Харківський національний університет імені В. Н. Каразіна
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Лисицький Костянтин Євгенійович

УДК 681.3.06

ДИСЕРТАЦІЯ
«МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ З ПІДВИЩЕНОЮ СТІЙКІСТЮ ТА ШВИДКОДІЄЮ»

Спеціальність 122 - «Комп'ютерні науки»
(Галузь знань 12 - Інформаційні технології)
Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей результатів і текстів інших авторів мають посилання на відповідне джерело.

К. Є. Лисицький

Науковий керівник: Горбенко Іван Дмитрович, доктор технічних наук, професор.

Харків — 2021

Усі примірники дисертації ідентичні за змістом.
Голова спеціалізованої вченої ради ДФ 64.051.020 Валентин ПАЗИРИК

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.

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];

---

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

- 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.

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

---

[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.

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.

ABSTRACT

Lysytskyi K. E. Methods and tools for building block symmetric cipher with increased stability and performance. – Qualification scholarly paper: a manuscript.

Thesis submitted for obtaining the Doctor of Philosophy degree in Computer Science, Speciality 122 — Computer sciences. — V. N. Karazin Kharkiv National University, Ministry of Education and Science of Ukraine, Kharkiv, 2021.

The main content of the work is to present the results of the author's participation in substantiation of a new methodology for assessing the resistance of block symmetric ciphers (BSC) to attacks of differential and linear cryptanalysis and its further development in the direction of creating and developing advanced methods of designing block symmetric ciphers with increased stability and speed.

The main results. Known results of research on the justification of the new methodology of accelerated cryptanalysis of BSC to attacks of differential and linear cryptanalysis were performed at the Department of Information Technology Security (ITS) of Kharkiv National University of Radio Electronics [1;2;3;4;5;6] during 2008–2015. The author of the dissertation also took part in conducting experimental research and obtaining a number of important results. Personally and in co-authorship, more than 30 articles were published in professional publications in Ukraine and abroad.

The most important results on the formation of a new methodology for assessing the resistance of BSC to attacks of differential and linear cryptanalysis are presented in this dissertation [1].

Recall the essence of the new methodology and the most important results obtained with the participation of the author. These latest results in this direction became the basis for the formation of improved methods for designing block symmetric ciphers and the main content of research in this work.

In [1] the essence of the new methodology is formulated as follows:

All modern block symmetric ciphers through a certain number of cycles, regardless of the S-blocks used in them (this is not about their degenerate structures) acquire the properties of random substitutions. According to combinatorial indicators, as well as according to the laws of distribution of transitions of tables of differential differences and laws of distribution of displacements of tables of linear approximations repeat the corresponding indicators of random substitutions. As a result, the values of the maxima of complete differentials and linear bodies can be determined by calculation by formulas for the laws of distribution of probabilities of transitions of XOR tables and displacements of tables of linear approximations of random permutations of the corresponding degree. Reduced models allow computational experiments in a reasonable time.

In the process of substantiation of these provisions, a large set of theoretical and experimental studies of the indicators of randomness of modern block symmetric ciphers and random substitutions, performed, including with the participation of the author of this work, in particular:

- developed reduced models of block symmetric ciphers, including ciphers submitted to the Ukrainian competition for the selection of a candidate for the national standard of block symmetric encryption) [9; 10; 11; 29] and others of this work, in particular;

- new indicators of resistance (evidence-based security) to attacks of differential and linear cryptanalysis of BSC are substantiated;

- as such indicators it is offered to consider values of maxima of laws of distribution of transitions of XOR tables (full differentials) and shifts of tables LAT (linear cases) instead of MADP and MALP (maxima of average values of differential probabilities and maxima of average values of linear probabilities (MADP and MALP at fixed cells of differential tables and tables of linear approximations);

- it is proposed to use AMDP and AMLP (respectively, the average value of the maxima of the differential tables and the average value of the offsets of the tables of linear approximations) [29] and others;

- a study of the indicators of randomness of the developed models, which considered the combinatorial properties (laws of distribution of inversions, increments and cycles), as well as the laws of probability distribution of complete differentials and linear bodies [14, 16, 80] and others;

- the indicators of randomness of large prototypes in the mode of their launch by abbreviated (16-bit) segments of input and output data blocks [9, 10] and others were studied;

- developed a mathematical theory of random substitutions in terms of proving the teorems that determine the laws of distribution of transitions of XOR tables and displacements of tables of linear approximations [8, 23];

- the calculated ratios for determining the maximum values of differential and linear probabilities of BSC, which today allow to measure the indicators of their evidentiary resistance to attacks of differential and linear cryptanalysis [8, 15, 23] and others;

- improved mathematical model of random substitution;

- it is shown that in advanced ciphers as random substitutions it is possible to use substitutions from the output of the generator of random substitutions without their additional filtering [7; 12; 14] and others.

At the final stage of work:

- the laws of distribution of maxima of differentials and linear cases of ciphers are calculated that allowed to specify values of indicators of resistance of ciphers to attacks of differential and linear kryptonalysis [16];

- studied the dynamic indicators of the arrival of ciphers to the state of random subtenings [17; 18; 20] and others;

- advanced methods of designing block symmetric ciphers are proposed and developed.

The essence of the proposed methods is based on the following additional provisions [22; 117; 118] and others:

1. All modern iterative ciphers, regardless of the S-blocks used in them, at full cycle length by combinatorial, differential and linear indicators (by the values of the maxima of differential and linear probabilities) acquire the properties of random substitutions. Substitution transformations (S-blocks) affect only the dynamics (number of cycles) of the arrival of the cipher to the state of random substitution.

2. The dynamic indicators of the arrival of the cipher to the state of random substitution are determined by the minimum number of active S-blocks that fall on the first cycles of transformations. The minimum number of active S-blocks of the first cycle in the known constructions BSC (ciphers with single-layer substitution transformations) is equal to one. Linear transformations based on MAD transformations do not provide activation of all S-blocks of the second and third cycles.

3. To improve the randomness of their encryption transformationit is necessary to build with ensuring activation of as much as possible the minimum number of S-blocks of the first cycles.

4. The maximum number of branches (when one S-block activates an increased number of S-blocks of subsequent cycles) can be implemented on the basis of the design with the principle of sequential activation of S-blocks of the cyclic function included in the chain one after another. It is necessary to create conditions to ensure the activation of the chain from the very beginning. For such a construction of the cyclic function, it is possible to activate almost all S-blocks in the second cycle.

5. One of the possible ways to increase the number of S-blocks of the first cycle, activated by single-byte input differences, is to build the first cycle with a two-layer substitution transformation. For a cipher with two-layer substitution transformation on the first loop, it is possible to make almost all (or all) bytes of the second layer active with one active input byte and create conditions under which the cipher becomes a random substitution for two cycles for 128-bit ciphers and for

three cycles for 256-bit ciphers. Moreover, the following cycles can be constructed using standard (known) methods.

6. Increasing the minimum number of S-blocks activated in the first cycles is an effective means of ensuring the independence of encryption transformations from the properties of the used S-blocks. This is a way to build ciphers without reducing cryptographic stability with the possibility of using S-blocks of the random type (almost without their prior selection).

The work is devoted to the substantiation and development of these provisions, as well as their use to justify the possibility of increasing the stability and speed of BSC, in particular in the presence of quantum computers.

The scientific novelty of the obtained results of the dissertation is as follows:

1. Research confirms a new methodology for estimating the evidence-based resistance of block symmetric ciphers to attacks of differential and linear cryptanalysis, which, in contrast to existing ones, is based on the use of theoretical values of maximums of transition laws of XOR tables encryption transformations. In this case, encryption transformations are considered as random substitutions.

2. For the first time, an approach to the design of SPN block symmetric ciphers with improved dynamic indicators of arrival to the state of random substitution, which is sufficient to increase the minimum number of S-blocks activated in the first cycles of encryption transformations.

The basis for the implementation of this approach was the use separately or jointly of three methods aimed at increasing the number of S-blocks activated in the first cycles of encryption transformations, namely:

1) for the first time proposed a method of using in the first cycle SPN cipher increased number of S-blocks based on the implementation of its two-layer design, which allows to increase the minimum number of S-blocks activated in the first cycle and thus mix the number of cycles of cipher arrival to random substitution ;

2) for the first time proposed a method of constructing the first cycle of the cipher using a layer of controlled aggregated S-blocks connected in a chain by

sequentially including them one by one with the addition of the next data segment to the input of each aggregated S-block of the cyclic function S-block with the outputs of others, which provides in the construction of large S-blocks on the strategy of a wide trace activation of all S-blocks of the second cycle and thereby mix the number of cycles of arrival of the cipher to a state of random substitution;

3) for the first time a method of constructing the whole cipher structure using the principles of sequential inclusion of enlarged S-blocks in a chain one after another with the addition of another data segment to the input of each enlarged S-block of the cyclic function allows to increase the number of S-blocks activated on the first cycles of the encryption transformation, and thereby mix the number of cycles of arrival of the cipher to a state of random substitution.

3. A new method for determining the number of cycles of arrival of the cipher to the indicators of random substitution based on the minimum number of only those active S-blocks that fall on the first cycles of transformations and participate in the formation of limit values of differential and linear probabilities.

4. For the first time constructed and confirmed experimentally the laws of distribution of maxima (extreme distributions) of transitions of XOR tables and offsets of tables of linear approximations of ciphers that allowed to confirm the hypothesis concerning rather small range of change of maxima of full differentials and maxima of .

5. The model of random substitution, which in contrast to existing approaches is determined by the values of the maxima of tables of differential differences and displacements of tables of linear approximations of substitutions close to the values of maxima of extreme laws of distribution of transitions XOR tables and displacements of tables of linear approximations of values of random substitutions substitutions close to 3, which provides the use as random (byte) substitutions in the ciphers directly substitutions generated by a random substitution generator.

6. For the first time, the possibility of constructing ciphers using random S-blocks with increased stability and speed, and for the conditions of application of quantum computers.

Practical meaning.

These approaches and methods were used for comparative analysis of ciphers submitted at the time for the competition to create a national standard for block symmetric encryption in Ukraine, and later in the study of cipher Kalyna-2, which became a national standard. Recent developments in this field determine the direction of further improvement of the properties and indicators of evidence-based stability of block symmetric ciphers, focused on the use in the post-quantum period of cryptography.

The results of the work were used in the research work of the private joint-stock company "Institute of Information Technologies" (JSC "IIT") of Kharkiv National University of Radio Electronics and in research and educational process of Kharkiv National University named after V. N. Karazin. Relevant acts of implementation of research results are provided in the appendices.

The research results fully confirm all the proposed provisions.

Keywords: block symmetric encryption technologies, block symmetric cipher, dynamic indicators of cipher arrival to random substitution state, resistance to differential and linear cryptanalysis attacks, active S-blocks, proof stability, maximum differential probability, maximum linear probability, random substitution, random substitution model, cipher performance indicators, randomness indicators, methods of improving encryption transformations.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

у фахових виданнях України:

1. Горбенко И.Д., Лисицкий К.Е. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным. *Радиотехника.* 2014. № 176. С. 27–39. (Особистий внесок здобувача: участь у формуванні всіх розділів роботи та в обґрунтуванні методики експериментів).

2. Лисицкая И. В., Настенко А. А., Лисицкий К. Е. Большие шифры – случайные подстановки. Сравнение показателей статистической безопасности блочных симметричных шифров, представленных на украинский конкурс. *Восточно-Европейский журнал передовых технологий*. 2012. Т. 6, № 9(60). С. 11–21. (Особистий внесок здобувача: участь у формуванні всіх розділів роботи, особливо вступу та обґрунтуванні методики експериментів).

у фахових виданнях України, що входять до міжнародних наукометричних баз:

3. Лисицкая И. В., Лисицкий К. Е., Родинко М. Ю., Головко И. А., Жариков И. И., Корниенко М. А., Кулеба М. В. Экспериментальные данные по определению динамических показателей прихода блочных симметричных шифров к состоянию случайной подстановки. *Радіоелектроніка, інформатика, управління.* 2017. № 1. С. 129–141. (Web of Science). (Особистий внесок здобувача: участь у формуванні узагальнених показників приходу сучасних шифрів до стану випадкової підстановки, відбір та редагування матеріалу статті).

4. Лисицкий К. Е. Вырожденные S-блоки. *Радіоелектроніка, інформатика, управління*. 2018. № 1. С. 129–138. (Web of Science).

у періодичному науковому виданні держави, яка входить до Організації економічного співробітництва та розвитку, що входить до міжнародної наукометричної бази:

5. Dolgov V. I., Lisitska I. V., Lisitskiy K. Ye. The new concept of block symmetric ciphers design. *Telecommunications and Radio Engineering*. 2017. Vol. 76, Is. 2. P. 157–184. (SCOPUS, United States). (Особистий внесок здобувача: виконання розрахунків відносно показників використання випадкових S-блоків, оцінок продуктивності конструкції, а також участь у виконанні аналізу відомих рішень по побудуванню сучасних шифрів і формуванні вдосконалених методів їх проєктування).

6. Lisitskiy K. E. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers. *International Journal of Computer Network and Information Security.* 2013. Vol. 6, No. 1. P. 11–18. (Hong Kong S.A.R., China).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Лисицкая И., Лисицкий К. Сравнение по эффективности цикловых преобразований современных шифров // Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XVI міжнар. наук.-практ. конф., 21–24 травня 2013 р., Київ, 2013. С. 53. (Очно). (Особистий внесок здобувача: участь в підготовці матеріалів доповіді та виступ перед фахівцями).

8. Лисицкий К. Е. Новое усовершенствование Rijndael // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : матеріали міжнар. наук.-практ. конф., 10–11 квітня 2016 р., Київ, 2016. С. 51.

9. Lisickiy K. E., Dolgov V. I., Lisickaya I. V. Cipher with improved dynamic indicators of the condition of a random substitution // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) : 4th International Date of Conference, 10–13 Oct. 2017 // Date Added to IEEE Xplore : ISBN Information: INSPEC Accession **Number:** 17484901, 04 Jan. 2018, P. 396–399. **DOI:** 10.1109/INFOCOMMST.2017. 8246424 (Заочно). (Особистий внесок

здобувача: участь у створенні тенічного рішення, розробка програмної моделі та дослідженні її показників).

10. Лисицький К. Є. Удосконалена конструкція початкового перетворення для SPN шифрів // Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XX ювілейної міжнар. наук.-практ. конф., 22–24 травня. 2018 р., Буга, Київська область, 2018. С. 106–108. (Очно).

Наукові праці, які додатково відображають наукові результати дисертації:

11. Лисицкий К. Е. Максимальные значения полных дифференциалов и линейных корпусов блочных симметричных шифров. *Технологический аудит и резервы производства.* 2014. Т. 1, № 1(15). С. 47-52.

12. Лисицкий К. Е. Закон распределения вероятностей смещений таблиц аппроксимаций случайных подстановок. *Радиотехника*. 2017. № 189. С. 81–89.

13. Лисицький К. Є. Оптимізація перспективних алгоритмів блокового симетричного перетворення по критеріям швидкодії і стійкості. *Математичне та комп'ютерне моделювання*: зб. наук. праць / Інститут кібернетики імені В. М. Глушкова Національної академії наук України. Кам'янець-Подільський національний університет імені Івана Огієнка. 2017. Вип. 15. С. 115-119.

14. Лисицкий К. Е., Лисицкая И.В. Математическая модель случайной подстановки. *Радиотехника*. 2020. № 202. С. 116–124. (Особистий внесок здобувача: участь у формуванні всіх розділів роботи та в обґрунтуванні методики та постановці експериментів).

15. Лисицкий К. Е. О методике оценки законов распределения вероятностей максимумов полных дифференциалов и смещений линейных оболочек блочных симметричных. *Прикладная радиоэлектроника.* 2015. Т. 14, № 4. С. 335–338.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БСШ (BSC) — блоковий симетричний шифр;

$DP_{\max}$ — максимальне значення диференціальної ймовірності таблиці XOR різниць S-блоку;

$LP_{\max}$ — максимальне (виключаючи перші входи в перший рядок і перший стовпець) значення лінійної ймовірності таблиці ЛАТ S-блоку;

ЛАТ — лінійна апроксимаційна таблиця підстановки;

$AMDP$ — середнє значення максимумів таблиць XOR різниць шифруючого перетворення (шифру);

$AMLHP$ — середнє значення максимумів лінійних апроксимаційних таблиць (лінійних корпусів) шифруючого перетворення (шифру);

SPN — підстановлювально-перестановлювальна схема;

$N_S(\Delta x, \Delta y)$— значення комірки таблиці XOR різниць для вхідної різниці Δx і вихідної різниці Δy S-блоку S;

$NS_\alpha(\alpha,\beta)$ — значення зміщення комірки таблиці лінійних апроксимацій S-блоку S_a для вхідної маски α і вихідної маски β;

δ-рівномірне відображення — відображення F: $G_1 \to G_2$, таке, що для усіх $\alpha \in G_1$, $\alpha \neq 0$ та $\beta \in G_2$ виконується умова $\{z \in G_1 | F(z + \alpha) - F(z) = \beta\}| \leq\leq \delta$;

ß — число розгалужень;

$ß_L(D)$ — лінійне число розгалужень дифузійного шару D;

$ß_D(D)$ — диференціальне число розгалужень дифузійного шару D;

MADP — максимум середнього (за множиною ключів) значення диференціальної ймовірності шифруючого перетворення (шифру);

MALHP— максимум середнього (за множиною ключів) значення лінійної ймовірності шифруючого перетворення (шифру);

EDP (*ADP*) — середнє (за множиною ключів) значення диференціальної ймовірності шифруючого перетворення (шифру);

ELP (ALP) — середнє (за множиною ключів) значення лінійної ймовірності шифруючого перетворення (шифру);

π — підстановка;

S_n — симетрическьа група підстановок;

$Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k)$ — ймовірність події, яка міститься в тому, що значення диференціальної таблиці випадково взятої підстановки π степеня 2^m для переходу вхідної різниці ΔX в відповідну вихідну різницюΔY буде дорівнювати $2k$;

$\Lambda_{m,2k}$ — число переходів таблиці диференціальних різниць підстановки степеня 2^mобумовленого типу рівних $2k$;

LAT_π — лінійна апроксимаційна таблиця (ЛАТ) для підстановки π;

LAT_π^* — лінійна апроксимаційна таблиця зміщень для підстановки π;

$LAT_\pi(\alpha, \beta)$ — число рівностей парності між лінійною комбінацією вхідних бітів (що визначаються маскою α по входу в LAT_π підстановки по рядках) і лінійною комбінацією вихідних бітів (що визначаються маскою β по входу в таблицю LAT_π підстановки по стовпцях);

$\lambda(\alpha, \beta)$ — випадкове число, що відповідає значенню лінійної апроксимаційної таблиці підстановки $LAT_\pi(\alpha, \beta)$, коли підстановка π обрана рівноймовірно з множини S_2^n;

$E[\lambda(\pi, 2k)]$ — очікуване число комірок таблиці LAT_π^*, що мають значення $2k$;

$\lambda(\pi)$ — найбільший вхід LAT_π^* для відображення π, узятого над всіма невиродженими α і β;

МДВ функція — породжуюча матриця сепарабельного коду з максимальною відстанню.

ВСТУП

Обґрунтування вибору теми дослідження. Технології блокового симетричного шифрування через ряд переваг були й залишаються основним методом реалізації однієї з базових послуг інформаційної безпеки – конфіденційності. Основні з них: висока захищеність даних, висока швидкість перетворень, простота апаратної, програмної й програмно-апаратної реалізацій та інші. Під технологіями блокового симетричного шифрування далі розуміються дві основні складові: науково-методичний апарат проєктування й розробки блокових симетричних шифрів, а також науково-методичний апарат криптоаналізу й оцінки показників ефективності алгоритмів блокового симетричного шифрування. Процес удосконалення цих технологій не залишається на місці. На зміну шифрам, що виправдали себе, приходять більш перспективні алгоритми.

Особливістю сучасного етапу розвитку криптографії є поява квантових комп’ютерів, властивості яких суттєво розширюють можливості криптоаналізу.

Це вимушує заново переглядати існуючі концепції та підходи для визначення показників стійкості багатьох алгоритмів шифрування. Особливо залежними від можливостей квантових комп’ютерів виявилися несиметричні методи шифрування. Однак суттєві обмеження виникли і для симетричних схем.

Зараз вже розгорнута інтенсивна робота по визначенню вимог до криптографії постквантового періоду. Цей напрям досліджень став провідним у розвитку сучасних технологій захисту інформації. Головним завданням стало визначення шляхів і підходів для забезпечення надійності систем захисту інформації з урахуванням можливостей квантової криптографії.

Для симетричної криптографії, як свідчать дослідження, постквантовий етап потребує використання шифрів з підвищеною довжиною блоку шифрування (більше ніж 256 біт) і швидкодією. Багато з відомих шифрів не вкладаються в ці межі і вимагають удосконалення. Для технологій БСШ на перспективу є необхідність подальшого збільшення стійкості і швидкодії шифрів з орієнтацією на їх використання в постквантовий період розвитку криптографії.

Наведене визначає актуальність теми дисертаційної роботи, яка спрямована на удосконалення методів проєктування БСШ з підвищеною стійкістю та швидкодією для умов постквантової криптографії.

Метою досліджень є удосконалення методів побудови блокових симетричних шифрів з підвищеною криптостійкістю і швидкодією в умовах можливого застосування квантових методів криптоаналізу.

Завдання досліджень:

- аналіз наявних методів і засобів побудови перспективних БСШ за критеріями стійкості і швидкодії;

- обґрунтування вимог до БСШ при їх використанні в перехідний та постквантовий період;

- удосконалення та подальший розвиток методології оцінки стійкості БСШ у частині математичного опису властивостей шифрів як випадкових підстановок;

- розробка вдосконаленої математичної моделі випадкової підстановки;

- розробка (удосконалення) методів оцінки динамічних показників приходу БСШ до стану випадкової підстановки;

- обґрунтування вдосконалених методів проєктування БСШ в умовах постквантової криптографії за критеріями стійкості та швидкодії;

- практичне застосування запропонованих методів для побудови перспективних БСШ з поліпшеними показниками стійкості та швидкодії;

- розробка програмних моделей вдосконалених блокових симетричних криптоперетворень;

- експериментальне дослідження показників стійкості та швидкодії розроблених моделей БСШ;

- розробка рекомендацій та пропозицій стосовно застосування отриманих наукових та практичних результатів.

Підсумком досліджень роботи має стати вирішення важливої наукової та практичної задачі, яка полягає в формуванні вдосконалених методів проєктування блокових симетричних шифрів з підвищеною стійкістю та швидкодією, орієнтованих на використання в постквантовий період розвитку криптографії.

Зв'язок роботи з науковими програмами, темами. Дисертаційна робота виконувалася відповідно до планів наукових досліджень Харківського національного університету радіоелектроніки, Харківського національного університету імені В.Н. Каразіна, а також Акціонерного товариства (ЗАТ «ІІТ», м. Харків).

В Харківському національному університеті радіоелектроніки та ЗАТ «ІІТ» автор роботи брав участь у виконанні НДР «Розробка перспективних методів та засобів криптографічного захисту інформації в державних відомствах України» №ДР0102U003739, а також в НДР «Дослідження та розробка перспективних криптографічних систем та протоколів захисту інформації у телекомунікаційних системах та мережах України» № ДР 0103U001981 та інших.

В Харківському національному університеті імені В.Н. Каразіна брав участь у виконанні держбюджетної науково-дослідної теми "Аналіз стану, обґрунтування вимог та напрямків розвитку, стандартизація розробка та впровадження криптографічних систем для надання електронних довірчих послуг" (№ ДР 0116U000810). Приказ МОН України № 158 від 26.02.2016 г.

Об'єктом дослідження є процеси проєктування і створення блокових симетричних шифрів з підвищеною криптостійкістю і швидкодією для застосування в постквантовий період.

Предметом дослідження є методи й засоби побудови блокових симетричних шифрів з підвищеною криптостійкістю і швидкодією для застосування в постквантовий період.

Методи дослідження: теорія ймовірностей, математична статистика, системний аналіз, методи статистичних іспитів і прикладної криптографії.

Методи системного аналізу використовувалися при обґрунтуванні рішень з побудови удосконалених конструкцій БСШ і порівняльної оцінки показників стійкості.

Методи теорії ймовірностей і математичної статистики використовувались при дослідженні показників випадковості підстановок і підстановлювальних перетворень (шифрів), а також в процесі обробки результатів статистичних експериментів.

Методи статистичних випробувань використовувалися при виконанні експериментальних досліджень з оцінки ефективності застосування підстановлювальних конструкцій різних типів сучасних шифрів, а також при вивченні динамічних показників приходу шифрів до стану випадкової підстановки.

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 зі 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 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 випадкові (байтові) підстановки 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.

Ці підходи та методи були використані для порівняльного аналізу шифрів, представлених у свій час на конкурс по створенню національного стандарту блокового симетричного шифрування України, а пізніше при дослідженні шифру Калина-2, що став національним стандартом.

Останні розробки в цієї галузі визначають напрям подальшого вдосконалення властивостей і показників доказової стійкості блокових симетричних шифрів, орієнтованих на використання в постквантовий період розвитку криптографії.

Практичне значення отриманих результатів:

Результати роботи використані при виконанні ряду НДР, а також в навчальному процесі, зокрема знайшли зацікавленість і застосування такі з них:

1. Вперше розраховані та підтверджені експериментально закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій підстановлювальних перетворень і шифрів, як підстановлювальних перетворень. Відповідно до отриманих результатів зроблено висновок, що всі сучасні шифри мають досить малий діапазон зміни максимумів повних диференціалів і максимумів зміщень лінійних корпусів. Практично для оцінки показників доказової стійкості цих шифрів можна користуватися результатами оцінок максимальних диференціальних ймовірностей і максимальних лінійних ймовірностей. Ці результати використано при розробці нових конструкцій сучасних шифрів (у тому числі національного стандарту БСШ України) та при їх криптоаналізі.

2. Розроблені та запатентовані нові конструкції шифрів ШУП-1 і ШУП-1М з 256-бітовим входом, що пропонуються для використання в постквантовій криптографії. Ці шифри володіють поліпшеними показниками стійкості й швидкодії. За динамічними показниками приходу до стану випадкової підстановки запропоновані конструкції перевершують всі відомі рішення.

3. Розроблені нові конструкції шифрів ШУП-2 і ШУП-2М з 256-бітовим входом, орієнтовані на використання в постквантовій криптографії. Ці шифри стають випадковими підстановками вже на другому циклі, чого не може реалізувати жоден з відомих SPN шифрів.

4. Розроблено та запатентовано вдосконалену конструкцію шифру Rijndael і розроблено вдосконалену конструкцію шифру Калина з поліпшеними динамічними показниками приходу до стану випадкової підстановки. Запропоновані конструкції знімають обмеження на криптографічні показники S-блоків цих шифрів.

5. Розроблені програмні моделі засобів оцінки динамічних показників приходу шифрів до стану випадкової підстановки, які використовуються при

криптоаналізі сучасних БСШ. Використано при розробці національного стандарту України.

6. Отримані конкретні значення показників стійкості розроблених конструкцій шифрів (значення *AMDP* і *AMLHP*) до атак диференціального та лінійного криптоаналізу, що дозволило зробити висновок про те, що розглянуті шифри не поступаються за даними показниками шифру Rijndael і іншим відомим конструкціям сучасних шифрів. Вони використані при розробці і аналізі показників стійкості національного стандарту України.

Запропоновані методи оцінки стійкості та проєктування БСШ реалізовані в системах криптографічного захисту інформації при виконанні ряду державних НДР: Акт реалізації результатів наукових досліджень аспіранта Харківського національного університету ім. В. Н. Каразіна Лисицького Костянтина Євгенійовича у діяльність Приватного Акціонерного Товариства ЗАТ «Інститут інформаційних технологій» від 17 квітня 2018 р., Акт впровадження результатів наукових досліджень аспіранта Харківського національного університету імені В. Н. Каразіна Лисицького Костянтина Євгенійовича в наукову роботу кафедри БІСТ Харківського національного університету імені В. Н. Каразіна від 15 квітня 2018 р., та Акт реалізації результатів наукових досліджень аспіранта Харківського національного університету імені В. Н. Каразіна Лисицького Костянтина Євгенійовича в наукову роботу кафедри БІТ Харківського національного університету радіоелектроніки від 14.05.2018 р., які надані у Додатку Д.

Результати роботи втілені також в навчальний процес кафедри БІСТ національного університету імені В. Н. Каразіна при читанні дисципліни «Криптологічні методи в кібербезпеці» для магістрів спеціальності «Кібербезпека», а також для магістрів спеціальності «Безпека інформаційних і комунікаційних систем», при курсовому проєктуванні з дисципліни «Прикладна криптологія» а також при виконанні магістерських дипломних робіт (Акт впровадження результатів дисертаційних досліджень аспіранта факультету комп’ютерних наук Харківського національного університету імені

В. Н. Каразіна Лисицького Костянтина Євгенійовича в навчальний процес від 10 квітня 2018 року також представлений в Додатку Д).

Особистий внесок здобувача.

У роботах, які написані у співавторстві, автору належить: в [1] – участь у формуванні всіх розділів роботи та в обґрунтуванні методики експериментів; в [2] – собистий внесок здобувача: участь у формуванні всіх розділів роботи, особливо вступу та обґрунтуванні методики експериментів; [3] – особистий внесок здобувача: участь у формуванні узагальнених показників приходу сучасних шифрів до стану випадкової підстановки, відбір та редагування матеріалу статті; [5] – собистий внесок здобувача: виконання розрахунків відносно показників використання випадкових S-блоків, оцінок продуктивності конструкції, а також участь у виконанні аналізу відомих рішень по побудуванню сучасних шифрів і формуванні вдосконалених методів їх проєктування; [7] – особистий внесок здобувача: участь в підготовці матеріалів доповіді та виступ перед фахівцями; [9] – особистий внесок здобувача: участь у створенні тенічного рішення, розробка програмної моделі та дослідженні її показників; [14] – особистий внесок здобувача: участь у формуванні всіх розділів роботи та в обґрунтуванні методики та постановці експериментів.

Дисертація є розвитком результатів робіт [1; 2; 3; 4; 5; 6].

Апробація результатів дисертації. Основні результати дисертації доповідалися та були ухвалені на науково-технічних конференціях. В їх числі: XVI Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, Державна служба спеціального зв'язку та захисту інформації України, 21–24 травня 2013 р.); XVIII Науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, Державна служба спеціального зв'язку та захисту інформації України, 25–26 травня 2016 р.); Науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (Київ, Київський національний університет імені Тараса Шевченка,

10–11 квітня 2016 р.); Міжнародна наукова конференція «Питання оптимізації обчислень (ПОО-XLIV)» (Кам’янець-Подільський, Кам’янець-Подільський національний університет імені Івана Огієнка, 26–29 вересня 2017 р.); XX Ювілейна Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Буча, 22–24 травня 2018 р.); International Conference «TCSET’2010», (Lviv-Slavske, February 23–27 2010) та інші.

Публікація результатів роботи.

Публікації. Основні результати дисертаційної роботи викладені у 11 статтях: 2 з них в наукових фахових виданнях України, 2 у закордонних виданнях, 2 в виданнях, що входять до науково-метричних баз SCOPUS, Web of science та більш ніж в 6 матеріалах і тезах наукових конференцій.

Структура та обсяг дисертації.

Дисертаційна робота складається зі вступу, п'яти розділів, загальних висновків, списку використаних джерел і п'яти додатків. Обсяг загального тексту дисертації складає 220 сторінок (9,25 д. а.)., з них основного тексту 164 сторінки (6,7 д. а.). Робота ілюстрована 38 таблицями 5 рисунками. Список використаних джерел містить 130 найменувань.

РОЗДІЛ 1

СТАН СУЧАСНИХ ТЕХНОЛОГІЙ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ. ОБГРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ

Стрімкий розвиток сучасних інформаційних технологій в Україні, що почався в кінці XX століття, не знижує своїх темпів і на початку XXI століття. Комп'ютерні технології роблять все більший вплив на всі сфери людської діяльності. Постійне збільшення швидкості й обсягів переданих в інформаційних системах даних підвищує ефективність виробничих процесів, сприяє розширенню ділових операцій.

Саме тому посилюються вимоги до інформаційної безпеки. Під нею розуміється захищеність інформації та підтримуючої інфраструктури від випадкових і навмисних впливів, які можуть завдати шкоди власникам або користувачам інформації. Забезпечення безпеки інформаційної системи є однією з найважливіших задач при її експлуатації. Від збереження конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежить швидкість прийняття рішень, ефективність і надійність її роботи[5] [31]. Рішення цього завдання покладається на криптографічні методи й засоби, без наявності яких сьогодні не мислиться жодної скільки-небудь відповідальної державної інформаційної системи.

На даному етапі розвитку криптографії застосовуються як симетричні, так і несиметричні криптографічні алгоритми захисту. Це обумовлюється тим, що перші здатні забезпечити високу швидкість шифрування, а другі – модель взаємної недовіри й захисту, тобто ситуацію, коли користувачі інформаційних систем не хочуть нікому довіряти свої особисті ключі та параметри, але при цьому хочуть мати гарантію компенсації втрат, якщо їх обдурять. Засоби блокового симетричного шифрування при цьому займають особливе місце в

[5] Тут 30-ма джерелами, виключаючи 6-ть перших, закінчується перелік частини робіт, виконаних з участю автора, і починаються посилання на роботи інших авторів.

загальному комплексі засобів захисту, бо вони забезпечують з одного боку найбільш масові транзакції, а з другого, – блокові шифри використовують як будівельні блоки для створення генераторів псевдовипадкових чисел, потокових шифрів, геш-функцій і таке інше. БСШ можуть служити основою механізмів автентифікації повідомлень, забезпечення цілісності даних, симетричних схем цифрового підпису (імітоприкладок) і різних криптопротоколів [31; 32; 33; 34; 35; 36; 37; 38].

Тут слід зазначити, що рівень криптографічного захисту інформаційного простору держави суттєво впливає на забезпечення її національного суверенітету і можливості проведення незалежної економічної політики. Тому природним є прагнення провідних держав світу вирішувати задачі захисту інформації найбільш сучасними на даному етапі розвитку методами, причому засобами національної розробки.

Все це свідчить про те, що розвиток технологій блокового шифрування є особливо актуальним для технологічно розвинених держав, в тому числі й України. Нові досягнення та відкриття в цій галузі можуть посприяти створенню найбільш актуальних стандартів шифрування з максимальними показниками стійкості до атак криптоаналізу, більшої швидкодії, максимальним розміром блоку даних і таке інше.

1.1 Загальна характеристика сучасного етапу розвитку технологій захисту інформації в Україні

Далі будемо говорити про блокові симетричні шифри. Скористаємося частково матеріалами роботи [6].

І сьогодні блокове шифрування продовжує користуватися великою популярністю у всьому світі. Реалізація блокових шифрів досить проста, а швидкість виконання програмних реалізацій знаходиться на рівні, що дозволяє якісно вирішувати завдання інформаційного обміну в сучасних системах телекомунікацій як єдине ціле. Це значно збільшує стійкість перетворень до атаки повним перебором і дозволяє використовувати різні математичні та алгоритмічні перетворення при побудові криптографічних примітивів.

Блокові шифри стали основою, на якій реалізовані практично всі криптосистеми. Методика створення ланцюжків із зашифрованих блоковими алгоритмами байтів дозволяє шифрувати ними пакети інформації необмеженої довжини. Така властивість блокових шифрів, як швидкість роботи, використовується асиметричними криптоалгоритмами, повільними по своїй природі. Відсутність статистичної кореляції між бітами вихідного потоку блокового шифру використовується для обчислення контрольних сум пакетів даних і при гешуванні.

Розвиток сучасної технологічної бази захисту інформації не мислиться без вдосконалення і подальшого розвитку власне технологій блокового симетричного шифрування. У даному разі розуміється дві основні складові. Перша – це науково-методичний апарат проєктування і розробки блокових симетричних шифрів, і друга, – науково-методичний апарат криптоаналізу і оцінки показників ефективності алгоритмів блокового симетричного шифрування.

Одночасно з розвитком технологічної бази криптографічного захисту інформації в Україні за останній час зроблені серйозні кроки і в напрямку розвитку і зміцнення законодавчої бази.

Виконана велика робота по гармонізації національних стандартів з міжнародними (стандарти ISO/IEC 18033-1,2,3, і ін.). Прийнятий закон про документи і документообіг забезпечив надання кожному користувачеві послуги із захисту інформації з необхідним рівнем гарантій. Відповідні вимоги визначені до захисту платіжних документів в системах клієнт-Банк, в внутрішньобанківських та міжбанківських платіжних системах. У всіх цих документах та системах важлива роль в забезпеченні завдань захисту інформації відводиться симетричним методам шифрування.

Актуальність подальшого прогресивного розвитку технологій симетричного шифрування яскраво підтверджується організацією і проведенням міжнародних конкурсів, що пройшли в останні десятиліття AES (за вибором нового стандарту шифрування США), а також NESSIE і CRYPTREC.

Аналогічним шляхом пішла й Україна. 30 червня 2006 року на сайті ДСТЗІ України з’явилося офіційне оголошення про проведення конкурсу з висунення кандидатів на національний стандарт шифрування [39]. У процесі проведення конкурсу було розглянуто п’ять пропозицій, з яких на остаточний розгляд було представлено чотири (шифри ADE, Калина, Мухомор і Лабіринт). У відборі та аналізі представлених рішень взяли участь вчені та розробники колективу ЗАТ ”ІІТ”, які представили на конкурс дві свої пропозиції (шифри Калина і Мухомор). Робота над експертизою проєктів зажадала освоїти й вже наявний міжнародний досвід, і форсувати розробку власних підходів і методик, що дозволяють прискорити процес аналізу і прийняття рішень. За порівняно невеликий термін вдалося виконати завдання якісної експертизи представлених рішень і встановити, що українські пропозиції знаходяться на досить високому рівні (не гірше переможців минулих конкурсів Rijndael-я та інших). Підсумком цієї великої роботи стало те, що чотири роки тому модифікований варіант шифру Калина був прийнятий як національний стандарт блокового симетричного шифрування [40].

Прийняття стандарту, однак, не зупинило подальшого пошуку шляхів удосконалення наявних рішень. Навіть якщо вважати, що запас стійкості прийнятих стандартів блокового шифрування є достатнім і для перспективи, продовжують залишатися актуальними питання подальшого нарощування їх показників продуктивності та оперативності (тут маються на увазі реалізація принципів розпаралелювання обчислювань і скорочення витрат на реалізацію процедур розгортання ключів). До того ж прогрес в зростанні можливостей обчислювальних засобів ставить перед криптографами нові задачі.

Сьогодні технології захисту інформації вступають в епоху квантової криптографії, що змушує заново переглянути багато аспектів забезпечення надійного захисту комплексів систем зв’язку й управління.

Це означає, що робота з пошуку найбільш перспективних рішень і подальшого розвитку і вдосконалення технологій блокового симетричного шифрування для України зберігає свою актуальність і потрібність.

1.2 Відомості про сучасні методи проєктування БСШ

У роботах [22,30], виконаних з участю автора дисертації, а також роботі [41] представлений огляд принципів побудови сучасних шифрів.

Поміж лідерів технологій блокового симетричного шифрування в [22] названі шифр Rijndael [42], що став переможцем конкурсів AES і NESSIE, а також шифр IDEA NXT, який народився на основі шифру IDEA (International Data Encryption Algorithm – Міжнародний алгоритм шифрування даних [43]), розроблений свого часу як пропонований стандарт шифрування [44]. Компанія MediaCrypt AG – власник технології IDEA NXT вважає, що IDEA NXT є сімейством блокових симетричних алгоритмів шифрування наступного покоління. Це і визначило включення цього сімейства шифрів в коло перспективних розробок.

Відмічені також чотири останніх розробки з побудови блокових шифрів: Мухомор [45; 46], розроблений працівниками ЗАТ «ІІТ» (м. Харків), блоковий шифр з білоруського стандарту СТБ 34.101. 31-2011, що з’явився порівняно нещодавно [47], новий стандарт блокового симетричного шифрування України Калина-2 [48] і новий російський стандарт «Кузнечик» [49, 50].

В процесі виконання огляду була розглянута робота Susan Landau [51], присвячена саме детальному аналізу джерел появи нового стандарту AES і обговоренню й оцінки перспективності прийнятих основних проєктних рішень. Це забезпечило підтримку стандарту світовою криптографічною спільнотою. Проводиться точка зору, що ця розробка стала закономірним підсумком розвитку світової криптографічної думки.

В роботі [51] відзначається ряд робіт і пропозицій, виконаних на шляху до Rijndael-я. Нагадаємо їх тут.

Willi Meier і Othmar Staffelbach припустили, що певні приклади нелінійностей, що використовуються математиками, можуть бути придатними для криптографічного системного проєкту [52]. Ґрунтуючись на цих ідеях, Josef Pieprzyk запропонував алгебраїчні методи для будівництва нелінійних

функцій [53; 54]. Kaisa Nyberg досліджувала S-блоки й застосувала деякі з ідей Pieprzyk-а при проєктуванні S-блоків [55]. Joan Daemen вивчив циклові функції з точки зору диференціального і лінійного криптоаналізу шифру і запропонував нову парадигму – підхід широкого сліду [56]. З іншими дослідниками, він використовував широкий слід і S-блоки Nyberg в криптосистемі SHARK [57]. Thomas Jakobsen і Lars Knudsen знайшли "інтерполяційну атаку" проти простих алгебраїчних шифрів, таких як SHARK [58]. Двом розробникам SHARK-а Daemen і Vincent Rijmen протиставили криптосистему Square [59]. Knudsen зламав Square, використовуючи різні атакуючі методи [59]. Rijndael, як зазначає автор цитованої роботи, піднявся з праху Square. Далі в роботі відстежується, як ці нитки ткали Rijndael. Загострюється увага на новій пропозиції по реалізації стратегії широкого сліду і обговорюються алгебраїчні аспекти використання математики (вибір поліномів [42; 60]), а також реалізаційні питання [61].

Далі докладно розглядаються принципи побудування та властивості блокових симетричних IDEA подібних шифрів [62; 63], а також висвітлюються особливості побудування шифрів Мухомор [45;46], блокового шифру з білоруського стандарту СТБ 34.101. 31-2011 [47], нового стандарту блокового симетричного шифрування України Калина-2 [48] і нового російського стандарту «Кузнечик» [49; 50].

Огляд особливостей побудування цих відомих конструкцій, представлено в роботі [22]. Зосередимо увагу одразу на зроблених висновках. Основні з них наступні:

1. Безумовним досягненням сучасних конструкторських рішень з побудови шифрів слід вважати реалізацію стратегії широкого сліду, що будується на основі матричного множення в розширеннях полів.

2. Заслуговують на схвалення і підтримку принципи проєктування, застосовані розробниками AES-а такі як:

- простота специфікації й простота аналізу;

- прозорість;

- ефективність.

3. Запропонована нова концепція гнучкого шифрування безумовно є кроком вперед в технологіях блокового симетричного шифрування і якщо є бажання легко може бути реалізована з використанням багатьох інших розробок, а не тільки за допомогою сімейства шифрів IDEA NXT.

4. Наведені в публікаціях підходи й результати оцінки показників стійкості шифрів до атак диференціального та лінійного криптоаналізу є наближеними й потребують уточнення.

5. Сьогодні вже існує підхід, що дозволяє обчислювальним шляхом визначити точні показники стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу. Відповідно з цим підходом відмічені шифри сімейства IDEA NXT. За своїми показниками стійкості вони знаходяться на рівні показників стійкості, що реалізуються багатьма іншими шифрами. Проте, розглянута розробка, також як і шифр Калина-2 в цьому відношенні має деяку перевагу в порівнянні з багатьма іншими (тут маються на увазі Rijndael і шифри, представлені на український конкурс). У трьох зазначених розробках (шифри Мухомор, IDEA NXT, Калина-2 і сюди можна віднести й шифр «Кузнечик») вдається реалізувати динамічні показники приходу шифру до стану випадкової підстановки зменшені на один цикл у порівнянні з іншими відомими рішеннями.

6. Структура X. Lai й J. Massey (архітектура верхнього рівня) не створює скільки-небудь відчутних переваг в порівнянні з конструкцією циклової функції, застосованої в шифрі Калина-2 (Rijndael).

7. В останніх розробках (не SPN шифрів) проглядається прагнення поліпшити динамічні характеристики приходу шифрів до стаціонарних значень максимумів повних диференціалів і лінійних корпусів на основі збільшення числа S-блоків і створення механізмів збільшення мінімального числа S-блоків, що активізуються на першому циклі (шифри Мухомор, IDEA NXT, Білоруський шифр). Це дозволило привести лавинні показники шифрів

останніх розробок (не SPN шифрів) до глибини лавинного ефекту, що дорівнює трьом циклам.

Далі висловлюються нові накопичені думки та пропозиції. Вони спрямовані на подальше вдосконалення технологій проєктування і розробки блокових симетричних шифрів.

