МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАКУТОНІНА ЛІДІЯ ВІКТОРІВНА

УДК 004.056.55

МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ З ДОКАЗОВОЮ СТІЙКІСТЮ, ЩО ЗАСНОВАНІ НА ІДЕНТИФІКАТОРАХ ТА АЛГЕБРАЇЧНИХ РЕШІТКАХ

05.13.21 – системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2015

Дисертацією є рукопис

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України, м. Харків.

Науковий керівник: доктор технічних наук, професор
Горбенко Іван Дмитрович,
професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Міністерство освіти і науки України, м. Харків

Офіційні опоненти: доктор технічних наук, професор
Толюпа Сергій Васильович,
директор інституту захисту інформації, Міністерство освіти і науки України, м. Київ;

кандидат технічних наук, доцент
Неласа Ганна Вікторівна,
доцента кафедри програмних засобів Запорізького національного технічного університету, Міністерство освіти і науки України, м. Запоріжжя.

Захист відбудеться « 24 » березня 2015 р. о 13^{00} годині на засіданні спеціалізованої вченої ради К64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розіслано « 20 » лютого 2015 р.

Вчений секретар
спеціалізованої вченої ради І.В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В сучасному світі інформаційних технологій захист інформації, що передається цифровими каналами зв’язку, відіграє ключову роль як на державному рівні, так і для пересічної людини. Майже в усіх галузях суспільного життя управління інформацією здійснюється саме в цифровому вигляді. Всі адміністративні суб’єкти по всьому світу здійснюють взаємодію завдяки електронному документообігу, задіяні такі соціально-громадські сфери, як урядові, політичні, науково-технічні, промислові, економічні тощо. На сьогодні майже всі державні і комерційні структури взаємодіють завдяки глобальній мережі електронного зв’язку. Тому, для забезпечення конфіденційності, цілісності, справжності, неспростовності інформації, що передається, застосовуються, асиметричні та симетричні криптосистеми.

Для вирішення задач забезпечення цілісності, неспростовності та справжності, а також реалізації моделі взаємної недовіри, застосовуються асиметричні криптографічні перетворення в кільцях, скінчених полях та групах точок еліптичних кривих. Перспективними напрямками розвитку асиметричних криптографічних систем є напрямки, які пов’язані з перетвореннями на ідентифікаторах, кільцями зрізаних поліномів тощо. Застосування перетворень в кільцях та скінченних полях показало, що дані криптографічні перетворення вже не задовольняють за критеріями стійкості та швидкодії. Незважаючи на виконання вимог відносно стійкості, швидкодія криптоперетворень на еліптичних кривих залишається низькою. Вже майже сорок років потужно розвиваються криптосистеми, що базуються на ідентифікаторах, які мають ряд переваг над класичними асиметричними системами та можуть психологічно сприйматися користувачами. Але, на жаль дані криптосистеми використовують перетворення білінійних відображень, які є достатньо складними, а значить і швидкодія є низькою, водночас методи доведення стійкості даних криптоперетворень є розмитими і дозволяють отримати оцінки тільки в інтервалі від субекспоненційної до експоненційної. Останнім часом суттєві надії покладені на вирішення проблем стійкості та швидкодії на основі застосування криптографічних перетворень у фактор-кільцях, які ще називають перетвореннями в кільцях зрізаних поліномів. Як показали дослідження, застосування криптоперетворень у фактор-кільцях задовольняють за критерієм підвищення швидкодії, в порівнянні з класичними криптосистемами направленого шифрування на два–три порядки.

Тому є актуальною тема даної дисертації, яка направлена на вирішення науково-прикладної задачі удосконалення та розробку нових методів і програмних моделей криптографічних перетворень, що засновані на ідентифікаторах та алгебраїчних решітках, для підвищення швидкодії криптоперетворень та забезпечення необхідного рівня криптографічної стійкості.

Зв'язок роботи з науковими програмами, темами. Дослідження, результати яких знайшли відображення в дисертаційній роботі, виконувались

здобувачем у межах науково-дослідних робіт (НДР): держбюджетної НДР № 262-1 «Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП, на національному та міжнародному рівнях», яка затверджена наказом МОНУ № 1177 від 30.11.2010 р. (ДР № 0111U002628); госпдоговірної НДР № 11-06 «Розробка методів, комплексів та засобів інфраструктури відкритих ключів (ІВК) для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій» (ДР №.0111U002634), держбюджетної НДР № 275-1 «Аналіз стану, визначення напрямів розвитку, стандартизація, удосконалення, розробка та впровадження криптографічних систем, включаючи систему ЕЦП» (ДР № 0113U000363). В даних роботах автор брав участь як виконавець.

Мета і задачі дослідження. *Метою роботи* є оцінка існуючих, удосконалення та розробка нових методів і програмних моделей криптографічних перетворень, які засновані на ідентифікаторах та алгебраїчних решітках для підвищення швидкодії криптоперетворень та забезпечення необхідного рівня криптографічної стійкості.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– визначити та обґрунтувати систему умовних і безумовних критеріїв та показників оцінки систем направленого шифрування на ідентифікаторах та алгебраїчних решітках;

– провести аналіз стійкості асиметричних методів криптоперетворень на ідентифікаторах та алгебраїчних решітках з використанням вибраних критеріїв і показників;

– визначити, за результатами проведеного аналізу, та обґрунтувати алгоритм направленого шифрування (НШ) на ідентифікаторах, що є більш прийнятним для інтегрування в існуючу систему електронно-цифрового підпису (ЕЦП);

– удосконалити обраний метод направленого шифрування за критеріями криптографічної стійкості та складності основних етапів перетворювань;

– розробити методи НШ на ідентифікаторах та алгебраїчних решітках з метою досягнення підвищення швидкодії;

– розробити програмні моделі НШ на ідентифікаторах та алгебраїчних решітках та провести теоретичні та практичні узагальнення результатів дослідження.

Об'єкт досліджень – процеси направленого шифрування на ідентифікаторах та алгебраїчних решітках із заданим рівнем захищеності та покращеною швидкодією.

Предмет досліджень – методи та засоби здійснення та застосування криптографічних перетворень на ідентифікаторах на алгебраїчних решітках.

Методи дослідження ґрунтуються на теорії кілець, груп і полів під час побудови; абстрактної алгебри в ході дослідження та застосування алгебраїчних решіток і під час розроблення математичної моделі методу направленого шифрування на ідентифікаторах та алгебраїчних решітках; теорії складності обчислень при оцінці швидкодії виконання операцій під час вироблення алгоритмів направленого зашифрування та розшифрування; теорії

ймовірностей та математичної статистики при визначенні ймовірності виникнення колізій окремих елементів криптографічних перетворень; практичної криптографії та системного аналізу при порівнянні існуючих методів направленого шифрування на ідентифікаторах та алгебраїчних решітках; програмного моделювання в ході реалізації процесів вироблення основних структурних елементів криптографічних алгоритмів та протоколів на ідентифікаторах та алгебраїчних решітках.

