ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

НЕСТЕРЕНКО Оксана Борисівна

УДК 004.056.55:004.312.2

ДИСЕРТАЦІЯ

МЕТОДИ ТА ЗАСОБИ СИНТЕЗУ ОПЕРАЦІЙ ПОТОКОВОГО ШИФРУВАННЯ ЗА КРИТЕРІЄМ СТРОГОГО СТІЙКОГО КОДУВАННЯ

05.13.05 – комп’ютерні системи та компоненти

Подається на здобуття наукового ступеня кандидата технічних наук

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

О.Б. НЕСТЕРЕНКО

Науковий керівник Рудницький Володимир Миколайович, доктор технічних наук, професор

Черкаси - 2019

АНОТАЦІЯ

Нестеренко О.Б. Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.05 «комп'ютерні системи та компоненти» (123 – комп'ютерна інженерія). – Черкаський державний технологічний університет, Черкаси, 2019.

Дисертаційна робота присвячена підвищенню невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення й синтезованих за критерієм строгого стійкого кодування.

Перший розділ присвячений аналізу якості систем криптографічного перетворення інформації. Обґрунтовується актуальність і необхідність проведення аналізу якості криптографічних систем. Проводиться огляд сучасних вимог до криптографічних систем та вибираються вимоги, які доцільно використовувати в даному дисертаційному дослідженні. Для подальшого дослідження проводиться аналіз відомих досліджень стосовно лавинного ефекту, який оцінюється критерієм строгого лавинного ефекту. Детально аналізуються властивості лавинного ефекту та критерії їх оцінки. Проводиться огляд наукових досліджень стосовно надійності та безпеки криптографічних систем. Аналізуються підходи до оцінки стійкості криптографічних алгоритмів. Розглядаються атаки на криптоалгоритми, уточнюються особливості атак на асиметричну криптосистему. Розглядаються аспекти і чинники надійності криптосистем. На основі проведеного аналітичного огляду сучасного стану та тенденцій розвитку комп'ютерної криптографії формулюються мета і задачі наукового дослідження. Другий розділ присвячений дослідженню двохрозрядних операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування. Проведене дослідження двохрозрядних

елементарних функцій для криптоперетворення на відповідність критерію строгого лавинного ефекту показало, що жодна з елементарних функцій, на основі яких будуються операції криптоперетворення, не відповідають вимогам критерію, бо не забезпечують зміну половини бітів інформації на повній множині вхідних даних. По аналогії із критерієм строгого лавинного ефекту, для оцінки якості операцій крипто перетворень, було запропоновано ввести критерій строгого стійкого кодування. Криптографічний алгоритм, або операція криптографічного перетворення інформації задовольняє критерією строгого стійкого криптографічного кодування, якщо незалежно від ключової послідовності та вхідної інформації кожний біт вихідної послідовності змінюється відносно вхідної інформації з імовірністю одна друга. В процесі досліджень визначені чотири двох розрядні операціїх яці відповідають критерію строгого стійкого кодування. Встановлено наступне: якщо в двохрозрядних операціях інвертується один з переставлених бітів, то інверсія буде «плаваючою», а отже, біт буде інвертуватися і визначатися не тільки інверсією розряду в операції, а й вхідною інформацією. Відзначений факт показує можливість створення потокових шифрів, у яких результат побітового шифрування залежить не тільки від значення бітів гамуючої послідовності, а й від значення бітів інформації, яка шифрується. Третій розділ присвячено розробці методу синтезу операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування. Запропоновано етапи побудови чртирьох двохоперандних операцій, які досліджено: будується таблиця відстаней за Хеммінгом; видаляються з таблиці значення відстаней всі, крім одиниці; замінивши в кожному рядку однакові значення відстаней, що залишилися, значенням рядка, отримаємо проміжну таблицю вибору варіантів підстановки; видаливши зсувом пусті клітинки, отримаємо таблицю вибору варіантів підстановки; послідовним вибором у кожному стовпчику результату шифрування значення першого рядка, не допускаючи повторів, отримаємо

