Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ОЛІЙНИКОВ РОМАН ВАСИЛЬОВИЧ

УДК 681.3.06:006.354

МЕТОДИ АНАЛІЗУ І СИНТЕЗУ ПЕРСПЕКТИВНИХ СИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

05.13.05 – комп’ютерні системи та компоненти

Автореферат дисертації на здобуття наукового ступеня
доктора технічних наук

Харків - 2014

Дисертацією є рукопис.

Робота виконана в Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий консультант — доктор технічних наук, професор
Горбенко Іван Дмитрович,
Харківський національний університет радіоелектроніки,
професор кафедри безпеки інформаційних технологій

Офіційні опоненти: — доктор технічних наук, професор
Корченко Олександр Григорович,
Національний авіаційний університет, МОН України,
завідувач кафедри безпеки інформаційних технологій, м. Київ

доктор технічних наук, професор
Олексійчук Антон Миколайович,
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України „Київський політехнічний інститут", МОН України,
професор спеціальної кафедри №1, м. Київ

доктор технічних наук, професор
Харченко Вячеслав Сергійович,
Національний аерокосмічний університет ім. М.Є.Жуковського «ХАІ», МОН України,
завідувач кафедри комп'ютерних систем та мереж, м. Харків

Захист відбудеться "____" _____ 2014 р. о _____ годині на засіданні спеціалізованої вченої ради Д 64.052.01 Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Леніна, 14.

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

Автореферат розісланий "____" _____ 2014 р.

Учений секретар
спеціалізованої вченої ради О.А. Винокурова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Тенденції розвитку сучасного постіндустріального суспільства демонструють необхідність подальшого інтенсивного впровадження нових інформаційних технологій. Децентралізація і віртуалізація обчислень, масове застосування безпровідних каналів зв'язку додатково збільшують існуючу критичну залежність як всього суспільства в цілому, так і його окремих інститутів від надійності та безпеки інформаційно-телекомунікаційних систем (ІТС). Зловмисне втручання в нормальну роботу життєво важливих ІТС може призвести до найважчих техногенних катастроф, значних фінансових, матеріальних та репутаційних втрат. Провідні держави світу вже створили власні стратегії ведення кібервійн, в яких інформаційний простір (кіберпростір) визначається як «операційний домен з метою максимального застосування потенціалу для отримання повної переваги».

В таких умовах забезпечення інформаційної безпеки сучасних і перспективних ІТС стає однією з найпріоритетніших задач. Тенденції широкого застосування хмарних обчислень, засобів віддаленого підключення з мобільних та віддалених стаціонарних пристроїв через цифрові мережі загального призначення призводять до «зникнення периметра» критичних систем і значного ускладнення задач забезпечення їх безпечного функціонування. Фактично, для будь-якого повідомлення, блоку даних або програмного коду, що передається між обчислювальними системами або такого, що зберігається локально, потрібне забезпечення основних послуг безпеки.

Необхідною умовою для цього є застосування систем криптографічного захисту інформації (КЗІ). Тільки в цьому випадку можливо ефективне забезпечення послуг конфіденційності та цілісності для розподілених обчислювальних систем.

Водночас засоби криптографічного захисту інформації, які існують зараз, у ряді випадків не можуть забезпечити рівень пропускної здатності, який повністю відповідає сучасним вимогам. Ця проблема може бути вирішена за допомогою декількох підходів. Крім екстенсивного, який передбачає масштабування систем КЗІ з їх ускладненням за рахунок додаткових модулів балансування навантаження, збільшення вартості та зниження надійності, існує підхід, який передбачає вдосконалення алгоритмів криптографічного перетворення, зниження їхньої обчислювальної складності при збереженні або збільшенні стійкості.

Оскільки основний обсяг інформації, що передається каналами зв'язку, захищається за допомогою симетричних криптографічних примітивів, основну увагу необхідно приділяти саме цьому типу перетворень.

Параметри симетричних криптоалгоритмів, такі як довжина ключа і розмір блоку шифрування, довжина значення, що повертається функцією ґешування тощо суттєво впливають на ефективність програмної або апаратної реалізації криптографічних примітивів. На основі цих параметрів обчислюються граничні показники стійкості до різних видів криптоаналізу, і, відповідно, необхідні властивості та складність раундового перетворення, а також потрібна кількість циклів для ітеративних алгоритмів.

Зайвий запас стійкості призводить до неефективного використання ресурсів, дорожчання або уповільнення роботи обчислювальної системи, водночас, недостатній рівень стійкості дозволяє зловмиснику реалізувати атаку на послуги безпеки та

нанести втрати. За цих умов обґрунтування параметрів перетворень є необхідним для ефективної реалізації криптографічних засобів захисту ІТС.

Сучасні блокові шифри є одним із найбільш розповсюджених криптографічних примітивів. Крім забезпечення конфіденційності, вони використовуються як конструктивний елемент в ході побудови функцій ґешування, кодів автентифікації повідомлення, генераторів псевдовипадкових послідовностей тощо. Значення цього примітива підкреслює проведення низки міжнародних і національних криптографічних конкурсів, які були орієнтовані на розробку блокового шифру (як основної мети або у складі набору перспективних перетворень). Обґрунтування конструкції раундового відображення блокового шифру із заданими криптографічними властивостями необхідно для забезпечення ефективності перетворення. Більш того, ці конструкції можуть використовуватися як нелінійне перетворення в ході синтезу потокових шифрів, ітеративних ґеш-функцій та ін. Крім того, для блокових шифрів потрібно обґрунтування показників ефективності основних високорівневих конструкцій і нових схем генерації циклових ключів для перспективних шифрів. Додатково, при функціонуванні в недовіреному середовищі (засоби автентифікації користувача, модулі доступу до цифрового телебачення, що знаходяться безпосередньо у абонента та ін.), можлива реалізація атак, які орієнтовані не на властивості математичного перетворення, а на апаратні засоби криптографічного захисту. Захист від низки атак такого типу може бути реалізований як за рахунок вдосконалення перетворення, так і при безпосередній розробці засобів криптографічного захисту.

Стандарти, що визначають симетричні криптографічні перетворення, які зараз задіють в Україні, були розроблені 20–25 років тому. Хоча вони все ще забезпечують практичну стійкість задовільного рівня, тим не менш, для них відомі ефективні методи криптоаналізу, які мають складність значно меншу, ніж переборні атаки.

Алгоритм блокового шифрування ГОСТ 28147-89 вже виведений із дії в Білорусії та, відповідно до результатів наукових конференцій, планується до заміни в Росії. Міждержавний стандарт ГОСТ 34.311-95, що визначає криптографічну ґеш-функцію, замінений новими національними стандартами в Росії та Білорусії. Крім того, стандарти симетричного перетворення, які зараз використовуються в Україні, на сучасних обчислювальних архітектурах загального призначення мають суттєво меншу швидкодію порівняно з іноземними аналогами. Тому актуальною є проблема обґрунтування параметрів і синтезу стійких та продуктивних симетричних криптографічних перетворень для заміни стандартів, що зараз діють в Україні.

Додатково слід відзначити особливість алгоритму шифрування, який визначений у ДСТУ ГОСТ 28147:2009, – відсутність стандартного довгострокового ключового елементу (ДКЕ), який, як вказано у стандарті, постачається в установленому порядку. Дослідження залежності криптографічної стійкості та можливості дешифрування криптограм третьою авторизованою стороною, що постачає ДКЕ, без знання ключа шифрування, а також формування класу шифрів, які допускають наявність такої властивості, також є суттєвою науковою проблемою.

Перераховані фактори свідчать про існування протиріччя між необхідністю залучення значних ресурсів для вирішення задач синтезу в умовах обмеження на час розробки, кількості залучених фахівців та доступних обчислювальних потужностей та

актуальність теми дисертаційних досліджень в напряму розробки стійких і одночасно продуктивних симетричних криптографічних перетворень.

Науковою проблемою, яка розв'язується в дисертації, є розвиток теорії побудови симетричних криптографічних перетворень, що забезпечують необхідний рівень стійкості щодо аналітичних методів криптоаналізу, високу швидкодію і компактність реалізації в умовах обмеження часових, дослідницьких і обчислювальних ресурсів під час розробки перспективних симетричних криптографічних алгоритмів.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проводилися в рамках науково-дослідних робіт: № 390 «Розробка політики та концепції побудови захищених інформаційних технологій, розробка та дослідження методів та математичних моделей обробки та захисту інформації в системах та мережах» (№ ДР 0198U004445); № 125-1 «Дослідження та розробка перспективних технологій криптографічного захисту інформації в телекомунікаційних системах і мережа» (№ ДР 0101U005125); «Вибір та дослідження алгоритму шифрування для використання в апаратно-програмному комплексі» (№ ДР 0104U002433); «Розробка перспективних методів та засобів криптографічного захисту інформації в державних відомствах України» (№ДР0102U003739); «Дослідження та розробка перспективних криптографічних систем та протоколів захисту інформації у телекомунікаційних системах та мережах України» (№ ДР 0103U001981).

Мета і задачі дослідження. Метою дисертаційної роботи є обґрунтування принципів побудови та оцінки властивостей симетричних криптографічних перетворень, що задовольняють вимоги щодо стійкості і швидкодії.

Для досягнення мети сформульовано та вирішено такі задачі досліджень:

1. Розробка математичної моделі проведення атак на основі таблиць передобчислень (із застосуванням точок розрізнення, rainbow та fuzzy-rainbow), яка дозволяє формувати множину унікальних врахованих елементів, з потужністю, близькою до потужності множини значень невідомого стану криптографічного перетворення, для реалізації ефективних криптоаналітичних атак на симетричні примітиви успадкованого рівня стійкості й обґрунтування параметрів перспективних алгоритмів.

2. Розробка методу порівняння високорівневих конструкцій симетричних блокових шифрів на основі ланцюга Фейстеля, схеми Лей-Мессі і SPN-структури з відповідною кількістю раундів, який дозволяє отримати аналітичну оцінку ефективності основних конструкцій, яка не залежить від властивостей раундового перетворення, та обґрунтувати вибір конкретної структури для перспективного алгоритму шифрування.

3. Розробка методу синтезу симетричних блокових шифрів, що дозволяє авторизованій стороні виконувати читання криптограм без ключів із заздалегідь заданою обчислювальною складністю, при цьому забезпечуючи експоненційну обчислювальну складність дешифрування для третьої сторони, який може бути використаний для виявлення небажаних властивостей криптографічного перетворення під час проведення експертизи блокового алгоритму.

4. Вдосконалення методів синтезу схем генерації циклових ключів симетричних блокових шифрів, які дозволяють захистити алгоритм від атак на зв'язаних ключах, при цьому забезпечуючи ефективну реалізацію.

5. Розробка перспективного симетричного блокового шифру і функції ґешування, які забезпечують високий і надвисокий рівень криптографічної стійкості, із швидкодією, що дорівнює або перевищує іноземні аналоги на сучасних 64-бітових платформах.

Об'єкт дослідження – процеси захисту інформації із використанням симетричних криптографічних перетворень та їх властивості.

Предмет дослідження – рівень стійкості та ефективність реалізації існуючих та перспективних симетричних криптографічних перетворень.

Методи дослідження. Під час проведення дисертаційних досліджень використовувалися методи теорії ймовірностей, теорії скінчених груп та полів, теорії інформації і теорії складності, комбінаторного та системного аналізу.

Методи теорії ймовірностей, комбінаторного та системного аналізу, теорії складності і теорії інформації використовувалися під час вирішення задач оцінки ефективності атак на основі передобчислень і обґрунтування необхідних параметрів перспективних симетричних криптографічних перетворень, під час отримання точних оцінок складності розрізнення випадкової перестановки і високорівневих конструкцій симетричних блокових шифрів, під час розробки методу їх порівняння, і під час розробки нового методу побудови схем розгортання циклових ключів ітеративних блокових шифрів.

Методи теорії скінчених груп і полів, теорії ймовірностей, комбінаторного та системного аналізу використовували під час розробки методу синтезу блокових шифрів, які допускають зниження складності дешифрування для авторизованої сторони.

Достовірність отриманих результатів підтверджується коректним застосуванням математичного апарату, збіжністю теоретичних та експериментальних результатів.

Наукова новизна одержаних результатів. В ході вирішення задач дисертаційних досліджень отримано такі наукові результати.

1. Вперше запропоновано метод оцінки складності етапу передобчислень криптоаналітичної атаки на основі rainbow-таблиць в умовах, коли потужність множини унікальних елементів, які враховані у таблиці, є близькою до потужності множини значень невідомого стану криптографічного перетворення, що дозволяє реалізовувати такі атаки із заданою ймовірністю успіху, а також обґрунтовувати параметри перспективних симетричних криптографічних примітивів для захисту від криптоаналітичних атак на основі передобчислень.

2. Вперше запропоновано математичну модель виконання криптоаналітичних атак на основі застосування декількох fuzzy-rainbow-таблиць, із потужністю множини унікальних елементів, близьких до потужності множини значень невідомого стану криптографічного перетворення, що дозволяє отримати значення складності виконання етапу передобчислень в умовах забезпечення високої ймовірності успіху і низької обчислювальної складності виконання оперативного етапу криптоаналітчної атаки.

3. Вперше запропоновано метод порівняння високорівневих конструкцій симетричних блокових шифрів на основі оцінки складності розрізнення криптографічного перетворення і випадкової перестановки, що дозволяє визначити високорівневу конструкцію із найкращим співвідношенням криптографічної стійкості до кількості раундів блокового шифру.

4. Вперше запропоновано метод синтезу симетричних блокових шифрів на основі таємних несюр'єктивних S-блоків, що дозволяє авторизованій стороні виконувати безключеве читання криптограм із заздалегідь заданою постійною обчислювальною складністю та забезпечує експоненційну складність дешифрування для третьої сторони.

5. Отримав подальшого розвитку метод оцінки ефективності ланцюга Фейстеля як високорівневої конструкції блокового шифру на основі застосування випадкових функцій у раундовому перетворенні, який відрізняється від відомих відмовою від припущення про рівноймовірність і несумісність подій колізій вихідних значень раундових функцій, а також використанням випадкових перестановок у раундовому перетворенні, що дозволяє отримати аналітичні співвідношення для обчислення уточненої оцінки верхньої межі показника переваги алгоритмів розрізнення випадкової перестановки і перетворення блокового шифру на основі ланцюга Фейстеля.

6. Отримав подальшого розвитку метод оцінки ефективності високорівневої конструкції блокового шифру на основі схеми Лей-Мессі, який відрізняється від відомих урахуванням ймовірності події появи колізії на вході функції раундового перетворення і застосуванням випадкових перестановок у раундовому перетворенні, що дозволяє отримати аналітичну оцінку верхньої межі показника переваги алгоритмів розрізнення блокового шифру на основі схеми Лей-Мессі та випадкової перестановки.

7. Отримав подальшого розвитку метод синтезу схем генерування циклових ключів симетричних блокових шифрів, який забезпечує небієктивну відповідність множини циклових ключів і ключів шифрування, що відрізняється від відомих застосуванням складнооборотного генератора псевдовипадкових послідовностей, який заснований на раундовому перетворенні блокового шифру, що дозволяє забезпечити стійкість шифру до атак на зв'язаних ключах і підвищити стійкість до атак на реалізацію.

Практичне значення одержаних результатів.

1. На основі моделі виконання атак із використанням таблиць передобчислень запропонований метод побудови криптоаналітичного комплексу для дешифрування криптограм, які сформовані алгоритмами успадкованого рівня стійкості. Зокрема, час дешифрування алгоритму A5/1 (ключ довжиною 64 біта), який використовується в мережах мобільного зв'язку GSM, може бути зменшено до однієї секунди при вартості обладнання порядку 10 тис. дол. США (повний перебір вимагає декілька місяців роботи криптоаналітичного комплексу вартістю декілька мільйонів доларів США).

2. Виконано обґрунтування параметрів перспективних симетричних алгоритмів на основі запропонованої моделі виконання атак із використанням таблиць передобчислень із урахуванням перспектив розвитку масових напівпровідникових технологій із конвеєрною архітектурою.

3. Запропонований метод синтезу симетричних блокових шифрів на основі таємних носюр'єктивних S-блоків, який дозволяє авторизованій стороні виконувати безключове читання криптограм із заздалегідь заданою обчислювальною складністю, дозволяє виконати додаткові перевірки для виявлення небажаних властивостей криптографічного перетворення під час проведення експертизи блокового алгоритму.