Наукова новизна отриманих результатів роботи полягає в тому, що:

1. Вперше запропоновано сукупність умовних і безумовних критеріїв та показників оцінки гібридних систем направленого шифрування на ідентифікаторах, застосування яких дозволяє отримати оцінки стійкості як відносно окремих атак так і за інтегральним критерієм.

2. Вперше встановлено зв'язок між основними задачами, що можуть вирішуватися в ході оцінки стійкості криптоперетворень на алгебраїчних решітках, що дозволило обґрунтувати та вибрати SVP-задачу, складність вирішення якої для криптоаналітика є максимальною.

3. Вперше запропоновано математичну модель гібридного криптографічного перетворення направленого шифрування на ідентифікаторах та алгебраїчних решітках, стійкість якої базується на SVP-задачі, застосування якої дозволяє довести, що складність атаки «повне розкриття» носить (має) експоненційний характер.

4. Отримав подальший розвиток метод направленого шифрування на ідентифікаторах на основі запропонованої математичної моделі за критерієм швидкодії, для застосування в криптографічних механізмах та протоколах, який відрізняється від існуючих тим, що на основі моделі на алгебраїчній решітці, що дозволило довести експоненційну складність криптоаналізу методом повного розкриття, а також підвищити швидкодію криптографічного перетворення на 2–3 порядки, та реалізувати програмну модель криптоперетворень і провести з її використанням експериментальні дослідження.

Практичне значення отриманих результатів:

1. Розроблено методику дослідження властивостей криптосистем на ідентифікаторах, яка може бути застосована для оцінки стійкості та складності шифрування за умовними та безумовними критеріями.

2. Розроблено умови та рекомендації з підвищення швидкодії гібридних криптосистем на ідентифікаторах, що дозволяє підвищити швидкодію на 2-3 порядки.

3. Розроблено комплекси програмного забезпечення (програмні моделі), що реалізують розроблені гібридні методи направленого шифрування на ідентифікаторах у кільцях зрізаних поліномів з підвищеною швидкодією, та отримані з їх використанням експериментальні результати, які дозволили підтвердити результати теоретичних досліджень.

4. Надано ряд аналітичних відношень та умов реалізації криптографічних перетворень на ідентифікаторах та алгебраїчних решітках, які можуть бути

використані при гармонізації та/або розробці відповідних стандартів направленого шифрування.

Основні результати досліджень впроваджені у діяльності Приватного акціонерного товариства «Інститут інформаційних технологій» та у навчальному процесі Харківського національного університету радіо-електроніки, що підтверджується відповідними актами.

Достовірність і обґрунтованість отриманих наукових результатів підтверджується їх несуперечністю з відомими положеннями теорії імовірності, абстрактної алгебри, відомими результатами, подібністю експериментальних результатів до теоретичних.

Особистий внесок здобувача. Нові наукові результати отримано здобувачем особисто. У роботах, виконаних у співавторстві, здобувачу належать такі результати: в [1] – проведено порівняльний аналіз існуючої нормативної бази в галузі побудування систем направленого шифрування на ідентифікаторах; в [2] – отримано результати теоретичного аналізу основних недоліків та переваг криптографічних систем на ідентифікаторах; в [3] – запропоновано методику оцінки гібридних методів направленого шифрування на ідентифікаторах за обраними критеріями. Під час проведення досліджень в [4] – здобувачем отримано оцінку безпеки та рекомендації щодо вибору системних параметрів гібридних методів направленого шифрування на ідентифікаторах та алгебраїчних решітках; в [5] – проведено аналіз стійкості основних обчислювальних задач на білінійних відображеннях; в [6] – надано оцінку обчислювальної складності основних задач на алгебраїчних решітках; в [7] – проведено порівняльний аналіз відомих обчислювальних задач алгебраїчних решітках та надано обґрунтування взаємозв’язку між даними задачами.

Апробація результатів дисертації. Основні результати роботи представлені та обговорювалися на таких науково-технічних конференціях: на науково-технічній конференції з міжнародною участю «Наукові дослідження молоді – вирішенню проблем європейської інтеграції» (Харків, 2010 р., 2011 р.) [8, 9]; 14-му, 15-му, 16-му Міжнародному молодіжному форумі «Радиоэлектроника и молодежь в XXI веке», (Харків, 2010 р., 2011 р., 2012 р.) [10–12]; Науково-технічній конференції з міжнародною участю «Комп’ютерне моделювання в наукоємних технологіях» (КМНТ-2010, КМНТ-2012), (Харків, 2010 р., 2012 р.) [13, 14]; XIII-й, XV-й, XVI-й міжнародній науково-практичній конференції «Безопасность информации в информационно-телекоммуникационных системах» (Київ, 2010 р., 2012 р., 2013 р.) [15-18]; 17-й Міжнародній науково-технічній конференції «Физические и компьютерные технологии» (Харків, 2011 р.) [19]; II-й Міжнародній науково-технічній конференції «Компьютерные науки и технологии» (Бєлгород, РФ, 2011 р.) [20]; Міжнародній науково-практичній конференції «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньо-економічній діяльності та управлінні організаціями» (Дніпропетровськ, 2011 р.) [21]; II-й Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем» (Львів, 2013 р.) [22]; Міжнародній науковій

конференції «Питання оптимізації обчислень (ПОО-XL)», присвяченій 90-річчю від дня народження академіка В.М. Глушкова (Київ, 2013 р.) [23].

Публікації. Основні наукові результати за темою дисертації опубліковані в семи статтях, з них 6 статей у періодичних виданнях, які входять до переліку фахових видань України та 1 стаття опублікована в зарубіжному журналі, видано 16 тез доповідей на наукових конференціях.

Структура і обсяг роботи. Дисертаційна робота складається із вступу, п'яти розділів, висновків, списку використаних джерел та 5 додатків. Повний обсяг дисертації складає 205 сторінок. Основний обсяг дисертації міститься на 150 сторінках та має 5 ілюстрацій за текстом, 9 таблиць за текстом, у тому числі 5 ілюстрацій на 5 сторінках, 5 додатків на 32 сторінках, список використаних літературних джерел із 204 найменувань на 23 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми та сформульовані об'єкт, предмет, мета, наукова задача досліджень, показано зв'язок роботи з науковими темами і програмами, наукова новизна та практичне значення отриманих результатів, визначено особистий внесок автора в друкованих працях із співавторами, наведено дані про апробацію, публікації і впровадження основних результатів роботи.

У першому розділі на основі аналізу існуючих методів і механізмів направленого шифрування на ідентифікаторах та алгебраїчних решітках показано, що класичні (традиційні) методи направленого шифрування на ідентифікаторах не є задовільними за критеріями стійкості та швидкодії, а класичні (традиційні) методи направленого шифрування на сертифікатах відкритих ключів не є психологічно сприйнятими для кінцевих користувачів.

