Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

МЕЛЬНИЧУК ЄВГЕН ДМИТРОВИЧ

УДК 681.3.06

МЕТОДИ ОЦІНКИ КРИПТОГРАФІЧНОЇ ПРИДАТНОСТІ ВУЗЛІВ НЕЛІНІЙНИХ ЗАМІН БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

05.13.21 – системи захисту інформації

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.
Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник -

доктор технічних наук, професор
Долгов Віктор Іванович,
Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій.

Офіційні опоненти:

доктор технічних наук, професор
Краснобаєв Віктор Анатолійович,
Полтавський національний технічний університет імені Юрія Кондратюка, завідувач кафедри комп'ютерної інженерії;

кандидат технічних наук, доцент
Єсін Віталій Іванович,
Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій.

Захист відбудеться « 24 » вересня 2013 р. о 13 годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки (просп. Леніна, 14).

Автореферат розісланий « 9 » 08 2013 р.

Вчений секретар
спеціалізованої вченої ради І.В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. На сьогоднішній день безпека як «процес» є однією з основних складових економічного і політичного розвитку держав. Немає жодної економічно розвиненої країни, в якій би не було стандарту шифрування або цифрового підпису. Проводяться великомасштабні міжнародні конкурси, в яких беруть участь провідні вчені, криптографи, математики. Серед таких конкурсів можна відзначити європейський конкурс NESSIE, американський конкурс AES, що завершилися відкриттям одного з найбільш широко застосовуваних алгоритмів шифрування сучасності Rijndael. На сьогодні вже завершився ще один великий міжнародний конкурс – SHA-3, метою якого був відбір найбільш перспективних алгоритмів гешування.

Україна в цій гонці «озброєнь» надійними засобами забезпечення захисту інформації також бере активну участь. Так, у 2002 році в Україні був прийнятий національний стандарт електронного цифрового підпису ДСТУ-4145. У 2006 році в Україні було проведено конкурс на вибір національного стандарту блокового симетричного шифрування і, незважаючи на те, що стандарт так і не був прийнятий, були створені досить перспективні шифри. У зв'язку з цим, очевидним фактом є необхідність проведення подальших досліджень сучасних алгоритмів шифрування, їх криптографічних властивостей для пошуку більш перспективних рішень. Особливу увагу при цьому приділено вдосконаленню методичного апарату оцінки стійкості шифрів до численних атак, виявлених до теперішнього часу.

Певний прорив у технологіях та методах криптоаналізу сьогодні пов'язується з роботами д-ра. техн. наук Лисицької І.В., у яких обґрунтовується новий метод оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу. Ця ідеологія, яка виникла зовсім недавно, будується на ряді нових положень, а саме:

– криптографічні властивості шифрів (крім шифру DES) не залежать від використаних в шифрах S-блоків (не виродженого типу);

– всі ітеративні шифри асимптотично є випадковими підстановками;

– випадкові властивості шифрів можна встановити на основі вивчення показників випадковості їх зменшених версій;

– диференціальні та лінійні властивості шифрів асимптотично повторюють властивості випадкових підстановок і закони розподілу переходів XOR таблиць та зміщень таблиць лінійних апроксимацій асимптотично не є рівноймовірними і ряд інших моментів.

Ці положення суперечать багатьом з відомих теоретичних підходів і результатів, тому становлять надзвичайну важливість і актуальність перевірка цих положень і їх додаткове обґрунтування.

Інтереси роботи зосереджуються саме на додатковому обґрунтуванні одного з центральних положень нового методу, який полягає в тому, що показники стійкості сучасних шифрів на відміну від існуючих підходів від

властивостей застосованих S-блоків практично не залежать. Мова йде про більш повне вивчення й дослідження питань оцінки криптографічної придатності блоків нелінійних замін (S-блоків) сучасних шифрів, більш поглибленого і цільового вивчення ролі та місця S-блоків, і, зокрема випадкових S-блоків у забезпеченні стійкості шифрів. Вищезазначене і визначає актуальність теми та досліджень цієї роботи.

Зв'язок роботи з науковими програмами, темами. Дисертаційну роботу виконано в рамках: держбюджетної НДР № 262-1 «Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП на національному та міжнародному рівні» (за наказом МОНУ №1177 від 30.11.2010 р.); госпдоговірної НДР № 09-06 «Дослідження та розробка комбінованих інфраструктур з відкритими ключами на основі використання існуючих ІВК та системи на ідентифікаторах» (ДР №0109U002498); госпдоговірної НДР № 11-06 від 01.01.2011 р. «Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій» (ДР №0111U002634).

Мета та задачі дослідження. Метою роботи є подальший розвиток нового методу оцінки стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, що дозволяє визначити нову позицію у відношенні S-блоків сучасних шифрів, обґрунтувати їх нову роль у забезпеченні стійкості шифрів до атак диференціального та лінійного криптоаналізу.

Об'єктом досліджень є процеси захисту інформації при блоковому симетричному шифруванні.

Предметом досліджень є моделі та методи оцінки криптографічної стійкості шифрів до атак диференціального і лінійного криптоаналізу.

Методи досліджень спираються на використання теорії ймовірностей, математичної статистики, комбінаторики та системного аналізу, методів статистичних випробувань і методів програмного моделювання.

Методи системного аналізу використовувалися в ході визначення ролі і місця S-блокових конструкцій у структурі сучасного шифру, а також в ході обґрунтування удосконаленої методики відбору підстановок із використанням системи критеріїв для оцінки показників їх випадковості.

Методи теорії ймовірностей і математичної статистики використовувались під час дослідження показників відбору підстановок з граничними (теоретичними або асимптотичними) показниками випадковості та в процесі обробки результатів статистичних експериментів з формування підстановок із заданими показниками випадковості.

Методи статистичних випробувань використовувалися під час виконання експериментальних досліджень кореляційних властивостей різних конструкцій підстановних перетворень і оцінки ефективності застосування підстановних конструкцій нових типів у зменшених моделях ряду сучасних шифрів.

Методи комбінаторики використовувалися під час виконання досліджень комбінаторних властивостей підстановних конструкцій.

Для досягнення поставленої мети в роботі сформульовано та розв'язано такі *основні задачі:*

– дослідити підходи щодо виконання оцінки показників криптографічної придатності S-блоків, що використовуються в конструкціях сучасних блокових симетричних шифрів;

– виконати додаткове обґрунтування положення нового методу оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу, яке полягає в тому що всі сучасні блокові шифри через певну кількість циклів незалежно від використаних у шифрах S-блоків набувають властивостей випадкової підстановки;

– сформувати пропозиції з удосконалення моделі випадкової підстановки, уточнити визначення випадкової підстановки;

– вдосконалити метод відбору випадкових S-блоків, який будується на оцінці числа циклів зашифрування, необхідних шифру для досягнення стаціонарного стану, властивого випадковій підстановці;

– дослідити очікувану ефективність удосконаленого методу відбору випадкових підстановок на основі оцінки близькості емпіричних законів розподілу XOR таблиць і таблиць лінійних апроксимацій підстановок теоретичним законам розподілу випадкових підстановок;

– сформувати методи перевірки одного з основних положень нового методу оцінки показників стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу про практичну незалежність показників стійкості шифрів від властивостей підстановних перетворень, які використані при їх побудові;

– дослідити показники випадковості S-блокових конструкцій сучасних БСШ, у тому числі і БСШ, представлених на Український конкурс з вибору кандидата національного стандарту;

– запропонувати конструкції випадкових S-блоків для сучасних шифрів, що забезпечують граничні показники стійкості шифрів до атак диференціального та лінійного криптоаналізу;

– створити програмний комплекс для оцінки диференціальних та лінійних показників зменшених та повномасштабних моделей блокових симетричних шифрів.