4. Розроблений симетричний блоковий шифр «Калина», який забезпечує високий і надвисокий рівень криптографічної стійкості, із рівнем швидкодії, що перевершує іноземні аналоги на сучасних 64-бітових платформах, використаний під час створення проекту специфікації нового національного стандарту України.

5. Розроблена криптографічна ґеш-функція «Купина», яка забезпечує високий і надвисокий рівень стійкості, із рівнем швидкодії, що перевершує російські та білоруські аналоги на 32- і 64-бітових платформах, використана під час створення проекту специфікації нового національного стандарту України для алгоритму ґешування.

Теоретичні і прикладні результати дисертаційних досліджень реалізовано в Державній службі спеціального зв'язку і захисту інформації України (акт від 29.09.2012), військовій частині Р 9000 (акт від 14.09.2012), приватному акціонерному товаристві «Інститут інформаційних технологій» (акт від 08.10.2012). Крім того, отримані результати застосовуються у навчальному процесі Харківського національного університету радіоелектроніки (акт від 31.08.2012) й Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут» (акт від 12.09.2012).

Особовий внесок здобувача. Всі наукові результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, опублікованих у співавторстві, автору належать такі результати: [1] - модель атаки та її застосування для аналізу шифру A5/1; [2] - аналіз властивостей перспективних криптографічних перетворень; [3] - вдосконалення критеріїв відбору для діючого стандарту шифрування; [4] - основні конструктивні рішення блокового шифру; [5] - доведено існування небажаних криптографічних властивостей для симетричного шифру; [6] - метод формування вузлів нелінійного перетворення; [7] - показники стійкості до алгебраїчного криптоаналізу; [8] - підхід до обґрунтування стійкості схеми розгортання ключів; [10] - метод оцінки властивостей вузлів заміни; [11] - вдосконалена модель оцінки стійкості до диференційного криптоаналізу; [13] - модель оцінки ефективності; [14] - вдосконалення методу оцінки складності атаки; [15] - запропонований набір нелінійних перетворень; [16] - оцінка ефективності ланцюга Фейстеля; [17] - аналіз криптографічних властивостей компонентів потокового шифру; [18] - аналіз властивостей малоресурсного шифру; [19] - оцінка ефективності схеми Лей-Мессі, методика порівняння; [20] - обґрунтування набору базових перетворень; [21] - показник оцінки ефективності криптоаналітичної атаки; [22] - вдосконалення набору показників оцінки випадковості; [23] - оцінка складності методу; [24] - оцінки стійкості шифру до диференційного криптоаналізу; [25] - аналіз принципів побудови і криптографічних властивостей блокового шифру; [26] - аналіз криптографічних властивостей блокових шифрів; [27] - вимоги до перспективного блокового шифру; [28] - метод синтезу схем розгортання ключів та доведені криптографічні властивості; [30] - структура перетворення, яке шифрує; [31] - метод ефективної реалізації,

перетворення, яке шифрує; [32] - структура перетворення і схема формування циклових ключів; [33] - методика та порівняння низки перспективних шифрів; [34] - сформульовані та обґрунтовані основні вимоги до блокових шифрів на основі схеми Лей-Мессі; [35] - обґрунтування конструкцій, які реалізовані у блоковому шифрі; [36] - обґрунтування стійкості шифру до диференційного та лінійного криптоаналізу; [37] - основні конструктивні рішення перспективного шифру; [38] - обґрунтування запропонованих конструкцій блокового шифру; [39] - обґрунтування криптографічної стійкості до низки методів криптоаналізу; [40] - обґрунтування стійкості шифру; [41] - підхід до оцінки криптографічних властивостей симетричних перетворень; [42] - метод кількісної оцінки властивостей перетворення; [43] - оцінка ефективності ланцюга Фейстеля; [44] - метод оцінки верхньої та нижньої межі довжини циклу раундового перетворення шифру; [45] - оцінка складності методу; [46] - метод оцінки ефективності перетворення; [47] - аналіз властивостей булевих функцій; [48] - метод лінеаризації блокового шифру; [49] - метод побудови перевизначеної системи; [50] - методика порівняння шифрів; [51] - порівняння низки перспективних шифрів; [52] - вдосконалення критеріїв відбору; [53] - аналіз властивостей підстановок; [54] - обґрунтування запропонованих конструкцій блокового шифру; [55] - обґрунтування криптографічної стійкості до низки методів криптоаналізу; [56] - основні конструктивні рішення блокового шифру; [57] - обґрунтування конструкцій, які реалізовані у блоковому шифрі; [58] - метод ефективної реалізації перетворення; [59] - вдосконалений метод оцінки стійкости; [60] - метод синтезу схем розгортання ключів шифру та доведення властивостей; [61] - доведення існування небажаних криптографічних властивостей для шифру; [62] - вдосконалення методу диференційного криптоаналізу; [63] - методика пошуку циклів; [64] - метод синтезу схем розгортання ключів та доведення криптографічних властивостей; [65] - підхід щодо оцінки потужності множини ключів, які видають виродженні вихідні послідовності; [66] - показники стійкості до алгебраїчного криптоаналізу; [67] - метод побудови блокових шифрів, що дозволяють зниження складності дешифрування криптограм; [68] - метод оцінки колізійних властивостей схеми розгортання; [69] - метод оцінки властивостей вузлів заміни; [71] - оцінка ефективності ланцюга Фейстеля; [72] - вибір показників оцінки ефективності методу; [73] - аналіз властивостей малоресурсного шифру; [74] - оцінка ефективності ланцюга Фейстеля та методи її порівняння; [75] - метод побудови перевизначеної систем рівнянь; [76] - оцінка ефективності схеми Лей-Мессі та її порівняння.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи були представлені, доповідалися й обговорювалися на: ***7 міжнародних наукових і науково-практичних конференціях, які проведені за кордоном:*** IX-й Міжнародній науковій конференції «Central European Conference on Cryptography (CECC-2009)» (Чехія, м. Прага, 2009 р.); VI-й Міжнародній науково-практичній конференції «International Conference on Network Architectures and Information Systems Security (SAR-SSI 2011)» (Франція, м. Ля-Рошель, 2011 р.); VI-й Міжнародній науково-практичній конференції «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011)» (Чехія, м. Прага, 2011 р.); VII і X Міжнародних науково-практичних конференціях «Информационная безопасность» (Росія, м. Таганрог, 2007, 2010 рр.); I-й та II-й

Міжнародних науково-практичних конференціях «Компьютерные науки и технологии» (Росія, м.Бєлгород, 2009, 2011 рр.); ***на 22 міжнародних наукових і науково-практичних конференціях, які проведені в Україні:*** VI–XV Міжнародних науково-практичних конференціях "Безпека інформації в інформаційно-телекомунікаційних системах" (м. Київ, 2003 – 2012 рр.); VI-VII-му Міжнародному молодіжному форумі «Радіоелектроніка і молодь у XXI сторіччі» (м. Харків, 2003 – 2004 рр.); Міжнародних наукових конференціях «Теорія і техніка прийому, передавання і обробки інформації» (м. Харків, 2003 – 2004 рр.); I-й та II-й Міжнародних наукових конференціях «Глобальні інформаційні системи. Проблеми й тенденції розвитку» (м. Харків, 2006 – 2007 рр.); X-й Міжнародній науковій конференції «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії» (м. Львів, 2010 р.); V-й та VI-й Міжнародних наукових конференціях „Гарантоздатні системи, сервіси та технології – Dependable Systems, Services and Technologies, DESSERT" (м. Кіровоград, м. Севастополь, 2011 – 2012 рр.); I-й Міжнародній науковій конференції «Системний аналіз та інформаційні технології» (м. Київ, 2011 г.); VI-й Міжнародній науковій конференції «Наука і соціальні проблеми суспільства: інформатизація та інформаційні технології» (м. Харків, 2011 р.); IV-му Міжнародному радіоелектронному форумі «Прикладна радіоелектроніка. Стан та перспективи розвитку» (м. Харків, 2011 р.); ***на Міжнародному науковому симпозіумі*** «Питання оптимізації обчислень» (пгт. Кацивелі, 2011, 2013 рр.); ***на наукових семінарах*** «Математичні методи захисту інформації» (НТУУ КПІ, 2007 р.) і «Cryptography, Coding Theory, and Secure Communication» (науковий центр ім. Е.Селмера, Бергенський університет, Норвегія, м. Берген, 2012 р.).

Публікації. За результатами дисертаційних досліджень опубліковано 76 наукових праць (4 одноосібні): 1 колективна монографія, 29 статей, які висвітлюють основні результати роботи, у фахових виданнях з технічних наук, з них 25 в Україні та 4 за кордоном; отримано 3 патенти на винахід; 9 статей, що додатково висвітлюють результати роботи, у фахових виданнях з технічних наук в Україні; 35 публікацій матеріалів і тез доповідей на міжнародних науково-технічних конференціях, з них 4 на закордонних конференціях.

Структура та обсяг дисертації. Дисертація складається із вступу, п'яти розділів, висновків, списку використаних джерел і чотирьох додатків. Повний обсяг дисертації складає 423 сторінки, що включає 75 рисунків, 35 таблиць, 4 додатки (на 70 сторінках), список використаних джерел з 263 найменувань (на 29 сторінках).

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність напрямку досліджень, сформульовано мету та задачі дисертаційної роботи, визначено об'єкт, предмет і методи досліджень, наукову новизну та практичне значення отриманих результатів.

У **першому** розділі виконано аналіз стану проблеми синтезу симетричних криптографічних перетворень. Розглянуто загальну характеристику чинних та перспективних криптографічних перетворень, що використовуються в Україні, інших країнах СНД та світі. Проведено аналіз існуючих методів синтезу та обґрунтування стійкості симетричних блокових шифрів і ґеш-функцій. Розглянуто математичні моделі

криптоаналітичних атак, відомі результати щодо аналізу та оцінки ефективності високорівневих конструкцій блокових шифрів і ґеш-функцій на їх основі, а також основного рандомізуючого перетворення ітеративних симетричних алгоритмів. На основі аналізу наукових публікацій показано, що, незважаючи на відчутний прогрес в окремих напрямках досліджень, загальна теорія синтезу симетричних перетворень знаходиться на етапі розробки. Зокрема, залишається невирішеним ряд актуальних наукових задач: розробка математичної моделі атак із використанням таблиць передобчислень для обґрунтування вибору параметрів перспективних перетворень; розробка методів і моделей порівняння високорівневих конструкцій блокових шифрів для аналітичного обґрунтування перспективного алгоритму; розробка методів синтезу блокових симетричних шифрів, що мають незадокументовану властивість дешифрування повідомлень третьою стороною, для вдосконалення методів експертизи перспективних перетворень; вдосконалення методів синтезу схем розгортання ключів блокового алгоритму, що дозволяють захистити шифр від атак на зв'язаних ключах, та ефективних при програмній та апаратній реалізації. З практичної точки зору, актуальним питанням є синтез перспективного блокового шифру і функції ґешування, що забезпечують високий рівень стійкості, та ефективно працюють на 64-бітових платформах.

Зазначені факти, поряд з іншими об'єктивними факторами, визначають наукову проблему, окремі задачі та напрямки дисертаційних досліджень.

У **другому** розділі розроблено математичні моделі та методи реалізації атак переборного типу, а також виконано обґрунтування параметрів перспективних симетричних криптографічних перетворень, що забезпечують захист в умовах реалізації таких атак порушником третього рівня (який має науково-технічний ресурс спеціальної служби економічно розвинутої держави).

У рамках моделі передбачається, що до початку проведення атаки криптоаналітику відомий опис криптосистеми – відповідна алгебра $\mathrm{A} \in \{\Sigma_A, \Psi_A, \Xi_A, \Gamma_A\}$, що описує симетричний примітив із заданими множинами вхідних (X) та вихідних (Y) послідовностей, множиною ключів або прообразів (K) і множиною параметризованих відображень ($G = \{G_\chi\}: X \to Y, \chi \in K$).

З початку атаки криптоаналітик отримує вхідне і відповідне вихідне значення, отримане на основі використання одного невідомого параметра: $\{x_i\} \neq \varnothing$, $\{y_i\} \neq \varnothing$, $x_i \in X$, $y_i \in Y$, $G_\chi(x_i) = y_i$. Передбачається, що множина отриманих вихідних значень достатня для досягнення відстані єдності. Задача криптоаналітика – на основі перебору або пошуку в таблиці передобчислень визначити невідомий параметр $\chi \in K$, який був використаний в ході формування вихідних послідовностей $G_\chi(x_i) = y_i$.

При розгляді атак на основі компромісу «час-пам'ять» (time-memory trade-off, TMTO) використовується функція переходу, що дозволяє реалізувати псевдовипадкове відображення елементів ключової множини на себе (обмежень на властивості сюр'єктивності або ін'єктивності не накладається). Функція переходу має забезпечувати властивості випадкового відображення і, як правило, є композицією прямого криптографічного перетворення і додаткового параметризованого відображення:

$$F_q : K \to K,\ F_q = f_q \circ G_{k_i}, \qquad (1)$$

де G_{k_i} – пряме криптографічне перетворення, яке параметризоване $k_i \in K$; $f_q : \Delta \times Y \to K$, $q \in \Delta$ – псевдовипадкове параметризоване відображення множини вихідних послідовностей до ключової множини.

Найбільш ефективні сучасні атаки з використанням передобчислень застосовують моделі Ґеллмана, на основі точок розрізнення, rainbow-таблиць та fuzzy-rainbow-таблиць.

Таблиця на основі точок розрізнення є набором рядків (ланцюгів) виду $k_{i,1}^{(q)} \xrightarrow{F_q} k_{i,2}^{(q)} \xrightarrow{F_q} ... \xrightarrow{F_q} k_{i,\rho(i,q)}^{(q)}$. Довжина ланцюга $\rho(i,q)$ є випадковою величиною, що розподілена відповідно до геометричного закону.

Для таблиці на основі точок розрізнення отримано такі співвідношення: в ході використання d бітів у точці розрізнення для реалізації атаки переборного типу на симетричний криптографічний примітив з потужністю допустимих значень невідомого параметра 2^k, побудови таблиці, що складається із m рядків ($m \le 2^{k-d}$) із довжинами $\rho(1,q), \rho(2,q), ..., \rho(m-1,q)$ кожна:

– на етапі передобчислень – математичне сподівання верхньої межі складності побудови таблиці (кількості рядків, які генеруються) не перевищує значення

$$\Theta^{dp} \le m \cdot \left(1 - \frac{1}{2^k} \sum_{j=1}^{m-1} \rho(j,q)\right)^{-\rho(m,q)} \cdot \left(1 - \frac{\rho(m,q)}{2^k}\right)^{-\frac{\rho(m,q)\cdot(\rho(m,q)-1)}{2}} \approx$$

$$\approx m \cdot e^{\frac{2^{2d}\cdot(2m-1)-2^d}{2^{k+1}}}; \qquad (2)$$

– на оперативному етапі – ймовірність успішного відновлення при випадковому, рівноймовірному і незалежному виборі невідомого стану дорівнює

$$P_{succ}^{dp} = \frac{1}{2^k} \cdot \sum_{j=1}^{m} \rho(j,q) \approx \frac{m}{2^{k-d}}. \qquad (3)$$

У рамках звичайного для криптопримітива припущення, що послідовність, яка формується, має властивості випадкового відображення, складність алгоритму прямої перевірки попадання до циклу дорівнює $O\left(n^2\right)$, де n – довжина сформованої послідовності. Пряма оптимізація цього алгоритму знижує складність тільки до $O(n \cdot \log n)$. Додатковий запропонований алгоритм, який визначає входження до циклу із заздалегідь заданою ймовірністю, має часову та просторову складність $O(1)$.

Задачею розробки методу передобчислень на основі rainbow-таблиць було зниження ймовірності злиття різних ланцюгів, що визначає основну складність етапу передобчислень, із збереженням фіксованого розміру таблиці. Основною відмінністю rainbow-таблиць від раніше відомих методів є використання унікальної функції переходу в кожній колонці, тобто рядок має фіксовану довжину і представляється як

$k_{i,1} \xrightarrow{F_1} k_{i,2} \xrightarrow{F_2} \ldots \xrightarrow{F_{t-1}} k_{i,t}$. Застосування унікального відображення для кожного елементу дозволяє суттєво знизити ймовірність колізій, і для низки задач криптоаналізу достатньо побудувати одну таблицю великого розміру (замість значної кількості порівняно малих таблиць Ґеллмана або точок розрізнення).