Показано, що для розв'язання наукової задачі побудування методу направленого шифрування на ідентифікаторах, що задовольняє критерії стійкості та швидкодії, на підставі удосконалення існуючих математичних моделей методів направленого шифрування в кільцях зрізаних поліномів необхідно вирішити такі взаємозалежні наукові задачі:

– оцінити стан нормативно-правової бази, відносно побудування систем на ідентифікаторах та алгебраїчних решітках;

– враховуючи особливості та відмінності криптографічних систем на ідентифікаторах та алгебраїчних решітках від існуючих систем направленого шифрування надати визначення та обґрунтувати системи умовних і безумовних критеріїв та показників оцінки криптографічних систем направленого шифрування на ідентифікаторах та алгебраїчних решітках;

– за визначеними критеріями та показниками оцінки провести аналіз стійкості методів асиметричних криптографічних перетворень на ідентифікаторах та алгебраїчних решітках;

– за результатами аналізу стійкості визначити метод направленого шифрування на ідентифікаторах та алгебраїчних решітках, що є більш прийнятним для інтегрування в існуючу систему ЕЦП;

– вдосконалити обраний метод направленого шифрування за критеріями криптографічної стійкості та складності основних етапів перетворювань;

– розробити основні структурні елементи алгоритмів і протоколів реалізації криптографічної системи на ідентифікаторах та алгебраїчних решітках;

– розробити та провести експериментальні дослідження на програмні моделі, провести теоретичні та практичні узагальнення результатів дослідження;

– розробити рекомендації та пропозиції застосування реалізованої схеми.

У другому розділі проведено оцінку стійкості класичних систем на ідентифікаторах, надається методика оцінки криптосистем на ідентифікаторах та алгебраїчних решітках за безумовними та умовними критеріями, надано оцінку стану сучасної міжнародної нормативно-правової бази в сфері побудування криптосистем на ідентифікаторах.

На відміну від інфраструктури відкритих ключів на сертифікатах, системи IBE не вимагають складної перевірки, попередньої реєстрації або відкликання сертифікатів. Також відсутнім є необхідність підтримки списків відкликаних сертифікатів тощо. Замість підтримання складної системи обслуговування сертифікатів відкритий ключ користувача генерується з його ідентифікатора. Для усунення основних недоліків систем НШ на ідентифікаторах та системи на сертифікатах, необхідним є поєднання даних систем. Рівень стандартизації IBE-систем на міжнародному рівні не є достатнім, а в Україні не існує жодного керівного нормативного документа для даних систем. Але, тим не менш, ведуться роботи над міжнародним стандартом ISO/IEC DIS 18033-5, в якому будуть стандартизовані методи НШ на ідентифікаторах. Тому, необхідним є вироблення національного стандарту, або технічної специфікації, який/яка б визначав(ла) методи НШ на ідентифікаторах, а також загальну структуру побудування та представлення IBE-систем.

Стійкість BDH-задач над еліптичною кривою $E(F_q)$, а також над кінцевим полем F_{q^k}, залежить від стійкості задачі Діффі-Геллмана. Найчастіше, для криптографічних перетворень, що засновані на білінійних відображеннях, використовується підгрупа над $E(F_q)$ достатньо великого простого порядку r. Мінімальним рівнем безпеки для наведених задач є $r > 2^{160}$ і $q^k > 2^{1024}$. Взагалі ефективність криптосистеми залежить від особливостей побудування усієї схеми, але, чим менше значення приймає q, тим швидше виконуються арифметичні операції над кривою $E(F_q)$. Тому, необхідно, щоб параметр q приймав найменше значення, тоді основним параметром безпеки виступатиме k, яке повинне приймати якомога більші значення. Найчастіше обираються точки на $E(F_q)$, для яких $q \approx 2^{170}$, і еліптичні криві з вкладеним ступенем $k = 6$, тобто $q^k \approx 2^{1024}$.

Для криптографічних систем на білінійних відображеннях основними питаннями є: як знайти підходящу еліптичну криву і як швидко обчислити $e(P,Q)$, тому важливим завданням є аналіз обчислювальних задач на решітках,

що на наш погляд дозволить прискорити криптографічні перетворення та покращити показники стійкості криптографічних систем на ідентифікаторах.

Доцільною і актуальною задачею є визначення критеріїв та показників оцінки якості направленого шифрування. Спочатку сформулюємо безумовні критерії, тобто такі, виконання яких, не залежно від типу реалізації криптографічних перетворень НШ, є обов'язковим. Якщо безумовний критерій задовольняється, тоді вважатимемо, що експертна оцінка за безумовним критерієм є позитивною. Кожному безумовному критерію відповідає задане позначення:

1. Необхідність реалізації моделі взаємної недовіри і взаємного захисту. Відкриті та секретні ключі мають вироблятися незалежно, випадково, ймовірно. Даний критерій позначимо, як $K_{Б1}$.

2. Надійність криптографічних примітивів і математичної бази. Складність атаки «повне розкриття» має бути не меншою за експоненційну, а для внутрішніх мереж – за субекспоненційну. Даний критерій позначимо, як $K_{Б2}$.

3. Складність реалізації алгоритмів зашифрування та розшифрування не вище за поліноміальну. Даний критерій позначимо, як $K_{Б3}$.

4. Захищеність від усіх відомих практичних і теоретичних, а також потенційно можливих криптоаналітичних атак. Даний критерій позначимо, як $K_{Б4}$.

5. Статистична захищеність криптографічних перетворень в системі НШ. Статистична незалежність вхідного тексту від зашифрованого блоку повідомлення, вихідної послідовності від ключового матеріалу. Даний критерій позначимо, як $K_{Б5}$.

6. Захищеність протоколів генерації та управління ключами, що використовуються в системі НШ від усіх відомих аналітичних атак. Даний критерій позначимо, як $K_{Б6}$.

7. Надійність ключового матеріалу, що циркулює в системі НШ (відсутність криптографічно слабких ключів). Даний критерій позначимо, як $K_{Б7}$.

8. Складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптоперетворення має бути не вища за поліноміальну. Даний критерій позначимо, як $K_{Б8}$.

Критерієм добору є логічна зміна так/ні (1/0), тоді безумовним інтегральним критерієм для даного асиметричного криптоперетворення є функція відповідності відносно вимог, що висуваються, такого виду:

$$f_{БК}[\ ] = K_{Б1} \cap K_{Б2} \cap K_{Б3} \cap K_{Б3} \cap K_{Б4} \cap K_{Б5} \cap K_{Б6} \cap K_{Б7} \cap K_{Б8}$$

Також, для подальшої оцінки якості направленого шифрування, пропонуються такі умовні критерії та показники оцінки:

1. Критерій придатності щодо застосування відповідно до існуючої нормативно-правової бази України. Даний критерій позначимо, як $K_{У1}$.

2. Критерій випробування часом, тобто знаходження слабких місць та недоліків, прийнятність кінцевими користувачами тощо. Даний критерій позначимо, як K_{y2}.

