АНОТАЦІЯ

Родінко М. Ю. Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки (Галузь знань 12 – Інформаційні технології). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2020.

Дисертація присвячена розробці та удосконаленню методів аналізу криптографічних властивостей компонентів симетричних блокових шифрів та побудові перспективних криптографічних перетворень.

Метою дисертаційної роботи є підвищення продуктивності симетричних криптографічних перетворень і удосконалення методів аналізу їх стійкості.

У першому розділі дисертації *(Актуальний стан та перспективи розвитку методів аналізу та синтезу симетричних блокових шифрів)* виконано аналіз актуального стану розвитку технологій симетричного блокового шифрування та постановку задач дослідження. Зокрема, проаналізовані основні високорівневі конструкції, а також принципи побудови циклової функції та схеми розгортання ключів симетричних блокових шифрів. Виконано аналіз сучасних малоресурсних блокових шифрів та вимог до симетричних примітивів, що застосовуються у пристроях з обмеженою кількістю споживання енергії. За результатами аналізу виявлені недоліки та невирішені питання, що стосуються існуючих малоресурсних блокових шифрів, виходячи з яких сформульовані задачі дисертаційного дослідження.

У другому розділі *(Розробка удосконаленого методу генерації оптимальних S-блоків з високими нелінійністю та алгебраїчним імунітетом)* вирішена задача щодо підвищення швидкості (зниження обчислювальної складності) генерації оптимальних S-блоків на доступній обчислювальній

техніці. Отримано *перший науковий результат*: *удосконалено* метод градієнтного спуску для генерації нелінійних таблиць заміни, що відрізняється від відомого обґрунтованим оптимальним порядком застосування критеріїв при перевірці підстановок на відповідність криптографічним показникам, що дозволяє суттєво знизити складність генерації оптимальних S-блоків.

Отримано *перший практичний результат*: удосконалений метод градієнтного спуску дозволяє зменшити середній час генерації оптимального байтового S-блока з нелінійністю 104, δ-рівномірністю 8, алгебраїчним імунітетом 3 та мінімальною степінню булевих функцій 7 на персональному комп'ютері з 2,5 годин до 30 хвилин (скорочення часу розрахунків у 5 разів).

В основу оптимізації методу градієнтного спуску покладено той факт, що критерії відбору підстановок є частково взаємозалежними. Таким чином, час перевірки підстановки на відповідність набору критеріїв суттєво залежить від порядку застосування цих критеріїв у процесі перевірки. У зв'язку з цим, запропоновано аналітичний вираз для визначення порядку застосування критеріїв, за якого час перевірки підстановки буде мінімальним.

В процесі перевірки запропонованого підходу для чотирьох обраних критеріїв були розраховані значення часу перевірки підстановки (та, відповідно, часу генерації) для всіх можливих комбінацій критеріїв. Розрахунки показали, що вибір найоптимальнішого порядку застосування критеріїв дозволяє зменшити час генерації S-блока майже в 5 разів. Аналітично отримані значення були підтверджені й експериментально. Середній час генерації оптимальних підстановок за допомогою програмної реалізації з урахуванням запропонованого вдосконалення склав 30 хвилин.

У третьому розділі *(Розробка методу оцінки колізійних властивостей неін'єктивних схем розгортання ключів симетричних блокових шифрів)* вирішена задача удосконалення оцінок щодо ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін'єктивною схемою розгортання циклових ключів, і множини ключів шифрування для симетричних шифрів. Отримано *другий науковий результат*:

отримав подальший розвиток математичний метод оцінки колізійних властивостей неін’єктивних схем розгортання ключів блокових шифрів, що відрізняється застосуванням вдосконаленої математичної моделі та більш ефективного математичного апарату та дозволяє отримати уточнену оцінку ймовірності колізії двох послідовностей циклових ключів.

Отримано *другий практичний результат*: удосконалено значення оцінки нижньої границі стійкості діючого національного стандарту ДСТУ 7624:2014, а саме доведено, що складність атак переборного типу на неін’єктивні схеми розгортання ключів практично дорівнює складності атак на ін’єктивні схеми.

За допомогою удосконаленого математичного методу оцінки ймовірності співпадіння потужностей множини послідовностей циклових ключів, які формуються неін’єктивною схемою розгортання ключів, і множини ключів шифрування, доведено, що для повномасштабного шифру ця ймовірність практично дорівнює 1. При цьому неін’єктивні схеми розгортання ключів забезпечують додаткову стійкість до атак на реалізацію та деяких інших методів криптоаналізу. Таким чином, при побудуванні перспективного симетричного блокового шифру доцільно використовувати саме неін’єктивну схему розгортання циклових ключів.

У четвертому розділі *(Побудова та аналіз властивостей перспективного постквантового малоресурсного блокового шифру)* вирішені наступні задачі:

– розробка малоресурсного блокового симетричного шифру, що задовольняє вимогам щодо забезпечення високого та надвисокого рівня стійкості (за класифікацією NESSIE), а також має компактну реалізацію та високу продуктивність на різних програмно-апаратних платформах;

– розробка математичної моделі для оцінки стійкості визначеного класу ARX-подібних шифрів до диференційного криптоаналізу, що базується на відомих положеннях теорії криптоаналізу та обґрунтованих припущеннях щодо властивостей компонентів таких шифрів;

– розробка методів пошуку найбільш ймовірних одноциклових диференційних характеристик визначеного класу ARX-шифрів з урахуванням

особливостей побудови циклової функції, що використовується у шифрах визначеного класу;

– удосконалення методів пошуку багатоциклових диференційних характеристик визначеного класу ARX-шифрів із використанням відомих підходів та результатів застосування розроблених методів пошуку одноциклових диференційних характеристик.

