АНОТАЦІЯ

Лисицький К. Є. Методи та засоби побудови блокових симетричних шифрів з підвищеною стійкістю та швидкодією. — 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 й науки України, Харків, 2021.

Основний зміст роботи — це викладення результатів участі автора в обґрунтуванні нової методології оцінки стійкості блокових симетричних шифрів (БСШ) до атак диференціального та лінійного криптоаналізу та подальшому її розвитку в напряму створення й розробки вдосконалених методів проєктування блокових симетричних шифрів з підвищеною стійкістю і швидкодією.

Основні результати. Відомі результати досліджень з обґрунтування нової методології прискореного криптоаналізу БСШ до атак диференціального та лінійного криптоаналізу виконані на кафедрі безпеки інформаційних технологій (БІТ) Харківського національного університету радіоелектроніки [1; 2 ; 3; 4; 5; 6] упродовж 2008–2015 років. У проведенні експериментальних досліджень та отриманні ряду важливих результатів брав участь і автор дисертаційної роботи. Особисто і в співавторстві було опубліковано більше ніж 30 статей у фахових виданнях України та за кордоном.

Найбільш важливі результати з формування нової методології оцінки стійкості БСШ до атак диференціального і лінійного криптоаналізу представлено в даній дисертаційній роботі [1].

Сутність нової методології й найбільш важливі результати отримані за участю автора роботи. Ці новітні результати в даному напряму стали

основою формування вдосконалених методів проєктування блокових симетричних шифрів та основним змістом досліджень даної роботи.

В роботі [1] сутність нової методології сформульована наступним чином.

Всі сучасні блокові симетричні шифри через певне число циклів незалежно від S-блоків використаних в них (*мова йде не про вироджені їх конструкції*) *набувають властивостей випадкових підстановок. За комбінаторними показниками* (*числу інверсій, зростань і циклів*)*, а також за законами розподілу переходів таблиць диференціальних різниць (XOR)* (*повних диференціалів*) *і законами розподілу зміщень таблиць лінійних апроксимацій* (*лінійних корпусів*) *повторюють відповідні показники випадкових підстановок.*

В результаті значення максимумів повних диференціалів і лінійних корпусів можуть бути визначені розрахунковим шляхом за формулами для законів розподілу ймовірностей переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок відповідного степеня. Виходячи з цього, перевірку показників випадковості великих шифрів можна виконати на основі розробки і подальшого аналізу показників випадковості зменшених моделей. Зменшені моделі допускають проведення обчислювальних експериментів в прийнятні (*реальні*) *строки.*

У процесі обґрунтування цих положень проведений великий комплекс теоретичних і експериментальних досліджень показників випадковості сучасних блокових симетричних шифрів і випадкових підстановок, виконаних у тому числі з участю і автора цієї роботи, зокрема:

- розроблені зменшені моделі блокових симетричних шифрів, представлених на український конкурс з відбору претендента на національний стандарт блокового симетричного шифрування [9; 10; 11; 29] та інші;

- обґрунтовано нові показники стійкості (доказової безпеки) до атак диференціального і лінійного криптоаналізу БСШ;

- такими показниками запропоновано розглядати значення максимумів законів розподілу переходів XOR таблиць (повних диференціалів) і зміщень таблиць ЛАТ (лінійних корпусів) замість *MADP* і *MALP* (максимумів середніх значень диференціальних ймовірностей і максимумів середніх значень лінійних ймовірностей (*MADP* і *MALP* прив'язано до фіксованих осередків диференціальних таблиць і таблиць лінійних апроксимацій[1]);

- запропоновано використовувати *AMDP* і *AMLP* (відповідно середнє значення максимумів диференціальних таблиць і середнє значення зміщень таблиць лінійних апроксимацій[2]) [29] та інші;

- проведено дослідження показників випадковості розроблених моделей розглядалися комбінаторні властивості (закони розподілу інверсій, зростань і циклів), а також закони розподілу ймовірностей повних диференціалів і лінійних корпусів [14;16;80] та інші;

- досліджено показники випадковості великих прототипів в режимі їх запуску скороченими (16-бітними) сегментами вхідних і вихідних блоків даних [9; 10] та інші;

- розвинено математичну теорію випадкових підстановок в частині доведення теорем, що визначають закони розподілу переходів XOR таблиць та зміщень таблиць лінійних апроксимацій [8; 23];

- отримані розрахункові співвідношення для визначення максимальних значень диференціальних та лінійних ймовірностей БСШ, що дозволяють сьогодні вимірювати показники їх доказової стійкості до атак диференціального та лінійного криптоаналізу [8; 15; 23] та інші;

- вдосконалена математична модель випадкової підстановки;

- показано, що в удосконалених шифрах як випадкові підстановки можна використовувати підстановки з виходу генератора випадкових підстановок без додаткової їх фільтрації [7; 12; 14] та інші.