Оцінки ефективності rainbow-таблиць, що наведені в низці робіт у відкритому друку, дають деяке наближення значення для ймовірності успіху та складності побудови таблиці. За необхідності отримання високої ймовірності успіху (значного обсяга таблиці) відомі методи дають значну похибку, яка викликана використанням низки припущень.

Отримані у розділі співвідношення дозволяють одержати точну оцінку складності побудови таблиці передобчислень і проведення атаки.

Для rainbow-таблиці, яка складається із m рядків і t стовпців, що використовується для реалізації атаки на симетричний криптографічний примітив із потужністю допустимих значень невідомого стану 2^k, ($m << 2^k$):

– на етапі передобчислень – математичне сподівання верхньої межі складності побудови таблиці (кількості рядків, що генеруються) не перевищує значення

$$\Theta^{rb} < m \cdot \left(1 - \frac{m-1}{2^k}\right)^{1-t} \approx m \cdot e^{\frac{(m-1)(t-1)}{2^k}}; \qquad (4)$$

– на оперативному етапі – ймовірність успішного відновлення при випадковому, рівноймовірному і незалежному виборі значення параметра невідомого стану криптосистеми дорівнює

$$p^{rb} = 2^{-k} \sum_{i=1}^{t} m_i \text{, де } m_j = m \cdot \left(1 - 2^{-k} \sum_{i=1}^{j-1} m_i\right), m_1 = m. \qquad (5)$$

Із оцінки складності побудови випливає, що навіть при великих обсягах таблиці ($m \cdot t \approx 2^k$) при $m << 2^k$ ймовірність відсутності колізії в ході завершення побудови таблиці залишається достатньо високою: $p_{nc}^{rb} \approx e^{-1}$, що означає, що навіть для додавання m-го рядка потрібно, в середньому, не більш ніж 3 спроби.

Застосування rainbow-таблиці для криптоаналізу дозволяє отримати мінімальну складність етапу передобчислень навіть для таблиць, з обсягом, близьких до потужності множини станів невідомого параметра. Порівняно з іншими типами таблиць (Ґеллман, точки розрізнення, fuzzy-rainbow) у rainbow-таблиці буде найбільша кількість унікальних елементів. Ще однією перевагою при практичній реалізації є те, що rainbow-матриця (множина початкових та кінцевих точок) такого обсягу зберігатиметься на декількох носіях, що дозволить значно прискорити виконання криптоаналізу.

Недоліком методу є необхідність перевірки значення на належність до кожного стовпця, що, в свою чергу, веде до значного збільшення часу виконання атаки.

Обчислювальна складність перевірки наявності елемента в rainbow-таблиці на оперативному етапі дорівнює $O\left(t^2 \cdot \log m\right)$, де t – довжина рядка.

Таким чином, застосування виключно rainbow-таблиць дозволить максимально знизити складність етапу передобчислень, але оперативний етап утворюється достатньо тривалим за рахунок великої кількості вибірок із пам'яті.

Fuzzy-rainbow-таблиці об'єднують можливості rainbow-таблиць і ланцюгів на основі точок розрізнення, що дозволяє отримати компромісне рішення. На момент виконання досліджень у відкритому друці представлені результати тільки для визначення співвідношення обсягу необхідної пам'яті та кількості різних функцій переходу для фіксованої ймовірності виникнення колізії. Fuzzy-rainbow-таблиця складається із m рядків, кожен з яких отриманий шляхом багаторазового застосування функцій переходу $F_1, F_2, ..., F_s$. Зміна функції в таблиці $F_i \to F_{i+1}$ виконується після появи в ланцюгу значень $k_{i,r}^{(q)}, k_{i,r+1}^{(q)}, k_{i,r+2}^{(q)}, ...$ деякої ознаки (як правило, появи заданої кількості (d) нульових бітів у фіксованих позиціях змінної k, що описує невідомий стан примітива).

У розділі отримано співвідношення, які дозволяють оцінити складність передобчислень і виконання атаки.

В ході реалізації атаки на симетричний криптографічний примітив з потужністю допустимих значень невідомого стану криптосистеми 2^k, на основі fuzzy-rainbow-таблиці, яка містить m рядків ($m << 2^k$) та s різних функцій переходу, що змінюються при виході на точку розрізнення довжиною d біт:

– на етапі передобчислень – математичне сподівання верхньої межі складності побудови таблиці (кількості рядків, що генеруються) не перевищує значення

$$\theta^{fr} < m \cdot \left(1 - \frac{1}{2^k}\right)^{s \cdot l - s \cdot l^2 \left(m - \frac{1}{2}\right)} \cdot \left(1 - \frac{m-1}{2^{k-d}}\right)^{1-s} \approx$$

$$\approx m \cdot e^{2^{-k}\left(s 2^{2d}\left(m - \frac{1}{2}\right) + 2^d((s-1)(m-1) - s)\right)}; \qquad (6)$$

– на оперативному етапі – ймовірність успішного відновлення при випадковому, рівноймовірному і незалежному виборі значення параметра невідомого стану криптосистеми дорівнює

$$p_{succ}^{fr} = 2^{-k} \sum_{i=1}^{s} m_i \text{, де } m_j = m \cdot l \cdot \left(1 - \frac{1}{2^k} \sum_{i=1}^{j-1} m_i\right), m_1 = m \cdot l. \qquad (7)$$

Таким чином, fuzzy-rainbow-таблиці дозволяють отримати компромісне рішення для досягнення високої ймовірності успіху, порівняно малий час проведення атаки і припустимий рівень складності на етапі передобчислень. Додаткове експоненційне зниження складності попереднього етапу можливо досягти за рахунок лінійного збільшення складності часу виконання атаки.

Застосування розробленого методу на основі fuzzy-rainbow-таблиць до аналізу потокового шифру успадкованого рівня стійкості A5/1 в умовах мереж мобільного зв'язку GSM демонструє можливість створення криптоаналітичного комплексу, який здатний відтворювати невідомий ключ шифрування (K_C) по відомому блоку гами

довжиною 456 біт за період часу не більш ніж 1,97 с при собівартості апаратних засобів для оперативного етапу в 14 тис. дол. США (у цінах станом на січень 2011 р.). Етап передобчислень (побудову таблиць) можливо реалізувати на серверах NVidia Tesla S 2050 в термін від 30 до 130 днів, залежно від ймовірності успіху та додаткових умов (без застосування припущень, які були зроблені під час розробки відкритого проекту Kraken).

Порівняння складності етапів передобчислення і виконання атаки (оперативного) для різних методів наведено у табл.1, де m – кількість рядків, t – кількість стовпців, s – кількість різних функцій переходу для fuzzy-rainbow-таблиць, при цьому завжди $s < t$.

Таблиця 1 – Порівняння складності етапів передобчислення і виконання атаки

Етап/метод	Точки розрізнення	Rainbow	Fuzzy-rainbow
Передобчислень	$O\left(m \cdot e^{m \cdot t^2}\right)$	$O\left(m \cdot e^{m \cdot t}\right)$	$O\left(m \cdot e^{\frac{m \cdot t^2}{s}}\right)$
Оперативний	$O(\log m)$	$O\left(t^2 \cdot \log m\right)$	$O(t \cdot s \cdot \log m)$

Алгебраїчні моделі, які використані, призначені для аналізу стійкості до атак на основі таблиць передобчислень, розглядають криптографічний примітив без урахування його внутрішньої структури. Відповідно, стійкість до цих методів криптоаналізу визначається виключно зовнішніми параметрами перетворення (розмір блоку, довжина ключа та ін.). Для успішної протидії порушнику 3-го рівня доцільно розглянути наступну модель атаки.

Час експлуатації криптографічного алгоритму – 30 років. У державі щосекунди формується близько 10 тис. повідомлень, для яких використовується криптографічний захист для передавання відкритим каналом зв'язку. Криптоаналітична служба порушника має можливість перехоплювати і зберігати кожну криптограму, яка залишається актуальною для розкриття протягом всього часу використання алгоритму. У розпорядженні криптоаналітика є ефективна обчислювальна система, яка складається із 100 млн процесорів, кожен з яких працює на частоті 5 ГГц (близько до практично досяжної межі масових напівпровідникових технологій) із конвеєрною архітектурою.

На основі розроблених моделей і ймовірності розкриття криптоаналітиком хоча б одного повідомлення $p_{вскр} = 10^{-9}$ потужність множини значень невідомого стану криптоперетворення має бути не менш ніж 2^{162} за умови відповідності властивостей випадковому відображенню і неможливості реалізації аналітичної атаки, яка використовує особливості внутрішньої структури перетворення.

Для симетричних криптографічних перетворень, що розробляються, необхідно реалізувати запас стійкості із урахуванням особливостей існуючих і перспективних архітектур. Зокрема, із врахуванням запасу стійкості та вирівнюванні слова по 64- або 128-бітовій межі, доцільно використовувати потужність множини значень не менш ніж 2^{192} або 2^{256}. Для ефективної програмної або програмно-апаратної реалізації доцільно

використовувати значення $N_{кл} \geq 2^{256}$ під час розробки перспективних високостійких симетричних криптографічних примітивів.

Для ґеш-функцій і кодів автентифікації повідомлення, аналогічно шифрам, із урахуванням можливості розробки криптоаналітичних атак і необхідності ефективної програмної реалізації на сучасних і перспективних архітектурах, потужність множини значень ґеш-функції і кодів автентифікації повідомлення доцільно задати не менш ніж $N_{зн} \geq 2^{256}$.

Запропоновані в розділі методи та моделі показали ефективність атак на основі передобчислень і були використані для обґрунтування параметрів перспективних високостійких криптографічних перетворень.

У **третьому** розділі розроблено математичні моделі оцінки ефективності високорівневих конструкцій симетричних блокових шифрів (незалежних від властивостей раундового перетворення), запропоновано метод їх порівняння і виконано обґрунтування вибору такої конструкції для перспективного блокового шифру.

Досвід проведення відкритих криптографічних конкурсів показав, що сьогодні в ході проектування блокових шифрів основна увага приділяється раундовому перетворенню і схемі формування циклових ключів. Вибір високорівневої конструкції шифру здійснюється на основі переваг розробника і у більшості випадків не має теоретичного обґрунтування.

Ефективність високорівневої конструкції блокового шифру доцільно аналітично визначати через складність розрізнення перестановки, яка сформована цією структурою, від випадкової відповідного степеня, оскільки саме множина випадкових перестановок є моделлю ідеального блокового шифру. Складність виконання алгоритму розрізнення і досяжна ймовірність успіху є чисельними показниками ефективності високорівневої конструкції. Для виключення впливу властивостей конкретної раундової функції необхідно використовувати рандомизоване перетворення, таке як випадкова функція або випадкова перестановка.

В ході отримання відомої оцінки ефективності розрізнення 3-раундового ланцюга Фейстеля було використано припущення про рівноймовірність подій виникнення колізій. Крім того, виходячи із складання ймовірностей у доведенні, автори відомої оцінки застосували припущення про несумісність подій, що є коректним для визначення верхньої межі ймовірності, але невірно для точного значення.

Точний результат, отриманий у розділі, формується таким чином: верхня межа ймовірності розрізнення 3-раундового ланцюга Фейстеля ψ на основі випадкових функцій $\{F_n\}$ та випадкової функції F_{2n} для k запитів на вході алгоритму розрізнення дорівнює

$$Adv_{\eta^*}(\psi, F_{2n}) = \left| P_1\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R \psi(F_n, F_n, F_n)\right) - P_1^*\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R F_{2n}\right) \right| \leq$$

$$\leq 1 - \prod_{i=0}^{k-2} \left(1 - \frac{1}{2^n - i}\right)^{2(k-(i+1))} \approx 1 - \left(1 - \frac{1}{2^n}\right)^{k(k-1)}. \qquad (8)$$

Залежність верхньої межі переваги алгоритму розрізнення від кількості вхідних пар для ланцюга Фейстеля над випадковою функцією, яке обчислено за відомим

співвідношенням, отримане в ході досліджень точне значення і його апроксимації наведені на рис. 1 для блоків довжиною 16 біт ($n=8$, ліворуч) і 32 біта ($n=16$, праворуч). По осі абсцис наведено кількість аргументів, які подаються на вхід, по осі ординат наведено значення переваги (ймовірність розрізнення випадкової перестановки і ланцюга Фейстеля).

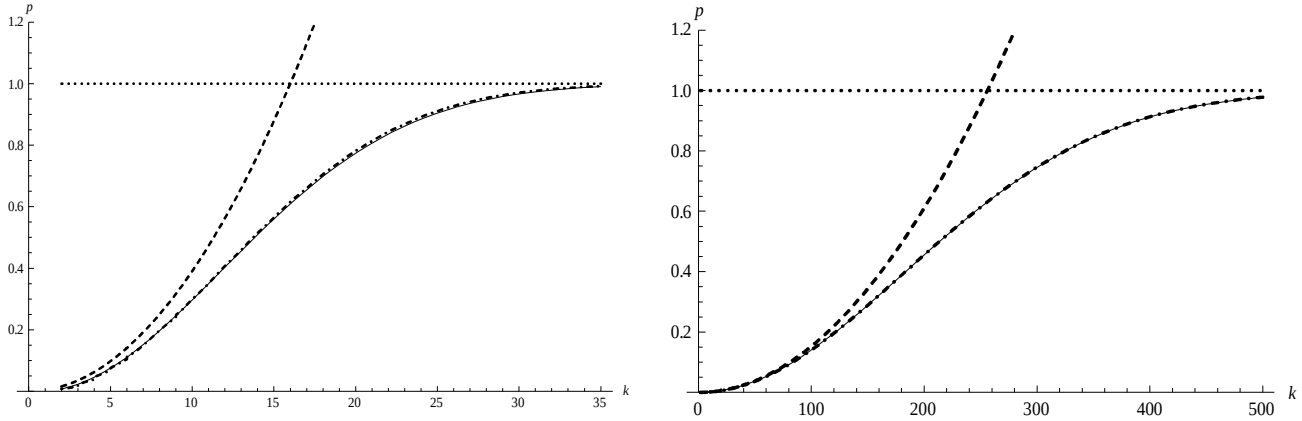

Рисунок 1 – Залежність верхньої межі переваги довільного алгоритму розрізнення від кількості вхідних пар для 3-раундового ланцюга Фейстеля

Для відомого алгоритму розрізнення ланцюга Фейстеля ψ на основі випадкових функцій отримано точні оцінки ефективності розрізнення криптографічного перетворення і випадкової перестановки σ_{2n}:

$$\mathrm{Adv}_{\eta_1}(\psi,\sigma_{2n}) \le \left| \prod_{i=0}^{k-2} \left(1-\frac{1}{2^n-i}\right)^{k-(i+1)} - \prod_{i=0}^{k-2} \left(1-\frac{1}{2^{2n}-1-i}\right)^{k-(i+1)} \right| \le$$

$$\le \left| \left(1-\frac{1}{2^n}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{1}{2^{2n}-1}\right)^{\frac{k(k-1)}{2}} \right|. \qquad (9)$$

Залежність верхньої межі переваги від кількості вхідних пар для $n=8$ і $n=16$ наведена на рис.2.

Аналогічні результати отримано і для інших відомих алгоритмів розрізнення ланцюга Фейстеля на основі випадкових функцій.