1.3 Результати аналізу кращих проєктних рішень з побудування БСШ

Незважаючи на прогресивність рішень розробників розглянутих шифрів, в них реалізовані далеко не всі потенційні можливості забезпечення ефективності виконання початкових циклових перетворень. Так, за динамічними показниками приходу шифру Rijndael-128 до випадкової підстановки (див. розділ 5) він стає випадковою підстановкою за диференціальними показниками мінімум на третьому циклі, а за лінійними показниками лише на четвертому. Це пов’язано з тим, що при активізації одного байту входу в цикловій функції першого циклу активізується лише один S-блок, який на другому циклі активізує чотири S-блоки. Лише на третьому циклі активізуються вже всі 16-ть S-блоків. В результаті на трьох циклах виходить активними мінімум 21 S-блок. Це дозволяє за диференціальними показниками прийти шифру до стану випадкової підстановки на третьому циклі [22]. Для приходу шифру до стану випадкової підстановки за лінійними показниками йому необхідний додатний четвертий цикл [22].

До найбільш прогресивних конструкцій можна віднести шифри Калина-2, Мухомор, «Кузнечик» і шифр з білоруського стандарту. Ці шифри реалізують показники приходу до стану випадкової підстановки близькі до граничних.

Нагадаємо тепер, що відповідно до нової методології оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, запропонованої останнім часом [1; 6], всі шифри (в тому числі і Rijndael) на повноцикловій довжіні стають випадковими

підстановками. Їх стійкість не пов’язана з властивостями S-блоків, що входять в шифр. S-блоки впливають лише на динаміку приходу шифру до стану випадкової підстановки (на число циклів необхідних шифру для приходу за диференціальними та лінійними показниками до показників випадкової підстановки).

Відзначимо далі, що в ході розробки нової методики оцінки стійкості блокових симетричних шифрів був введений додатковий показник ефективності шифруючих перетворень. Цей показник – кількість циклів для приходу шифру до стану випадкової підстановки [1; 4]. Шифр вважається більш досконалим, якщо число циклів приходу до стану випадкової підстановки виявляється меншим.

Звернемо тут увагу також на практику проєктування сучасних шифрів. Кількість циклів шифрування в них обирається в три-чотири рази більшим ніж потрібно для приходу шифру за диференціальними та лінійними властивостями до показників випадкової підстановки (запас стійкості).

Відповідно до вимог конкурсу AES автори зафіксували довжину блоку 128-ю бітами (у вигляді квадрата – матриці стану розміром 4×4 байти) і для 128 бітного ключа кількість раундів шифрування взято рівним 10. Це на межі запасу стійкості. Використання S-блоків з гіршими диференціальними і лінійними показниками виводить шифр за границі встановленого запасу стійкості. Збільшення довжини вхідного блоку і ключів призводить до рішень зі збільшеним числом циклів шифрування (12 і 14 циклів відповідно). У шифрі IDEA NXT використовується 12 циклів зашифрування.

Лінійне перетворення у вигляді матричного добутку, як основа реалізації стратегії широкого сліду, не є єдиним досконалим перетворенням (з максимальним числом розгалужень). Мається на увазі конструкція з включенням S-блоків циклової функції у ланцюжок з послідовним їх запуском одного за іншим [22], що відкриває можливість збільшення числа S-блоків, що активізуються на другому і подальших циклах. А це означає, що динамічні показники SPN шифрів можуть бути поліпшені. До ще одного недоліку можна

віднести і ускладнені схеми розгортання ключів в розглянутих шифрах. Прагнення зробити схеми розгортання ключів подібними за лавинними характеристиками самим шифрам можливо не виправдане. Експерименти зі зменшеними моделями шифрів [64] показали, що шифри з нульовими цикловими підключами приходять до випадкових підстановок за те ж число циклів, що і з ненульовими цикловими підключами (в штатному режимі роботи). Показників випадковості самих S-блоків виявляється цілком достатньо, щоб шифр став випадковою підстановкою незалежно від значень ключових бітів.

Представлені результати дозволяють охарактеризувати стан сучасних технологій проєктування БСШ (орієнтуючись на найбільш прогресивні з них) наступними основними положеннями [22]:

1. Вважається, що показники стійкості шифрів до атак диференціального і лінійного криптоаналізу безпосередньо пов’язані зі значеннями диференціальних і лінійних ймовірностей нелінійних перетворень (S-блоків), що входять до шифрів. Тому в криптографічній літературі вже давно і інтенсивно розвивається науковий напрямок досліджень, пов’язаний з розробкою і пошуком S-блоків з поліпшеними криптографічними показниками;

2. Найбільш прогресивні рішення з побудови БСШ пов’язані з реалізацією ітеративної багатоциклової процедури з використанням лінійного перетворення, що реалізує стратегію широкого сліду (Rijndael, IDEA NXT, Лабіринт, Камелія, Калина, Мухомор, Grand Cru і ін.);

3. Практика побудови блокових шифрів визначила число використовуваних циклів шифрування (запас стійкості), що в три-чотири рази перевищує глибину лавинного ефекту (число циклів, необхідних для приходу шифру до стану випадкової підстановки);

4. Застосовані в більшості відомих шифрів конструкції циклових перетворень забезпечують прихід шифрів до стану випадкової підстановки за

мінімальне число циклів, що перевищує три (виключення становить алгоритм блокового шифрування з білоруського стандарту і шифр Мухомор);

5. Практично всі відомі розробки орієнтовані на використання S-блоків з граничними й близькими до них значеннями диференціальних та лінійних показників, що дозволяє поліпшити показники приходу шифрів до стану випадкової підстановки на один цикл;

6. Досягнуті показники по швидкодії шифрів характеризуються граничним значенням питомих витрат XOR операцій (тактів), що припадають на один S-блок, близьким до двох-трьох (без урахування витрат на виконання процедури розгортання ключів);

7. Наявна концепція побудови схем розгортання ключів для блокових симетричних шифрів орієнтована на реалізацію процедур, що наближаються за своїми властивостями до додаткового шифруючого перетворення.

1.4 Особливості сучасного етапу розвитку криптографії

Світ вступає зараз в період розвитку криптографії, коли з'явилися реальні розробки по побудуванню квантових комп'ютерів. Властивості квантових комп'ютерів суттєво розширюють можливості виконання атак криптоаналізу на чинні шифри [65]. Це вимушує заново переглядати теперішні концепції та підходи для визначення показників стійкості багатьох алгоритмів шифрування.

Особливо залежними від можливостей квантових комп'ютерів виявилися несиметричні методи шифрування. Однак, суттєві обмеження виникли і для симетричних схем. Зараз вже розгорнута інтенсивна робота по визначенню вимог до криптографії постквантового періоду.

Цей напрямок досліджень став провідним у розвитку сучасних технологій захисту інформації. Головним завданням стало визначення шляхів і підходів для забезпечення надійності систем захисту інформації з урахуванням можливостей квантової криптографії.

У США та ЄС вже кілька років назад розпочалися активні роботи щодо підготовки до проведення та реалізації конкурсів на майбутніх кандидатів

квантово-захищених алгоритмів КЗІ [66÷74]. На період до прийняття нових стандартів КЗІ органи зі стандартизації також зробили спроби надати рекомендації стосовно застосування теперішніх стандартизованих алгоритмів КЗІ з урахуванням можливого застосування для криптоаналізу квантових комп'ютерів. Вимоги NIST США до квантово-захищених алгоритмів анонсовано на VII міжнародній конференції з постквантової криптографії, що проходила у лютому 2016 року у Японії [66; 67]. NIST планував вже майже два роки тому назад виконати етапи аналізу, а потім підготоувати відповідні стандарти. Тобто, приблизно у 2022 році слід очікувати появу нових криптографічних стандартів.

Вже зараз NIST США висунув до кандидатів такі мінімальні вимоги:

- відкритість алгоритмів для криптографічного аналізу криптографічною спільнотою світу;
- ефективна реалізація алгоритмів у широкому діапазоні платформ;
- забезпечення як мінімум однієї з функцій криптографічного перетворення – електронний підпис, направлене шифрування, симетричне блокове чи потокове перетворення, гешування, криптографічний протокол тощо;
- наявність теоретичних та емпіричних доказів щодо забезпечення вимог безпеки (стійкості).

Більш конкретні вимоги формулюються NIST США у трьох напрямках [67]:

- вимоги з безпеки (вимоги до стійкості до криптографічного аналізу);

- техніко-економічні вимоги (складність обчислень та витрати на пам'ять);

- технічні характеристики реалізації алгоритмів в різних умовах.

NIST США та ETSI до алгоритмів КЗІ постквантового періоду концентруються на таких вимогах:

*Вимоги до стійкості як цільові вимоги**:***

- мінімальною вимогою до стійкості кандидатів є еквівалент стійкості відносно СБП з довжиною ключа 128 бітів;

- стійкість шифрування до адаптивної атаки на основі обраного шифр тексту;

- забезпечення захисту електронного підпису (ЕП) від екзистенційної підробки в умовах адаптивного вибору повідомлення;

- для протоколу обміну ключів - в умовах моделі безпеки Canetti-Krawczyk [73].

В цілому стандартизовані алгоритми мають забезпечувати криптографічну стійкість:

- до найкращих відомих атак;

- до атак, реалізованих за допомогою квантових обчислень;

- до атак на множині ключів;

- до атак, що допускають паралельні обчислення;

- до атак на основі обраних шифртекстів з встановленим обмеженням на кількість запитів на обрання шифртекстів.

Причому, криптографічна стійкість має буди теоретично доведена, а також надані кількісні та якісні результати попереднього криптоаналізу.

Техніко-економічні вимоги — це обчислювальна ефективність та ефективність використання ресурсів (пам’яті). При цьому обчислювальна ефективність має порівнюватися для апаратної та програмної реалізації за такими показниками як:

- швидкість генерації ключів;
- швидкість зашифрування/розшифрування;
- швидкість накладення/перевірки підпису;
- швидкість обміну ключами.

Стосовно ефективності використання ресурсів, пропонуються такі показники:

- довжина ключів та потужність множини ключів для конкретного рівня безпеки:

- розмір шифртексту та електронного підпису.

Техніко-експлуатаційні вимоги.

Як техніко-експлуатаційні вимоги висуваються вимоги мінімальної складності реалізації, простоти використання. При цьому легкість реалізації може бути забезпечена:

- налаштуванням параметрів стандартизованого алгоритму;
- можливістю реалізації на широкому колі платформ та в широкому діапазоні прикладних додатків;
- можливістю реалізації розпаралелювання обчислень;
- стійкістю до фізичних атак типу side-channel.

На початку 2016 року ЄС також розпочав приймати рішення стосовно підготовки до переходу до квантово-захищених алгоритмів [66; 67]. У складі ETSI була сформована робоча група з розробки постквантових стандартів КЗІ. В процесі розгорнутих робіт на першому етапі групою був проаналізований сучасний стан безпеки теперішніх алгоритмів. На основі проведеного аналізу, робоча група сформувала рекомендації щодо параметрів криптографічних алгоритмів, які можуть використовуватися у приватній сфері, а частково і в державному секторі. Більш детальні дані наведено в [66; 67; 68; 69; 70; 71; 72; 73; 74].

1.5 Результати аналізу можливостей застосування симетричної криптографії у постквантовому світі

Перспективним для криптоаналізу блокових симетричних шифрів на квантових комп'ютерах є метод Гровера [65; 66; 67; 68; 69; 70; 71; 72; 73; 74; 75; 76; 77; 78]. Цей метод розв'язує задачу, яку можна сформулювати наступним чином.

Нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент з деякою властивістю (яка легко перевіряється). Потрібно знайти цей елемент. Відмічається, що алгоритм Гровера може бути застосований для криптоаналізу геш-функцій чи симетричних шифрів. При його використанні секретний ключ можна знайти виконавши $\sqrt{K}$ операцій, де

K – розмір ключа. Детальний опис стійкості симетричних систем проти квантового криптоаналізу наведено в табл. 1.1, запозиченої з роботи [76].

З табл. 1.1 видно, що стійкість симетричних шифрів в разі атаки з використанням квантового алгоритму суттєво зменшується. Це означає, що DES може бути повністю скомпрометований і неможливо вважати його стійким.

Таблиця 1.1

Стійкість популярних симетричних шифрів проти квантового криптоаналізу в разі атаки на ключ та на блок повідомлення

№ з/п	Шифр	Розмір блока/ ключа біт	Кількість необхідної пам'яті для атаки на блок повідомлення/ ключ /кубіт	Стійкість у разі атаки на	
				Блок повідомл. квантов. гейтів	Ключ квантов. гейтів
1	AES/128	128/128	128/128	$2^{64}(10^{19,2})$	$2^{64}(10^{19,2})$
2	AES/256	128/256	128/256	$2^{64}(10^{19,2})$	$2^{128}(10^{38,4})$
3	DES	64/56	64/56	$2^{32}(10^{9,6})$	$2^{28}(10^{8,4})$
4	TDES	64/168	64/168	$2^{32}(10^{9,6})$	$2^{134}(10^{40,2})$
5	ГОСТ-28147	64/256	64/256	$2^{32}(10^{9,6})$	$2^{128}(10^{38,4})$
6	Калина-128	128/128	128/128	$2^{32}(10^{9,6})$	$2^{64}(10^{19,2})$
7	Калина-256	256/256	256/256	$2^{128}(10^{38,4})$	$2^{128}(10^{38,4})$
8	Калина-512	512/512	512/512	$2^{128}(10^{38,4})$	$2^{128}(10^{38,4})$
9	Blowfish	64/448	64/448	$2^{32}(10^{9,6})$	$2^{224}(10^{67,2})$

Його стійкість дорівнюватиме 2^{28}. Навіть при AES бажано використовувати ключ довжиною 256 бітів. Тобто алгоритм Гровера, хоча і зменшує стійкість сучасних симетричних криптосистем, але все одно потребує

субекспоненційної кількості квантових гейтів, на відміну від алгоритму Шора. Згідно з табл. 1.1 умовам використання у постквантовій криптографії відповідають лише шифри AES-256, Калина-256, Калина-512.

Усі інші шифри, у тому числі і шифр «Кузнечик-128» і білоруський 128-бітний шифр нездатні забезпечити необхідний рівень стійкості в умовах застосування квантових комп'ютерів (в білоруському шифрі передбачено використання 256 бітного ключа зашифування).

Майже усі наявні шифри потребують удосконалення. Забезпечення необхідного рівня стійкості симетричних криптографічних систем при появі квантового комп'ютера можна тільки за допомогою збільшення розмірів довжини блока та довжини ключа.

Але і за умови збільшення розмірів системних параметрів симетричні системи можуть бути при певних параметрах уразливими для квантового криптоаналізу.

Інше питання полягає в тому, що з ростом довжини блоку, що шифрується, закономірно підвищується і обчислювальна складність виконання операцій шифрування і розшифрування, тобто падає швидкодія.

Наведемо данні з роботи [79]. В цій роботі розглядається випадок досягнення максимальної продуктивності процедури шифрування. Для цього були застосовані наступні програмні та алгоритмічні методи оптимізації:

- загальна таблична реалізація S-блоку і нелінійного змішування байт;

- реалізація байтових перестановок по можливості «явним» способом, тобто з нульовими обчислювальними витратами;

- застосування технік «розгортання» циклів і «inline-підстановки» підпрограм.

Під елементарними мікрооперaціями ALU (Arithmetic and Logic Unit – арифметико-логічний пристрій) розуміються операції, які виконуються як окрема команда ALU мікропроцесора.

Розглядалися мікрооперації ALU, що використані в алгоритмах:

- додавання за модулем 2 (XOR);

- складання з перенесенням розрядів за модулем 2^m, де $m>1$ (ADD); віднімання з перенесенням розрядів за модулем 2^m, де $m>1$ (SUB);

- зрушення вправо (ROTR);

- зрушення вліво (ROTL);

- пересилання машинного слова між регістрами або регістром і пам'яттю (MOV).

Отримані результати для шифрів AES, Калина і Мухомор узагальнені у таблиці 1.2.

Тобто, складність циклового перетворення в залежності від кількості S-блоків можна оцінити як близьку до двох-трьох XOR-ів на S-блок. При переході до шифрування 256-ти бітних блоків обчислювальна складність підвищується майже в три рази

Таблиця 1.2

Складність циклових перетворень шифрів AES, Калини, Мухомор

Алгоритм шифрування	Довжина блоку в бітах (LB)			Кількість циклів шифрування
	LB = 128	LB = 256	LB = 512	
AES	36–38	72–76	144–156	11,13.18
Калина	56–58	112–116	224–232	10,14,30
Мухомор	51–54	131–139	329–345	11,13,18

Перехід від 128 бітного шифрування до 512 бітного (для 30 циклів зашифрування) для Калини коштуватиме зниженням швидкодії більше ніж в 11-ть разів.

Отже, практично усі наявні шифри потребують удосконалення. Розрахунки тут велись простим кратним збільшенням складності одноциклового перетворення.

Більш об'єктивні дані наведені в табл. 1.3, запозиченій з роботи [79].

Таблиця 1.3

Обчислювальні витрати 128-ми бітних шифрів

Кількість циклів	AES	Калина	Мухомор	ADE	Лабіринт
1	48	125	71	48	212
2	84	181	122	84	280
3	120	237	173	120	348
4	156	293	224	156	416
5	192	349	275	192	484
6	228	405	326	228	552
7	264	461	377	264	620
8	300	517	428	300	688
9	336	573	479	336	-
10	393	629	530	393	-
11	-	-	581	-	-

Таким чином, актуальним для постквантового періоду розвитку криптографії становиться питання щодо збільшення швидкодії алгоритмів шифрування, хоча воно зберігає свою актуальність і в сучасній криптографії.

Отже, потрібно вирішити протиріччя між вимогами підвищення стійкості і підвищення швидкодії.

1.6 Постановка задач досліджень роботи

Ця робота виконувалась вже після того, як була сформульована і опублікована нова методологія оцінки БСШ до атак диференційного та лінійного криптоаналізу. У формуванні деяких результатів нової методології приняв участь і автор цієї роботи. Накопичені результати дозволили по новому переосмислити механізми забезпечення стійкості та продуктивності сучасних блокових симетричних шифрів, виявити нові резерви щодо подальшого удосконалення технологій блокового симетричного шифрування, запропонувати нові рішення по побудуванню шифрів, які забезпечують

підвищення стійкості та швидкодії в умовах застосування квантових комп’ютерів.

Отже, метою роботи є підвищення (забезпечення) потрібної стійкості блокових симетричних шифрів при суттєвих обмеженнях на складність їх практичної реалізації в умовах можливого застосування квантових комп’ютерів.

Завдання досліджень сформульовані таким чином:

- виконати аналіз наявних методів побудування блокових симетричних шифрів з підвищеною стійкістю і швидкодією, виділити переваги і недоліки методів;

- розробити теоретичні та експериментальні методи оцінки стійкості блокових симетричних шифрів з використанням апарату випадкових підстановок;

- розробити теоретичні та експериментальні методи оцінки динамічних показників приходу БСШ до стану випадкової підстановки;

- підтвердити працездатність запропонованих методів шляхом побудови нових БСШ з поліпшеними показниками та модернізації вже наявних алгоритмів;

- експериментально підтвердити отримані результати.

Підсумком досліджень роботи має стати вирішення важливої наукової та практичної задачі, яка полягає в розробці методів побудування блокових симетричних шифрів з підвищеною стійкістю та швидкодією орієнтованих на використання в постквантовий період розвитку криптографії.

Висновки до розділу 1

1. Блокові симетричні шифри зберігають свою актуальність й перспективи широкого застосування в сучасних і майбутніх технологіях захисту інформації.

2. Криптографія входить у новий етап розвитку, пов’язаний з очікуваною появою квантових комп’ютерів, що змушує заново переглянути оцінки, на яких зараз базується стійкість сучасних шифрів.

3. Постквантовий період зберігає основний склад критеріїв та вимог, що висувалися до них раніше. На сьогодні стосовно квантових комп’ютерів можна рахувати перспективним криптоаналіз на основі методу Гровера, який вимагає для захисту від атаки довжину блока і ключа більше ніж 256 бітів. Отже, тільки шифри Калина і Мухомор відповідають вимогам їх використання в постквантовий період розвитку криптографії. Тільки перехід до збільшеної довжини вхідного блоку пов’язаний з суттєвим зростанням обчислювальної складності процедур шифрування і розшифрування.

4. Поміж наукових задач, що потребують свого вирішення актуальною для України є задача розробки методів та засобів побудування блокових симетричних шифрів з підвищеною стійкістю і швидкодією.

При підготовці матеріалів розділу використана публікація з участю автора [22].

РОЗДІЛ 2

ОБГРУНТУВАННЯ НОВОЇ МЕТОДОЛОГІЇ ОЦІНКИ СТІЙКОСТІ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ ДО АТАК ДИФЕРЕНЦІАЛЬНОГО ТА ЛІНІЙНОГО КРИПТОАНАЛІЗУ

Ця робота виконувалася в умовах, коли в теорії і методах криптоаналізу, і, зокрема диференціального і лінійного криптоаналізу, відкрився новий напрям натхненний роботами, виконаними протягом останніх років групою вчених кафедри БІТ ХНУРЕ [1; 2; 3; 4; 5; 6].

У проведенні експериментальних досліджень і отриманні ряду важливих результатів взяв участь і автор цієї роботи, спочатку студент ХНУРЕ, а пізніше студент університету імені В.Н. Каразіна [7÷15,24,28,29,80] та інші.

Отримані результати формулюються як нова методологія оцінки стійкості БСШ до атак диференціального і лінійного криптоаналізу.

В цьому розділі нагадуються найбільш суттєві з отриманих за участю автора результати, які вже захищені.

Пошуки, дослідження і результати, отримані саме в цьому напрямку, стали основою формування вдосконалених методів проєктування блокових симетричних шифрів, які є основним науковим результатом цієї роботи.

2.1 Сутність нової методології оцінки стійкості БСШ до атак диференціального і лінійного криптоаналізу

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

Всі сучасні блокові шифри через певне число циклів незалежно від використовуваних в шифрах S-блоків (*звичайно, тут мова йде не про вироджених їх конструкціях*) *набувають властивості випадкових підстановок.*

Тобто по комбінаторним показникам (*числу інверсій, зростань і циклів*), *а також за законами розподілу переходів таблиць XOR різниць* (*повних*

диференціалів) *і законам розподілу зсувів таблиць лінійних апроксимацій* (*лінійних корпусів*) *повторюють відповідні показники випадкових підстановок.*

В результаті значення максимумів повних диференціалів і лінійних корпусів можуть бути визначені розрахунковим шляхом з формул для законів розподілу ймовірностей переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок відповідного степеня.

При цьому, перевірка показників випадковості великих шифрів може бути виконана на основі розробки й подальшого аналізу показників випадковості зменшених моделей, що допускають проведення обчислювальних експериментів в прийнятні (*реальні*) *терміни.*

Малі моделі шифрів, що повторюють свої прототипи, дозволяють оцінити не тільки середні значення максимумів таблиць диференціальних ймовірностей (*AMDP*), і середніх значень максимумів лінійних ймовірностей AMLP) для обмеженої множини ключів, але і розв'язати задачу визначення (перевірки) абсолютного значення максимуму на повній їх множині.

Цей результат перевірений з участю автора на великому числі зменшених моделей багатьох сучасних шифрів [9; 10; 11; 12; 13; 14; 15, 24, 96] та інші.

Він був також підтверджений з використанням повномасштабних версій шифрів при їх активізації 16-бітними вхідними різницями, (роботи з участю автора [9, 10]).

Сформульовані вище положення ілюструються прикладами аналізу диференціальних і лінійних властивостей двох відомих шифрів AES і ГОСТ 28147-89 і ще двох шифрів Калина і Мухомор, представлених на український конкурс (розглядалися повні версії цих шифрів).

Довжина ключа і блоку для AES взята 256 біт, а для шифрів Калина і Мухомор довжини ключів і блоків однакові і рівні 128 бітам (див. табл. 2.1, табл. 2.2).

У таблицях представлені результати, отримані при використанні шифрів в режимі шифрування 16-бітових блоків даних (публікація з участю автора

[29]) (значення 32768 на перших циклах шифрів AES і ГОСТ в таблиці 2.2 та значення 65536 в таблиці 2.1 виникли за рахунок невдалого вибору вихідних двох байтів).

Таблиця 2.1

Поциклові середні значення максимумів повних диференціалів деяких сучасних шифрів

Кількість циклів	AES	ГОСТ 28147-89	Калина	Мухомор
1	65536	65536	65536	**19,4**
2	3652,26	3968.3	40,63	19,2
3	**19,0666**	61952	**18,8**	19,6
4	19,0666	56008.6	18,8	19,2
5	18,8666	31358	19,2	19
6	19,1332	2046,7	18,8	19,2
7	19,2666	973,4	18,6	19,8
8	19,1332	52,2	18,8	19
9	19,0666	**19,1**	19	19,2
10	19,3333	19,5	18,8	19,6
11	19.4	18,7	19,4	19
13	18,8666	19,1	18,6	18,6
14	18.9332	19,4	19	19,2

Для всіх чотирьох шифрів було виконано обчислення максимумів повних диференціалів і зміщень лінійних корпусів з використанням 10-ти ключів шифрування.

Довжина ключа і блоку для Rijndael-я і Serpent-а однакова і дорівнює 128 бітам, а в реалізації шифру Threefish використовувалася довжина для блоку і ключа, що дорівнює 512 бітам.

Таблиця 2.2

Поциклові середні значення максимумів зміщень лінійних корпусів деяких шифрів

Кількість циклів	AES	ГОСТ 28147-89	Калина	Мухомор
1	32768	32768	11008,392	**824,742**
2	9284.27	16384,5	**817,271**	818,621
3	**818.467**	17162	817,718	827,431
4	815	31181,7	814,19	824,193
5	818.5	16150,1	837,349	831,753
6	815.967	16669,5	810,733	814,155
7	832.1	2144,77	820,384	820,975
8	823.133	2380,93	837,917	823,024
9	829.9	**826,833**	809,273	810,196
10	827.4	828,1	821,755	821,316
11	815.6	823,767	827,462	822,385
12	819	821,433	820,291	816,753

В таблицях 2.3 и 2.4 представлені поциклові значення повних диференціалів і поциклові значення зміщень лінійних корпусів для шифрів Rijndael, Serpent, Threefish. Знову взяті повні версії даних шифрів.

Зауважимо, що в шифрі Threefish не застосовуються S-блоки.

Для всіх трьох шифрів було виконано обчислення максимумів повних диференціалів і максимумів зміщень лінійних корпусів з використанням 10 різних випадково згенерованих ключів.

Маються аналогічні результати, виконані за участю автора цієї роботи, з іншими шифрами.

Таблиця 2.3

Поциклові значення максимумів повних диференціалів для 16-битних сегментів

Кількість циклів, *r*	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	16384	18,93	65536
2	8904,25	19,24	65536
3	1911.47	18,64	65536
4	19,24	18,33	42440,04
5	20,31	18,75	30704,23
6	18,83	19,21	9534,57
7	19,21	18,98	37,75
8	19,4	18,37	19,27
9	18,33	19,24	18,78
10	19,17	19,63	18,44

Таблиця 2.4

Математичні сподівання максимальних зміщень лінійних корпусів повних моделей шифрів

Кількість циклів, *r*	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	32768	810,4	32768
2	16313,36	825,0667	32680,93
3	7728,66	828,2667	31306,13
4	817,43	825,9333	23730,93
5	821,98	828,4667	19722,67
6	825,716	824,8667	19722,67

Продовження таблиці 2.4

Кількість циклів, *r*	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
7	817,367	820,3333	7899,8
8	820,167	817,5333	844,0667
9	821,767	820,4	822,1333
10	820,167	816,6	815,8

Наведені результати добре ілюструють процеси приходу шифрів до стаціонарного стану, що повторюють характеристики випадкових підстановок відповідного степеня (роботи з участю автора [8,23]).

Найбільш «повільним» виявився шифр Threefish, а ось шифр Мухомор вийшов на асимптотичні показники відразу після першого циклу (для 16-ти бітного входу).

2.2 Умови приходу ітеративних шифрів до стаціонарного стану випадкової підстановки

Далі увага зосереджується на результатах робіт, виконаних з участю автора. присвячених додатковому обґрунтуванню основного положення нової методології про прихід шифрів до стану випадкової підстановки. В основному тут буде поданий матеріал у вигляді стислого огляду.

До теорії марківських шифрів. Почнемо з одного важливого напрямку розвитку нової методології, пов’язаному з новим підходом до класифікації блокових симетричних шифрів.

Мова йде про можливу помилковість широко експлуатуємої в криптографічній літературі точки зору, відповідно до якої блокові симетричні шифри поділяються на марківські та немарківські [87-90].

Нагадаємо ще один науковий результат, зафіксований в дисертації Настенко А.А. [5]. Результат сформульований наступним чином.

Отримав подальший розвиток математичний апарат опису блокових ітеративних шифрів за допомогою теорії марківських шифрів першого та другого порядків. Доведено, що поциклова послідовність матриць перехідних ймовірностей марківських шифрів збігається до розподілу, що є характерним для розподілу переходів таблиць XOR-різниць випадкових підстановок. Слід додати, що остання частина твердження справедлива і для розподілу зміщень таблиць лінійних апроксимацій випадкових підстановок.

Відправною тут стала робота [91]. В цій роботі запропоновано визначення марківських процесів першого і більш високих порядків у вигляді відповідних рівнянь, що пов’язують сусідні (два або більше) поциклових значень результатів зашифрування.

Розвиток цього напрямку за участю автора цієї роботи відбито в публікації [29]. Наведемо тут її основні положення.

В роботі [91] спочатку виконується критичний огляд робіт по марківським шифрам. Відмічається, що знайомство з роботами по марківським шифрам виявило декілька моментів, що представляються спірними.

Виділено три публікації, в яких оцінки стійкості марківських шифрів будуються на основі використання матриць перехідних ймовірностей одноциклових перетворень [88; 89; 90].

В роботі [89] автори оперують матрицями перехідних ймовірностей для ланцюгів маркова і розглядають результат багатоциклового перетворення за допомогою зведення матриці перехідних ймовірностей одноциклового перетворення в степінь рівну кількості циклів перетворення. Доводиться, що послідовність матриць ймовірностей диференціальних апроксимацій марківського блокового шифру приходить до рівноймовірної матриці при збільшенні кількості циклів.

В роботах [89; 90 та ін.] також вважається справедливим положення про збіжність послідовності матриць ймовірностей диференціальних переходів марківського блокового шифру до рівноймовірної матриці при збільшенні

кількості циклів. В основі цих тверджень лежить математичне зведення в степінь матриць перехідних ймовірностей таблиць диференціальних різниць підстановок. Можна назвати і інші роботи, в яких матриця диференціальних ймовірностей шифру будується на зведенні матриці перехідних ймовірностей одноциклового перетворення в степінь рівну числу циклів (раундів).

Це відмічається в роботі [29]. Маємо своє бачення щодо цих двох випадків, як і щодо твердження про збіжність послідовності матриць середніх диференціальних і лінійних ймовірностей шифрів до рівноймовірних.

Нагадується, що зведення в степінь за правилами прийнятими в математиці обчислення добутку матриць справедливо лише в тому випадку, коли над відліковими значеннями вибірки, що входять в рівняння марківського процесу, здійснюється лінійне перетворення. Коли мова йде про повні диференціали (лінійні корпуси), то для практично всіх відомих ітеративних шифрів цього робити не можна, тому що в таких шифрах циклове перетворення будують з використанням нелінійних операцій (S-блоків).

Подальшим розвитком результатів цієї роботи стала публікація [12]. Вона присвячена приходу ітеративних шифрів до стаціонарного стану, властивому випадковій підстановці.

В цій роботі представлено обґрунтування властивості підстановлювальних перетворень, щодо результату їх добутку. Результатом добутку підстановлювальних перетворень є підстановка випадкового типу.

В [6] говориться, що ця властивість (твердження) є певним «законом природи», який виконується незалежно від нашого бажання.

Розглядається механізм збалансованого перемішування блоків даних при формуванні добутків підстановлювальних перетворень.

Звичайно, тут мова йде не про вироджені підстановки, до яких віднесені підстановки з диференціальними і лінійними показниками, що виходять далеко за рамки середньостатистичних показників випадкових підстановок [26; 93]. Одночасно стає зрозумілим, що використання різних S-блоків в шифрі не приноситиме для них скільки-небудь відчутних переваг.

Відносно шифрів і шифруючих перетворень. Відмічається, що розглянутий в роботі механізм збалансованого перемішування блоків даних буде характерним (справедливим) і для послідовностей шифруючих перетворень ітеративних шифрів. Тільки для шифрів цей механізм не може обійтися без перехідного періоду, пов’язаного з перемішуванням блоків даних з виходів S-блоків між собою.

Це дозволяє перетворити послідовність циклових перетворень в підстановлювальне перетворення з необхідними лавинними властивостями (послідовність шифруючих перетворень (циклів) є добутком підстановлювальних перетворень).

Залишається відзначити, що отримані результати повністю узгоджуються з результатами 3-го розділу цієї роботи про випадкові підстановки. Вони свідчать, що закони розподілу переходів XOR таблиць і таблиць лінійних апроксимацій шифрів повторюють відповідні закони розподілу ймовірностей, наведені в розділі 3 для випадкових підстановок.

Ітеративні шифри є добутком підстановлювальних перетворень. Навіть без введення в цикли випадкових підключів шифр після деякого числа початкових циклових перетворень стає випадковою підстановкою [64]. Для шифрів з сильним лінійним перетворенням цей процес є досить короткочасним (до трьох-чотирьох циклів).

Для шифрів зі слабким лінійним перетворенням цей процес переходу шифру до випадкової підстановки може затягуватися до 7 і більше циклів. Перехідний період приходу до випадкової підстановки, характерний для шифрів, пов’язаний з тим, що при малому числі циклів шифрування булеві векторні функції, що описують циклові перетворення, ще не пов’язані з усіма бітами входу в циклове перетворення.

Необхідно, щоб спрацював механізм перемішування вихідних бітів підстановок, що входять в шифр, який реалізується за допомогою відповідних лінійних перетворень.

Представлені результати повністю підтверджують нову точку зору з питання оцінки безпеки блокових шифрів до атак диференціального і лінійного криптоаналізу [1; 6; 11; 80; 81; 82; 82; 84; 85; 86; 95] та інші.

Максимуми середніх ймовірностей диференціалів і лінійних корпусів повноциклових версій шифрів не залежать від властивостей використовуваних в них S-блоків (виключаючи вироджені їх конструкції).

Далі викладаються результати двох публікацій [16] і [20], які претендують на новизну.

2.3 Розподіл максимумів повних диференціалів і зміщень лінійних оболонок БСШ

Якщо погодиться з тим, що шифри асимптотично стають випадковими підстановками (для кожного ключа це своя випадкова підстановка), то представляється апріорно очевидним, що одна з основних властивостей шифрів повинна полягати в тому, що показники їх стійкості не залежать від ключового матеріалу.

Цей результат перевірено експериментально на великому числі зменшених і великих моделей багатьох сучасних шифрів [6; 84; 95], а також відбито у публікаціях з участю автора [9; 10; 12; 15; 16; 17; 18; 64] та інші.

Проведені експерименти прив’язані до обмеженої множини ключів шифрування (маються поодинокі результати визначення максимумів на всій множині ключів зашифрування для зменшених моделей шифрів [6]).

На основі цих результатів зроблений висновок, що показники стійкості шифрів можна визначати не шляхом усереднення по безлічі ключів, а на підставі визначення максимальних значень диференціальної та лінійної ймовірностей для будь-якого (одного) довільно взятого ключа шифрування. Але цей висновок скоріше варто вважати гіпотезою.

Щоб визнати його достовірним, необхідно переконатися в тому, що для будь-якого шифру – підстановки не існує ключів шифрування, для яких

максимальні диференціальна і лінійна ймовірності помітно відрізняються від результату, отриманого для довільно взятого ключа шифрування.

Вже на рівні представлених в роботах [11; 13; 18 з участю автора], а також в роботах [1; 6; 81; 82; 83; 84; 85 ; 95], результатів експериментів помічено, що результати практично не залежать від використовуваних ключів. Ключі впливають лише на розподіл одного і того ж набору переходів диференціальної таблиці всього шифру.

У цьому підрозділі й ставиться задача визначення максимально досяжних значень переходів таблиць XOR різниць і зміщень таблиць лінійних апроксимацій малих моделей шифрів.

Загальним підходом до вирішення цієї задачі є вивчення поведінки шифруючих перетворень на всій множині ключів шифрування.

В експериментальному відношенні цей підхід ґрунтується на оцінці за допомогою обчислювальних експериментів значень максимумів повних диференціалів і зміщень лінійних корпусів для зменшених моделей шифрів для всієї множини ключів шифрування (це дозволяють зменшені моделі шифрів) і визначенню найбільших досягнутих в процесі експериментів значень цих максимумів і їх числа для диференціальних і лінійних таблиць підстановок.

У математичному відношенні ця задача приводиться до вивчення розподілів максимумів над дуже великою множиною незалежних випадкових величин.

Сьогодні вже є розроблений математичний апарат, який вирішує в загальнотеоретичному плані цю задачу.

Мається на увазі спільна робота вчених Joan Daemen, Vincent Rijmen [92], в додатку до якої вдалося знайти відповідну методику.

Інтерес до цієї методики був викликаний тим, що множинами незалежних змінних, що мають одні і ті ж закони розподілу, можна описати переходи таблиць повних диференціалів і зміщень таблиць лінійних

апроксимацій блокових симетричних шифрів, що розглядаються як підстановлювальні перетворення (випадкові підстановки).

Ця методика була успішно застосована в роботі [20] для визначення законів розподілу максимумів переходів таблиць повних диференціалів і максимумів зміщень таблиць лінійних апроксимацій для зменшених моделей шифрів.

Відповідно до отриманих результатів зроблено важливий висновок.

Всі сучасні шифри мають досить малий діапазон зміни максимумів повних диференціалів і максимумів зміщень лінійних корпусів.

Це означає, що практично для оцінки показників доказової стійкості цих шифрів можна користуватися результатами оцінок максимальних диференціальних ймовірностей і максимальних лінійних ймовірностей, обчислених для довільно взятого (одного) ключа шифрування.

Цей результат відповідно до нової методології оцінки показників стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, що розвивається в роботах Лисицької І.В. [1; 6] та інші, може бути поширений і на повномасштабні версії цих шифрів, що дозволяє перейти до практичного обчислення показників їх стійкості до зазначених атак.

Більш глибокий аналіз матеріалів роботи [92] показав, що по ходу викладу методики її авторами був допущений ряд неточностей (описок), внаслідок чого вихідні положення методики не узгоджуються з результатами їх застосування до розглянутих законів розподілу ймовірностей.

Слід зазначити, що ці неточності не вплинули на правильне уявлення підсумкових результатів. Відповідно правильними слід вважати і результати досліджень, представлених в роботі [20].

Порядок в описі цієї важливої методики і її переклад з виправленнями наведений у Додатку В дисертації.

Далі наводяться результати використання цієї методики визначення законів розподілу максимумів переходів таблиць повних диференціалів і максимумів зміщень таблиць лінійних апроксимацій для зменшених моделей

шифрів і, зокрема, для шифру з нового білоруського стандарту і повномасштабному шифру AES.

Матеріал розділу побудований на публікаціях автора [20; 23].

Вихідною позицією цього підрозділу є основне положення нової методології, відповідно до якого шифри асимптотично становляться випадковими підстановками.

Випадковим підстановкам буде присвячений наступний розділ.

А тут нагадаємо два важливих для теперішнього розділу факти:

- закони розподілу переходів XOR таблиці випадкової підстановки є пуассонівськими;
- закони розподілу зміщень лінійної апроксимаційної таблиці випадкової підстановки є нормальними.

Це означає, що можливо повністю скористатися наведеними в Додатку Б результатами для побудування законів розподілу максимумів XOR таблиць і зміщень таблиць лінійних апроксимацій шифрів, як випадкових підстановок.

Далі розглядається задача оцінки значень максимумів повних диференціалів для міні шифру з 16-бітним входом і 16-бітним майстер-ключем.

Як показано в роботах [8; 16], закони розподілу переходів XOR таблиць міні шифрів асимптотичне повторюють відповідні закони розподілу переходів XOR таблиці випадкової підстановки, які як раз виявляються пуассонівськими [98].

Наведемо спочатку кінцеві результати по побудуванню інтегрального закону розподілу максимумів переходів таблиці повних диференціалів міні шифру.

Результати отримані з використанням математичного апарату, наведеного у Додатку В. Цей інтегральний закон має вигляд:

$$D_{\max}(X) \approx e^{-e^{\frac{18-2\cdot X}{0,692}}}. \qquad (2.1)$$

У табл. 2.5 наводяться результати розрахунків розподілу значень максимумів для всієї множини з 2^{16} ключів.

Таблиця 2.5

Розподіл значень максимумів міні шифру для всієї множини з 2^{16}ключів, розрахованих за виразом (2.1) і результати експерименту

k^* (X_1, X_2)	Pr(k^*)	Розрахунк. значення	Експери-мент
18 (18,16)	$0{,}368 - 1{,}2 \cdot 10^{-8} = 0{,}368$	24117	31268
20 (20,18)	0,9459 – 0,368= 0,5779	37876	32039
22 (22,20)	0,99691 – 0,9459 = 0,051	3343	2126
24 (24, 22)	0,99982 – 0,99691 = 0,0029	191	101
26 (26,24)	0,999990 – 0,99982 = 0,00016	10	2
28 (28,26)	0,9999995 – 0,999990= $8{,}5 \cdot 10^{-6}$	0,5	0

У правій колонці табл. 2.5 наведені також результати обчислювальних експериментів зі зменшеною моделлю білоруського шифру.

З представлених результатів слідує, що значення максимуму максиморуму для зменшених моделей шифрів одне і дорівнює 26, а інші значення максимумів складаються з двох найбільш типових значень 18 і 20.

Значення 26 практично не відрізняється від середнього значення максимумів диференціальних таблиць зменшених моделей шифрів.

Тим самим підтверджується висловлене в роботі [24] та роботах положення про те, що оцінку доказової стійкості шифру можна виконувати на основі значення максимумів диференціальної та лінійної ймовірностей,

отриманих для одного (будь-якого) ключа шифрування (для ітеративних шифрів виконується гіпотеза статистичної еквівалентності [87]).

Для обчислення розподілу значень максимумів лінійних корпусів міні шифру отриманий інтегральний закон у вигляді

$$D_{\max}(X) \approx e^{-e^{\frac{810-X}{20,2}}}. \qquad (2.2)$$

У табл. 2.6 представлені результати розрахунків по визначенню розподілу значень максимумів лінійних корпусів на основі інтегрального закону розподілу ймовірностей (2.2).

Більш детальне застосування цієї методики представлено в розділі 3 при побудуванні законів розподілу максимумів диференціалів XOR таблиць і зміщень таблиць лінійних апроксимацій байтових випадкових підстановок.

Зауважимо, що за результатами раніше виконаної теоретичної та експериментальної оцінки, значення максимуму зміщення лінійної апроксимаційної таблиці випадкової підстановки степеня 2^{16} є 748 (розрахунок) і 720 (експеримент) [23].

Тут вже враховані результати виконаних експериментів, представлених в роботі [8].

З урахуванням цих результатів, а також відповідно до (3.20, див розділ три) маємо $\sigma = 2^{\frac{16-4}{2}} = 2^6$ і тоді a = 64·6,33+0 = 405,2 і b = 64·0,1579 = 10,11.

Видно, що і в. цьому випадку результати експериментів практично повторюють результати розрахунків.

Отже, вперше розраховані й підтверджені експериментально закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій міні шифрів.

Відповідно до отриманих результатів зроблено висновок, що розглянуті шифри мають досить малий діапазон зміни максимумів повних диференціалів і максимумів зміщень лінійних корпусів.

Таблиця 2.6

Розподіл значень максимумів зміщень міні шифру для всієї множини з 2^{16} ключів, розрахованих за виразом (2.2) і результати експерименту

k^* (X_1, X_2)	Pr(k^*)	Число значень	Експери-мент
< 768	$3{,}02 \cdot 10^{-4}$	20	27
770 (770,768)	$6{,}5\ 10^{-4} - 3{,}02 \cdot 10^{-4} = 3.48\ 10^{-4}$	23	21
772 (772,770)	$13 \cdot 10^{-4} - 6{,}5\ 10^{-4}$	42	44
774 (774,772)	0,00244–0,0013 = 0,0011	72	67
776 (776,774)	0,00431– 0,00244 = 0,00189	124	143
778 (778,776)	0,0072 – 0,0043 = 0,0254	190	149
…	…	…	
796 (796,794)	0,1334 – 0,108 = 0,01	1664	1696
…	…	…	
800 (800,798)	0,1918 – 0,1614 = 0,03	1991	2033
…	…	…	
808 (808,806)	**0,3298 – 0,2937 = 0,036**	**2367**	**2382**
810 (810,808)	0,368 – 0,3298 = 0,0382	2503	2476
812 (812,810)	0,4028 – 0,368 = 0,0348	2280	2354
814 (814,812)	0,4390 – 0,4028 = 0,0362	2374	2399
816 (816,814)	0,4746 – 0,4390 = 0,0356	2333	2467
818 (818,816)	0,5093– 0,4746 = 0,0346	2273	2359
820 (820,818)	0,5428 – 0,5093= 0,3358	2200	2320
822 (822,820)	0,5752 – 0,5428 = 0,0324	2123	2243
…	…	…	
840 (840,838)	0,7977 – 0,7791 = 0,0186	1219	1259
…	…	…	
880 (880,878)	0,96954 – 0,9664 = 0,0031	205	186
…	…	…	
900 (900,898)	0,9886 – 0,98744 = 0,0011	76	57
…	…	…	
948 (948,946)	0,9989 – 0,99884 = 0,0001	7	4
950 (950,948)	$0{,}9990 - 0{,}9989 = 1{,}4 \cdot 10^{-4}$	9	6
…	…	…	
978 (978,976)	$0{,}99976 - 0{,}99973 = 2 \cdot 10^{-5}$	1	1
…	…	…	…
1008 (1008,1006)	$0{,}999946 - 0{,}999941 = 5 \cdot 10^{-6}$	0,327	1

Так що практично для оцінки показників доказової стійкості цих шифрів можна користуватися результатами оцінок максимальних диференціальних ймовірностей і максимальних лінійних ймовірностей, обчислених для довільно взятого (одного) ключа шифрування.