---

[1] Означення *MADP* і *MALP* див. Додаток Б
[2] Означення *AMDP* і *AMLP* див. Додаток Б

На фінальному етапі виконання роботи:

- обчислені закони розподілу максимумів диференціалів і лінійних корпусів шифрів, що дозволило уточнити значення показників стійкості шифрів до атак диференціального і лінійного криптоаналізу [16];

- вивчені динамічні показники приходу шифрів до стану випадкових підстановок[3] [17; 18; 20] та інші;

- запропоновані й розроблені вдосконалені методи проєктування блокових симетричних шифрів.

Сутність запропонованих методів базується на наступних додаткових положеннях [22; 117; 118] та інші:

1. Всі сучасні ітеративні шифри незалежно від S-блоків, що використані в них, на повноцикловій довжині за комбінаторними, диференціальними і лінійними показниками (за значеннями максимумів диференціальних та лінійних ймовірностей) набувають властивостей випадкових підстановок. Підстановлювальні перетворення (S-блоки) впливають лише на динаміку (кількість циклів) приходу шифру до стану випадкової підстановки.

2. Динамічні показники приходу шифру до стану випадкової підстановки визначаються мінімальною кількістю активних S-блоків[4], що припадають на перші цикли перетворень. При цьому мінімальне число активних S-блоків першого циклу у відомих конструкціях БСШ (шифрів з одношаровими підстановлювальними перетвореннями) дорівнює одному. Лінійні перетворення, що будуються на основі МДВ перетворень, не забезпечують активізації всіх S-блоків другого і третього циклів.

3. Для покращення показників випадковості шифруючих перетворень їх потрібно будувати із забезпеченням активізації як можна більшої мінімальної кількості S-блоків перших циклів.

---

[3] Динамічні показники шифру визначаються мінімальним числом активованих S-блоків, що припадають на перші цикли перетворень, які дозволяють шифру прийти до стану випадкової підстановки.

[4] Активний S-блок – це S-блок, що має ненульову різницю на виході (вході), або ненульовий перехід таблиці ЛАТ вхідної маски в вихідну.

4. Гранична кількість розгалужень (коли один S-блок активізує збільшене число S-блоків наступних циклів) може бути реалізована на основі конструкції із забезпеченням принципу послідовної активізації S-блоків циклової функції, включених в ланцюжок одного за іншим. При цьому необхідно створити умови для забезпечення активізації ланцюжка з самого його початку. Для такої конструкції циклової функції існує можливість активізації вже в другому циклі майже всіх S-блоків.

5. Одним з можливих шляхів збільшення кількості S-блоків першого циклу, що активізуються однобайтовими різницями входу, є побудування першого циклу з двошаровим підстановлювальним перетворенням. Для шифру з двошаровим підстановлювальним перетворенням на першому циклі існує можливість при одному активному байті входу зробити активними майже усі (або усі) байти другого шару і створити умови, при яких шифр стає випадковою підстановкою за два цикли для 128-бітних шифрів і за три цикли для 256-бітних шифрів. Наступні цикли можуть бути побудовані з використанням стандартних (відомих) методів.

6. Збільшення мінімального числа S-блоків, що активізуються на перших циклах, є ефективним засобом забезпечення незалежності шифруючих перетворень від властивостей використаних S-блоків. Це шлях побудування шифрів без зниження криптографічної стійкості та з можливістю застосовування S-блоків випадкового типу (практично без попереднього їх відбору).

Робота присвячена обґрунтуванню і розвитку цих положень, а також їх використанню для забезпечення можливостей підвищення показників стійкості й швидкодії БСШ, зокрема в умовах наявності квантових комп’ютерів.

Наукова новизна отриманих результатів дисертаційної роботи полягає в наступному:

1. Результатами досліджень підтверджена нова методологія оцінки показників доказової стійкості блокових симетричних шифрів до атак

диференціального і лінійного криптоаналізу, яка на відміну від наявних підходів будується на основі використання теоретичних значень максимумів законів розподілу переходів XOR таблиць (повних диференціалів) і змішень таблиць ЛАТ (лінійних корпусів) шифруючих перетворень. При цьому шифруючи перетворення розглядаються як випадкові підстановки.

