Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

КАЙДАЛОВ ДМИТРО СЕРГІЙОВИЧ

УДК 681.3.06

МЕТОДИ АНАЛІЗУ ВЛАСТИВОСТЕЙ ВИСОКОРІВНЕВИХ КОНСТРУКЦІЙ ТА СХЕМ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

05.13.21 – системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2016

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

Науковий керівник: доктор технічних наук, доцент **Олійников Роман Васильович**, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій.

Офіційні опоненти: доктор технічних наук, професор **Олексійчук Антон Миколайович,** Державний заклад «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», професор спеціальної кафедри №1;

кандидат технічних наук, доцент **Петренко Ольга Євгенівна,** Харківський навчально-науковий інститут Державного вищого навчального закладу «Університет банківської справи», доцент кафедри вищої математики.

Захист відбудеться 1 березня 2016 року о 14:00 годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Науки, 14.

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

Автореферат розісланий 27 січня 2016 р.

Вчений секретар
спеціалізованої вченої ради Т.В. Носова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У сучасному інформаційному суспільстві системи захисту інформації відіграють надзвичайно важливу роль. Криптографічні алгоритми застосовуються практично при кожній транзакції в інформаційних системах. Одним із основних криптографічних примітивів є блоковий симетричний шифр (БСШ), який історично з'явився першим та на сьогодні є найбільш розповсюдженим криптографічним перетворенням нарівні з асиметричними алгоритмами. За допомогою БСШ можна вирішувати такі задачі: шифрування даних (забезпечення конфіденційності), формування ґеш-кодів (забезпечення цілісності), генерування псевдовипадкових чисел та ін. Основною перевагою блокових шифрів, безумовно, є швидкість виконання операцій, що робить їх незамінними при організації високошвидкісних каналів зв'язку.

Основою будь-якого БСШ є його високорівнева конструкція, яка визначає загальну модель побудови шифру. Більшість сучасних блокових шифрів побудовані на основі ланцюга Фейстеля, схеми Лей-Месі або SPN-структури (substitution-permutation network). Проте, незважаючи на таку популярність блокових шифрів, не так багато досліджень присвячено оцінці впливу високорівневих конструкцій на їх стійкість. У зв'язку з цим, в ході проектування нових алгоритмів розробники не мають достатньої кількості об'єктивних оцінок для відбору високорівневої конструкції. Тому виникає запитання про створення критеріїв кількісної оцінки ефективності тієї чи іншої конструкції.

Іншим важливим напрямком досліджень є оцінка захищеності сучасних блокових шифрів проти атак на зв'язаних ключах. Цей напрямок мав особливу важливість під час розробки в Україні нового національного стандарту блокового симетричного шифрування. Оскільки новий алгоритм має конструкцію, схожу до алгоритму AES, який є вразливим до подібних атак, то стала актуальною задача оцінки його захищеності.

Вищеописане визначає актуальність теми дисертаційної роботи, яка спрямована на удосконалення існуючих методів оцінки стійкості блокових симетричних шифрів, заснованих на оцінці ймовірності розрізнення високорівневих конструкцій із випадковою функцією та пошуку диференційних характеристик для повноциклових версій шифрів. Результати роботи нададуть можливість підвищити якість експертних рішень щодо ступеня захищеності шифрів та нададуть розробникам нових шифрів додаткові кількісні оцінки існуючих базових конструкцій шифрів.

Зв'язок роботи з науковими програмами, темами. Дисертаційна робота виконувалася відповідно до планів наукових досліджень Харківського національного університету радіоелектроніки.

Автор роботи був виконавцем у НДР №275 «Аналіз стану, визначення основних напрямів розвитку, уніфікація, стандартизація, удосконалення, розробка та впровадження криптографічних систем, включаючи систему ЕЦП

на національному рівні та інфраструктури відкритих ключів на міжнародному рівні» (ДР №0113U000363).

Також результати роботи були використані під час розробки національного стандарту блокового симетричного шифрування України ДСТУ 7624:2014.

Мета та задачі дослідження. Метою дослідження є оцінка властивостей блокових симетричних шифрів на основі аналізу їх конструктивних елементів.

Науково-технічна задача дисертації складається в отриманні кількісних оцінок ефективності існуючих високорівневих конструкцій блокових шифрів, а також у доведенні стійкості розроблюваного алгоритму шифрування «Калина» до атак на зв'язаних ключах.

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

Предметом досліджень є методи оцінки показників ефективності та захищеності блокових симетричних шифрів.

Методи досліджень: теорія ймовірностей, математична статистика, методи системного аналізу, методи статистичних випробувань.

Методи теорії ймовірностей та математичної статистики використовувались при теоретичному доведенні низки теорем відносно алгоритмів розрізнення та знаходження максимально можливих ймовірностей розрізнення високорівневої конструкції та випадкової функції.

Методи статистичних випробувань використовувались під час проведення експериментальних випробувань щодо застосування розроблених алгоритмів-розрізнювачів.

Методи системного аналізу використовувались під час розробки та обґрунтування методу оцінки захищеності шифру проти атак на зв'язаних ключах на основі пошуку найкращої диференційної характеристики.

Для досягнення поставленої мети в роботі сформульовано такі *основні задачі:*

1. Удосконалення методу оцінки ймовірності розрізнення блокового шифру на основі ланцюга Фейстеля та випадкової функції. Розробка нових алгоритмів-розрізнювачів для три- та чотираундових варіантів цієї конструкції.

2. Дослідження властивостей схеми Лей-Месі, розробка та обґрунтування ефективності алгоритмів-розрізнювачів для різних варіантів цієї конструкції.

3. Дослідження властивостей SPN-структури. Застосування методу оцінки, заснованого на розрізненні даної конструкції від випадкової перестановки. Розробка нового алгоритму розрізнення для SPN-структури.

4. Розробка методу порівняльної оцінки трьох конструкцій блокових шифрів: ланцюга Фейстеля, схеми Лей-Месі та SPN-структури, з вибором та обґрунтуванням найбільш ефективної.

5. Розробка методу оцінки захищеності SPN-подібного шифру проти атаки на зв'язаних ключах. Застосування методу до розроблюваного алгоритму шифрування Калина (який на момент оформлення дисертації був прийнятий як

стандарт ДСТУ 7624:2014) та доведення його стійкості до розглянутого методу криптоаналізу.

Наукова новизна отриманих результатів дисертаційної роботи. У результаті виконання досліджень у рамках дисертаційної роботи вирішено важливе науково-технічне завдання, що має практичне значення для удосконалення технологій блокового симетричного шифрування. Це завдання полягало в оцінці ефективності основних високорівневих конструкцій блокових шифрів, а також у розробці методу оцінки стійкості SPN-подібного шифру проти атак на зв'язаних ключах.

Під час виконання дисертаційного дослідження отримано такі нові наукові результати:

1. Отримав подальший розвиток метод оцінки максимальної ймовірності розрізнення блокового шифру на основі ланцюга Фейстеля та випадкової функції, який відрізняється від існуючого відмовою від низки допущень о неможливості колізій усередині циклового перетворення, що дозволяє отримати точне значення ймовірності розрізнення блокового шифру та випадкової функції.

2. Вперше запропонований метод розрізнення блокового шифру на основі трираундового ланцюга Фейстеля з випадковими перестановками у якості раундових перетворень, що дозволяє отримати додаткову кількісну оцінку ефективності цієї конструкції.

3. Вперше запропонований метод розрізнення блокового шифру на основі трираундової схеми Лей-Месі та випадкової функції (випадкової перестановки), що дозволяє отримати кількісну оцінку ефективності цього перетворення як високорівневої конструкції блокового шифру.