Для отримання більш точної оцінки високорівневої конструкції блокових шифрів із бієктивним раундовим перетворенням (ГОСТ 28147-89, Camellia та ін.) у розділі запропоновано модель, де раундове перетворення розглядається як випадкова перестановка (не випадкова функція). Для трьох і чотирьох раундів ланцюга Фейстеля такого шифру запропоновано алгоритми розрізнення. Показано, що в цьому випадку складність розрізнення блокового шифру ψ і випадкової перестановки σ_{2n} обмежена зверху величиною

$$\mathrm{Adv}_{\eta_3}(\psi,\sigma_{2n}) = \left|\mathrm{P}_{\eta_3} - \mathrm{P}^{*}_{\eta_3}\right| = 1 - \frac{2^{n(k-1)}\left(2^n-1\right)_k}{\left(2^{2n}-1\right)_k} \le 1 - \left(\frac{2^n}{2^n+1}\right)^{\frac{k(k-1)}{2}}. \qquad (10)$$

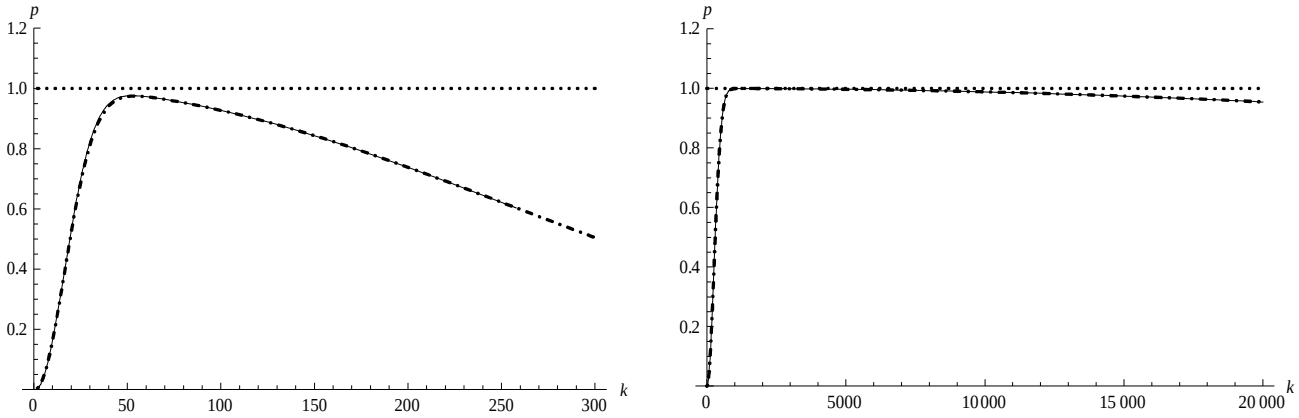

Рисунок 2 – Залежність переваги алгоритму розрізнення ланцюга Фейстеля від кількості вхідних пар

Під час проведення досліджень аналогічні результати отримано для схеми Лей-Мессі ς, яка використана у шифрах IDEA, FOX (IDEA-NXT), з кількістю раундів $r \ge 3$ та із застосуванням випадкових функцій у раундовому перетворенні: при k різних запитах максимальний рівень ймовірності розрізнення довільним алгоритмом не перевищує значення

$$Adv_{\eta^*}(\varsigma, F_{2n}) \le 1 - \left(\frac{2^n-2}{2^n-1}\right)^{\frac{k(k-1)}{2}}. \qquad (11)$$

Для конкретного алгоритму розрізнення схеми Лей-Мессі ς і випадкової перестановки σ_{2n} отримана точну оцінку верхньої межі ефективності розрізнення:

$$Adv_{\eta_6}(\varsigma,\sigma_{2n}) = \left|\prod_{i=0}^{k-2}\left(1-\frac{1}{2^n-i}\right)^{2(k-(i+1))} - \prod_{i=0}^{k-2}\left(1-\frac{2^n}{2^{2n}-1-i\cdot 2^n}\right)^{k-(i+1)}\right| \le$$

$$\le \left|\left(1-\frac{2^n}{2^{2n}-1}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{2^{n+1}-1}{2^{2n}}\right)^{\frac{k(k-1)}{2}}\right|. \qquad (12)$$

Як і для ланцюга Фейстеля, для схеми Лей-Мессі введено модель із випадковими перестановками у раундовому перетворенні. Перевага запропонованого алгоритму розрізнення 3-раундової схеми Лей-Мессі на основі випадкових перестановок не перевищує значення

$$Adv_{\eta_7}(\varsigma,\sigma_{2n}) = \left|\prod_{i=0}^{k-2}(1-\frac{1}{2^n-1-i})^{2(k-(i+1))} - \prod_{i=0}^{k-2}(1-\frac{2^n}{2^{2n}-1-i\cdot 2^n})^{k-(i+1)}\right| \le$$

$$\leq \left| \left(1-\frac{2^n}{2^{2n}-1}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{1}{2^n-1}\right)^{k(k-1)} \right|. \qquad (13)$$

Введення однієї метрики для оцінки дозволяє чисельно порівняти ефективність ланцюга Фейстеля (ψ) і схеми Лей-Мессі (ς) як високорівневих конструкцій блокових шифрів як на основі верхніх меж, так і за конкретними алгоритмами розрізнення.

Верхня межа переваги розрізнення двох конструкцій на основі випадкових функцій оцінюється як

$$Adv_{\eta^*}(\psi,\varsigma) = Adv_{\eta^*}(\psi,F_{2n}) - Adv_{\eta^*}(\varsigma,F_{2n}) = \left(\frac{2^n-2}{2^n-1}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{1}{2^n}\right)^{k(k-1)}. \qquad (14)$$

Під час застосування найкращих алгоритмів розрізнення перевага визначається як

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

$$- \left| \left(1-\frac{2^n}{2^{2n}-1}\right)^{\frac{k(k-1)}{2}} - \left(1-\frac{2^{n+1}-1}{2^{2n}}\right)^{\frac{k(k-1)}{2}} \right|. \qquad (15)$$

Графік різниці ймовірностей розрізнення (ефективності) конструкцій на основі ланцюга Фейстеля і схеми Лей-Мессі в ході використання випадкових функцій в раундовому перетворенні для верхньої межі переваги розрізнення і кращих відомих алгоритмів розрізнення залежно від кількості запитів наведений на рис.3 (ліворуч і праворуч відповідно).

Як видно із співвідношень (14), (15) та графіків на рис. 3, $Adv_{\eta^*}(\psi,\varsigma) > 0$ і $Adv_{\eta-opt}(\psi,\varsigma) > 0$, звідки випливає більш висока ефективність схеми Лей-Мессі порівняно з ланцюгом Фейстеля за критерієм складності розрізнення блокового шифру і випадкової перестановки.

Крім вже розглянутих рішень, SPN-структура є однією із найбільш поширених високорівневих конструкцій блокових шифрів. Зокрема, це перетворення використано у найбільш поширеному в світі алгоритму AES/Rijndael, шифрах Anubis, GrandCru, Noekeon, «Калина» та ін. Для виключення впливу властивостей раундового перетворення доцільно використовувати випадкові перестановки замість шару S-блоків із наступним лінійним відображенням. Степінь перестановок, що використовуються, визначається розміром матриці лінійного перетворення (аналогічно, у низці робіт з диференційного криптоаналізу, 32-бітове перетворення,

яке об’єднує чотири S-блоки із наступним множенням на матрицю, позначено як AES Super-S-box).

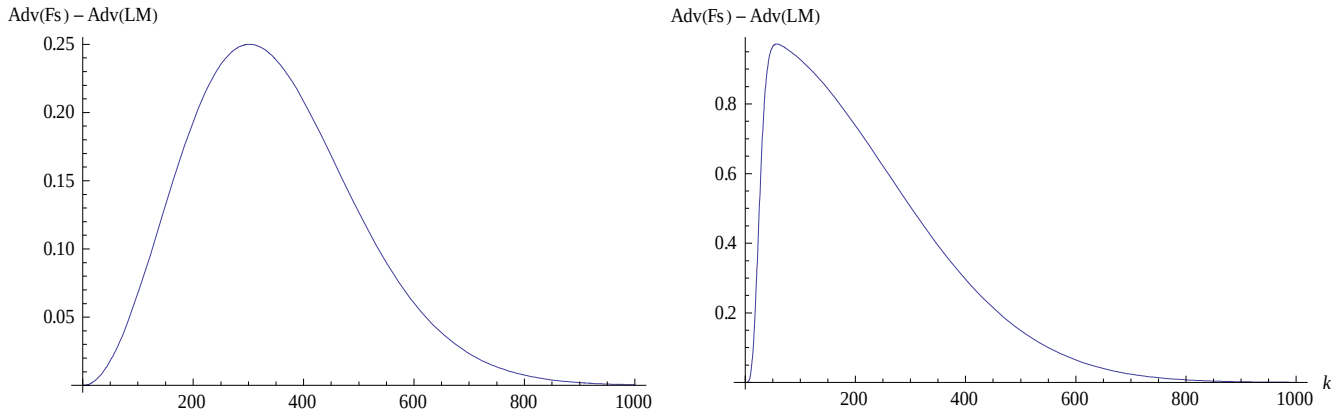

Рисунок 3 – Графік різниці ефективності високорівневих конструкцій на основі ланцюга Фейстеля і схеми Лей-Мессі при застосуванні випадкових функцій у раундовому перетворенні

Отримано і доведено наступне співвідношення: максимальна ймовірність розрізнення випадкової перестановки σ_{2n} і 2-циклової SPN-структури $\vartheta^{(2)}$ із розміром блоку $2n$ бітів і внутрішнім станом, який подається у вигляді матриці розміром $n_c \times n_b$ елементів, кожен з яких має розмір n_e біт ($2n = n_c \times n_b \times n_e$), при відповідності розмірів матриці умові $n_c = n_b \cdot 2l, l \in \{1,2,...\}$, застосуванні випадкових перестановок $\sigma_{\frac{2n}{n_c \cdot n_e}}$ у раундовому перетворенні, для k запитів $\left(2 \le k \le 2^{\frac{n_c \cdot n_e}{n_b}}\right)$ на вході алгоритму розрізнення не перевищує значення

$$Adv_{\eta^*}(\vartheta^{(2)}, \sigma_{2n}) \le$$

$$\le \left| 1 - \prod_{i=0}^{k-2} \left(1 - 2^{i - \frac{n_c \cdot n_e}{n_b}}\right)^{(n_b-1)(k-i-1)} - \prod_{i=0}^{\frac{k(k-1)}{2}-1} \left(\left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b} - i \right) \cdot \left(2^{n_c \cdot n_e} - i\right)^{-1} \right| \approx$$

$$\approx \left| 1 - \left(1 - 2^{-\frac{n_c \cdot n_e}{n_b}}\right)^{\frac{k(k-1)(n_b-1)}{2}} - 2^{-\frac{n_c \cdot n_e \cdot k \cdot (k-1)}{2}} \cdot \left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{\frac{n_b k(k-1)}{2}} \right|. \qquad (16)$$

Із (16) випливає, що 2-циклова SPN-структура, яка відповідає сформульованим вимогам, буде визначена алгоритмом розрізнення не більш ніж за $2^{\frac{n_c \cdot n_e}{n_b}} + 1$ запитів.

Далі у розділі показано, що не існує ефективного алгоритму розрізнення для 3-циклової SPN-структури і випадкової перестановки. Вихідні значення будь-якого такого алгоритму є деякою випадковою величиною, яка не залежить від типу перетворення, що аналізується:

$$Adv_{\eta^*}(\vartheta^{(3)}, \sigma_{2n}) =$$

$$= \left| P_1\left(\eta_*(f(x_1),..., f(x_k)) = 1 : f \in_R \vartheta^{(3)}\right) - P_1^*\left(\eta_*(f(x_1),..., f(x_k)) = 1 : f \in_R \sigma_{2n}\right) \right| = 0 . \quad (17)$$

Таким чином, запропоновані методи дозволили отримати чисельну оцінку ефективності різних високорівневих перетворень блокових шифрів і обґрунтувати вибір SPN-структури як найкращого варіанта побудови перспективного симетричного блокового шифру, який забезпечує високий рівень стійкості.

У **четвертому** розділі розроблено та обґрунтовано методи синтезу блоків криптографічного перетворення ітеративних симетричних примітивів, шарів лінійного та нелінійного відображень, які забезпечують оптимальні криптографічні властивості при ефективній програмній реалізації на перспективних архітектурах. Для вдосконалення методів експертизи блокових шифрів запропоновано метод синтезу таких перетворень, що дозволяють безключове читання криптограм уповноваженою установою, при цьому забезпечивши захист від читання третьою стороною.

В умовах технічних і економічних обмежень під час розробки засобу криптографічного захисту інформації, блок перетворення у складі високорівневої конструкції симетричного примітиву доцільно подати у вигляді композиції лінійних та нелінійних вузлів, які дозволяють отримати потрібні криптографічні властивості.

У розділі показано, що побудова нелінійного відображення на базі табличного перетворення (S-блоків) має низку переваг у порівнянні з використанням набору логічних або арифметичних функцій на основі команд процесорів деякої архітектури для програмної реалізації або відповідного набору логічних функцій в ході апаратної реалізації. Крім того, виконано обґрунтування переваг МДВ-перетворення для реалізації блока лінійного відображення порівняно із транспозицією або застосуванням лінійної операції загального вигляду, яка задана над деякою алгебраїчною структурою.

Мінімізація максимальних значень таблиць розподілу різниць і модулів таблиць лінійних апроксимацій S-блоків дозволяє забезпечити стійкість до диференційного і лінійного криптоаналізу за найменшу кількість раундів криптографічного перетворення.

Тим не менш, відомий підхід, який дозволяє побудувати перевизначену систему рівнянь над скінченим полем для опису всього перетворення – алгебраїчний криптоаналіз. Застосування S-блоків із гранично досяжними показниками властивостей для захисту від статистичних видів криптоаналізу (диференційного, лінійного) призводить до можливості побудови перевизначеної системи, яка описує S-блок, із низьким степенем (в т.ч. другим). А оскільки лише S-блоки визначають нелінійність багатьох шифрів, то низка алгоритмів, таких як AES/Rijndael, Camellia та ін. можуть бути описані розрідженою системою другого степеня. Практична стійкість криптографічних систем, що використовують такі шифри, забезпечується лише відсутністю універсальних методів вирішення систем 2-го ступеня (низка алгоритмів, у

тому числі поширений потоковий шифр, вже була успішно атакована за допомогою цього методу аналізу).

У розділі показано, що для S-блоку з n бітами на вході та m бітами на виході, степінь системи, яка описує перетворення, не перевищує значення $d_{\min}$, яке знаходиться із співвідношення

$$\left(\sum_{i=0}^{d_{\min}} C_{n+m}^{i} \right) > 2^{n}. \qquad (18)$$

З (18) можна визначити максимальний степінь перевизначеної системи, якою може бути описано довільне перетворення із заданими розмірностями вхідних та вихідних значень. Зокрема, для байтових S-блоків степінь перевизначеної системи, що описує перетворення, менша або дорівнює 3.

У розділі наведено критерії для відбору S-блоків, які забезпечують максимальний рівень захисту симетричних криптографічних примітивів від алгебраїчних та статистичних атак:

– максимально досяжний степінь системи, що описує S-блок;

– мінімально досяжний максимум перетворення нетривіальних вхідних різниць;

– мінімально досяжний максимум модуля значень для нетривіальних лінійних апроксимацій;

– відсутність нерухомих точок.

За допомогою алгоритму, який формує підстановки відповідно до запропонованих критеріїв, були отримані S-блоки для застосування у перспективному блоковому шифрі та ґеш-функції, із наступними властивостями (табл.2).

При порівнянні характеристик сформованих підстановок і S-блоків такого ж розміру низки блокових і потокових шифрів та ґеш-функцій (Crypton, Safer+, Skipjack, SNOW, Twofish, Whirlpool, CS, Anubis, DESX, ГОСТ Р 34.11-12 «Стрибог», СТБ 34.101.31-2011) відзначено, що саме побудовані підстановки мають найбільший рівень нелінійності при забезпеченні 3-го ступеня перевизначеної системи.

Таблиця 2 – Характеристики S-блоків для перспективних перетворень

Характеристика	Номер S-блоку			
	1	2	3	4
Мінімальне значення нелінійності БФ	104			
Мінімальний алгебраїчний степінь БФ	7			
Макс. значення табл. розпод. різн. (ДК)	8			
Макс. значення табл. лін. апрокс. (ЛК)	24			
Степінь перевизначеної системи	3 (441 рівняння)			
Кількість циклів	4	4	6	4
Мінімальна довжина циклу	6	8	4	4

Під час аналізу властивостей блоків лінійного розсіювання доведено, що для симетричного блокового шифру на базі SPN-структури і подання внутрішнього стану у вигляді матриці розміром $n_c \times n_b$ елементів (кожен елемент за розміром співпадає із бієктивним S-блоком перетворення), раундове перетворення якого складається із шару S-блоків, шару перестановки і множення кожного стовпця на МДВ-матрицю (лінійні

перетворення), в ході виконання перестановки здійснюється перенесення n_f фрагментів із однієї колонки до іншої, нижня межа кількості активних S-блоків у 4-раундовій диференційній характеристиці або лінійній апроксимації дорівнює

$$\left(n_b+1\right)\cdot\left(n_f+1\right). \tag{19}$$

Порівняння МДВ-перетворення, що реалізоване в AES (розміром 32 біта, $n_b=4$), і перетворення на матриці розміром 64 біта ($n_b=8$) демонструє перевагу збільшеного варіанта. Ефективність збільшується із зростанням розміру блоку, і для 512-бітового перетворення збільшена матриця забезпечує 81 активний S-блок, в той же час як матриця, що використана в AES, на тому ж розмірі блоку може гарантувати лише 25 активних S-блоків (див. рис. 4).