варіанти таблиць підстановок Виконавши мінімізацію таблиць підстановки як таблиць істинності операцій перетворення, отримаємо відомі нам чотири операції. Узагальнивши отримані результати, було побудовано метод синтезу операцій за критерієм строгого стійкого кодування. Встановлено, що якщо крипто перетворення відповідаює вимогам критерію строгого стійкого криптографічного кодування, то виконання декількох раундів не приводить до підвищення невизначеності результатів шифрування. Четвертий розділ присвячено розробці методу синтезу операцій криптографічного перетворення інформації мінімальної складності та оцінці можливості застосування синтезованих операцій у потоковому шифруванні. В процесі синтезу і аналізу моделей операцій, які відповідають критерію строгого стійкого кодування, було відмічено, що складність моделей відрізняється, а моделі операцій, які мають найменшу складність, складаються лише з перестановок і інверсій. Узявши це припущення за основу моделювання операцій, було отримано 42 чотирьохрозрядні операції. На основі отриманих результатів було сформульовано метод синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування. Сутність методу полягає в наступному: синтез операцій, які задовольняють критерію строгого стійкого кодування і мають мінімальну складність, проводиться на основі парних перестановок та інверсії, шляхом інверсії половини бітів, за умови однієї інверсії в кожній парній перестановці. Для вирішення третьої наукової задачі були запропоновано використовувати синтезовані операції потокового шифрування, в блоці шифрування. Вибір операцій проводити під управлінням гамуючої послідоверсті, яка модифікується в другий операнда операції. Удосконалення методів синтезу програмно-апаратних засобів комп'ютерної криптографії полягає в побудові операцій криптоперетворення мінімальної складності без виконання етапів синтезу таблиць істинності та етапу мінімізації логічних функцій. Для апаратної реалізації потокового шифрування

максимальної невизначеності побудовано варіанти функціональних схем пристроїв криптоперетворення. Наводиться варіант алгоритму програмної реалізації високошвидкісного шифрування інформації з забезпеченням максимальної невизначеності результатів перетворення. Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS, крім того, застосування даних послідовностей в імовірнісних моделях, забезпечило підвищення точності моделювання.

Наукова новизна отриманих результатів:

- вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;
- вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;
- набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування, шляхом застосування методів синтезу моделей операцій з новими властивостями, які забезпечили спрощення процесу синтезу програмних і апаратних криптографічних засобів і дозволили реалізувати синтез аналогічних засобів мінімальної складності без побудови таблиць істинності та мінімізації.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні розроблених методів до моделей, функціональних схем і програмних модулів для реалізації операцій потокового шифрування, які гарантовано забезпечують зміну кожного біта інформації з імовірністю одна друга.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS. Крім того, застосування цих послідовностей в імовірнісних моделях на прикладі інтегральної моделі розвитку і припинення пожежі забезпечило підвищення точності моделювання.

Акти впровадження результатів дисертаційного дослідження додатково підкреслюють практичну цінність роботи.

Реалізація. Дисертаційна робота виконувалася відповідно до планів НДР Черкаського інституту пожежної безпеки ім. Героїв Чорнобиля Національного Університету цивільного захисту України та Черкаського державного технологічного університету. Одержані в ній теоретичні й практичні результати використані та впроваджені у таких закладах:

– Черкаський державний технологічний університет на кафедрі інформаційної безпеки та комп'ютерної інженерії – у матеріалах лекційних курсів «Основи криптографічного захисту інформації», «Комп'ютерні методи та засоби захисту інформації». Акт впровадження від 20.06.2017 р.;

– Приватне підприємство «Сенсорна Електроніка» – для забезпечення конкурентоспроможності та переваги над аналогами на ринках електронної техніки в частині пристроїв захисту інформації. Акт впровадження від 20.12.2018 р.