4. Отримав подальший розвиток метод оцінки ймовірності розрізнення SPN-структури та випадкової перестановки, що відрізняється від існуючих застосуванням узагальненої моделі компонентних блоків раундового перетворення як випадкових перестановок відповідного ступеня, що дозволяє отримати кількісні оцінки ефективності цієї конструкції.

5. Отримав подальший розвиток метод порівняння трьох основних високорівневих конструкцій блокових шифрів (ланцюг Фестеля, схема Лей-Месі та SPN-структура) по критерію розрізнюваності від випадкової функції/перестановки, який відрізняється від існуючих застосуванням узагальнених показників ефективності, що дозволяє отримати точний порівняльний аналіз трьох конструкцій.

6. Вперше запропонований метод автоматизованого пошуку диференційних характеристик для блокових шифрів на основі SPN-структури на основі обчислення виключно кількості активних байтів у стані шифруючого перетворення, що дозволяє виконати обґрунтування практичної стійкості до атак на зв'язаних ключах.

Практичне значення отриманих результатів полягає у тому, що:

1. На основі розроблених теоретичних моделей було отримано кількісні оцінки ефективності розрізнення ланцюга Фейстеля. За допомогою

розробленого програмного забезпечення були реалізовані алгоритми-розрізнювачі, які також дозволили отримати кількісні оцінки ефективності розрізнення три- та чотирираундової конструкції.

2. Розроблене програмне забезпечення дозволило отримати кількісні оцінки ефективності трираундової схеми Лей-Месі. Також практичні експерименти підтвердили обґрунтованість теоретичних результатів.

3. Отримані кількісні оцінки ефективності SPN-структури, що дозволило порівняти її з іншими високорівневими коснтрукціями та зробити висновок відносно найбільш ефективної з них. Отримані результати можуть бути використані при проектуванні нових алгоритмів шифрування даних, оскільки на даний момент розробники не мають достатньої кількості об'єктивних оцінок.

4. Розроблений метод пошуку найкращих диференційних характеристик дозволив оцінити стійкість алгоритму шифрування Калина до атаки на зв'язаних ключах. Було встановлено, що кількість активних байтів у найкращій диференційній характеристиці не виходить за рамки теоретично розрахованої межі, що дозволяє стверджувати о стійкісті алгоритму Калина до подібних атак.

Обґрунтованість і достовірність наукових положень дисертації підтверджується:

– коректністю застосування математичного апарату;

– несуперечністю з існуючою теорією ймовірностей та математичної статистики;

– збігом теоретично отриманих результатів з багатьма обчислювальними експериментами;

– несуперечністю з існуючими результатами у досліджуваній області криптографії.

Отримано акти впровадження результатів досліджень у діяльність Приватного акціонерного товариства «Інститут інформаційних технологій» (від 07.09.2015 р.) та у навчальний процес у Харківському національному університеті радіоелектроніки (від 24.08.2015 р.).

Особистий внесок здобувача. Дисертація є результатом самостійної роботи автора. У роботах, які написані у співавторстві, автору належить: в [1] – постановка обчислювальних експериментів і статистична обробка результатів експериментальних досліджень диференційних властивостей шифру FOX; [2] – удосконалення існуючого виразу для оцінки максимально можливої ймовірності розрізнення ланцюга Фейстеля та випадкової функції, розробка двох алгоритмів-розрізнювачів для цієї конструкції; [3] – доведення теореми про максимально можливу ймовірність розрізнення схеми Лей-Месі, розробка алгоритмів-розрізнювачів для трираундової конструкції як із випадковими функціями, так і з випадковими перестановками у якості раундових перетворень; [4] – участь у розробці методу оцінки стійкості сучасного SPN-подібного блокового шифру проти атаки на зв'язаних ключах, постановка обчислювальних експериментів; [5] – обґрунтування теоретичних результатів оцінки ефективності SPN-структури, уточнення теореми про максимально можливу ймовірність розрізнення із випадковою перестановкою; [6] – розробка

методу автоматизованого пошуку кращої диференційної характеристики шляхом підрахунку кількості активних байтів на різних циклах шифрування, розробка програмного забезпечення для проведення обчислювальних експериментів, застосування розробленого методу до алгоритму шифрування Калина; [7] – аналіз стійкості нового алгоритму шифрування Калина до атак на зв'язаних ключах, розробка методу для оцінки стійкості.

Основні результати роботи використано в діяльності АТ «Інститут інформаційних технологій», а також у навчальному процесі у Харківському національному університеті радіоелектроніки. Крім того, наукові результати використано під час розробки нового національного стандарту блокового симетричного шифрування України ДСТУ 7624:2014.

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

- IV-й Всеукраїнській студентській науково-практичній конференції «Наукові дослідження молоді – вирішенню проблем європейської інтеграції», Харків, ХІБД УБД НБУ, 2011;
- XV-му Ювілейному міжнародному молодіжному форумі «Радіоелектроніка та молодь в XXI сторіччі», Харків, ХНУРЕ, 2011;
- III-й Науково-технічній конференції студентів та аспірантів «Захист інформації з обмеженим доступом та автоматизація її обробки», RISAP-2011, Київ, НАУ, 2011;
- XIV-й Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ, сан. Пуща-Озерна, 2011;
- The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 15-17 September 2011, Prague, Czech Republic;
- VI-й Міжнародній науково-практичній конференції «Наука та соціальні проблеми суспільства: інформатизація та інформаційні технології», Харків, ХНУРЕ, 2011;
- XV-й Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ, сан. Пуща-Озерна, 2012;
- XL-й Міжнародній науковій конференції «Питання оптимізації обчислень», Крим, смт. Кацивелі, 2013;
- XVI-й Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ, сан. Пуща-Озерна, 2013;
- XI-й Міжнародній науково-практичній конференції «Теоретичні та практичні аспекти побудови програмних систем», TAAPSD-2014, Київ, 2014.

Публікація результатів роботи. Основні положення та результати дисертаційної роботи викладено у семи наукових статтях у фахових виданнях з технічних наук (з них одна стаття у журналі, що входить до міжнародних наукометричних баз та одна стаття у міжнародному журналі у Словаччині), десяти матеріалах конференцій та тезах доповідей.

Структура та обсяг дисертації. Дисертація складається із вступу, шістьох розділів, висновків та переліку використаних джерел. Повний обсяг

дисертації складає 161 сторінку, що включає 49 рисунків, 4 таблиці, перелік використаних джерел, що містить 134 найменування (на 19 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 інформаційних технологій. Зазначається, що актуальність захисту інформації безперервно зростає у житті сучасного суспільства. Обґрунтовується важлива роль, яку відіграють блокові симетричні шифру у сучасних системах захисту інформації.

В ході обговорення сучасних алгоритмів блокового симетричного шифрування відзначається, що більшість із них у своїй основі мають одну з трьох високорівневих конструкцій: ланцюг Фейстеля, схему Лей-Месі чи SPN-структуру. Детально розглядається кожна із конструкцій з наданням прикладів використання у сучасних алгоритмах шифрування.

Розглядаються сучасні підходи щодо оцінки ефективності високорівневих конструкцій блокових шифрів. На сьогодні більшість досліджень присвячена оцінці стійкості до атак лінійного та диференційного криптоаналізу, при якій аналізується певний шифр, натомість небагато робіт присвячено оцінці високорівневих конструкцій. Робиться огляд існуючих досліджень за даною тематикою.