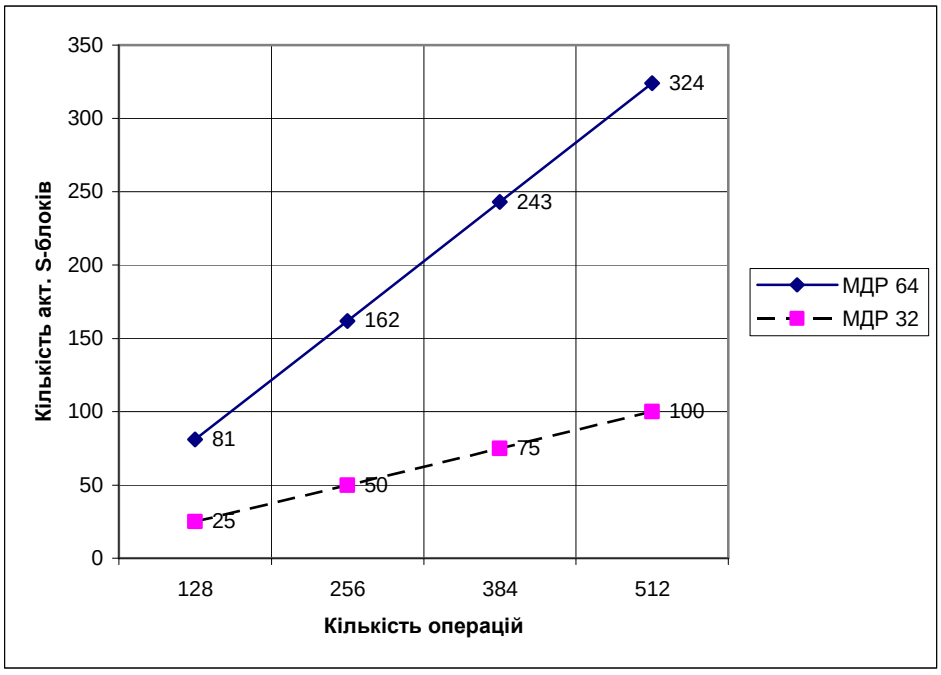

Рисунок 4 – Залежність кількості активних S-блоків від кількості операцій для розміру блоку 512 біт

Відповідно, збільшення розміру МДВ-матриці дає суттєвий виграш з точки зору забезпечення потрібних криптографічних властивостей, зберігаючи ефективність програмної та програмно-апаратної реалізації на сучасних та перспективних платформах.

Під час проведення експертизи блокових шифрів важливо виявлення небажаних властивостей криптографічних перетворень, які можуть бути вбудовані розробниками.

Однією з особливостей ланцюга Фейстеля та схеми Лей-Месси є відсутність вимоги щодо бієктивності раундової функції. Як наслідок, зашифрування і коректне розшифрування можливо на довільних S-блоках. У зв’язку з цим виникає питання оцінки криптографічної стійкості симетричних блокових шифрів, які побудовані на основі ланцюга Фейстеля або схеми Лей-Месси, в ході використання S-блоків із неповною множиною значень на виході (несюр’єктивними таблицями заміни).

Для алгоритму на основі ланцюга Фейстеля шифрований текст $\left(c^L, c^R\right)=\left(x_{n+1}^R, x_{n+1}^L\right)$ може бути виражений через відкритий текст $\left(p^L, p^R\right)=\left(x_1^L, x_1^R\right)$ таким чином (із урахуванням заміни місць напівблоків, що шифруються):

$$\begin{cases} c^L = p^R \oplus \left(\bigoplus\limits_{i=1}^{n/2} f_{2i}\left(x_{2i}^R, k_{2i}\right) \right) \\ c^R = p^L \oplus \left(\bigoplus\limits_{i=1}^{n/2} f_{2i-1}\left(x_{2i-1}^R, k_{2i-1}\right) \right). \end{cases} \tag{20}$$

Раундова функція $f\left(x_i, k_i\right)$ складається із початкового лінійного перетворення вхідного значення, складання із раундовим ключем, застосування вузлів нелінійної заміни і наступного лінійного перетворення:

$$f\left(x_i, k_i\right)=s\left(x_i \cdot E + k_i\right) \cdot L\,. \tag{21}$$

У розділі показано, що для блокового шифру, який побудований на основі ланцюга Фейстеля, із перетворенням відкритого тексту у шифртекст, що описується співвідношенням (20), застосуванням переставної матриці L у раундовій функції (21), *при невідомому ключі шифрування, але зі знанням дешифрувальною стороною довгострокового ключового елементу* (S-блоків) і наявності у неї критерію, що дозволяє відрізнити припустиме повідомлення від випадкової комбінації символів, обчислювальна складність розкриття (читання) одного блоку шифртексту дорівнює

$$\Theta=\left(\prod_{i=1}^{t}\theta_i^S\right)^2, \tag{22}$$

де θ_i^S – потужність множини підгрупи, що утворюється виходами i-го S-блоку раундової функції шифру; t – кількість S-блоків, які застосовуються паралельно у шарі нелінійного перетворення раундової функції блокового шифру.

У розділі також показано, що в тих самих умовах, але *за відсутності у дешифрувальної сторони довгострокового ключового елементу*, обчислювальна складність розкриття (читання) одного блоку шифртексту дорівнює

$$\Theta^S=\prod_{i=1}^{t}\left(\theta_i^S\,\frac{\left(2^{l/t}-1\right)!}{\left(2^{l/t}-\theta_i^S\right)!}\right). \tag{23}$$

де l – бітова розрядність виходу раундової функції блокового шифру.

Як ілюстрацію доцільно використати ГОСТ 28147-89, для якого, відповідно до стандарту, поставка заповнення таблиць блоку підстановки (ДКЕ) виконується уповноваженою організацією у встановленому порядку (на спеціальному носії).

Відповідно, S-блоки є таємними і невідомі як користувачу обладнання, що шифрує, так і зовнішньому криптоаналітику. Ключ шифрування генерується користувачем обладнання і недоступний як зовнішньому криптоаналітику, так і установі, яка виконала постачання ДКЕ.

Складність відновлення одного блоку відкритого тексту виключно по шифртексту без знання ключа для уповноваженої установи (Θ^{E}), яка формувала довгостроковий ключ, і для зовнішнього криптоаналітика (Θ^{SE}) залежно від порядку підгрупи, що утворена значеннями виходів S-блоків, наведена у табл.3.

Таблиця 3 – Порівняння складності відновлення одного блоку відкритого тексту

Порядок підгрупи	Складн. для уповнов. установи	Складн. для зовн. аналізу	Примітка
1	1	1	Відсутність шифрування
2	2^{16}	$2^{39,3}$	
4	2^{32}	$>2^{64}$	
8	2^{48}	$>2^{64}$	
16	2^{64}	$>2^{64}$	Норм. режим роботи

Таким чином, якщо користувачу засобів КЗІ із застосуванням ГОСТ 28147-89 нав’язується застосування таємних небієктивних (відповідно, несюр’єктивних) S-блоків, то, використовуючи підгрупи вихідних значень порядку 4 або більше, уповноважена установа має можливість порівняно просто отримати відкриті повідомлення із шифрованих без суттєвого ризику компрометації інформації шляхом дешифрування іншими установами.

Запропоновані у розділі методи дозволяють синтезувати перетворення, які забезпечують високий рівень криптографічної стійкості і швидкодії в ході програмної реалізації на процесорних архітектурах загального призначення. Додатково запропоновано методи, які дозволяють оцінити складність виконання криптоаналітичних атак на блокові шифри на базі ланцюга Фейстеля і схеми Лей-Мессі за умови наявності властивостей, що не були задекларовані розробником алгоритму.

У **п’ятому** розділі розроблено перспективні симетричні криптографічні перетворення: блоковий шифр та схема розгортання ключа для нього, ґеш-функція, виконано обґрунтування криптографічних властивостей, отримано оцінку стійкості щодо криптоаналітичних атак і показники швидкодії на поширених та перспективних програмних платформах.

У розділі сформульовано основні вимоги до перспективного блокового шифру:

- високий рівень криптографічної стійкості (складність реалізації відомих криптоаналітичних атак має бути вище складності атак переборного типу);
- швидкодія нового криптографічного перетворення має бути вищою, ніж у чинних стандартів, на сучасних і перспективних програмних платформах;
- шифр має забезпечувати ефективну реалізацію.

Відповідно до результатів розрахунків параметрів, які отримано у другому розділі, перспективний алгоритм шифрування підтримує наступні комбінації довжини ключа і розміру блоку (табл.4).

Таблиця 4 – Комбінації довжини ключа і розміру блоку перспективного шифру

Розмір блоку	Довжина ключа
128	128, 256
256	256, 512
512	512

На основі аналізу, який проведений у третьому розділі, як високорівнева конструкція перспективного шифру обрана SPN-структура. Крім того, додатковим аргументом на користь саме цієї конструкції служить неможливість використання прихованих властивостей, які описані у четвертому розділі (несюр'єктивні S-блоки призводять до небієктивності перетворення та, відповідно, неможливості коректного розшифрування в SPN-структурі).

Конструкція раундового перетворення обрана на основі результатів четвертого розділу, і складається з шару S-блоків розміром «8 біт – у 8 біт», з можливістю використання від одного до восьми різних S-блоків (рекомендовані чотири), та 64-бітної МДВ-матриці. Запропонований підхід дозволяє досягти високої швидкодії шифру при компактної реалізації, забезпечуючи достатній запас стійкості щодо відомих криптоаналітичних атак. Кількість циклів (ітерацій) криптографічного перетворення вибрано на основі запасу стійкості до різних видів криптоаналізу (див. нижче), і наведено у таблиці 5.

Таблиця 5 – Кількість циклів перспективного шифру

Довжина ключа , біт	Кількість циклів
128	10
256	14
512	18

Для запропонованого блокового шифру перетворення зашифрування представляється таким чином:

$$\Im = \eta_t^{(l)} \circ \psi \circ \tau^{(l)} \circ \pi' \circ \prod_{i=1}^{t-1} \left(\kappa_i^{(l)} \circ \psi \circ \tau^{(l)} \circ \pi' \right) \circ \eta_0^{(l)}, \qquad (24)$$

де $\kappa_i^{(l)}$ – операція додавання циклового ключа за модулем 2; $\eta_i^{(l)}$ – операція додавання циклового ключа за модулем 2^{64}; π' – шар нелінійного перетворення (S-блоки); $\tau^{(l)}$ – циклічний зсув рядків внутрішнього стану шифру; ψ – множення кожного вектора-стовпця матриці стану шифру на МДВ-матрицю (основне лінійне перетворення); t – кількість циклів перетворення, що шифрує; l – розмір блоку шифру.

Для забезпечення необхідних криптографічних та експлуатаційних властивостей в розділі запропоновано основні та додаткові вимоги до схеми розгортання ключів перспективного шифру:

- нелінійна залежність кожного біта кожного раундового ключа від кожного біта ключа шифрування;
- циклові ключі істотно відрізняються й мають складну нелінійну залежність;
- схема розгортання забезпечує захист від відомих криптоаналітичних атак;
- відсутність слабких ключів, за яких погіршуються криптографічні властивості;
- обчислювальна складність формування всіх циклових ключів не перевищує складності зашифрування трьох блоків;
- простота реалізації;
- неможливість (висока обчислювальна складність) отримання ключа шифрування за одним або декількома цикловими ключами;
- можливість формування циклових ключів у довільному порядку (однакова обчислювальна та просторова складність для зашифрування і розшифрування).

Запропонована схема розгортання ключів виконується в два етапи.

На першому етапі роботи схеми розгортання формується допоміжний ключ K_t із ключа шифрування K і константи, яка залежить від розміру блоку і довжини ключа, на основі такої процедури:

$$\Xi_K^{(l,k)} = \psi \circ \tau^{(l)} \circ \pi' \circ \eta_K^{(l)} \circ \psi \circ \tau^{(l)} \circ \pi' \circ \kappa_K^{(l)} \circ \psi \circ \tau^{(l)} \circ \pi' \circ \eta_K^{(l)}. \qquad (25)$$

На другому етапі формуються циклові ключі з ключа шифрування K і проміжного ключа K_t :

$$\Re_K^{(l,k)} = \eta_{K_t + tmv_i}^{(l)} \circ \psi \circ \tau^{(l)} \circ \pi' \circ \kappa_{K_t + tmv_i}^{(l)} \circ \psi \circ \tau^{(l)} \circ \pi' \circ \eta_{K_t + tmv_i}^{(l)}. \qquad (26)$$

Окрім забезпечення односпрямованості схеми розгортання, під час розробки розгортання додатково враховувалася необхідність руйнування симетрії шифрувального перетворення і формування унікальної послідовності циклових ключів для кожної комбінації розміру блоку і довжини ключа. Повна специфікація розробленого блочного шифру (режим простої заміни) наведена в додатку до дисертації.

Для забезпечення високої обчислювальної складності отримання ключа шифрування за одним або декількома цикловими ключами функція розгортання реалізована як неін’єктивне відображення, що теоретично допускає існування еквівалентних ключів.

Відповідно, для отримання показників стійкості щодо атак переборного типу, в розділі отримано аналітичну оцінку співвідношення потужностей множин циклових ключів та ключів шифрування через рекурентне співвідношення (у рамках допущення про схему розгортання як про випадкове відображення) :

$$s_l = s_{l-1} + s_u(1 - s_{l-1}), \text{ де } s_u = s_1 = \left(1 - \frac{1}{e}\right) \approx 0{,}632. \qquad (27)$$

У розділі показано, що потужність множини значень послідовностей циклових ключів запропонованої схеми розгортання ключів практично збігається з потужністю

множини значень ключа шифрування (від 0,9817 до 0,9999 залежно від розміру блоку і довжини ключа). Відповідно, неін'єктивність схеми розгортання, яка необхідна для реалізації властивості односпрямованості, не дозволяє криптоаналітику зменшити складність атак переборного типу, водночас забезпечуючи додаткову стійкість до низки методів криптографічного аналізу, спрямованого, в тому числі і на реалізацію перетворення.

Складність найефективніших криптоаналітичних атак і найбільшу кількість циклів, до яких вони можуть бути застосовані, наведено в табл. 6 (розмір блоку 128 біт, 10 циклів).

Таблиця 6 – Складність найефективніших криптоаналітичних атак для блокового шифру (розмір блоку і довжина ключа 128 біт, 10 циклів перетворення)

Методи криптоаналізу	Мін. кількість циклів, за яких шифр стійкий	Показники атак		
		Макс. кількість циклів	Обчисл. складність, екв. оп. шифрув.	Пам'ять, байт
Диференційний	5	4	2^{55}	
Лінійний	5	3	$2^{52,8}$	
Усічен. диф.	4	3		
Інтегральний	6	5	2^{97}	2^{33+4}
Нездійсн. диф.	6	5	2^{62}	2^{66}
Бумеранг	5	4	2^{120}	

Аналогічні результати отримано і для розміру блоку 256 і 512 біт.

З результатів проведеного аналізу випливає, що перспективний шифр забезпечує захист до всіх розглянутих методів криптоаналізу і достатній запас стійкості. Для вихідних послідовностей перетворення блокового алгоритму і його схеми розгортання було проведено статистичне тестування згідно з методикою NIST STS.

Статистичний профіль вихідної послідовності схеми розгортання для розміру блоку 128 біт і довжини ключа 128 біт наведено на рис.5 (горизонтальні лінії визначають поріг проходження кожного тесту). Для інших перевірених послідовностей отримано аналогічні результати, які додатково підтверджують отримані теоретичні оцінки криптографічної стійкості. Для інших співвідношень розміру блоку і ключа отримані такі ж оцінки.

Порівняння продуктивності розробленого шифру (всі комбінації розміру блоку і довжини ключа) з AES-128, AES-256, ДСТУ ГОСТ 28147:2009 і блоковим шифром із СТБ 34.101.31-2011 на 64-бітовій платформі наведено на рис.6.