Наукова новизна отриманих результатів дисертаційної роботи. Під час виконання дисертаційного дослідження отримано такі нові наукові результати:

1. Набула подальшого розвитку модель випадкової підстановки, що відрізняється уточненими критеріями випадковості, побудованими на основі використання властивостей вибірки випадкових підстановок, що дозволяє обґрунтувати як практичний метод формування випадкових підстановок використання безпосередньо підстановок з виходу генератора випадкових

підстановок, які, як встановлено, мають значення максимумів диференціальних таблиць і значення максимумів зміщень таблиць лінійних апроксимацій, зосереджені в істотно обмеженій області та концентруються навколо теоретичних значень максимумів таблиць випадкових підстановок відповідних степенів.

2. Набув подальшого розвитку метод оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, який на відміну від існуючих засновується на використанні показників стійкості зменшених моделей, що дозволяє, виходячи зі встановленої властивості шифрів асимптотично набувати властивостей випадкових підстановок, визначати показники стійкості великих шифрів з розрахункових співвідношень, властивих випадковим підстановкам. Зокрема, підтверджено працездатність нового методу оцінки стійкості БСШ до атак лінійного та диференціального криптоаналізу в частині додаткового обґрунтування положення, яке полягає в тому, що показники стійкості БСШ (виключаючи DES) не залежать від використаних у шифрах S-блоків, а визначаються показниками випадкових підстановок відповідного степеня.

3. Набув подальшого розвитку метод побудови (відбору) S-блоків з поліпшеними криптографічними показниками, що відрізняється від відомих використанням для відбору S-блоків нового показника криптографічної придатності у вигляді числа циклів, після якого шифр стає випадковою підстановкою, що дозволяє відібрати S-блоки, які забезпечують найкращі динамічні показники ефективності шифрів.

4. Запропоновано новий показник ефективності шифруючих перетворень у вигляді числа циклів, необхідних шифру для переходу до асимптотичного стану, властивому випадковій підстановці, що дало можливість порівнювати різні рішення по побудові шифрів між собою для вибору більш досконалого.

Практичне значення отриманих результатів полягає у тому, що:

– введено нове визначення випадкової підстановки, засноване на застосуванні системи жорстких критеріїв відбору (комбінаторних критеріїв, доповнених диференціальними та лінійними критеріями), виконано теоретичну оцінку очікуваного числа підстановок – критеріям відбору задовольнятиме приблизно 0,4% усіх підстановок;

– отримано практичні результати, які свідчать про те, що шифри Калина, Мухомор і Лабіринт, представлені на український конкурс, є більш досконалими, ніж шифр Rijndael – вони набувають властивостей випадкової підстановки в середньому на 1-2 циклів раніше;

– встановлено практичну недоцільність застосування алгебраїчних методів оцінки властивостей булевих функцій для виконання реальних оцінок криптографічних показників S-блоків;

– отримано практичні рекомендації щодо підстановної конструкції випадкового типу для застосування в існуючих і перспективних шифрах;

– встановлено, що як S-блоки, які дозволяють виконати ефективне шифрувальне перетворення, можуть виступати S-блоки, обрані випадковим чином. Це означає, що задача пошуку конструкцій досконалих S-блоків, якій приділяється величезна увага в сучасній літературі, втратила практичний сенс. Цю задачу у рамках даної роботи повністю розв'язано.

Обґрунтованість і достовірність наукових положень дисертації підтверджується збігом результатів експериментальних даних статистичних експериментів та іспитів малих і великих версій шифрів із розрахунковими, що випливають з теоретичних співвідношень, а також їх несуперечливістю з відомими результатами криптоаналізу БСШ, математичної теорії підстановок, теорії ймовірностей та математичної статистики.

Отримано акти реалізації результатів досліджень на виробництві у діяльності АТ «Інститут інформаційних технологій» (від 16.01.2013 р.) та у навчальному процесі Харківського національного університету радіоелектроніки (від 17.01.2013 р.).

Особистий внесок здобувача. У роботах, які написані у співавторстві, автору належить: [1] – постановка статистичного експерименту та статистична обробка результатів експериментальних досліджень з визначення показників відбору підстановок, що володіють теоретичними значеннями законів розподілу переходів з XOR таблиць і зсувів таблиць лінійних апроксимацій; [2] – статистичний аналіз властивостей таблиць диференціальних різниць і таблиць лінійних апроксимацій для випадково відібраних блоків нелінійних перетворень порядку 2^4 і 2^8; [3] – дослідження диференціальних і лінійних показників стійкості блокового шифру з Білоруського стандарту 34.101.31-2011 з використанням стандартних і випадкових підстановок; [4] – постановка експерименту та обробка результатів досліджень з визначення диференціальних та лінійних показників стійкості блокових шифрів AES, Калина, Мухомор і Лабіринт з використанням стандартних і випадкових підстановок; [5] – постановка експерименту з визначення диференціальних і лінійних показників алгоритму Хейса і зменшеної моделі шифру Rijndael.

Апробація результатів дисертації. Основні результати дисертації доповідалися та були ухвалені на таких науково-технічних конференціях:

– 5-й Міжнародній науково-технічній конференції «Гарантоздатні (надійні та безпечні) системи, сервіси та технології» (Кіровоград, 2010 р.);

– 8-й Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2010 р.);

– 15-й Міжнародній молодіжній науково-технічній конференції «Радіоелектроніка і молодь в XXI столітті» (Харків, 2011 р.);

Публікація результатів роботи. Основні положення та результати дисертаційної роботи викладено у 11 наукових працях: 6 статей, 5 матеріалів конференцій та тез доповідей. З них 5 статей у трьох наукових журналах, що входять до переліку фахових наукових видань України, 1 стаття у міжнародному фаховому виданні.

Структура та обсяг дисертації. Дисертація складається із вступу, 5 розділів, висновків, списку використаних джерел та 2 додатків. Повний обсяг дисертації становить 186 сторінок, що включає 2 рисунки, 53 таблиці (рисунки та таблиці, що займають окрему площу на 11 стор.), 2 додатки (на 11 сторінках) список використаних джерел з 173 найменувань (на 22 сторінках).

ОСНОВНИЙ ЗМІСТ

Вступ містить обґрунтування актуальності роботи, мету, об’єкт та задачі досліджень, визначення наукової новизни та практичної значущості отриманих результатів, відомості про їх апробацію та реалізацію, а також характеристику публікацій.

У **першому** розділі надано загальну характеристику сучасного етапу розвитку технологій захисту інформації в Україні. Відмічається, що інформація стала характерною рисою життя сучасного суспільства.

Обґрунтовується важливе місце блокових симетричних шифрів у сучасних технологіях захисту інформації, їх нова роль, яка з’явилася з появою принципів шифрування з відкритим ключем. Нагадуються ідеї побудови широко розповсюдженого SKIP протоколу, що реалізований в багатьох сучасних стандартах у вигляді гібридних шифрів, де ″асиметричні шифри використовуються для зашифрування секретного ключа, який у свою чергу використовується для зашифрування фактичного повідомлення із застосуванням симетричних криптографічних методів″.

В ході обговорення сучасних методів проектування і розробки БСШ розглядається шифр Rijndael, стисло висвітлюються перспективні принципи, які використані при побудові цього шифру, відмічається важлива роль, яка була приділена розробниками шифру вибору S-блоків (нелінійної заміни).

На основі аналізу публікацій викладається стисла характеристика сучасних підходів щодо оцінки показників стійкості БСШ до атак диференціального та лінійного криптоаналізу. Як конструктивні висновки відмічаються три.

Перший висновок полягає у тому, що оцінки відповідних показників стійкості відрізняються в різних роботах у значних межах.

Другий висновок полягає у тому, що результуючі показники доказової стійкості (доказовою безпеки) шифрів практично у всіх роботах зв'язуються з відповідними криптографічними показниками S-блокових конструкцій, що входять в шифри.