Аналізуються існуючі дослідження з аналізу ланцюга Фейстеля. Відомий метод оцінки базується на пошуку деякого алгоритма-розрізнювача, який з ненульовою ймовірністю може відрізнити таку конструкцію від випадкової функції. Роботи авторів М. Лубі та Ч. Ракофа за цією тематикою дали поштовх до цілої низки досліджень, в тому числі і для інших високорівневих конструкцій. Також зазначається, що подібного роду дослідження для SPN-структури практично відсутні, що робить цей напрямок надзвичайно важливим. Аналіз усіх трьох базових конструкцій надасть можливість провести порівняльний аналіз між ними та визначити найбільш ефективну за зазначеним критерієм.

Оскільки одним з напрямів досліджень у дисертаційній роботі є розробка методу оцінки стійкості сучасного алгоритму шифрування даних проти атак на зв'язаних ключах, то частина першого розділу присвячена розгляду існуючого стану у цьому напрямку. Дане питання набуло актуальності після знайдених атак на всесвітньо відомий алгоритм AES. Наводяться роботи Алекса Бірюкова та Дмитра Ховратовіча, які показали застосування цієї атаки до алгоритмів AES-192 та AES-256.

Цей напрямок набув надзвичайної актуальності у зв'язку з тим, що необхідно було оцінити стійкість алгоритму шифрування Калина, оскільки він

був заснований на алгоритмі AES і міг успадкувати його недоліки. На момент проведення досліджень цей алгоритм був у стадії розробки та аналізу, а до моменту оформлення дисертації став вже повноцінним стандартом блокового симетричного шифрування в Україні ДСТУ 7624:2014.

Розділ завершується формулюванням напрямків досліджень дисертаційної роботи. Наводяться конкретні задачі досліджень, які вимагають вирішення.

Другий розділ присвячується аналізу ланцюга Фейстеля. Спочатку надається опис самої конструкції та приклади її використання у блокових шифрах.

Розглядається метод оцінки ефективності, заснований на використанні алгоритма-розрізнювача. Алгоритм заснований на такій властивості: по суті, блоковий шифр реалізує визначену підмножину перестановок, кількість яких дорівнюється кількості можливих ключів шифрування. Оскільки вибір такої підмножини визначається структурою шифру і не є випадковим, то можлива побудова алгоритма-розрізнювача, який би міг визначити чи є задана перестановка випадково обраною із загальної множини, чи отриманою внаслідок дії блокового шифру.

Загалом робота алгоритма-розрізнювача описується так: на вхід подається визначена кількість пар відкритих/зашифрованих текстів, аналізуючи ці дані на виході алгоритму формується вихідне значення – «1» або «0». «1» у тому випадку, якщо вважається, що вхідні дані отримані за допомогою блокового шифру, та «0» у іншому. Відмічається, що розрізнення можливе завдяки появі колізій між вхідними та вихідними напівблоками даних. Для блокового шифру та випадкової функції ймовірності таких колізій матимуть суттєві відмінності.

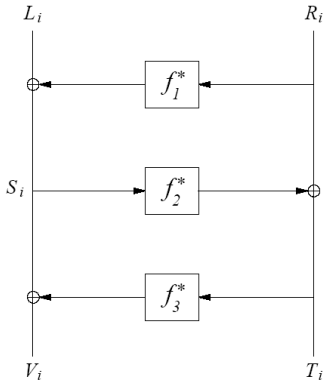


Рисунок 1 – Трираундовий ланцюг Фейстеля

У розділі розглядається існуючий вираз (1) для оцінки максимально можливої ймовірності розрізнення ланцюга Фейстеля:

$$| P[g(f(x_1),...,f(x_k)) = 1 : f \in_R \psi(F_n, F_n, F_n)] - P_g | \leq \frac{k^2}{2^n} \ , \qquad (1)$$

де $(P_g = P[g(f(x_1),...,f(x_k)) = 1 : f \in_R F_{2n}])$ – ймовірність появи «1» для випадкової функції;

$f \in_R X$ – функція заданого типу X (випадкова функція або ланцюг Фейстеля), яка обрана з усієї множини функцій подібного типу (з різними F_n);

F_n – випадкова функція із розміром вхідного/вихідного блоків даних у n бітів;

$\psi(F^n, F^n, F^n)$ – трираундовий ланцюг Фейстеля (рис. 1);

n – довжина напівблока даних (у бітах);

k – кількість вхідних аргументів ($k \geq 2$).

В ході досліджень було розроблено удосконалений вираз (2) для оцінки максимально можливої ймовірності розрізнення, який відрізняється від існуючого відмовою від низки допущень про неможливість колізій усередині циклового перетворення. Удосконалений вираз дозволяє отримати значно точнішу оцінку:

$$|P[g(f(x_1),...,f(x_k)) = 1 : f \in_R \psi(F_n, F_n, F_n)] - P_g| \leq 1 - \prod_{i=0}^{k-2}(1 - \frac{1}{2^n - i})^{2(k-(i+1))} \leq 1 - (1 - \frac{1}{2^n})^{k(k-1)}. \quad (2)$$

У тексті дисертації наводяться порівняльні графіки цих двох виразів, завдяки яким можна побачити переваги удосконаленої формули.

Загалом же, ймовірність розрізнення визначається за таким виразом:

$$Advantage(\psi, F^*) = |P_\psi - P_{F^*}|, \quad (3)$$

де P_ψ – ймовірність розрізнення алгоритмом блокового шифру;

P_{F^*} – ймовірність розрізнення алгоритмом випадкової функції (перестановки).

Наведені вище вирази (1-3) визначають лише теоретичні межі ймовірностей розрізнення. Практичні ймовірності можна отримати, побудувавши алгоритми-розрізнювачі. В існуючих публікаціях наводяться декілька алгоритмів-розрізнювачів для трираундового ланцюга Фейстеля. Вони подаються у вигляді лем у тексті дисертації. По суті такий алгоритм є деяким рівнянням між напівблоками вхідних та вихідних текстів пари аргументів.

Алгоритм-розрізнювач №1 для трираундового ланцюга Фейстеля із випадковими функціями в якості раундових перетворень. Для кожного набору з $k \geq 2$ аргументів $x_1...,x_k$ перевіряється виконання рівняння $\mathrm{L_i} \oplus V_i = \mathrm{L_j} \oplus V_j$ та $T_i = \mathrm{T_j}$ (рис. 1). Ймовірність розрізнення за допомогою цього виразу дорівнює:

$$\mathrm{Adv}(\psi, F^*) \leq |(1 - \frac{1}{2^n})^{\frac{k(k-1)}{2}} - (1 - \frac{1}{2^{2n} - 1})^{\frac{k(k-1)}{2}}|. \quad (4)$$

Такий алгоритм з приблизно $\sqrt{2^n}$ вхідними аргументами дає ймовірність розрізнення близьку до одиниці (рис. 2).