2. Вперше запропоновано підхід до проєктування SPN блокових симетричних шифрів з поліпшеними динамічними показниками приходу до стану випадкової підстановки, який дозволяє збільшити мінімальну кількість S-блоків, що активізуються на перших циклах шифруючих перетворень.

Основою реалізації цього підходу стало використання окремо або спільно трьох методів, спрямованих на збільшення числа S-блоків, що активізуються на перших циклах шифруючих перетворень, а саме:

1) вперше запропоновано метод використання в першому циклі SPN шифру збільшеного числа S-блоків на основі реалізації двошарової його конструкції, що дозволяє збільшити мінімальне число S-блоків, що активізуються на першому циклі, й шляхом цього зменшити число циклів приходу шифру до стану випадкової підстановки;

2) вперше запропоновано метод побудування першого циклу шифру за допомогою шару керованих укрупнених S-блоків, що з’єднані в ланцюжок шляхом послідовного їх включення одного за іншим з додаванням чергового сегменту даних до входу кожного укрупненого S-блоку циклової функції й складанням виходу останнього укрупненого S-блоку з виходами інших, що забезпечує при побудові укрупнених S-блоків за стратегією широкого сліду активізацію усіх S-блоків другого циклу й внаслідок цього дозволяє зменшити число циклів приходу шифру до стану випадкової підстановки;

3) вперше запропоновано метод побудування всієї конструкції шифру з використанням принципів послідовного включення укрупнених S-блоків в ланцюжок одного за іншим з додаванням чергового сегменту даних до

входу кожного укрупненого S-блоку циклової функції зі складанням виходу останнього укрупненого S-блоку з виходами інших, що дозволяє збільшити число S-блоків, що активізуються на перших циклах шифруючого перетворення, й внаслідок цього зменшити число циклів приходу шифру до стану випадкової підстановки.

3. Вперше запропонований метод визначення кількості циклів приходу шифру до показників випадкової підстановки на основі врахування мінімальної кількості тільки тих активних S-блоків, що припадають на перші цикли перетворень і беруть участь у формуванні граничних значень диференціальної та лінійної ймовірностей.

4. Вперше побудовані й підтверджені експериментально закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій шифрів, що дозволило підтвердити гіпотезу стосовно досить малого діапазону зміни максимумів повних диференціалів і максимумів зміщень лінійних корпусів сучасних шифрів і їх практичну незалежність від ключового матеріалу.

5. Набула подальшого розвитку модель випадкової підстановки, яка на відміну від наявних підходів визначається значеннями максимумів таблиць диференціальних різниць і зміщень таблиць лінійних апроксимацій підстановок близькими до значень максимумів екстремальних законів розподілу переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок і значеннями алгебраїчної імунності для байтових підстановок близькими до 3, що забезпечує використання як випадкових (байтових) підстановок в шифрах безпосередньо підстановок, породжених випадковим генератором підстановок.

6. Вперше обґрунтована можливість побудування шифрів з використанням випадкових S-блоків з підвищеними показниками стійкості й швидкодії, і для умов застосування квантових комп’ютерів.

Практичне значення. Розвинуті підходи та методи були використані для порівняльного аналізу шифрів, представлених у свій час на український

конкурс з вибору національного стандарту блокового симетричного шифрування, а також при дослідженні шифру Калина-2, що став національним стандартом України. Напрям подальшого вдосконалення властивостей і показників доказової безпеки БСШ орієнтовано на постквантовий період розвитку криптографії.

Результати роботи використані при виконанні науково-дослідних робіт Приватного акціонерного товариства «Інститут інформаційних технологій» (ЗАТ «ІІТ») Харківського національного університету радіоелектроніки та в наукових дослідженнях і навчальному процесі Харківського національного університету імені В. Н. Каразіна. Відповідні акти впровадження результатів досліджень надані в додатках.

Результатами досліджень повністю підтверджені всі висунуті положення.

Ключові слова: технології блокового симетричного шифрування, блоковий симетричний шифр, динамічні показники приходу шифру до стану випадкової підстановки, стійкість до атак диференціального і лінійного криптоаналізу, активні S-блоки, доказова стійкість, максимальна диференціальна ймовірність, максимальна лінійна ймовірність, випадкова підстановка, модель випадкової підстановки, показники швидкодії шифру, показники випадковості, методи вдосконалення шифруючих перетворень.