Ключові слова: захист комп'ютерної інформації, потокові шифри, операції криптографічного перетворення, синтез операцій, складність, стійкість, надійність.

ABSTRACT

Nesterenko O.B. The methods and means of synthesizing the stream ciphering operations on the criterion of strict stable coding. – Qualification scientific work with the manuscript copyright.

The thesis for a candidate of technical science degree in speciality (PhD) 05.13.05 "Computer Systems and Components" (123 – Computer Engineering). – Cherkasy State Technological University, Cherkasy, 2019.

The dissertation is devoted to increasing the uncertainty of the results of stream ciphering due to the using new operations of cryptographic transformation and synthesized by the criterion of strict stable coding.

The first chapter is devoted to the analysis of the quality of cryptographic information transformation systems. The relevance and necessity of the analysis of quality of cryptographic systems is substantiated. An overview of modern requirements for cryptographic systems is carried out and the requirements that are appropriate to be used in this dissertation study are selected. For further research, a analysis of well-known studies is carried out in relation to the avalanche effect, which is assessed by the criterion of strict avalanche effect. The properties of the avalanche effect and the criteria for their evaluation are analyzed in detail. A review of scientific studies on the reliability and security of cryptographic systems. The approaches to assessing the stability of cryptographic algorithms are analyzed. Cryptographic algorithms attacks are considered, peculiarities of asymmetric cryptosystem attacks are specified. The aspects and factors of cryptosystem reliability are considered. On the basis of the conducted analytical review of the current state and trends in the development of computer cryptography, the purpose and objectives of scientific research are formulated. The second chapter is devoted to the study of two-digit operations of cryptographic information transformation on the criterion of strict stable cryptographic coding. Conducted research of two-digit elementary functions for cryptographic transformation to match the criterion of strict avalanche effect has shown that none of the elementary

functions on the basis of which cryptographic transformation operations synthesed do not meet the requirements of the criterion because they do not provide a change in the half of the information bits on the complete set of input data. By analogy with the criterion of strict avalanche effect, for the evaluation of the quality of cryptographic transformations operations, it was proposed to introduce the criterion of strict stable coding. A cryptographic algorithm or a cryptographic information transformation operation satisfies the criterion of strict stable cryptographic encoding, if, regardless of the key sequence and the input data, each bit of the original sequence changes relative to the input data with the probability of 1/2. In the process of research identified four two-bit operations that meet the criteria of strict stable coding. The following is established: if two-bit operations invert one of the permuted bits, then the inversion will be "floating", and hence, the bit will be inverted and determined not only the inversion of the bit in the operation, but also the input information. The noted fact shows the possibility of creating stream ciphers, in which the result of bitwise encryption depends not only on the value of the bits of the fetch sequence, but also on the value of the bits of data that is encrypted. The third chapter is devoted to the development of a method for synthesizing cryptographic information transformation operations based on the criterion of strict stable cryptographic coding. The stages of construction of four two-operand operations that have been investigated are proposed: a distances table on Hamming is being constructed; the values of distances are removed from the table, except for the one; replacing in each row the same values of the remaining distances, the value of the row, we obtain an intermediate table of the choice of permutation options; removing the empty cells from the shift, we get a table for selecting permutation options; sequential selection in each encryption result column the value of the first row, not allowing repetitions, we get variants of permutation tables; by completing the minimization of the permutation tables as truth tables of the transformation operations, we get four operations known to us. Summing up the obtained results, the method of synthesizing operations was constructed according to the criterion of strict stable