Третій висновок зводиться до того, що практично у всіх роботах показники стійкості шифрів до атак диференціального і лінійного криптоаналізу оцінюються за допомогою показників MADP – максимальна середня диференціальна ймовірність і MALP (MALHP) – максимальна середня лінійна ймовірність (максимальна середня ймовірність лінійного корпусу), які характеризують не потенційні, а середні значення відповідних показників.

Відмічається, що дослідження, проведені вченими кафедри БІТ ХНУРЕ, свідчать, що точка зору, яка розвивається у багатьох публікаціях, не є об'єктивною. Вченими кафедри висунуто нову концепція визначення показників доказової стійкості шифрів до атак диференціального та лінійного криптоаналізу, яка в протилежність існуючої точки зору не пов'язана з властивостями S-блоків, що входять в шифр.

Тому дуже актуальним є напрямок досліджень цієї роботи – більш ґрунтовно розібратися в ролі S-блоків у вирішенні питань забезпечення стійкості шифрів до атак диференціального і лінійного криптоаналізу.

Розділ завершується формулюванням задач досліджень роботи, які наведені вище.

Другий розділ присвячується викладенню сутності методу оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу.

Використання методу оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу виглядає наступним чином:

1. Обирається блоковий симетричний шифр.
2. Будується зменшена модель шифру.
3. Обраховуються диференціальні та лінійні показники випадкової підстановки: будуються закони розподілу таблиці диференціальних різниць та таблиці лінійних апроксимацій
4. Виконується перевірка чи набуває поменше на модель шифру властивостей випадкової підстановки;
5. Робиться припущення що повнорозмірна модель шифру теж набуває властивостей випадкової підстановки відповідної степені.
6. (необов'язковий крок) Перевіряється припущення що повнорозмірна модель шифру набуває властивостей випадкової підстановки відповідної степені.
7. Згідно з доведеною у роботі Лисицької І.В. методологією для оцінки криптографічної стійкості шифру до атак диференціального та лінійного криптоаналізу скористаємось формулами для розрахунку максимумів таблиці диференціальних різниць та таблиці лінійних апроксимацій для випадкової підстановки відповідного степеню.
8. Отримані значення (за формулами для розрахунку максимумів таблиці диференціальних різниць та таблиці лінійних апроксимацій для випадкової підстановки відповідної степені) і будуть показниками доказової стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу.

Сама сутність нового методу оцінки стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу ґрунтується на наступному положенні: Всі сучасні блокові шифри через певну кількість циклів незалежно від використовуваних у шифрах S-блоків (звичайно, тут йдеться не

про вироджені їхні конструкції) набувають властивостей випадкових підстановок, тобто за комбінаторними показниками (кількість інверсій, зростань і циклів), а також за законами розподілу переходів таблиць XOR різниць (повних диференціалів) і законами розподілу зміщень таблиць лінійних апроксимацій (лінійних корпусів) повторюють відповідні показники випадкових підстановок. У результаті значення максимумів повних диференціалів і лінійних корпусів можуть бути визначені розрахунковим шляхом з формул для законів розподілу ймовірностей переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок відповідного степеня. При цьому, перевірка показників випадковості великих шифрів може бути виконана на основі розробки і подальшого аналізу показників випадковості зменшених моделей, що допускають проведення обчислювальних експериментів в прийнятні (реальні) терміни.

Далі наводиться понятійний апарат лінійного та диференціального криптоаналізу. Визначаються такі поняття, як: диференціальна ймовірність DP^f та лінійна ймовірність LP^f, максимальне значення диференціальної і лінійної ймовірностей $DP_{\max}^f$ и $LP_{\max}^f$ для ключезалежної функції *f*, середнє значення диференціальної ймовірності (*ADP*) функції $f[k](x)$, середнє значення ймовірності лінійного корпусу (*ALHP*) функції $f = f[k](x)$, максимум середнього значення диференціальної ймовірності (*MADP*) та максимум середнього значення ймовірності лінійного корпусу (*MALHP*) для ключезалежної функції $f = f[k](x)$ з *n*-бітовим входом *x* і *n*-бітовим виходом *y*.

У новому методі пропонується для оцінки стійкості БСШ до атак диференціального криптоаналізу користуватися не *MADP* (максимумом середньої диференціальної ймовірності) для деякого фіксованого переходу вхідної різниці у вихідну різницю, а середніми (за множиною ключів) значеннями максимумів диференціальних ймовірностей (*AMDP*) ключезалежної функції, а для лінійного криптоаналізу відповідно користуватися не *MALHP* а *AMLHP*). Наведемо визначення цих понять.

Визначення 1. (*AMDP*). Середнє (за множиною з 2^h ключів) значення максимальних диференціальних ймовірностей ключезалежної функції $f[k](x)$ є

$$AMDP^f = \underset{k}{ave}\, DP_{\max}^{f[k]} = \frac{1}{2^h}\sum_{k=1}^{2^h} DP_{\max}^{f[k]}. \qquad (1)$$

Визначення 2. (*AMPLH*). Середнє (за ключами) значення максимальних ймовірностей лінійних корпусів функції $f[k](x)$ є

$$AMLHP^f = \underset{k}{ave}\, LP_{\max}^f(Гx \to Гy) = \frac{1}{2^h}\sum_{k=1}^{2^h} LP_{\max}^{f[k]}. \qquad (2)$$

Тут $DP_{\max}^{f[k]}$ і $LP_{\max}^{f[k]}$ – максимальне значення диференціальної і лінійної ймовірності для ключезалежної функції $f[k](x)$, k – значення ключа зашифрування.

Ці показники є більш адекватними розв'язуваній задачі.

Саме з використанням цих двох показників виконано обґрунтування нової ідеології оцінки доказової стійкості БСШ у великому числі робіт на цю тему.

У розділі наводяться два важливих результати з теорії випадкових підстановок. Тут йдеться про закони розподілу ймовірностей переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок.

Ми наведемо теореми, які визначають ці закони.

Твердження 1. Для будь-яких відмінних від нуля фіксованих $\Delta X, \Delta Y \in Z_2^n$ у припущенні, що підстановка π обрана рівноймовірно з множини S_2^n і $0 \le k \le 2^{n-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \binom{2^{m-1}}{k}^2 \cdot \frac{k! \cdot 2^k \cdot \Phi(2^{m-1} - k)}{2^m!}, \tag{3}$$

де функція $\Phi(d)$ визначається виразом

$$\Phi(d) = \sum_{i=0}^{d} (-1)^i \cdot \binom{d}{i}^2 \cdot 2^i \cdot i! \cdot (2d - 2i)!. \tag{4}$$

Тут $\pi : Z_2^n \to Z_2^n$ – бієктивне *n*-бітне відображення, S_2^n – множина усіх таких відображень, $\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)$ – ймовірність, що перехід вхідної різниці ΔX у вихідну різницю ΔY дорівнюватиме $2k$.

Твердження 2. Нехай $\lambda(\alpha, \beta)$ буде випадковим числом, що відповідає значенню лінійної апроксимаційної таблиці підстановки $LAT_\pi(\alpha, \beta)$, коли підстановка π обрана рівноймовірно з множини S_2^n і маски α, β ненульові. Тоді $\lambda(\alpha, \beta)$ для цілих значень k, $0 \le k \le 2^{n-1}$ приймає тільки парні значення і ймовірність $\Pr\left(\lambda(\alpha, \beta) = 2k\right)$, що $\lambda(\alpha, \beta) = 2k$ визначається виразом

$$\Pr\left(\lambda(\alpha, \beta) = 2k\right) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \binom{2^{n-1}}{k}^2. \tag{5}$$

Один з основних висновків нового методу полягає в тому, що наведені закони розподілу ймовірностей випадкових підстановок асимптотично виконуються й для шифруючих перетворень усіх сучасних блокових симетричних шифрів.