Продуктивність перспективного блокового шифру «Калина» на 64-бітовій платформі значно вище, ніж у чинного в Україні та Росії стандарту ГОСТ 28147-89, а також стандарту республіки Білорусь СТБ 34.101.31-2011. На цій самій платформі «Калина» має перевагу в продуктивності і порівняно з алгоритмом AES з аналогічною довжиною ключа (водночас забезпечуючи значно більший запас криптографічного стійкості).

Криптографічна ґеш-функція повинна відповідати таким основним вимогам:

- односпрямованість;

– захист від атаки другого прообразу;
– колізійна стійкість;
– стійкість до атаки збільшення довжини повідомлення;
– забезпечення високої швидкодії, простоти і компактності реалізації.

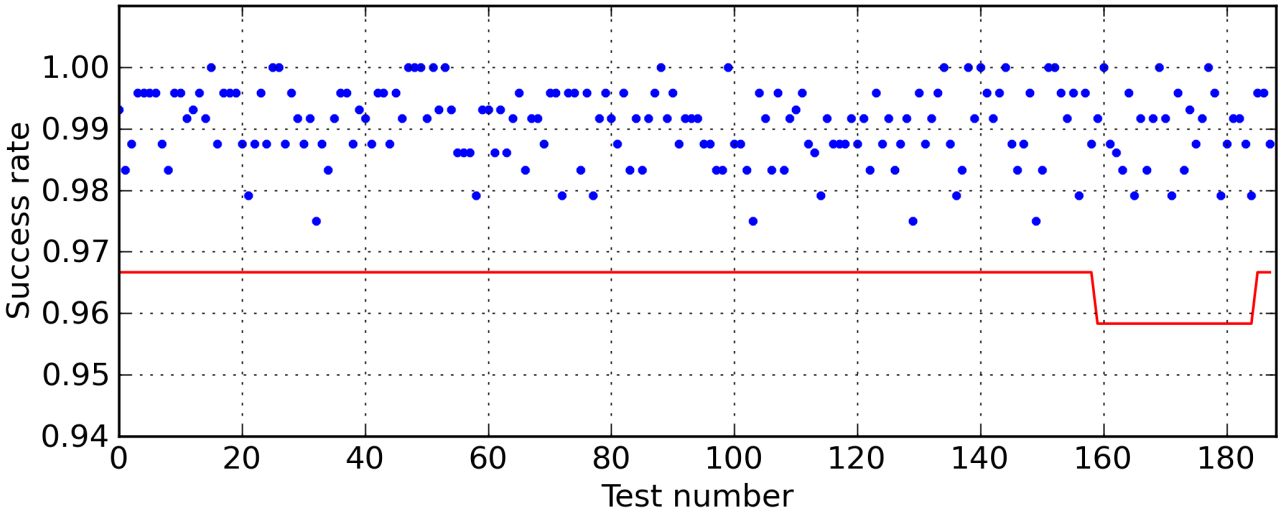

Рисунок 5 – Статистичний профіль вихідної послідовності схеми розгортання ключів для розміру блоку 128 біт і довжини ключа 128 біт

Відповідно до результатів другого розділу, перспективне перетворення підтримує довжину ґеш-коду 256, 384 та 512 біт (з можливістю завдання інших проміжних значень).

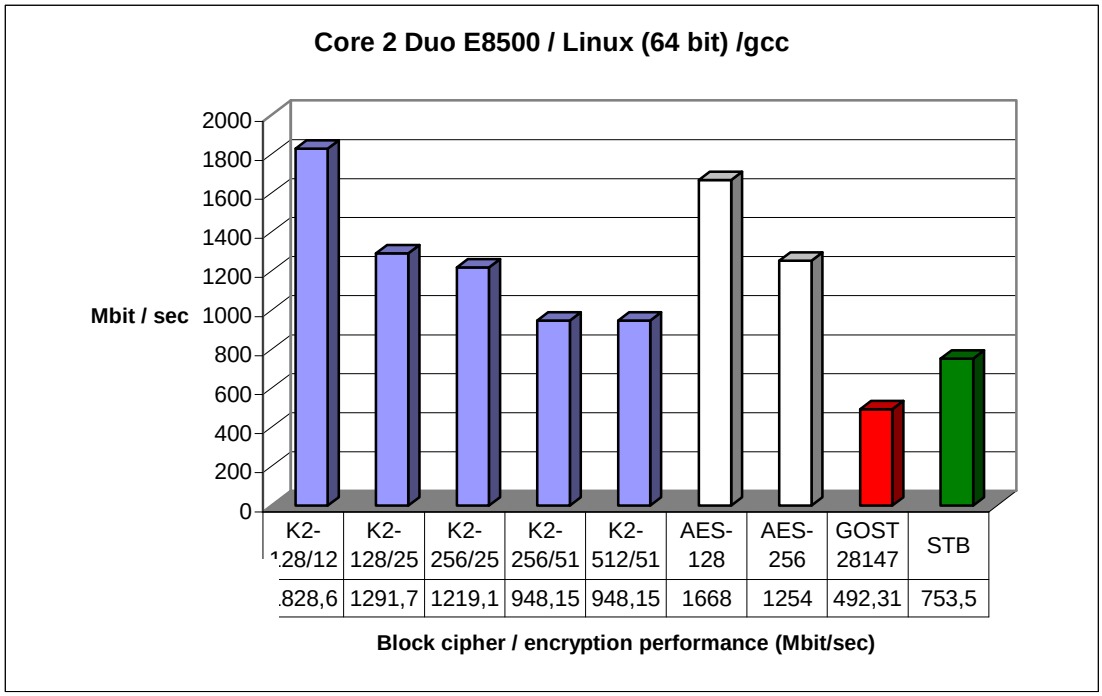

Рисунок 6 – Порівняння продуктивності блокових шифрів на 64-бітовій платформі

Як загальна конструкція ґеш-функції використовується найбільш поширена схема Меркля-Дамгарда з додатковим завершальним перетворенням. Ґеш-функція побудована на основі блокового шифру, і з відомих схем, що мають схожі властивості і швидкодію, обрана найбільш поширена схема Девіса-Мейєра, яка застосовується,

зокрема, в ґеш-функціях SHA-1 і SHA-2, з блоковим шифром конструкції Івена-Мансура на випадкових перестановках.

Обчислення ґеш-функції відбувається відповідно до ітеративної процедури:

$$\begin{aligned} &h_0 = IV, \\ &h_\nu = T_l^{\oplus}(h_{\nu-1} \oplus m_\nu) \oplus T_l^{+}(m_\nu) \oplus h_{\nu-1}, \quad \nu = 1,2,...,k,. \\ &H(IV, M) = R_{l,n}\left(T_l^{\oplus}(h_k) \oplus h_k\right), \end{aligned} \tag{28}$$

де IV – вектор ініціалізації; $T_l^{\oplus}$, T_l^{+} – рандомізуючі бієктивні перетворення; $R_{l,n}(x)$ – завершуюча функція.

Для ефективності програмної та апаратної реалізації перестановки $T_l^{\oplus}$ і T_l^{+} мають бути подібними, але, водночас, для забезпечення необхідних криптографічних властивостей (захисту від колізій), повинні мати істотні відмінності.

Для вирішення цього протиріччя запропонована наступна конструкція. Циклове перетворення, яке є ефективним для програмної та апаратної реалізації (через таблиці підстановки), є загальним для $T_l^{\oplus}$ і T_l^{+}, і заснованим на перетворенні блокового шифру. Операція введення циклових констант (ключів), і самі константи є різними для обох перетворень.

До циклових констант $T_l^{\oplus}$ накладається єдина вимога (унікальність для відсутності подібності раундів), і ці значення обираються, виходячи з простоти програмно-апаратної реалізації. Як операція введення циклових констант для перетворення T_l^{+} вибрано додавання за модулем 2^{64}, яке є ефективним як при програмній, так і при апаратній реалізації, і не вимагає додаткової пам’яті в кеші.

З точки зору забезпечення криптографічних властивостей, для байт-орієнтованого перетворення при використанні операції модульного додавання необхідно формування максимальної кількості незалежних один від одного переносів для захисту від диференціального, лінійного криптоаналізу, усічених диференціалів тощо.

Для вибору оптимального значення було отримано математичне сподівання кількості взаємно незалежних переносів, що з’являються у 64-бітовому суматорі, залежно від довжини груп 11...1 і 00...0 (у двійковому поданні) у цикловій константі, за умови, що другий аргумент – випадкова величина, яка розподілена відповідно до рівномірного закону:

$$En_c = \sum_{i=1}^{\frac{n}{k+l}} i \cdot \left(\left(1-2^{-k}\right)\left(1-2^{-l}\right)\right)^i \cdot \left(1-\left(1-2^{-k}\right)\left(1-2^{-l}\right)\right)^{\frac{n}{k+l}-i}, \tag{29}$$

де n – розрядність двійкового суматора; k – кількість одиничних біт у групі; l – кількість нульових біт у групі.

Таким чином, виникає оптимізаційна задача цілочисельної максимізації функції математичного сподівання кількості незалежних переносів:

$$En_C(k,l) \to \max,\ n = const,\ k,l \in Z^+. \qquad (30)$$

Оскільки залежність має досить складний нелінійний характер, екстремум у цілих числах був знайдений за допомогою системи комп'ютерної алгебри: максимум функції математичного сподівання кількості незалежних переносів (29) для фіксованої розрядності суматора $n = 64$ і цілих аргументів $k,l \in Z^+$ досягається при $k = 4$ і $l = 4$, на підставі чого була обрана циклова константа 0xF0F0F0F0F0F0F0F3.

Доказ стійкості компонентів перспективної ґеш-функції до різних видів криптоаналізу аналогічний проведеному доказу для блокового шифру. Запропонована перспективна криптографічна ґеш-функція «Купина» захищена від відомих методів криптоаналізу і забезпечує достатній запас стійкості.

Для вихідних послідовностей ґеш-функції, як і для блокового шифру, було проведено статистичне тестування згідно з методикою NIST STS . Всі тести успішно пройдені, і отримано статистичні профілі аналогічні наведеним на рис.5.

Порівняння швидкодії перспективної криптографічної ґеш-функції (два розміри блоку) виконувалося з такими алгоритмами: ГОСТ 34.311-95 (чинний в Україні стандарт), ГОСТ Р 34.11-12 «Стрибог», Keccak 256,-512 (переможець конкурсу NIST SHA3), SHA 256,-512 (чинний стандарт США). Білоруський стандарт ґешування із СТБ 34.101.31-2011 не розглядався як напевно значно повільніший. Продуктивність замірювалась як для 64-бітових, так і 32-бітових реалізацій під Windows і Linux.

За результатами вимірювання швидкодія розробленого перспективного перетворення вище, ніж у чинного стандарту ГОСТ 34.311-95 та російського стандарту ГОСТ 34.11-12 (Стрибог), але нижче, ніж у стандартів США SHA-2 і SHA-3 (Keccak), що обумовлено відмовою від експериментальних конструкцій і використанням консервативного підходу, який використовує максимально перевірені конструкції з достатнім запасом криптографічної стійкості, під час розробки ґеш-функції.

Таким чином, практичне застосування запропонованих методів дозволило синтезувати високопродуктивний блоковий шифр та ґеш-функцію, які забезпечують високий і надвисокий рівень криптографічної стійкості.

У **додатках** наведено опис методу реалізації криптоаналітичної атаки на потоковий шифр A5/1, який застосовується у мережах мобільного зв’язку; специфікація перспективного блокового шифру «Калина»; результати статистичного тестування вихідних послідовностей блокового шифру; специфікація перспективної ґеш-функції «Купина»; акти впровадження результатів дисертаційних досліджень.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну наукову проблему синтезу симетричних криптографічних перетворень в рамках об’єктивного протиріччя: необхідності забезпечення високого рівня криптографічної стійкості щодо методів криптоаналізу, високої продуктивності і компактності реалізації в умовах обмеження часових, дослідницьких і обчислювальних ресурсів під час розробки перспективних алгоритмів. Найбільш важливі наукові та практичні результати, отримані під час проведення дисертаційних досліджень, полягають у наступному.

1. Вперше запропоновані математичні моделі для низки переборних атак на основі таблиць передобчислень дозволили обґрунтувати необхідність істотного збільшення потужності множин невідомого порушнику стану криптосистеми (розмір блоку і довжина ключа блокового шифру, розмір внутрішнього стану ґеш-функції та ін).

2. Для атаки, що використовує таблиці передобчислень на основі точок розрізнення, доведено, що складність побудови експоненційно залежить від кількості рядків у таблиці і від довжини кожного ланцюга, яка, в свою чергу, експоненційно залежить від кількості біт у точці розрізнення. Ймовірність успіху лінійно залежить від кількості рядків і їх довжини. В ході побудови рядка таблиці для пошуку зациклення доцільно користуватися запропонованим алгоритмом, який має складність $O(1)$, замість відомого зі складністю $O(n \cdot \log n)$.

3. Вперше розроблено математичну модель атак на основі rainbow-таблиць в умовах, коли потужність множини врахованих значень близька до потужності множини значень невідомого стану криптографічного перетворення. В рамках запропонованої моделі доведено, що складність побудови rainbow-таблиць експоненційно залежить від кількості рядків у таблиці і їх довжини (кількості різних функцій переходу). Ймовірність успіху лінійно залежить від розміру таблиці. Показано, що цей метод має найменшу складність попереднього етапу, але оперативний етап вимагає найбільшого часу в порівнянні з іншими типами розглянутих таблиць.

4. Вперше розроблено метод оцінки складності криптоаналізу на основі fuzzy-rainbow-таблиць на базі математичої моделі, яка розглядає умови, коли потужність множини врахованих значень близька до потужності множини всіх значень невідомого стану криптографічного перетворення. Показано, що цей метод дозволяє отримати оптимальне компромісне рішення для досягнення високої ймовірності успіху, порівняно малий час криптоаналізу і прийнятний рівень складності на етапі передобчислень. Розроблений метод застосування декількох fuzzy-rainbow-таблиць дозволяє добитися високої ймовірності успіху на оперативному етапі, порівняно малого часу криптоаналізу і прийнятого рівня складності на попередньому етапі. Додаткове експоненціальне зниження складності передобчислень можна досягти за рахунок лінійного збільшення складності проведення етапу криптоаналізу.

5. Показано, що в рамках розробленої моделі криптоаналітичної атаки, коли криптографічне перетворення експлуатується протягом 30 років, причому кожну секунду легітимні користувачі формують 10 тис. криптограм, і необхідно забезпечити захист від порушника третього рівня (спеціальної служби економічно і технологічно розвиненої держави), який володіє суперкомп'ютером на основі напівпровідникової технології, що виконує $5 \cdot 10^9 \cdot 10^8 = 5 \cdot 10^{17}$ операцій прямого криптографічного перетворення за секунду, з імовірністю розкриття не більше 10^{-9}, для забезпечення стійкості криптографічного примітиву:

- довжина ключа перспективного блокового симетричного алгоритму шифрування має бути не менше 256 бітів;
- для ґеш-функцій та кодів автентифікації повідомлень необхідно мати вихідне значення довжиною не менше 256 бітів.

З урахуванням досить тривалого терміну експлуатації, протягом якого можуть бути запропоновані нові ефективні методи криптоаналізу і технічні засоби, необхідний додатковий запас стійкості, який задається параметрами перспективного симетричного криптографічного примітиву.

6. Для ланцюга Фейстеля на основі випадкових функцій вперше:

- для трьох раундів перетворення отримано точну оцінку теоретично досяжної верхньої межі ефективності розрізнення та її апроксимацію, що має низьку похибку. Показано, що при оптимальній кількості запитів можливе досягнення переваги розрізнення, близької до 1;
- для чотирьох раундів сформульовано і доведено теорему, що дозволяє отримати точну оцінку і апроксимацію переваги алгоритму розрізнення, для якого можливе досягнення переваги, близької до 0,25, при оптимальної кількості запитів.

7. Для ланцюга Фейстеля на основі випадкових перестановок вперше доведено теореми, що дозволяють отримати точну оцінку і апроксимацію переваги алгоритмів розрізнення. Складність розрізнення однакова для трьох і чотирьох раундів перетворення, і зі збільшенням кількості запитів перевага розрізнення прагне до 1.

8. Для 3-раундової (і більше) схеми Лей-Массі з випадковими функціями в раундовому перетворенні вперше сформульовано критерії розрізнення і доведено теореми, які дозволяють отримати точну оцінку і апроксимацію верхньої межі переваги кращого гіпотетичного алгоритму розрізнення; для кращого відомого алгоритму отримано точну оцінку і апроксимацію переваги, яка може досягати значення, близького до 0,25, при оптимальній кількості запитів. Аналогічний результат отриманий для 3-раундової схеми Лей-Массі з випадковими перестановками в раундовому перетворенні.