3. Рівень захищеності системи при реалізації всіх відомих атак та загроз у різних умовах функціонування системи. Даний критерій позначимо, як K_{y3}.

4. Відкритість алгоритму, що лежить в основі конкретної системи. Даний критерій позначимо, як K_{y4}.

5. Прозорість архітектури, наприклад, наявність контролю за діями центру сертифікації та видачі ключів, аудит та контроль дій користувачів. Даний критерій позначимо, як K_{y5}.

6. Прозорість використання системи НШ для кінцевих користувачів. Повинні бути реалізовані центри навчання користувачів та персоналу, працювати центри технічної підтримки. Даний критерій позначимо, як K_{y6}.

7. Надійність операційної роботи системи НШ, позначимо даний критерій, як K_{y7}.

8. Підтримка масштабованості архітектури. До цього критерію відносяться: можливість використання додаткових сервісів, застосування декількох режимів, підтримка різних баз ключів (наприклад, як на базі сертифікатів, так і на базі ідентифікаторів). Даний критерій позначимо, як K_{y8}.

9. Просторові показники оцінки роботи системи НШ. Просторова складність обчислення системних параметрів, вироблення ключових даних, роботи алгоритмів зашифрування та розшифрування. Даний критерій позначимо, як K_{y9}.

10. Швидкісні показники оцінки роботи системи НШ. Часова складність обчислення системних параметрів, вироблення ключових даних, роботи алгоритмів зашифрування та розшифрування. Даний критерій позначимо, як K_{y10}.

11. Вартісні показники впровадження та підтримки роботи системи для організації і для кінцевого користувача вході використання даної системи. Даний критерій позначимо, як K_{y11}.

У третьому розділі дисертаційної роботи було проаналізовано основний існуючий стандартизований метод НШ у кільцях зрізаних поліномів, установлено зв’язок між основними задачами на алгебраїчних решітках, що можуть вирішуватися в ході оцінки стійкості криптографічних перетворень на алгебраїчних решітках, що дозволило обґрунтувати та вибрати SVP-задачу, складність вирішення якої для криптоаналітика є максимальною.

Більшість існуючих криптосистем на алгебраїчних решітках засновані саме на пошуку найкоротших векторів у решітці. Якщо можна знайти потрібний вектор для досить невеликого апроксимаційного фактору, тоді існує можливість провести успішну атаку на дані криптосистеми. Таким чином, щоб оцінити безпеку даних криптосистем, важливо розуміти взаємозв’язок між задачею, що лежить в основі алгоритму, і її апроксимаціями, а також, існуючими алгоритмами вирішення наближених задач.

Так, найбільш важливими обчислювальними задачами на алгебраїчних решітках є задачі SVP і CVP, майже всі інші обчислювальні задачі на решітках можуть бути зведеними до даних задач. Водночас, CVP-задача є неоднорідним варіантом задачі SVP, у якому для даної решітки і деяких цільових точок необхідно знайти відстань до найближчої точки в решітці.

Під SVP-задачею для заданого базису решітки L розумітимемо задачу пошуку такого найкоротшого $y \in L$, що $\|y\| = \lambda_1(L)$. Водночас, під CVP-задачею для заданого базису решітки L і цільового вектора $t \in R^n$ розумітимемо задачу пошуку такого найближчого ненульового вектора $y \in L$, що $\|t - y\| = n(t, L)$.

Стійкість загальних задач на решітках частково залежить від факту існування безлічі можливих базисів для однієї решітки. Обчислювальна складність окремих апроксимацій залежить від параметрів, обраних саме для цієї задачі.

Схеми на основі функцій з секретом, з обраним прообразом, тобто з підібраним базисом за допомогою розподілення Ґаусса, зі стандартним відхиленням, що наближається до найбільшого з векторів Грама-Шміта, отриманих завдяки ортогоналізації цього базису, забезпечують складність найгіршого випадку вирішення задачі на решітках, у моделі випадкового оракулу.

На рис. 1 видно, що SVPγ-задача має декілька вхідних стрілок, що показує, що всі наведені задачі на рисунку можуть бути зведеними до цієї задачі, і навіть, CVPγ-задача через інші апроксимації. Це ще раз показує, що SVP-задача є центральною задачею в теорії алгебраїчних решіток.

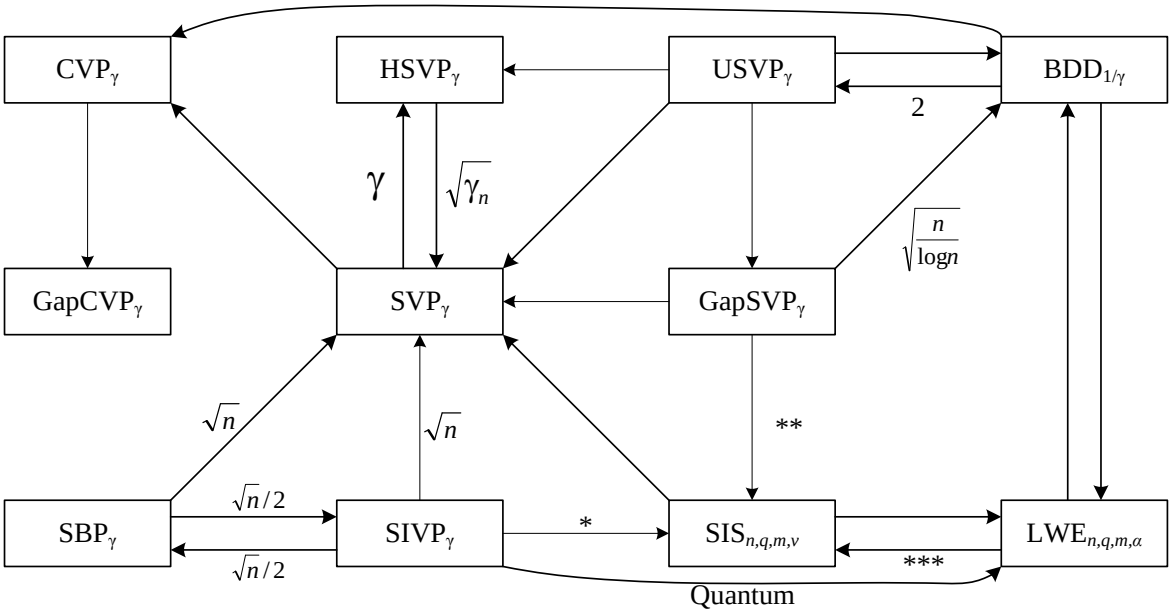

Рисунок 1 – Взаємозв’язок між основними задачами на алгебраїчних решітках

Індекс γ для всіх задач, окрім GapSVP, uSVP і BDD, позначає апроксимаційний фактор. Для GapSVP індекс γ позначає розрив між вихідною задачею, для uSVP індекс γ позначає розрив λ_2 / λ_1, і для BDD індекс $1/\gamma$ позначає зв'язану відстань, якщо стрілка від задачі А до задачі Б позначена, наприклад, фактором α, це означає, що апроксимація задачі А з фактором $\alpha\gamma$ зводиться до апроксимації задачі Б з фактором γ. Тобто, це означає, що якщо можлива апроксимація задачі Б з фактором γ, тоді можлива апроксимація задачі А з фактором $\alpha\gamma$. Задачі SIS і LWE не мають апроксимацій, які б залежали від загальних позначень, їх редукції (позначені *, **, ***) залежать від вибору деяких змінних. Редукція між задачами SIVP і LWE позначена «Quantu», оскільки вона вимагає квантового комп'ютера. Зазначимо, що якщо існує орієнтований шлях від задачі А до задачі Б, тоді задача А також може бути зведена до задачі Б, але, щоб уникнути нерозбірливості, ці редукції були опущені.