З використанням цих математичних законів формуються розрахункові співвідношення для визначення максимальних значень повних диференціалів і максимальних значень лінійних корпусів для випадкових підстановок.

У висновках зазначається, що центральним положенням нового методу є визнання того факту, що максимальні значення повних диференціалів і лінійних корпусів для БСШ, які визначають за сучасними мірками показники стійкості шифрів до атак диференціального і лінійного криптоаналізу, можуть бути отримані розрахунковим шляхом. Вони не залежать (при достатній кількості циклових перетворень ні від властивостей використаних у шифрах

підстановних конструкцій, ні від методів введення в циклові функції циклових підключів, ні від способу побудови розширеного лінійного перетворення циклової функції, а є функцією тільки розміру бітового входу в шифр (степеня підстановки). Додатному обґрунтуванню цього положення й присвячена ця дисертаційна робота.

Третій розділ присвячений удосконаленню математичної моделі випадкової підстановки, на яку орієнтовані дослідження даної роботи. Об'єктом такої моделі є випадкова підстановка. Визначення випадкової підстановки засновано на використанні відомих з комбінаторики асимптотичних законів розподілу інверсій, зростань та циклів, на законах розподілу елементів таблиць диференційних різниць та лінійних апроксимацій.

Випадковою при цьому підході вважається підстановка, яка за кількістю інверсій, зростань і циклів попадає в інтервали, що задаються середньоквадратичним відхиленням кожного із цих параметрів від математичного очікування відповідного асимптотичного (нормального) закону розподілу, який відповідає значенню критерію відбору за комбінаторними показниками $a = 1$ (a – нормуючий коефіцієнт перед середньоквадратичним відхиленням, яке також визначається з теоретичного розподілу), а також у якої з заданою мірою відповідності співпадають закони розподілу диференціальних різниць та лінійних апроксимацій випадкової підстановки.

Таким чином, стан об'єкту існуючої моделі можна описати співвідношеннями для середньоквадратичного відхилення кожного із трьох критеріїв від математичного очікування відповідного асимптотичного закону розподілу в також співвідношеннями для законів розподілу диференціальних різниць та лінійних апроксимацій випадкової підстановки.

Задля удосконалення математичної моделі випадкової підстановки пропонується удосконалити визначення об'єкту моделі, а саме доповнити визначення випадкової підстановки наступним чином: до показників випадкової підстановки віднести кількість циклів зашифрування за яких шифр набуває стаціонарного стану при впровадженні до циклової функції підстановки. Так, пропонується увести критерій (правило) переваги, що формулюється наступним чином: кращою є та випадкова підстановка з використанням якої шифр за меншу кількість циклів набуває стаціонарного стану. З визначення витікає то що удосконалена модель випадкової підстановки стає застосовною для конкретного шифру.

Також пропонується удосконалити існуючий метод відбору випадкових S-блоків уведенням додатного критерію що ґрунтується на кількості циклів зашифрування за яких шифр набуває стаціонарного стану.

Стисло сутність існуючого методу виглядає так:

1. Обирається довільна підстановка.

2. Обраховуються значення комбінаторної групи показників (розподіл інверсій, циклів та зростань) випадкової підстановки.

3. Порівнюються відповідні значення показників обраної та випадкової підстановок (перевіряються критерії 1-3 випадковості існуючого методу).

4. Обраховуються значення законів розподілу для таблиці диференційних різниць та таблиці лінійних апроксимацій. Порівнюються теоретичні та емпіричні закони, оцінюється максимальна різниця законів (критерії 4 та 5 випадковості відповідно до існуючого методу). Якщо на третьому та п’ятому кроці розраховані та емпіричні показники співпадають у рамках встановлених параметрів, то вважається що підстановка є випадковою.

Пропонується увести новий критерій переваги що передбачає додатні кроки методу:

7. Будується зменшена (або повнорозмірна) модель шифру для якого обирається підстановка.

8. Обрана підстановка впроваджується у циклову функцію шифру.

9. Виконується побудова повного диференціалу та таблиця зміщень лінійних корпусів шифру за виконання різної (від нуля до повноциклової довжини) кількості циклової функції у шифруючому перетворенні.

10. Виконується пошук необхідної кількості циклів шифрування для досягнення шифром стаціонарного стану за диференційними та лінійними показниками.

11. Кращою (за новим критерієм переваги) буде та підстановка, за використання якої шифр швидше набуде стаціонарного стану.

Спочатку увага зосереджується на стислому викладенні підходу щодо визначення випадкових підстановок, що базується на використанні відомих з комбінаторики асимптотичних законів розподілу інверсій, зростань та циклів.

Випадковою при цьому підході вважається підстановка, яка за кількістю інверсій, зростань і циклів попадає в інтервали, що задаються середньоквадратичним відхиленням кожного із цих параметрів від математичного очікування відповідного асимптотичного (нормального) закону розподілу, який відповідає значенню критерію відбору за комбінаторними показниками $a = 1$ (a – нормуючий коефіцієнт перед середньоквадратичним відхиленням, яке також визначається з теоретичного розподілу).

Далі уточнюються відомі комбінаторні критерії відбору у напрямку підвищення їх жорсткості. Встановлено, що підвищення жорсткості критеріїв відбору (аж до $a = 0$) призвело до суттєвого зменшення множини допустимих підстановок (старі критерії проходили близько 50% усіх підстановок).

Подальші дослідження концентруються на двох нових методах (нових критеріях) відбору випадкових підстановок. Вони були сформульовані у вигляді четвертого і п'ятого критеріїв (1-й, 2-й та 3-й – це комбінаторні критерії).

Стисло сутність досліджень, виконаних у цьому напрямку, можна прокоментувати таким чином.

Додатні критерії відбору були побудовані на основі оцінки близькості емпіричних законів розподілу переходів XOR таблиць і зміщень таблиць

лінійних апроксимацій теоретичним законам (використовувався критерій згоди Колмогорова).

Була поставлена задача оцінити вплив на показники відбору підстановок граничних значень критерію Колмогорова.

Для розв'язання цієї задачі був розроблений програмний комплекс, що дозволив генерувати випадкові підстановки. Досліджувалися підстановки степеня 2^4 та 2^8, що є найбільш популярними в ході конструювання сучасних шифрів.

З використанням цього комплексу проведено численні експерименти при різних сполученнях і значення п'яти критеріїв. У результаті обробки даних експериментів встановлено, що всі критерії випадковості є значною мірою незалежними, кожен із критеріїв вносить свою частку у відсів підстановок, що виключаються з кандидатів на випадкові підстановки. Граничні значення параметрів відбору (допустимих розбіжностей емпіричного та теоретичного законів розподілу ймовірностей) істотно залежать від степеня досліджуваних підстановок. Зі збільшенням степеня підстановки мінімально досяжна ступінь розбіжності розподілів швидко зменшується. Встановлено також, що критерії відбору з диференціальних і лінійних властивостей є більш жорсткими.

Далі було виконано теоретичну оцінку очікуваного числа випадкових підстановок с заданими розподілами переходів парних різниць XOR таблиць та зміщень таблиць лінійних апроксимацій.

Результати експериментів підтвердили можливість генерації підстановок з показниками, що відповідають ″еталонним″ значенням законів розподілу ймовірностей. Підстановки, що проходять систему найжорсткіших критеріїв відбору за всіма п'яти критеріями запропоновано називати досконалими.

Окремо також виконано дослідження на відповідність новим критеріям відбору підстановних конструкцій сучасних БСШ. Всі вони опинилися далекими від досконалих.