2.4 Розподіл максимумів диференціалів і зміщень для 128-бітних шифрів

Зараз ми застосуємо методику визначення інтегральних законів розподілу максимумів для 128-бітного шифру. Відповідно до формул з Додатку Б будуємо інтегральний закон розподілу диференціальних переходів.

Для 128-ми бітного шифру це буде такий результат: $e^{-e^{\frac{98-2X}{0,436}}}$.

Приклади розрахунків за цією формулою ілюструє табл. 2.7.

Таблиця 2.7

Визначення найбільш ймовірних значень максимумів

$2i$	$e^{-e^{\frac{98-2X}{0,436}}}$
96	2,035828665659390555880640669272 8e-44
98	0,367879441171442321595523770161 46
100	0,990024312861776321390710003798 91
102	0,999999000861533295139221936592 55
104	0,999899919319259798068726688340 32
106	0,999999990025760160015160338175 33
108	0,999999999900428804426781088460 06
126	0,999999999999999999999999999901 96

З представлених результатів випливає, що і в цьому випадку будуть найбільш вираженими (найбільш ймовірними) два значення максимумів: 98 і 100. Решта значень максимумів будуть істотно менш імовірними.

При оцінці стійкості шифру до атак диференціального криптоаналізу можна орієнтуватися на значення максимуму, отримане для одного випадково взятого ключа шифрування, що призводить до результуючої диференціальної ймовірності $.\approx 2^{-121}$.

Для інтегрального закону максимумів зміщень таблиць лінійних апроксимацій 128-бітного шифру відповідно до (3.20, див. третій розділ і додаток В) маємо:

$$\sigma = 2^{(n-4)/2} = 2^{62},$$

$$a = 19 \cdot 2^{62} = 2^{4,25} \cdot 2^{62} = 2^{66} = 87747997204358712186.$$

Ми отримали значення a близьке до розрахункового для випадкової підстановки степеня 2^{128} [15]. І далі відповідно до додатку В

$$b = \sigma b_s = 2^{62} \cdot 0,0526 = 2^{57}.$$

В результаті приходимо до висновку, що максимуми зміщень будуть концентруватися навколо значення 2^{66}, і для максимальної лінійної ймовірності приходимо до результату

$$\left(\frac{2^{66}}{2^{128-1}} \right)^2 = 2^{-122},$$

що добре узгоджується з раніше отриманими автором результатами.

Таким чином, ми змогли розрахунковим шляхом отримати показники доказової стійкості і для повномасштабного шифру.

Отже, вперше розраховані закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій сучасних шифрів.

Висновки до розділу 2

Результатами досліджень підтверджена справедливість і обґрунтованість нової методології оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, що будується на основі використання теоретичних значень максимумів законів

розподілу переходів XOR таблиць (повних диференціалів) і змішень таблиць ЛАТ (лінійних корпусів) шифруючих перетворень, що розглядаються як випадкові підстановки. Цей підхід, на відміну від наявних підходів, дозволяє отримати точні значення показників стійкості шифрів. Зокрема, продемонстрована можливість обчислення показників стійкості (максимальних значень диференціальної та лінійної ймовірностей) для 128-ми бітних шифрів.

В результаті проведених теоретичних і експериментальних досліджень вперше встановлені закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць й зміщень таблиць лінійних апроксимацій шифрів, як випадкових підстановок. Відповідно до отриманих результатів можна зробити висновок, що всі сучасні шифри мають досить малий діапазон зміни максимумів повних диференціалів та максимумів зміщень лінійних корпусів. Так що практично для оцінки показників доказової стійкості цих шифрів можна користуватись результатами оцінок максимальних диференціальних ймовірностей та максимальних лінійних ймовірностей, обчислених для довільно взятого (одного) ключа шифрування.

Експериментами підтверджено, що криптографічні перетворення, властиві SPN конструкціям шифрів (шифрів з квадратними S-блоками), є збалансованими в тому сенсі, що якість перетворень практично не залежить від ключів шифрування. Обґрунтування цього результату можна вважати новим.

Для шифру, як и для випадкової підстановки значення максимумів диференціалів й максимумів лінійних корпусів не є непрогнозованими значеннями. Вони підпорядковуються інтегральному закону розподілу (2.5) екстремальних значень множини незалежних випадкових змінних, що мають один и той же розподіл.

В цілому в розділі викладені авторські розробки по розрахунку законів розподілу максимумів (екстремальних розподілів) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій сучасних шифрів, тобто вперше

реалізовані обчислювальні методи визначення максимумів диференціальних та лінійних ймовірностей, що визначають показники стійкості шифрів до атак диференціального та лінійного криптоаналізу.

Матеріали, опубліковані з участю автора і самостійно по цьому розділу в роботах [15; 20; 24].

РОЗДІЛ 3

РОЗРОБКА УДОСКОНАЛЕНОЇ МАТЕМАТИЧНОЇ МОДЕЛІ ВИПАДКОВОЇ ПІДСТАНОВКИ

У цьому розділі узагальнюються результати, присвячені формуванню моделі випадкової підстановки, яка має важливе значення для обґрунтування нової методології оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, подальшому розвитку і обґрунтуванню якої присвячена дана робота.

Одним з центральних положень нової методології оцінки стійкості блокових симетричних шифрів є твердження про те, що всі шифри асимптотично зі збільшенням числа циклів шифрування стають випадковими підстановками.

Інше її положення полягає в тому, що показники стійкості БСШ не залежать від використовуваних S-блоків. S-блоки впливають лише на показники приходу шифрів до стану випадкової підстановки.

Ці положення були детально обґрунтовані в роботах [1; 6; 80; 81; 82; 83; 84; 85; 86; 95 та ін.]. У формуванні цих положень брав участь, і автор цієї роботи [8; 9; 10; 11; 12; 13; 23 та ін.].

Зробимо короткі підсумки результатів досліджень, виконаних в роботах [1; 2; 3; 4; 5; 8; 9; 14; 23 та ін.], пов’язаних з підстановлювальними конструкціями (S-блоками). Буде представлений також зміст двох публікацій, підготовлених з участю автора цієї роботи [8; 23], які є важливими у формуванні моделі випадкової підстановки.

3.1 Стислий огляд попередніх результатів

Слід зазначити, що формування нової методології розпочалось близько 10-ти років тому назад. І для автора цієї роботи участь в цих дослідженнях почалась саме з вивчення властивостей випадкових підстановок. Далі підстановки стали основним об’єктом досліджень в дисертаціях, підготованих

Широковим А. В. і Мельничуком Є. Д. [3; 4]. В отриманні ряду важливих результатів здобутих в цьому напрямку прийняв участь і автор цієї роботи [7; 13; 14; 16; 23; 28] та інші.

Спочатку нагадаємо про закони розподілу інверсій, зростань і циклів випадкових підстановок степеня 2^n, $n \geq 4$ і зменшених до 16 - бітних входів моделей сучасних шифрів (робота з участю автора [28]). Було встановлено, що вони розподілені відповідно з теорією випадкових підстановок за нормальними законами розподілу ймовірностей з назалежними числовими характеристиками, що визначаються степенями підстановок [100].

На основі цього було введено поняття випадкової підстановки, яке пов’язувалося з перевіркою відповідності комбінаторних показників підстановок (числа інверсій, зростань і циклів) з числовими характеристиками асимптотичних законів розподілу. Роботи за участю автора [3; 16 та ін.].

Далі були встановлені закони розподілу диференціальних і лінійних показників підстановлювальних перетворень. Роботи за участю автора [8; 23], а також [1; 6].

Потім була обґрунтована і вивчена модель випадкової підстановки у вигляді набору критеріїв близькості комбінаторних показників, а також законів розподілу переходів диференціальних таблиць і зміщень таблиць лінійних апроксимацій підстановок до еталонних. Як еталонні закони розглядалися відповідні закони розподілу максимумів випадкових підстановок, отримані теоретичним шляхом. Роботи автора [8; 23].

Велику увагу було приділено використанню алгебраїчних методів опису підстановлювальних перетворень за допомогою відомого математичного апарату булевих функцій [3; 4 та ін.].

У підсумку в роботах [1; 4; 6], а також в авторських розробках [7; 14] було зроблено висновок, що хоча і в сучасній літературі приділяється дуже велика увага розвитку і застосуванню для оцінки криптографічних показників S-блоків алгебраїчних методів на основі математичного апарату булевих

функцій, тим не менш, цей алгебраїчний підхід для багатьох відомих конструкцій S-блоків не став визначальним. Більш того, S-блокові конструкції, що застосовуються в сучасних шифрах, володіють далеко не кращими, а по ряду показників і досить низькими криптографічними властивостями булевих функцій, що входять до них. Реальні конструкції S-блоків будуються, скоріше, спираючись на показники, які можуть бути визначені (обчислені) без залучення апарату булевих функцій (хоча і є прямий зв'язок деяких з цих показників з властивостями булевих функцій S-блоків).

Виявилося, що застосування підстановок, відібраних з використанням розроблених критеріїв випадковості не привело до яких-небудь помітних переваг.

Можна тут нагадати і останні розробки по побудуванню S-блоків сучасних шифрів. Так, в шифрі Калина пішли по шляху використання випадкових S-блоків з подальшим жорстким відбором підстановок за показником нелінійності [104]. Експерименти свідчать, що ймовірність знайти підстановку з таким показником нелінійності дорівнює 0,0000007 [123]. В цій роботі вказується, що для породження оптимального S-блоку необхідно в середньому перебрати 1100000 підстановок. По аналогічному шляху пішли і при виборі S-блоків в шифрі «Кузнечик» та білоруському шифрі.

У цій роботі розглядається позиція, що більш плідним слід вважати підхід, орієнтований на побудову циклових перетворень шифрів, інваріантних до показників випадковості підстановок, коли як підстановлювальні перетворення використовуються практично підстановки породжені генератором без будь-яких обмежень.

Основним результатом виконаних досліджень в цьому напрямку можна вважати уточнене визначення (уточнену модель) випадкової підстановки, що будується на властивостях вибірки з випадкових підстановок. Як виявилося, для випадкових підстановок максимуми диференціальних таблиць і максимуми зміщень таблиць лінійних апроксимацій приймають істотно обмежене число можливих значень, які концентруються навколо теоретичних

значень максимумів диференціальних і лінійних таблиць випадкових підстановок відповідних степенів [15].

Отже, виявилося, що головну роль в формуванні математичної моделі випадкової підстановки грають властивості законів розподілу максимумів XOR таблиць і таблиць лінійних апроксимацій,

Далі буде представлений зміст двох важливих публікацій [8; 23], підготованих у співучасті й самостійно автором цієї роботи, що відносяться до цього напрямку.

А починалося все з наукової роботи, яка була присвячена дослідженню диференціальних властивостей підстановок різних циклових класів (пізніше була зроблена публікація [80]). Результати перших проведених автором експериментів з аналізу властивостей випадкових підставок визначили його прилучення до наукового напряму, що розглядається.

Вже тоді в ході експериментів були отримані перші наукові результати. Вдалося встановити, що диференціальні властивості підстановок не залежать від циклових класів, до яких вони належать. Підстановки мають практично одні й ті ж значення максимумів диференціальних переходів, близькі до середніх значень максимумів XOR таблиць, що залежать від степенів підстановок. Пізніше ці результати були опубліковані в роботах з участю автора.

В роботі [8] вдалося побудувати свій варіант доведення теореми, знайденої в роботі вченого Люка О'Конор-а [102], яка дала змогу отримати розрахункове співвідношення для визначення максимумів таблиць XOR різниць випадкових підстановок різного степеня. Хоча в цій роботі вказано кілька співавторів, але основну роботу з підбору матеріалу і формуванню окремих етапів доведення виконав сам автор цієї роботи під керівництвом проф. Долгова В. І.

Не менш важливий результат був отриманий в роботі [101], опублікованій Долговим В. І. Лисицькою І. В. і Олешко О. І. Він присвячений доведенню закону розподілу зміщень випадкової підстановки, в якій

запропоновано новий варіант доведення теореми, теж свого часу сформульованій Люка О'Конор-ом [102; 103; 104]. Виявилося, що доведення теореми в цій роботі виконано не зовсім коректно і нова (вдосконалена) її редакція розроблена автором цієї дисертації в роботі [23], що вийшла вже в процесі підготовки матеріалів дисертації.

Інтерес до цих теорем пов'язаний з тим, що на них будується методика визначення показників стійкості БСШ відповідно до розвинутої нової методології. Результати цих трьох робіт були використані для отримання розрахункових співвідношень для визначення показників стійкості шифрів, які претендують на об'єктивність і точність.

Оскільки результати цих робіт стали важливими для обґрунтування нової методології оцінки показників доказової стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, яка народилася на кафедрі безпеки інформаційних технологій Харківського національного університету радіоелектроніки (БІТ ХНУРЕ), тут наведений уточнений зміст цих робіт практично в повному обсязі. Хоча, як зазначено вище, вони були вже опубліковані в старому варіанті доведень в дисертаціях Лісицької І. В. і Олешко О. І. [1; 2]. Автор вважає, що з урахуванням публікації [23] і він причетний до отримання цих важливих результатів.

Будуть представлені також останні результати по дослідженню законів розподілу максимумів випадкових підстановок [16].

3.2 Закон розподілу переходів диференціальних таблиць випадкових підстановок

Публікація [8] з участю автора не поміщена в список робіт, що відображають основний матеріал дисертації. Доведення закону розподілу переходів диференціальних таблиць випадкових підстановок вже висвітлювалося в дисертаціях Лисицької І. В. і Олешко О. І. [1; 2]. Але цей результат представляється важливим в обґрунтуванні нової методології оцінки

стійкості блокових шифрів до атак диференціального та лінійного криптоаналізу і є стрижнем цієї роботи.

Інше діло, що в роботі [8] були допущені помилки в записі використаних позначень.

Тут збережений матеріал оригінального викладення цієї роботи (з виправленнями), тому що головну участь в отриманні її результатів прийняв автор цієї дисертації.

Далі йде безпосередньо викладення роботи [8] з деякими правками.

Отже, відповідно до роботи [102], покладемо, що $\pi : Z_2^m \to Z_2^m$ є бієктивним m-бітним зображенням, і нехай $S_{2^m} = S_2^m$ буде множиною всіх таких відображень, відомим в математичній літературі як симетрическая група. Нехай $\Lambda_\pi(\Delta X, \Delta Y)$ буде значенням XOR таблиці (її осередку) для пари значень різниць входів і виходів $\Delta X, \Delta Y \in Z_2^m$, $\Delta X = X \oplus X'$,
$\Delta Y = \pi(x) \oplus \pi(X')$ підстановки $\pi \in S_2^m$.

Нагадаємо, що XOR таблиця являє собою матрицю $2^m \times 2^m$, у якій $\mathrm{XOR}_\pi(i,j) = \Lambda_\pi(i,j)$, $0 \le i,j \le 2^m - 1$. Для m-бітної підстановки π XOR таблиця має таку загальну форму

$$\mathrm{XOR}_\pi = \begin{vmatrix} 2^m & 0 & 0 & \mathrm{L} & 0 \\ 0 & a_{1,1} & a_{1,2} & \mathrm{L} & a_{1,2^m-1} \\ 0 & a_{2,1} & a_{2,2} & \mathrm{L} & a_{2,2^m-1} \\ \mathrm{L} & \mathrm{L} & \mathrm{L} & \mathrm{L} & \mathrm{L} \\ 0 & a_{2^m-1,1} & a_{2^m-1,2} & \mathrm{L} & a_{2^m-1,2^m-1} \end{vmatrix} \overset{def}{=} \begin{vmatrix} 2^m & 0 \\ 0 & A_{ij} \end{vmatrix}.$$

Ми будемо цікавитися властивостями $(2^m - 1) \times (2^m - 1)$ підматриці $A_\pi = \left|a_{i,j}\right|$, $1 \le i,j \le 2^m - 1$, яка відповідає частці XOR таблиці з входами (осередками), що приписуються до ненульових характеристик.

Розглянемо задачу визначення ймовірності події, що полягає в тому, що значення диференціальної таблиці випадково взятої підстановки π степеня 2^m для переходу вхідної різниці ΔX в відповідну вихідну різницю

ΔY дорівнюватиме $2k$ (значення осередків XOR таблиці завжди парні). Як і в [102] цю ймовірність позначимо $Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k)$.

В [102] наводиться теорема, яка визначає цю ймовірність у вигляді:

Твердження *Для будь-яких ненульових фіксованих* $\Delta X, \Delta Y \in Z_2^m$ *в припущенні, що підстановка* π *обрана рівноймовірно з множини* S_2^m *і* $1 \le k \le 2^m - 1$,

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \binom{2^{m-1}}{k}^2 \cdot \frac{k! \cdot 2^k \cdot \Phi(2^{m-1} - k)}{2^m!}, \tag{3.1}$$

де функція $\Phi(d)$ *визначається виразом*

$$\Phi(d) = \sum_{i=0}^{d} (-1)^i \cdot \binom{d}{i}^2 \cdot 2^i \cdot i! \cdot (2d - 2i)!. \tag{3.2}$$

Варіант доведення виходить дуже простим.

Д о в е д е н н я. Будемо цікавитися властивостями $(2^m - 1) \times (2^m - 1)$ підматриці $A_\pi = \left|a_{i,j}\right|$, $1 \le i, j \le 2^m - 1$, яка відповідає частці XOR таблиці з входами (осередками), що приписуються до ненульових характеристик.

Зауважимо спочатку, що при операції обчислювання різниць XOR входів підстановки π вони утворюють дві пари з однаковими переходами. Тому в диференціальній таблиці число переходів вхідних різниць в вихідні різниці (значення осередку таблиці диференціальних різниць) завжди парне, і до того ж входи (і відповідні виходи) підстановки розподіляються по парам, так що для однієї й тієї ж ненульової різниці ми маємо справу з 2^{m-1} парами входів.

Одночасно стає зрозумілим, що для заданого поєднання входів і виходів підстановки π кожне конкретне значення вхідної різниці може переходити не в усі можливі значення вихідних різниць, і що різні пари входів з однією і тією ж різницею можуть переходити в одну і ту ж вихідну різницю. Для підстановок, які обираються рівноймовірно з множини $\pi \in S_2^m$, під шуканою ймовірністю, очевидно, слід розуміти відношення числа підстановок, що

володіють бажаною властивістю (реалізують необхідне число $2k$ разів заданий перехід $\Delta X \to \Delta Y$), до загальної кількості підстановок симетрическької групи S_2^m, тобто:

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \frac{\#\left\{\Lambda_\pi(\Delta X, \Delta Y) = 2k\right\}}{2^m!}. \qquad (3.3)$$

Далі в роботі [8] виконано обчислення числа підстановок $\#\{\Lambda_\pi(\Delta X, \Delta Y) = 2k\}$ з обумовленою кількістю переходів $2k$ вхідної різниці ΔX в вихідну різницю ΔY.

Отже, виконаємо обчислення числа підстановок $\#\{\Lambda_\pi(\Delta X, \Delta Y) = 2k\}$ з обумовленою кількістю переходів вхідних різниць ΔX в вихідну різницю ΔY. Очевидно, що в це число входитимуть підстановки, що відрізняються конфігураціями (поєднаннями) входів і виходів, які беруть участь в реалізації бажаної властивості (що реалізують необхідну кількість $2k$ раз заданий перехід $\Delta X \to \Delta Y$).

Зауважимо, що різні підстановки з $2k$ переходами будуються з використанням k різних пар переходів $\Delta X \to \Delta Y$. Отже, будемо цікавитися наявністю в підстановках наборів з k різних пар переходів, що задовольняють умові $\Delta X \to \Delta Y$.

Оскільки k пар різних переходів будь-якої підстановки, що беруть участь в реалізації необхідної властивості $\Delta X \to \Delta Y$ $(\Lambda_\pi(\Delta X. \Delta Y) = 2k)$, і $2^{m-1} - k$ пар, що залишилися із загального числа 2^{m-1} пар переходів з властивістю $\Delta X \not\to \Delta Y$ (позначення з роботи Елі Біхама і Аді Шаміра [105]) компонуються в довільному поєднанні (переходи кожної з цих двох груп входів і виходів підстановки формуються незалежно одна від іншої), то число, що нас цікавить, включає дві компоненти (два співмножники):

- перший співмножник визначається числом різних підстановок π, у яких k пар входів з наявного в підстановці числа таких пар 2^{m-1} реалізують заданий перехід $\Delta X \to \Delta Y$ незалежно від залишившихся $2^{m-1} - k$ пар, що не реалізують заданого переходу;

- другий співмножник визначається додатковим розширенням множини підстановок, у яких k пар входів реалізують заданий перехід $\Delta X \to \Delta Y$, за рахунок різноманіття варіантів вибору $2^{m-1} - k$ залишившихся пар входів кожної з підстановок, які заданого переходу не реалізують, тобто для яких $\Delta X \not\to \Delta Y$.

Тепер розраховуємо число варіантів підстановок, що визначають перший співмножник.

Почнемо з того, що відповідно до комбінаторних міркувань для фіксованого набору з k пар входів, що мають різницю $\Delta X \neq 0$ (розглядаються входи в матрицю $A_\pi = |a_{i,j}|$), які мають задану вихідну різницю ΔY, можливо $k!$ варіантів різних перестановок k пар виходів по заданому набору входів (підстановки нормалізованого виду відрізняються розміщенням пар вихідних значень по парам вхідних).

Для першої пари вхідних різниць можна обрати одну з k вихідних різниць k способами. Для другої пари залишається $k - 1$ варіантів вихідних пар і т.д.

Черговою можливістю розширення множини підстановок, котрі мають задане число k переходів вхідної різниці ΔX в вихідну різницю, є варіювання наборами входів і виходів підстановки, які беруть участь у формуванні переходів вхідної різниці ΔX в вихідну різницю ΔY. Із загальної кількості 2^{m-1} пар входів, що мають різницю ΔX, в формуванні переходів, що цікавлять нас, бере участь тільки k пар входів.

Очевидно, що вони можуть бути обрані із загального числа 2^{m-1} пар входів $C_{2^{m-1}}^{k}$ способами.

Аналогічне становище характерно і для множини пар виходів, що мають різницю ΔY. Оскільки компоновка вхідних і вихідних пар здійснюється незалежно, то приходимо до загальної кількості $\left(C_{2^{m-1}}^{k}\right)^2$ варіантів підстановок з властивістю, що нас цікавить.

Нарешті, є ще одна ступінь свободи в побудові підстановок з заданим числом переходів вхідної різниці ΔX в вихідну різницю ΔY. Одна і та ж пара входів з різницею ΔX може реалізувати два варіанти переходів в вихідну різницю ΔY (виходи підстановки, тобто елементи підстановки що входять в пару, можна поміняти місцями). Але тоді множина можливих підстановок з фіксованим переходом вхідної різниці ΔX в вихідну різницю ΔY додатково збільшиться ще в 2^k разів, при цьому число переходів підстановки з різницею ΔX що переходять в пари виходів з різницею ΔY збільшується в два рази, тобто підстановка буде мати $2k$ переходів потрібного типу.

В результаті ми дійсно для ймовірності того, що значення диференціальної таблиці випадково взятої підстановки π степеня 2^mз переходом вхідної різниці ΔX в відповідну вихідну різницю ΔY буде дорівнювати числу $2k$, приходимо до співвідношення (3.1), в якому роль другого співмножника, про який йшла мова вище, грає функція $\Phi(2^{m-1} - k)$.

Залишається врахувати варіанти розширення множини підстановок виду, що нас цікавлять, внаслідок другого співмножника. В роботі [102], щоб визначити другий співмножник виводиться розрахункове співвідношення для функції $\Phi(d)$ у вигляді (3.2).

Для отримання цього розрахункового співвідношення в роботі [102] використана «Спаривающая теорема», коротке доведення якої без пояснень, наводить автор. Тут пропонується свій варіант виводу розрахункового співвідношення для функції $\Phi(d)$, що є по суті наслідком доведеного вище співвідношення (3.1).

Дійсно, будемо тепер цікавитися «хвостом» з $2^{m-1} - k$ пар входів і виходів, які в попередньому розгляді вважалися фіксованими. За обумовленим це пари, які не мають визначеного переходу $\Delta X \to \Delta Y$.

Множину цих пар можна розглядати як окрему підстановку степеня $2^{m-1} - k$ тоді для визначення числа підстановок степен $2^{m-1} - k$ що не мають заданого переходу $\Delta X \to \Delta Y$, очевидно можна просто із загального

числа підстановок такого степеня відняти число підстановок, що мають заданий перехід.

Підстановки степеня $2^{m-1}-k$ з обумовленим переходом можуть містити одну пару з таким переходом, дві пари, і так до $2^{m-1}-k$ пар переходів.

В результаті в термінах функції $\Phi(d)$ вираз для розрахунку другого співмножника в роботі [8] представлений у вигляді

$$\Phi(d)=(2d)!-\sum_{i=1}^{d} i!\cdot 2^{i}\binom{d}{i}^{2}\Phi(d-i). \qquad (3.4)$$

В [8] показано, що уявлення (3.2) і (3.4) еквівалентні.

Далі, як і в [102] позначимо очікуване число ненульових характеристик $\Delta X, \Delta Y$, для яких $\Lambda_\pi(\Delta X,\Delta Y)=2k$ як $\Lambda_{m,2k}$.

При виведені виразу (3.1) не фіксувалося значення пар різниць, $\Delta X,\Delta Y\in Z_2^m$ для яких його було отримано.

Це означає, що співвідношення (3.1), справедливо для довільних поєднань різниць на вході і виході підстановок.

Вираз (3.1) визначає ймовірність того, що в XOR таблиці випадково взятої підстановки число переходів вхідної різниці $\Delta X\in Z_2^m$ в вихідну різницю $\Delta Y\in Z_2^m$ буде дорівнювати $2k$.

Але тоді стає зрозумілим, що вираз для числа $\Lambda_{m,2k}$ переходів таблиці диференціальних різниць підстановки степеня 2^m обумовленого типу, – а саме для середнього значення числа ненульових характеристик $\Delta X\to\Delta Y$, таких, що $\Lambda_\pi(\Delta X,\Delta Y)=2k$може бути отримано шляхом множення виразу (3.1) на число осередків підматриці таблиці XOR_π, що дорівнює $(2^m-1)^2$:

$$\Lambda_{m,2k}=\frac{(2^m-1)^2}{2^m!}\cdot\binom{2^{m-1}}{k}^{2}\cdot k!\cdot 2^{k}\cdot\Phi(2^{m-1}-k). \qquad (3.6)$$

Цей вираз і є той, що нам потрібний.

Нас тепер буде цікавити середнє значення максимуму таблиці XOR різниць. Воно знаходиться зі співвідношення (3.6) просто шляхом визначення максимального значення k, при якому результат розрахунків за цим виразом призводить до найменшого цілого значення (близького до одиниці). Іншими словами, нам потрібно знайти рішення рівняння

$$\frac{(2^m-1)^2}{2^m!}\cdot\binom{2^{m-1}}{k}^2\cdot k!\cdot 2^k\cdot\Phi(2^{m-1}-k)\approx 1. \qquad (3.7)$$

Це рішення можна шукати переборним методом, орієнтуючись при цьому на експериментальні дані. Корисною апроксимацією для виконання розрахунків може стати й ще один результат, також наведений в роботі [102].

Мається на увазі зауваження про те, що в знакозмінній сумі в виразі (3.2) перший терм (при $i = 0$) є переважним, і що

$$\Phi(d) \approx (2d)!/e^{\frac{1}{2}}. \qquad (3.8)$$

Залишається помітити, що $e^{-\frac{1}{2}} = 0,6065$.

Розрахунки, виконані відповідно до співвідношень (3.1), (3.2) і (3.7), представлені в таблиці 3.1.

Тут далі також наводяться результати з роботи, яка нагадана в сносці нижче[6], що підготовлена ще у 2009 році. Їх ілюструє табл. 3.2.

Зіставлення результатів таблиць 3.1 і 3.2 свідчить про добре узгодження експериментальних даних з результатами, що прямують з теоретичних розрахунків.

Цікаво відзначити, що для закону розподілу (3.1), що розглядається над підматрицею $A_\pi = |a_{i,j}|$, виконується співвідношення

$$\sum_{k=0}^{k^*}(2^m-1)^2\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)\approx(2^m-1)^2.$$

[6]. Олейников Р.В, Лисицкий К.Е. Исследование дифференциальных свойств подстановок различных цикловых классов Двенадцатая Международная научно-практическая конференция *"Безопасность информации в информационно-телекоммуникационных системах"*, 19-22 МАЯ 2009 г., Тезисы докладов. К.: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ". 2009. С. 24-25.

Таблиця 3.1

Порівняння обчислень за формулою 3.6. і експериментальних результатів

M	$\Lambda_\pi(\Delta X, \Delta Y) = 2k$	$2k$	Експеримент
4	3,379 0,459	6 8	6,7 $\leq (m + 3)$
5	3,08 1,708	6 8	7,94 $\leq (m + 3)$
6	6,6 0,675	8 10	9,1 $\leq (m + 4)$
7	2,641 0,221	10 12	10,3 $\leq (m + 4)$
8	0,8748	12	11,4
9	3,474 0,248	12 14	12,5 $\leq (m + 4)$
10	13,8495 0,99	12 14	13,4 $\leq (m + 4)$
11	3,952 0,247	14 16	14,5 $\leq (m + 4)$
12	15,787 0,987	14 16	15,3 $\leq (m + 4)$
14	15,76 0,87	16 18	17,6 $\leq (m+ 4)$
16	14,01 0,7	18 20	19,5 $\leq (m + 4)$
24	8,155 0,239	32 34	Не розраховувалось

Це означає, що для виразу (3.1) з великою точністю виконується умова нормування (повної групи подій):

$$\sum_{k=0}^{k^*} \Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k) \approx 1. \qquad (3.9)$$

Тут k^* являє собою половину від максимального значення числа переходів XOR таблиці випадкової підстановки.

Цим підтверджується висловлена на початку підрозділу установка, що властивості окремої випадкової підстановки однозначно виражаються через

властивості ансамблю випадкових підстановок. Результати обчислювальних експериментів надані в табл. 3.2.

Таблиця 3.2

Результати обчислювальних експериментів

Степень подст. / число циклов подст.	$2^3 = 8$	$2^4 = 16$	$2^5 = 32$	$2^6 = 64$	$2^7 = 128$	$2^8 = 256$	$2^9 = 512$	$2^{10} = 1024$	$2^{11} = 2048$	$2^{12} = 4096$
1	4.8014	6.69454	7.94398	9.11202	10.2827	11.4222	12.0	13.75	15.3333	14.0
2	4.2591	6.71003	**7.94526**	9.11991	10.2921	11.3765	12.3467	13.6429	14.1538	15.0
3	4.7807	6.68965	7.94006	9.11311	10.3022	11.4241	12.3697	13.2647	14.3947	15.68
4	4.2616	6.71753	7.94177	9.10912	10.3097	11.3012	12.5144	13.4481	14.5745	15.3235
5	4.9487	6.6881	7.94223	9.10677	10.3043	11.3252	12.4528	13.4565	14.3969	15.4066
6	4.5187	6.71281	7.95425	9.11403	10.3178	11.3645	12.4948	13.3743	14.529	15.3509
7	8.0	6.72067	7.94278	9.11009	10.3157	11.3144	12.4095	13.4121	14.3967	15.37
8	8.0	6.84496	7.94878	9.11502	10.3248	11.3216	12.4316	13.4607	14.5284	15.4055
9		7.0137	7.95743	9.11899	10.3165	11.2887	12.4122	13.3596	14.5089	15.4027
10		6.91892	7.98563	9.1015	10.3071	11.3538	12.5669	13.4009	14.4336	15.4268
11		8.0	8.03191	9.15496	10.3183	11.359	12.4249	13.3284	14.4715	15.368
12			7.6	9.0	10.2954	11.3429	12.3457	13.2179	14.4822	15.3313
13			8.0	9.42222	10.2264	11.0667	12.7109	13.55	14.4785	15.2735
14				9.0	10.5882	11.0	12.7619	13.125	14.3939	15.625
15				10.0	9.33333	11.0	12.0	13.4667	14.1935	15.4333
16					10.0	12.0	12.0	13.5	14.4	15.5333
17					10.0			13.0	14.0	15.7143
18								14.0	14.05.09	15.6
19									-	16.5
Число подстановок	1000000	1000000	1000000	500000	100000	10000	5000	5000	5000	5000

Як виявилося, обчислення за формулою (3.7) вдається виконати тільки для значень степенів підстановок, що не перевищують $m = 24$. При великих значеннях m розрахунки виходять за сітку ЕОМ.

На щастя в роботі [1] була встановлена дуже важлива властивість розподілу (3.1), яка тут наводиться у вигляді твердження.

Твердження. Для відношення диференціальних ймовірностей сусідніх значень комірок таблиці XOR різниць випадкової підстановки для $k = 1,\ldots,k^*$ справедливо співвідношення:

$$\frac{\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2(k-1)\right)}{\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)}\approx 2k \qquad (3.10)$$

або $\#\left\{\Lambda_\pi(\Delta X,\Delta Y)=2(k-1)\right\}=2k\cdot\#\left\{\Lambda_\pi(\Delta X,\Delta Y)=2k\right\}$.

Це співвідношення дозволяє дуже просто реконструювати закон розподілу ймовірностей (3.1) по максимальному значенню повного диференціалу випадкової підстановки або за кількістю нульових осередків диференціальної таблиці підстановки. Зокрема, якщо згадати роботу [102], де встановлено, що для числа нульових осередків диференціальної таблиці випадкової підстановки справедливо співвідношення (3.8), що виконується з великою точністю, а саме при значенні $d = 2^{m-1}$:

$$\Phi(2^m) = 2^m! \cdot 0{,}6065\ldots,$$

то можна прийти до висновку, що для закону розподілу ймовірностей значень переходів таблиці XOR різниць випадкової підстановки справедлива апроксимація, яка являє собою відомий з теорії ймовірностей пуасонівський закон розподілу:

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=e^{-1/2}\cdot\frac{1}{2^k\cdot k!}. \qquad (3.11)$$

В результаті для числа елементів таблиці XOR різниць випадкової підстановки степеня 2^m, що мають заповнення $2k$, в [1; 97], отримано розрахункове співвідношення:

$$\Lambda_{m,2k}=(2^m-1)^2\cdot\frac{e^{-1/2}}{2^k k!}.$$

Розрахунки, виконані по цьому співвідношенню ілюструє табл. 3.3. Ці результати знадобляться надалі.

Як видно, значення максимуму дорівнює $2k$*.

Далі подаються результати досліджень, виконаних в ще одній роботі за участю автора [23], де наводиться уточнена версія доведення теореми, що визначає закон розподілу ймовірностей зміщень таблиць лінійних

апроксимацій випадкових підстановок. Вона наведена з невеликими скороченнями.

Таблиця 3.3

Очікувані значення максимумів таблиць диференціальних різниць випадкових підстановок

m	k*	$\Lambda_{n,2k} = (2^m - 1)^2 \cdot \frac{e^{-1/2}}{2^k k!}$
16	10 11	1,15 0,026
32	18 20	8,35 2,336
64	30 32	0,0012 $3{,}01\times10^{-7}$
128	50 52	0,003 $3{,}18\times10^{-7}$
256	86 88	0,007 $2{,}3\times10^{-7}$

3.3 Закон розподілу ймовірностей зміщень таблиць лінійних апроксимацій випадкових підставок

В [23] спочатку нагадуються позначення, використані в роботах [103; 104].

Нехай $\pi : Z_2^n \to Z_2^n$ – бієктивне n-бітове відображення і нехай S_2^n буде множиною всіх таких відображень. Для n-бітного вектору $X \in Z_2^n$ нехай $X[i]$ позначає i-тий біт вектору X. Лінійна апроксимаційна таблиця для підстановки π позначається як LAT_π є таблицею розміру $2^n \times 2^n$ з елементами $LAT_\pi(\alpha, \beta)$ які визначаються співвідношенням

$$LAT_\pi(\alpha,\beta) \overset{def}{=} \overset{def}{=} \#\left\{ X \,/\, X \in Z_2^n,\ \bigoplus_{i=1}^{n} X[i]\cdot\alpha[i] = \bigoplus_{i=1}^{n} \pi\big(X[i]\big)\cdot\beta[i] \right\}, \tag{3.12}$$

де $\alpha, \beta \in Z_2^n$. Суми в лівій та правій частині рівностей представляють собою скалярні добутки векторів входу і виходу на маскові вектори α та β.

Відповідно до наведеного визначення $LAT_\pi(\alpha, \beta)$ представляє собою число рівностей парності між лінійною комбінацією вхідних бітів (визначаються маскою α по входу в таблицю підстановки за рядками) і лінійною комбінацією вихідних бітів (визначаються маскою β по входу в таблицю підстановки за стовпцями).

Теорема, про яку йде мова, сформульована в [1; 104] наступним чином.

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

$$\Pr(\lambda(\alpha, \beta) = 2k) = \frac{(2^{n-1}!)^2}{2^n!} \cdot \binom{2^{n-1}}{k}^2. \qquad (3.13)$$

Далі викладається новий (уточнений) варіант її доведення.

В новому варіанті введені ще три додатних твердження, яких, як виявилося, не вистачає для виконання коректного доведення цієї теореми.

Д о в е д е н н я. Поцікавимося числом підстановок з загального їх числа $2^n!$, осередки таблиць $LAT_\pi(\alpha, \beta)$ яких для заданого значення входу в таблиці по рядках α і заданого значення входу в таблиці по стовпцях β (заданого поєднання пари входів в таблицю) мають заповненням (значенням) число $2k$.

За визначенням, якщо підстановка π має значення комірки таблиці $LAT_\pi(\alpha, \beta)$ рівне $LAT_\pi(\alpha, \beta) = 2k$, то це означає, що число входів в підстановку X із загального їх числ 2^n які пройшли при побудові таблиці маску α з ознаками парне і непарне (мають результатом скалярного добутку $\alpha \cdot X$ нуль або одиницю), збігається з числом відповідних виходів підстановки $\pi(X)$, які пройшли маску β з ознаками парне і непарне (мають результатом скалярного добутку $\beta \cdot \pi(X)$ нуль або одиницю), дорівнює $2k$, тобто число

входів і виходів, що задовольняють рівності парності $\alpha \cdot X = \beta \cdot \pi(X)$, дорівнює $2k$.

Отже, нас цікавить подія, що пов'язана зі збігом ознак парне чи непарне для вхідних текстів підстановки і її вихідних текстів, які пройшли відповідні маски. Нам надалі буде потрібно використати кілька додаткових тверджень, перші три з котрих дозволять встановити, що значення комірок лінійної апроксимаційної таблиці є завжди парними числами.

Твердження 1 *Для будь-якого поєднання масок входу α і масок виходу β,* $\alpha, \beta \in Z_2^n$ *рівно половина* (2^{n-1}) *із загального числа скалярних добутків для всієї множини входів в підстановку* (*як і для всієї множини виходів підстановки*) *приймають значення парні* (0), *а решта* 2^{n-1} *скалярних добутків приймають значення непарні* (1).

Перед тим як доводити твердження 1 попередньо доведемо ще одне твердження.

Твердження 2

Сума за модулем 2 *двійкових символів повного набору з* 2^l *l-бітних векторів на всьому наборі цих векторів в половині випадків дорівнює нулю, а в іншій половині випадків дорівнює одиниці.*

Д о в е д е н н я. Число одиниць в векторах повного набору з 2^l двійкових векторів змінюється від 0 до l, причому число векторів без одиниць дорівнює $C_l^0 = 1$, число векторів з однією одиницею дорівнює $C_l^1 = l$, з двома одиницями дорівнює $C_l^2 = \frac{l(l-1)}{2}$, число векторів з k одиницями дорівнює C_l^k, число векторів з lодиницями дорівнюватиме $C_l^l = 1$. Але вектори з непарним числом одиниць при додаванні бітів за модулем 2 (при обчислюванні скалярних добутків) будуть давати результатом одиницю, а вектори з парним числом одиниць при додаванні бітів за модулем 2 даватимуть результатом нуль.

Тоді на повній множині з 2^l векторів число результатів парні (0) і непарні (1) для $l = 2s + 1$ парного) буде визначатися виразом $\sum_{k=0}^{s} C_l^{2k}$ для векторів з парним числом одиниць, або відповідн $\sum_{k=1}^{s} C_l^{2k-1}$ для векторів з непарним числом одиниць, а для $l = 2s + 1$ (непарного) буде відповідно визначатися виразом $\sum_{k=0}^{s} C_l^{2k}$ для векторів з парним числом одиниць і $\sum_{k=0}^{s} C_l^{2k+1}$ для векторів з непарним числом одиниць. Неважко переконатися (безпосередньою перевіркою), що $\sum_{k=0}^{s} C_l^{2k} = \sum_{k=1}^{s} C_l^{2k-1} = 2^{l-1}$ для $l = 2s$ (парного), як і те, що $\sum_{k=0}^{s} C_l^{2k} = \sum_{k=0}^{s} C_l^{2k+1} = 2^{l-1}$ для $l = 2s + 1$ (непарного). Можна, однак, рахувати очевидним, що число векторів з парним числом одиниць з повного набору із 2^l двійкових векторів буде завжди дорівнювати числу векторів з непарним числом одиниць (і для *l* парного і для *l* непарного).

Тим самим доведена справедливість твердження 2.

Повернемося тепер до доведення твердження 1.

Д о в е д е н н я. Будемо інтерпретувати маски входу в підстановку і маски виходу підстановки як *l*-бітові і *m*-бітові одиничні вектори, накладені на *n*-бітові блоки входів і виходів в підстановку. Тоді скалярні добутки $\alpha \cdot X$ для масок, що містять *l* одиниць, (також як і скалярні добутки $\beta \cdot \pi(X)$ для масок, що містять *m* одиниць), накладених на повний набір *n*-бітових блоків входів і виходів) незалежно від розташування одиничних символів масок будуть включати повні набори *з l*-бітних (*m*-бітових) двійкових послідовностей, які повторюються на повному наборі *n*-бітових векторів $2^n / 2^l = 2^{n-l}$ ($2^n / 2^m = 2^{n-m}$ разів).

З огляду на те, що відповідно до твердження 2 сума за модулем 2 двійкових символів для повного набору з 2^l *l*-бітних векторів на всьому наборі

цих векторів в половині випадків дорівнює нулю, а в іншій половині випадків дорівнює 1, маємо для кожного набору з 2^l l-бітних векторів 2^{l-1} нулів і стільки ж одиниць. Приходимо до висновку, що для будь-якої l-бітної маски входу на всієї множині n-бітових векторів $2^{l-1} \times 2^{n-l} = 2^{n-1}$ скалярних добутків будуть давати результатом нуль і стільки ж 2^{n-1} скалярних добутків будуть давати результатом одиницю. Аналогічний результат випливає і для скалярних добутків з m-бітними масками виходу. Тим самим доведено твердження 1.

Таким чином, відповідно до доведеного положення рівно половина 2^{n-1} із загального числа скалярних добутків для всієї множини входів в підстановку (як і для всієї множини виходів з підстановки) приймають значення парне (нуль), а решта 2^{n-1} скалярних добутків приймають значення непарне (одиниця). В результаті різні підстановки при обчисленні $LAT_\pi(\alpha, \beta)$ практично будуть відрізнятися тільки розподілом парних (нульових) і непарних (одиничних) значень множин скалярних добутків $\alpha \cdot X$ і $\beta \cdot \pi(X)$ з одного і того ж набору, що включає 2^{n-1} парних і 2^{n-1} непарних значень цих добутків.

