Неспростовність	Неспростовність об'єкта А здійснюється за рахунок Z_A	Неспростовність об'єкта А здійснюється за рахунок d_A

Для того, щоб обрати кращий протокол автентифікації, зробимо процедуру декомпозиції та побудуємо дерево цілей. Для цього розіб'ємо 15 критеріїв, що характеризують протокол на 3 підгрупи:

1. Критерії, які стосуються ключа:
   - автентифікація ключа;
   - вид автентифікації ключа;
   - підтвердження ключа;
   - новизна ключа;
   - керування ключовими даними;
   - криптостійкість ключа.
2. Загальні вимоги:
   - автентифікація суб'єкта;
   - вид автентифікації суб'єкта;
   - число обмінів повідомленнями;
   - складність обчислень;
   - можливість використання попередніх обчислень;
   - вимоги до 3-ї сторони.
3. Показник захищеності:
   - захист від атак типу «повтор раніше переданого повідомлення»;
   - складність реалізації атак «повне розкриття»;
   - неспростовність.

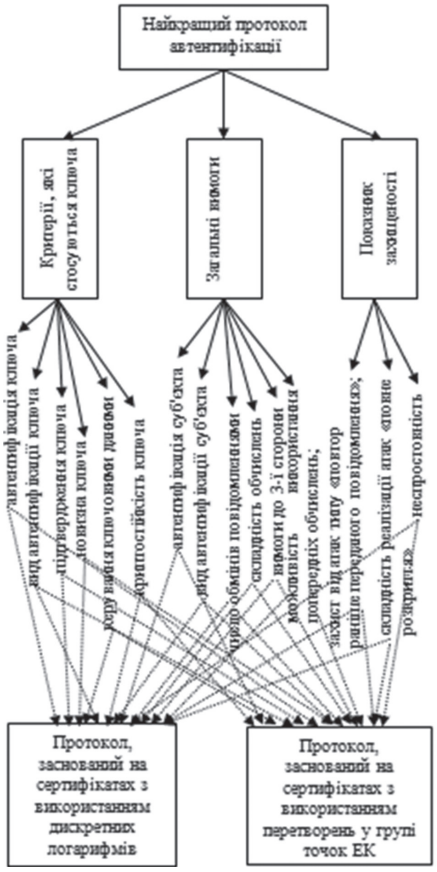


Рис. 4. Схема методу аналізу ієрархій

Далі наводяться матриці попарних порівнянь для кожного рівня ієрархії.

Таблиця 7

Матриця попарних порівнянь 1-го рівня

Вибір кращого протоколу	Критерії, які стосуються ключа	Загальні вимоги	Показник захищеності	q	γ
Критерії, які стосуються ключа	1	1/3	1/7	0,362	0.081
Загальні вимоги	3	1	1/5	0.843	0.188
Показник захищеності	7	5	1	3.271	0.731

$\lambda_{max} = 3.066$ ІУ=0,033 ВУ= 0,057

Таблиця 8

Матриця попарних порівнянь
2-го рівня, 1-ї групи критеріїв

Критерії, які стосуються ключа	Автентифікація ключа	Вид автентифікації ключа	Підтвердження ключа	Новизна ключа	Керування ключовими даними	Крипостійкість ключа	q	γ
Автентифікація ключа	1	1	1/3	1/3	1/4	1/9	0.382	0.040
Вид автентифкації ключа	1	1	1/3	1/3	1/4	1/9	0.382	0.040
Підтвердження ключа	3	3	1	1/2	1/3	1/8	0.757	0.078
Новизна ключа	3	3	2	1	3	1/5	1.487	0.154
Керування ключовими даними	4	4	3	1/3	1	1/9	1.101	0.114
Крипостійкість ключа	9	9	8	5	9	1	5.548	0.575