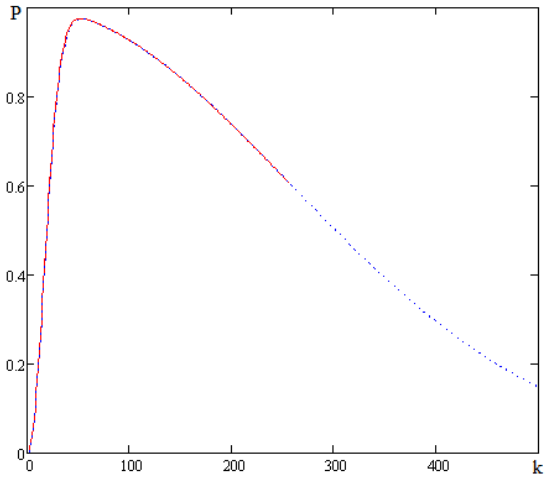


Рисунок 2 – Графік залежності ймовірності розрізнення від кількості вхідних аргументів для $n = 8$

Алгоритм-розрізнювач №2 для трираундового ланцюга Фейстеля із випадковими функціями в якості раундових перетворень. Для кожного набору з $k \geq 2$ аргументів $x_1 ..., x_k$ перевіряється виконання рівняння $\mathrm{R_i} \oplus T_i = \mathrm{R_j} \oplus T_j$ при $\mathrm{R_i} \neq \mathrm{R_j}$ та $\mathrm{L_i} = \mathrm{L_j}$ (рис. 1). Ймовірність розрізнення за допомогою цього виразу дорівнює:

$$\mathrm{Adv}(\psi, F^*) = \leq | \left(1 - \frac{1}{2^n}\right)^{2\frac{k(k-1)}{2}} - \left(1 - \frac{2^n}{2^{2n} - 1}\right)^{\frac{k(k-1)}{2}} | . \qquad (5)$$

Такий алгоритм з приблизно $\sqrt{2^n}$ вхідними аргументами дає ймовірність розрізнення близьку до 0.25.

Слід зазначити, що вирази (4,5) для розрахунку ймовірностей зазначених алгоритмів були виведені в ході досліджень. В тексті дисертації наводяться усі докази та порівняльні графіки для різних комбінацій вхідних даних.

Зазначені вище алгоритми-розрізнювачі орієнтовані на те, що як раундові перетворення використовуються випадкові функції. Якщо як раундові перетворення використовувати випадкові перестановки, то можна отримати ще кращі результати з розрізнення (до того ж такі перетворення важливі тому, що вони використовуються в ряді блокових шифрів, наприклад, в ГОСТ 28147-89). Тому під час досліджень розроблено алгоритм-розрізнювач саме для такої конфігурації.

Алгоритм-розрізнювач №3 для трираундового ланцюга Фейстеля із випадковими перестановками в якості раундових перетворень. Для кожного набору з $k \geq 2$ аргументів $x_1 ..., x_k$ перевіряється виконання рівняння $\mathrm{T_i} \neq T_\mathrm{j}$ при $\mathrm{R_i} = \mathrm{R_j}$ та $\mathrm{L_i} \neq \mathrm{L_j}$ (рис. 1). Ймовірність розрізнення за допомогою цього виразу дорівнює:

$$\mathrm{Adv}(\psi, F^*) = 1 - \prod_{i=0}^{k-2} \prod_{j=0}^{k-i-2} \left(1 - \frac{2^n - 1}{2^{2n} - 1 - j - i \cdot 2^n}\right). \qquad (6)$$

Такий алгоритм з приблизно $\sqrt{2^n}$ вхідними аргументами дає ймовірність розрізнення близьку до одиниці.

Також під час досліджень розроблено алгоритм-розрізнювач для чотирираундового ланцюга Фейстеля.

Алгоритм-розрізнювач №4 для чотирираундового ланцюга Фейстеля із випадковими функціями в якості раундових перетворень. Для кожного набору з $k \geq 2$ аргументів $x_1 ..., x_k$ перевіряється виконання рівняння $\mathrm{L_i} \oplus V_i = \mathrm{L_j} \oplus V_j$ при $\mathrm{R_i} = \mathrm{R_j}$ та $\mathrm{L_i} \neq \mathrm{L_j}$. Ймовірність розрізнення за допомогою цього виразу дорівнює:

$$\mathrm{Adv}(\psi, F^*) \leq | (1 - \frac{1}{2^n})^{2\frac{k(k-1)}{2}} - (1 - \frac{2^n}{2^{2n} - 1})^{\frac{k(k-1)}{2}} | . \quad (7)$$

Такий алгоритм з приблизно $\sqrt{2^n}$ вхідними аргументами дає ймовірність розрізнення близьку до 0.25.

Третій розділ роботи присвячений дослідженню схеми Лей-Месі. Спочатку надається опис загальної конструкції та наводяться приклади використання у сучасних блокових шифрах.

У розділі наводиться лема про максимальну вірогідність розрізнення схеми Лей-Месі та випадкової функції. На відміну від ланцюга Фейстеля, для цієї конструкції подібні дослідження у відкритій літературі відсутні. Повний доказ леми із графіками наводиться у тексті дисертації.

Лема про максимальну ймовірність розрізнення схеми Лей-Месі та випадкової функції. Максимальна ймовірність розрізнення схеми Лей-Месі (рис. 3), з кількістю раундів $r \geq 3$, та випадкової функції при k вхідних аргументів дорівнює такому значенню:

$$Adv_{\eta^*}(\varsigma, F_{2n}) \leq 1 - \left(\frac{2^n - 2}{2^n - 1} \right)^{\frac{k(k-1)}{2}} . \quad (8)$$

Зазначається, що максимальна ймовірність розрізнення (8) наближається до одиниці із збільшенням кількості k вхідних аргументів.

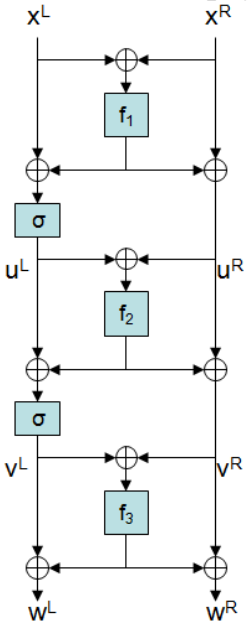


Рисунок 3 – Трираундова схема Лей-Месі

Як і для ланцюга Фейстеля, наведений вище вираз (8) визначає лише теоретичну межу ймовірності розрізнення. Практичні ймовірності можна отримати побудувавши алгоритми-розрізнювачі. В ході досліджень було розроблено два такі алгоритми для трираундової схеми Лей-Месі (рис. 3).

Алгоритм-розрізнювач для трираундової схеми Лей-Месі із випадковими функціями в якості раундових перетворень. Для кожного набору з $k \geq 2$ аргументів $x_1 ..., x_k$ перевіряється виконання рівняння $\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R) \oplus x_i^R \oplus x_j^R$ при $\sigma(x_i^L \oplus x_j^L) = x_i^R \oplus x_j^R$ та $\Delta x_i \neq \Delta x_j$ (рис. 3). Ймовірність розрізнення за допомогою цього виразу дорівнює:

$$Adv(\varsigma, F_{2n}) \leq | (1 - \frac{2^n}{2^{2n} - 1})^{\frac{k(k-1)}{2}} - (1 - \frac{2^{n+1} - 1}{2^{2n}})^{\frac{k(k-1)}{2}} | . \quad (9)$$

Такий алгоритм з приблизно $\sqrt{2^n}$ вхідними аргументами дає ймовірність розрізнення близьку до 0.25.