Результуюче число ″проходів″ (виконань рівності) $\alpha \cdot X = \beta \cdot \pi(X)$ для будь-якої пари входів в таблицю α і β буде визначаються числом збігів ознак парне чи непарне в ″списках″ відповідних наборів скалярних добутків для входів і виходів підстановки, причому одне і те ж значення числа ″проходів″ матимуть підстановки, які відрізняються переходами (перестановками), що зберігають парність (непарність) компонент, що формують значення $\lambda(\alpha, \beta)$. Нагадаємо, що параметр $\lambda(\alpha, \beta)$ фіксує число випадків виконання рівності $\alpha \cdot X = \beta \cdot \pi(X)$ для кожної пари α,β.

Буде потрібно ще два твердження.

Відповідно до твердження 1 двійкові послідовності складені з результатів скалярних добутків масок входу α і масок виходу β для всієї множини входів і виходів в підстановку містять однакове число символів кожного типу.

Твердження 3. *Дві послідовності, що складаються з* 2^n *двійкових елементів, які містять однакове число* 2^{n-1} *символів кожного типу, мають тільки парне число співпадінь.*

Д о в е д е н н я. Нехай $\xi = \{0,1\}^{2^n}$ і $\zeta = \{0,1\}^{2^n}$ дві випадково взяті 2^n-бітні послідовності з однаковим числом нулів і одиниць. Доведення будемо вести ″від противного″. Припустимо, що послідовності ξ і ζ мають непарне число збігів. Нехай для конкретності символи, що збігаються, мають парне число нулів і непарне число одиниць. Тоді (незбіжні) символи послідовностей, що залишилися для однієї з них будуть мати непарне число нулів і парне число одиниць, в той час як друга послідовність тоді повинна мати парне число нулів і непарне число одиниць (адже вони протилежні). В результаті виходить, що в одній послідовності має бути парне число нулів і парне число одиниць, в той час як у другій повинно бути непарне число нулів і непарне число одиниць, а це суперечить вихідному припущенню, що обидві послідовності складаються з однакового парного числа нулів і парного числа одиниць. Отже, наше припущення про те, що послідовності ξ і ζ можуть мати непарне число збігів не вірно.

З доведеного випливає справедливість твердження першої частини теореми про те, що параметр $\lambda(\alpha, \beta)$ лінійних апроксимаційних таблиць підстановок приймає тільки парні значення, так як набори ознак парне і непарне в скалярних добутках можна інтерпретувати як відповідні двійкові послідовності.

І ще одне твердження.

Твердження 4. *Для двох послідовностей, складених з* 2^n *двійкових елементів і таких, що містять однакове число* 2^{n-1} *символів кожного типу, збіжні* (*незбіжні*) *послідовності символів містять для кожної з послідовностей однакове число одиниць і нулів.*

Д о в е д е н н я. Нехай $\xi = \{0,1\}^{2^n}$ і $\zeta = \{0,1\}^{2^n}$ – дві випадково взяті 2^n-бітні послідовності з однаковим числом нулів і одиниць і нехай $2k = s + t$,

$s \neq t$, буде числом співпадаючих символів. Нехай далі для конкретності символи, що збігаються містять s одиниць і t нулів (в обох частинах рівності парності міститься по s одиниць і t нулів). Але кожна послідовність складається з однакового числа символів кожного типу. Знову доведення від супротивного. Нехай тепер, скажімо, для першої послідовності ξ в числі незбіжних символів виявляється $2^{n-1} - s$ одиниць і $2^{n-1} - t$ нулів. Але це не співпадаючі символи і, отже, друга послідовність повинна містити $2^{n-1} - s$ нулів і $2^{n-1} - t$ одиниць (протилежні символи).

В результаті виходить, що перша послідовність містить як і належить $2^{n-1} - s + s = 2^{n-1}$ одиниць и $2^{n-1} - t + t = 2^{n-1}$ нулів, а друга $2^{n-1} - s + t$ нулів и $2^{n-1} - t + s$ одиниць, що при $s \neq t$ суперечить вихідному положенню, що кожна з послідовностей складається з однакового числа нулів і одиниць, тобто ми повинні вважати, що $s = t$.

Таким чином, відповідно до твердження 4 серед $2k$ пар збігів ознак парне і непарне в рівностях $\lambda(\alpha, \beta)$ для кожної підстановки половина збігів парне і ще половина непарне.

Перейдемо тепер до визначення числа $\lambda(\alpha, \beta)$ для підстановки степеня 2^n, що нас цікавить.

Зауважимо відразу, що підстановки з одним і тим же значенням параметра збігів відрізняються одна від одної розподілом в лівій і правій частині рівності парних і непарних компонент.

Раніше вже встановлено (твердження 1), що з 2^n скалярних добутків в правих частинах рівностей (як і в лівих) половина добутків мають ознаку парне, а інша половина ознаку непарне (їх 2^{n-1} кожного типу). Причому рівність зберігається, якщо міняються місцями між собою переходи (виходи) підстановки, які дають результатами скалярні добутки з однаковою ознакою парності.

Для 2^{n-1} входів в підстановку з однаковою ознакою парності відповідні виходи утворюють підстановку степен, тобто саму підстановку степеня

можна розглядати як дві підстановки степеня 2^{n-1} (адже переходи випадкової підстановки формуються незалежно одні від інших). Це означає, що для кожного значення маски виходів β існує $2^{n-1}!$ різних підстановок, що відрізняються між собою закріпленням (розстановкою) виходів, які формують ознаки парне і стільки же (тобто $2^{n-1}!$ різних підстановок, що відрізняються між собою закріпленням виходів) підстановок, які формують ознаки непарне. Дійсно, виходи підстановки, що мають відповідні входи з однаковою ознакою парності для фіксованої маски α, зберігаються за кількістю парне і непарне для вихідній маски β при їх перестановці між собою.

В силу незалежності розподілу виходів підстановок по входам всього виходить, що існує $(2^{n-1}!)^2$ варіантів різних підстановок, що мають один і той же розподіл ознак парне чи непарне (2^{n-1} скалярних добутків кожного типу парності), що відрізняються розташуванням виходів підстановки за своїми входами.

Тепер кожна з таких підстановок реалізує значення параметра $\lambda(\alpha,\beta) = 2k$, що нас цікавить, прив'язкою збігів ознак парне і непарне, що входять в $2k$ рівностей $\alpha \cdot X = \beta \cdot \pi(X)$.

У відповідності з твердженням 4 таких збігів буде в $2k$ переходах $\lambda(\alpha,\beta)$ по k кожного типу парності. Ці два набори з рівними значеннями кількості переходів кожного типу (k рівностей $\alpha \cdot X = \beta \cdot \pi(X)$ кожного з типів) можуть бути реалізовані для кожного унікального набору із 2^{n-1} скалярних добутків $\beta \cdot C$ одного типу парності $C_{2^{n-1}}^{k}$ варіантами розстановки виходів підстановки за її входами, а всього виходить, що рівності обох типів парності, що утворюють $2k$ цікавих переходів $\lambda(\alpha,\beta)$, можуть бути реалізовані $\sum_{k=1}^{s} C_l^{2k-1}$ різними способами ($C_{2^{n-1}}^{k} = \binom{2^{n-1}}{k}$ – біноміальний коефіцієнт).

В результаті приходимо до результату, який і стверджується в теоремі.

Далі вже цитуються результати роботи [103].

В лінійному криптоаналізі цікавляться значеннями комірок в лінійній апроксимаційній таблиці підстановки степеня 2^n, які отримані після відрахування з них нормованого значення 2^{n-1}, тобто значеннями комірок лінійної апроксимаційної це відмінності (зміщення) дійсного значення на число 2^{n-1}.

Як зазначено в [102;103;104], вони представляють собою кореляцію лінійних комбінацій входів і виходів підстановки.

В результаті приходять до так званих лінеаризованих таблиць підстановок, які в [103;104] визначаються виразом

$$LAT_\pi^*(\alpha,\beta) = |LAT_\pi(\alpha,\beta) - 2^{n-1}|. \quad (3.14)$$

Модуль у правій частині записаного співвідношення призводить до того, що значення $\lambda(\alpha,\beta) = 2k$ для $2k' = 2k - 2^{n-1},\ 0 \le k \le 2^{n-1}$ можуть бути отримані як при позитивному зміщенні $k' = k - 2^{n-2}$ ($2^{n-2} \le k \le 2^{n-1}$), так і при негативному зміщенні $k' = k - 2^{n-2}$ ($0 \le k \le 2^{n-2}$), причому можливі й нульові значення зміщення ($\lambda*(\alpha,\beta) = 0$), коли $k = 2^{n-2}$.

Повертаючись до старого позначення змінної k (тепер вже для зміщення), теорему можна переписати у вигляді:

Теорема 2: *Нехай $\lambda*(\alpha,\beta)$ буде випадковим числом, що відповідає значенню лінійної апроксимаційної таблиці підстановки $LAT_\pi^*(\alpha,\beta) = |LAT_\pi(\alpha,\beta) - 2^{n-1}|$, коли підстановка π вибрана рівноймовірно з множини S_2^n та маски α,β не нулеві. Тоді $\lambda*(\alpha,\beta)$ для цілих значень $|k| \le 2^{n-2}$ приймає тільки парні значення та ймовірність, що $\lambda*(\alpha,\beta) = 2k$ визначається виразом*

$$\Pr(\lambda^*(\alpha,\beta) = 2k) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + |k| \end{pmatrix}^2. \quad (3.15)$$

Визначемо найбільшого значення таблиці LAT_π^*.

Нехай тепер, як і в [1; 103; 104], $\lambda(\pi)$ буде найбільшим значенням таблиці взятим над усіма невиродженими α і β:

$$\lambda(\pi) \stackrel{\text{def}}{=} \max_{\alpha,\beta\neq 0} LAT_{\pi}^{*}(\alpha,\beta).$$

Тут пропущено ряд міркувань, представлених в роботі [1], зокрема перевірка умов нормування для отриманого закону розподілу ймовірностей.

Позначимо, відмічається далі в роботі [104], $E[\lambda(\pi, 2k)]$ очікуване число комірок таблиці LAT_{π}^{*}, що мають значення $2k$.

У цьому місці, повторюючи міркування роботи [104], ми зробимо перехід від властивостей ансамблю підстановок до властивостей окремої підстановки.

Рахуючи, що отриманий закон розподілу ймовірностей (3.13) справедливий для кожної окремо взятої підстановки, розглянемо його тепер стосовно множини з $(2^n-1)^2$ комірок таблиці LAT_{π}^{*}, що відповідають ненульовим її входам і виходам.

В результаті можна отримати вираз для розрахунку $E[\lambda*(\pi, 2k)]$як просте множення формули (3.13) на загальну кількість комірок таблиці підстановки, виключаючи першу строку та перший стовпець

$$\Pr\left(\lambda^{*}(\alpha,\beta)=2k\right)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\ 2^{n-2}+|k|\end{pmatrix}^2, \qquad (3.16)$$

(для позитивних та негативних значень зміщень результат буде один і той же).

Далі знову наші міркування.

Вираз (3.16) має тенденцію швидко прагнути до нуля з зростанням k. Середньому значенню максимуму таблиць LAT_{π}^{*}підстановки, як слід з співставлення результатів обчислення з експериментальними даними, буде відповідати k^{*}, при якому отримується найменше значення $E[\lambda*(\pi, 2k)]$, що перевищує або дорівнює одиниці, тобто для визначення k^{*}потрібно знайти округлене в бік збільшення до найближчого цілого рішення рівняння

$$\mathrm{E}\left[\lambda^*(\pi,2k)\right]=\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\ 2^{n-2}+|k|\end{pmatrix}^2. \qquad (3.17)$$

Це і є потрібний нам результат.

Порівняємо розрахункові та експериментальні результати. Варіанти рішення рівняння (3.17) (переборним методом, який істотно спрощується при використанні результатів експериментів), разом з даними експериментів, які наведені і в роботі [23], ілюструє таблиця 3.4.

Як випливає з результатів, представлених у таблиці 3.4, знайдені значення максимумів таблиць лінійних апроксимацій випадкових підстановок добре узгоджуються з даними, отриманими експериментально.

Таблиця 3.4

Порівняння теоретичних і експериментальних результатів

n	$2k^*$	$\mathrm{E}\left[\lambda(\pi,2k)\right]$	Експеримент
4	4 6 8	3,89 1,118 0,017	5,498 $\left(\frac{3}{2}\right)^8=5{,}06$
6	12 14 16	9,013 1,7 0,239	14,48 $\left(\frac{3}{2}\right)^6=11{,}39$
8	32 34	2,12 0,7457	34,68 $\left(\frac{3}{2}\right)^8=25{,}62$
10	74 76	1,16 0,64	78,8 $\left(\frac{3}{2}\right)^{10}=57{,}66$
12	162 164	1,129 0,82	116,24 $\left(\frac{3}{2}\right)^{12}=129{,}74$
14	350 352	1,069 0,900	314 $\left(\frac{3}{2}\right)^{14}=291$
16	748 750	1,027 0,93	720 $\left(\frac{3}{2}\right)^{16}=657$

Зауважимо тут, що в правій колонці таблиць представлені також результати по запропонованій в [101] спрощеній формулі

$$\mathrm{E}\left[\lambda(\pi,2k)\right]=\left(\frac{3}{2}\right)^{n}. \tag{3.18}$$

Якщо йти далі, то можна переконатися, що вираз (3.15) можна розглядати як закон розподілу ймовірностей значень $\lambda*(\alpha,\beta)$ таблиці $LAT_{\pi}^{*}(\alpha,\beta)$ окремо взятої випадкової підстановки π. В [101] показано, що для нього виконується умова нормування $Pr(|\lambda(\pi)|\leq 2^{n-1})=1$.

Далі наводяться додаткові матеріали з роботи [6], котрі спрямовані на те, щоб отримати формулу, що піддається розрахунку.

Як показує аналіз, отримане розрахункове співвідношення добре працює для значень $n\leq 32$. Щоб результати представити у закінченому вигляді, тобто для отримання практичних результатів при великих значеннях n в роботі [6] запропоновано скористатися теоремою 9 з роботи [92], в якій обґрунтовується допустимість апроксимації співвідношення (3.15) нормальним законом розподілу ймовірностей. Ця теорема в роботі [92] наводиться під номером 3.

Теорема 3: *Для випадкової n-бітової підстановки, з* $n\geq 5$ *дисбаланс Imb(v, u) апроксимації є випадковим значенням з розподілом, який може бути апроксимованим у вигляді*

$$\Pr(\mathrm{Imb}(\mathrm{v},\mathrm{u})=\mathrm{z})\approx 2Z\left(\frac{z}{2^{(n-2)/2}}\right) \tag{3.19}$$

для z парного і нуль для z непарного.

Якщо в (3.19) підставити $z = 2x$, то його можна переписати в вигляді

$$\Pr(\mathrm{Imb}(v,u)=2x)\approx Z\left(\frac{x}{2^{(n-4)/2}}\right). \tag{3.20}$$

При виводі цього співвідношення автори користуються лемою, що повторює результат (3.13):

$$\Pr(\mathrm{Imb}(v, u) = 2x) = \frac{\binom{2^{n-1}}{2^{n-2}+x}^2}{\binom{2^n}{2^{n-1}}}, \qquad (3.21)$$

тобто в наших позначеннях дисбаланс $\mathrm{Imb}(v, u) = z$ при $z = 2k$ як раз відповідає $\lambda(\pi) = 2k$.

В табл. 3.5 запозиченої з роботи [14] приводяться для порівняння результати оцінки максимального значення лінійної таблиці випадкової підстановки (половинного значення) отримані при використанні апроксимуючого виразу (3.18), апроксимації, використаній в виразі (3.21), і точного розрахунку за формулою (3.15).

Таблиця 3.5

Порівняння результатів здобутих різними шляхами

N	Значення $x = k_L^*$ для нормального закону	Значення x для апроксимації	Розрах. знач. k_L^*
8	16	12,81	16-17
16	334	328,42	374
20	1466	1662,62	1670
24	6342	8417	7302
28	27142	42611,346	31504
32	115080	215719	135649
128	62316975567822669939 $\approx 2^{67} \rightarrow \approx 2^{-120}$	17324119207854702237560 $\approx 2^{75} \rightarrow \approx 2^{-104}$	-

Експериментальні дані у вигляді нормального закону (3.20), виявляються близькими до розрахункових. Видно також, що, якщо

апроксимація нормальним законом дає оцінки занижені, то наша апроксимація призводить до завищених оцінок.

Для значень $n > 32$ залишається орієнтуватися на апроксимуюче співвідношення. Якщо вважати, що співвідношення граничних (оціночних) значень з відповідними апроксимуючими виразами, з істинними значеннями зберігається і для значень $n > 32$, то у відповідності з підходом, що розвивається в роботі [23], можна перейти до розрахунків очікуваних значень максимумів лінійних ймовірностей для повномасштабних шифрів.

Наприклад, використання представлених апроксимуючих співвідношень для 128-ми бітного шифру дозволяє отримати граничні значення для максимальної лінійної ймовірності (зліва і справа) виду

$$2^{-120} \leq LP_{max}^{f^{-104}}.$$

Тут позначення LP_{max}^{f} відповідає максимальному значенню лінійної ймовірності шифруючого перетворення f (підстановки). Зауважимо, однак, що апроксимація нормальним законом для значень $n \geq 32$ виходить істотно точніше нашої апроксимації (судячи з наведених даних, відношення розрахункового і апроксимуючого виразів для апроксимації у вигляді нормального закону приймає значення: при $n = 20 \rightarrow \frac{1670}{1466} = 1{,}139$ при $n = 24 \rightarrow \frac{7302}{6384} = 1{,}144$, при $n = 32 \rightarrow \frac{135649}{115080} = 1{,}178$).

Якщо вважати, що близьке до цього співвідношення (відношення менше двійки) збережеться і для великих значень n, то можна прийти до очікуваного значення ймовірності більш близького до лівого з двох наведених кордонів, тобто як досить точна оцінки лінійної ймовірності для 128 бітового розміру входу в шифр слід розглядати значення $LP_{\max}^{f} \approx 2^{-119}$.

Запропонована апроксимація в цьому випадку дає помилку в 2^{15} рази.

Вона виявляється хорошою для малих версій шифрів. Робота по уточненню результатів триває.

Наведений в роботі закон розподілу ймовірностей для числа зміщень таблиць лінійних апроксимацій випадкових підстановок дозволяє, як показано в роботах [1; 6], ввести більш суворі критерії відбору випадкових підстановок, що впритул наближають їх властивості до властивостей шифруючих перетворень блокових симетричних шифрів. Виведені розрахункові співвідношення для середніх значень максимумів таблиць лінійних апроксимацій дозволяють більш обґрунтовано підійти до оцінки показників стійкості блокових симетричних шифрів до атак лінійного криптоаналізу.

Далі подаються результати досліджень, виконаних в ще одній роботі за участю автора [14]. Вони теж наводяться тут з невеликими скороченнями.

3.4 Уточнена математична модель випадкової підстановки

У цьому підрозділі спробуємо змінити позицію до визначення показників випадковості, що були введені в роботі [7]. Потрібно відповісти на питання щодо властивостей вибірки випадково взятих підстановок. З якими підстановками в цьому випадку реально маємо справу? Як вони співвідносяться з наведеними в роботах [4; 7; 10] критеріями відбору?

Отже, увага зосереджується на вибірці випадкових підстановок.

Будемо цікавитися не законами розподілу таблиць XOR переходів і зміщень таблиць лінійних апроксимацій цих підстановок, а максимальними значеннями, що при цьому виходять. У такій постановці задача зводиться до визначення законів розподілу максимумів вибірки, складеної з заповнень таблиць XOR різниць і зміщень таблиць лінійних апроксимацій підстановок.

Математичний апарат, що буде використаний далі, наведений у Додатку В.

3.4.1 Розподіл максимумів XOR таблиць вибірки з байтових підстановок

Основу представлених далі матеріалів складає робота [14].

Зосередимо увагу на вибірці випадкових байтових підстановок. Будемо цікавитись не законами розподілу таблиць XOR переходів і зміщень таблиць

лінійних апроксимацій цих підстановок, а максимальними значеннями отриманих законів. Знову, як і в попередньому розділі, цікавимося двома випадками.

1-й випадок, коли вибірка складається із значень переходів XOR таблиць випадкової підстановки. Як відомо [97], в цьому випадку закони розподілів ймовірностей переходів підкоряються пуасонівському закону (3.10).

2-й випадок, коли вибірка складається із значень, що представляють зміщення таблиць лінійних апроксимацій випадкових підстановок, що підкоряються нормальному закону розподілу ймовірностей (3.21).

В обох випадках будемо мати справу з великими за обсягами вибіркових часток незалежних однаково розподілених випадкових величин, тобто в умовах застосування математичного апарату, наведеного в Додатку В.

У випадку з байтовою підстановкою будемо розглядати вибірку розміром 2^n, $n = 8$. Для $n = 8$.

$$i = \frac{\ln(2)\cdot 16 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}. \qquad (3.22)$$

З результатів, представлених у табл. 3.6, рішенням рівняння (3.21) є значення $i = a$ близьке до числа 6.

Таблиця 3.6

Рішення рівняння (3.21) перебірним методом

I	$\frac{\ln(2)\cdot 16 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}$
5	6,8
5,5	6,3
5,9	5,98
6	5.9
7	5,3

Відповідно $b = \frac{1}{\ln(12)} = 0{,}4$. Але зауважимо тут, що формула (3.22), по якій визначалось значення a, працює з половинним значенням переходу диференціальної таблиці.

При підрахунку дійсного середнього значення необхідно отриманий результат подвоїти, і тоді отримаємо значення $\mu(X) = 2 \cdot 6 + 2 \cdot 0{,}4 \cdot 0{,}58 = 12{,}4$.

Якщо орієнтуватися на результати реального експерименту, то середнє значення максимуму має бути близьким до 11,55.

Тому скорегуємо отримане значення до $a = 5$. Значення добре узгоджується з результатами розрахунків та експериментів, представлених в [2].

Оскільки розподіл максимумів дискретний, то мала величина стандартного відхилення $b = \frac{1}{\ln(12)} = 0{,}4$ призводить до того, що розподіл зосереджено в двох цілочисельних значеннях поблизу $\mu(X) \approx 2a$.

У експериментах з байтовими підстановками це два значення 10 і 12.

Розрахунок далі пропонується вести за розподілом

$$D_{\max}(X) \approx e^{-e^{\frac{10-2 \cdot X}{0{,}87}}}, \qquad (3.23)$$

в якому використано значення $a = 5$ (формула записана з урахуванням реального подвоєння значень переходів XOR таблиці).

У таблиці 3.7 наводиться розподіл значень максимумів для 256 бітових підстановок розрахованих за виразом (3.23) і результати експерименту.

З представлених результатів слідує, що теоретичні і експериментальні результати практично повторюють один одного.

Це означає, що для розподілу диференціалів байтових підстановок виконується пуасонівський закон розподілу ймовірностей.

Цей закон використаний при побудові інтегрального закону розподілу максимумів розглядаємих підстановок.

Таблиця 3.7

Розподіл значень максимумів вибірки з підстановок степеня 2^8 розрахованих за виразом (3.23) і результати експерименту

k^* (X_1, X_2)	Pr(k^*)	Розрахункове значення	Експери - мент
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	92
12 (12,10)	0,905 – 0,368 = 0,537	137	147
14 (14, 12)	0,9901 – 0,905 = 0,008	22	14
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	3
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0

3.4.2 Розподіл максимумів зміщень таблиць лінійних апроксимацій вибірки з байтових підстановок

Для випадку, коли вибірка складається з випадкових значень, що представляють зміщення таблиць лінійних апроксимацій випадкових підстановок приходимо до рівняння

$$a_s = \sqrt{ln(2)32 - ln(2\pi) - 2\,ln(a_s)} \qquad (3.24)$$

У табл. 3.8 представлені результати вирішення рівняння (3.24) способом підбору.

Для орієнтовного вибору початкових значень, використовуваних в переборі цілком можна спиратися на результати розрахунків і експериментів, наведених в роботі [2].

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s} = \frac{1}{4} = 0{,}25 \qquad (3.25)$$

В цьому випадку зроблено невелику корекцію результату, орієнтуючись на дані експериментів.

Таблиця 3.8

Рішення рівняння (3.24) способом підбору

a_s	$\sqrt{\ln(2)32 - \ln(2\pi) - 2\ln(a_s)}$
4	4,19
5	4.13
6	4,09
8	4

Як значення a_s розглядалось значення a_s= 4 і відповідно (враховано результати експериментів, представлених в табл. 3.3).

Для підстановок степеня 2^8 відповідно до (3.20) маємо $\sigma = 2^{\frac{8-4}{2}} = 2^2$ і тоді $a = \sigma a_s + \mu(X) = 4 \cdot 4 + 0 = 16$ і відповідно до (3.18) $b = 4 \cdot 0{,}25 = 1$, і ми приходимо до інтегрального закону розподілу максимумів лінійних зміщень байтової підстановки у вигляді:

$$D_{\max}(X) \approx e^{-e^{\frac{16-X}{1}}}, \qquad (3.26)$$

або з урахуванням реального подвоєння результатів зміщень таблиці лінійних апроксимацій

$$D_{\max}(X) \approx e^{-e^{\frac{32-X}{2}}} \qquad (3.27)$$

У табл. 3.9 представлені результати розрахунків по визначенню розподілу значень максимумів зміщень лінійної апроксимаційної таблиці випадкової підстановки на основі інтегрального закону розподілу ймовірностей (3.27).

Цікаво, що як показали експерименти [1], саме випадкові підстановки отримані без всяких обмежень, з дуже великою ймовірністю виявилися придатними з точки зору криптографічних прикладень.

Таблиця 3.9

Розподіл значень максимумів зміщень для множини байтових підстановок, розрахованих за виразом (3.27) і результати експерименту.

k^* (X_1, X_2)	Pr(k^*)	Число значень	Експеримент
< 26	$3.41\ 10^{-7}$	0	0
28 (28,26)	$5{,}6\ 10^{-4} – 3{,}4110^{-7} = 5{,}6\ 10^{-4}$	0,14	0
30 (30,28)	$0{,}064 – 5{,}6\ 10^{-4} = 0{,}0638$	16,3328	10
32 (32,30)	0,368–0,064 = 0,304	77,824	86
34 (34,32)	0,692 – 0,304 = 0,388	99,328	98
36 (36,34)	0,874 – 0,692 = 0,181	46,336	46
38(38,36)	0,9518 – 0,874 = 0,078	19,968	10
40 (40,38)	0,9821 – 0,9518 = 0,03	7,68	6
42 (42,40)	0,9933 – 0,9821 = 0,011	2,816	0
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

Вони дозволили забезпечити динамічні показники виходу шифрів з сильним лінійним перетворенням до асимптотичних показників випадкових підстановок, які не поступаються кращим (відібраним за спеціальними методиками) S-блокам практично всіх сучасних шифрів [3; 4]. Можна впевнитись, що значення максимумів для диференціальних таблиць байтових підстановок дорівнює 8-10, а для таблиць лінійних апроксимацій дорівнює 32-34. Це характерно для більшості симетрическьких груп байтових підстановок.

У таблиці 3.10 запозиченої з роботи [106], ми наводимо розподіл максимумів диференціальних і лінійних ймовірностей для всіх 16! напівбайтових підстановок (для байтових підстановок такий експеримент обчислювально не реалізований).

Таблиця 3.10

Розподіл 16! підстановок щодо диференціального криптоаналізу (рядки) і лінійного криптоаналізу (колонки)

$LC \rightarrow DC\downarrow$	$\varepsilon \le 1/4$		$\varepsilon \le 3/8$		$\varepsilon \le 1/2$	
	n	%	*n*	%	*n*	%
$p \le 1/4$	749123665920	3,5804	326998425600	1,5629	0	0,0000
$p \le 3/8$	10404495336000	4,9728	11448247910400	54,7166	118908518400	0,5683
$p \le 1/2$	520222476800	0,2486	5812644741120	27,7814	330249830400	1,5784
$p \le 5/8$	0	0,0000	738314675200	3,4810	193458585600	0,9246
$p \le 3/4$	0	0,0000	52022476800	0,2486	680988572900	0,3255
$p \le 1$	0	0,0000	309657600	0,0015	1940520960	0,0093

Навіть усічені розподіли байтових підстановок (табл. 3.7 і табл. 3.9) практично повторюють розподіл максимальних переходів для основної маси напівбайтових підстановок (див. табл. 3.10). З таблиці також видно, що основна маса, 54,7155% всіх напівбайтових S-блоків, мають диференціальну границю $p < 3/8$ і лінійний кордон $\varepsilon < 3/8$, при цьому:

$p = 1/4$ відповідає значенню переходу напівбайтової підстановки рівному 4;

$p = 3/8$ відповідає значенню переходу напівбайтової підстановки рівному 6;

$p = 1/2$ відповідає значенню переходу напівбайтової підстановки рівному 8;

p = 3/4 відповідає значенню переходу напівбайтової підстановки рівному 12.

Тут $p = n/|S|$ – диференціальна ймовірність.

В роботі [89] зміщення визначається як

$$\varepsilon = \text{abs}\left(\frac{n}{|S|} - \frac{1}{2}\right),$$

де n– значення комірки таблиці ЛАТ, $|S|$ – число входів в таблицю.

Це означає що:

ε = 1/4 відповідає зміщенню таблиці напівбайтової підстановки рівному 12 (для байтової підстановки це буде значення менше 30-ти);

ε = 3/8 відповідає зміщенню таблиці напівбайтової підстановки рівному 14. (для байтової підстановки це значення близьке до 34);

ε = 1/2 відповідає зміщенню таблиці напівбайтової підстановки рівному 16 (для байтової підстановки це значення, що перевищує 42).

Видно, що результати експериментів добре узгоджуються з даними таблиці 10. Тут найбільш ймовірним значенням максимуму диференціальної таблиці є значення 6.

Отже, можна впевнитись, що значення максимумів XOR різниць для диференціальних таблиць байтових підстановок в більшості випадків дорівнюють 8-10, а значення максимумів зміщень таблиць лінійних апроксимацій дорівнюють 32-34.

Більше того, як випливає з представлених результатів, підстановки зі значенням максимумів XOR різниць менше ніж 12 складають 99% (менше ніж 10 складають 93%).

Значення максимумів зміщень для лінійних таблиць байтових підстановок в більшості випадків дорівнюють 32-34. З представлених результатів випливає, що підстановки зі значенням максимуму зміщень менше ніж 36 складають 94% (менше ніж 34 складають 76%).

3.5 Криптографічні властивості випадкових S-блоків

Сьогодні для визначення криптографічних показників S-блоків широко використовується математичний апарат булевої алгебри. Він будується на представленні S-блоків у вигляді композиції булевих функцій.

Напрацьована ціла система показників для визначення криптографічних властивостей булевих функцій і S-блоків (векторних булевих функцій) такі як: високий алгебраїчний степінь, урівноваженість і досконала урівноваженість, лавинні характеристики, відсутність лінійних структур, кореляційна імунність і стійкість, висока нелінійність, статистична незалежність, алгебраїчна імунність, диференціальна рівномірність та інші.Зв’язок цих показників з методами криптоаналізу та їх визначення добре проілюстровані в роботі [107].

Вище було зроблено висновок щодо низької ефективності цього апарату відносно застосування випадкових S-блоків в сучасних шифрах (правда, розробники відмічають, що S-блоки шифру Калина-2 вибиралися з випадкових підстановок. Шукались S-блоки з високою нелінійністю (104) і високою алгебраїчною імунністю (3). Оскільки цей апарат багато спеціалістів вважають дуже важливим, наведемо відомості з використання цього апарату і для оцінки криптографічних показників випадкових S-блоків.

Будемо цікавитись використанням в шифрах саме випадкових S-блоків, тобто безпосередньо S-блоків з виходу генератора випадкових підстановок. Вони будуть володіти з великою ймовірністю гарними криптографічними показниками з наведеного вище списку. Цей тезис, однак, визиває у багатьох спеціалістів заперечення.

Вони вважають, що випадково взяті S-блоки не будуть гарантувати високі показники стійкості насамперед до алгебраїчних методів криптоаналізу. В криптографічній літературі задача пошуку S-блоків з високими криптографічними (алгебраїчними) показниками виділяється в окремий напрямок вдосконалення шифрів.

Особливий інтерес визиває показник алгебраїчної імунності і його зв’язок з алгебраїчним степенем булевої функції. Деякі відповіді були

знайдені у публікації журналу “Дискретна математика” [107]. З наведеної в цьому виданні статті А. А. Городілової, присвяченій викладенню властивостей булевих функцій і їх зв’язку з методами криптоаналізу виділемо декілька теорем (результатів).

Спочатку про нелінійність випадкової функції.

Теорема 6. (нелінійність випадкової функції). *Існує константа* $c < 1$ *така, що для майже всіх булевих функцій* f *від* n *змінних виконується умова* $N_f \geq 2^{n-1} - 2c\sqrt{n}2^{n/2-1}$.

Для $n = 8$, $c = 0{,}7$ виходить $N_f \geq 128 - 32$.

Даний результат говорить, що нелінійність довільної функції близька до верхньої межі $N_f \leq 2^{n-1} - 2^{n/2-1}$, але відмічається в [107], як це часто буває, знаходження конкретних функцій з високою нелінійністю є нетривіальною задачею. Використовують детерміновані, часом дуже складні методи побудування таких функцій (методи Себері, К. Нюберг та інші).

А чого не взяти випадково породжений S-блок і не перевірити його властивості? Нетривіальна задача стає тривіальною. Щодо алгебраїчної імунності. В цій роботі наводяться такі відомі факти з огляду [107]. Відмічається, що алгебраїчна степінь $deg\, f$ служить природною верхньою оцінкою для алгебраїчної імунності AI булевої функції f. Крім того, справедлива наступна верхня межа алгебраїчної імунності, що залежить від числа змінних n.

Теорема 11. (верхня оцінка для AI*). Для довільної булевої функції* f *від* n *змінних виконано* $\mathrm{AI}(f) \leq \lceil n/2 \rceil$, *де* $\lceil k \rceil$ *– ціла частина числа k.*

При цьому відомо, що дана оцінка досяжна. Хоча існують приклади функцій з максимальною алгебраїчною імунністю, відомо, що цій клас функцій вельми малий. Однак цікавим є той факт, що алгебраїчна імунність довільної функції досить висока.

Наведемо також теорему 13 з цієї роботи.

Теорема 13. (AI випадкової функції*). Для будь-якого α<1 і для майже усіх булевих функцій від n змінних виконана умова*

$\mathrm{AI}(f) > n/2 - \sqrt{n/2 \cdot ln(\, n/2\alpha \, ln\, 2)}.$

Для n = 8, α = 1 виходить $\mathrm{AI}(f) > 4 - 2{,}64 = 1{,}36.$

Наведемо також відому точну нижню оцінку нелінійності функції через її алгебраїчну імунність.

Теорема 14. (зв'язок AI і N_f). *Для булевій функції f від n змінних справедлива оцінка* $N_f \geq 2 \sum_{i=1}^{\mathrm{AI}(f)-2} C_{n-1}^{i}$.

Для n = 8, $\mathrm{AI}(f) = 4$ виходить $N_f \geq 58.$

В роботі [108] робиться дуже важливий для нас висновок: *теоретичні результати показують, що у випадково взятій булевій функції більшість криптографічних параметрів близькі до оптимальних.*

Доречним на закінчення буде також навести результати експериментів з випадковими байтовими S-блоками отриманими в роботі [94], що наведені в таблиці 3.11 (з позначеннями з цієї роботи).

Таблиця 3.11

Криптографічні властивості випадково згенерованих байтових підстановок

Критерій	Значення	% згенерованих S-блоків
Максимум *DDT*	8	0,004
Максимум ЛАТ (нелінійність)	32(96)	11
	30(98)	0,15
	28(100)	0
Мінімальна степінь *BF*	7	30
Алгебраїчна імунність	3	100

Експеримент проводився для 10 мільйонів підстановок.

Отже важливий висновок з цих результатів міститься в тому, що всі 100 % випадкових S-блоків мають алгебраїчну імунність рівну трьом. Кожний третій випадковий S-блок володіє оптимальними криптографічними показниками (має максимальну алгебраїчну степінь 7).

Випадкова підстановка з виходу генератора випадкових підстановок з великою імовірністю буде хорошим S-блоком. Це підтверджують численні експерименти.

Але враховуючи все ще не великий опит використання випадкових підстановок для побудови шифрів і досить критичне відношення до цієї моделі більшості спеціалістів, як удосконалену модель випадкової підстановки пропонується розглядати випадкову підстановку з виходу генератора випадкових підстановок, що проходить перевірку на відповідність мінімум чотирьом показникам S-блоку і булевих функцій що його утворюють:

1. Максимальне значення XOR переходу знаходиться в діапазоні 8÷10;

2. Максимальне значення зміщення ЛАТ знаходиться в діапазоні 32÷34 (тобто нелінійність дорівнює 94÷96).

Висновки до розділу 3

Пройдено довгий шлях по обґрунтуванню критеріїв відбору випадкових підстановок від найпростіших комбінаторних до досить жорстких додатково розроблених критеріїв, що будуються на використанні оцінок близькості законів розподілу XOR таблиць і зміщень таблиць лінійних апроксимацій до теоретичних законів.

Проте не вдалось знайти будь-яких особливих переваг підстановок, відібраних з використаним навіть жорстких критеріїв. Вони за своїми криптографічним показником, які визначаються за допомогою відомих методів, в тому числі і алгебраїчних, нічим особливо не виділяються на тлі інших відомих конструкцій [3; 4]. Від усіх розглянутих критеріїв відбору випадкових підстановок в поданій редакції довелося відмовитися. Ми

перейшли до уточненої більш практичної математичної моделі випадкової підстановки, побудованої на властивостях вибірки випадкових підстановок (ця модель увібрала в себе і знайдені диференціальний і лінійний закони розподілу переходів відповідних таблиць підстановок).

Підстановки є одним з важливих елементів в конструкціях сучасних шифрувальних перетворень, виконуючи роль додаткового, якщо не головного, механізму ефективного випадкового перемішування блоків даних.

Основним підсумком розділу є уточнена модель випадкової підстановки. Відповідно до цієї моделі підстановка вважається випадковою, якщо вона належить до ансамблю підстановок, максимуми XOR таблиць і зміщень таблиць лінійних апроксимацій яких підкоряються закону розподілу екстремальних значень Фішера-Тіппета (log-Вейбула). Це дає можливість у якості випадкових (байтових) підстановок в шифрах використовувати безпосередньо підстановки, сформовані випадковим генератором підстановок.

Отже, вперше запропоновано як S-блоки шифрів використовувати випадкові підстановки з виходу генератора випадкових підстановок, що проходять перевірку на відповідність додатним критеріям відбору. Зокрема, байтова підстановка вважається випадковою, якщо:

1. Максимальне значення XOR переходу знаходиться в діапазоні 8÷10;

2.Максимальне значення зміщення ЛАТ знаходиться в діапазоні 32-÷34;

3. Алгебраїчний степінь не менше 7;

4. Показник алгебраїчної імунності не менше 3.

Важливий висновок міститься в тому, що для випадково взятої булевої функції більшість її криптографічних параметрів близькі до оптимальних.

В результаті набуває актуальності задача побудування шифрів, в яких без зниження стійкості можуть бути використані випадкові S-блоки. Вивченню можливостей її здійснення присвячені наступні розділи роботи.

Матеріал розділу побудований на публікаціях автора [8; 16; 20; 23] та інших.

РОЗДІЛ 4

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ДИНАМІЧНИХ ПОКАЗНИКІВ ПРИХОДУ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ ДО СТАНУ ВИПАДКОВОЇ ПІДСТАНОВКИ

Основний матеріал для цього розділу взятий з роботи [21].

Слід зазначити, що не перший раз звертаємося до вивчення динамічних показників приходу блокових симетричних шифрів до стану випадкових підстановок. Тут можна вже назвати кілька робот, виконаних за участю автора дисертації, що опубліковані раніше [15; 17; 18; 109].

І в цьому розділі мова буде йти про нову методику (методологію) оцінки стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу [1]. Основна увага в розділі приділена визначенню експериментальним шляхом динамічних показників приходу ряду сучасних блокових симетричних шифрів до стану випадкової підстановки. Серед розглянутих шифрів Rijndael, IDEA NXT, Мухомор, Білоруський шифр, Калина-2, Camelia та інші. Показано, що всі розглянуті (відомі) конструкції сучасних блокових симетричних шифрів в більшості своїй забезпечують динамічні показники приходу до стану випадкової підстановки, що перевищують 3÷4 цикли. Зазначається, що основну роль в забезпеченні високих динамічних показників приходу шифрів до стану випадкової підстановки грають перші цикли перетворень (мінімальне число активізуємих S-блоків першого і другого циклів). До найбільш прогресивних рішень з побудови блокових симетричних шифрів віднесені шифри ШУП-2, IDEA NXT, білоруський шифр і шифр Мухомор. У цих шифрах внаслідок активізації одним байтом входу відразу декількох S-блоків циклової функції забезпечується збільшене в порівнянні з іншими шифрами мінімальна кількість S-блоків, що активізуються на перших циклах. Криптографічні властивості таких шифрів практично не залежать від диференціальних і

лінійних властивостей використаних S-блоків. Лідером за динамічними показниками приходу шифрів до стану випадкової підстановки виступають шифри Мухомор [45] і ШУП-2 [22]. Останній буде розглянутий в даній роботі. В цих шифрах при побудові циклових функцій застосовується двошарове підстановлювальне перетворення. Це єдині шифри, у яких з великою ймовірністю активізуються всі (або майже всі) S-блоки другого шару підстановлювальних перетворень. Сюди ж можна було б віднести і шифр «Кузнечик», якщо переформатувати його два цикли в одноциклову функцію, однак це 128 бітний шифр. І ніхто ще не придумав, як реалізувати множення на МДВ матрицю розміру 32×32. Нам вдалося реалізувати стратегію широкого сліду без застосування сепарабельних кодів [19] і в разі SPN шифрів з 256-бітовим входом, орієнтованих на застосування в постквантовий період розвитку криптографії.

Об’єктом досліджень даного розділу є процеси приходу блокових симетричних шифрів до стану випадкової підстановки.

В рамках цього розділу в усіх випадках незалежно від способу введення в шифри ключової інформації інтерес буде зосереджений в основному на проходженні через шифри XOR різниць. Оскільки всі шифри відносно до XOR різниць асимптотичне поводяться однаково (як випадкові підстановки), з’явилась можливість привести всі шифри до єдиної шкали оцінок стійкості до атак диференціального криптоаналізу.

Методика, що розвивається, орієнтована на використання повномасштабних алгоритмів шифрування. Підхід дозволяє виконати більш точне порівняння шифрів по стійкості. При загальних однакових максимальних значеннях диференціальних (та лінійних) ймовірностей повноциклових версій шифрів їх можна порівнювати за кількістю циклів необхідних для приходу до стану випадкової підстановки. Це реальний шлях виконання порівняння шифрів за ефективністю. Той шифр вважається більш ефективним, який приходить до стану випадкової підстановки за меншу кількість циклів.

Метою даного розділу є уточнення за допомогою обчислювальних експериментів значень динамічних показників приходу ряду сучасних шифрів до стану випадкової підстановки, які можуть стати важливими при порівняльній оцінці їх ефективності. Фактично мова йде про обґрунтування нового методу оцінки ефективності блокових симетричних шифрів, який представляється у вигляді нового наукового результату дисертаційної роботи.

У попередніх роботах [17; 18; 109] та інші вже викладені теоретичні та практичні міркування щодо формування оцінок динамічних показників приходу шифрів до стану випадкових підстановок. Тут і далі під динамічними показниками приходу шифру до стану випадкової підстановки розуміється мінімальна кількість циклів шифрування, після яких шифр стає випадковою підстановкою (приходить до стаціонарних значень максимумів диференціальних і лінійних ймовірностей, характерних для випадкових підстановок). У цьому розділі ставиться завдання узагальнення раніше отриманих результатів та доповнення їх визначенням тепер уже експериментальним шляхом мінімальної кількості S-блоків, що активізуються на перших циклах шифрування, що забезпечує досягнення теоретичних (розрахункових) показників стійкості (значень максимумів диференціальних і лінійних ймовірностей). На основі цих показників можна оцінити мінімально допустиму кількість циклів зашифрування, після яких шифри стають випадковими підстановками.

4.1 Стислий огляд попередніх результатів досліджень

Обсяг дисертації обмежений. Тому частина виконаних досліджень представляється в реферативному вигляді.

Повернемося до вже зазначених вище робіт [17; 18; 109].

Найбільш важливий результат, з представлених в роботі [17], полягає у введенні рівнянь зашифрування, що зв’язують диференціальні та лінійні показники S-блоків шифрів з диференціальними й лінійними показниками (показниками стійкості) шифрів в цілому. З їх допомогою вдалося пояснити

одну з центральних ідей нової методології – прихід шифрів після декількох початкових циклів шифрування незалежно від використовуваних S-блоків до станів випадкових підстановок.