λ_{max} =6,5 ІУ= 0,1 ВУ= 0,08

Таблиця 9

Матриця попарних порівнянь
2-го рівня, 2-ї групи критеріїв

Загальні вимоги	Автентифікація суб'єкта	Вид автентифікації суб'єкта	Число обмінів повідомленнями	Складність обчислень	Вимоги до 3-ї сторони	Використання попередніх	q	γ
Автентифікація суб'єкта	1	2	1/2	1/4	4	1/5	0,765	0,085
Вид автентифікації суб'єкта	1/2	1	1/3	1/6	4	1/7	0,501	0,056
Число обмінів повідомленнями	2	3	1	1/5	3	1/6	0,918	0,102
Складність обчислень	4	6	5	1	6	1/3	2,493	0,277
Вимоги до 3-ї сторони	1/4	1/4	1/3	1/6	1	1/7	0,281	0,031
Використання попередніх обчислень	5	7	6	3	7	1	4,049	0,449

λ_{max} =6.537 ІУ=0.107 ВУ= 0.087

Таблиця 10

Матриця попарних порівнянь 2-го рівня,
3-ї групи критеріїв

Показник захищеності	Захист від атак типу повтор раніше	Складність реалізації атак «повне розкриття»	Неспростовність	q	γ
Захист від атак типу «повтор раніше переданого повідомлення»	1	1/4	2	0,794	0,219
Складність реалізації атак «повне розкриття»	4	1	3	2,289	0,63
Неспростовність	1/2	1/3	1	0,55	0,151

λ_{max} =3.109 ІУ= 0.055 ВУ= 0.094

Таблиця 11

Матриця попарних порівнянь
3-го рівня, 1-ї групи критеріїв

Автентифікація ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 12

Матриця попарних порівнянь
3-го рівня, 2-ї групи критеріїв

Вид автентифікації ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 13

Матриця попарних порівнянь
3-го рівня, 3-ї групи критеріїв

Підтвердження ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 14

Матриця попарних порівнянь
3-го рівня, 4-ї групи критеріїв

Новизна ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 15

Матриця попарних порівнянь
3-го рівня, 5-ї групи критеріїв

Керування ключовими даними	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 16

Матриця попарних порівнянь
3-го рівня, 6-ї групи критеріїв

Криптостійкість ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1/4	0,5	0,2
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	4	1	2	0,8

Таблиця 17

Матриця попарних порівнянь
3-го рівня, 7-ї групи критеріїв

Автентифікація суб'єкта	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 18

Матриця попарних порівнянь
3-го рівня, 8-ї групи критеріїв

Вид автентифікації суб'єкта	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 19

Матриця попарних порівнянь
3-го рівня, 9-ї групи критеріїв

Число обмінів повідомленнями	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 20

Матриця попарних порівнянь
3-го рівня, 10-ї групи критеріїв

Складність обчислень	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1/5	0,447	0,167
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	5	1	2,236	0,833

Таблиця 21

Матриця попарних порівнянь
3-го рівня, 11-ї групи критеріїв

Вимоги до 3-ї сторони	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 22

Матриця попарних порівнянь
3-го рівня, 12-ї групи критеріїв

Можливість використання попередніх обчислень	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 23

Матриця попарних порівнянь
3-го рівня, 13-ї групи критеріїв

Захист від атак типу «повтор раніше переданого повідомлення»	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 24

Матриця попарних порівнянь
3-го рівня, 14-ї групи критеріїв

складність реалізації атак «повне розкриття»	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1/7	0,378	0,125
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	7	1	2,646	0,875

Таблиця 25

Матриця попарних порівнянь
3-го рівня, 15-ї групи критеріїв

Неспростовність	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Розглянемо матриці впливу різних рівнів.

Внесок підцілей першого рівня в основну мету:

$$Y^{1,0}{}_1 = \begin{pmatrix} 0{,}081 \\ 0{,}188 \\ 0{,}731 \end{pmatrix}.$$

Внесок підцілей другого рівня в підцілі першого рівня виглядає так:

$$Y^{2,1}{}_1 = \begin{pmatrix} 0{,}04 \\ 0{,}04 \\ 0{,}078 \\ 0{,}154 \\ 0{,}114 \\ 0{,}575 \end{pmatrix};\ Y^{2,1}{}_2 = \begin{pmatrix} 0{,}085 \\ 0{,}056 \\ 0{,}102 \\ 0{,}277 \\ 0{,}031 \\ 0{,}449 \end{pmatrix};\ Y^{2,1}{}_3 = \begin{pmatrix} 0{,}219 \\ 0{,}63 \\ 0{,}151 \end{pmatrix}.$$