Застосування наведених вище критеріїв для практичного відбору випадкових підстановок зустріло певні труднощі, через те що не зрозумілою стала сама стратегія застосування цих критеріїв. Начебто ми породжуємо випадкові підстановки, а потім починаємо їх фільтрувати. Не зрозуміло, які ж показники відбору є кращими.

В останньому підрозділі ми змінили позицію до визначення показників випадковості. Було поставлене питання, якими властивостями володітиме вибірка випадково взятих підстановок? З якими підстановками в цьому випадку реально ми маємо справу? Як вони співвідносяться з введеними вище критеріями відбору?

Отже, увага була зосереджена на вивченні властивостей вибірки випадкових підстановок. Ми зацікавились максимальними значеннями таблиць XOR переходів і зміщень таблиць лінійних апроксимацій на множині випадкових підстановок.

У роботі відмічається, що розподіл максимумів великих за обсягом вибірок незалежних однаково розподілених випадкових величин добре

вивчений в теорії ймовірностей і описується розподілом екстремальних значень Фішера-Тіппета або log-Вейбула у вигляді:

$$D_{\max}(X) \approx e^{-e^{\frac{a-X}{b}}}. \quad (6)$$

Цей розподіл має математичне очікування $\mu(X) = a + b\gamma$ с $\gamma \approx 0{,}58$ й середньоквадратичне відхилення $\frac{\pi}{\sqrt{6}}b \approx 1{,}3b$. Параметр a є розв'язком рівняння

$$\ln(2)Y = f(x), \quad (7)$$

а b є одиницею, поділеною на похідну функції $f(x)$ у точці a.

Вирішено завдання визначення законів розподілу максимумів XOR таблиць та максимумів зміщень таблиць лінійних апроксимацій вибірки байтових підстановок, коли розподіл множини незалежних випадкових змінних у першому випадку підкоряється пуассонівському закону, а в другому – нормальному.

Ми тут наведемо, для ілюстрації, розрахункове співвідношення, отримане для визначення інтегрального закону розподілу максимумів переходів XOR таблиць вибірки випадкових підстановок степеня 2^8. Воно має вигляд

$$D_{\max}(X) \approx e^{-e^{\frac{10-2\cdot X}{0{,}87}}}. \quad (8)$$

У табл. 1 наведено результати визначення розподілу значень максимумів таблиць XOR різниць для 256 бітних підстановок, розрахованих за виразом (8) разом із результати проведених експериментів.

Таблиця 1 – Розподіл максимумів вибірки для підстановок степеня 2^8

k^* (X_1, X_2)	$\Pr(k^*) = D_{\max}(X_1) - D_{\max}(X_2)$	Розрахункове значення	Експеримент
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	95
12 (12,10)	0,905 – 0,368 = 0,537	137	143
14 (14, 12)	0,9901 – 0,905 = 0,008	22	19
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	1
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0

Результати експериментів практично повторюють теоретичні дані. Вони свідчать, що максимальні значення диференціальних і лінійних ймовірностей зосереджені поблизу своїх середніх значень, і для оцінки показників доказової стійкості шифрів цілком достатньо визначати диференціальні й лінійні показники шифрів для одного довільно взятого ключа зашифрування.

Аналогічні результати отримані для закону розподілу максимумів зміщень таблиць лінійних апроксимацій.

Відповідно до отриманих результатів вводиться уточнене визначення випадкової підстановки. Зокрема, байтова підстановка є випадковою, якщо:

1) значення максимуму її XOR таблиці приймає значення 10,12,14,16, причому значення 10 і 12 є більш істотно ймовірними, ніж 14 і тим більше 16;

2) значення максимумів зміщень її таблиці лінійних апроксимацій мають значення в діапазоні 30–42 (а практично 32–38).

Цими визначеннями ми уточнюємо критерії 4 і 5, введені раніше. Уточнення стосується накладення (виконання) обмежень лише на максимальні значення переходів XOR таблиць і зсувів таблиць лінійних апроксимацій.

Таким чином, результатом виконаних досліджень цього розділу є уточнене визначення випадкової підстановки (уточнена модель випадкової підстановки), що побудована на властивостях вибірки з випадкових підстановок. Як виявилось з дуже великою ймовірністю ми отримуватимемо підстановки, для яких значення максимумів диференціальних таблиць і значення максимумів зміщень таблиць лінійних апроксимацій приймають істотно обмежену кількість можливих значень. Всі вони концентруються навколо теоретичних значень максимумів таблиць випадкових підстановок відповідних степенів.

Четвертий розділ роботи присвячений дослідженню зв’язку диференціальних та лінійних показників S-блокових конструкцій з криптографічними показниками блокових симетричних шифрів – це основний розділ роботи. Тут спочатку наводяться результати аналізу більшості публікацій, що присвячені побудові S-блоків з покращеними криптографічними властивостями.

Обговорюється методика виконання досліджень, визначаються довірчі інтервали для визначення моментів приходу шифрів до стаціонарного стану.

Розглядаються дві зменшені моделі шифрів: одна зі слабким лінійним перетворенням, а інша з сильним лінійним перетворенням (коефіцієнт розгалуження в одному випадку близький до 3-х, а в другому дорівнює 5-ти).

Як універсальна модель шифрів зі слабким лінійним перетворенням у роботі обраний 16-бітний шифр, запропонований в роботі професора Хеуса.

Шифром із сильним лінійним перетворенням виступає зменшена до 16-бітного входу конструкція шифру Rijndael з операцією MixColumn на весь текст (з множенням на матрицю розміру 4×4).

У роботі наводяться у вигляді таблиць численні результати експериментів, у яких подано поциклові значення максимумів XOR таблиць та зміщень таблиць лінійних апроксимацій для шифру Хеуса і шифру Rijndael для великої кількості напівбайтових S-блоків, починаючи від ідеальних (отриманих шляхом повного перебору), квадратичних S-блоків, S-блоків шифру Serpent, а також S-блоків випадкового типу. У всіх випадках шифри прийшли до асимптотичного стану випадкової підстановки. Тільки, якщо у випадку слабкого лінійного перетворення шифри приходять до випадкових підстановок за 6–9 циклів шифрування, то у випадку сильного лінійного перетворення всі шифри приходять до випадкових підстановок за 3–4 цикли. Ми тут для

ілюстрації наводимо дві з таких таблиць (див. табл. 2,3) для шифру baby-Rijndael, у якому використовуються підстановки випадкового типу.

Результати експериментів, виконані в даній роботі, та й в інших роботах на цю тему, показали, що властивості (відмінність) підстановок можна відчути (побачити) тільки в шифрах з поганим (малоефективним) дифузійним шаром. Шифри з хорошим дифузійним шаром цієї різниці просто не відчувають! Сама різниця, якщо вона є, виявляється в кількості циклів, необхідних шифру для приходу до стаціонарного стану.

Залишається зазначити, що до аналогічних висновків ми та інші дослідники дійшли і при використанні великих шифрів. Експерименти з ними також повністю підтвердили вихідну гіпотезу про збіжність шифрів із зростанням кількості циклів до показників випадкових підстановок відповідного степеня. Усі розглянуті шифри повноциклової довжини незалежно від S-блоків прийшли до стану випадкової підстановки! Отже гарне лінійне перетворення (з високим значенням коефіцієнта розгалуження) нівелює різницю між S-блоками.