Якщо існує оракул, що вирішує $\sqrt{n}$-наближені SVP-задачі факторизації цілого числа, або дискретного логарифму, тоді алгоритми на решітках є більш криптографічно стійкими, ніж алгоритми на основі теоретико-числових проблем. Тобто, можна зробити висновок, що складність вирішення SVP-задачі є максимальною.

У четвертому розділі надано оцінку стійкості існуючих гібридних методів направленого шифрування, що використовують алгебраїчні решітки, надано ряд аналітичних відношень та умов реалізації криптографічних перетворень на ідентифікаторах та алгебраїчних решітках, які можуть бути використані при гармонізації та/або розробці відповідних стандартів направленого шифрування.

Визначено, що основні існуючі гібридні методи НШ на ідентифікаторах у кільцях зрізаних поліномів базуються на LWE-задачі та мають відповідати таким умовам реалізації та аналітичним відношенням:

1. Для алгоритму генерування решітки з функцією з секретом необхідно, щоб $m \geq 5n \log q$. Враховуючи це обмеження для m, вихідною послідовністю алгоритму TrapGen є базис Грама-Шміта довжиною не більше $m \cdot \sqrt{\log m}$. Використовуючи алгоритм SamplePre, секретний ключ вектор e_j, є взятим з дискретного рівняння Ґаусса зі стандартним відхиленням $\sigma \geq m \cdot \log m$, і, таким чином, з майже експоненційно малою ймовірністю, має довжину не більшу за $\sigma\sqrt{m} \leq m^{1.5} \cdot \log m$.

2. Встановлюється розподілення з шумом $\chi = \overline{\psi}_\alpha^m$, де $\alpha \geq 2\sqrt{m}/q$, до якого застосовується редукція Регева. Вектор $\mathbf{x}$, вибраний з цього розподілення, має довжину $O(\alpha q\sqrt{m}) \leq 2m$ з майже експоненційно малою ймовірністю.

3. Для забезпечення коректності розшифрування, необхідно, щоб задовольнялося рівняння $q \geq m^3 \log m \cdot 2^{5l}$.

Стосовно налаштування конкретних параметрів під ці обмеження, враховуючи постійну $\epsilon \in (0,1)$, встановлюється:

- параметр безпеки $n = l^{1/\epsilon}$;
- модуль q має бути простим числом в інтервалі $[n^6 2^{5l}, 2 \cdot n^6 2^{5l}]$;
- $m = n^{1.5} \geq 5n \log q$, має задовольняти першу вимогу.

Проаналізувавши останні два пункти, можна побачити $q \geq m^3 \log m \cdot 2^{5l}$, параметр шуму $\alpha = 2\sqrt{m} / q = 1/(2^{5n\epsilon} \cdot \text{poly}(n))$.

Зв'язавши наведене вище, в найгіршому та середньому випадку, отримуємо захищеність, що відповідає стійкості $2^{O(n^\epsilon)}$ - апроксимацій gapSVP або SIVP на n-мірних решітках, якщо використовувати алгоритми, що працюють в часі $q \cdot \text{poly}(n) = 2^{O(n^\epsilon)}$. З даним рівнем знань алгоритм є LWE-стійким для $\epsilon < 1/2$.

У п'ятому розділі запропоновано математичну модель гібридного криптографічного перетворення направленого шифрування на ідентифікаторах та алгебраїчних решітках, стійкість якої базується на SVP-задачі, застосування якої дозволяє довести, що складність атаки «повне розкриття» носить (має) експоненційний характер. На основі запропонованої математичної моделі удосконалено гібридний метод направленого шифрування на ідентифікаторах та алгебраїчних решітках за критерієм швидкодії, для застосування в криптографічних механізмах та протоколах, який відрізняється від існуючих тим, що на основі моделі на алгебраїчній решітці можна довести експоненційну складність криптоаналізу методом повного розкриття, а також підвищити швидкодію криптографічного перетворення на 2 – 3 порядки, та реалізувати програмну модель криптоперетворень і провести з її використанням експериментальні дослідження. Проведено експериментальні дослідження на програмні моделі, проведено теоретичні та практичні узагальнення результатів дослідження.

Запропонована математична модель побудована на основі криптосистеми NTRU, відмінність полягає в методі генерації ключових даних. Замість відкритого ключа користувача використовується заданий користувачем ідентифікатор, який за допомогою спеціальної функції відображення перетворюється в елемент алгебраїчної решітки. Секретний ключ користувача, на відміну від класичного NTRU методу, виробляється за допомогою відповідного ідентифікатора, а також майстер-ключа системи. Стійкість отриманої математичної моделі базується на складності вирішення задачі пошуку найкоротшого вектора в решітці (SVP-задача) та є експоненційною. Математична модель гібридного методу шифрування наведена в таблиці 1.

На основі запропонованої математичної моделі було розроблено модифікований метод направленого шифрування на ідентифікаторах та алгебраїчних решітках, стійкість якого є експоненційною та заснована на вирішенні задачі пошуку найкоротшого вектора в решітці (SVP-задачі).

Таблиця 1 – Математична модель гібридного методу

	Зашифрування	Розшифрування
Вхідні дані	Відкрите повідомлення m, ідентифікатор користувача ID.	Зашифроване повідомлення c, ідентифікатор користувача ID, майстер-ключ F_{msk}.
Вихідні дані	Зашифроване повідомлення c.	Зашифроване повідомлення m.
Основна операція	Зашифрування: $c \leftarrow h_{ID} b + m$.	Розшифрування $m \leftarrow F_{ID} c$.

Основні компоненти, що використовує запропонований гібридний метод шифрування на ідентифікаторах та алгебраїчних решітках, наведені нижче:

1. Майстер-ключ F_{msk}. У розробленому гібридному методі на ідентифікаторах та алгебраїчних решітках генерується майстер ключ F_{msk}, що складається з N поліномів f_i секретних ключів: $F_{msk} \in \{f_i \mid f_0, \ldots, f_{N-1}\}$.

2. Ідентифікатор користувача ID. Подається у вигляді N бітового рядка, використовуючи функцію гешування: $H(ID)$.