Внесок підцілей третього рівня в підцілі другого рівня виглядає так:

$$Y^{3,2}_{1-6} = \begin{pmatrix} 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}2 \\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}8 \end{pmatrix}$$

$$Y^{3,2}_{7-12} = \begin{pmatrix} 0{,}5\ 0{,}5\ 0{,}5\ 0{,}167\ 0{,}5\ 0{,}5 \\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}833\ 0{,}5\ 0{,}5 \end{pmatrix}$$

$$Y^{3,2}_{13-15} = \begin{pmatrix} 0{,}5\ \ 0{,}125\ 0{,}5 \\ 0{,}5\ 0{,}875\ 0{,}5 \end{pmatrix}$$

$$Y^{3,1}_1 = Y^{2,1}_1 * Y^{3,2}_{1-6} =$$

$$= \begin{pmatrix} 0{,}328 \\ 0{,}673 \end{pmatrix}\ Y^{3,1}_2 = Y^{2,1}_2 * Y^{3,2}_{7-12} = \begin{pmatrix} 0{,}408 \\ 0{,}592 \end{pmatrix}$$

$$Y^{3,1}_3 = Y^{2,1}_3 * Y^{3,2}_{13-15} = \begin{pmatrix} 0{,}264 \\ 0{,}736 \end{pmatrix}$$

Результуючий вектор значущості розраховується так:

$$Y^{3,0}_1 = Y^{1,0}_1 * Y^{1,1}_{1-3} = \begin{pmatrix} 0{,}081 \\ 0{,}188 \\ 0{,}731 \end{pmatrix} * \begin{pmatrix} 0{,}328\ 0{,}408\ 0{,}264 \\ 0{,}673\ 0{,}592\ 0{,}736 \end{pmatrix} =$$

$$= \begin{pmatrix} 0{,}296 \\ 0{,}704 \end{pmatrix}.$$

Виходячи із отриманих нами даних, можна зробити висновок про те, що найкращим протоколом автентифікації (із порівнюваних) є протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК.

ВИСНОВКИ

Забезпечення безпеки інформаційної системи є одним з найважливіших завдань в ході її експлуатації, оскільки від збереження конфіденційності, цілісності і доступності інформаційних ресурсів багато в чому залежить швидкість прийняття рішень, ефективність і надійність роботи. Зараз для будь-якої компанії, чи особи, яким необхідно захищати дані, як ніколи важлива безпека та перевірка автентичності. На сьогодні існує багато протоколів автентифікації. Важливим є завдання пошуку найкращого протоколу. Однією із вразливостей протоколу простої автентифікації є те, що після того, як Пред'явник передасть свій пароль Перевіряючому, останній може використовувати його та видавати себе за Пред'явника. Протоколи суворої автентифікації мають кращу стійкість, проте їх вразливість полягає в тому, що Пред'явник зобов'язаний продемонструвати знання секретного ключа, хай навіть і одноразово; при цьому передана інформація не може бути безпосередньо використана Перевіряючим, проте деяка її частина допоможе отримати додаткову інформацію про секрет Пред'явника. Наприклад, Перевіряючий має можливість так сформувати запити, щоб відповіді, які передавались, аналізувалися на предмет вмісту додаткової інформації.

Протоколи з нульовими знаннями були розроблені спеціально для вирішення даної

проблеми. Вони дозволяють встановити істинність твердження і при цьому не передавати будь-якої додаткової інформації про саме твердження.

В роботі запропоновано удосконалений протокол нульових знань, заснований на сертифікатах з використанням перетворень у групі точок ЕК. Проведено порівняльний аналіз методом аналізу ієрархій удосконаленого протоколу із протоколом, заснованим на сертифікатах з використанням дискретних логарифмів. Після проведення порівняльного аналізу і отримання результуючого вектора значущості, доведено, що удосконалений протокол має кращі властивості безпеки.

Література

[1] ISO/IEC 9798-5. Методи захисту. Автентифікація об'єктів. Частина 5: Протоколи, що використовують методи які грунтуються на нульових знаннях.