Таблиця 2 – Поциклові значення максимумів повних диференціалів (XOR таблиць) шифру baby-Rijndael з випадковими S-блоками

Випадкові підстановки		1	2	3	4	5	6
1	0,A,4,C,3,7,E,9,1,F,2,B,5,6,D,8	24576	335,9	25,27	**19,27**	18,93	19,27
2	B,5,A,2,7,D,8,E,4,3,1,F,6,C,9,0	32768	768	34,4	**19,07**	18,87	19,27
3	3,B,4,C,1,A,8,5,2,0,D,E,7,6,9,F	24576	355,2	21,93	**19**	19,33	19,2
4	3,6,C,7,0,D,5,A,B,1,2,4,9,8,F,E	24576	223,2	**19,53**	19,2	19	18,93
5	2,4,5,A,9,E,7,B,C,6,F,3,1,0,8,D	24576	223,1	**19,53**	19,33	19,33	19,27
6	C,A,E,2,0,9,4,8,5,1,6,B,7,D,F,3	24576	524,00	32,13	**19,33**	19,27	19,00
7	0,D,F,5,7,4,3,B,E,6,9,2,8,C,1,A	24576	190,40	20,93	**19,07**	19,07	19,4
8	7,F,E,B,1,2,0,D,5,C,4,8,A,3,6,9	24576	328,00	35,6	**19,33**	19,13	19,2
9	4,2,0,E,6,B,D,7,C,A,9,F,1,5,3,8	24576	216	**19,16**	19,2	19,33	19,47
10	6,1,7,F,C,4,5,D,0,E,8,2,A,3,B,9	24576	336	29,07	**19,2**	19,53	19,27

Таблиця 3 – Поциклові значення максимумів зміщень лінійних корпусів шифру baby-Rijndael для випадкових S-блоків

Випадкові підстановки		1	2	3	4	5	6
1	0,A,4,C,3,7,E,9,1,F,2,B,5,6,D,8	24576	5184	1000	**796**	814	824
2	B,5,A,2,7,D,8,E,4,3,1,F,6,C,9,0	24576	5248	1616	**828**	838	836
3	3,B,4,C,1,A,8,5,2,0,D,E,7,6,9,F	24576	3584	984	**816**	808	794
4	3,6,C,7,0,D,5,A,B,1,2,4,9,8,F,E	24576	3584	**816**	794	820	808
5	2,4,5,A,9,E,7,B,C,6,F,3,1,0,8,D	24576	3520	**856**	886	844	866
6	C,A,E,2,0,9,4,8,5,1,6,B,7,D,F,3	24576	5248	1096	**826**	804	822
7	0,D,F,5,7,4,3,B,E,6,9,2,8,C,1,A	24576	3584	928	**858**	816	810
8	7,F,E,B,1,2,0,D,5,C,4,8,A,3,6,9	24576	3520	**808**	874	850	842
9	4,2,0,E,6,B,D,7,C,A,9,F,1,5,3,8	16384	2048	**816**	800	784	880
10	6,1,7,F,C,4,5,D,0,E,8,2,A,3,B,9	24576	5248	1576	900	**814**	850

Залишається зазначити, що до аналогічних висновків ми та інші дослідники прийшли і при використанні великих шифрів. Експерименти з ними також повністю підтвердили вихідну гіпотезу про збіжність шифрів із зростанням кількості циклі до показників випадкових підстановок відповідного степені. Усі розглянуті шифри повно циклової довжини незалежно від S-блоків (за виключенням шифру DES) приходять до стану випадкової підстановки! Отже гарні лінійні перетворення (з високим значенням коефіцієнта розгалуження) нівелює різницю між S-блоками.

Усі відомі конструкції S-блоків, що використані в шифрах, показують практично однакові значення показника ефективності (числа циклів виходу до стаціонарного стану).

В цілому ж, якщо говорити про асимптотичні значення максимумів диференціалів і лінійних корпусів шифрів при повному наборі шифруючих перетворень, що визначають за сучасними мірками показники їх доказовою стійкості, то для практично всіх відомих шифрів вони не залежать від властивостей, застосованих у шифрах S-блокових конструкцій. Цей факт призводить до важливого для криптографії висновку, що займатися пошуком S-блокових конструкцій із поліпшеними криптографічними показниками для шифрів з сильним лінійним перетворенням є неперспективною задачею. Цей напрямок, що інтенсивно розвивається в криптографії, не має скільки-небудь істотних продовжень. Для шифрів зі слабким лінійним перетворенням задача пошуку більш досконалих S-блокових конструкцій для напівбайтових S-блоків розв’язана методом прямого перебору, тобто тут задача пошуку S-блоків з поліпшеними криптографічними показниками також повністю розв’язана.

Водночас, S-блоки є необхідним і суттєвим елементом ефективного шифрувального перетворення, що виконує одну з головних функцій процедури зашифрування – нелінійного переплутування бітових виходів, при цьому основне значення має властивість хаотичності нелінійного перетворення, яке проявляється в тому, що здійснюється масова значною мірою випадкова зміна бітових позицій на його виході. При послідовному виконанні декількох таких перетворень практично незалежно від конкретного характеру нелінійного перетворення (нетривіального типу) відбувається статистичне урівноваження вихідних ефектів від впливу кожного з бітів входу, що і призводить до результуючого однорідного (стаціонарного) розподілу для кожного переходу вхідної різниці у вихідну різницю.

Окремо можна відзначити важливу роль нелінійних підстановних перетворень у формуванні механізму випадкового перемішування. Вони (S-блоки) самі є джерелом хаотичної перестановки бітів вхідного блоку даних. І без введення випадкової компоненти, що задається цикловими підключами, добуток підстановних перетворень (навіть однотипних) призводить до результуючого підстановного перетворення випадкового типу (закони розподілу переходів XOR таблиць і зміщень таблиць лінійних апроксимацій

повторюють відповідні закони розподілів випадкової підстановки) незалежно від виду вихідного підстановного перетворення (не тривіального типу). Саме на основі цього механізму (можна сказати закону природи) здійснюється перехід будь-якого шифру із зростанням кількості циклів до стаціонарного стану, після досягнення якого подальше збільшення кількості циклів не призводить до зміни показників його стійкості.

Отже у розділі набув подальшого розвитку метод оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу. Зокрема, виконано додаткове обґрунтування положення, яке полягає в тому, що показники стійкості БСШ (виключаючи DES) не залежать від використаних у шифрах S-блоків, а визначаються показниками випадкових підстановок відповідної степені.

Отже у розділі отримала подальший розвиток методологія оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу. Зокрема, виконано додаткове обґрунтування положення, яке складається в тому, що показники стійкості БСШ (виключаючи DES) не залежать від використаних у шифрах S-блоків, а визначаються показниками випадкових підстановок відповідної степені.

Додатним науковим результатом розділу э запропонований новий метод оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів, пов’язаний з оцінкою ефективності криптографічного перетворення в цілому.

У п’ятому розділі ставиться задача підтвердити положення про те, що S-блоки для блокових симетричних шифрів з гарними криптографічними показниками можна брати на основі випадкового відбору. Вона розв’язується на прикладі відбору підстановок (випадкових S-блоків) для відомого світового лідера – шифру Rijndael і шифрів, представлених на минулому українському конкурсі за вибором претендента на національний стандарт шифрування. У розділі виконаний пошук випадкових S-блоків для шифрів Rijndael, Калина, Мухомор, Лабіринт. Основою методики виконання досліджень є визначення поциклових значень максимумів 16-бітних різниць (повних диференціалів) і 16-бітних значень максимумів зміщень лінійних оболонок для сегментів блоків даних на входах та виходах повномасштабних шифрів з різними конструкціями S-блоків з подальшим порівнянням між собою цих рішень за кількістю циклів, необхідних для приходу кожного з шифрів до показників випадкової підстановки, і на основі порівняльної оцінки показників цих усічених таблиць приймається рішення про переваги того чи іншого варіанта побудови шифру, а значить і S-блоків, використаних у ньому. Результати ілюструються численними табличними даними. Приклад однієї з таких таблиць наведений нижче (див. табл. 4). Нагадаємо тут, що в шифрі Калина використовується вісім різних підстановок.