3. Секретний ключ користувача F_{ID}. Обчислюється шляхом множення ненульових бітів даного ідентифікатора ID_i з відповідними поліномами f_i майстер ключа F, тобто, якщо $ID_i = 1$: $F_{ID} \leftarrow \left(\left(\prod_{i=0}^{N-1} f_i \right) \bmod p \right) p + 1.$

4. Відкритий ключ користувача h_{ID}. Обчислюються таким чином: $h_{ID} = (F_{ID})_q \cdot g \cdot p$, де: $(F_{ID})_q$ – зворотний елемент $(F_{ID})_q = F_{ID}^{-1} \bmod q$; g – поліном, тимчасова випадкова компонента; $p = 3$.

5. Сліпий поліном b, що є випадковим компонентом, використовується під час зашифрування для захисту методу НШ від атаки за обраними зашифрованими текстами.

Використовуючи запропонований гібридний метод НШ на ідентифікаторах та алгебраїчних решітках, було розроблено програмну модель, основні просторові та швидкісні результати роботи якої, для різних рівнів захищеності та заданих наборів параметрів, наведені у Таблицях 2 – 3. В ході виконання роботи реалізованого методу використовувався великий модуль $q = 2048$. Для отримання результатів, наведених у таблиці 3, виконувалося 50 генерацій ключових даних та 10000 операцій зашифрування/розшифрування для кожного набору параметрів та обчислювалося усереднене значення часу виконання даних операцій.

Запропоновану модель модифікованого методу направленого шифрування було розроблено за допомогою мови програмування C; результати, наведені в таблиці 3 отримані на ПЕОМ з такими технічними характеристиками:

- процесор Intel Core i5 3570K 3.4GHz, який працював на частоті 3.6GHz;
- оперативна пам’ять 16 Gb RAM, з частотою 1600 MHz;
- операційна система Windows 7 x64 Professional;
- середовище розробки Microsoft Visual Studio Express 2012.

Таблиця 2 – Просторові показники роботи розробленого гібридного методу

Рівень захищеності	Ступінь поліному кільця, N	Максимальна довжина вхідного повідомлення, l_m, біт	Довжина шифротексту, l_c, біт	Коефіцієнт зростання розміру шифротексту, $k_{m\to c}$
112	401	480	4411	9,18958
112	541	688	5951	8,64970
112	659	864	7249	8,39004
128	449	536	4939	9,21455
128	613	776	6743	8,68943
128	761	1000	8371	8,37100
192	677	808	7447	9,21658
192	887	1128	9757	8,64982
192	1087	1360	11957	8,79191
256	1087	1424	11957	8,39676
256	1171	1488	12881	8,65658
256	1499	1976	16489	8,34463

Таблиця 3 – Швидкісні показники роботи розробленого гібридного методу

Ступінь поліному кільця, N	Кількість генерацій ключових даних, шт/с	Кількість операцій зашифрування, шт/с	Кількість операцій розшифрування, шт/с	Швидкість зашифрування, Мбіт	Швидкість розшифрування, Мбіт
401	15.4188	6967.3243	7657.6308	3.3443	33.7778
541	4.2413	10090.8575	11206.9177	6.9425	66.6923
659	3.0191	9823.0132	2778.2307	8.4870	20.1393
449	6.7132	5033.4905	6248.5969	2.6979	30.8618
613	3.4030	8479.7662	9278.6489	6.5802	62.5659
761	2.1193	8167.6245	2221.3485	8.1676	18.5949
677	2.9366	3890.1118	4083.8548	3.1432	30.4124
887	1.1992	5011.5006	5351.9093	5.6529	52.2185
1087	14.7003	4855.5538	5156.2409	6.6035	61.6531
1087	14.7002	3115.0124	3226.9298	4.4357	38.5843
1171	11.9373	3053.0802	3176.2735	4.5429	40.9135
1499	7.3374	2970.6264	3083.5112	5.8699	50.8440

Реалізована модель методу направленого шифрування на ідентифікаторах та алгебраїчних решітках виконує вироблення ключової пари для заданого набору параметрів, зашифрування та розшифрування повідомлення, а також виконує ініціалізацію набору параметрів і ключових даних, що може бути виконана попередньо, або під час виконання операцій зашифрування та/або розшифрування.

У висновках викладено основні результати дисертаційної роботи, розкрито їх наукову та практичну цінність.

ВИСНОВКИ

У дисертаційній роботі отримано нове вирішення актуальної науково-прикладної задачі розробки нових методів і програмних моделей криптографічних перетворень, які засновані на ідентифікаторах та алгебраїчних решітках, а також підвищення швидкодії криптоперетворень та забезпечення необхідного рівня криптографічної стійкості. При цьому отримано наступні нові результати.

В області теорії:

1. Вперше запропоновано сукупність умовних і безумовних критеріїв та показників оцінки гібридних систем направленого шифрування на ідентифікаторах, застосування яких дозволило отримати оцінки стійкості як відносно окремих атак так і за інтегральним критерієм.

2. Вперше встановлено зв'язок між основними задачами, що можуть вирішуватися в ході оцінки стійкості криптоперетворень на алгебраїчних решітках, що дозволило обґрунтувати та обрати SVP-задачу, складність вирішення якої для криптоаналітика є максимальною.

3. Вперше запропоновано математичну модель гібридного криптографічного перетворення направленого шифрування на ідентифікаторах та алгебраїчних решітках, стійкість якої базується на SVP-задачі, застосування якої дозволило довести, що складність атаки «повне розкриття» носить (має) експоненційний характер.

4. Отримав подальший розвиток метод направленого шифрування на ідентифікаторах на основі запропонованої математичної моделі за критерієм швидкодії, для застосування в криптографічних механізмах та протоколах, який відрізняється від існуючих тим, що на основі моделі на алгебраїчній решітці, що дозволило довести експоненційну складність криптоаналізу методом повного розкриття, а також підвищити швидкодію криптографічного перетворення на 2–3 порядки, та реалізувати програмну модель криптоперетворень і провести з її використанням експериментальні дослідження.

В області практичних розробок та експериментальних досліджень:

1. Отримала подальший розвиток методика дослідження властивостей криптосистем на ідентифікаторах, яка може бути застосована для оцінки стійкості та складності шифрування за умовними та безумовними критеріями.

2. Обґрунтовано умови та розроблено рекомендації з підвищення швидкодії криптосистем на ідентифікаторах, що дозволило підвищити швидкодію на 2 – 3 порядки.

3. Розроблено комплекси програмного забезпечення (програмні моделі), що реалізують розроблені методи направленого шифрування на ідентифікаторах в кільцях зрізаних поліномів з підвищеною швидкодією.

4. Запропоновано ряд аналітичних відношень та умов реалізації криптографічних перетворень на ідентифікаторах та алгебраїчних решітках, які доцільно використати при гармонізації та/або розробці відповідних стандартів направленого шифрування.