9. Порівняння теоретично досяжних верхніх меж ефективності розрізнення показує перевагу схеми Лей-Массі в порівнянні з ланцюгом Фейстеля (конструкції як на основі випадкових функцій, так і випадкових перестановок).

10. Вперше доведено теорему про нерозрізнюваність 3-циклової SPN-структури та випадкової перестановки. Показано, що для критерію розрізнення випадкової перестановки і шифрувального перетворення SPN-структура є кращим варіантом побудови перспективного симетричного блокового шифру, який забезпечує високий рівень стійкості.

11. Запропоновано метод дешифрування для алгоритмів, побудованих на основі ланцюга Фейстеля, який заснований на застосуванні таємних S-блоків і дозволяє виконувати безключове читання криптограм уповноваженою організацією (що володіє тільки секретними S-блоками і простим критерієм розрізнення допустимого повідомлення від випадкової комбінації символів), при цьому забезпечивши захист від читання третьою стороною, яка не знає як ключ шифрування, так і набір S-блоків, який був використаний.

Застосування розробленого методу для ГОСТ 28147-89 показало, що несюр'єктивні S-блоки з порядком підгрупи вихідних значень, рівному 4 або 8, дозволяють уповноваженій організації порівняно просто отримати відкриті повідомлення з шифрованих без значного ризику компрометації інформації шляхом дешифрування іншими організаціями.

12. Розроблений блоковий шифр підтримує нормальний, високий і надвисокий рівень стійкості (розмір блоку і ключа довжиною 128, 256 і 512 біт), побудований на основі SPN-конструкцій, з S-блоками, які орієнтовані на захист від диференціального, лінійного і алгебраїчного криптоаналізу, і лінійним перетворенням на базі 64-бітової МДВ-матриці. Алгоритм шифрування має ефективну реалізацію і забезпечує захист до всіх розглянутих методів криптоаналізу (диференційний, лінійний, інтегральний, нездійсненні диференціали тощо) і має достатній запас стійкості: для 128-бітового ключа перетворення є стійким на 6 циклах із 10; для 256-бітового ключа – 7 циклах з 14, для 512-бітового ключа – 9 циклах з 18.

13. Схема розгортання ключа перспективного шифру відповідає вимогам нелінійності, захисту від криптоаналітичних атак і відсутності слабких ключів. Конструкція схеми розгортання заснована на циклових перетвореннях, обчислювальна складність формування всіх циклових ключів не перевищує складності зашифрування трьох блоків, при цьому обчислювальна та просторова складність однакова для зашифрування і розшифрування.

Розроблена неін’єктивна схема забезпечує стійкість до переборних атак на рівні традиційних ін’єктивних схем, водночас забезпечуючи додатковий захист від ряду криптоаналітичних атак, в т.ч. на реалізацію криптографічного алгоритму.

15. Розроблена ґеш-функція підтримує нормальний, високий і надвисокий рівень стійкості (рекомендовані довжини ґеш-значень – 256, 384 і 512 біт), і побудована із застосуванням модифікованої схеми Меркля-Дамгарда і конструкції Девіса-Мейєра. Як внутрішнє перетворення застосовано схему Івена-Мансура на основі запропонованого перспективного блокового шифру. Ґеш-функція, як і блоковий шифр в її основі, має достатній запас стійкості та ефективну реалізацію, з конструктивними елементами, спільними для ґеш-функції і блокового шифру.

16. Продуктивність розробленого блокового шифру «Калина» (1828 Мбіт/с) на тестовій 64-бітовій платформі значно вище, ніж у чинного в Україні та Росії стандарту ГОСТ 28147-89 (492 Мбіт/с), а також стандарту республіки Білорусь СТБ 34.101.31-2011 (753 Мбіт/с). На цій же платформі «Калина» має перевагу в продуктивності і порівняно з алгоритмом AES (1668 Мбіт/с) з аналогічною довжиною ключа (водночас забезпечуючи більший запас криптографічної стійкості). Продуктивність перспективної ґеш-функції «Купина» вище, ніж у чинного в Україні стандарту ГОСТ 34.311-95 та російського стандарту ГОСТ Р 34.11-12 «Стрибог», але нижче, ніж у стандартів США SHA-2 і SHA-3 (Keccak), при цьому отримані результати є оптимальними в рамках відмови від експериментальних конструкцій і використання консервативного підходу, який використовує максимально перевірені конструкції з достатнім запасом криптографічної стійкості.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: коллективная монография / [Р.В. Олейников, В.М. Безрук и др.]. – Х.: Компания СМИТ, 2013. – 397 с.

2. Олійников Р.В. Аналіз властивостей алгоритмів блокового симетричного

шифрування (за результатами міжнародного проекту NESSIE) / Р.В. Олійников, Горбенко І.Д., Г.М. Гулак, В.І. Руженцев // Радиотехника. - 2005.- №141. - С.7-24.

3. Олійников Р.В. Критерии случайности таблиц подстановок алгоритма шифрования ГОСТ 28147 / Р.В. Олейников, В.И. Долгов, В.И. Руженцев, А.И. Шумов // Прикладная радиоэлектроника. - 2006. - №5 (1). - С.127-133.

4. Олійников Р.В. Перспективний блоковий симетричний шифр «Мухомор»: основні положення та специфікація / Р.В. Олійников, І.Д. Горбенко, М.Ф. Бондаренко, В.І. Руженцев// Прикладная радиоэлектроника. - 2007. - №6(2). - С.147-156.

5. Олейников Р.В. Результаты анализа алгоритма шифрования ADE / Р.В. Олейников, В.И. Руженцев, М.С. Михайленко, А.Б. Небывайлов // Прикладная радиоэлектроника. - 2008. - №7 (3). - С.210-214.

6. Олейников Р.В. Подстановочные конструкции современных симметричных шифров / Р.В. Олейников, В.И. Долгов, И.В. Лисицкая // Радіоелектронні і комп'ютерні системи. - 2009. - №6 (40). - С.97-115.

7. Олейников Р.В. Построение переопределенной системы уравнений для описания алгоритма шифрования «Лабиринт» / Р.В. Олейников, А.В. Казимиров // Прикладная радиоэлектроника. - 2009. - №8 (3). - С.247-251.

8. Казимиров А.В. Алгебраические свойства схемы разворачивания ключей блочного симметричного шифра «Калина» / А.В. Казимиров, Р.В. Олейников // Радіоелектронні і комп'ютерні системи. - 2010. - №6 (40). - С. 61-66.

9. Олійников Р.В. Оцінка стійкості симетричних блокових шифрів на базі ланцюга Фейстеля при використанні несюр'єктивних S-блоків / Р.В. Олійников // Спеціальні телекомунікаційні системи та захист інформації. - 2010. - №1 (17). - С. 77-84.

10. Олейников Р. В. Выбор S-блоков для симметричных криптографических алгоритмов на основе анализа алгебраических свойств / Р. В. Олейников, А.В. Казимиров // Вісн. Харк. нац. ун-ту. Сер. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління . - 2010. - № 925. - С. 79–86.

11. Горбенко И.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / И.Д. Горбенко, В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Прикладная радиоэлектроника. - 2010. - №9(3). - С. 312 – 320.

12. Олійников Р.В. Криптоаналіз на основі передобчислень: уточненення ефективності rainbow-таблиць / Р.В. Олійников // Спеціальні телекомунікаційні системи та захист інформації. - 2010. - №2 (18). - С. 26-32.

13. Олейников Р.В. Сравнение функций разворачивания ключа симметричных блочных шифров / Р.В. Олейников, А.В. Казимиров // Защита информации. Сборник научных трудов Национального авиационного университета. - 2010. - №17. - С. 162-165.

14. Казимиров А.В. Оценка количества допустимых внутренних состояний в поточном алгоритме MICKEY / Р.В. Олейников, А.В. Казимиров // Прикладная радиоэлектроника. - 2011. - №10(2). - С.112-115.

15. Oliynykov R. V. An impact of S-box boolean function properties to strength of modern symmetric block ciphers / R. V. Oliynykov, O. V. Kazymyrov // Радиотехника. -

2011.- №166. - С. 11-17.

16. Олейников Р.В. Уточнение эффективности различения цепи Фейстеля и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // Радиотехника. - 2011.- №167. - С. 190-202.

17. Oliynykov R.V. Linear transformation properties of ZUC cipher / R.V. Oliynykov, R.I. Kiyanchuk // Вісник Харківського національного університету. - «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». - 2012. - №1015. - С.155-166.

18. Oliynykov R.V. Perspective symmetric block cipher optimized for hardware implementation / R.V. Oliynykov, R.I. Kiyanchuk // Радіоелектронні і комп'ютерні системи. - 2012. - №5 (57). - С.42-47.

19. Олейников Р.В. Оценка сложности различения схемы Лей-Месси и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // Прикладная радиоэлектроника. - 2012. - №11(2). - С.152-159.

20. Казимиров А.В. Использование векторных функций при генерации подстановок для симметричных криптографических преобразований / А.В. Казимиров, Р.В. Олейников // Системи обробки інформації. - 2012.- №6 (104).- С. 97 – 102.

21. Казимиров А.В. Криптоанализ шифра Mickey на основе анализа внутренних состояний / А. В. Казимиров, Р. В. Олейников // Радиотехника. - 2012. - №171.- С. 24-28.

22. Долгов В.И. Исследование показателей случайности блочного шифра из белорусского стандарта СТБ 34.101.31-2011 / В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Специальные телекомуникационные системы и защита информации. - 2012. - №2 (22). - С. 38–51.

23. Казимиров А.В. Метод построения нелинейных узлов замены на основе градиентного спуска / А. В. Казимиров, Р. В. Олейников // Радиотехника. - 2013. - №172. - С. 104-108.

24. Олейников Р.В. Исследование свойств подстановок ГОСТ 28147-89, построенных на основе анализа свойств координатных функций. / Р.В. Олейников, И.В. Лисицкая // Науково-технічний збірник «Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні». - 2002. - №5. - С.123-129.

25. Основные принципы проектирования, оценка стойкости и перспективы использования в Украине алгоритма шифрования AES. / Р.В. Олейников, Г.Н. Гулак, И.Д. Горбенко, А.И. Шумов // Науковотехнічний збірник «Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні».- 2003. - №7. - С.14-24.

26. Results of Ukrainian national public cryptographic competition / R.V. Oliynykov, I.D. Gorbenko, V.I. Dolgov, V.I. Ruzhentsev. Tatra Mountains Mathematical Publications. - 2010.- №47. - P. 99-114.

27. Разработка требований и принципы проектирования перспективного симметричного блочного алгоритма шифрования / И.Д. Горбенко, В.И. Долгов, Р.В. Олейников [та ін.] // Известия ЮФУ. Технические науки. — Россия, Таганрог: Изд-во ТТИ ЮФУ (Таганрогского технологического института Южного федерального университета). - 2007. - №1 (76). - С. 238-241.

28. Oliynykov R.V. A new approach of key schedule construction for symmetric block ciphers / R.V. Oliynykov, V.I. Ruzhentsev // Известия ЮФУ. Технические науки. Россия, Таганрог: Издво ТТИ ЮФУ (Таганрогского технологического института Южного федерального университета). - 2010. - №11(112). - С. 156-161.

29. Олейников Р.В. Оценка стойкости симметричных блочных шифров на базе цепи Фейстеля при использовании несюръективных S-блоков / Р.В. Олейников // Информационное противодействие угрозам терроризма. Научно-практический журнал. - 2013. - №20. - С.121-128.

30. Пат. 89382 Україна, UA89382. Спосіб шифрування двійкових блоків даних «Калина» / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев; Заявник та патентовласник АТ «ІІТ».— № H04L 9/06 ; заявл. 26.03.2007 ; опубл. 15.01.2010.

31. Пат. 89651 Україна, UA89651. Спосіб шифрування двійкових блоків даних (варіанти) / Р.В. Олійников, В.І. Долгов, І.В. Лисицька; Заявник та патентовласник АТ «ІІТ».— № H04L 9/14 ; заявл. 21.05.2007; опубл. 25.02.2010.

32. Пат. 103726 Україна, UA103726, МПК (2013.1). Спосіб шифрування двійкових блоків даних / Р.В. Олійников, І.Д. Горбенко, В.І. Руженцев, О.В. Казимиров, Ю.І. Горбенко. Заявник та патентовласник АТ «ІІТ».— H04L 12/00, H04L 9/00. заявл. 18.10.2012; опубл. 11.11.2013, бюл.№21.

Наукові праці, що додатково характеризують результати дисертації:

33. Олійников Р.В. Порівняльний аналіз алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE) / Р.В. Олійников, І.Д. Горбенко, Г.М. Гулак, В.І. Руженцев // Радиотехника. - 2005.- №141. - С.25-30.

34. Олійников Р.В. Принципи побудування та властивості блокових симетричних IDEA подібних шифрів / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев // Прикладная радиоэлектроника. - 2007.- №6 (2). - С.158-173.

35. Олійников Р.В. Обгрунтування вимог та розробка основних рішень з побудування та властивості перспективного БСШ «Мухомор». / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев // Прикладная радиоэлектроника. - 2007.- №6 (2). - С.174-185.

36. Олійников Р.В. Криптостійкість шифру «Мухомор» / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев // Прикладная радиоэлектроника. 2007. - №6 (2). - С.186-194.

37. Олійников Р.В. Перспективний блоковий симетричний шифр «Калина» основні положення та специфікація / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев // Прикладная радиоэлектроника. - 2007. - №6 (2). - С.195-208.

38. Олійников Р.В. Принципи побудування та властивості блокового симетричного симетричного шифру «Калина» / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев // Прикладная радиоэлектроника. - 2007. - №6 (2). - С.208-216.

39. Олійников Р.В. Криптостійкість шифру «Калина» / Р.В. Олійников, І.Д. Горбенко, В.І. Долгов, В.І. Руженцев // Прикладная радиоэлектроника. 2007. - №6 (2). - С.217-229.

40. Олейников Р.В. Обоснование стойкости стандарта шифрования FIPS197 к атаке усеченных дифференциалов / Р.В. Олейников, В.И. Руженцев // Прикладная радиоэлектроника. - 2008. - №7 (3). - С.215-227.

41. Олейников Р.В. Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. - 2010. - №9(3). - С.326-333.

Наукові праці апробаційного характеру:

42. Ruzhentsev V.I. Properties of Linear Transformations for Symmetric Block Ciphers on the basis of MDS-codes / V.I. Ruzhentsev, R.V. Oliynykov // Proc. of 6th IEEE Conference Network Architecture and Information Systems Security.- France : La Rochelle. May 18-21, 2011. La Rochelle: 2011. - P. 193-196.

43. Oliynykov R. Improvement for Distinguisher Efficiency of the 3 Round Feistel Network and a Random Permutation / R. Oliynykov, I. Gorbenko, V. Dolgov, D. Kaidalov // Proc. of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Czech Republic, Prague: September 15-17, 2011. - Prague: 2011. - P. 737 – 747.

44. Олейников Р.В. Анализ цикловых свойств перспективного блочного симметричного алгоритма шифрования «Калина-2» / Р.В. Олейников, И.Д. Горбенко // Вторая Международная научно-техническая конференция «Компьютерные науки и технологии «КНиТ2011», 3-7 октября 2011 г., Белгород, Россия. Материалы конференции. - Б.: Белгородский государственный национальный исследовательский университет, 2011. – С. 496-500.

45. Kazymyrov O. A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent / V. Kazymyrova, O. Kazymyrov, R. Oliynykov // Proc. of the Second workshop on Current Trends in Cryptology (CTCrypt 2013), Ekaterenburg, Russian, June 23–24, 2013. – Ekaterenburg, 2013. – P. 107–115.

46. Oliynykov R. Construction of MDS-matrix for linear transformation of symmetric block ciphers / R. Oliynykov, V. Ruzhentsev, V. Stupak // Proc. of the X-th IEEE International Conference on Modern Problems of Radioengineering, Telecommunications and Computer Science: TCSET'2010: Lviv, February 23-27, 2010. Lviv: Publishing House of Lviv Polytechnic, 2010. - P.284-285.