Нагадаємо ці рівняння. Вони становлять теоретичну основу методу, що розвивається. При записі рівнянь шифрування в [17] береться до уваги (як це було зроблено в роботі Е. Біхама при аналізі шифру DES [105]), що ймовірності диференціальних і лінійних характеристик шифрів для рівноймовірних і незалежних послідовностей ключових бітів визначаються добутками ймовірностей переходів активних S-блоків, що входять до них. Це є підставою для подання зв'язків між диференціальними та лінійними показниками шифрів в цілому (показниками їх стійкості) за диференціальними й лінійними (з обліком накопичувальної леми [110]) показниками S-блоків, що входять в них, у вигляді двох очевидних співвідношень:

$$IPS_D = \left(DP^{\pi}_{\max}\right)^k \tag{4.1}$$

$$IPS_L = 2^{k-1}\left(LP^{\pi}_{\max}\right)^k \tag{4.2}$$

Тут DP^{π}_{max} і LP^{π}_{max}– значення диференціальної й лінійної ймовірностей підстановлювальних перетворень $\pi(x)$. IPS_D (Differential Indicator of Provable Security)–диференційний показник доказової стійкості, IPS_L (Linear Indicator of Provable Security) – лінійний показник доказової стійкості, $k = k_{min}$– мінімальне число активних S-блоків, що беруть участь у формуванні переходу шифру до випадкової підстановки (визначення DP^{π}_{max} і LP^{π}_{max} наведені у Додатку В).

Ці рівняння дозволили пояснити властивість незалежності показників стійкості шифрів від диференціальних і лінійних властивостей S-блоків, що використовуються в шифрах, яка була підтверджена в ході експериментів для багатьох шифрів.

У цій же роботі зроблений висновок, що існують шифри, в яких як нелінійні перетворення можуть бути успішно використані підстановки,

сформовані генератором випадкових чисел. Для цих шифрів пошук підстановок з поліпшеними криптографічними показниками втрачає будь-який сенс. Це досягається завдяки тому, що циклові перетворення цих шифрів мають запас за кількостю S-блоків, що активуються на перших циклах, в порівнянні з їх мінімальною кількістю, необхідною для приходу шифру до випадкового стану.

Одночасно вдалося підтвердити довіру до результатів оцінок диференціальних і лінійних показників повномасштабних шифрів і їх зменшених моделей, отриманих в численних експериментах [6; 17; 18] та інші.

Відзначається, що в більшості наявних шифрів циклові перетворення побудовані таким чином, що лінійні та диференціальні показники S-блоків, що входять до них, впливають (в межах одного циклу), на динамічні показники приходу шифру до стану випадкової підстановки.

Це шифри з малими значеннями кількості активних S-блоків на перших циклах шифрування, необхідних для відповідного переходу (Rijndael, Калина і деякі інші).

У таких шифрах кількість активних S-блоків перших циклів знаходяться на межі забезпечення мінімальної їх кількості, необхідної для приходу шифру до стану випадковій підстановки.

І, отже, диференціальні та лінійні показники S-блоків впливають на мінімально необхідну кількість циклових перетворень приходу шифру до випадкової підстановці, а це означає, що випадкові S-блоки можуть бути не оптимальними для застосування в шифрі.

У цих випадках можна ставити та вирішувати завдання оптимізації S-блоків за лінійними, диференціальними та іншими показниками випадковості. Але далі буде показано, що відповідно до методів проектування БСШ, що розвиваються, можна вдосконалити відомі конструкції шифрів, забезпечивши без втрати їх стійкості можливість використання в шифрах випадкових S-блоків.

В роботі [17] відзначається, що результати виконаних розрахунків також підтверджують, що серед відомих конструкцій шифрів абсолютними чемпіонами по динаміці приходу шифрів до стаціонарного стану, властивого випадковій підстановки, є шифри Мухомор, Білоруський шифр і ШУП-2. Ці шифри стають випадковими підстановками після двох циклів шифрування, чого не може бути реалізовано іншими відомими шифрами.

Цей ефект досягається внаслідок того, що в цих шифрах використовуються конструкції циклових функцій зі збільшеною кількістю S-блоків у перших циклах шифрування (це не SPN шифри) в порівнянні з шифрами з одношаровими підстановлювальними цикловими перетвореннями класичних конструкцій.

В шифрах Мухомор і ШУП-2 також застосовується ефективний механізм послідовного запуску S-блоків, що дозволяє забезпечити граничний коефіцієнт розгалуження (один вхідний байт з ненульовою вихідною різницею активує майже всі S-блоки другого шару першого циклу!).

Відповідно до результатів тестування по швидкодії шифрів AES, Мухомор і ГОСТ-28147-89, наведених в роботі [111], шифр Мухомор в повній версії демонструє показники швидкодії, близькі до шифру AES.

Це дозволяє зробити висновок, що зниження кількості застосовуваних циклів шифрування робить шифр Мухомор безумовним лідером серед багатьох відомих шифрів і за показниками швидкодії.

Можна відзначити, що при зменшенні кількості циклів, і інші показники шифру Мухомор залишаються на досить високому рівні (безпечність проти інтегрального криптоаналізу, бумеранг атаки, інтерполяційної атаки, атаки на пов’язані ключі [45]).

Табл. 4.1 ілюструє встановлені з допомогою зрозумілих міркувань оцінки відповідного мінімального числа циклів для виходу різних шифрів за диференціальними показниками до стаціонарного стану випадкової підстановки.

Таблиця 4.1

Мінімальне число циклів для виходу шифру за диференціальними показниками до стаціонарного стану випадкової підстановки

Шифр	$r_{\min}$
Rijndael-128	3
Калина-128	3
FOX-64	2
FOX-128	2
ГОСТ 28147-89	9
Хеус-16	6-12
Мухомор-128	3
Мухомор-256	3
Serpent	3
Лабіринт	≥ 3
Шифр с цикловою функцією М-64	2
Шифр с цикловою функцією М-128	2

В роботі [17] показано, що для Rijndael-подібних шифрів, до яких відноситься сам шифр Rijndael, а також шифри Калина, Anubis, ADE, GrandCru і декілька інших, конструкція циклового перетворення для будь-яких S-блоків не дозволяє реалізувати перехід до випадкової підстановки за лінійними показниками менше ніж за чотири цикли.

Представлені в цій роботі результати свідчать, що висновок, зроблений в роботі [6] про те, що задача пошуку S-блоків з поліпшеними криптографічними показниками втратила перспективу для таких шифрів виявляється не зовсім вірним.

В роботі [96] увага зосереджується на обліку при побудові диференціальних і лінійних характеристик S-блоків з не максимально можливими переходами (в тому числі випадкових S-блоків).

Знову робиться висновок, що майже всі відомі сучасні шифри мають число циклів виходу до стану випадкової підстановки 3 і більше, тому що майже всі відомі конструкції не орієнтовані на активізацію всіх S-блоків другого циклу (для відомих SPN шифрів мінімальне число активізуємих S-блоків першого циклу дорівнює одному).

Знову в кращу сторону виділяються блокові шифри Мухомор і білоруський стандарт (вони мають двошарову конструкцію першого циклу). На закінчення ставиться питання про можливості побудувати шифр, який би став випадковою підстановкою відразу з першого циклу.

В процесі подальших досліджень був зроблений висновок, що для SPN шифрів з одношаровими підстановлювальними перетворенням такий шифр побудувати не можна. Для шифру з одношаровим підстановлювальним перетворенням можна ставити й вирішувати задачу тільки активізації всіх S-блоків другого циклу.

4.2 Методика виконання досліджень

У цій роботі увага зосереджується на самому процесі (динаміці) переходу шифрів до стану випадкових підстановок. У цьому напрямку вже був виконаний ряд робіт. Так, в роботах [17; 18; 109] викладена методика визначення динамічних показників приходу шифрів до стану випадкової підстановки.

На основі цієї методики визначені значення показників приходу до стану випадкової підстановки ряду сучасних шифрів в основному виходячи з інтуїтивних міркувань.

Ця методика будується на положенні, що результуючі значення диференціальних і лінійних ймовірностей шифрів формуються на основі добутку відповідних перехідних ймовірностей активних S-блоків, що входять в їх характеристики.

Справедливість цього підходу в теоретичному відношенні пов’язана з припущенням про незалежність циклових підключів шифрів. Насправді механізм випадкового перемішування виходів S-блоків в реальних

конструкціях циклових перетворень працює і без ключових добавок. Як показали численні експерименти, показники випадковості шифрів як з реальними підключами, так і з підключами з нульовими значеннями (їх відсутності) збігаються [96]. Активними S-блоками за диференціальними показниками тут і далі названі S-блоки з ненульовими вхідними та вихідними різницями.

Активними S-блоками для лінійних показників названі S-блоки з ненульовими переходами для ненульових масок на їх входах і виходах.

Далі мова йде про диференціальні показники.

Для виконання експериментів використовуються програмні моделі шифрів, тому що необхідно мати можливість підключатися до виходів S-блоків циклових функцій і визначати байтові значення різниць на їх виходах (значень переходів для таблиць лінійних апроксимацій).

Методика виконання експериментів полягає в активізації шифрів (програмних моделей) наборами вхідних різниць і подальшого визначення мінімальної кількості S-блоків, що активізуються на перших циклах шифрування. Вона дозволяє отримати значення диференціальної ймовірності відповідне показнику стійкості розглянутого шифру (яке задовольняє рівнянню (4.1)).

При визначенні лінійних показників перебираються ненульові маски входів в S-блоки і ненульові маски їх виходів. На вході шифру активізується один байт вхідного блоку даних, причому вибирається байт, який активізує мінімальне число S-блоків першого циклу.

4.3 Результати експериментальних досліджень

Шифр Rijndael [42]. Для шифрів, таких як Rijndael і інші з прозорою структурою порівняно легко визначити мінімальне число активних S-блоків для приходу шифру до стану випадкової підстановки і без обчислювальних експериментів.

Наведемо тут і динамічні показники шифру Rijndael, отримані експериментальним шляхом. Ці результати ілюструє табл. 4.2.

Таблиця 4.2

Розподіл числа активних S-блоків на перших циклах шифрування при активізації одного байту входу шифру Rijndael (65280 значень ненульових різниць)

Число активних S-блоків	Число ненульових однобайтових різниць			
	1-й цикл	2-й цикл	3-й цикл	4-й цикл
0	0	0	0	0
1	65280	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	65280	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	1
14	0	0	0	119
15	0	0	0	3883
16	0	0	65280	61275

У цій таблиці наведена кількість активізуємих S-блоків на відповідних циклах шифрування при однобайтових різницях входу. Ці ж результати випливають і з міркувань, представлених в роботах [17; 18; 109]. За

наведеними даними шифр Rijndael приходить до стану випадкової підстановки за диференціальними показниками за три цикли, а за лінійними за чотири.

Шифри сімейства IDEA NXT [43; 44]. Шифр IDEA NXT можна розглядати у вигляді розвитку стратегії широкого сліду по шляху збільшення числа активізуємих S-блоків циклової функції. В шифрі IDEA NXT використовується подвоєне (два шари) число S-блоків функцій ускладнення.

В результаті чого мінімальне число активізуємих S-блоків першого циклу виходить рівним 5 для 32-бітної функції ускладнення і 9 для 64-бітної функції ускладнення. Помітимо тут, що в кожному циклі шифру IDEA NXT, використовується додавання з трьома лінійками циклових підключів.

В роботі [109] припускалося, що основна роль схеми Lai-Massey – це отримати внаслідок зовнішнього контуру перетворення (схеми Lai-Massey) ефект подвоєння числа S-блоків циклового перетворення, що активізуються. Але тоді для 64-бітного шифру очікуване число активних S-блоків на першому циклі буде рівним 10, а для 128-бітного шифру рівним 18. На другому циклі для 128-бітного шифру додається з урахуванням подвоєння ще 32 активних S-блоки. В результаті шифр IDEA NXT-128 становиться випадковою підстановкою на другому циклі. Якщо вважати, що зазначеного подвоєння не виходить, то для 64-бітного шифру очікуване число активних S-блоків на першому циклі буде рівним 5, а для 128-бітного шифру рівним 9. На другому циклі для 128-бітного шифру додається ще 16 активних S-блоків.

В результаті шифр IDEA NXT-128 зі своїми S-блоками ($DP_{max}^{\pi} = LP_{max}^{\pi} = 2^{-4}$) стає за диференціальними показниками випадковою підстановкою на третьому циклі.

Для перевірки цього припущення далі наводяться результати експериментів, виконаних практично в одних і тих же умовах, по визначенню поциклових значень повних диференціалів для 128-бітових версій шифрів FOX і Rijndael, запозичені з роботи [1]. Вони представлені в таблиці 4.3 і таблиці 4.4.

Таблиця 4.3

Поциклові значення максимумів повних диференціалів для 128-бітної версії шифру FOX (для підрахунку різниць до уваги приймаються окремі 16 біт блоків даних)

Кіль-кість цик-лів	Біти 64..79 шифртекстів		Біти 80..95 шифртекстів		Біти 96..109 шифртекстів		Біти 112..127 шифртекстів	
	Макси-мум ДХ	Кіль-ксть макс.	Макси-мум ДХ	Кіль-кість макс.	Макси мум ДХ	Кіль-кість макс	Макси-мум ДХ	Кіль-кість макси мумів
1	32	1	38	1	32	1	38	1
2	18	10	20	1	20	1	18	11
3	18	14	22	1	20	1	18	10
4	18	10	22	1	18	20	22	1
5	18	10	18	19	20	1	18	16
6	18	15	18	14	18	13	18	15
7	20	1	20	1	20	1	20	2
8	20	1	18	18	20	1	18	17
9	18	13	20	1	18	20	20	2
10	18	12	18	17	20	3	20	1
11	20	1	20	1	20	1	20	1

У першому випадку наводяться результати оцінки максимальних значень повних диференціалів для 128-бітної версії шифру FOX (з усіченням шифрованих блоків (різниць) до 16-бітного розміру). Розглядались різні варіанти вхідних 16-бітних різниць. У другій серії експериментів використовувався шифр Rijndael. У процесі експериментів здійснювалося зашифрування 16-бітних блоків даних на 30 випадково обраних ключах. Потім отримані результати усереднювалися по цій множині ключів (обчислювалися, як визначено в роботі [13], *AMDP* – середні значення максимумів диференціальних ймовірностей, дивись додаток Б).

Таблиця 4.4

Поциклові значення максимумів повних диференціалів при активізації шифру Rijndael 16-бітними блоками різниць

Число Циклів *r*	Значення максимуму повного диференціалу	Середнє-квадратичне відхилення
1	1024	0
2	3652,26	±630,312
3	19,0666	± 1,436
4	19,0666	±0,99777
5	18,8666	±1,23108
6	19,1332	±0,99106
7	19,2666	± 1,0934
8	19,1332	± 1,431394
9	19,0666	± 1,23648
10	19,3333	± 1,2995
11	19.4	± 1,474222
12	18,8666	± 0,991072
13	18,8666	± 0,991072
14	18.9332	± 1,123486

З представлених результатів видно, що великий шифр Rijndael вже з третього циклу шифрування приходить до сталого значення максимуму повного диференціала, що повторює відповідне значення рівне 19, що властиве випадковій підстановки степеня 2^{16}.

Також видно, що це асимптотичне значення практично не залежить від використаних ключів шифрування (середньоквадратичне відхилення не перевищує 1,5). В той самий час шифр FOX у всіх випадках стає випадковою

підстановкою вже на другому циклі (FOX виграє у Rijndael-я за диференціальними показниками один цикл). Це ж випливає і з результатів експериментів по визначенню законів розподілу кількості активних S-блоків на перших циклах зашифрування 128-бітного шифру IDEA NXT (для функції f64), представлених в табл. 4.5.

Таблиця 4.5

Кількість активних S-блоків на перших циклах шифрування при активізації різницею одного байту входу шифру (функції f64))

Число активних S-блоків	1-й цикл	2-й цикл	3-й цикл
0	0	0	0
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	100	0	0
10	0	0	0
11	0	0	0
12	0	0,000784	0,000392
13	0	0,002353	0,003529
14	0	0,270196	0,169412
15	0	7,479216	5,896078
16	0	92,24745	93,93058

128-бітний шифр для 16-бітових блоків вхідних різниць повинен приходити до стану випадкової підстановки за один цикл (5 активних S-блоків першого циклу формують значення диференціальної ймовірності що дорівнює $(2^{-4})^5 = 2^{-20}$ і при подвоєнні числа активних S-блоків. диференціальний індикатор доказової безпеки шифру з 16-бітовим входом істотно перевищує значення $IPS_D = 2^{-12}$).

Це свідчить про те, що зовнішній контур перетворень не володіє цією властивістю.

Дійсно, якщо враховувати зовнішній контур перетворення (схему Lai-Massey), який за припущенням забезпечує подвоєння кількості активних S-блоків циклової функції, то 128-ми бітна версія шифру повинна приходити до стану випадкової підстановки за один цикл.

Проте шифр IDEA NXT можна віднести до числа рішень більш ефективних, ніж шифр Rijndael (для S-блоків цього шифру $DP_{max}^{\pi} = 2^{-4}$ і, отже, $k_{\min} = 30$, для $LP_{max}^{\pi} = 2^{-4}$ відповідно маємо $k_{\min} = 40$ [21; 23]).

Шифр Мухомор [45; 46]. Цей шифр теж використовує зовнішній контур зашифрування у вигляді схеми Lai-Massey.

Наведемо показники активізації S-блоків шифру Мухомор-128. Їх ілюструє таблиця 4.6.

Очевидно, що мінімальне число активних S-блоків виходить мінімум 9, а на другому активні всі 16 S-блоків.

За два цикли становляться активними 24 S-блоки функції ускладнення M-64, і шифр Мухомор приходить до стану випадкової підстановки для S-боків з $DP_{max}^{\pi} = 2^{-4}$ запасом за два цикли.

Наведемо для ілюстрації результати визначення поциклових значень максимумів переходів таблиць повних диференціалів для повної 128-бітної версії шифру Мухомор в режимі його ініціалізації 16-бітними різницями відповідно до методики роботи [10].

Таблиця 4.6

Розподіл мінімального числа активних S-блоків в % на перших циклах шифрування шифру Мухомор (для функції ускладнення М-32)

Число активних S-блоків	1-й цикл	2-й цикл	3-й цикл
0	0	0	0
1		0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	100	0	0
6	0	0	0
7	0	0	0
8	0	100	100

Результати експериментів ілюструє табл. 4.7, запозичена з цієї роботи. Тут наводяться диференціальні показники відразу для трьох шифрів, представлених на український конкурс.

Блоковий шифр з білоруського стандарту. Тут спочатку наводиться короткий опис цього шифру, тому що він є не так давно прийнятим стандартам і має оригінальну конструкцію [47].

Шифр побудований на восьмикратному використанні однієї і тієї ж циклової функції, наведеної на рис. 4.1. У кожному циклі шифру, як випливає з рис. 4.1, використовується 28 S-блоків. Наведемо розшифровку позначень використаних на цьому Рис.4.1 [47].

⊞ – суматор за модулем 2^{32};

⊕–суматор за модулем 2 (XOR);

⊟ – блок обчислення різниць вхідних 32-бітних слів за модулем 2^{32};(u ⊟ v для u, v ∈ $\{0, 1\}^{8n}$ слово w∈$\{0, 1\}^{8n}$ таке, що u = v⊞w;

$<i>_{32}$ позначає представлення числа циклів в двійковому вигляді (в вигляді 32-ух бітного слова);

a, b, c, d– змінні зі значеннями з діапазону $\{0,1\}^{32}$.

Таблиця 4.7

Поциклові значення максимумів переходів таблиць повних диференціалів для повних версій українських шифрів при 16-бітних різницях входу

Число циклів	Калина	ADE	Мухомор
1	19,47	65536	19,13
2	19,0	20	18,8
3	19,13	20	19,4
4	19,2	18	19,13
5	19.27	18	19,07
6	18,87	20	19,6
7	19,47	20	19,27
8	19.2	18	19,13
9	19,0	18	19,13
10	19,33	18	19,276

Перетворення G_r (r = 5,13,21)

Перетворення G_r: $\{0,1\}^{32} \rightarrow \{0,1\}^{32}$ ставить у відповідність 32-х бітному слову на своєму вході $u = u_1||u_2||u_3||u_4$, $u_i \in \{0,1\}^8$ слово $G_r(u)$ = Rot Hi^r((H(u_1) ||H(u_2) | |H(u_3) || H(u_4)) на виході, що відповідно с позначеннями роботи [57] відповідає представленню вхідного 32-х бітного слова в вигляді 4 послідовних байтів, виконанню над кожним байтом операції нелінійного

перетворення (підстановки) H і подальшого циклічного зміщення (конкатенації) байтів з виходів підстановок на r = 5, 13 або 21 біт наліво.

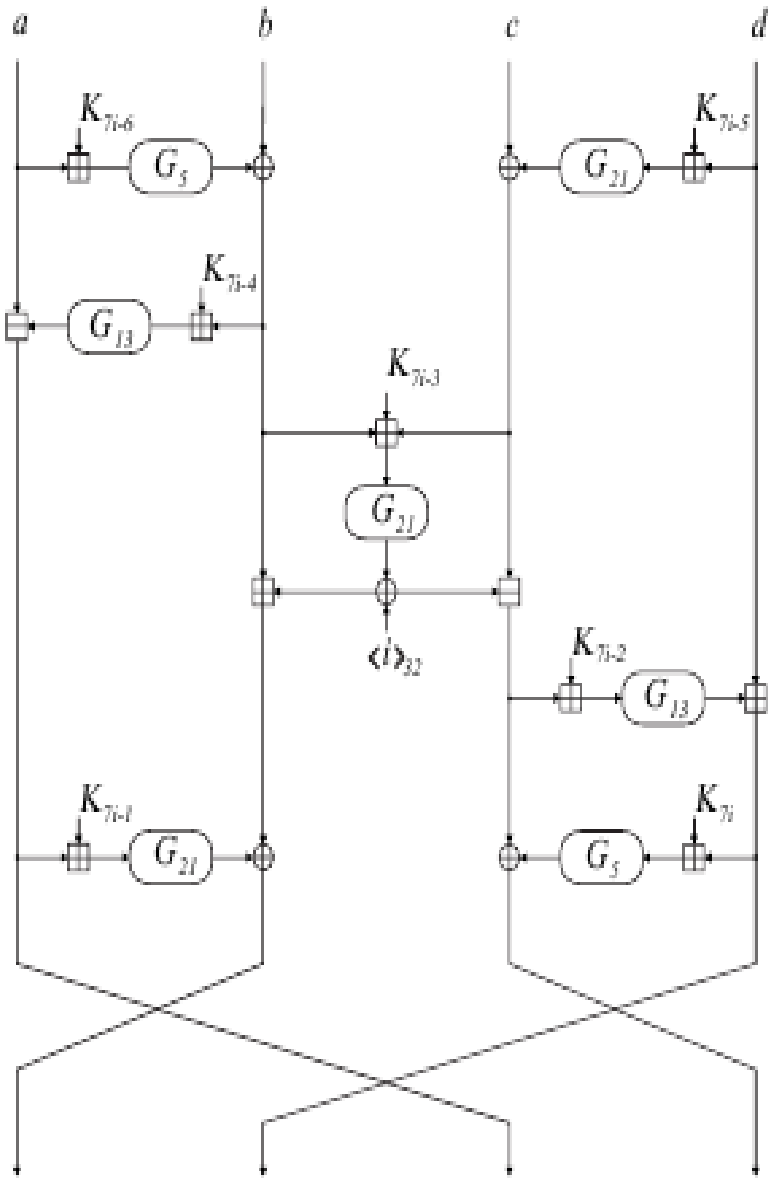

Рис. 4.1 Обчислення на і-му циклі зашифрування

Вхідними даними алгоритмів зашифрування і розшифрування є вхідні 128-бітні блоки даних $X \in \{0,1\}^{128}$ і 128-ми бітний, 192-бітний або 256-бітний ключі.

Число активних S-блоків на відповідних циклах при активізації одного байту входу білоруського шифру представлено в таблиці 4.8.

Це означає, що на двох циклах при 31 активному S-блоці білоруський шифр стає випадковою підстановкою при будь-яких (випадкових) S-блоках

[17]. У всіх експериментах використовувалися випадкові циклові підключи.

Таблиця 4.8

Число активних S-блоків на відповідних циклах при активізації одного байту входу білоруського шифру

Число актив-них S-блоків	Число ненульових однобайтових різниць в %, що приходяться на 65025 пар текстів				
	Ключ: 467e18547e73341f2a2e553b7516187233c667063d402b8fad936c53c551b9e			Ключ:270b40f162313b061e777f457caf216227221a4b53c24df8d3220e620d3225d	
	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл
6	0,000000	0,000000	0,000000	0,000000	0,000000
7	0,002745	0,000000	0,000000	0,001569	0,000000
8	0,017647	0,000000	0,000000	0,030980	0,000000
9	0,190588	0,000000	0,000000	0,221569	0,000000
10	1,014510	0,000000	0,000000	1,223922	0,000000
11	0,485098	0,000000	0,000000	0,592941	0,000000
12	1,776078	0,000000	0,000000	2,171765	0,000000
13	9,105098	0,000000	0,000000	10,983529	0,000000
14	8,710196	0,000000	0,000000	10,402745	0,000000
15	3,964706	0,000000	0,000000	4,513333	0,000000
16	53,669804	0,000000	0,000000	63,663529	0,000000
17	4,491765	0,000000	0,000000	3,099216	0,000000
18	1,077647	0,000000	0,000000	0,182745	0,000000
19	15,494118	0,000000	0,000000	2,912157	0,000000
20	0,000000	0,000000	0,000000	0,000000	0,000000
21	0,000000	0,000000	0,000000	0,000000	0,000000
22	0,000000	0,000000	0,000000	0,000000	0,000000
23	0,000000	0,000000	0,000000	0,000000	0,000000
24	0,000000	0,000000	0,000392	0,000000	0,000392
25	0,000000	0,018431	0,021961	0,000000	0,020784
26	0,000000	0,472549	0,503922	0,000000	0,522745
27	0,000000	9,610980	9,993333	0,000000	10,259216
28	0,000000	90,289412	89,871765	0,000000	89,587843

Шифр Калина-2. У табл. 4.9 представлена картина активізації S-блоків трьох перших циклів шифру Калина-2 [48].

Таблиця 4.9

Розподіл числа активних S-блоків на перших циклах (в %) при активізації одного байту входу шифру Калина-2

Число активних S-блоків	Число ненульових однобайтових різниць у процентах			
	1-й цикл	2-й цикл	3-й цикл, Key 1	3-й цикл, Key 2
0	0	0	0	0
1	100	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	100	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0,000392
13	0	0	0,002745	0,005490
14	0	0	0,183137	0,169020
15	0	0	5,818431	5,936078
16	0	0	93,995686	93,88902

Розглядалися ненульові різниці для самого лівого і самого правого байтів вхідного блоку даних.

І в цьому випадку використовувалися випадково згенеровані циклові підключи.

Результати для самого лівого і самого правого байту вхідного блоку даних вийшли ідентичними.

Представлені результати свідчать, що шифр Калина-2 стає випадковою підстановкою після трьох циклів (за диференціальними і за лінійними показниками), тобто за динамічними показниками шифр Калина-2 має дещо вищі показники, ніж шифр Rijndael (за три цикли активізується мінімум 24-ри S-блоки).

Відзначимо далі, що, як уже зазначалося вище, в ході розробки нової методики оцінки стійкості. блокових симетричних шифрів, був введений додатковий показник ефективності шифруючих перетворень у вигляді кількості циклів, потрібних для приходу шифру до стану випадкової, підстановки [17].

Той шифр вважається більш досконалим, для якого кількість циклів приходу до стану випадкової підстановки виявляється меншим.)

Camellia [112]. Camellia–це наступне покоління 128-бітного блокового криптографічного алгоритму, розробленого в Японії фахівцями телеграфній і телефонній Корпорації Nippon і електричної Корпорації Mitsubishi, який підтримує три розміри ключів: l_k = 128, 192 і 256 біт.

На Рис. 4.2 приведена конструкція F-функції, яка визначає перетворення на перших циклах шифру Camellia.

Блоковий симетричний алгоритм Camellia був розроблений не тільки як високо захищений криптографічний шифр, але також як алгоритм, що легко переноситься на різні апаратні платформи.

Наведемо показники активізації S-блоків перших циклів шифру Camelia, прийнятого як стандарт в Японії.

В табл. 4.10 приводиться розподіл числа активних S-блоків на перших циклах шифрування при активізації одного байту входу шифру Camellia.

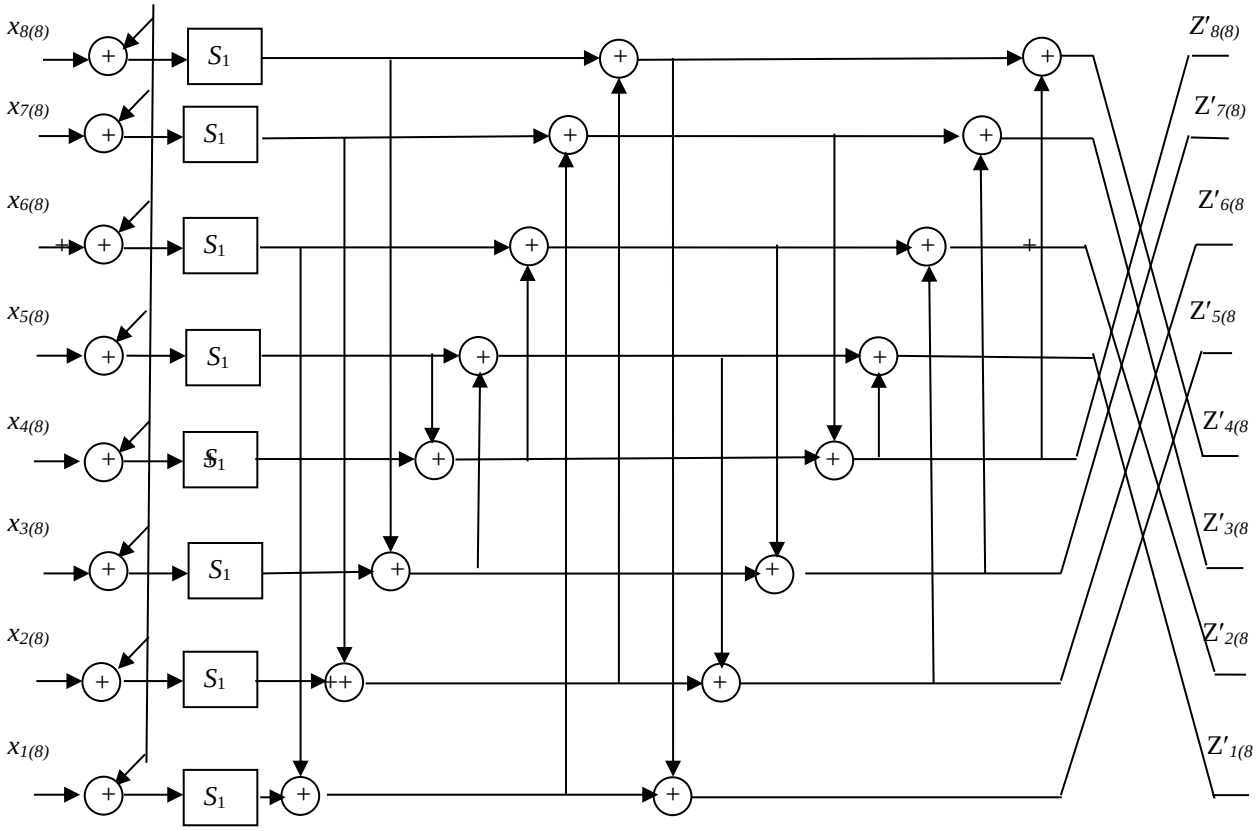

Рис. 4.2 *F*- функція шифру Camellia

Представлені результати дозволяють зробити висновок, що шифр Camellia стає випадковою підстановкою на четвертому циклі (DP^{π}_{max}= 2^{-6}).

Таким чином, за показниками випадковості цей шифр поступається шифру Rijndael на один цикл.

У підсумку, до найбільш прогресивних з розглянутих вище конструкцій слід віднести шифри Мухомор і Калину-2, а також шифр з білоруського стандарту.

Ці шифри реалізують показники приходу до стану випадкової підстановки близькі до граничних.

Serpent [113]. У цьому 128-ми бітному шифрі циклова функція будується з допомогою напівбайтових S-блоків (золотих S-блоків [106]). для таких S-блоків DP^{π}_{max}= 2^{-2}, і, отже, $k_{\min}$, = 60.

Таблиця 4.10

Кількість активних S-блоків на відповідних циклах при активізації одного байту входу шифру Camellia

Число активн. S-блоків	Число ненульових однобайтових різниць в %, що приходяться на 65025 пар текстів					
	Ключ: 469c57096730bd15fd71a975c503dee469c57096730bd15fd71a975c503dee			Ключ: 46e148be3fdf41c22df55cb45ba14dcd46e148be3fdf41c22df55cb45ba14dcd		
	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл
1	100	0	0	100	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	100	0,004706	0	100	0,003137
6	0	0	0,024706	0	0	0,029804
7	0	0	3,071765	0	0	3,081176
8	0	0	96,898824	0	0	96,885882

У табл. 4.11 наводиться розподіл активних S-блоків на перших трьох циклах шифрування для цього шифру.

З наведених результатів випливає, що шифр Serpent стає випадковою підстановкою після 4 і більше циклів.

У підсумку, до найбільш прогресивних з розглянутих вище конструкцій слід віднести шифри Мухомор і Калину-2, а також шифр з білоруського стандарту.

Ці шифри реалізують показники приходу до стану випадкової підстановки близькі до граничних.

Таблиця 4. 11

Частка активних S-блоків в% на відповідних циклах при активізації одного байту входу шифру Serpent

Число активних S-блоків	Число ненульових повторень активізації в %, що приходяться на 65025 пар текстів		
	1-й цикл	2-й цикл	3-й цикл
1	5.490196	0	0
2	16.47058	0	0
3	27.45098	0	0
4	27.45098	0	0
5	16.47058	0	0
6	5.490196	0.1952941	0
7	0.784313	0.683921	0
8		0.1952941	0
9	0	0.6894117	0
10	0	1.0545098	0
11	0	1.0996078	0
12	0	1.1458823	0
13	0	1.2576470	0
14	0	2.9360784	0
15	0	3.5913725	0
16	0	6.3505882	0
17	0	7.0235294	0
18	0	9.0090196	0.00313725
19	0	10.6764705	0.00941176
20	0	11.1760784	0.05411764
21	0	12.0721568	0.18078431

Продвження таблиці 4. 11

Число активних S-блоків	Число ненульових повторень активізації в %, що приходяться на 65025 пар текстів		
	1-й цикл	2-й цикл	3-й цикл
22	0	12.2772549	0.76941176
23	0	9.17450980	2.39960784
24	0	5.70313725	7.14745098
25	0	2.79411765	16.35411764
26	0	0.79450980	27.37098039
27	0	0.09960784	29.83411764
28	0	0	15.87686274

4.4 Аналіз результатів експериментальних досліджень

Отримані результати свідчать про те, що конструкції перших циклових перетворень блокових симетричних шифрів грають важливу роль в забезпеченні динамічних показників приходу шифрів до стану випадкової підстановки, і істотно впливають на значення числа циклів, необхідних для забезпечення запасу їх стійкості. Всі розглянуті (відомі) конструкції сучасних блокових симетричних шифрів, за винятком шифрів IDEA NXT (FOX), Калина, Мухомор і білоруського шифру, забезпечують динамічні показники приходу до стану випадкової підстановки, що перевищують три-чотири цикли.

Шифр Rijndael виявляється далеко не в лідерах щодо даного показника (для приходу до стану випадкової підстановки йому необхідно 4-ри цикли).

До найбільш прогресивних рішень з побудови блокових симетричних шифрів можна віднести шифри Калина-2, білоруський шифр і шифр Мухомор.

У цих шифрів за рахунок активізації одним байтом входу відразу декількох S-блоків циклової функції першого циклу забезпечується збільшене в

порівнянні з іншими шифрами мінімальне число S-блоків, що активізуються на перших циклах.

Криптографічні властивості таких шифрів практично не залежать від диференціальних і лінійних властивостей використаних S-блоків.

А це означає, що в цих шифрах можуть застосовуватися без будь-яких обмежень довільні S-блоки, породжені генератором випадкових підстановок. Для таких шифрів задача пошуку S-блоків з покращеними криптографічними показниками, якій приділяється велика увага в публікаціях з криптографічної тематиці, втрачає будь-який сенс.

Висновки до розділу 4

Запропоновані в роботах [17; 18; 109] обчислювальний, і доповнений в цій роботі експериментальний методи визначення динамічних показників приходу блокових симетричних шифрів до стану випадкової підстановки дозволяють для повномасштабних шифрів оцінити мінімальне число циклів шифрування, після яких шифри приходять до стану випадкової підстановки.

В результаті відкривається додаткова можливість порівняння по ефективності шифрів між собою. У той же час знання показників приходу шифрів до стану випадкової підстановки дозволяє обґрунтовано підійти до визначення кількості циклів зашифрування, що забезпечують необхідний запас стійкості шифрів.

Як показала практика, цей запас вибирається так, що він в три-чотири рази перевищує число циклів шифрування, необхідне для приходу шифру до стану випадкової підстановки.

У розділі вирішена задача уточнення і підтвердження за допомогою обчислювальних експериментів ефективності нової методики оцінки динамічних показників приходу блокових симетричних шифрів до стану випадкової підстановки.

Наукова новизна результатів полягає в тому, що вперше отримані обґрунтовані об’єктивні дані для значень кількості циклів приходу до стану випадкової підстановки ряду сучасних шифрів.

Практична значимість запропонованої методики і представлених результатів бачиться в їх конструктивізмі. Вони дозволяють виконати обґрунтування мінімального числа циклів шифруючих перетворень, які забезпечують досягнення граничного рівня їх стійкості.

Перспективи подальших досліджень бачаться в розробці додаткових удосконалень вже наявних конструкцій шифрів в напрямку поліпшення їх динамічних показників приходу до випадкової підстановки,

Наукові результати цього розділу підкріплюються опублікованими роботами [17; 18; 21; 109].

РОЗДІЛ 5

УДОСКОНАЛЕННЯ МЕТОДІВ ПРОЄКТУВАННЯ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ З ПІДВИЩЕНОЮ СТІЙКІСТЮ І ШВИДКОДІЄЮ

Як уже відзначено в першому розділі, в даній роботі поставлена основна задача, яка полягає в розробці більш перспективних рішень із побудови блокових симетричних шифрів, орієнтованих на застосування в постквантовий період розвитку криптографії.

Ці можливості враховані в запропонованому удосконаленому підході в проєктуванні блокових симетричних шифрів, що будується на ряді висунутих положень. Її реалізація демонструється далі на прикладах декількох нових шифрів, побудованих на основі запропонованих трьох методів, орієнтованих на розробку і використання нових конструкцій першого циклу шифрування. Запропоновані конструкції шифрів по простоті і прозорості рішень, а також за показниками доказової стійкості до атак диференціального і лінійного криптоаналізу і за показниками продуктивності не поступаються визнаному лідеру технологій блокового симетричного шифрування шифру Rijndael (AES), а по динаміці приходу шифрів до стану випадкової підстановки вони перевершують практично всі відомі рішення.

5.1 Сутність вдосконалення методів прєктування БСШ

Підхід, про який йде мова далі, будується на деяких нових (свіжих) ідеях, що дозволяють його трактувати як розробку удосконалених методів проєктування БСШ. Проведені до цього часу результати досліджень [1; 6; 16; 17; 109] та інші дозволяють сформулювати вихідні положення розвинутого підходу у вигляді наступних положень.

Наводимо вже уточнену в процесі виконання цієї роботи редакцію матеріалу з роботи [22]:

1. Всі сучасні ітеративні шифри незалежно від використаних в них S-блоків (підстановлювальних перетворень) на повноцикловій довжині за комбінаторними, а також за диференціальними і лінійними показниками (за значеннями максимумів диференціальних та лінійних ймовірностей) стають випадковими підстановками. Підстановлювальні перетворення впливають лише на динаміку (кількість циклів) приходу шифру до стану випадкової підстановки.

2. Динамічні показники шифру визначаються мінімальною кількістю активованих S-блоків, що припадають на перші цикли перетворень, які дозволяють шифру прийти до стану випадкової підстановки, при цьому мінімальне число активізованих S-блоків першого циклу для відомих конструкцій блокових симетричних шифрів (шифрів з одношаровими підстановлювальними перетвореннями) дорівнює одному. Лінійні перетворення, що будуються на основі МДВ перетворень, не забезпечують активізацію всіх S-блоків другого і третього циклів.

3. Для покращення показників випадковості шифруючих перетворень їх потрібно будувати так, щоб вони забезпечували активізацію як можна більшої кількості S-блоків перших циклів, що активізуються одним байтом входу.

4. Одним з можливих шляхів збільшення кількості S-блоків першого циклу, що активізуються однобайтовою різницею входу, є побудування першого циклу з двошаровим підстановлювальним перетворенням. Шифр з двошаровим підстановлювальним перетворенням на першому циклі дозволяє 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. Наступні цикли можуть бути побудовані з використанням стандартних (відомих) методів.

5. Гранична кількість розгалужень (коли один S-блок активізує всі наступні S-блоки циклу) може бути реалізована на основі конструкції циклового перетворення, в якій забезпечується принцип послідовної активізації S-блоків циклової функції, включених в ланцюжок один за іншим.

При цьому необхідно створити умови, коли забезпечується активізація ланцюжка з самого його початку. Ця конструкція циклового перетворення дозволяє реалізувати активізацію збільшеної (більше ніж два) кількості S-блоків першого циклу, чого не дозволяє жодне з відомих рішень.

6. Збільшення мінімальної кількості S-блоків, що активізуються на перших циклах є ефективним засобом забезпечення незалежності шифруючих перетворень від властивостей використаних S-блоків. Це шлях побудування шифрів, в яких без зниження криптографічної стійкості можна застосовувати S-блоки випадкового типу (практично без попереднього відбору).

7. Схеми розгортання ключів може бути побудовані з використанням суттєво спрощених підходів ніж у відомих конструкціях сучасних шифрів. Основна вимога до схем розгортання ключів – відсутність самоподібності в послідовності циклових підключів.

8. Паралельна обробка даних може бути забезпечена внаслідок побудування циклових функції з відсутністю операції, що покривають усі байти вхідного блоку даних.

Далі ставиться задача побудувати циклове перетворення шифру, що дозволяє активізувати відразу всі (майже всі) S-блоки другого і наступних циклів і збільшену кількість S-блоків першого циклу.Така можливість вже відзначалася в роботі [17] і в попередньому розділі для перетворень M-64, M-128, M-256 шифру Мухомор. У цій роботі, розвиваючи ідеї побудови функції ускладнення M-256, а для постквантовій криптографії будуть цікавими 256-бітні шифри і шифри з більшими довжинами шифрованих блоків і ключів, можна обґрунтувати новий підхід більш докладно.

Основою розв’язання поставленої задачі є побудова перетворення, яке реалізується на основі скоріше не паралельної, а послідовної активізації S-блоків циклового перетворення з одночасним забезпеченням взаємозв'язку між сусідніми S-блоками. Кожен поточний S-блок повинен залежати від результатів активізації попередніх S-блоків. Подальший матеріал ґрунтується на публікації [22].

5.2 Удосконалений БСШ з керованими підстановками ШУП-1

Звернемося до ідеї використання при побудові циклової функції блокового симетричного шифру принципів управління за допомогою поточних даних в процесі виконання підстановлювальних перетворень. Мається на увазі патент, підготований у свій час Долговим В. І., Лисицькою І. В. та Супранюком С. В. [114]. Тоді цей принцип побудови циклової функції був названий недетермінованим криптографічним перетворенням. Слід відразу зазначити, що запропоноване тоді рішення виявилося далеко не досконалим. Подальшим розвитком відмічених принципів стала чергова пропозиція, підготована з участю проф. Долгова В. І., що була реалізована в шифрі Мухомор [45], представленого на український конкурс. В цій розробці вдалося на основі введення в процеси формування входів в S-блоки додаткових зворотних зв’язків з виходами інших S-блоків усунути слабкості попередніх розробок. Цей шифр пройшов експертизу авторитетних фахівців і був визнаний одним з лідерів сучасних алгоритмів шифрування.

Розвинений в [45] підхід у своїй основі був орієнтований на використанні двоетапного принципу формування циклової функції. На верхньому (зовнішньому) рівні перетворення використовувалася відома схема Lai-Massey [43], а динамічне управління підстановлювальними перетвореннями виконувалося на нижньому рівні у схемах ускладнення. Тоді розробники порахували таку двоетапну процедуру перемішування бітів даних більш ефективною з точки зору забезпечення високого рівня криптографічної стійкості шифру. Проведені до сьогоднішнього дня дослідження [17] та інші, однак, показали, що введений зовнішній рівень перемішування циклової функції виявився зайвим. Прихід шифру до випадкової підстановки за два цикли можна реалізувати й без зовнішнього рівня перемішування циклової функції (схеми Lai-Massey). Циклове перетворення нижнього рівня виявляється цілком самодостатнім для реалізації граничних показників динаміки приходу шифру до стану випадкової підстановки. Крім того, сама функція ускладнення сьогодні представляється вже кілька обтяженою через

те, що деякі перетворення вийшли дублюючими одне одного (надлишковими) і до того ж складними для математичного аналізу. Тут маються на увазі зв'язки через додавання за модулем 2 поточних виходів SL перетворень [45] з попередніми і наступними лінійками вхідних блоків даних. Загалом, і тут зберігає актуальність задача знаходження розумного компромісу між стійкістю і швидкодією.