Наукові та прикладні результати досліджень, які отримані в дисертації, доцільно використовувати: в ході оцінки гібридних методів направленого шифрування, оцінки їх надійності, виявлення переваг і недоліків, прогнозування можливості впровадження даних систем; у державних та приватних установах і підприємствах, включаючи національну систему електронного цифрового підпису, під час створення систем захисту інформації.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Макутоніна, Л.В. Результати аналізу криптосистем на ідентифікаторах, аналіз документів IEEE P1636.3, RFC 5091, RFC 5408 / М.Ф. Бондаренко, П.О. Кравченко, Л.В. Макутоніна // Прикладная радиоэлектроника. Научно-технический журнал. – 2010. – Т.9, №3. – С. 394–400.

2. Макутоніна, Л.В. Криптосистеми на ідентифікаторах, як системи захисту інформації в комп'ютерних мережах на виробництві / І.Д. Горбенко, Л.В. Макутоніна // Наукове видання: Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка «Технічний сервіс АПК, техніка та технології у сільськогосподарському машинобудуванні». – 2010. – Випуск 101. – С. 291–297.

3. Макутоніна, Л.В. Обґрунтування та вибір критеріїв та показників оцінки комбінованих ІВК / І.Д. Горбенко, П.О. Кравченко, Л.В. Макутоніна // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – Тематический выпуск «Информационная безопасность». – 2011. – Выпуск 166. – С. 56–63.

4. Макутоніна, Л.В. Аналіз криптографічних алгоритмів на ідентифікаторах, що використовують алгебраїчні решітки / І.Д. Горбенко, Л.В. Макутоніна // Прикладная радиоэлектроника. – Научно-технический журнал. – 2012. – Том 11, №2. – С. 200–209.

5. Макутоніна, Л.В. Аналіз стійкості обчислювальних задач, що засновані на білінійних відображеннях / І.Д. Горбенко, Л.В. Макутоніна //Радиотехника. Всеукраинский межведомственный научно-технический сборник. – Тематический выпуск «Информационная безопасность». – 2012. – Выпуск 171. – С. 79–89.

6. Макутоніна, Л.В. Обчислювальна складність основних задач на алгебраїчних решітках / М.Ф. Бондаренко, Л.В. Макутоніна // Прикладная радиоэлектроника. – Научно-технический журнал. – 2013. – Том 12, № 2. – С. 258– 264.

7. Макутоніна, Л.В. Взаємозв'язок між основними обчислювальними задачами на алгебраїчних решітках / І.Д. Горбенко, Л.В. Макутоніна, В.В. Котенко // Информационное противодействие угрозам терроризма. – Научно-практический журнал. РФ. – 2013. – №20. – С. 178–182.

Наукові праці апробаційного характеру:

8. Макутоніна, Л. В. Результати порівняльного аналізу криптосистем на ідентифікаторах [Електронний ресурс] / Л.В. Макутоніна // Наукові дослідження молоді - вирішенню проблем європейської інтеграції: зб. наук. статей, 8 квітня 2010 р. – К. : УБС НБУ. – 2010. – 1 електрон. опт. диск (CD-R). – Назва з екрана.

9. Макутонина, Л.В. Анализ существующих механизмов согласования общего ключа на основе идентификационных данных [Електронний ресурс] / Л.В. Макутонина // Наукові дослідження молоді - вирішенню проблем європейської інтеграції: Збірник наукових статей, 7 квітня 2011 р. – К. : УБС НБУ. – 2011. – 1 електрон. опт. диск (CD-ROM). – Назва з екрана.

10. Макутоніна, Л.В. Результати порівняльного аналізу крипто систем на ідентифікаторах / Л.В. Макутоніна // 14-й Міжнародний молодіжний форум Харківського національного університету «Радиоэлектроника и молодежь в XXI веке»,18-20 березня 2010 р. – Харків, Україна. – 2010. – Ч.2 – С. 70.

11. Макутонина, Л.В. Анализ многостороннего протокола согласования общего ключа, на идентификаторах, предложенного Barua, Dutta, Sarkar / Л.В. Макутоніна // 15-й Ювілейний Міжнародний молодіжний форум Харківського національного університету «Радиоэлектроника и молодежь в XXI веке», 18-20 травня 2011р. – Харків, Україна. – 2011. – Т.5. – С. 165–166.

12. Макутоніна, Л.В. Аналіз криптографічних алгоритмів на ідентифікаторах, що використовують алгебраїчні решітки / Л.В. Макутоніна, І.Д. Горбенко//16-й Міжнародний молодіжний форум Харківського національного університету «Радиоэлектроника и молодежь в XXI веке», 17-19 квітня 2012 р. – Харків, Україна. – 2012. – Т.5. – С. 98–99.

13. Макутоніна, Л.В. Результати порівняльного аналізу криптосистем на ідентифікаторах згідно стандартів IEEE P1636.3, RFC 5091, RFC 5408 / П.О. Кравченко, Л.В. Макутоніна // Науково-технічна конференція з міжнародною участю «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2010)» Харківського національного університету ім. В.Н. Каразіна, 18-21 травня 2010 р. – Харків, Україна. – 2010. – Ч.1. – С. 185–189.

14. Макутоніна, Л. В. Аналіз криптографічних алгоритмів на ідентифікаторах, що використовують математичні решітки / Л.В. Макутоніна, І.Д. Горбенко // Науково-технічна конференція з міжнародною участю «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2012)» Харківського національного університету ім. В.Н. Каразіна, 24-27 квітня 2012 р. – Харків, Україна. – 2012. – С. 289–292.

15. Макутоніна, Л.В. Порівняльний аналіз проектів стандартів в галузі криптосистем на ідентифікаторах для інфраструктур відкритих ключів / І.Д. Горбенко, Л.В. Макутоніна // Тринадцатая международная научно-практическая конференция «Безопасность информации в информационно-телекоммуника-ционных системах» НТУУ «КПИ», 18-21 травня 2010 р. – Київ, Україна. – 2010. – С. 57.

16. Макутонина, Л.В. Анализ криптоалгоритмов на идентификаторах, использующих алгебраические решетки / Л.В. Макутонина // Пятнадцатая юбилейная международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» НТУУ «КПИ», 22-25 травня 2012 р. – Київ, Україна. – 2012. – С. 28.

17. Макутонина, Л.В. Анализ комбинированных схем шифрования с открытым ключом по предложенным критериям / Л.В. Макутонина // Пятнадцатая юбилейная международная научно-практическая конференция «Безопасность

информации в информационно-телекоммуникационных системах» НТУУ «КПИ», 22-25 травня 2012 р. – Київ, Україна. – 2012. – С. 37.

18. Макутонина, Л.В. Вычислительная сложность основных задач на алгебраических решетках / Л.В. Макутонина // Шестнадцатая международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах» НТУУ «КПИ», 21-24 травня 2012 р. – Київ, Україна. – 2013. – С. 60.