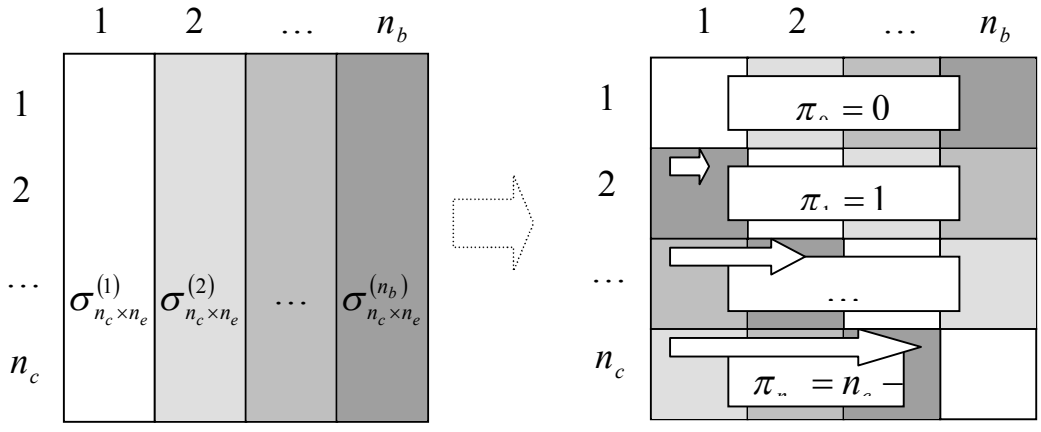
Алгоритм-розрізнювач для трираундової схеми Лей-Месі із випадковими перестановками в якості раундових перетворень. Для кожного набору з $k \geq 2$ аргументів $x_1 ..., x_k$ перевіряється виконання рівняння $\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R \oplus x_i^L \oplus x_j^L)$ при $\sigma(x_i^L \oplus x_j^L) \oplus x_i^R \oplus x_j^R \neq 0$ та $\Delta x_i \neq \Delta x_j$ (рис. 3). Ймовірність розрізнення за допомогою цього виразу дорівнює:

$$Adv(\varsigma, F_{2n}) \leq | (1 - \frac{2^n}{2^{2n} - 1})^{\frac{k(k-1)}{2}} - (1 - \frac{1}{2^n - 1})^{k(k-1)} | . \quad (10)$$

Такий алгоритм також дає ймовірність розрізнення близьку до 0.25 з приблизно $\sqrt{2^n}$ вхідними аргументами.

Четвертий розділ роботи присвячений дослідженню SPN-структури. Ця структура є однією з найбільш популярних у сучасній криптографії. Наводяться приклади її використання, зокрема, всесвітньо відомий алгоритм AES.

У розділі надається загальний опис конструкції. Зазначається, що основу перетворення складають операції перемішування (diffusion) та розсіювання (confusion). Внутрішній стан може бути поданий у вигляді матриці $n_c \times n_b$ елементів. Один цикл шифрування при $n_c = n_b$ наведений на рис. 4.



пласт перестановок пласт обміну елементів між стовпцями

Рисунок 4 – Цикл шифрування алгоритмом на базі SPN-структури

В ході досліджень було висунуто та доведено теорему про максимальну ймовірність розрізнення двоциклової SPN-структури.

Теорема (про верхню межу розрізнення двоциклової SPN-структури та випадкової перестановки на обмеженій кількості запитів). Нехай є SPN-структура з розміром блока $2n$ бітів та внутрішнім станом у вигляді матриці розміром $n_c \times n_b$ елементів, кожен з яких має розмір n_e бітів ($2n = n_c \times n_b \times n_e$). При цьому виконується умова $n_c = n_b \cdot 2l, l \in \{1,2,...\}$ та як раундові перетворення використовуються випадкові перестановки $\sigma_{\frac{2n}{n_c \cdot n_e}}$. Тоді максимальна ймовірність розрізнення двоциклової SPN-структури та випадкової перестановки σ_{2n} при k запитах ($2 \le k \le 2^{\frac{n_c \cdot n_e}{n_b}}$) на вході алгоритму-розрізнювача не перевищує такого значення:

$$Adv_{\eta^*}(\vartheta, \sigma_{2n}) = \left| P_1\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R \vartheta^{(2)}\right) - P_1^*\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R \sigma_{2n}\right) \right| \le$$

$$\le \left| 2^{-\frac{n_c \cdot n_e \cdot k \cdot (k-1)}{2}} \cdot \left(2^{\frac{n_c \cdot n_e}{n_b}} - 1 \right)^{\frac{n_b k(k-1)}{2}} - \left(1 - 2^{-\frac{n_c \cdot n_e}{n_b}} \right)^{\frac{k(k-1)(n_b-1)}{2}} \right| . \quad (11)$$

Для двоциклової SPN-структури можна побудувати такий алгоритм-розрізнювач.

Алгоритм-розрізнювач для двоциклової SPN-структури. Для k вхідних запитів (x_i, x_j), де $2 \le k \le 2^{\frac{n_c \cdot n_e}{n_b}} + 1$, виконуючих активізацію однієї перестановки: $x_i^{(t)} \ne x_j^{(t)}, x_i^{(l)} = x_j^{(l)}, 1 \le l \le n_b, l \ne t, t = const$, $x_i = \left(x_i^{(1)} \bullet x_i^{(2)} \bullet ... \bullet x_i^{(n_b)}\right)$, $x_j = \left(x_j^{(1)} \bullet x_j^{(2)} \bullet ... \bullet x_j^{(n_b)}\right)$, $1 \le i < j \le k$ перевіряється наявність колізії на виході кожної з перестановок другого циклу: $y_i^{(l)} = y_j^{(l)}, 1 \le l \le n_b$, $1 \le i < j \le k$. Якщо хоча б для одного запиту була знайдена колізія, то вихідне значення алгоритму буде дорівнюватиме одиниці, інакше нулю.

Для такого алгоритму та SPN-структури з конфігурацією $n_c = 4, n_b = 4, n_e = 8$ (яка відповідає двоцикловому AES із випадковими перестановками Super-S-box як раундові перетворення) максимальна ймовірність розрізнення дорівнюватиме близько 0.6.

Також у тексті дисертації теоретично доведено теорему про неможливість розрізнення трициклової SPN-структури. Зазначається, що побудова алгоритму-розрізнювача, який би мав ймовірність розрізнення із випадковою перестановкою більше нуля, неможлива.

П'ятий розділ присвячений порівняльному аналізу трьох розглянутих у попередніх розділах високорівневих конструкцій. Показником, за яким проводиться порівняння, є ймовірність розрізнення із випадковою функцією чи перестановкою.

Запропонований метод порівняння передбачає аналіз високорівневих конструкцій попарно. Для кожної пари складаються рівняння, які є різницею виразів для знаходження ймовірностей розрізнення тієї чи іншої конструкції.

Для порівняння ланцюга Фейстеля та схеми Лей-Месі використовується такий вираз:

$$Adv_{\eta^*}(\psi,\varsigma) = Adv_{\eta^*}(\psi, F_{2n}) - Adv_{\eta^*}(\varsigma, F_{2n}) = \left(\frac{2^n-2}{2^n-1}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{1}{2^n}\right)^{k(k-1)}. \quad (12)$$

У даному випадку порівнюються максимально можливі ймовірності розрізнення обох конструкцій. Аналогічно складаються вирази для порівняння конкретних алгоритмів-розрізнювачів. У тексті дисертації наведено усі вирази для оцінки, а також побудовано графіки для різних конфігурацій. Зазначається, що схема Лей-Месі є більш ефективною ніж ланцюг Фейстеля.

Аналогічні порівняння проводились також для SPN-структури та ланцюга Фейстеля. У даному випадку порівнювалися вирази для знаходження ймовірності алгоритмів-розрізнювачів трираундового ланцюга Фейстеля та двораундової SPN-структури:

$$Adv_{\eta p-opt}(\psi,\vartheta) = \left|1-\left(\frac{2^n}{2^n+1}\right)^{\frac{k(k-1)}{2}}\right| - \left|2^{-\frac{n_c\cdot n_e\cdot k\cdot(k-1)}{2}}\cdot\left(2^{\frac{n_c\cdot n_e}{n_b}}-1\right)^{\frac{n_b k(k-1)}{2}} - \left(1-2^{-\frac{n_c\cdot n_e}{n_b}}\right)^{\frac{k(k-1)(n_b-1)}{2}}\right|. \quad (13)$$

Навіть двораундова SPN-структура виявилась ефективнішою ніж трираундовий ланцюг Фейстеля.