47. Олейников Р.В. Криптографические свойства булевых функций / Р.В. Олейников, А.И. Шумов // 7-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке», Харьков, 22-24 апреля 2003.: Материалы конференции. - Х.: ХНУРЭ, 2003. - С.79-80.

48. Олейников Р.В. Подходы к выполнению линейного криптоанализа ГОСТ 28147-89 / Р.В. Олейников, А.И. Шумов // Шоста Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». Київ, 13-16 травня 2003. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2003. - С.93-94.

49. Олейников Р.В. Построение переопределjнной системы уравнений для описания алгоритма шифрования AES / Р.В. Олейников, А.И. Шумов, В.И. Руженцев // Сьома Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». Київ, 12-14 травня 2004. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2004. - С. 14-15.

50. Олійников Р.В. Методика порівняльного аналізу блокових симетричних шифрів / Р.В. Олійников, І.Д. Горбенко, Ю.І. Горбенко, В.І. Долгов // Сьома Міжнародна науково-практична конференція «Безпека інформації в інформаційно-

телекомунікаційних системах». Київ, 12-14 травня 2004. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2004. - С. 52.

51. Олейников Р.В. Сравнительный анализ алгоритмов блочного симметричного шифрования (по результатам международного проекта NESSIE) / Р.В. Олійников, І.Д.Горбенко, Г.М. Гулак, В.І. Руженцев // Сьома Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». Київ, 12-14 травня 2004. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2004. - С. 17-18.

52. Олейников Р.В. Критерии случайности таблиц подстановок алгоритма шифрования ГОСТ 28147-89 / Р.В. Олейников, В.И. Долгов, В.И. Руженцев, А.И. Шумов // IX Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Київ, 17-19 травня 2006. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2006. - С.30.

53. Олейников Р.В. Оценка случайности таблиц подстановок алгоритма шифрования ГОСТ 28147-89 / Р.В. Олейников, В.И. Руженцев, М.С. Михайленко // I-я международная конференция «Глобальные информационные системы. Проблемы и тенденции развития». Харьков, 3-8 октября 2006. Материалы конференции. - Х.: ХНУРЭ, 2006. - С. 384 – 385.

54. Олейников Р.В. Обоснование требований и принципы построения блочного симметричного алгоритма шифрования «Калина» / Р.В. Олейников, И.Д Горбенко, В.И. Долгов, В.И. Руженцев // X Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Київ, 16-18 травня 2007. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2007. - С.15-16.

55. Олейников Р.В. Методика и результаты исследования криптографической стойкости алгоритма шифрования «Калина» / Р.В. Олейников, И.Д. Горбенко, В.И. Долгов, В.И. Руженцев // X Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Київ, 16-18 травня 2007. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2007. - С.16-17.

56. Олейников Р.В. Спецификация и характеристики блочного симметричного шифра «Мухомор» / Р.В. Олейников, И.Д Горбенко, В.И. Долгов, В.И. Руженцев // X Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Київ, 16-18 травня 2007. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2007. - С.17-18.

57. Олейников Р.В. Исследование криптоаналитической стойкости блочного симметричного шифра «Мухомор» / Р.В. Олейников, Горбенко И.Д, В.И. Долгов, В.И. Руженцев // X Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Київ, 16-18 травня 2007. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2007. - С.18-19.

58. Олейников Р.В. Использование управляемых подстановок для построения шифрующего преобразования с улучшенными свойствами / Р.В. Олейников, В.И. Долгов, И.В. Лисицкая // II-я международная научная конференция «Современные информационные системы. Проблемы и тенденции развития». - Харьков, 2-5 октября 2007. Материалы конференции. - Х.: ХНУРЭ, 2006. - С. 61-63.

59. Олейников Р.В. Подход к криптоанализу современных шифров / Р.В. Олейников, В.И. Долгов, И.В. Лисицкая // II-я международная научная конференция

«Современные информационные системы. Проблемы и тенденции развития». - Харьков, 2-5 октября 2007. Материалы конференции. - Х.: ХНУРЭ, 2006.- С.25-26.

60. Олейников Р.В. Подходы к проектированию схемы разворачивания ключей для перспективного блочного алгоритма шифрования / Р.В. Олейников, С.В. Казьмина // II-я международная научная конференция «Современные информационные системы. Проблемы и тенденции развития». Харьков, 2-5 октября 2007. Материалы конференции. - Х.: ХНУРЭ, 2006.— С.31-32.

61. Олейников Р.В. Слабые ключи в алгоритме шифрования ADE / Р.В. Олейников, В.И. Руженцев, М.С. Михайленко // 11-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 20-22 травня 2008. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2008. - С.15-16.

62. Олейников Р.В. Дифференциальные свойства масштабированных моделей блочных симметричных шифров / Р.В. Олейников, В.И. Долгов, В.И. Руженцев // 11-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 20-22 травня 2008. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2008. - С.24-25.

63. Олейников Р.В. Циклические свойства масштабированных моделей блочных симметричных шифров / Р.В. Олейников, В.И. Долгов, В.И. Руженцев // 11-ая Международная научно-практическая конференция «Безопасность информации в информационнотелекоммуникационных системах». - Київ, 20-22 травня 2008. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2008. - С.71-72.

64. Олейников Р.В. Анализ свойств схемы разворачивания ключей алгоритма шифрования «Калина» / Р.В. Олейников, В.И. Руженцев, В.Д. Дырявый // 12-ая Международная научно-практическая конференция «Безопасность информации в информационнотелекоммуникационных системах». - Київ, 21-23 травня 2009. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2009. - С.35-36.

65. Олейников Р.В. Оценка мощности множества потенциально слабых ключей алгоритма А5/1 / Р.В. Олейников, О.Е. Барыльник, А.В. Григорьев // 12-ая Международная научно-практическая конференция «Безопасность информации в информационнотелекоммуникационных системах». - Київ, 21-23 травня 2009. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2009. - С.40-41.

66. Казимиров А.В. Алгебраическая атака на модифицированный вариант алгоритма «Лабиринт» / А.В. Казимиров, Р.В. Олейников // 12-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 21-23 травня 2009. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2009. - С.29.

67. Олейников Р.В. Особенности применения несюръективных S-блоков в раундовых функциях симметричных блочных шифров / Р.В. Олейников, М.С. Михайленко // 13-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 19-21 травня 2010. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2010. - С.10-11.

68. Олейников Р.В. Оценка эффективности перспективных конструкций схем разворачивания ключей симметричных блочных шифров / Р.В. Олейников, И.Д. Горбенко // 13-ая Международная научно-практическая конференция

«Безопасность информации в информационно-телекоммуникационных системах». - Київ, 19-21 травня 2010. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2010. - С.12-13.

69. Казимиров А. Выбор узлов нелинейного преобразования на основе анализа алгебраических свойств подстановок / А.В. Казимиров, Р.В. Олейников // 13-ая Международная научно-практическая конференция «Безопасность информации в информационнотелекоммуникационных системах». - Київ, 19-21 травня 2010. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2010. - С.17-18.

70. Олейников Р.В. Анализ свойств перспективной схемы разворачивания ключей для блочных симметричных алгоритмов шифрования / Р.В. Олейников // Proc. of International Conference on System Analysis and Information Technologies: SAIT'2011. Kyiv, May 23-28, 2011. К.: Institute of Applied Systems Analysis of National Technical University of Ukraine «Kyiv Polytechnic Institiute», 2011.- Р.480.

71. Олейников Р.В. Эффективность различения случайной перестановки и цепи Фейстеля на основе биективной раундовой функции / Р.В. Олейников, Д.С. Кайдалов // VI-ая Международная научно-практическая конференция «Наука и социальные проблемы общества: информатизация и информационные технологии». Харьков, 24-25 мая 2011: Сборник научных трудов. - Х.: ХНУРЭ, 2011. с.258-259.

72. Казимиров А.В. Восстановление ключей шифра ГОСТ 28147-89 на основе слайд-атаки / А. В. Казимиров, Р.В. Олейников // VI Междунар. науч.-практ. конф. «Наука и социальные проблемы общества: информатизация и информационные технологии», Харьков, 24–25 мая 2011 г.: тез. докл. – Х.:ХНУРЭ, 2011. – С. 272–273.

73. Олейников Р.В. Перспективный блочный шифр, оптимизированный для аппаратной реализации / Р.В. Олейников, Р.И. Киянчук // Международный радиоэлектронный форум. Харьков, 18-21 октября 2011: Материалы форума. - Х.: ХНУРЭ, 2011. с.327-330.

74. Олейников Р.В. Особенности различения трехраундовой цепи Фейстеля и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // 14-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 18-20 травня 2011. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2011. - С.11-12.

75. Олейников Р.В. Алгебраический криптоанализ ГОСТ 28147-89 / Р.В. Олейников, Р.И. Киянчук, И.Д. Горбенко // 15-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 21-24 травня 2012. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2012. - С.26-27.

76. Олейников Р.В. Оценка сложности различения схемы Лей-Месси и случайной перестановки / Р.В. Олейников, Д.С. Кайдалов // 15-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». - Київ, 21-24 травня 2012. Матеріали конференції. - К: НДЦ „ТЕЗІС”, 2012. - С.29-30.

АНОТАЦІЯ

Олійников Р.В. Методи аналізу і синтезу перспективних симетричних криптографічних перетворень. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2014.

Дисертаційна робота присвячена вирішенню актуальної науково-технічної проблеми синтезу симетричних криптографічних перетворень, які забезпечують високий рівень стійкості та швидкодії. Для основних типів криптоаналітичних атак на основі таблиці передобчислень вперше запропоновано методи оцінки складності виконання етапу побудови таблиць в умовах, коли потужність множини врахованих унікальних елементів близька до потужності множини значень невідомого стану криптографічного перетворення. Вперше запропонований метод порівняння високорівневих конструкцій симетричних блокових шифрів дозволяє визначити найкращу конструкцію на основі співвідношення стійкості до кількості раундів перетворення. Вперше запропонований метод синтезу блокових шифрів на основі таємних несюр'єктивних S-блоків дозволяє безключове читання криптограм для сторони, яка авторизована, і забезпечує стійкість щодо розкриття для інших сторін. Запропонований метод синтезу схем генерації циклових ключів блокових алгоритмів забезпечує небієктивну відповідність множин циклових ключів і ключів шифрування, захист від атак на зв'язаних ключах та підвищення стійкості до атак на реалізацію, зберігаючи стійкість до переборних атак. Запропоновані методи дозволили розробити блоковий шифр «Калина» та ґеш-функцію «Купина», які мають високий та надвисокий рівень криптографічної стійкості та швидкодію, що перевищує іноземні аналоги на сучасних 64-бітових програмних платформах, і використані під час розробки проектів специфікацій національних стандартів України.

Ключові слова: блоковий шифр, ґеш-функція, криптоаналіз, ланцюг Фейстеля, схема Лей-Массі, SPN-структура, rainbow-таблиця, fuzzy-rainbow-таблиця, S-блок.

АННОТАЦИЯ

Олейников Р.В. Методы анализа и синтеза перспективных симметричных криптографических преобразований. – На правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Харьковский национальный университет радиоэлектроники, Министерство образования и науки Украины, Харьков, 2014.

Диссертационная работа посвящена решению актуальной научно-технической проблемы синтеза симметричных криптографических преобразований, обеспечивающих высокий уровень стойкости и производительности. Наиболее важные научные и практические результаты, изложенные в работе, состоят в следующем.

Для основных типов криптоаналитических атак, использующих таблицы предвычислений, впервые предложены методы оценки сложности выполнения этапа построения таблиц в условиях, когда мощность множества учтенных уникальных

элементов близка к мощности множества значений неизвестного состояния криптографического преобразования, что позволяет реализовывать атаки такого типа с заранее заданной высокой вероятностью успеха проведения оперативного этапа. Показано, что при практической реализации таких атак на шифры унаследованного уровня стойкости (с длиной ключа 64 бита или менее) возможно успешное выполнение оперативного этапа в реальном масштабе времени. При проектировании перспективных симметричных криптографических преобразований разработанные методы использованы при выборе внешних параметров, таких как длина ключа, размер блока шифра и др., для обоснования стойкости разрабатываемых примитивов к усовершенствованным атакам переборного типа.

Впервые предложен метод сравнения высокоуровневых конструкций симметричных блочных шифров на основе оценки сложности различения высокоуровневой конструкции шифра и случайной перестановки, что позволяет определить высокоуровневую конструкцию с наилучшим соотношением криптографической стойкости к количеству раундов преобразования блочного шифра. Для схем на основе цепи Фейстеля и схемы Лей-Месси впервые предложена модель использования случайных перестановок вместо случайных функций в раундовом преобразовании, что позволило получить более точные оценки для наиболее распространенных блочных шифров с биективной раундовой функцией. Для цепи Фейстеля со случайными функциями в раундовом преобразовании получены более точные оценки за счет отказа от допущения о равновероятности и несовместности событий коллизий выходных значений раундовых функций.

Впервые предложен метод синтеза симметричных блочных шифров на основе секретных несюръективных S-блоков, позволяющих авторизованной стороне выполнять дешифрование криптограмм с заранее заданной вычислительной сложностью (разработка шифра с дополнительными возможностями для разработчика, скрытыми от пользователя алгоритма), при этом обеспечив высокую вычислительную сложность реализации атаки для третьей стороны. Предложенный метод позволяет реализовать дополнительные проверки для обнаружения нежелательных свойств криптографического преобразования при проведении экспертизы блочного алгоритма.

Предложенное усовершенствование метода синтеза схем генерации цикловых ключей симметричных блочных шифров обеспечивает небиективное соответствие множеств цикловых ключей и ключей шифрования, с сохранением свойств нелинейной зависимости каждого бита каждого раундового ключа от каждого бита ключа шифрования и стойкости к переборным атакам. Сформированная с помощью метода схема разворачивания дополнительно задает существенные отличия (крайне сложную зависимость) цикловых ключей и позволяет защитить шифр от атак на связанных ключах и увеличить стойкость к атакам на реализацию. С практической точки зрения, аппаратные или программные модули, реализующие формирование цикловых ключей, не требуют дополнительных функций или блоков и используют только компоненты основного шифрующего преобразования.

Предложенные методы позволили разработать симметричный блочный шифр «Калина», обеспечивающий высокий и сверхвысокий уровень криптографической стойкости, с уровнем производительности, превосходящим зарубежные аналоги на современных 64-битовых программных платформах. Алгоритм использован при

создании проекта спецификации нового национального стандарта шифрования Украины.

На основе блочного шифра построена криптографическая хэш-функция «Купина», обеспечивающая высокий и сверхвысокий уровень стойкости, с производительностью, превосходящей российские и белорусские аналоги на 32-битовых и 64-битовых программных платформах. Разработанное преобразование использовано при создании проекта спецификации нового национального стандарта Украины для алгоритма хэширования.

Ключевые слова: блочный шифр, хэш-функция, криптоанализ, цепь Фейстеля, схема Лей-Месси, SPN-структура, rainbow-таблица, fuzzy-rainbow-таблица, S-блок.

ABSTRACT

Oliynykov R.V. Methods for analysis and synthesis of perspective symmetric cryptographic transformations. - Manuscript.

A Thesis for a Doctor of Technical Sciences degree in the specialty 05.13.05 – computer systems and components. – Kharkiv National University of Radio Electronics, Ministry education and science of Ukraine, Kharkiv, 2014.

The thesis is dedicated to solving of the important scientific problem of symmetric cryptographic transformations synthesis providing high level strength and performance. For main types of cryptanalytic attacks based on precomputed tables methods of table computation stage complexity estimation in conditions where the set cardinality of accounted unique elements is near to unknown state values set cardinality of cryptographic transformation are proposed for the first time. Comparison method of block cipher high level constructions allows selection of the best construction based on strength to number of encryption rounds ratio is proposed for the first time. Method of block ciphers synthesis based on secret non-surjective S-boxes allows keyless decryption for authorized party and provides security to encrypted message compromising to any other unauthorized party is proposed for the first time. Proposed synthesis method of block cipher key schedule provides non-bijective correspondence of round key and encryption key sets, protection from related keys attacks and improving strength to side-channel attacks, keeping security against brute force attacks. Proposed methods allow development of block cipher «Kalyna» and hash function «Kupyna» providing high level of cryptographic strength and performance exceeding international standards on 64-bit software implementations. These cryptographic transformations were used during Ukrainian national cryptographic standards project development.

Keywords: block cipher, hash function, cryptanalysis, Feistel network, Lai-Massey scheme, SPN-structure, rainbow table, fuzzy-rainbow table, S-box.