19. Макутонина, Л.В. Комбинированная инфраструктура открытых ключей, как система защиты электронного документооборота на производстве / Л.В. Макутонина // Семнадцатая Международная научно-техническая конференция «Физические и компьютерные технологии» ХНПК «ФЭД», 20-21 вересня 2011р. – 2011. – С. 136–138.

20. Макутонина, Л.В. Анализ комбинированных инфраструктур открытых ключей, обоснование и выбор критериев / И.Д. Горбенко, П.А. Кравченко, Л.В. Макутонина // Вторая Международная научно-техническая конференция «Компьютерные науки и технологии», 3-5 жовтня 2011 р. – Бєлгород, РФ. – 2011. – С. 408–411.

21. Макутонина, Л.В. Обоснование и выбор критериев для комбинированных инфраструктур открытых ключей / М.Ф. Бондаренко, П.А. Кравченко, Л.В. Макутонина // Міжнародна науково-практична конференція «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями» Академії митної служби України, 2 грудня 2011р. – Дніпропетровськ. – 2011. – С. 130–132.

22. Макутоніна, Л.В. Аналіз криптографічних систем на ідентифікаторах, що використовують математику алгебраїчних решіток / І.Д. Горбенко, Л.В. Макутоніна //2-га Міжнародна науково-технічна конференцію «Захист інформації і безпека інформаційних систем», 30 травня – 01 червня 2013р. – Львів, Україна. – 2013. – С. 74–75.

23. Макутоніна, Л.В. Взаємозв’язок між основними обчислювальними задачами на алгебраїчних решітках / Л.В. Макутоніна // 40-а Міжнародна наукова конференція «Питання оптимізації обчислень (ПОО-XL)», присвячена 90-річчю від дня народження академіка В.М. Глушкова, 30 вересня – 4 жовтня 2013 р. – Кацивелі, Велика Ялта, АР Крим, Україна. – 2013. –С. 158–159.

АНОТАЦІЯ

Макутоніна Л.В. Методи та моделі криптографічних перетворень з доказовою стійкістю, які засновані на ідентифікаторах та алгебраїчних решітках. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Харківський національний університет радіоелектроніки, Харків, 2014.

У дисертації запропоновано та обґрунтовано методику оцінки гібридних методів направленого шифрування на ідентифікаторах за сукупністю умовних і безумовних критеріїв та показників оцінки, застосування якої дозволяє

отримати оцінки стійкості як відносно окремих атак, так і за інтегральним критерієм.

Запропоновано гібридний метод направленого шифрування на ідентифікаторах та алгебраїчних решітках та його програмну модель, для застосування в криптографічних механізмах і протоколах, який відрізняється від існуючих тим, що на основі моделі на алгебраїчній решітці дозволяє довести експоненційну складність криптоаналізу методом повного розкриття, а також підвищити швидкодію криптографічного перетворення на 2 – 3 порядки.

Отримані результати впроваджено до навчального процесу Харківського національного університету радіоелектроніки, а також в АТ «ІІТ».

Ключові слова: направлене шифрування, криптографічні системи на ідентифікаторах, алгебраїчні решітки, кільця зрізаних поліномів, гібридний метод, комбінований метод.

АННОТАЦИЯ

Макутонина Л.В. Методы и модели криптографических преобразований с доказанной стойкостью, которые основаны на идентификаторах и алгебраических решетках. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Харьковский национальный университет радиоэлектроники, Харьков – 2014.

Важной проблемной задачей является развитие теории и практики анализа состояния криптографической защиты информации с учетом развития систем и средств криптографического анализа. Данную задачу можно решить на основе применения криптографических преобразований на идентификаторах и алгебраических решетках.

В диссертации предложен и обоснован комбинированный метод направленного шифрования на идентификаторах и алгебраических решетках, который отличается от существующих тем, что за счет использования криптографических преобразований в кольцах срезанных полиномов обладает экспоненциальной сложностью задачи криптографического анализа методом полного раскрытия, а также позволяет повысить быстродействие криптографического преобразования на 2 – 3 порядка.

Разработана эффективная методика оценки методов направленного шифрования, относительно системы условных и безусловных критериев и показателей оценки, гибридных систем направленного шифрования на идентификаторах, применение которых позволяет получить оценки защищённости, как в отношении отдельных атак, так и по интегральному критерию.

Получена математическая модель гибридного криптографического преобразования направленного шифрования на идентификаторах и алгебраических решетках, применение которой позволяет доказать, что сложность атаки «полное раскрытие» имеет экспоненциальный характер.

Разработаны комплексы программного обеспечения (программные модели), реализующие предложенные методы направленного шифрования на

идентификаторах в кольцах срезанных полиномов с повышенным быстродействием.

Получены ряд аналитических отношений и условий реализации криптографических преобразований на идентификаторах и алгебраических решетках, которые могут быть использованы при гармонизации и / или разработке соответствующих стандартов направленного шифрования.

В целом полученные научные и практические результаты подтвердили возможность реализации механизмов гибридного направленного шифрования на идентификаторах и алгебраических решетках. Основным преимуществом данного метода является возможность доказательства того, что сложность криптоанализа методом полного раскрытия носит экспоненциальный характер, а также обеспечить основное преимущество – уменьшить сложность прямых и обратных криптографических преобразований и, как следствие повысить быстродействие.

Результаты диссертационных исследований внедрены в учебный процесс Харьковского национального университета радиоэлектроники, а также в АТ «ІІТ».

Ключевые слова: направленное шифрование, криптографические системы на идентификаторах, алгебраические решетки, кольца срезанных полиномов, гибридный метод, комбинированный метод.

SUMMARY

Makutonina L.V. Methods and models of cryptographic transformations with proven resistance, which is based on an identity and algebraic lattices. – The manuscript.

Thesis for the candidate`s degree on specialty 05.13.21 – Information security system. – Kharkiv National University of Radio Electronics, Kharkiv, 2014.

In the thesis proposed and proved methods of assessment methods directional hybrid encryption identifier for a set of conditional and unconditional criteria and indicators for assessing the use of which allows you to assess the stability, both in terms of individual attacks, and by a combined criterion.

The dissertation is devoted to solving important scientific and technical task – the development of the combined method Identity-Based Encryption from Lattices and its programming model, for use in cryptographic mechanisms and protocols, which differs from the current that models based on algebraic lattice can bring exponential complexity of cryptanalysis method of full-disclosure, and improve the performance of cryptographic conversion to 2 – 3 orders of magnitude.

Results of dissertations were introduced in educational process of the Kharkiv National University of Radio Electronics and AT “IIT”.

Keywords: asymmetric encryption, identity-based encryption, algebraic lattice ring of truncated polynomials, hybrid method, the combined method.

Підп. до друку 18.02.15. Формат 60х84 1/16. Спосіб друку – ризографія.
Умов. друк. арк. 1,2. Тираж 100 прим. Зам № 2/18.
Ціна договірна

ФЛП Андреев К.В.
Харків, вул. Серпова, 4