Також порівнювалися між собою схема Лей-Месі та SPN-структура. Для оцінки цих двох конструкцій використовувались кращий алгоритм-розрізнювач трираундової схеми Лей-Месі та алгоритм-розрізнювач двораундової SPN-структури. Порівняльний вираз має такий вигляд:

$$Adv_{\eta p-opt}(\varsigma,\vartheta) = \left|\left(1-\frac{2^n}{2^{2n}-1}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{1}{2^n-1}\right)^{k(k-1)}\right| -$$

$$-\left|2^{-\frac{n_c\cdot n_e\cdot k\cdot(k-1)}{2}}\cdot\left(2^{\frac{n_c\cdot n_e}{n_b}}-1\right)^{\frac{n_b k(k-1)}{2}} - \left(1-2^{-\frac{n_c\cdot n_e}{n_b}}\right)^{\frac{k(k-1)(n_b-1)}{2}}\right|. \quad (14)$$

У цьому випадку трираундова схема Лей-Месі виявилась більш ефективною. Слід враховувати, що порівняння проводилось із двораундовою SPN-структурою, для якої алгоритмів-розрізнювачів для трьох і більше раундів взагалі не існує.

Саме тому, враховуючи результати усіх проведених експериментів зроблено висновок, що SPN-структура є найбільш ефективною конструкцією

для побудови блокових шифрів за критерієм розрізнення із випадковою функцією (перестановкою).

Шостий розділ присвячується розробці та аналізу методу оцінки стійкості SPN-подібного шифру проти атак на зв'язаних ключах. Робота у цьому напрямку була важливою тому, що до недавнього часу в Україні проводився конкурс на національний стандарт блокового симетричного шифрування, в ході якого був відібраний алгоритм Калина. Цей шифр побудовано на основі Rijndael-подібної SPN-конструкції, аналогічної до тої, що використовується у AES. Однак, відомо, що на AES були знайдені теоретичні атаки, тому першочерговою задачею є оцінка стійкості проти атак, до яких вразливий AES, зокрема проти атаки на зв'язаних ключах. Слід зазначити, що на момент оформлення дисертації алгоритм Калина вже був прийнятий як національний стандарт блокового симетричного шифрування України ДСТУ 7624:2014.

У розділі наводиться стислий опис алгоритму Калина. На відміну від AES він має повністю перероблену схему розгортання ключа. Всі дослідження проводилися для 128-бітної версії шифру. Така конфігурація подається у вигляді матриці із двох стовпців та восьми рядків байтових елементів.

У тексті дисертаційної роботи надається опис атаки на зв'язаних ключах із прикладом. Загальна сутність атаки полягає в тому, що підбираючи деякі різниці для пари вхідних текстів на вході шифруючого перетворення знайти колізії у внутрішньому стані перетворення, які б нівелювали розповсюдження вхідної різниці.

Запропонований метод оцінки стійкості базується на пошуку найкращої диференційної характеристики та підрахунку кількості активних байтів, задіяних у ході її побудови. Активним є такий байт, який, маючи ненульове значення різниці, проходить через таблицю підстановки. Краща диференційна характеристика знаходиться шляхом повного автоматизованого перебору для всіх можливих різниць ключа та вхідних текстів.

Перебір усіх можливих характеристик для повної версії шифру є надзвичайно складною задачею, тому під час досліджень був розроблений алгоритм, який значно зменшує складність такого перебору. Його сутність в тому, що в ході побудови диференційної характеристики для певних вхідних різниць ключа та текстів, контролюються не конкретні значення різниці та позиції активних байтів, а лише їх кількість у стовпчику стану шифру. Це значно скоротить складність обчислень та дозволить знайти потрібну характеристику за прийнятний час.

Для цього для кожної операції шифруючого перетворення (підстановка байтів, перемішування у стовпцях, зсув рядків і додавання ключа) були обґрунтовані припущення щодо розповсюдження байтів. Точність отриманих подібним шляхом результатів може погіршитися в тому плані, що можуть з'явитися характеристики, які в дійсності відтворити неможливо. Такі характеристики можуть мати лише меншу кількість активних байтів, ніж реальні. Однак головною властивістю алгоритму є те, що він ніколи не видасть

найкращу характеристику, яка б мала кількість активних байтів більше, ніж може бути насправді. Таким чином, можна стверджувати, що він знаходить мінімальну межу активних байтів для будь-якої реальної диференційної характеристики. Якщо така кількість не перевищує встановленої межі, то можна стверджувати, що шифр є стійким проти атак на зв'язаних ключах.

Для алгоритму шифрування Калина теоретично розрахованою межею є 26 активних байтів. Це значення випливає з того факту, що кожен активний байт вносить невизначеність 2^{-5} на виході таблиць підстановок 5 в 5 байтів, які використовуються в Калині. Тоді, якщо складність прямого перебору 128-бітної версії шифру складає 2^{128} операцій, то маємо такий вираз для розрахунку безпечної межі кількості активних байтів: $(2^{-5})^x > 2^{-128}$. Тобто з кількістю активних байтів $x \geq 26$ складність атаки на зв'язаних ключах перевищуватиме складність прямого перебору, що означає стійкість шифру.

На рис. 5 наведений приклад роботи алгоритму для трьох раундів формування проміжного значення K_t у схемі розгортання ключа.

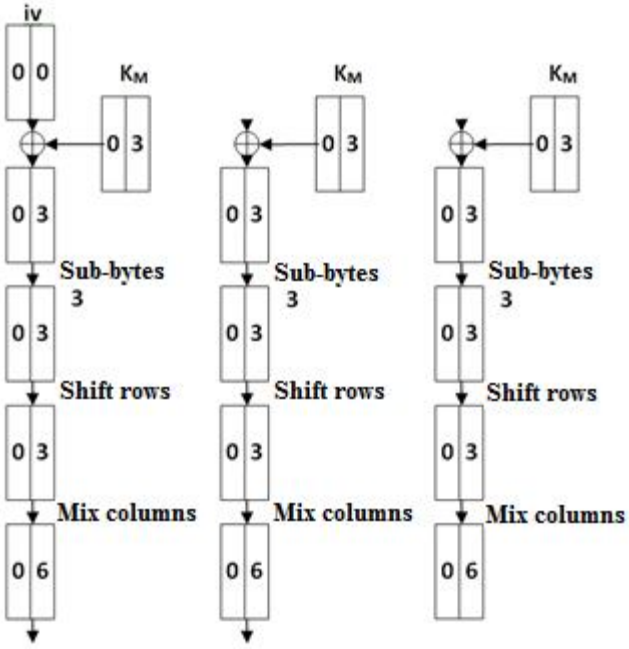


Рисунок 5 – Розрахунок активних байтів при формуванні значення K_t

Застосувавши алгоритм пошуку до шифру Калина було встановлено, що найкраща диференційна характеристика має 27 активних байтів і не перевищує встановленої межі у 26 активних байтів. Тобто даний алгоритм можна вважати стійким проти атак на зв'язаних ключах.

Також у розділі обґрунтовується обчислювальна складність такого методу. Зазначається, що на комп'ютері з чотириядерним процесором AMD Phenom з тактовою частотою 3.2 ГГц та 4 Гб оперативної пам'яті даний алгоритм повністю відпрацьовує за 10 хвилин.