У підсумку в цій роботі пропонується шифр, який використовує у своїй конструкції принципи побудови нижнього рівня шифру Мухомор [45], з якого збережена тільки ідея управління поточними значеннями входів SL перетворень значеннями виходів попередніх SL перетворень. Тут SL перетвореннями названі “цеглинки”, що складають циклову функцію. Це четвірки S-блоків з наступним множенням виходів S-блоків на матриці МДВ кодів розміром 4×4 (операції аналогічні операціям ByteSub і MixColumn шифру Rijndael). Управління реалізується за допомогою додаткового додавання за модулем 2 поточних 32-бітних вхідних блоків даних з попередніми результатами виконання нелінійних перетворень (SL перетворень). За прийнятою в літературі класифікацією це SPN шифр. Перша запропонована конструкція названа «Шифром с управляемыми подстановками 1-ой версии» (ШУП-1) [22].

При розробці цього рішення в основу були покладені наступні критерії (тут внесено корекцію в формулювання роботи [22], що враховує останні отримані результати):

1) Довжина блоку, що шифрується і майстра-ключа повинна бути не менше ніж 256 бітів (шифр повинен бути орієнтований на постквантовий період його використання);

2) Шифр повинен приходити до стану випадкової підстановки максимум за три цикли, при цьому він повинен володіти запасом за кількостю активізуємих S-блоків на перших циклах, щоб дозволити без втрати стійкості застосовувати випадкові S-блоки

3) Конструкція циклової функції повинна певною мірою бути простою і прозорою.

4) Обчислювальна складність виконання операцій шифрування і розшифрування повинна бути вище ніж у відомих конструкцій шифрів з таким же розміром бітового входу;

5) Шифр повинен допускати паралельну обробку даних;

6) Схема розгортання ключів повинна бути простою і швидкодіючою. Основна вимога для цієї схеми відсутність самоподібності циклових підключів.

Логічно було б відразу піти по шляху застосування функції ускладнення М-256, використаної в шифрі Мухомор,

Короткий опис шифру Мухомор наведений у Додатку Г.

Дійсно, якщо повторювати циклову функцію ускладнення шифру Мухомор М-256, то треба було б її будувати з двома шарами SL перетворень (конструкція основної цеглинки циклової функції шифру Мухомор– SL перетворення теж наведена у Додатку Г).

Було б отримано шифр з керованими підстановками, який приходив би до випадкової підстановки за два цикли (в шифрі Мухомор в першому циклі використовується два шари SL перетворень. При цьому активізується мінімум 33 S-блоки (одне SL перетворення у першому шарі і 8 SL перетворень у другому). Але аж надто така конструкція схожа на шифр з подвоєною кількістю циклових перетворень. Ефекту збільшення кількості активних S-блоків першого циклу можна було б домогтися і в шифрі AES, якщо його двоциклову конструкцію переформатувати в одноциклову. Тому, щоб обійти можливі критичні зауваження, що можуть стосуватися неоригінальності конструкції, спочатку представляється версія шифру, яка повторює класичний підхід до побудови циклових функцій SPN шифрів (в кожному циклі буде використовуватися один шар SL перетворень). Основна перевага цієї конструкції буде полягати в тому, що на відміну від шифру AES-256 вона буде приходити до стану випадкової підстановки за три цикли замість чотирьох-

п’яти.Це відбувається завдяки тому, що в циклах, починаючи з другого, в шифрі будуть активізуватися по можливості всі S-блоки циклових функцій. Підкреслимо тут, що залишається можливість побудувати перетворення першого циклу з двома шарами SL перетворень, що відкриває, як буде видно з подальшого, можливість побудування шифру, який стає випадковою підстановкою вже на другому циклі.

Далі представляється опис однієї з перших розробок - шифру з керованими підстановками (ШУП-1) [22]. Він виконаний у традиційній манері викладу матеріалу, як це свого часу було зроблено при описі шифру «Мухомор» та інших українських шифрів [55].

5.2.1 Опис конструкції удосконаленого шифру ШУП-1

При викладенні матеріалу використовувався опис шифру Мухомор [55], що став у певній мірі прототипом пропозиції. Потрібно було з нього виділити частину, пов’язану з описом функції ускладнення М-256, як основу для побудування циклової функції ШУП-а.

Параметри алгоритму. Алгоритм шифрування ШУП-1 підтримує довжину вхідного блоку даних 256 бітів і ключів шифрування довжиною 256 і 512 бітів.

Процедура шифрування. На вхід процедури подається відкритий текст і підключи шифрування. Вхідний блок даних проходить початкову рандомізацію, потім задану кількість разів (вісім разів) обробляється цикловою функцією, і в завершення проводиться фінальна рандомізація за допомогою операції XOR з додатковим десятим цикловим підключем. Отриманий в результаті блок даних є шифртекстом.

Циклове перетворення. Конструкція циклового перетворення шифру надмірно не ускладнена, вважаючи, що рішення з побудови шифру має володіти певною елегантністю і простотою. Тому при побудові циклової функції ШУП-1 з базової конструкції шифру Мухомор виключили другий шар SL перетворень, а також ряд додавань результатів. проходження SL перетворень з подальшими й попередніми блоками даних. Вони дублювали

операції, що реалізуються послідовністю SL перетворень. Крім того, ці ланцюги ускладнювали сам аналіз процесів активізації S-блоків. Збережено лише додавання за модулем 2 виходу останнього в поточному шарі SL перетворення з виходами всіх попередніх SL перетворень. Цим забезпечується при формуванні виходу циклової функції ефект проходження кожним байтом входу всіх SL перетворень (отримується на наступному циклі максимально можлива кількість активних S-блоків) для кожної четвірки байтів входу. Особливу увагу приділено конструкції першого циклу. Була поставлена задача побудувати його так, щоб була забезпечена активізація вхідними блоками даних (колонками) одночасно і збалансовано по можливості всіх S-блоків другого циклу. В результаті як циклове перетворення використовується дещо змінена функція ускладнення M-256 шифру Мухомор. Крім виключення ряду додавань виходів SL перетворень з подальшими і попередніми результатами проходження SL перетворень перший цикл ШУП-1 фактично включає тільки верхню половину перетворення функції ускладнення M-256. Крім зазначених вище винятків ряду підсумовувань для забезпечення активізації будь-яким 32-бітовим словом (сегментом) входу першого SL перетворення в лінійці динамічно керованих переходів інших SL перетворень, в першому циклі після операції складання з цикловими підключами (за модулем 2^{32}) перед входом в перше SL перетворення вводиться додаткове складання за модулем 2 (XOR) всіх 4-байтових сегментів вхідних блоків даних на вході першого SL перетворення. Ця операція має сенс тільки для обраного способу запуску SL перетворень, де SL перетворення включені в ланцюжок з послідовним запуском один одного. Для інших (відомих) конструкцій шифрів ця процедура не має сенсу, тому що в інших шифрах S-блоки в циклову функцію входять незалежно один від одного або незалежними групами.

Схема першого циклового перетворення ШУП-1 гранично проста і наведена на Рис. 5.1.

При такій схемі запуску SL перетворень виходить, що фактично як укрупненні S-блоки (SL перетворень) виступають латинські квадрати [116].

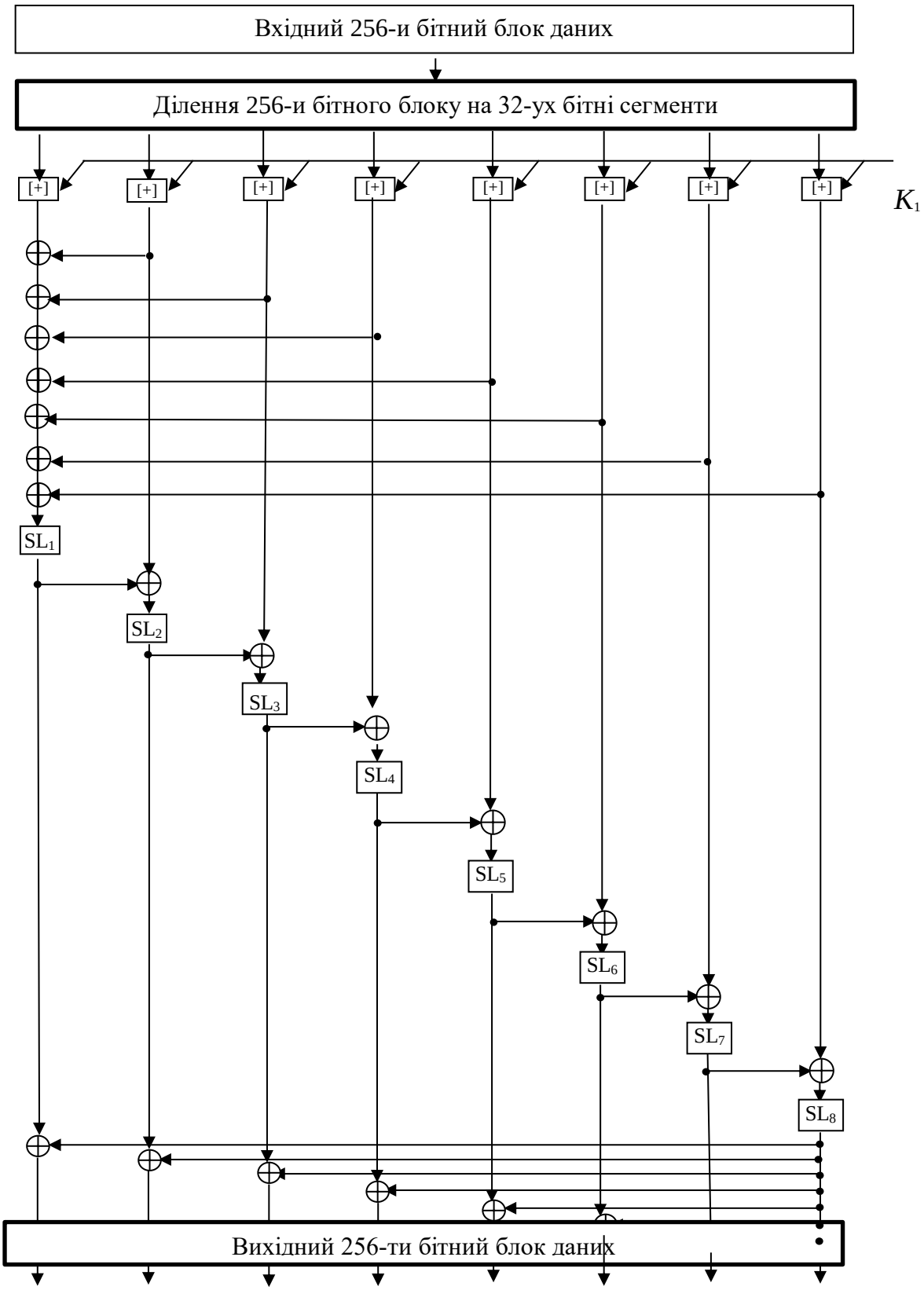

Рис. 5.1 Структурна схема першого циклу ШУП-1

Якщо вважати, що SL перетворення є підстановкою, то рядками латинського квадрата виступають циклічні зрушення другого рядка матриці

вихідної 4-байтової підстановки. Тобто замість однієї вихідної підстановки використовується 2^{32} різних підстановок (рядків латинського квадрата).

При цьому рядок (стовпець) входу в латинський квадрат задається виходом попереднього SL перетворення, а стовпець (рядок) підстановки задається її первинним входом в цикл.

Решта 7 циклів будуються без складань за модулем два на вході першого. SL перетворення і без складань за модулем 2 виходу останнього SL перетворення з виходами інших SL перетворень, крім першого. Після цього виконується складання за модулем 2 виходу останнього SL перетворення з виходом першого.

Далі виконується складання за модулем 2 виходу останнього SL перетворення восьмого циклу з виходами інших SL перетворень цього циклу і здійснюється остаточне складання результату з останнім цикловим підключем за модулем 2.

Конструкція основної "цеглинки" циклової функції, яка використана у шифрі – SL перетворення шифру Мухомор, наведена при описі цього шифру у Додатку Г.

Процедура розшифрування

Алгоритм розшифрування є зворотним до алгоритму шифрування. Навхід алгоритму подаються блоки зашифрованого тексту і підключи розшифрування. На самому початку процедури розшифрування здійснюється зняття фінальної рандомізації шифртексту, після чого отриманий блок даних необхідне число раз (вісім) в зворотному порядку обробляється цикловими функціями.

Отриманий блок даних є блоком відкритого тексту. Залишається відзначити, що при розшифруванні:

- у зворотному порядку також подаються підключи розшифрування;
- як підстановки використовуються інверсні S-блоки;

- в лінійному перетворенні використовується матриця, обернена застосованій при зашифруванні.

Процедура розгортання ключів.

У шифрі Мухомор використовується складна схема розгортання майстер ключа. У нашому шифрі ми хочемо скористатися більш простим рішенням – патент [117]. При його формуванні забезпечена відсутність періодичності в побудові циклових підключів. Використовується майстер ключ, в якому відсутнє повторення байтів (підстановка).

Сама процедура розгортання майстер ключа включає його поділ на окремі байти з наступним виконанням циклічного зміщення майстер ключа на величину, що задається значеннями суміжних (сусідніх) байтів. Ці байти і використовуються як чергові підключи.

В цьому випадку для формування всього набору циклових підключів потрібно десять послідовних байтів. Вибір байтів для розгортання ключів може стати додатковим секретним параметром шифру (варіантів вибору байтів).

Для ключа довжиною 512 біт значенням байту можна задавати кількість біт, що відкидаються від майстер ключа. Поточний підключ визначається 256 бітами, що йдуть після відкинутих (в цьому випадку).

Головною перевагою цієї схеми розгортання ключів є підвищена стійкість до атак на ключовий розклад.

Дійсно при запропонованому способі побудування циклових підключів практично виключається можливість знайти хоч який-небудь детермінований зв’язок між цикловими підключами.

5.2.2 Ефективність перетворення

Далі наводяться результати експериментів по оцінці ефективності пропонованого рішення.

У табл. 5.1 представлені результати обчислювального експерименту по визначенню закону розподілу числа S-блоків, що активізуються на першому циклі при активізації одного байту входу в %.

Таблиця 5.1

Закон розподілу числа активізуємих S-блоків першого циклу

Кількість активних S-блоків	Доля від загального числа переходів
0	0,0039
1	0
...	...
27	0
28	0,0000057
29	0,000279
30	0,0070
31	0,1094
32	0,879

Обчислення кількості S-блоків, що активізуються проводився для кожного з 32 байтів вхідних різниць. При цьому для кожної різниці з множини 2^8 бітових сегментів перебиралися всі можливі пари. Разом сума другої колонки (кількість повторень) в таблиці дорівнює $2^{21} = 2097152$. Нулів вийшло 8192 (це при нульових вхідних різницях). Як випливає з представлених результатів, на першому циклі з великою ймовірністю активізуються всі 32 S-блоки. Такою ефективністю перемішування не володіє жоден з відомих 256-бітних шифрів.

Зауважимо, що як виявилося в подальших дослідженнях, запропонована схема додатного змішування сегментів вхідного блоку даних на вході першого SL перетворення не виключила можливості активізації у першому циклі одного S-блоку. Така можливість може бути реалізована коли будуть мати ненульові однакові різниці перший і восьмий сегменти на вході першого та останнього SL перетворення. В той час як усі інші різниці сегментів входу будуть нульовими.

Усього можливо для 4 байтових SL перетворень 255×4 = 1020 таких варіантів на 2^{64} двобайтових входів у два SL перетворення. Отже, мінімальна кількість S-блоків, що активізуються на перших двох циклах, близька до 33. Зауважимо, що без складання сегментів на вході першого SL перетворення ці 1020 варіантів приходилися б на 2^{32} входів в останнє SL перетворення. Отже, мінімальне число S-блоків, що активізується на першому циклі в нашій конструкції залишається рівним одному, а 32 S-блоки активізується вже на другому циклі.

5.2.3 Результати оцінки показників випадковості ШУП-1

У цьому розділі наводяться результати оцінки очікуваних параметрів приходу ШУП-1 до стану випадкової підстановки.

Відповідно до ідеї підходу, що розвивається в роботах [17; 109], необхідно виконати оцінку мінімального числа активних (залучених S-блоків), після проходження яких, шифр стає випадковою підстановкою. Це мінімальне число визначається диференціальними та лінійними показниками самих S-блоків, що застосовуються в шифрі, конструкціями та властивостями його циклових перетворень, а також значеннями показників доказової стійкості шифру. Останні залежать від розміру його бітового входу. В роботі [17] цей зв'язок між зазначеними показниками визначений у вигляді двох співвідношень:

$$\text{IPS}_D = (DP^{\pi}_{max})^k, IPS_L = 2^{k-1} \cdot (LP^{\pi}_{max}()^k), \qquad (5.1)$$

де DP^{π}_{max} і LP^{π}_{max}— максимальні значення диференціальної і лінійної ймовірностей підстановлювального перетворення $\pi(x)$. IPS_D. (Differential Indicator of Provable Security) — диференційний показник доказової безпеки і IPS_L (Linear Indicator of Provable Security) – лінійний показник доказової безпеки, $k = k_{min}$– мінімальне число активних S-блоків, що беруть участь у формуванні переходу шифру до випадкової підстановки. Ці співвідношення вже наводилися раніше див вирази (4.1), (4.2). Отже, для розрахунків потрібно мати значення IPS_D. і IPS_L.

Скористуємося тут методикою розрахунків з роботи [18]. Розрахунки дозволяють прийти до висновку, що для приходу шифру до стану випадкової підстановки очікуване значення максимуму числа диференціальних переходів для шифру з 256-бітовим входом виявляється близьким до 190, а очікуване значення максимуму зміщення лінійного корпусу для шифру з 256-бітовим входом виявляється близьким до 2^{130}. Відповідно отримуємо, що максимальні значення лінійної і диференціальної ймовірностей для шифру з 256-бітовим входом виходять близькими одна до одної й рівними приблизно $IPS_D \approx IPS_L = 2^{-248} \div 2^{-250}$.

Виходячи з наведених вище співвідношень можна зробити висновок, що для шифру з 256-бітовим входом для приходу до стану випадкової підстановки за диференціальними показниками при використанні S-блоків з граничними показниками δ-рівномірності рівними $DP^{\pi}_{max} = 2^{-6}$ (відповідно до рівності $2^{-248} = (2^{-6})^k$ буде потрібно $k_{\min} = 41$ S-блок.

Аналогічно, для приходу до стану випадкової підстановки за лінійними показниками при використанні S-блоків з граничними показниками нелінійності рівними $LP^{\pi}_{max} = 2^{-6}$ потрібно $(2^{-250} = 2^{k-1} \cdot (2^{-6})^k)$ $k_{\min} = 50$ S-блоків (для S-блоків шифру Мухомор з показниками нелінійності $LP^{\pi}_{max} = 2^{-5}$ для всіх переходів маємо в цьому випадку $k_{\min} = 62{,}25$).

Відповідно до структури циклового перетворення ШУП-1 (рис. 5.1) на першому циклі слід очікувати активізацію мінімум одного найправішого S-блоку, що призводить до активізації 4 байтів виходу останнього SL перетворення. Тому внаслідок складання виходів усіх SL перетворень на виході першого циклу активізуються майже всі 32 S-блоки другого циклу.

Це означає, що в кращому випадку активізується 32 S-блоки, крім можливих одного-двох переходів МДВ перетворень в один-два або три активних байти з ймовірністю меншою ніж 2^{-59}. У гіршому випадку це буде 29 або 31 S-блок.

Потім на третьому циклі вхідні блоки даних проходять також майже через всі 32 S-блоки. В результаті очікується, що за три цикли активізується мінімум 61÷65 S-блоків. Виходить, що трьох циклів цілком достатньо (з запасом) для того, щоб ШУП-1 прийшов до стану випадкової підстановки й при використанні S-блоків з граничними диференціальними та лінійними показниками, і при використанні S-блоків шифру Мухомор.

Використання випадкових S-блоків. Як випливає з результатів роботи [17], значення мінімального числа циклів виходу шифру до стану випадкової підстановки безпосередньо пов’язане з диференціальними і лінійними властивостями S-блоків.

Звернемо тепер увагу на те, що в розрахунках орієнтувалися на значення ймовірностей максимумів переходів S-блоків, близьких до гранично досяжних значень. Однак, як показує аналіз, розподіл максимумів переходів S-блоків істотно залежить від значень досягнутих максимумів.

У таблиці 5.2 представлені результати, що ілюструють залежність кількості максимумів, що зустрічаються у S-блоків, від їх значень максимумів [17].

Таблиця 5.2

Залежність числа максимумів від значень максимумів для таблиць підстановок різних шифрів

S-блоки шифрів	Max. DT	Число максимумів	Max. Lat	Число максимумів
ADE, AES, GrandCru, Лабіринт	4	255	112	1275
Iseberg, Khazad	8	80	98	6
Мухомор	8	90	98	8
Випадкові	10 12	12 1	96 94	3 1

З представлених даних випливає, що для S-блоків з граничними лінійними і диференціальними показниками (S-блоків шифрів ADE, AES, GrandCru, Лабіринт, та ряду інших) число значень максимумів виходить великим (достатнім для побудови диференціальних і лінійних характеристик з максимально ймовірних переходів).

Однак для інших шифрів (S-блоки шифрів Iseberg, Khazad, Мухомор і випадкових підстановок) зі значеннями диференціальних і лінійних переходів S-блоків, що мають максимуми, які перевищують гранично досяжні мінімальні значення, числа цих максимумів виражаються десятками, а то й одиницями (їх виходить мало).

Це означає, що при побудові диференціальних і лінійних характеристик з такими S-блоками, в більшості випадків будуть використовуватися переходи й не з максимально можливими значеннями (максимальних значень дуже мало).

Тому реальні значення ймовірностей диференціальних і лінійних характеристик будуть визначатися випадковим набором переходів, в яких беруть участь переходи й не з мінімальними значеннями ймовірностей.

Це буде призводити до зменшення необхідного числа S-блоків, що активізуються в порівнянні з випадком використання переходів з мінімальними значеннями.

У зв’язку з зазначеним була виконана оцінка можливостей використання в ШУП випадкових S-блоків.

Методика виконання розрахунків представлена в роботі [17]. У табл. 5.3 представлені результати розрахунків числа переходів різного типу в 48 рядках диференціальної таблиці підстановки.

В цих розрахунках методом перебору вибрано відразу таке максимальне число активних S-блоків, що дозволяє реалізувати прихід шифру до випадкової підстановки.

Для диференціальних показників воно дорівнює 48.

Таблиця 5.3

Розрахунок числа переходів різного типу в 48-ми рядках диференціальної таблиці випадкової підстановки

Значення переходу таблиці	Число переходів диференціальної таблиці	Число переходів в рядку	Число переходів у 48-ми рядках
12	1	0,003906	0,19
10	10	0,039065	1,87
8	104	0,40625	19,5
6	830	3,24218	155,62

З представлених результатів випливає, що 48 активних S-блоків (активних переходів) можна вибрати при випадкових входах в S-блоки при їх послідовному запуску на основі використання:

- двох переходів зі значенням 10;
- двадцяти переходів зі значенням 8;
- двадцяти шести переходів зі значенням 6;

(використовуються максимально ймовірні переходи, при цьому вважається, що вхід в перший S-блок буде максимально можливим). Всього 48 переходів (48 активних S-блоків). Обчислення в цьому випадку призводять до результату:

$$\left(\frac{10}{256}\right)^2 \times \left(\frac{8}{256}\right)^{20} \times \left(\frac{6}{256}\right)^{26} = 2^{-250}.$$

Це означає, що випадкові S-блоки за диференціальними показниками забезпечують гарантований прихід шифру ШУП-1 до стану випадкової підстановки за три цикли (на трьох циклах активізується близько 65 S-блоків).

Розглянемо тепер закон розподілу переходів для зміщень лінійної апроксимаційної таблиці. У загальне число переходів тут входять і позитивні і негативні зміщення.

Користуючись результатами роботи [22], можемо розрахувати кількість переходів різного типу в 64 рядках лінійної апроксимаційної таблиці випадкової підстановки.

Підсумки розрахунків представлені в табл. 5.4.

Знову будемо вважати, що за рахунок введення циклових поідключей входи в S-блоки будуть випадковими і статистично незалежними. Методика розрахунків представлена в роботі [22].

Таблиця 5.4

Розрахунок числа переходів різного типу в 64-х рядках лінійної таблиці випадкової підстановки

Значення переходу	Число переходів в таблиці ЛАТ	Число переходів в рядку таблиці ЛАТ	Число переходів в 64 випадково взятих рядках таблиці ЛАТ
±34	1,998	0,0078	0,4992
±32	4	0,0156	0,9984
±30	10	0,0392	2,5088
±28	28	0,1098	7,0272
±26	65	0,2588	16,5632
±24	146	0,572	36,608
±22	298	1,164	74,496

З таблиці 5.4 випливає, що для 64 активних S-блоків при використанні максимально ймовірних переходів можна очикувати при випадкових входах у випадкові S-блоки:

- один перехід зі значенням 34;
- один перехід зі значенням 32;
- один перехід зі значенням 28;
- один перехід зі значенням 26;
- один перехід зі значенням 24.

Вважаючи далі, що рядки в S-блок вибираються зі всієї множини 256 рядків. При цьому переходи по S-блокам йдуть в довільному порядку і здійснюються за найбільш ймовірним шляхом, можемо виконати оцінку ймовірності приходу шифру до стану випадкової підстановки з випадковими S-блоками. Обчислення для 64 S-блоків призводять до результату

$$2^{63}\times\left(\frac{34}{128}\right)^2\times\left(\frac{32}{128}\right)^2\times\left(\left(\frac{30}{128}\right)^2\right)^3\times\left(\left(\frac{28}{128}\right)^2\right)^7\times$$

$$\times\left(\left(\frac{26}{128}\right)^2\right)^{16}\times\left(\left(\frac{24}{128}\right)^2\right)^{36}=2^{-235}.$$

Тут вже 64 випадкових S-блоків не достатньо, щоб шифр став випадковою підстановкою. Однак, значення лінійної ймовірності 2^{-235} (для 64 S-блоків) все одно виявляється цілком прийнятним показником стійкості трициклового перетворення.

Для гарантованого приходу ШУП до випадкової підстановки за лінійними показниками потрібно вже чотири цикли. Практично ж можна вважати, що шифр є стійким проти атак лінійного криптоаналізу і при трьох циклах шифрування.

Результати обчислювальних експериментів покращення показників приходу шифру ШУП до стану випадкової підстановки ілюструють таблиці 5.5 і 5.6.

Для порівняння наведено данні для шифрів AES, Калина і Мухомор, раніше наведених в таблицях 2.1 і 2.2 для 30 випадково взятих майстер ключів. Во всіх експериментах були розглянуті повні версії шифрів при активізації їх 16-бітними блоками даних.

В табл. 5.5 узагальнені результати таких експериментів для шифрів Мухомор, Калина, і ШУП-1.

Таблиця 5.5

Поциклові значення максимумів переходів таблиць повних диференціалів для повних версій українських шифрів і шифру ШУП-1

Число цик-- лів	Калина	Rijndael	Мухомор (рідні S-блоки)	Мухомор (випадк. S-блоки)	ШУП-1 (S-блоки Мухомор)	ШУП-1 (випадк. S-блоки)
1	301,56	1024	19,13	19,3	2560,3	3072,38
2	40,63	3652,26	18,8	19,3	18,8	19,082
3	19,13	19,0666	19,4	19,4	19	19,122
4	19,2	19,0666	19,13	18,9	18,6	19,122
5	19.27	18,8666	19,07	19,1	19,4	19,142

У табл. 5.6 представлені результати обчислювальних експериментів по визначенню поциклових середніх значень максимумів зміщень лінійних корпусів шифрів у вигляді модульних значень їх максимумів.

Як випливає з представлених результатів шифр ШУП-1 приходить до стану випадкової підтановки на другому циклі, а шифр ШУП-2 повторює результати характерні для шифру Мухомор.

Він досягає середнього значення максимуму зміщення лінійного корпусу 820, характерного для випадкової підстановки степеня 2^{16}, вже після першого циклу шифрування (на першому циклі) і середнє значення

максимуму диференціального переходу 19, характерного для випадкової підстановки аналогічного степеня.

Таблиця 5.6

Поциклові значення максимумів зміщень таблиць лінійних апроксимацій повних версій шифрів зі значеннями середньоквадратичних відхилень (30 ключів)

Число циклів	Калина 30 ключів	Мухомор 30 ключів	ШУП-1	ШУП-2
1	11008,392± 1785,34	824,742± 20,1286	8192,56	876,333
2	3968±307	818,621± 25,9742	825,52	828,1
3	862,66±50	827,431± 21,2352	828,92	823,707
4	826,44±23	824,193± 17,8115	825,34	821,433
5	837,349±28	831,753± 25,7731	814,22	826,067

Як видно, шифри серії ШУП, як і шифр Мухомор перевершують по ефективності циклових перетворень шифр Калина. Нагадаємо на закінчення, що шифр Rijndael-256 приходить до стану випадкової підстановки за диференціальними та лінійними показниками лише на п’яти циклах.

5.2.4 Результати оцінки показників обчислювальної складності

Як і в роботі [115], при оцінці обчислювальної складності будемо орієнтуватися на число XOR операцій, що виконуються шифром в процесі шифрування і розшифрування.

Для виконання SL перетворення (матричного множення) потрібно виконати 12 XOR операцій (кожне множення на МДР матрицю включає дванадцять підсумувань результатів добутків байтів на елементи МДР матриці).Відповідно до структури циклового перетворення, представленої на

рис. 5.1, в першому циклі ШУП-1 потрібно виконати 8 + 3×7 + 3×8 = 53 XOR (тактів).

Для 8 циклового шифру, якщо на інших циклах, крім першого використовувати тільки одну лінійку SL перетворень без складань за модулем два на вході лінійки, приходиться 53 + 46×8 + 8 = 429 XOR-ів. В AES-256 на 14 циклів припадає (12×8 + 8)×13 +8 = 1360 XOR, тобто ШУП-1 буде суттєво швидше AES. Але тут ще не враховуються витрати на процедуру розгортання майстер ключа.

5.3 Оцінка стійкості запропонованих рішень з побудови процедур шифрування до відомих методів криптоаналізу

Для оцінки стійкості до інших методів криптоаналізу можна послатися на відповідні висновки, зроблені для шифру Мухомор [111]. Сімейство шифрів ШУП наслідують усі властивості цього шифру.

Стійкість до лінійного і диференціального криптоаналізу. Відносно підвищеної стійкості до відомих методів криптоаналізу, і, зокрема до лінійного і диференціального криптоаналізу можна відзначити, що при використанні механізму керованої підстановки слід очікувати відсутність будь-яких статистично стійких асиметричних (зміщених по ймовірності) зв’язків між входами і виходами циклових перетворень і всього шифру в цілому.

Очевидно, що результуючі показники доказової стійкості для шифру ШУП збігаються з показниками стійкості відомих шифрів AES, Калина та інші.

Підвищення стійкості в даному випадку означає, що ШУП-2 становиться випадковою підстановкою вже на другому циклі. наявна практика побудування шифрів встановила правило, відповідно до якого число циклів шифрування береться у 3÷4 рази збільшеним відносно кількості циклів шифру потрібних для його виходу до стану випадкової підстановки.

Кількість циклів шифрування ШУП вибрано рівним 8, тобто вважається що шифр буде забезпечувати гарантовано граничні показники стійкості до

атак лінійного та диференціального криптоаналізу при 8 циклах шифрування. Це і дозволяє підвищувати показники обчислювальної складності в запропонованих рішеннях.

Інтегральна атака. Інтегральна атака застосовується до шифрів з добре збудованою структурою, подібній структурі SPN (AES).

Через те що запропонована циклова функція відрізняється від тих, що звичайно застосовуються в SPN конструкціях наявністю недетермінованого механізму управління підстановками, то навряд чи вдасться знайти інтегральний розрізнювач для цілої структури всього шифру .

Статистичні атаки. Враховуючи високі дифузійні властивості циклової функції, високу степінь нелінійності S блокового перетворення і “достатність” числа циклів, можна з упевненістю сказати, що пропоновані рішення будуть стійкими до всіх варіантів лінійного та диференційного криптоаналізу та їх поєднань, до бумерангових і rectangle атакам і їх узагальненням, подібним атакам з використанням усічених диференціалів і диференціалів високого порядку, неможливих диференціалів і багатьом іншим атакам.

Відносно-ключова і слайд атаки. Слайд атаки експлуатують періодичну структуру алгоритму розгортання ключів. Пропоноване рішення по формуванню циклових підключів виключає їх подібність.

Інтерполяційні і алгебраїчні атаки. Інтерполяційні атаки використовують переваги S-блокового представлення, а саме його просту алгебраїчну структуру. Представляється, що сам недетермінований механізм, реалізований за допомогою керованих підстановок, навряд чи може знайти аналітичний опис (вимоги до відбору підстановок у запропонованих рішеннях можуть виявитися істотно більш м’якими, ніж, наприклад, в шифрі FOX). Тому відмічені атаки не є скільки-небудь ефективними для запропонованих рішень. Тут можна також відмітити, що використання випадкових S-блоків забезпечує, як показано в розділі 3, їх оптимальні криптографічні властивості (високі значення алгебраїного степеня й алгебраїчної імунності).

Надалі ми також будемо використовувти конструкцію шифру ШУП-1 без операції додатного змішування на вході першого SL перетворення циклової функції. Ми будемо позначати її ШУП-1М.

5.4 Блоковий симетричний шифр з керованими підстановками ШУП-2

Зауважимо, нарешті, що якби перше циклове перетворення було зроблено двошаровим (використовувались би дві лінійки SL перетворень), то шифр ШУП став би випадковою підстановкою вже на другому циклі.

Назвемо цю модифікацію цього рішення шифром ШУП-2. Як вже було відмічено раніше, виявилося що складання сегментів даних на вході першого SL перетворення не приводить до підвищення показників випадковості шифру.

Тому схема першого циклу перетворень шифру ШУП-2 представлена на Рис. 5.2. вже без змішування сегментів даних на вході першого SL перетворення. Ця модифікація шифру позначена нами ШУП-2М.

Отже, верхня половина схеми повторює схему першого циклу шифру ШУП-1 без операції додатного змішування на вході першого SL перетворення. При наведеній схемі запуску SL перетвореннями виступають укрупненні S-блоки, які можна розглядати як латинські квадрати [116].

Другий шар (ланцюжок) SL перетворень підключається до виходів SL перетворень першого шару через суматори за модулем 2, на другі входи яких подаються значення виходів попередніх SL перетворень першого шару (ланцюжку). Складання за модулем 2 виходу останнього SL перетворення другого ланцюжка виконується тільки з виходом першого SL перетворення цього ланцюжка.

В шифрі ШУП-2 (ШУП-2М) на двох перших циклах буде активізуватись близько 65 S-блоків. Для цього шифру і при двох циклах зашифрування відпадають всі обмеження на диференціальні та лінійні показники використовуваних в шифрі S-блоків.

Надалі по аналогії з шифром ШУП-2М будемо конструкцію шифру ШУП-1 без операції додатного змішування на вході першого SL перетворення циклової функції будемо позначати ШУП-1М.

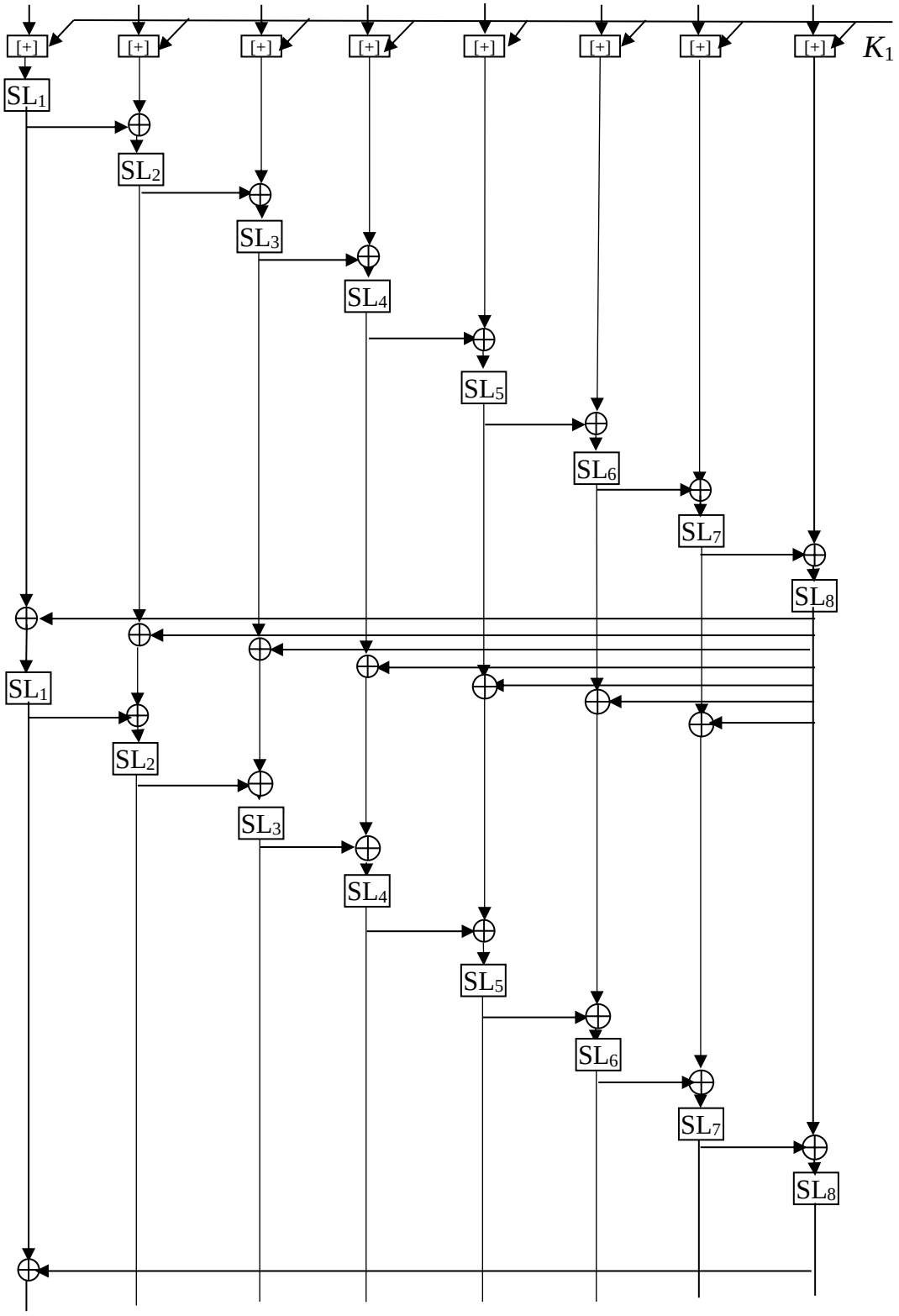

Рис.5.2 Перший цикл перетворення шифру ШУП-2М

Показники обчислювальної складності. Відповідно до структури циклового перетворення, представленої на рис. 5.2, в першому циклі потрібно виконати 8 + 2×3×8 + 2×14 = 84 XOR (такти). Для 8-циклового шифру тоді буде потрібно 84 + (24 + 8)×7 +8 = 316 XOR операцій.

5.5 Метод підвищення швидкодії на основі конвеєрної обробки даних

В принципі, конвеєрна обробка в ітеративному шифрі не може бути застосована, якщо операції його циклової функції покривають все циклове перетворення. Такою операцією в шифрах серії ШУП є операція додавання виходу останнього SL перетворення з виходом першого чи попередніх SL перетворень. Поки ця операція не виконана, циклове перетворення не закінчене.

Конвеєрна обробка вимагає, щоб циклова функція будувалася так, що її окремі операції могли б виконуватися паралельно (одночасно). Тому операції, що покривають всю циклову функцію, повинні бути виключені. Як показали експерименти, для шифрів ШУП це можна зробити після того, як шифри приходять до стану випадкової підстановки. Зокрема, в шифрі ШУП-2 (ШУП-2М) після перших двох циклів шифрування можна решту його циклів будувати, виключивши з циклових функцій операції додавання виходів останніх SL перетворень з виходами перших SL перетворень. Тобто циклові перетворення на циклах, починаючи з третього, повинні відрізнятися від циклових перетворень перших двох циклів.

В цьому випадку після формування виходу першого SL перетворення третього циклу можна відразу ж з формуванням виходу другого SL перетворення третього циклу формувати вихід першого SL перетворення четвертого циклу. Після формування виходу другого SL перетворення четвертого циклу формувати і вихід першого SL перетворення п’ятого циклу і т.і.

Якщо вважати, що для 32-бітної платформи для виконання операції SL перетворення необхідно затратити час T сек., То для окремої лінійки

(циклу) з m SL перетворень необхідно буде затратити $m(T + T_R)$ сек. Тут T_R– тимчасові витрати на виконання операції додавання сегментів даних на входах кожного з SL перетворень.

При конвеєрній обробці, яка починається з третього циклу, кожен черговий s-тий цикл здійснюватиметься із затримкою $(s–3)(T+T_R)$ сек, $3 \le s \le r$. В результаті, якщо для обробки l циклів при зашифруванні одним потоком буде необхідно затратити ml $(T+T_R)$ сек, то при паралельній обробці l циклів досить буде затратити $(m+l–1)$ $(T+T_R)$ сек. Отже, виграш у швидкодії, якого можна досягти можна розрахувати таким чином.

Якщо шифр будується з використанням 32-бітних SL перетворень, то для m=8, l=6 маємо виграш у швидкодії обчислення шести останніх циклів шифрування

$$\frac{ml}{m+l-1} = \frac{8\times 6}{8+5} = \frac{48}{13} = 3{,}7\,.$$

А з урахуванням перших двох циклів маємо:

$$\frac{8\times 8}{2\times 8+13} = \frac{64}{29} = 2{,}2\,.$$

В результаті виграш перевищує два рази.

Таким чином, описані шифри, названі ШУП-ами, представляються як найбільш перспективні рішення з побудови сучасних шифрів.

Далі наводяться додатні розробки, виконані в цьому же напрямку.

5.6 Методи удосконалення наявних шифрів

Відповідно до методів побудови блокових симетричних шифрів, що розвиваються в роботі [22], шифри потрібно конструювати так, щоб вони забезпечували активізацію якомога збільшене число S-блоків перших циклів.

Прикладами шифрів зі збільшеним числом S-блоків, які реалізують такий підхід, є шифри IDEA NXT, Мухомор, білоруський шифр. Але це шифри дворівневого типу, які мають зовнішній рівень, побудований з використанням схеми Lai-Massey, або використовують багатошарове багатомодульне перемішування (це не SPN шифри). Ці схеми виглядають

досить складними для аналізу, хоча і вважається, що вони володіють підвищеними показниками випадковості.

В цьому розділі хочеться зупинитися на шляхах підвищення ефективності саме SPN шифрів, які мають більш поширене застосування. Аналіз показує [18 та ін.], що для відомих конструкціях SPN шифрів мінімальне число S-блоків, що активізуються на першому циклі, дорівнює одному (шифри Rijndael, Калина-2, ADE, «Кузнечик», GrandCru, і багато інших). Ці шифри мають один шар S-блоків в циклової функції, і тому практично незалежно від операції забілювання один байт входу активізує тільки один S-блок першого циклу. Такі шифри приходять до стану випадкової підстановки за три-чотири і більшу кількість циклів. Далі пропонуються ще два методи вдосконалення вже наявних конструкцій шифрів Rijndael і Калина.

Метою теперішньої пропозиції є розробка і дослідження конструкції першого циклу, що дозволяє поліпшити динамічні показники приходу SPN шифрів до стану випадкової підстановки.

Матеріал, що викладається далі, орієнтований на можливість збільшення мінімального числа активізуємих S-блоків першого циклу на основі використання його побудування за двошаровою конструкцією. Це дозволяє активізувати в нашому випадку відразу всі (майже всі) S-блоки другого шару.

5.6.1 Удосконалений БСШ Rijndael

Відповідно до підходу, що розвивається, пропонується перший цикл шифрування зробити двошаровим за підстановлювальними перетвореннями. При цьому для побудови шарів перетворень застосувати включення укрупнених підстановлювальних перетворень (SL перетворень) в ланцюжок, в якому поточне підстановлювальне перетворення приймає на вхід поряд з черговим вхідним сегментом даних результат підстановлювального перетворення попереднього сегмента і подальшому розповсюдженні активізації на всі байти виходу циклового перетворення. Це дозволяє при одному активному байті входу зробити активними всі (або майже всі) S-блоки

другого шару підстановок першого циклу і створити умови, при яких шифр стає випадковою підстановкою за два цикли. Зазначений момент є принциповим для отримання конструкцій шифрів, в яких без зниження стійкості можна використовувати випадкові S-блоки.