Таблиця 4 – Поциклові значення максимумів таблиць диференціальних різниць для восьми стандартних підстановок шифру Калина

Число циклів	Стандартні підстановки	Випадкові підстановки (середнє значення для 10 ключів зашифрування)
1	1370	1638,4
2	18	25
3	18	19,6
4	20	18,6
5	20	18,8
6	20	19,4
7	18	18,6
8	18	19
9	18	19,2
10	20	19,6

Таким чином, дослідженнями розділу набула подальшого розвитку методика побудови (відбору) S-блоків з поліпшеними криптографічними показниками, що відрізняється від відомих використанням для відбору S-блоків нового показника криптографічної придатності у вигляді кількості циклів, після якого шифр стає випадковою підстановкою. Це дозволяє відібрати S-блоки, які забезпечують найкращі динамічні показники ефективності шифрів. Зокрема встановлено, що як S-блоки, які дозволяють виконати ефективне шифрувальне перетворення, можуть виступати S-блоки, обрані випадковим чином.

Одночасно для оцінки ефективності шифруючих перетворень запропонований новий показник у вигляді кількості циклів, необхідних шифру для переходу до асимптотичного стану, що властивий випадковій підстановці.

ВИСНОВКИ

У результаті виконання досліджень у рамках дисертаційної роботи розв’язано важливу науково-технічну задачу, яка має практичне значення для вдосконалення технологій блокового симетричного шифрування і полягає в обґрунтуванні нового методу визначення показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу в частині підтвердження основного положення нового методу про те, що показники стійкості шифрів не залежать від властивостей S-блоків, які входять до шифрів, а визначаються показниками випадкових підстановок відповідного степеня.

Отримані результати носять самостійне значення. Проведені дослідження дозволяють зробити такі висновки:

1. Набув подальшого розвитку метод оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, який на відміну від існуючих ґрунтується на використанні показників стійкості зменшених моделей, що дозволяє, виходячи зі встановленої властивості шифрів асимптотично ставати випадковими підстановками, визначати показники стійкості великих шифрів з розрахункових співвідношень, виведених для випадкових підстановок. Зокрема, результатами роботи підтверджена працездатність нового методу прискореної оцінки показників доказової стійкості БСШ до атак лінійного та диференціального криптоаналізу. Мова йде про те, що реальні показники стійкості бокових симетричних шифрів можуть бути отримані в реальні часові терміни, чого не дозволяють існуючі методики.

Отримано додаткові аргументи та свідоцтва, які підтверджують, що всі ітеративні шифри після декількох початкових циклів зашифрування стають випадковими підстановками. Це означає, що криптографічні властивості шифрів (крім шифру DES) не залежать від використаних у шифрах S-блоків.

2. Набув подальшого розвитку метод оцінки показників випадковості підстановних перетворень, що відрізняється від відомих введенням додаткових критеріїв відбору, побудованих на основі оцінки близькості інтегральних емпіричних законів розподілу ймовірностей переходів таблиць XOR різниць і зсувів таблиць лінійних апроксимацій відповідним теоретичним законам, отриманим для випадкових підстановок, що дозволило виконати відбір підстановок досконалого типу (досконалими названі підстановки, що пройшли найжорсткіші критерії відбору). Встановлено, що можливість породження досконалих підстановок істотно залежить від їх степеня. Породження підстановок степеня більшого 256 стає нереальним для обчислення. Водночас досконалими підстановками асимптотично є всі ітеративні шифрувальні перетворення. Запропоновано уточнені критерії випадковості, побудовані на основі використання властивостей вибірки випадкових підстановок. Встановлено, що з дуже великою ймовірністю вибірка випадкових підстановок має значення максимумів диференціальних таблиць і значення максимумів зміщень таблиць лінійних апроксимацій зосереджені в істотно обмеженій області можливих значень. Всі вони концентруються навколо теоретичних значень максимумів таблиць випадкових підстановок відповідних степенів.

3. Набула подальшого розвитку методика побудови (відбору) S-блоків з покращеними криптографічними показниками, що відрізняється від відомих використанням для відбору S-блоків нового показника криптографічної придатності у вигляді кількості циклів, після якого шифр стає випадковою підстановкою, що дозволяє відібрати S-блоки, які забезпечують найкращі динамічні показники ефективності шифрів. Зокрема встановлено, що як S-блоки, що дозволяють виконати ефективне шифрувальне перетворення, можуть виступати S-блоки, обрані випадковим чином. Це означає, що задача

пошуку конструкцій досконалих S-блоків, якій приділяється величезна увага в сучасній літературі, втратила практичний сенс.

4. Розроблено та обґрунтовано новий показник ефективності шифруючих перетворень у вигляді кількості циклів, необхідних шифру для переходу до асимптотичного стану, властивому випадковій підстановці. Встановлено, що всі сучасні ітеративні шифри з сильним лінійним перетворенням (з байтовими підстановками) стають випадковими підстановками після 3–4 циклів. Для шифрів зі слабким лінійним перетворенням (з напівбайтовими підстановками) процес приходу шифрів до стаціонарного стану може затягуватись до 9–10 циклів.

5. Запропонований новий метод оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів, пов’язаний з оцінкою ефективності криптографічного перетворення в цілому. Ті підстановки рахуються більш придатними, з якими шифр приходить до стану випадкової підстановки за меншу кількість циклів.

Достовірність отриманих наукових результатів підтверджується збігом результатів експериментальних даних статистичних експериментів та іспитів малих і великих версій шифрів із розрахунковими, що випливають з теоретичних співвідношень, а також їх несуперечливістю з відомими результатами криптоаналізу БСШ, математичної теорії підстановок, теорії ймовірностей та математичної статистики.

Практична значущість отриманих результатів бачиться в тому, що:

1. Результатами роботи повністю підтверджена справедливість і працездатність нового методу оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу і її основного положення про незалежність показників стійкості шифрів від використаних у шифрах S-блоків.

2. Зроблено висновок про практичну недоцільність застосування алгебраїчних методів оцінки властивостей булевих функцій для виконання реальних оцінок криптографічних показників S-блоків. Диференціальні та лінійні властивості підстановок можуть бути визначені і без залучення апарату булевої алгебри.

3. Запропоновано підстановні конструкції випадкового типу для застосування в існуючих і перспективних шифрах.

4. Встановлено що шифри Калина, Мухомор і Лабіринт, представлені на український конкурс, є більш досконалими, ніж шифр Rijndael. Вони мають перевагу на 1–2 цикли в динаміці переходу до стаціонарного стану, властивому випадковій підстановці відповідної степені.

Результати дисертаційного дослідження можуть бути використані:

- в організаціях, що займаються проектуванням і конструюванням засобів захисту інформації для уточнення показників вже експлуатованих алгоритмів шифрування, а також при проектуванні і розробці нових конструкцій БСШ;

- в організаціях, що займаються експертизою та оцінкою проектних і конструкторських рішень з побудови сучасних БСШ, в тому числі комісіями при проведенні конкурсів з відбору перспективних рішень.

Основні результати роботи вже використано ЗАТ ″Інститут Інформаційних Технологій″, а також у навчальному процесі в Харківському національному інституті радіоелектроніки.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Лисицкая И.В. Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и смещений таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Научно-технический журнал “Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности”. – Х., 2010. – Том 9. – № 3. – С. 341 – 345.

2. Лисицкая И.В. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / И.В. Лисицкая, К.Е. Лисицкий, А.В. Широков, Е.Д. Мельничук // Науково-технічний журнал “Радіоелектронні та комп’ютерні системи”. – Х., 2010. – Вип. 2(18). – С. 87 – 93.

3. Долгов В.И. Исследование показателей случайности блочного шифра из Белорусского стандарта СТБ 34.101.31-2011 / В.И. Долгов, Р.В. Олейников, И.В. Лисицкая, А.А. Настенко, Е.Д. Мельничук, К.Е. Лисицкий // Збірник наукових праць “Спеціальні телекомунікаційні системи та захист інформації”. – К., 2012. – Вип. 2 (22). – С. 38 – 52.