ВИСНОВКИ

У результаті виконання досліджень у рамках дисертаційної роботи вирішено важливе науково-технічне завдання, що має практичне значення для удосконалення технологій блокового симетричного шифрування. Це завдання полягало в оцінці ефективності основних високорівневих конструкцій блокових шифрів, а також у розробці методу оцінки стійкості SPN-подібного шифру проти атак на зв’язаних ключах.

Основні висновки за результатами виконаних досліджень:

1. Запропоновано удосконалений вираз для оцінки максимально можливої ймовірності розрізнення ланцюга Фейстеля та випадкової функції. Застосування удосконаленого виразу дозволило отримати значно точнішу оцінку максимальної ймовірності розрізнення.

2. Розроблено методи розрізнення блокового шифру на основі трираундового ланцюга Фейстеля та випадкової функції. Один базується на застосування випадкової функції в якості циклового перетворення, а інший передбачає використання випадкової перестановки. Отримані результати дозволили отримати кількісну оцінку ефективності ланцюга Фейстеля.

3. Розроблено метод розрізнення блокового шифру на основі трираундового ланцюга Фейстеля та випадкової перестановки. Отриманий результат дозволив кількісно оцінити ефективність трираундового ланцюга Фейстеля із випадковими перестановками в якості циклового перетворення.

4. Запропоновано метод розрізнення блокового шифру на основі чотирираундового ланцюга Фейстеля та випадкової перестановки. В даному випадку, як циклове перетворення використовувалась випадкова функція. Отриманий результат дозволив отримати додаткову оцінку ефективності ланцюга Фейстеля.

5. Запропоновано та математично доведено вираз для розрахунку максимально можливої ймовірності розрізнення схеми Лей-Месі з кількістю раундів 3 та більше. Отриманий результат дозволив оцінити ефективність схеми Лей-Месі та порівняти її з іншими високорівневими конструкціями.

6. Розроблено два методи розрізнення блокового шифру на основі трираундової схеми Лей-Месі. Отриманий результат дозволив отримати кількісну оцінку ефективності схеми Лей-Месі.

7. Проведено оцінку ефективності SPN-структури за допомогою критерію розрізнюваності із випадковою перестановкою. Був знайдений метод розрізнення для двораундової SPN-структури, а також доведено теорему про неможливість її розрізнення з кількістю раундів три і більше. Отриманий результат дозволив оцінити ефективність SPN-структури.

8. Всі теоретичні досліди з оцінки ефективності високорівневих конструкцій були підтверджені за допомогою розробленого програмного забезпечення, яке дозволило переконатися в коректності доведених теорем.

9. Проведено порівняльний аналіз усіх трьох розглянутих високорівневих конструкцій за критерієм розрізнюваності з випадковою функцією/

перестановкою. Отриманий результат дозволив зробити висновок, що найбільш ефективною за оцінюваним критерієм є SPN-структура та саме її слід рекомендувати використовувати під час проектування нових блокових симетричних шифрів.

10. Розроблено метод автоматизованого пошуку найкращої диференційної характеристики на основі підрахунку кількості активних байтів на різних циклах шифрування. Розроблений метод дозволив оцінити стійкість алгоритму шифрування Калина до атаки на зв'язаних ключах. Було встановлено, що цей шифр є стійким проти подібного роду атак. Розроблений метод з деякими модифікаціями може бути застосований до інших шифрів на основі SPN-структури.

Результати дисертаційних досліджень можуть бути використані:

− в організаціях, які займаються проектуванням нових алгоритмів блокового симетричного шифрування для обґрунтування вибору високорівневої конструкції шифру;

− в організаціях, які займаються експертизою та оцінкою проектних рішень з побудови сучасних БСШ для оцінки захищеності шифру проти атак на зв'язаних ключах.

Основні результати роботи впроваджені в діяльність Приватного акціонерного товариства «Інститут інформаційних технологій» і в навчальний процес у Харківському національному університеті радіоелектроніки. Крім того, наукові результати використано під час розробки нового національного стандарту блокового симетричного шифрування України ДСТУ 7624:2014.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Лисицкая И.В. Дифференциальные свойства шифра FOX / И.В. Лисицкая, Д.С. Кайдалов // Прикладная радиоэлектроника. – Харьков, ХНУРЭ, 2011. – Т. 10, № 2. – С. 122–126.

2. Олейников Р.В. Уточнение эффективности различения цепи Фейстеля и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // Радиотехника. – Харьков, ХНУРЭ, 2011. – № 167. – С. 190–202.

3. Олейников Р.В. Оценка сложности различения схемы Лей-Месси и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // Прикладная радиоэлектроника. – Харьков, ХНУРЭ, 2012. – Т. 11, № 2. – С. 152–159.

4. Oliynykov R. Related-key cryptalanysis of perspective symmetric block cipher / R. Oliynykov, D. Kaidalov // Applied Radio Electronics. – Kharkiv, KNURE, 2014. – V. 13, № 3. – P. 112–120.

5. Кайдалов Д.С. Оценка эффективности SPN-структуры блочного симметричного шифра / Д.С. Кайдалов, Р.В. Олейников // Восточно-

Европейский журнал передовых технологий. – Харьков, 2014. – Т. 6/9 (72). – С. 4–10.

6. Kaidalov D. A method for security estimation of the SPN-based block cipher against related-key attacks / D. Kaidalov, R. Oliynykov, O. Kazymyrov // Tatra Mountains. – Slovakia, Bratislava, VEDA, 2014. – V. 60. – P. 25–45.

7. Горбенко І.Д. Симетричний блоковий шифр "Калина" – новий національний стандарт України / І.Д. Горбенко, Р.В. Олійников, О.В. Казимиров, В.І. Руженцев, О.О. Кузнєцов, Ю.І. Горбенко, О.В. Дирда, В.І. Долгов, А.І. Пушкарьов, Р.І. Мордвінов, Д.С. Кайдалов, В.М. Казимирова // Радиотехника. – Харьков, ХНУРЭ, 2015. – № 181. – С. 5–22.

Наукові праці апробаційного характеру:

8. Кайдалов Д.С. Различение цепи Фейстеля и случайной перестановки / Д.С. Кайдалов // Научные исследования молодежи – решению проблем европейской интергации : сб. науч. тр. XVI Междунар. науч.-практ. конф., 16 марта 2011 г. – Харьков : УБД ХИБД, 2011. – С. 25.

9. Кайдалов Д.С. Уточненная оценка верхней границы вероятности различения цепи фейстеля и случайной функции / Д.С. Кайдалов, Р.В. Олейников // Радиоэлетроника и молодежь в XXI веке : сб. науч. тр. XV Юбил. междунар. молодежного форума. – Харьков : ХНУРЭ, 2011. – С. 203–204.

10. Кайдалов Д.С. Различение цепи Фейстеля и случайной перестановки / Д.С. Кайдалов, Р.В. Олейников // Защита информации с ограниченным доступом и автоматизация ее обработки : сб. науч. тр. III Науч.-техн. конф. студентов и аспирантов, 8–9 февраля 2011 г. – Киев : НАУ, 2011. – С. 9.

11. Олейников Р.В. Особенности различения трёхраундовой цепи фейстеля и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // Безопасность информации в информационно-телекоммуникационных системах : сб. науч. тр. XIV Междунар. науч.-практ. конф., 17–20 мая 2011 г. – Киев : ГСССЗИУ, 2011. – С. 30.