Зауважимо, що активізації всіх S-блоків другого циклу слід очікувати й в шифрі «Кузнечик» [50], де стратегія широкого сліду реалізована на основі використання лінійного перетворення з множенням виходів S-блоків на МДВ матриці розміром 16×16. Але шифр «Кузнечик»має 128-бітний розмір входу, що не задовольняє вимогам використання шифру в постквантовий період розвитку криптографії [74]. І ніхто ще не реалізував множення на матрицю МДВ кодів розміром 32×32. Хочеться вирішити цю задачу для 256-бітних шифрів, орієнтуючись на пропозиції по реалізації стратегії широкого сліду без застосування сепарабельних кодів [19]. Тут ця пропозиція застосовується для побудови циклової функції нової конструкції.

Метою теперішньої пропозиції є розробка і дослідження конструкції першого циклу, що дозволяє поліпшити динамічні показники приходу SPN шифрів до стану випадкової підстановки.

Далі буде розглядатися удосконалення 256-бітного шифру Rijndael, орієнтованого на використання в постквантовій криптографії [118]. Основна ідея розвинутого підходу будується на застосуванні циклової функції, що повторює перший цикл шифру ШУП-2М, який має два шари підстановлювальних перетворень, що складаються з ланцюжків керованих одного іншим SL перетворень. Пропонована конструкція практично повторює схему першого циклу шифру ШУП-2М (див. Рис. 5.2).

Показники випадковості перетворення тут відрізняються від показників, наведених в [22]. Як вже зазначалося, при ненульовій різниці на вході циклу для самого правого (одного) байту активізується мінімум тільки один S-блок першого ланцюжка, який 4 активними байтами активізує всі SL перетворення другого ланцюжка. Всього очікується в цій схемі активізація

з великою ймовірністю 33 S-блоків першого циклу, а на двох циклах буде з великою ймовірністю активізуватися близько 65 S-блоків.

Можна пропозицію на рис. 5.2 розглядати і як двоциклову конструкцію, але вона все одно буде набагато ефективніше оригінальної розробки. Підвищена ефективність перетворення повторює результати, наведені для шифру ШУП-1 (див. табл. 5.1). Видно, що з великою ймовірністю число S-блоків, що активізується на першому циклі виявляється близьким до 33. Навіть при дуже малоймовірному варіанті активізації 26 S-блоків на другому і (або) третьому циклах їх мінімальне число 53 все одно буде достатнім з запасом для приходу вдосконаленого шифру за три цикли до стану випадкової підстановки. Оригінальна конструкція потребує для приходу до випадкової підстановки 5 циклів.

Обчислювальна складність. Як і в роботі [115], при оцінці обчислювальної складності будемо орієнтуватися на число XOR операцій, що виконуються шифром в процесі шифрування і розшифрування. Будемо виходити з того, що для виконання SL-перетворення (матричного множення), як вже відмічено вище, потрібно виконати 12 XOR операцій.

Тоді відповідно до структури циклового перетворення, представленої на рис. 5.3 в удосконаленому першому циклі потрібно виконати 8 + 3×7 + + 2×12×8 = 221 XOR (тактів). Для 8-циклового шифру тоді буде потрібно 221 + 12×8×7 + 8 = 421 XOR операції.

У Rijndael-256 на 14 циклів припадає (12×8 + 8)×13 + 16 = 1368 XOR операцій, тобто вдосконалений Rijndael буде швидше оригінальної розробки.

Правда, тут ще не враховуються витрати на процедуру розгортання майстер ключа.

5.6.2 Удосконалений шифр Калина

Основним недоліком відомих конструкцій SPN блокових симетричних шифрів є вкрай мале число S-блоків, що активізуються різницями вхідних блоків даних на першому циклі. Повернемося до ідеї удосконалення наявних конструкцій блокових симетричних шифрів (БСШ), якій присвячена робота

[119]. У цій роботі пішли по шляху введення на вході шифру додаткового змішуючого перетворення на основі складання за модулем 2 сегментів блоків даних на вході шифрів, вважаючи, що це дозволить збільшити число активізуємих S-блоків першого циклу.

Як з'ясувалося в ході подальших досліджень, цей підхід дозволив збільшити число активізуємих S-блоків при активізації шифру однобайтовою різницею, але все ж таки не виключив можливості активізації одного S-блоку першого циклу в разі кількох ненульових різниць вхідного блоку даних. Наприклад, в разі, коли для четвірки сегментів входу $\Delta X_2 = \Delta X_3 = 0$, $\Delta X_1 = \Delta X_4 = \Delta \neq 0$, хоча і при цьому підході, як вже відмічалося вище, суттєво зменшується число таких випадків.

Спочатку вважалось справедливим твердження, що для SPN шифрів з цикловими функціями, які використовують одношарові підстановлювальні перетворення, мінімальне число активізуємих S-блоків першого циклу дорівнює одному. Саме через це процес приходу БСШ до стану випадкової підстановки затягується до трьох і більше циклів.

Було зроблено висновок, що єдина можливість збільшити число S-блоків першого циклу, що активізуються – це зробити його двошаровим. Це реалізовано в шифрах Мухомор, IDEA NXT, ШУП-2 [22].

Пізніше позицію було змінено і вирішено, що запропонована конструкція побудування циклової функції з використанням керованих підстановок дозволяє вийти за рамки цього обмеження. Відповідні пропозиції в цьому напрямку представлені в роботах [118; 119; 120; 121; 122; 123]. Надалі стало зрозуміло, що цей крок виявився хибним і ми знову повернулися до попереднього висновку. Увага зосередилась на введенні в шифри на першому циклі двошарових підстановлювальних перетворень.

У роботі [22] відмічено, що двошарове перетворення аж надто близько повторює двоциклову конструкцію. Хоча його гідністю можна вважати те, що

воно дозволяє обґрунтувати можливість зменшення числа циклів приходу шифру до стану випадкової підстановки.

Другою його гідністю є можливість активізації всіх S-блоків другого шару підстановлювальних перетворень першого циклу, яка потім поширюється на інші цикли.

Цей ефект активізації S-блоків другого і наступних циклів може бути реалізований і без другого шару SL перетворень, тобто при побудові першого циклу по одношаровій схемі, як це зроблено в шифрі ШУП-1 [22].

Тільки в цьому випадку необхідно подбати про те, щоб колонки матриці станів після складання за модулем 2 виходу останнього SL перетворення першого шару з виходами інших SL перетворень були різними (не збігалися).

Цього можна домогтися, якщо для колонок на виходах перетворень першого шару застосувати нову операцію, якої немає в оригінальному шифрі.

Ця операція полягає в циклічному зсуві колонок матриці станів. Назвемо її операцією ShiftColumns.

Оскільки для 256 бітного шифру виходить 4 колонки матриці станів, то потрібно зробити так, щоб циклічні зсуви між колонками були різними.

5.6.2.1 Сутність вдосконалення БСШ Калина

Схема запропонованої нової конструкції першого циклу для 256-бітного шифру Калина представлена на Рис. 5.3.

У цьому випадку на вхід першого циклу надходить вхідний блок даних, перетворений в матрицю станів з чотирьох колонок і восьми рядків (вісім S-блоків в колонці).

Після його складання з ключем забілювання, а SL перетворення беруться вісьми байтовими з множенням на МДР матриці розміром 8×8 (це фактично перетворення SubBute і MixColumn шифру Калина).

Додавання з циклових підключів для нового циклу (операція AddRoundKey) виконується за модулем 2. Після першого циклу йдуть стандартні перетворення шифру Калина, тільки в удосконаленій конструкції

шифру застосовується 8 циклів шифрування, замість 14, встановлених для стандарту.

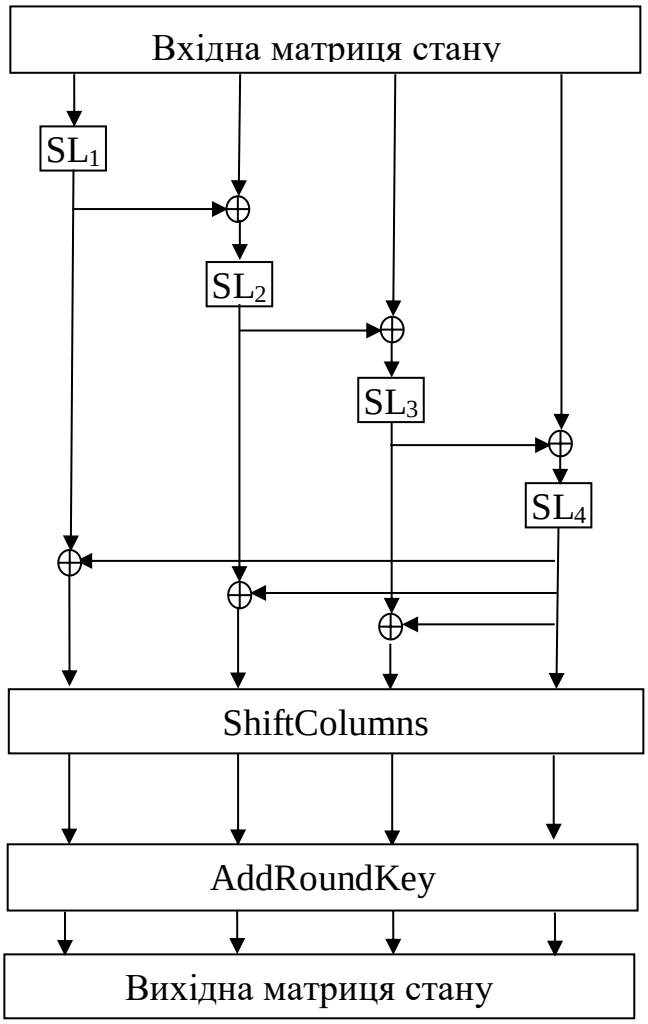

Рис. 5.3. Схема вдосконаленого першого циклу шифру Калина

Сам новий перший цикл вставляється в оригінальну конструкцію після початкового забілювання замість першого циклу оригінальної розробки. Представлена конструкція містить основні елементи схеми першого циклу шифру ШУП-1 [22]. В даному випадку число SL перетворень в шарі зменшено до 4. Як і в шифрі Калина в даному випадку обробляються 64-бітні сегменти вхідного блоку даних. Крім того, в конструкцію додано нове перетворення ShiftColumns і введено складання з цикловим підключем за модулем 2 (операція AddRoundKey). SL перетворення включені в ланцюжок, так що на вхід поточного перетворення надходить вихід попереднього, як в шифрі ШУП-1. Після першого циклу ідуть стандартні перетворення шифру Калина.

Далі можна скористатися результатами попереднього параграфа, з яких випливає, що розглянута конструкція шифру дозволяє без втрати стійкості застосовувати випадкові S-блоки.

Оригінальна версія шифру Калина приходить до стану випадкової підстановки за 4 цикли, а запропонована конструкція за три цикли, при цьому за три цикли активізується близько 65 S-блоків, в той час як в Калині за три цикли активізується 41 S-блок.

5.6.2.2 Оцінка показників удосконалення за критерієм складності

Як і в роботі [115], при оцінці обчислювальної складності будемо орієнтуватися на число XOR операцій, що виконуються шифром в процесі шифрування і розшифрування. Будемо виходити з того, що для виконання SL перетворення (матричного множення) потрібно виконати дванадцять XOR операцій.

Нагадаємо, що в шифрі Калина (ДСТУ 7624:2014) для компактності реалізації і підвищення швидкодії в останньому циклі збережена операція лінійного перетворення MixColumns.

Тоді відповідно до структури циклового перетворення, представленої на рис. 1, в новому першому циклі шифру буде потрібно виконати

$4 + 4 + 56\times4\times2 + 4 = 460$ XOR операцій. Для 8-циклового шифру тоді потрібно виконати $460 + (56\times4 + 4)\times 7 = 2056$ XOR операцій.

В Калині-256 на 14 циклів припадає $(56\times4 + 4)\times 13 = 2964$ XOR ,тобто вдосконалена Калина буде швидше оригінальної розробки майже у 1,5 рази. Тут знову, правда, не враховуються витрати на процедуру розгортання майстер ключа.

Висновки до розділу 5

Головним науковим результатом розділу слід вважати запропоновані удосконалені методи проєктування БСШ з істотно поліпшеними динамічними показниками їх приходу до стану випадкової підстановки, орієнтованих на використання у постквантовій криптографії.

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

1) побудування SPN шифру з використанням принципів послідовної активізації укрупнених S-блоків циклової функції одного за іншим і з забезпеченням на першому циклі активізації всіх байтів виходу циклової функції;

2) використання в першому циклі SPN шифру збільшеного числа S-блоків на основі побудування двошарової його конструкції, що дозволяє забезпечити при активізації всієї множини S-блоків другого шару разом з S-блоками наступного циклу досягнення граничних значень максимумів диференціальних і лінійних ймовірностей, що відповідають приходу шифру до стану випадкової підстановки;

3) введення додаткової процедури змішування вхідних сегментів даних на вході шифру на основі використання нової конструкції першого циклу, в якій забезпечується принцип послідовної активізації укрупнених S-блоків циклової функції одного за іншим зі складанням виходу останнього укрупненого S-блоку з виходами інших, що забезпечує при побудові укрупнених S-блоків за стратегією широкого сліду активізацію усіх байтів виходу першого циклу;

Запропоновано дві конструкції шифрів ШУП-1 і ШУП-2, в яких забезпечується активізація практично всіх S-блоків циклових функцій починаючи з другого циклу.

Встановлена і реалізована можливість активізації збільшеного числа S-блоків першого циклу, чого не дозволяють відомі конструкції шифрів з одношаровими підстановлювальними перетвореннями. Вона реалізована в модифікаціях шифрів ШУП-1 і ШУП-2, названих шифрами ШУП-1М і ШУП-2М, а також у вдосконалених конструкціях шифрів Rijndael та Калина.

Встановлено, що шифри пропонованої конструкції володіють найкращими з відомих SPN шифрів динамічними показниками приходу до

стану випадкової підстановки. Практично вони стають випадковими підстановками вже з другого - третього циклу, чого не дозволяє жоден з відомих 256 бітних SPN шифрів. Це означає їх підвищену стійкість до атак диференціального і лінійного криптоаналізу (дозволяють зменшити число циклів зашифрування). За показниками обчислювальної складності шифри можуть працювати істотно швидше AES.

За іншими показниками стійкості ці шифри успадкували всі високі показники стійкості, властиві шифру Мухомор [45]. Чудовою властивістю цих шифрів є те, що вони стають випадковими підстановками за два-три цикли і при використанні випадкових S-блоків. Тобто властивості ціх шифрів практично не залежать від властивостей S-блоків, що входять до них.

Запропонований варіант удосконалення шифру Rijndael дозволяє суттєво поліпшити показники випадковості цього шифру. Зокрема, вдосконалений шифр гарантовано приходить до стану випадкової підстановки за три цикли, як за диференціальними, так і за лінійними показниками. Він за своїми криптографічними показниками не поступається новому Українському стандарту – шифру Калина-2.

Запропонована конструкція удосконаленого шифру Калина з поліпшеними показниками приходу до стану випадкової підстановки. Основою побудови шифру є застосування при побудуванні першого циклу шару перетворень з керованими одна однією підстановками. Запропоноване удосконалення реалізує можливість активізації всіх S-блоків другого циклу. Вдосконалений шифр дозволяє зменшити допустиму кількість циклів шифрування, що призводить до підвищення його продуктивності в порівнянні з оригінальною версією без зниження стійкості.

У запропонованих шифрах можуть застосовуватися випадкові S-блоки без спеціального відбору, що відкриває реальний шлях усунення залежності властивостей шифру від властивостей застосовуваних в шифрі S-блоків.

Найкорисніший результат підходу, що розвивається полягає в тому, що вдається побудувати шифри зі зменшеним числом циклових перетворень без

втрати стійкості, що дозволяє домогтися подальшого підвищення продуктивності алгоритмів шифрування. Додатковим корисним результатом роботи є запропонована проста схема розгортання ключів, не прив’язана до процедури шифрування, яка дозволяє забезпечити відсутність самоподібності циклових підключів при їх формуванні. На шифр ШУП-1 сьогодні вже отримані патенти [25; 27].

Ще одним важливим результатом досліджень слід рахувати обґрунтування можливості реалізації стратегії широкого сліду без застосування сепарабельних кодів [63].

Матеріал цього розділу побудований на публікаціях автора [17; 18; 22; 123] та інші.

ЗАГАЛЬНІ ВИСНОВКИ

В результаті виконаних досліджень вирішена важлива науково-технічна задача, яка має практичне значення для удосконалення технологій блокового симетричного шифрування і складається в розробці методів поліпшення динамічних показників приходу БСШ до стану випадкової підстановки на основі збільшення числа S-блоків, що активізуються на перших циклах шифрування.

Основні висновки за результатами виконаних досліджень можна сформулювати наступним чином:

1. Засоби й технології блокового симетричного шифрування продовжують займати важливе місце в вирішенні завдань захисту комп'ютерних систем, мереж та їх компонентів. Проблеми забезпечення стійкості (надійності) блокових симетричних шифрів, використовуваних для захисту інформації, у багатьох випадках виходять на рівень захисту національних інтересів.

Майбутній етап розвитку криптографії характеризується зростанням обчислювальних можливостей. У найближчій перспективі очікується поява квантових комп'ютерів. Для блокових симетричних шифрів постквантова криптографія означає розробку і використання в найближчому майбутньому шифрів з довжиною блоку і ключа більше ніж 256 бітів.

Серед широкого спектру задач, що вимагають свого рішення, стоїть задача подальшого вдосконалення методів проєктування і розробки БСШ для постквантового періоду розвитку криптографії з підвищеними показниками стійкості і швидкодії.

2. Основою наявних методів оцінки стійкості сучасних БСШ до атак диференціального і лінійного криптоаналізу є визначення максимумів середніх значень повних диференціалів і зміщень лінійних корпусів.

Результатами досліджень підтверджена справедливість і обґрунтованість нової методології оцінки показників доказової стійкості блокових

симетричних шифрів до атак диференціального і лінійного криптоаналізу. Ця методологія будується на основі використання теоретичних значень максимумів законів розподілу переходів XOR таблиць (повних диференціалів) і змішень таблиць ЛАТ (лінійних корпусів) шифруючих перетворень, що розглядаються як випадкові підстановки. На відміну від наявних підходів отримані точні значення показників стійкості шифрів.

Методологія ґрунтується на встановленому факті, що на відміну від відомих результатів, які пов'язують показники стійкості шифрів з диференціальними й лінійними властивостями нелінійних перетворень шифрів, максимальні значення повних диференціалів і лінійних корпусів сучасних шифрів асимптотично не залежать ні від властивостей використовуваних в шифрах підстановлювальних конструкцій, ні від методів введення в циклові функції циклових підключив, ні від способу побудови лінійного перетворення. Вони виявляються функцією тільки розміру бітового входу в шифр (степеня підстановки). Це дозволяє максимуми повних диференціалів і лінійних корпусів шифрів отримати розрахунковим шляхом на основі використання математичних співвідношень, отриманих для випадкових підстановок.

3. Вперше розраховані й підтверджені експериментально закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій БСШ, як підстановлювальних перетворень. Відповідно до отриманих результатів зроблений висновок, що всі сучасні шифри мають досить малий діапазон зміни значень максимумів повних диференціалів і максимумів зміщень лінійних корпусів, що знаходяться в околиці відповідних значень максимумів випадкових підстановок. Для оцінки показників доказової стійкості шифрів можна користуватися результатами оцінок максимальних диференціальних ймовірностей і максимальних лінійних ймовірностей, обчислених для довільно взятого (одного) ключа шифрування.

4. Розвинута математична модель випадкової підстановки в частині доведення ряду теорем щодо виду законів розподілу XOR таблиць і таблиць лінійних апроксимацій випадкових підстановок На відміну від наявних підходів це дозволило розрахунковим шляхом отримати значення максимумів повних диференціалів та лінійних корпусів шифрів й внаслідок цього істотно прискорити процес визначення показників їх доказової безпеки до атак диференціального та лінійного криптоаналізу.

5. Вперше запропоновано обчислювальний і експериментальний методи оцінки динамічних показників приходу БСШ до стану випадкової підстановки . Запропоновано новий метод визначення реального числа циклових переходів шифру до показників випадкової підстановки на основі врахування мінімального числа тільки тих активних S-блоків, які припадають на перші цикли його перетворень і беруть участь у формуванні граничних значень диференціальної та лінійної ймовірностей.

6. Розроблені нові конструкції шифрів ШУП-1 і ШУП-1М з 256-бітовими входами, орієнтовані на використання в постквантовій криптографії. Ці конструкції володіють поліпшеними показниками по стійкості й швидкодії. За динамічними показниками приходу до стану випадкової підстановки запропоновані конструкції перевершують всі відомі розробки. На шифр ШУП-1 отримано патент.

7. Розроблено нові конструкції шифрів ШУП-2 і ШУП-2М з 256-бітовим входами, орієнтовані на використання в пост-квантовій криптографії, які стають випадковими підстановками вже на другому циклі, чого не може реалізувати жоден з відомих SPN шифрів. У розроблених конструкціях без зниження стійкості можуть застосовуватися S-блоки випадкового типу.

8. Розроблені й запатентовані вдосконалені конструкції шифрів Rijndael і Калина з поліпшеними динамічними показниками приходу до стану випадкової підстановці. Запропоновані конструкції знімають обмеження на криптографічні показники S-блоків, що використовуються в циклових перетвореннях шифрів.

9. Встановлено, що циклові перетворення сучасних шифрів побудовані так, що лінійні та диференціальні показники S-блоків, що входять в них, впливають на динамічні показники приходу шифрів до стану випадкової підстановки в межах одного циклу. Це шифри з мінімальними значеннями числа S-блоків, що активізуються на першому циклі (шифри Rijndael, Калина і ряд інших), що дорівнюють одному. У таких шифрах мінімальне число активізуємих S-блоків перших циклів знаходиться на кордоні забезпечення мінімальної їх кількості, необхідної для приходу шифрів до асимптотичних значень диференціальних і лінійних ймовірностей. Тому зміна диференціальних або лінійних показників S-блоків впливає на мінімальне число циклових перетворень необхідних для приходу шифру до стану випадкової підстановки. Для багатьох сучасних шифрів з відібраними S-блоками для приходу до випадкової підстановки необхідно виконати мінімум три-чотири цикли зашифрування.

10. Встановлено, що для шифру, як і для випадкової підстановки значення максимумів диференціалів і максимумів лінійних корпусів не є не прогнозованими значеннями. Вони підпорядковуються інтегральному закону розподілу екстремальних значень множини незалежних випадкових змінних, що мають один і той же розподіл.

Вірогідність отриманих наукових результатів підтверджується збіжністю експериментальних даних статистичних експериментів та випробувань повних версій шифрів та їх зменшених моделей з розрахунковими, що випливають з теоретичних співвідношень, а також їх несуперечливістю з відомими результатами криптоаналізу БСШ, математичної теорії підстановок, теорії ймовірностей та математичної статистики.

Практична значимість отриманих результатів:

1. Вперше розраховані й підтверджені експериментально закони розподілу максимумів (екстремальні розподіли) переходів XOR таблиць і зміщень таблиць лінійних апроксимацій підстановлювальних перетворень і шифрів, як підстановлювальних перетворень. Відповідно до отриманих

результатів зроблено висновок, що всі сучасні шифри мають досить малий діапазон зміни максимумів повних диференціалів і максимумів зміщень лінійних корпусів, так що практично для оцінки показників доказової стійкості цих шифрів можна користуватися результатами оцінок максимальних диференціальних ймовірностей і максимальних лінійних ймовірностей.

2. Розроблені програмні моделі засобів оцінки динамічних показників приходу шифрів до стану випадкової підстановки.

3. Розроблені програмні моделі конструкції вдосконалених шифрів, що підтверджують працездатність нових методів проєктування та розробки шифрів з підвищеними показниками стійкості та швидкодії, орієнтовані на використання в постквантовий період розвитку криптографії.

4. Отримані конкретні значення показників стійкості розроблених конструкцій шифрів (значення AMDP і AMLHP) до атак диференціального та лінійного криптоаналізу, що дозволило зробити висновок про те, що розглянуті шифри не поступаються за даними показниками шифру Rijndael і іншим відомим конструкціям сучасних шифрів .

5. Запропоновані методи проєктування БСШ, реалізовані в системах криптографічного захисту інформації при виконанні ряду державних НІР (акт реалізації результатів наукових досліджень у діяльності ЗАТ «Інститут інформаційних технологій» від 7 жовтня 2018 р., представлений в додатку Г, та акти реалізації результатів досліджень при виконанні держбюджетних науково-дослідних робіт Харківського національного університету імені В. Н. Каразіна) та Харківського національного університету радіоелектроніки, також представлені в Додатку Г).

6. Результати роботи реалізовані також в навчальному процесі кафедри БІСТ національного університету імені В. Н. Каразіна при читанні навчальної дисципліни «Криптологічні методи в кібербезпеці» для магістрів спеціальності «Кібербезпека» та при підготовці та читанні лекцій для магістрів спеціальності «Безпека інформаційних і комунікаційних систем» за темою «Нова

методологія оцінки стійкості БСШ до атак диференційного та лінійного криптоаналізу», зокрема безпосередньо використані результати застосування цієї методології для визначення показників доказової стійкості стандартизованого шифру Калина, нового шифру з білоруського стандарту та нової розробки по створенню криптоалгоритму, що задовольняє умовам використання в постквантовий період розвитку криптографії (акт реалізації представлений в Додатку Д).

Обґрунтованість і достовірність наукових положень дисертації підтверджується:

– збігом даних статистичних експериментів та випробувань малих і великих версій шифрів із розрахунковими, що випливають із теоретично доведених співвідношень;

– коректністю застосування математичного апарата;

– несуперечливістю з відомими результатами криптоаналізу блокових симетричних шифрів, математичною теорією підстановок, теорією ймовірностей і математичної статистики.

Результати дисертаційного дослідження можуть бути використані:

- в організаціях, що займаються проєктуванням та конструюванням засобів захисту інформації для уточнення показників алгоритмів шифрування, а також при проєктуванні та розробці нових конструкцій БСШ;

- в організаціях, що займаються експертизою та оцінкою проєктних та конструкторських рішень по побудові сучасних БСШ, у тому числі комісій при проведенні конкурсів на відбір перспективних рішень.

Цілі дослідження досягнуті, всі поставлені задачі розв’язані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лисицька І. В. Методологія оцінки стійкості блокових симетричних криптоперетворень на основі зменшених моделей: дис. … докт. техн. наук : 05.13.05. Харків, 2012. 293 с.

2. Олешко О. І. Методи прискореного криптоаналізу БСШ на основі аналізу показників стійкості зменшених моделей прототипів: дис … канд. техн. наук : 05.13.21. Харків, 2010. 176 с.

3. Широков О. В. Методи формування S-блокових конструкцій випадкового типу з покращеними показниками стійкості для блокових симетричних шифрів: дис. … канд. техн. наук : 05.13.21. Харків, 2010. 232 с.

4. Мельнічук Є. Д. Методи оцінки криптографічної придатності вузлів нелінійних замін блокових симетричних шифрів: дис. … канд. техн. наук : 05.13.21. Харків, 2013. 188 с.

5. Настенко А. О. Методи оцінки стійкості блокових симетричних шифрів на основі показників випадковості: дис. … канд. техн. наук : 05.13.21. Харків, 2015. 165 с.

6. Долгов В. И., Лисицкая И. В. Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа : монография. Харьков : Форт, 2013. 420 с.

7. Лисицкая И. В., Лисицкий К .Е., Широков А. В., Мельничук Е. Д. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок. *Радіоелектронні та комп'ютерні системи*. 2010. № 6 (47). С. 87-93.

8. Олейников Р. В., Олешко О. И., Лисицкий К .Е, Тевяшев А. Д. Дифференциальные свойства подстановок. *Прикладная радиоэлектроника*. 2010. Т.9, № 3. С. 326-333.

9. Лисицкая И. В., Настенко А. А., Лисицкий К. Е. Большие шифры – случайные подстановки. Сравнение показателей статистической безопасности

блочных симметричных шифров, представленных на украинский конкурс. *Восточно-Европейский журнал передовых технологий*. 2012. Т. 6. № 9(60) С. 11–21.

10. Лисицкая И. В., Настенко А. А., Лисицкий К. Е. Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс и их уменьшенных моделей. *Автоматизированные системы управления и приборы автоматики*. 2012. Вып.159. С. 4-10.

11. Долгов В. И., Олейников Р. В., Лисицкая И. В и др. Исследование показателей случайности блочного шифра из Белорусского стандарта СТБ 34.101.31-2011. *Спеціальні телекомунікаційні системи та захист інформації.* 2012. Вип. 2(12). С. 38-51.

12. Лисицкая И. В., Лисицкий К. Е. О приходе итеративных шифров к стационарному состоянию, свойственному случайной подстановке. *Прикладная радиоэлектроника*. 2013. Том. 12, № 2. С. 230-235.

13. Lisitskaya I. V., Melnichuk E. D., Lysytskiy K. E. Importance of S-Blocks in Modern Block Ciphers. *I. J. Computer Network and Information Security*, 2012, 10, 1-12.

14. Лисицкий К.Е., Лисицкая И.В. Математическая модель случайной подстановки. *Радиотехника*. 2020. Вип. 202. С. 116-124.

15. Лисицкий К. Е. Максимальные значения полных дифференциалов и линейных корпусов блочных симметричных шифров. *Технологический аудит и резервы производства*. 2014. №1/1 (15). С. 47-52.

16. Lisitskiy K. E. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers. *I.J. Computer Network and Information Security*. 2014. №1, P. 11-18. Published Online November 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis. 2014.01.02.

17. Горбенко І. Д., Лисицкий К. Е. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями

нелинейности близкими к предельным. *Радиотехника*. 2014. Вип. 176. С. 27–39.

18. Горбенко И. Д., Лисицкая И. В., Лисицкий К. Е. Уточнённые показатели прихода шифров к состоянию случайной подстановки. *Прикладная радиоэлектроника*. 2014. Том. 13, № 3. С. 213-216.

19. Rodinko M. YU., Lisitskiy K. E. The wide trail strategy without separable codes. *Radiotekhnika*. 2015. №181. P. 40-45.

20. Лисицкий К. Е. О методике оценки законов распределения вероятностей максимумов полных дифференциалов и смещений линейных оболочек блочных симметричных шифров. *Прикладная радиоэлектроника.* 2015. Том. 14, № 4. С. 335-338.

21. Лисицкая И. В., Лисицкий К. Е., Родинко М. Ю., Головко И. А., Жариков И. И., Корниенко М. А., Кулеба М. В. Экспериментальные данные по определению динамических показателей прихода блочных симметричных шифров к состоянию случайной подстановки. *Радіоелектроніка, інформатика, управління.* 2017. № 1. С. 129–141.

22. Dolgov V. I., Lisitska I. V., Lisitskiy K. Ye. The new concept of block symmetric ciphers design. *Telecommunications and Radio Engineering*. 2017. Vol. 76, № 2. P. 157–184.

23. Лисицкий К. Е. Закон распределения вероятностей смещений таблиц аппроксимаций случайных подстановок. *Радиотехника*. 2017. №189. С. 81-89.

24. Dolgov V. I., Lisitska I. V, Nastenko A. A, Lisitskiy K. E. Estimations of Maximal Values of Differentials and Linear Hulls of Markov Ciphers. *Applied radio electronics*, Scientific and Technical Journal. 2012. Vol. 11, № 2. P. 144-151.

25. Спосіб криптографічного перетворення двійкових даних (варіанти) : пат. 111547 Україна : МПК (2016.01) G09C 1/00 H04L 9/06 (2006.01); заявл. 06.02.2015; опубл. 10.05.2016, Бюл. № 9. 8 с.

26. Лисицкий К. Е. Вырожденные S-блоки. *Радіоелектроніка, інформатика, управління*. 2018. № 1. С. 129–138

27. Спосіб криптографічного перетворення двійкових даних: пат. 111448 Україна : МПК H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01); заявл. 25.04.2015; опубл. 25.04.2016, Бюл. № 8. 8 с.

28. Родинко М. Ю., Лисицький К. Е. Циклические свойства блочных симметричных шифров. Труды Международного молодёжного форума "*Радиоэлектроника и молодёжь в XXI веке*". Харьков. 2012. С. 142–144.

29. Долгов В. И., Лисицкая И. В., Настенко А. А., Лисицкий К. Е. Оценки максимальных значений дифференциалов и линейных корпусов марковских шифров. *Прикладная радиоэлектроника*. 2012. Т. 11, № 2 С. 144-151.

30. Лисицький К. Є. Оптимізація перспективних алгоритмів блокового симетричного перетворення по критеріям швидкодії і стійкості. *Математичне та комп'ютерне моделювання*: зб. наук. праць / Інститут кібернетики імені В. М. Глушкова Національної академії наук України. Кам'янець-Подільський національний університет імені Івана Огієнка. 2017. Вип. 15. С. 115-119.

31. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. 90 с.

32. Баяшев, Р. Г., Диев С. И., Розмахнин М. К. Основные направления развития и совершенствования криптографического закрытия информации. *Зарубежная электроника*. 1989. №12. С. 76-91.

33. Задірака, В. К. Олесю В. К., Недашковський. Н. О. Методи захисту банківської інформації. К.: Вища школа. 1999. 417 с.

34. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему. СПб: Мир и сім'я-95. 1997. 312 с.

35. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь. 1999. 328 с.

36. Моисеенков И. Н. Основы безопасности компьютерных систем. М.: Компьютер-пресс. 1991. №10. С. 19-24.

37. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке. М: Триумф, 2002. 727 с.

38. Шнаер Б. Секреты и ложь. Безопасность данных в цифровом мире. С. Петерб. Питер, 2003. 257 с.

39. Положення про проведення відкритого конкурсу криптографічних алгоритмів. http://dstszi.gov.ua/dstszi/control/uk/publish/, 2006.

40. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Київ. Держспоживстандарт України, 2015. 238 с.

41. Лисицкая И. В. Современные методы проектирования БСШ. От конкурсов к стандартам. *Радиотехника*. 2011. № 165**.** С. 226-239.

42. J. Daemen and V. Ridjmen. The Design of Rijndael: AES — the Advanced Encryption Standard, Springer-Verlag, Berlin, 2002.

43. Lai X. On the design and security of block ciphers volume 1 of ETH Series in Information Processing. Hartung-Gorre Verlag, 1992.

44. Lai X., Massey J. A proposal for a new block encryption standard. In I. Damg˚ard, editor, Advances in Cryptology – EUROCRYPT'90, volume 473 of Lecture Notes in Computer Science. Springer-Verlag, 1991. P. 389–404

45. Бондаренко М. Ф., Горбенко І. Д., Долгов В. І., Лисицька І. В., Родінко М. Ю., Лисицький К. Є., Горбенко Ю. І. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація. *Прикладная радиоэлектроника*. 2007. Том 6, №2. С. 147-157.

46. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія : монографія. Харків: Форт, 2013. 878 с.

47. СТБ 34.101.31-2011 Государственный стандарт республики Беларусь. Информационные технологии. Защита информации Криптографические алгоритмы шифрования и контроля целостности. Введен в действие постановлением Госстандарта Республики Беларусь от 31 января 2011 г. № 5. Изд-во Госстандарт, Минск, 2011. 35 с.

48. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: Київ, Держспоживстандарт України, 2015. 238 с.

49. ГОСТ Р 34.12 2015. Информационная технология. Криптографическая защита информации. Блочные шифры. Москва Стандартинформ. 2015. 21 с.

50. В. Шишкин. Принципы синтеза перспективного алгоритма симметричного шифрования с длиной блока 128 бит. Рус Крипто'2013, 28 марта 2013 г.

51. Susan Landau. Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard, February, 2004. P. 89-115/

52. Meier W. and Staffelbach O. Nonlinearity criteria for cryptographic functions, in *Advances in Cryptology:* Eurocrypt '89, eds Springer-Verlag, Berlin, 1989. P. 549-562.

53. Pieprzyk J., Quisquater J. and Vandewalle J. Nonlinearity of exponent permutations, in *Advances in Cryptology: Eurocrypt* '89, J. Pieprzyk, , eds., Springer-Verlag, Berlin, 1990, P. 89-92.

54. J. Pieprzyk, On Bent Permutations, Technical Report CS91/11, Department of Computer Science, University of New South Wales; presented at International Conference on Finite Fields, *Coding Theory, and Advances in Communications and Computing*, Las Vegas, 1991.

55. K. Nyberg, Differentially uniform mappings for cryptography, in Advances in Cryptology: Eurocrypt '93, T. Helleseth, ed., Springer-Verlag, Berlin, 1994, P. 53-64.

56. J. Daemen, Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis, Ph.D. thesis, Katholieke Universiteit, Leuven, Belgium, 1995. 249 p.

57. V. Ridjmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, The cipher SHARK, in Fast Software Encryption: Third International Workshop, D. Gollman, ed., Springer-Verlag, Berlin, 1996, P. 99-112.

58. T. Jakobsen and L. Knudsen, Attacks on block ciphers of low algebraic degree, J. Cryptology 14 (2001), P. 197-210.

59. J. Daemen, L. Knudsen, and V. Ridjmen, The Block Cipher Square, in Fast Software Encryption, E. Biham ed., LNCS 1267, Springer-Verlag, Berlin, 1997. P. 149-165

60. R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, 1986. 410 p.

61. B. Weeks, M. Bean, T. Rozylowicz, and C. Ficke, Hardware Performance Simulation of Round 2 Advanced Encryption Standard Algorithms (May 15, 2000); available at http://csrc.nist.gov/encryption/aes/ round2/r2anlsys.htm.

62. P. Junod and S. Vaudenay, FOX: a new family of block ciphers. In H. Handschuh and A. Hasan, editors, Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004. Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, pages 114-129. Springer-Verlag, 2004.

63. Горбенко І. Д., Долгов В. І., Олійников Р. В. Принципи побудування та властивості блокових симетричних IDEA подібних шифрів *Прикладная радиоэлектроника*. 2007. Том 6, №2. С. 158-173.

64. Лисицкая И. В., Настенко А. А., Лисицкий К. Е О криптографической значимости схем разворачивания ключей в обеспечении стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа. *Радиоэлектроника и інформатика*. 2012. №3(58) С. 56-65.

65. Chen L. Practical Imapct of Quntum Computing. The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Режим доступу: [https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf].

66. Moody D. Post-Quntum Cryptography: NIST’s Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Режим доступу:[https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf].

67. Корольков А. В. О некоторых прикладных аспектах квантовой криптографии в контексте квантовых вычислений и появления квантовых компьютеров. *Вопросы кибербезопасности*. 2015. №1(9). С. 1-8.

68. Електроний ресурс. gs_QKD011v010101p. ETSI GS QKD 011 V1.1.1 (2016-05).

69. Електроний ресурс: Eg 203310v010000m. Final draft ETSI EG 203 310 V1.0.0 (2016-04).

70. Електроний ресурс: Eg 203310v010101p. Final draft ETSI EG 203 310 V1.1.1 (2016-06).

71. Електроний ресурс: E. D. Dahl, D-Wave Systems. November 2013. Programming with D-Wave: Map Coloring Problem.

72. Електроний ресурс: pqc2016_nist_announcement. Post-Quantum Cryptography: NIST s Plan for the Future.

73. Li X., Ma J., Moon S. (2005) On the Security of the Canetti-Krawczyk Model. In: Hao Y. et al. (eds) Computational Intelligence and Security. CIS 2005. Lecture Notes in Computer Science, vol. 3802. Springer, Berlin, Heidelberg.

74. Grover L. K. A fast quantum mechanics algorithm for datable search. Proceeding of the 28th ACM Symposium 0n Theory of Computation, New York: ACM Press. 1996. P. 212-219.

75. Горбенко Ю. І. Ганзя Р. С. Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера. *Захист інформації*: науково-практичний журнал. К., 2014. Том 16, №2. С. 106–112.

76. Горбенко Ю. І., Ганзя Р. С. Аналіз стійкості пост-квантових систем. *Прикладна радіоелектроніка*. Харків: ХНУРЭ. 2014. Том 13. №3. С. 268-274.

77. Горбенко І. Д., Іванченко Є. В., Карпенко С. В., Гнатюк С. О. Методи перехоплення інформації у системах квантової криптографії, Науково-практичний журнал "*Захист інформації*". К.: НАУ, 2011. №2(51). С. 121-129.

78. Горбенко Ю. І., Ганзя Р. С. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем. *Східно-європейський журнал передових технологій*. 2014. № 1/9 (67). С. 8–15.

79. Сорока, Л. С., Кузнецов А. А.. Московченко И. В.. Исаев С. А. Исследование дифференциальных свойств блочно-симметричных шфров. *Системи обробки інформації.* Вип. 6 (87). 2010. С. 286–294.

80. Олейников Р. В., Лисицкий**.** К. Е Исследование дифференциальных свойств подстановок различных цикловых классов Двенадцатая Международная научно-практическая конференция «*Безопасность информации в информационно-телекоммуникационных системах*», 19-22 МАЯ 2009 г., Тезисы докладов. К.: ЧП “ЕКМО”, НИЦ “ТЕЗИС” НТУУ “КПИ”. 2009. С. 24-25.

81. Долгов В. И. Макарчук Я. А., Григорьев А. В., Дробатько Е. В. Исследование криптографических показателей уменьшенных моделей шифров ГОСТ и DES. *Прикладная радиоэлектроника*, 2011. Т.10. № 2. С. 127–134.

82. Долгов В. И., Олейников Р. В., Большаков А. Ю., Григорьев А. В., Дробатько Е. В. Криптографические свойства уменьшенной версии шифра «Калина». *Прикладная радиоэлектроника*ою. 2010. Т.9. № 3. С. 349-354.

83. Долгов В. И., Кузнецов А. А., Сергиенко Р. В., Белоковаленко А. Л. Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE). *Прикладная радиоэлектроника*. 2008. Т.7, №3. С. 215-224.

84. Долгов В. И., Кузнецов А. А., Исаев С. А. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. *Электронное моделирование*. 2011. Т 33, № 6. С. 81-99.

85. Лисицкая И. В. Криптографические свойства уменьшенной версии шифра «Мухомор» *Спеціальні телекомунікаційні системи та захист інформації.* Збірник наукових праць, Київ. 2010. Вип. 2(18). С. 33-42.

86. Лисицкая И. В. Настенко А. А. Большие шифры – случайные подстановки. *Радиотехника*. 2011. Вып. 166. С. 50-55.

87. Lai X., Massey J., and Murphy S. Markov ciphers and differential cryptanalysis, Advances in Cryptology—EUROCRYPT’91, LNCS 547. Springer-Verlag, 1991. P. 17-38,.

88. Keliher, H. Meijer, and S. Tavares, Toward the true random cipher: On expected linear probability values for SPNs with randomly selected s-boxes, chapter in Communications, Information and Network Security, V. Bhargava, H. Poor, V. Tarokh, and S. Yoon (Eds.), P. 123-146, Kluwer Academic Publishers, 2003.

89. Keliher L., Linear Cryptanalysis of Substitution-Permutation Networks. A thesis submitted to the School of Computing in conformity with the requirements for the degree of Doctor of Philosophy. 2003. 160 p.

90. Ковальчук Л. В. Сходимость последовательности матриц вероятностей дифференциальных аппроксимаций немарковского блочного шифра к равновероятной матрице при увеличении количества циклов. *Прикладная радиоэлектроника*. 2007. Т.5, № 2. С. 274-276.

91. Долгов В. И., Лисицкая И. В. Блочные симметричные шифры и Марковские процессы. *Прикладная радиоэлектроника*. 2012. Т. 11, № 2. С. 137-143.

92. Joan Daemen, Vincent Rijmen. Probability distributions of Correlation and Differentials in Block Ciphers. April 13, 2006, P. 1–38.

93. Лисицкая И. В. Вырожденные подстановки *Радиотехника*. 2012. Вып. 171. С. 41-49.

94. Rodinko M. Yu., Oliynykov R V., Hrinenko T. O. Improvement of the method for optimal S-boxes generation *Прикладная радиоэлектроника*. 2015. Том. 14, № 4. С. 315-320.

95. Кузнецов А. А., Лисицкая И. В., Исаев С. А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. *Прикладная радиоэлектроника.* 2011. Т.10, №2 С. 135-140.

96. Лисицкая И. В. Об участии S-блоков в формировании максимальных значений дифференциальных и линейных вероятностей блочных

симметричных шифров. *Спеціальні телекомунікаційні системи та захист інформації.* Вип. 7 (21) Київ. 2012. С. 71-84.

97. Лисицкая И. В. Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок. *Вісник Харківського національного університету імені В.Н. Каразіна.* Харків, 2011. №960, Вип.16. С. 196-206.

98. Feller. An Introduction to Probability Theory and Its Applications, Vol.1. Wiley & Sons. 1968.

99. Mathworld. http: //mathworld. wolfram.com/.

100. Сачков В. Н. Введение в комбинаторные методы дискретной математики. - М.: Наука. 1982 384 с.