Отримано *третій та четвертий наукові результати*:

– *вперше* запропоновано два методи пошуку одноциклових диференційних характеристик для визначеного класу ARX-шифрів, що дозволяють з низькою обчислювальною складністю отримувати оцінки стійкості циклової функції блокового шифру визначеного класу до диференційного криптоаналізу;

– *отримали подальший розвиток* методи пошуку багатоциклових диференційних характеристик для визначеного класу ARX-шифрів, що відрізняються вдосконаленим механізмом відбору вхідних різниць та формуванням початкової множини одноциклових диференційних характеристик, що дозволяє отримати оцінку щодо стійкості повномасштабного блокового шифру визначеного класу до диференційного криптоаналізу.

Отримано *третій та четвертий практичні результати*:

– розроблено перспективний постквантовий малоресурсний блоковий шифр «Кипарис», що забезпечує високий та надвисокий рівні стійкості та перевершує за швидкодією відомі малоресурсні блокові шифри на 32- та 64-бітових процесорах загального призначення та мобільних платформах;

– обґрунтовано стійкість симетричного блокового шифру «Кипарис-256» до диференційного криптоаналізу згідно з вимогами практичного критерію, а саме показано, що максимальна середня за ключами ймовірність диференційної характеристики є набагато меншою за ймовірність успіху атаки прямого перебирання ключів.

Запропонований блоковий шифр «Кипарис» заснований на мережі Фейстеля, а циклова функція шифру представляє собою ARX-перетворення.

Схема розгортання циклових ключів шифру є неін'єктивною та використовує принципи побудови схеми розгортання ключів шифру «Калина». Алгоритм підтримує довжину блока (ключа) 256 та 512 бітів, що дозволяє забезпечити високий рівень криптографічної стійкості.

Розроблена математична модель оцінки стійкості визначеного класу ARX-шифрів до диференційного криптоаналізу дозволяє отримати вираз для обчислення середньої (за ключами) ймовірності диференційної характеристики шифру та зробити обґрунтоване припущення щодо значень вхідних різниць, які при проходженні через цикл шифрування формують характеристику, що має високу ймовірність. Модель включає припущення про те, що шифр є марковським, про ймовірність перетворення диференційних різниць на модульних суматорах, про зв'язок кількості активних біт у вхідній різниці з ймовірністю диференційної характеристики, а також містить вирази для обчислення ймовірностей одноциклових та багатоциклових диференційних характеристик. На основі представленої моделі розроблено методи пошуку диференційних характеристик класу блокових ARX-шифрів.

Розроблено методи пошуку диференційних характеристик циклової функції визначеного класу ARX-шифрів (прямий метод пошуку, метод пошуку «у двох напрямках» та оптимізований метод пошуку диференційної характеристики з високою ймовірністю), що дозволяють знайти найбільш ймовірні одноциклові диференційні характеристики. Метою всіх трьох підходів є активізація найменшої кількості біт на входах суматорів циклової функції, що, в свою чергу, збільшує ймовірність заданого перетворення. Останній із запропонованих методів дозволив здійснити ефективний пошук диференційної характеристики на один цикл перетворення блокового шифру «Кипарис» з ймовірністю, що дорівнює 1/4.

Застосування запропонованого методу пошуку багатоциклових диференційних характеристик, заснованого на побудові множини високоймовірнісних одноциклових диференційних характеристик, до блокового шифру «Кипарис-256» показало, що побудовані одноциклові диференційні

характеристики, вихідні різниці яких мають малу вагу Гемінга (а значить і достатньо високу ймовірність), не можуть бути продовжені для побудування багатоциклових диференційних характеристик з високою ймовірністю.

Одна зі знайдених найбільш ймовірних багатоциклових диференційних характеристик для блокового шифру «Кипарис-256» може бути побудована лише для шести циклів шифрування з ймовірністю $\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}$. Таким чином, блоковий шифр «Кипарис-256» є стійким до диференційного криптоаналізу з точки зору практичного критерію.

У п’ятому розділі *(Експериментальні дослідження властивостей симетричного блокового шифру «Кипарис»)* досліджені статистичні, лавинні та швидкісні характеристики розробленого перспективного блокового шифру «Кипарис». Дослідження статистичних властивостей шифру показало, що шифруюче перетворення та схема розгортання ключів алгоритмів «Кипарис-256» та «Кипарис-512» задовольняють вимогам зі статистичного тестування випадкових послідовностей NIST STS.

Дослідження лавинних показників блокового шифру «Кипарис» показало, що «Кипарис-256» (число циклів дорівнює 10) та «Кипарис-512» (число циклів дорівнює 14) відповідають вимогам щодо лавинного ефекту починаючи з чотирьох циклів шифрування.

Порівняння швидкодії блокового шифру «Кипарис» зі швидкодією відомих малоресурсних алгоритмів здійснювалося на платформах Windows, Linux та Android (із залученням одного ядра процесора в однопотоковому застосуванні). Блоковий шифр «Кипарис» продемонстрував високу продуктивність на всіх досліджуваних програмно-апаратних платформах. На платформі Windows 10 з 32-бітовою архітектурою найкращий результат показав шифр «Кипарис-256» (порядку 3,5 Гбіт/сек). На платформі Windows 10 з 64-бітовою архітектурою найкращий результат показав шифр «Кипарис-512» (приблизно 5 Гбіт/сек). На платформі Linux з 64-бітовою архітектурою блоковий шифр «Кипарис-256» показав надвисокий результат зі швидкодії (понад 8 Гбіт/сек).

Ключові слова: симетричний блоковий шифр, малоресурсний блоковий шифр, S-блок, нелінійність, алгебраїчний імунітет, циклова функція, схема розгортання ключів, ARX-шифр, диференційний криптоаналіз, диференційна характеристика.