12. Gorbenko I. Improvement for Distinguisher Efficiency of the 3-Round Feistel Network and a Random Permutation / I. Gorbenko, R. Oliynykov, D. Kaidalov // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : by materials of the 6th IEEE International Conference, 15–17 September 2011. – Prague, Czech Republic : IEEE, 2011. – P. 743–746.

13. Олейников Р.В. Эффективность различения случайной перестановки и цепи Фейстеля на основе биективной раундовой функции / Р.В. Олейников, Д.С. Кайдалов // Наука и социальные проблемы общества: информатизация и информационные технологии : сб. науч. тр. VI Междунар. науч.-практ. конф., 24–25 мая 2011 г. – Харьков : ХНУРЭ, 2011. – С. 258–259.

14. Олейников Р.В. Оценка сложности различения схемы Лей-Месси и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // Безопасность информации в информационно-телекоммуникационных системах : сб. науч. тр.

XV Междунар. науч.-практ. конф., 22–25 мая 2012 г. – Киев : ГСССЗИУ, 2012. – С. 61–62.

15. Олейников Р.В. Новый подход к построению схемы разворачивания ключа блочных симметричных шифров / Р.В. Олейников, Д.С. Кайдалов // Вопросы оптимизации вычислений : сб. науч. тр. XL Междунар. науч. конф., 30 сентября – 4 октября 2013 г. – Киев : ИК НАНУ, 2013. – С. 200–201.

16. Олейников Р.В. Подход к построению схемы разворачивания ключа блочных симметричных шифров / Р.В. Олейников, Д.С. Кайдалов // Безопасность информации в информационно-телекоммуникационных системах : сб. науч. тр. XVI Междунар. науч.-практ. конф., 21–24 мая 2013 г. – Киев : ГСССЗИУ, 2013. – С. 34–35.

17. Горбенко І.Д. Проект національного стандарту симетричного блокового шифрування / І.Д. Горбенко, Р.В. Олійников, В.І. Руженцев, О.В. Казимиров, О.О. Кунзнецов, Ю.І. Горбенко, О.Є. Дирда, В.І. Долгов, А.І. Пушкарьов, Р.І. Мордвинов, Д.С. Кайдалов // Теоретичні та прикладні аспекти побудови програмних систем : сб. наук. праць XI Міжнар. наук.-практ. конф., 15–17 грудня 2014 р. – Київ : КНУ, 2014. – С. 65–69.

АНОТАЦІЯ

Кайдалов Д.С. Методи аналізу властивостей високорівневих конструкцій та схем формування циклових ключів 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 Міністерства освіти і науки України, Харків, 2016.

Дисертаційна робота присвячена аналізу властивостей сучасних блокових симетричних шифрів, зокрема проводиться оцінка ефективності основних високорівневих конструкцій блокових шифрів, а також аналізується стійкість блокового шифру Калина до атак на зв’язаних ключах.

У роботі отримано оцінки ефективності трьох високорівневих конструкцій блокових шифрів: ланцюга Фейстеля, схеми Лей-Месі та SPN-структури. Встановлено, що SPN-структура є найбільш ефективною конструкцією за критерієм розрізнювання із випадковою функцією/ перестановкою.

Запропонований метод оцінки стійкості блокових шифрів на основі Rijndael-подібної SPN-конструкції до атак на зв’язаних ключах (практичний критерій). Застосування методу до алгоритму шифрування Калина показало захищеність цього перетворення до розглянутого класу атак.

Ключові слова: блоковий симетричний шифр, високорівнева конструкція, алгоритм-розрізнювач, випадкова функція, випадкова перестановка, максимальна ймовірність розрізнення, атака на зв’язаних ключах,

диференційна характеристика, схема розгортання ключа, циклове перетворення.

АННОТАЦИЯ

Кайдалов Д.С. Методы анализа свойств высокоуровневых конструкций и схем формирования цикловых ключей 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 Министерства образования и науки Украины, Харьков, 2016.

Диссертационная работа посвящена анализу свойств современных блочных симметричных шифров, в частности проводится оценка эффективности основных высокоуровневых конструкций блочных шифров, а также анализируется стойкость блочного шифра Калина к атакам на связанных ключах.

Формулируется научно-техническая задача получить количественные оценки эффективности трех высокоуровневых конструкций: цепи Фейстеля, схемы Лей-Месси и SPN-структуры. Предполагается, что такими оценками будут являться вероятности различения исследуемой конструкции со случайной функцией или перестановкой. Решение этой задачи позволит оценить базовые конструкции блочных шифров, сравнить их между собой и сделать вывод относительно наиболее эффективной.

Другая научно-техническая задача состоит в разработке метода оценки стойкости SPN-подобного шифра к атакам на связанных ключах. Решение этой задачи позволит оценить стойкость алгоритма шифрования Калина к подобного рода атакам.

В работе выполнен комплекс исследований над тремя основными высокоуровневыми конструкциями блочных шифров. Для цепи Фейстеля было разработано усовершенствованное выражение для нахождения максимальной вероятности различения со случайной функцией. Также были проанализированы существующие и найдены несколько новых алгоритмов различения со случайной функцией/перестановкой для трех- и четырехраундовой цепи Фейстеля. Для схемы Лей-Меси также было выведено и доказано выражение для нахождения максимально возможной вероятности различения. Также было разработано два алгоритма-различителя трехраундовой схемы Лей-Меси. Один из них основывается на использовании случайной функции в качестве раундового преобразования, а другой на основе случайной перестановки. Аналогичные исследования проводились и для SPN-структуры. Было разработано выражение для оценки максимально возможной вероятности различения. Представлен алгоритм-различитель для двухраундовой SPN-структуры, а также доказано, что различение для трех и более раундов является невозможным. По результатам исследований была

проведена сравнительная оценка всех трех конструкций, в результате которой было установлено, что SPN-структура является наиболее эффективной по критерию различимости со случайной функцией/перестановкой.

Был предложен метод оценки стойкости блочных шифров на основе Rijndael-подобной SPN-конструкции к атакам на связанных ключах (практический критерий). Метод основывается на автоматизированном поиске наилучших дифференциальных характеристик для полноцикловой версии шифра. Применение метода к алгоритму шифрования Калина показало защищенность этого преобразования к рассмотренному классу атак.

Ключевые слова: блочный симметричный шифр, высокоуровневая конструкция, алгоритм-различитель, случайная функция, случайная перестановка, максимальная вероятность различения, атака на связанных ключах, дифференциальная характеристика, схема разворачивания ключа, цикловое преобразования.

ABSTRACT

Kaidalov D.S. Methods for analyzing properties of high-level constructions and key-expansion schemes of block symmetric ciphers. – Manuscript.

Thesis for a Ph.D. science degree by specialty 05.13.21 – information security systems. – Kharkiv National University of Radioelectronics of the Ministry of Education and Science of Ukraine, Kharkiv, 2016.

The thesis is devoted to the analysis of properties of modern block symmetric ciphers. In particular the efficiency of basic high-level constructions for block ciphers is being analyzed. Security of block cipher Kalina against related-key attacks has also been researched.

The thesis represents a complex of researches with the main three high-level constructions: Feistel scheme, Lai-Massey scheme and SPN-structure. Research results confirm that the SPN-structure is the most efficient high-level construction according to the criteria of distinguishing with the random function.

Research on security analysis of the Kalina cipher against related-key attacks was also made. The developed method proved that this cipher is secure against such attacks.

Keyworks: symmetric block cipher, high-level construction, distinguisher alghorithm, random function, random permutation, the maximal probability of distinguishing, key-related attack, differential characteristic, key-expansion scheme, round transformation.