101. Долгов В. И., Лисицкая И. В., Олешко О. И. Свойства таблиц линейных аппроксимаций случайных подстановок. *Прикладная радиоэлектроника*. 2010. Т. 9, № 3. С. 334-340.

102. O'Connor L., "On the Distribution of Characteristics in Bijective Mappings," Advances in Cryptology, Proceedings of Eurocrypt '93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1993, P. 360–370.

103. O'Connor Luke. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. P. 1-7.

104 Luke O'Connor. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

105. E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. Technical Report 708. Technion, Israel Institute of Technology, Haifa, 1991. P. 487-496.

106. Markku-Juhani O. Saarinen Cryptographic Analysis of All 16-Bit S-Boxes. 2008. Volume 7118 of the series Lecture Notes in Computer Science. P. 118-133.

107. Городилова А. А. От криптоанализа к криптографическому свойству булевой функции. *Прикладная дискретная математика*. 2016. № 3 (33). С. 16-41.

108. Carlet C. Vektorial Boolean funktions for cryptography // Ch. 9 of the Monograph «Boolean Methods and Models in Mathematics. Computer Science and Enginiring» Cambridge Univ. Press. 2010. P. 398-472.

109. Лисицкий К. Е. Динамические показатели прихода блочных шифров к состоянию случайной подстановки. Издательский дом LAPLAMBERT Academic Publishing, 2014, 60 с.

110. Matsui M. Linear cryptanalysis method for DES cipher. In Advances in Cryptology.- EUROCRYPT'93 (1994) vol. 765. Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York P, 386-397.

111. Бондаренко М. Ф., Горбенко І. Д., Долгов В. І., Олійников Р. В та інші. Обґрунтування вимог та розробка основних рішень з побудуванню та властивості перспективного БСШ «Мухомор». *Прикладная радиоэлектроника*. 2007. Том. 6, №2. С. 147-157.

112. Specification of Camellia – a 128 bit Block Cipher, version 2.0, September 2.6. 2001. 35 p.

113. Biham E. Serpent: A New Block Cipher Proposal / E. Biham, R. Anderson and L.R. Knudsen In S. Vaudenay, editor, 5th Fast Software Encryption Workshop, LNCS 1372, P. 222–238. Springer-Verlag, 1998.

114. Спосіб недетермінованого криптографічного перетворення блоків даних: пат. 53949A Україна. № 2002032372; заявл. 26.03.2003; опубл. 17.02.2003, Бюл. № 2. 2 с.

115. Горбенко И. Д., Чекалин Д. А. Свойства и возможности оптимизации криптографических преобразований в AES – RIJNDAEL *Радиотехника* . 2001. №119. С. 36-42.

116. Математическая энциклопедия в 5 т. / Гл. ред. И.М. Виноградов – М.: Советская энциклопедия, 1979. Т.2: Д-КОО. 278 с.

117. Спосіб формування циклових підключів для блокових симетричних шифрів: пат. 117158 Україна. № a 21607592; заявл. 11.07.2016; опубл. 25.06.2018, Бюл. № 12. 6 с. UA.

118. Лисицкий К. Е. Новое усовершенствование Rijndael-я Науково-практична конференція «*Проблеми кібербезпеки інформаційно-телекомунікаційних систем*» Київський національний університет імені Тараса Шевченко. 10–11 квітня 2016 р. С. 51.

119. Долгов В. И., Лисицкая И. В., Лисицкий К. Е. Усовершенствованный блочный симметричный шифр Калина 0485-8972. *Радиотехника*. 2016. №186. С. 119-131.

120. Lisitskaya Iryna, Lisitskiy Konstantin, Rodinko Mariya. Impruvd Rijndael Science and Education Studies “Stanford University Press” Volume II № 1(17), January- June 2016. P. 608-618.

121. Lisickiy K. E., Dolgov V. I., Lisickaya I. V. Block cipher with improved dynamic indicators of the condition of a random Scientific-Practical Conference *Problems of Infocommunications. Science and Technology* (PIC S&T), 2017 4th International Date of Conference: 10-13 Oct. 2017. Date Added to IEEE Xplore: 04 January 2018 ISBN Information: INSPEC Accession Number:17484901 DOI: 10.1109/INFOCOMMST.2017.8246424 Publisher:IEEE. P. 391-395.

122. Lisickiy K. E., Dolgov V. I., Lisickaya I. V. Cipher with improved dynamic indicators of the condition of a random substitution. Scientific-Practical Conference *Problems of Infocommunications. Science and Technology* (PIC S&T), 2017, 4th International Date of Conference: 10-13 Oct. 2017. Date Added to IEEE Xplore: 04 January 2018 ISBN Information: INSPEC Accession Number: 17484901 DOI:10.1109/INFOCOMMST.2017.8246424 Publisher: IEEE. P. 396-399.

123. Лисицький К. Є. Удосконалена конструкція початкового перетворення для SPN шифрів. Матеріали XX Ювілейної Міжнародної науково-практичної конференції «*Безпека інформації в інформаційно-телекомунікаційних системах*» 22-24 травня 2018 р. м. Буга, Київська область, ГПЦ “Зелена Буга”. С. 106-108.

124. Лисицька И. В., Лисицький К. Є. Порівняння по ефективності цікловых перетворень сучасних шифрів . Науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». 21–24 травня 2013 р. Київ С. 53. (очно).

125 Долгов В. И., Лисицкая И. В., Лисицкий К. Е. Усовершенствованный блочный симметричный шифр Калина. *Радиотехника*. 2016. №186. С. 119-131.

126. Спосіб криптографічного перетворення двійкових даних: пат. 111448 Україна. № а 201503976; заявл. 25.04.2015; опубл. 25.04.2016, Бюл. № 8. 20 с.

127. Спосіб криптографічного перетворення двійкових даних (варіанти): пат. 111547 Україна. № а 201500942; заявл. 06.02.2015; опубл. 10.05.2016, Бюл. № 9. 20 с.

128. Спосіб критографіччного перетворення двійкових даних: пат. 118625 Україна. № а 201707795; заявл. 24.07.2017; опубл. 11.02.2019, Бюл. № 3. 8 с.

129. Спосіб критографічного перетворення двійкових даних (варіанти): пат. 119097 Україна. № а 201708383; заявл. 14.08. 2017; опубл. 25.04.2019, Бюл. № 8. 8 с.

130. Спосіб критографіччного перетворення двійкових даних: пат. 118625 Україна. № а 201707795 ; заявл. 24.07.2017; опубл. 11.02.2019, Бюл. № 3. 8 с.

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

у фахових виданнях України:

1. Горбенко И.Д., Лисицкий К.Е. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным. *Радиотехника.* 2014. № 176. С. 27–39. (Особистий внесок здобувача: участь у формуванні всіх розділів роботи та в обґрунтуванні методики експериментів).

2. Лисицкая И. В., Настенко А. А., Лисицкий К. Е. Большие шифры – случайные подстановки. Сравнение показателей статистической безопасности блочных симметричных шифров, представленных на украинский конкурс. *Восточно-Европейский журнал передовых технологий*. 2012. Т. 6, № 9(60). С. 11–21. (Особистий внесок здобувача: участь у формуванні всіх розділів роботи, особливо вступу та обґрунтуванні методики експериментів).

у фахових виданнях України, що входять до міжнародних наукометричних баз:

3. Лисицкая И. В., Лисицкий К. Е., Родинко М. Ю., Головко И. А., Жариков И. И., Корниенко М. А., Кулеба М. В. Экспериментальные данные по определению динамических показателей прихода блочных симметричных шифров к состоянию случайной подстановки. *Радіоелектроніка, інформатика, управління.* 2017. № 1. С. 129–141. (Web of Science). (Особистий внесок здобувача: участь у формуванні узагальнених показників приходу сучасних шифрів до стану випадкової підстановки, відбір та редагування матеріалу статті).

4. Лисицкий К. Е. Вырожденные S-блоки. *Радіоелектроніка, інформатика, управління*. 2018. № 1. С. 129–138. (Web of Science).

у періодичному науковому виданні держави, яка входить до Організації економічного співробітництва та розвитку, що входить до міжнародної наукометричної бази:

5. Dolgov V. I., Lisitska I. V., Lisitskiy K. Ye. The new concept of block symmetric ciphers design. *Telecommunications and Radio Engineering*. 2017. Vol. 76, Is. 2. P. 157–184. (SCOPUS, United States). (Особистий внесок здобувача: виконання розрахунків відносно показників використання випадкових S-блоків, оцінок продуктивності конструкції, а також участь у виконанні аналізу відомих рішень по побудуванню сучасних шифрів і формуванні вдосконалених методів їх проєктування).

6. Lisitskiy K. E. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers. *International Journal of Computer Network and Information Security*. 2013. Vol. 6, No. 1. P. 11–18. (Hong Kong S.A.R., China).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Лисицкая И., Лисицкий К. Сравнение по эффективности цикловых преобразований современных шифров // Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XVI міжнар. наук.-практ. конф., 21–24 травня 2013 р., Київ, 2013. С. 53. (Очно). (Особистий внесок здобувача: участь в підготовці матеріалів доповіді та виступ перед фахівцями).

8. Лисицкий К. Е. Новое усовершенствование Rijndael // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : матеріали міжнар. наук.-практ. конф., 10–11 квітня 2016 р., Київ, 2016. С. 51.

9. Lisickiy K. E., Dolgov V. I., Lisickaya I. V. Cipher with improved dynamic indicators of the condition of a random substitution // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) : 4th International Date of Conference, 10–13 Oct. 2017 // Date Added to IEEE Xplore : ISBN Information: INSPEC Accession **Number:** 17484901, 04 Jan. 2018, P. 396–399. **DOI:** 10.1109/INFOCOMMST.2017. 8246424 (Заочно). (Особистий внесок

здобувача: участь у створенні тенічного рішення, розробка програмної моделі та дослідженні її показників).

10. Лисицький К. Є. Удосконалена конструкція початкового перетворення для SPN шифрів // Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XX ювілейної міжнар. наук.-практ. конф., 22–24 травня. 2018 р., Буга, Київська область, 2018. С. 106–108. (Очно).

Наукові праці, які додатково відображають наукові результати дисертації:

11. Лисицкий К. Е. Максимальные значения полных дифференциалов и линейных корпусов блочных симметричных шифров. *Технологический аудит и резервы производства.* 2014. Т. 1, № 1(15). С. 47-52.

12. Лисицкий К. Е. Закон распределения вероятностей смещений таблиц аппроксимаций случайных подстановок. *Радиотехника*. 2017. № 189. С. 81–89.

13. Лисицький К. Є. Оптимізація перспективних алгоритмів блокового симетричного перетворення по критеріям швидкодії і стійкості. *Математичне та комп'ютерне моделювання*: зб. наук. праць / Інститут кібернетики імені В. М. Глушкова Національної академії наук України. Кам'янець-Подільський національний університет імені Івана Огієнка. 2017. Вип. 15. С. 115-119.

14. Лисицкий К. Е., Лисицкая И.В. Математическая модель случайной подстановки. *Радиотехника*. 2020. № 202. С. 116–124. (Особистий внесок здобувача: участь у формуванні всіх розділів роботи та в обґрунтуванні методики та постановці експериментів).

15. Лисицкий К. Е. О методике оценки законов распределения вероятностей максимумов полных дифференциалов и смещений линейных оболочек блочных симметричных. *Прикладная радиоэлектроника.* 2015. Т. 14, № 4. С. 335–338.

Додаток Б

Понятійний апарат лінійного та диференціального криптоаналізу. Нові показники доказової стійкості

Основний понятійний апарат лінійного і диференціального криптоаналізу, яким користаємося в дисертації. Слідуючи роботі [6], наведемо ряд визначень.

Визначення 1. (Диференціальна і Лінійна ймовірності): Диференціальна ймовірність DP^f і лінійна ймовірність LP^f відповідно для ключезалежної функції f з n-бітовим входом x і n-бітовим виходом y, ($x,y \in GF(2^n)$) є

$$DP^f(\Delta x \to \Delta y) = \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y}{2^n}; \qquad (Б.1)$$

$$LP^f(\Gamma x \to \Gamma y) = \left(\frac{\#\{x \in GF(2)^n \mid x \cdot \Gamma x) = f(x) \cdot \Gamma y}{2^{n-1}} - 1 \right)^2, , \qquad (Б.2)$$

де Δx і Δy є вхідними і вихідними різницями, а Γx і Γy – це вхідна і вихідна маски; $x \cdot \Gamma x$ позначає результат скалярного добутку x на Γx, $f(x) \cdot \Gamma y$ – результат скалярного добутку $f(x)$ на Γy.

Визначення 2. (DP^f_{max} і LP^f_{max}): Максимальне значення диференціальної і лінійної ймовірностей для ключезалежної функції f визначаються відповідно як:

$$DP^f_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^f(\Delta x \to \Delta y), \qquad (Б.3)$$

$$LP^f_{\max} = \max_{\Gamma x,\ \Gamma x \neq 0,} LP^{f[k]}(\Gamma x \to \Gamma y). \qquad (Б.4)$$

Розглянемо значення $DP^f_{\max}$ і $DL^f_{\max}$ для випадків, коли як функції f виступають циклові перетворення і послідовності циклових перетворень ітеративних шифрів (ключезалежні функції), а також підстановлювальні перетворення (неключезалежні функції).

Нагадаємо також вирази для середніх ймовірностей *ADP*, *ALHP*,*MADP* і *MALHP* ключезалежної функції $f = f[k](x)$ з *n*-бітовим входом *x* і *n*-бітовим виходом, параметризовані ключем *k*, які використовуються в багатьох публікаціях по обґрунтуванню показників стійкості блокових шифрів.

Визначення 3. Середнє значення диференціальної ймовірності (*ADP*) функції $f[k](x)$ є

$$ADP^f = \underset{k}{ave}\, DP^{f[k]}(\Delta x \to \Delta y).$$

Визначення 4. Середнє значення ймовірності лінійного корпуса (*ALHP*) функції $f[k](x)$ є

$$ALHP^f = \underset{k}{ave} LP^{f[k]}(\Gamma x \to \Gamma y).$$

Визначення 5. Максимум середнього значення диференціальної ймовірності (*MADP*) і максимум середнього значення ймовірності лінійного корпусу (*MALHP*) функції$f = f[k](x)$ є

$$MADP^f = \max_{\Delta x \neq 0, \Delta y} ADP^f(\Delta x \to \Delta y). \quad (Б.5)$$

$$MALHP^f = \max_{\Gamma x,\, \Gamma y \neq 0} ALHP^f(\Gamma x \to \Gamma y). \quad (Б.6)$$

Зауважимо, що для *MALHP* використовується також позначення *MALP* — максимум середнього значення лінійної ймовірності.

Зауважимо також, що наведені тут визначення *MADP* і *MALHP*, повсюдно використовувані в публікаціях, як відмічено в [1, 6] не є адекватними завданню оцінці потенційних характеристик стійкості шифру до атак диференціального і лінійного криптоаналізу (вони характеризують лише максимуми середніх значень таких ймовірностей, обчислених для деякого фіксованого переходу $\Delta x \to \Delta y$або деякого фіксованого поєднання масок $|\Gamma x \to \Gamma y$). Більш адекватні (нові) визначення максимумів диференціальної і лінійної ймовірностей запропоновані в роботі [6] в такому вигляді.

Визначення 6 (*AMDP*). Середнє (по множині з 2^hключів) значення максимальної диференціальної ймовірності ключезалежної функції $f[k](x)$ є

$$ADMP^{f} = \underset{k}{ave}\, DP_{\max}^{f[k]} = \frac{1}{2^h}\sum_{k=1}^{2^h} DP_{\max}^{f[k]}(\Delta x \to \Delta y), \qquad (Б.7)$$

де 2^h–потужність використаної множини ключів зашифрування.

Визначення 7 (*AMPLH*). Середнє (по ключам) значення максимальної ймовірності лінійного корпусу функції $f[k](x)$ є

$$AMLHP^{f} = \underset{k}{ave} LP_{\max}^{f}(Гx \to Гy) = \frac{1}{2^h}\sum_{k=1}^{2^h} LP_{\max}^{f[k]}. \qquad (Б.8)$$

В обох випадках 2^h– потужність множини ключів шифрування, які використані при обчисленнях. Нагадаємо також розрахункові співвідношення для визначення максимальних значень диференціальної і лінійної ймовірностей підстановлювальних перетворень.

Визначення 8. Максимальна диференціальна ймовірність (максимальна ймовірність повного диференціалу) $DP_{\max}^{f}$ диференціальної таблиці підстановки визначається виразом

$$DP_{\max}^{f} = \frac{2k_D^*}{2^n}, \qquad (Б.9)$$

де $2k_D^* = k_{max}$– максимальне значення диференціальної таблиці підстановки.

Визначення 9. Максимальна лінійна ймовірність $DL_{\max}^{f}$ лінійної апроксимаційної таблиці (лінійної оболонки)підстановки визначається виразом

$$LP_{\max}^{f} = \left(\frac{2k_L^*}{2^{n-1}}\right)^2, \qquad (Б.10)$$

де $2k_L^* = k_{max}$–максимальне значення лінійної апроксимаційної таблиці підстановки.

Додаток В

Закони розподілу максимумів великих за обсягом вибірок незалежних однаково розподілених випадкових величин (за матеріалами публікації автора [20] з посиланнями на список літератури з дисертації)

В цьому додатку викладається математичний апарат, який вирішує в загальнотеоретичному плані задачу визначення розподілів максимумів над дуже великою множиною незалежних випадкових значень, запозичений з спільної роботи вчених Joan-a Daemen-a, Vincent-a Rijmen-a [92], в додатку до якої вдалося знайти цю методику. Наводиться переклад відповідного матеріалу з нашими виправленнями, викладеного в нашій роботі [20].

В.1 Закон розподілу максимумів

Розглядається випадок, коли всі значення множини незалежних випадкових змінних X мають одні і ті ж розподіли. Вважається, що їх щільності розподілу зменшуються експоненційно при великих значеннях X. Позначимо, пишуть автори [92], число таких значень 2^Y і скористаємося моделлю інтегрального розподілу $D(X)$ у вигляді

$$D(X) = 1 - e^{-f(X)} \tag{В.1}$$

(насправді, як буде видно з подальшого, автори цитованої роботи розглядають інтегральний розподіл у вигляді $D(X) = 1 - f(X)$, з $f(X)$ – функцією, яка описує щільності розподілу ймовірностей незалежних значень X.

З порядкових статистик [98,99] відомо, відзначають вони, що цей інтегральний розподіл максимального числа значень є добутком інтегральних розподілів цих значень. В цьому разі маємо:

$$D_{\max}(X) = D(X)^{2^Y} = (1 - e^{-f(X)})^{2^Y} \approx e^{-2^Y e^{-f(X)}} = e^{-e^{\ln(2)Y - f(X)}} \tag{В.2}$$

Насправді тут повинен бути записаний результат:

$$D_{\max}(X) = D(X)^{2^Y} = (1 - f(X))^{2^Y} \approx e^{-2^Y \cdot f(X)} = e^{-e^{\ln(2)Y + \ln f(X)}}.$$

Ми можемо апроксимувати функцію $ln(2)Y - f(X)$ (повинно бути $ln(2)Y + ln\, f\,(X)$), говорять автори роботи [92], лінійною функцією в околиці точки, де функція близька до нуля. Нехай a буде рішенням рівняння$ln(2)Y = f(X)$ (повинно бути рівняння $ln(2)Y = -\,ln\, f\,(X)$) і нехай b буде одиницею, поділеною на похідну функції $-f(X)$ (повинно бути поділеною на похідну функції – ln$f$(X))) в точці a. Тоді справедливий вираз

$$D_{\max}(X) \approx e^{-e^{\frac{a-X}{b}}} \qquad \text{(В.3)}$$

Цей розподіл добре вивчений в теорії ймовірностей, відзначається в [109] і відомий, як розподіл екстремальних значень, Fisher-Tippett розподіл або лог-Вейбулла розподіл [98;99]. Відповідна щільність зображена на рис. Б.1, запозиченого із цитованої роботи [92]. Відзначається, що пік цієї функції є a, а

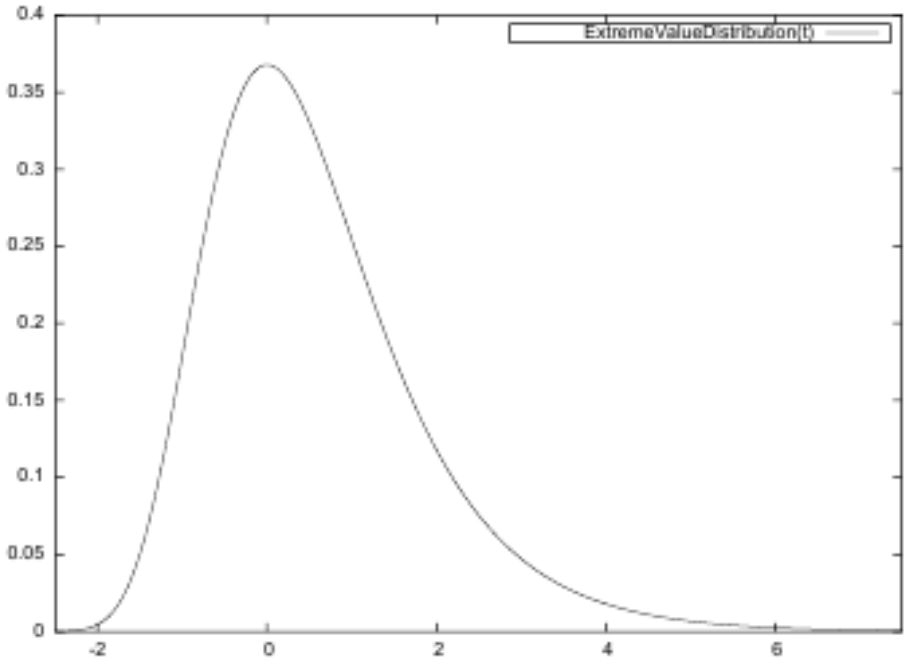

Рис. В.1. Розподіл екстремальних значень при a = 0, b = 1/

її ширина пропорційна b. Цей розподіл має математичне сподівання $\mu(X) = a + b\gamma$ з $\gamma \approx 0{,}58$ і середньоквадратичне відхилення $\frac{\pi}{\sqrt{6}}b \approx 1{,}3b$. Автори зауважують, що справедливість виразу (Б.3) залежить від якості лінійної апроксимації функції поблизу точки (a,0). Далі автори роботи [92] конкретизують уявлення

щільності ймовірності (Б.3) для змінних, що підкоряються деяким відомим законам розподілу. Нас будуть цікавити два закони розподілу: пуасонівский і нормальний, котрі як раз розглянуті в роботі [92]. Перший відповідає закону розподілу ймовірностей переходів XOR таблиці випадкової підстановки (шифру), другий – закону розподілу ймовірностей зміщень таблиці лінійних апроксимацій випадкової підстановки (шифру).

В.1.1 Максимум над *X* з пуасонівським розподілом

Якщо максимум береться за змінними з розподілом Пуассона, ми, зауважують автори цитованої роботи, повинні брати до уваги дискретний характер останнього. Однак, пишуть вони, можна отримати вирази для середнього значення і стандартного відхилення максимумів, якщо наблизити розподіл Пуассона безперервною функцією. Маємо:

$$\Phi(i;\lambda) = \sum_{x=0}^{i-1} \text{Poisson}\,(x;\lambda) = 1 - \sum_{x \geq i} \text{Poisson}\,(x;\lambda). \qquad \text{(В.4)}$$

Для $i >> \lambda$, цей вираз відповідно до [98,99] апроксимується так:

$$\Phi(i;\lambda) \approx 1 - \left(1 - \frac{\lambda}{i}\right) \cdot \text{Poisson}\,(i;\lambda) \approx 1 - \text{Poisson}\,(i,\lambda) = 1 - e^{-\lambda}\frac{\lambda^i}{i!} = 1 - f(i). \qquad \text{(В.5)}$$

Далі, використовуючи наближення Стірлінга для факторіала: $n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$ [92], можемо отримати такий вираз для $ln\ f\ (i)$

$$\ln f(i) = -\frac{1}{2}\ln(2\pi) - \lambda + i\ln\lambda - (\ln i - 1)i - \frac{1}{2}\ln(i). \qquad \text{(В.6)}$$

Якщо тепер абстрагуватися від факту, що i має бути цілим числом, то можна обчислити параметр а шляхом вирішення рівняння:

$$\ln(2)y = \frac{1}{2}\ln(2\pi) + \lambda - i\ln\lambda + (\ln i - 1)i + \frac{1}{2}\ln(i), \qquad \text{(В.7)}$$

або, що еквівалентно:

$$i = \frac{\ln(2)y - \frac{1}{2}\ln(2\pi i) - \lambda}{\ln\left(\frac{i}{\lambda}\right) - 1}. \quad \text{(B.8)}$$

Останнє рівняння може бути вирішено ітеративне. Похідна $f(i)$ (повинно бути похідна – ln$f(x)$) визначається за формулою:

$$\ln\left(\frac{i}{\lambda}\right) + \frac{1}{2i}. \quad \text{(B.9)}$$

Визначивши $i = a$ і використовуючи умову $a>>\lambda$, маємо:

$$b = \frac{1}{\ln\left(\frac{a}{\lambda}\right)}. \quad \text{(B.10)}$$

Звідси випливає, укладають автори цитованої роботи, що якщо a набагато більше, ніж λ, стандартне відхилення стає менше 1.

Оскільки розподіл максимуму дискретний, то ця мала величина стандартного відхилення призводить до того, що розподіл зосереджено в двох цілочисельних значеннях поблизу значення a.

B.1.2 Максимуми над X з нормальним розподілом

Тут розглядається окремий випадок, для змінної x зі стандартним нормальним розподілом. Ми маємо (цитуються результати з роботи [92]):

$$D(x) \approx \int_{-\infty}^{\infty} Z(u)\, du. \quad \text{(B.11)}$$

При великих x, цей інтегральний розподіл, стає близьким до [92]:

$$D(x) \approx 1 - \frac{1}{x} Z(x) \approx 1 - \frac{1}{x\sqrt{2\pi}} e^{-\frac{x^2}{2}}. \quad \text{(B.12)}$$

З цього результату отриманий такий вираз для $ln\, f\,(x)$:

$$-\ln f(x) = -\ln\left(\frac{1}{x}Z(x)\right) = \frac{1}{2}\ln(2\pi) + x^2 + \ln(x). \quad \text{(B.13)}$$

Параметр a_s (підрядковий індекс s для стандарту) є рішенням рівняння

$$a_s = \sqrt{2\,ln(2)y - ln(2\pi) - 2\,ln(a_s)}, \quad \text{(B.14)}$$

яке може бути знайдено ітеративним шляхом, не звертаючи уваги на правий член в першій ітерації. Похідна $f(x)$ визначається за формулою:

$$x + \frac{1}{x}, \quad \text{(B.15)}$$

і, отже,

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s}. \quad \text{(B.16)}$$

Грубо кажучи, максимум має розподіл із середнім значенням $1{,}17\sqrt{y}$ і стандартним відхиленням $1{,}11/\sqrt{y}$ [89]. Ми, відзначають автори роботи [92], можемо знайти значення a і b для будь-якого нормального розподілу із середнім $\mu(X)$ і стандартним відхиленням σ замінивши x на $\frac{X-\mu(X)}{\sigma}$. Це дає:

$$\begin{aligned} a &= \sigma a_s - \mu(X), \\ b &= \sigma b_s \end{aligned} \quad \text{(B.17)}$$

Наведені теоретичні результати і є ті, на які ми будемо орієнтуватися при проведенні розрахунків і експериментів.

Додаток Г

Стислий опис шифру Мухомор

Тут шифр Мухомор виступає прототипом розробки, тому нагадаємо конструкцію циклової функції шифру Мухомор [45]. Вона представлена узагальненими схемами рис. Г.1 і рис. Г.2.

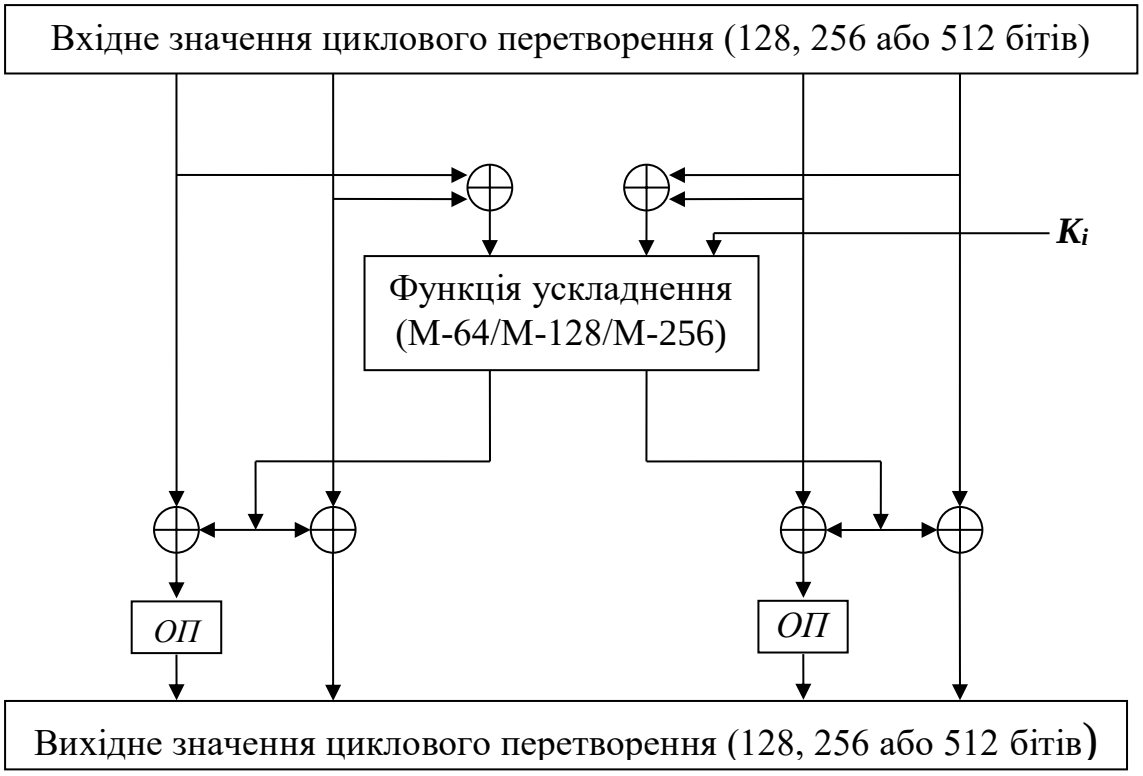

Рис. Г.1 Циклове перетворення алгоритму Мухомор

На вхід циклового перетворення шифру Мухомор подається блок даних, що співпадає за розміром з відкритим текстом (128, 256 або 512 бітів) і підключ K_1.

Вхідний блок даних розбивається на 4 рівних підблоки.

При розмірі блоку відкритого тексту 512 бітів функція ускладнення / М-256 приймає черговий 256-бітовий підключ K_i і два 128-бітні значення, перше з яких обчислюється як різниця за модулем 2 (XOR) між першим і другим підблоками даних на вході циклу, відповідно друге вхідне значення – різниця між третім і четвертим підблоками даних на вході циклу.

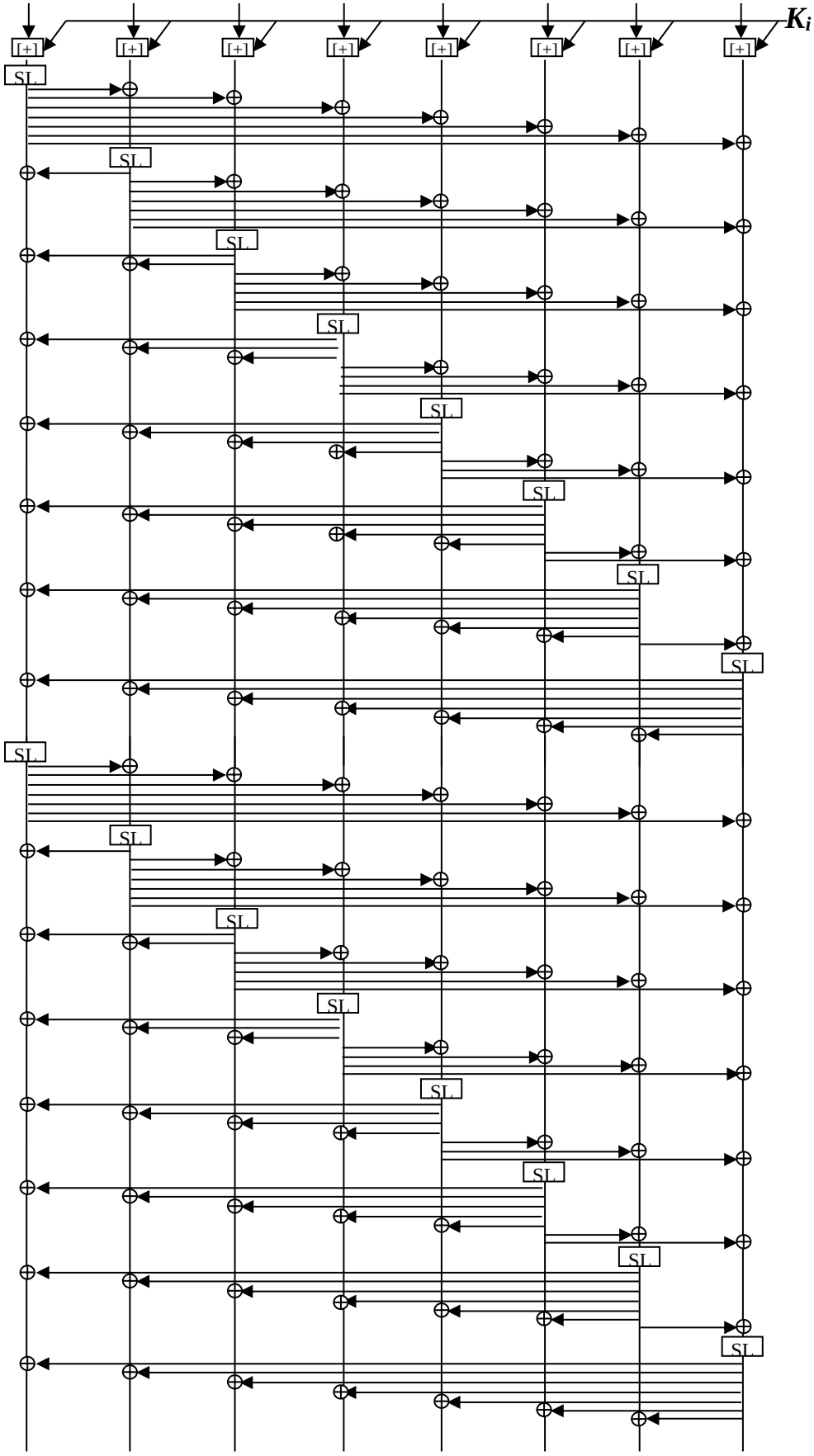

Рис. Г.2 Функція ускладнення M-256

Вихідне значення функції складається за модулем 2 з вихідними значеннями, після чого перший та третій підблоки обробляються операцією ортогонального перетворення (*ОП*).

Наведемо короткий опис операцій, які виконуються функцією ускладнення M-256 (див. Рис. В. 2).

128 бітні підблоки на вході функції ускладнення поділяються на 4-ри 32-х бітних сегменти (слова), формуючи результуючу послідовність з 8-ми таких 32-ох бітних сегментів (наборів), і далі робота йде вже з цими послідовними наборами (значеннями).

Кожне з 32-бітових вхідних значень функції M-256 складається за модулем 2^{32} з відповідною частиною чергового циклового підключа, поданого на вхід циклової функції. Потім кожне з отриманих 32-бітних слів проходить через своє SL перетворення, причому результат кожного перетворення складається за модулем 2 з усіма іншими результатами.

Описана операція виконується 2 рази (два шари SL-перетворень). Ліве вихідне 128 бітове слово формується як результат конкатенації чотирьох лівих 32-бітних слів, праве 128 бітове слово – як результат конкатенації чотирьох правих 32-х бітних слів.

SL перетворення шифру Мухомор. SL перетворення є основним елементом циклової функції. Схема SL перетворення наведена на рис. Г.3.

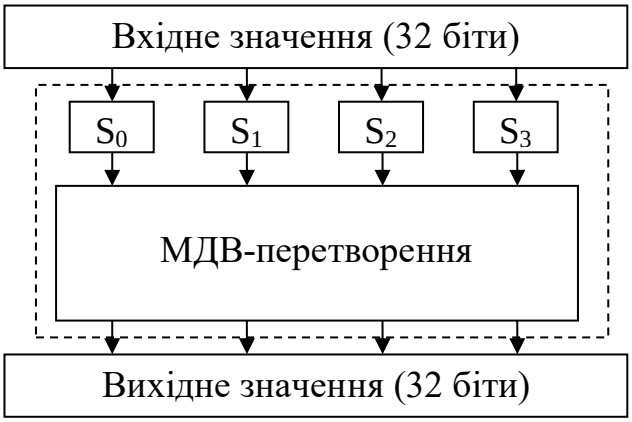

Рис. Г.3 SL-перетворення

Вхідне 32-бітове значення ділиться на 4 байти, кожен з яких замінюється відповідно до заданої таблиці підстановки. У перетворенні використовується 4-ри різні таблиці, по одній на кожен байт.

Після операції заміни в S-блоках 4 байти (a_0,a_1,a_2,a_3) подаються на вхід МДВ перетворення, яке виконує матричне множення наступного виду:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 02 \cdot a_0 \oplus 03 \cdot a_1 \oplus 01 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 02 \cdot a_1 \oplus 03 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 01 \cdot a_1 \oplus 02 \cdot a_2 \oplus 03 \cdot a_3 \\ 03 \cdot a_0 \oplus 01 \cdot a_1 \oplus 01 \cdot a_2 \oplus 02 \cdot a_3 \end{bmatrix}.$$

Матриця МДВ перетворення шифру Мухомор збігається з матрицею лінійного перетворення алгоритму Rijndael-AES, але при обчисленні добутку елементів вектору на матричні коефіцієнти у шифрі Мухомор використовується інший поліном

$$m(x) = x^8 + x^4 + x^3 + x^2 + 1,$$

або {01}{1d} в шістнадцятковому поданні.

Вихідний 32-бітний вектор МДВ перетворення (b_0,b_1,b_2,b_3) є вихідним значенням SL перетворення.

Додаток Д

Акти впровадження результатів роботи

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
Харківського національного університету
імені В.Н. Каразіна
Академік НАН України
професор. _____ М.О. Азаренков
"10" 04 2018

АКТ

впровадження результатів дисертаційних досліджень аспіранта факультету комп'ютерних наук Харківського національного університету імені В.Н. Каразіна Лисицького К.Є. в навчальний процес.

Комісія у складі голови комісії, доктора технічних наук, доцента Рассомахіна С.Г., та членів комісії, доктора технічних наук, професора Кузнецова О.О. та доктора технічних наук, доцента Олійникова Р.В. встановила, що у Харківському національному університеті імені В.Н. Каразіна впроваджені наступні результати, що одержані Лисицьким Костянтином Євгенійовичем

1. По дисципліні "Криптологічні методи в кібербезпекі" для магістрів спеціальності "Кібербезпека" при підготовці та читанні лекцій для магістрів спеціальності "Безпека інформаційних і комунікаційних систем" за темою "Нова методологія оцінки стійкості БСШ до атак диференційного та лінійного криптоаналізу", зокрема безпосередньо використані результати застосування цієї методології для визначення показників доказової стійкості стандартизованого шифру "Калина-2", нового шифру з білоруського стандарту та нової розробки по створенню криптоалгоритму, що задовольняє умовам використання у пост-квантовому періоді розвитку криптографії.

2. Результати дослідження диференціальних властивостей випадкових підстановок та формули по визначенню максимумів XOR таблиць та зміщень таблиць лінійних апроксимацій випадкових підстановок використані при курсовому проектуванні з дисципліни "Прикладна криптологія", а також при виконанні магістерських дипломних робіт.

Голова комісії д.т.н., доцент. С.Г. Рассомахін

Члени комісії:
д.т.н., професор О.О. Кузнецов

д.т.н., доцент Р.В. Олійников

"ЗАТВЕРДЖУЮ"

Виконавчий директор

АТ «ІІТ»

_____Кравченко В.Д.

"__" ____ 2018

АКТ

впровадження результатів наукових досліджень

аспіранта Харківського національного університету ім.. В.Н. Каразіна

Лисицького Костянтина Євгенійовича

в діяльність Приватного Акціонерного Товариства «Інститут інформаційних Технологій»

Комісія у складі голови комісії, кандидата технічних наук, першого заступника головного конструктора АТ "ІІТ" Горбенко Ю.І., та членів комісії, заступника головного конструктора АТ "ІІТ", кандидата технічних наук, професора Качко О.Г., технічного директора АТ "ІІТ" Шумова 0.І. з'ясувала наступне.

Протягом 2013 – 2017 років фахівцями АТ «Інституту інформаційних технологій» впроваджено на практиці результати та розробки аспіранта Харківського національного університету ім.. В.Н. Каразіна Лисицького Костянтина Євгенійовича, зокрема розвинуті підходи та методи були використані для порівняльного аналізу шифрів, представлених в свій час на Український конкурс по вибору національного стандарту блочного симетричного шифрування України, а пізніше при дослідженні шифру Калина-2, що став національним стандартом. Розробки останнього часу визначають напрям подальшого вдосконалення властивостей і показників доказової безпеки блочних симетричних шифрів, орієнтованих на використання в пост-квантовому періоді розвитку криптографії.

Ми тут відмітимо також монографію, підготовану Лисицким К.Є. "Динамические показатели прихода блочных шифров к состоянию случайной подстановки" / К.Е. Лисицкий // Издательский дом LAP LAMBERT Academic Publishing, 2014, 60 с. ISBN-13: 978-3-659-28919-4, наукові результати якої використані співробітниками АТ "ІІТ"-а для обґрунтування показників випадковості нового стандарту симетричного шифрування України та останніх розробок по поточному шифру "Струмок".

Голова комісії: перший заступник
головного конструктора АТ "ІІТ" Ю.І. Горбенко

Члени комісії:
Зам. головного конструктор АТ "ІІТ"
кандидат технічних наук, професор О.Г. Качко

Технічний директор АТ "ІІТ" О.І. Шумов

"ЗАТВЕРДЖУЮ"

Перший проректор з наукової роботи
Харківського національного
університету імені В.Н. Каразіна

В. Катрич

"15" 04 2018 р.

Акт

впровадження результатів наукових досліджень аспіранта Харківського національного університету імені В.Н. Каразіна Лисицького Костянтина Євгенійовича в наукову роботу кафедри БІСТ. Харківського національного університету імені В.Н. Каразіна.

Комісія у складі голови комісії, доктора технічних наук, доцента Рассомахіна С.Г., та членів комісії, доктора технічних наук, професора Кузнецова О.О. та доктора технічних наук, доцента Олійникова Р.В.. встановила, що у Харківському національному університеті імені В.Н. Каразіна впроваджені результати, що одержані Лисицьким Костянтином Євгенійовичем, при виконанні наступних науково-дослідних робіт:

1. "Аналіз стану, обґрунтування вимог та напрямків розвитку, стандартизація розробки та впровадження криптографічних систем для надання електронних довірчих послуг" (номер державної реєстрації 0116U000810). Наказ МОН України № 158 від 26.02.2016 р. в частині застосування перспективних методів оцінки стійкості стандартів та оціни показників їх випадковості.

2. «Механізми, методи та засоби криптографічного захисту інформації та стандартизації у перехідний та пост-квантовий період» (тема № 38-17 (від 30.06.2017 р.). Замовник ПАТ «ІІТ», м. Харків, в частині розробки вдосконалених методів проектування БСШ.

Голова комісії д.т.н., доцент. С.Г. Рассомахін

Члени комісії:

д.т.н., професор О.О. Кузнецов

д.т.н. доцент Р.В. Олійников

"ЗАТВЕРДЖУЮ"

Проректор з науково-методичної роботи

Харківського національного університету

радіоелектроніки

професор. _____ І.В. Рубан

„14" 05 2018

Акт

впровадження результатів наукових досліджень аспіранта Харківського національного університету імені В.Н. Каразіна Лисицького Костянтина Євгенійовича в наукову роботу кафедри БІТ Харківського національного університету радіоелектроніки.

Комісія у складі голови комісії, доктора технічних наук, доцента Халімова Г.З., та членів комісії, доктора технічних наук, професора Заболотного В.І. та кандидата технічних наук, доцента Сєвєрінова О.В. встановила, що у Харківському національному університеті радіоелектроніки результати досліджень, що одержані Лисицьким Костянтином Євгенійовичем використані при виконанні наступних науково-дослідних робіт:

«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);

«Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій» (ДР № 0111U002634) та інших, в частині формування нової методології оцінки стійкості блочних симетричних шифрів.

Голова комісії д.т.н., професор. Г.З. Халімов

Члени комісії:

д.т.н., професор В.І. Заболотний

к.т.н., доцент О.В. Сєвєрінов