4. 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.

5. Долгов В.И. Подстановочные конструкции современных симметричных блочных шифров / В.И. Долгов, Р.В. Олейников, И.В. Лисицкая, Р.В. Сергиенко, Е.В. Дроботько, Е.Д. Мельничук // Научно-технический журнал “Радиоэлектронные и компьютерные системы”. – Х., 2009. – Вып. 6(40) , – С. 121 – 133.

6. Lisitskaya I.V. Importance of S-Blocks in Modern Block Ciphers. / I.V. Lisitskaya, E.D. Melnichuk, K.E. Lysytskiy // Internet Journal “Computer Network and Information Security”. – Delhi., – 2012., – Vol. 10, P. 1 – 12.

7. Лисицкая И.В. Экспериментальные исследования критериев отбора подстановок по критериям близости эмпирических законов распределения вероятностей XOR таблиц и таблиц линейных аппроксимаций теоретическим / И.В. Лисицкая, Е.Д Мельничук, А.В. Широков // Материалы XIII Международной научно-практической конференции ″Безопасность информации в информационно-телекоммуникационных системах″. – Киев, 2010. – С. 49 – 50.

8. Лисицкая И.В. Анализ усовершенствований шифра Rijndael / И.В. Лисицкая, А.В. Казимиров, Е.Д. Мельничук, А.В. Широков, А.В. Обухов // Материалы XIII Международной научно-практической конференции ″Безопасность информации в информационно-телекоммуникационных системах″. – Киев, 2010. – С. 42.

9. Лисицкая И.В. Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и таблиц линейных аппроксимаций / И.В. Лисицкая, Е.Д. Мельничук, А.В. Широков // Материалы XIII Международной научно-практической конференции ″Безопасность информации в информационно-телекоммуникационных системах″. – Киев, 2010. – С. 43 – 44.

10. Мельничук Е.Д. Вдосконалення обчислювальних методів відбору випадкових підстановок / Е.Д. Мельничук // Материалы XV Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». – Харьков, 2011. – С. 213 – 214.

11. Лисицкая И.В. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / И.В. Лисицкая, К.Е. Лисицкий, А.В. Широков, Е.Д. Мельничук // Материалы V Международного научно-технической конференции «Гарантоспособные (надежные и безопасные) системы, сервисы и технологии». – Кировоград, 2010. – С. 87 – 93.

АНОТАЦІЯ

Мельничук Є.Д. Методи оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів.– На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Харківський національний університет радіоелектроніки МОН України, Харків, 2013.

Дисертаційна робота присвячена додатковому обґрунтуванню одного з центральних положень нового методу, який полягає в тому, що показники стійкості сучасних шифрів на відміну від існуючих підходів від властивостей застосованих S-блоків практично не залежать.

У роботі виконано комплекс досліджень з малими та повномасштабними моделями шифрів, зокрема досліджень диференціальних та лінійних показників шифрів при застосуванні в них різних, у тому числі й випадкових S-блоків, що ґрунтовно свідчать про справедливість вихідного положення.

Запропоновано та випробувано для застосування в сучасних шифрах (Rijndael, Калина, Мухомор, Лабіринт) S-блоки випадкового типу, які не знижують показників стійкості цих шифрів до атак диференціального і лінійного криптоаналізу.

В процесі досліджень обґрунтована вдосконалена модель випадкової підстановки, яка будується на основі використання відомих та додатково введених критеріїв відбору. Зокрема, встановлено що підстановки що пройшли

ці критерії (за інверсіями, зростаннями і циклами, а також додаткові критерії з використанням показників близькості законів розподілу переходів XOR таблиць та зміщень таблиць лінійних апроксимацій не є суттєво конструктивними для відбору підстановок з покращеними властивостями.

У якості практичної доцільності підходу відбору випадкових підстановок сформульовано та теоретично обґрунтовано метод що ґрунтується на використанні властивостей вибірки випадкових підстановок який є узагальненням додатково введених критеріїв то дозволяє з високою ймовірністю отримувати підстановки, для яких значення максимумів диференціальних таблиць й максимумів зміщень таблиць лінійних апроксимацій співпадають з теоретичними значеннями максимумів таблиць випадкових підстановок.

Ключові слова: блоковий симетричний шифр, диференціальний криптоаналіз, лінійний криптоаналіз, доказова стійкість, максимальна диференціальна ймовірність.

АННОТАЦИЯ

Мельничук Е.Д. Методы оценки криптографической пригодности узлов нелинейных замен блочных симметричных шифров. – На правах рукописи.

Диссертация на соискание учёной степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Харьковский национальный университет радиоэлектроники МОН Украины, Харьков, 2013.

Интересы работы сосредотачиваются на дополнительном обосновании одного из центральных положений новой методологии, состоящего в том, что показатели стойкости современных шифров в отличие от существующих подходов от свойств применяемых S-блоков практически не зависят. Речь идет о более полном изучении и исследовании вопросов оценки криптографической пригодности блоков нелинейных замен (S-блоков) современных шифров, глубокого и целевого изучения роли и места S-блоков, и, в частности случайных S-блоков в обеспечении стойкости шифров к атакам дифференциального и линейного криптоанализа.

В процессе обоснования основных положений проведен большой комплекс теоретических и экспериментальных исследований показателей случайности современных блочных симметричных шифров и случайных подстановок, в частности:

- разработаны уменьшенные модели большого числа блочных симметричных шифров, в том числе и шифров, представленных на украинский конкурс по отбору претендента на национальный стандарт блочного симметричного шифрования и шифра из нового белорусского стандарта;

- предложена новая модель случайной подстановки, которая построена на свойствах выборки случайных подстановок с выхода генератора подстановок, которая в отличие от существующих подходов может использовать сравнение значений максимумов эмпирических законов распределения переходов диффе-

ренциальных таблиц и смещений таблиц линейных аппроксимаций подстановок с теоретическими, что открыло возможность в качестве случайных (байтовых) подстановок использовать непосредственно подстановки, сформированные генератором случайных подстановок.

- исследованы линейные и дифференциальные свойства уменьшенных моделей шифров, в том числе универсальных моделей шифров со слабым линейным преобразованием и шифров с сильным линейным преобразованием, результатами которых подтверждена независимость показателей стойкости шифров от свойств используемых в них S-блоков;

- предложены и опробованы для применения в современных шифрах Rijndael, Калина, Мухомор, Лабиринт S-блоки случайного типа, не снижающие показателей стойкости этих шифров к атакам дифференциального и линейного криптаонализа;

Ключевые слова: блочный симметричный шифр, дифференциальный криптоанализ, линейный криптоанализ, доказуемая стойкость, максимальная дифференциальная вероятность, максимальная линейная вероятность, случайная подстановка, закон распределения переходов XOR таблицы подстановки, закон распределения смещений линейной аппроксимационной таблицы подстановки.

ABSTRACT

Melnichuk E.D. Cryptographic suitability assessing methods for substitution units of symmetric block ciphers. – The manuscript.

Thesis for a Ph.D. science degree by specialty 05.13.21 - information security systems. - Kharkiv National University of Radioelectronics of the MESYouthsport of Ukraine, Kharkiv, 2013.

The thesis is devoted to additional justification of one of the central positions of the new method that in contrast to existing approaches is based on the following idea: the stability indices of modern ciphers do not depend on the properties of used S-blocks.

The thesis represents a complex of research with small and full-scale cipher models, in particular the study of differential and linear parameters for ciphers using different types of substitutions, including random S-boxes. The research results indicate the validity of the original point.

Keywords: the block symmetric cipher, differential cryptanalysis, linear cryptanalysis, provable security, the maximum differential probabilities.