[2] FIPS PUB 186-3. Digital Signature Standard. – USA, 2009. – 130 p.

[3] Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах / І.Д. Горбенко, Т.О. Гріненко // Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004. – 368 с.

[4] Балагура Д.С. Методы оценки сложности криптоанализа для криптографических приложений в группе точек эллиптической кривой, учитывающие вероятность коллизий / Д.С. Балагура, Ю.И. Горбенко // Радиотехника: Всеукр. межвед. научн.-техн. сб. — 2005. Вып. 142. — С. 205–213.

[5] ISO/IEC 15946-2. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 2: Електронні цифрові підписи.

[6] Андрейчиков А.В. Анализ, синтез, планирование решений в экономике / А.В Андрейчиков, О.Н Андрейчикова // М.: Финансы и статистика, 2002. – 386 с.

[7] Саати Т. Принятие решений. Метод анализа иерархий: пер. с англ. М.: Радио и связь, 1989. – 316 с.

[8] ISO/IEC 9798-1. Information technology – Security techniques – Entity authentication – Part1: General.

Надійшла до редколегії 15.05.2013

Олешко Інна Вікторівна, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: електронна паспортна система, біометрична автентифікація.

УДК 681.3.06:519.248.681

Усовершенствование протокола нулевых знаний, основанного на дискретных логарифмах / И.В. Олешко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 363–372.

В работе предложена усовершенствованная версия протокола нулевых знаний, основанного на дискретных логарифмах — протокол нулевых знаний с использованием эллиптической кривой. С помощью метода анализа иерархий был проведен сравнительный анализ двух протоколов: существующего протокола на дискретных логарифмах и его усовершенствованной версии. Доказано, что лучшим протоколом является протокол нулевых знаний с использованием эллиптической кривой.

Ключевые слова: протокол нулевых знаний, дискретный логарифм, эллиптическая кривая, механизм аутентификации, Инициатор, сертификат, метод анализа иерархий.

Табл.: 25. Ил.: 4. Библиогр.: 8 назв.

UDC 681.3.06:519.248.681

Improving of zero-knowledge protocol based on discrete logarithms / I.V. Oleshko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 363–372.

The paper presents an improved version of an zero-knowledge protocol based on discrete logarithms — a zero-knowledge protocol using an elliptic curve. A comparative analysis of two protocols has been performed with the help of hierarchy analysis method: the discrete logarithms-based existing algorithm and its improved version. It is proved that the best protocol is the zero knowledge protocol using an elliptic curve.

Keywords: zero-knowledge protocol, discrete logarithm, elliptic curve, authentication mechanism, claimant, certificate, hierarchy analytic method.

Tab.: 25. Fig.: 4. Ref.: 8 items.

ПРИКЛАДНАЯ РАДИОЭЛЕКТРОНИКА

Научно-технический журнал

Ответственный секретарь

Е. Б. Исаева

Корректор

Б. П. Косиковская

Перевод на английский язык

К. Т. Умяров

Компьютерный дизайн и верстка

Е. Б. Исаева

Рекомендовано засіданням Бюро Президії Академії наук прикладної радіоелектроніки
(протокол № 2 від 26.06.2013 р.).

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки
(протокол № 23 від 05.07.2013 р.).

Свідоцтво про державну реєстрацію КВ № 6037 від 09.04.2002 р.

Журнал включений у список фахових видань ВАК України
з технічних наук
(постанова президії ВАК України № 1-05/2 от 10.03.2010),
з фізико-математичних наук (фізика)
(постанова президії ВАК України № 1-05/5 от 1.07.2010)

Підписано до друку 05.07.2013. Формат 60 × 84 $^1/_8$.
Папір офсет. Друк офсет. Умов.-друк. арк. 22,3. Облік.-вид. арк. 21,6.
Тираж 300 прим. Ціна договірна.

Віддруковано в ТОВ «ДРУКАРНЯ МАДРИД»
61024, м. Харків, вул. Ольмінського, 8. Тел.: (057) 717-41-79
www.madrid.in.ua, e-mail: info@madrid.in.ua