coding. It is established that if the cryptographic transformation meets the requirements of the criterion for strict stable cryptographic coding, then performing multiple circles of encryption does not increase the uncertainty of the encryption results. The fourth chapter is devoted to the development of a method for synthesizing cryptographic information transformation operations of minimal complexity and to assess the possibility of using synthesized operations in stream ciphering. In the process of synthesis and analysis of operations models that meet the criterion of strictly stable coding, it was noted that the complexity of the models is different, while the models of operations that have the least complexity consist only of permutations and inversions. Taking this assumption as the basis for the simulation of operations, 42 four-digit operations were received. On the basis of the obtained results the method of synthesizing cryptographic information transformation operations of minimal complexity according to the criterion of strict stable coding was formulated. The essence of the method is as follows. Synthesis of operations that satisfy the criterion of strict stable coding and have minimal complexity is made on the basis of pairwise permutations and inversion by inversion of half bits, provided one inversion in each pairwise permutation. To solve the third scientific task, it was proposed to use synthesized stream ciphering operations in the encryption block. Selection of operations carried out under controlled the fetch sequence is modified in the second operand operations. Improvement of the methods of synthesis of computer cryptography software and hardware consists in the construction of cryptographic transformation operations of minimal complexity without the steps of the synthesis of truth tables and the phase of logical functions minimization. For hardware implementation of stream ciphering of maximum uncertainty, variants of functional schemes of cryptographic transformation devices are constructed. The variant of software implementation algorithm of high-speed ciphering with the maximum uncertainty of transformation results is presented. Application of the models in the stream ciphering algorithms

ensures that the generated sequence requirements NIST_STS. In addition, the application of these sequences in probabilistic models improved modeling accuracy.

Scientific novelty of the obtained results:

- For the first time, a method for the synthesis of operations on the criterion of strictly stable coding was developed by using the minimal distances table on Hamming to construct the truth tables of discrete models that provide the maximum uncertainty of the results of the transformation and increasing the variability of cryptographic algorithms;
- For the first time, a method for the synthesis of operations on the criterion of strictly stable coding of minimal complexity was developed on the basis of the use of permutation and gamma operations, by the established restrictions and dependencies between transformation operations and the minimum distances on Hamming, which provide the maximum uncertainty of the transformation results with practically the minimal complexity of the circuit design and software implementation;
- have further developed methods of synthesis of software and hardware cryptographic means of computer technology on the basis of the using a new group of operations built on the criterion of strictly stable coding, by applying methods for synthesizing models of operations with new properties, which provided a simplification of the process of synthesis of software and hardware cryptographic means and allowed realize the synthesis of similar means of minimal complexity without constructing truth tables and minimizing them.

Practical significance of obtained results. The practical value of work is to bring developed methods to models , the functional schemes and software modules for implementating of stream ciphering operations that are guaranteed to provide a change in each bit of information with the probability of 1/2.

Application of the models in the stream ciphering algorithms ensures that the generated sequence requirements NIST_STS. In addition, the application of these

sequences in probabilistic models on the example of an integral model of fire propagation and termination improved modeling accuracy.

Implementing acts of results of the dissertation research further emphasize the practical significance of the study.

Implementation. The dissertational work was carried out in accordance with plan of research scientific work of Cherkasy Institute of Fire Safety named after Chornobyl Heroes of National University of Civil Protection of Ukraine and Cherkassy State Technological University. Obtained theoretical and practical results are used and implemented in such institutions:

– Cherkasy State Technological University at the Department of Information Security and Computer Engineering in materials of lecture courses “Basics of Cryptographic Protection of Information”, “Computer Methods and Means of Information Protection”. The implementing act from 20 June, 2017;

– Private Enterprise "Sensory Electronics" in order to ensure the competitiveness and advantages over analogues in the markets of electronic equipment in the part of information security devices. The implementing act from 20 December, 2018.

Keywords: the computer information protection, stream ciphers, cryptographic transformation operations, operations’ synthesis, complexity, stability, reliability.

Список публікацій здобувача:

1. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків: ХУПС ім. І. Кожедуба, 2015. С. 129–134.

2. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Аналіз дворозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту. *Наукові праці:* наук.-метод. журн. Чорномор. держ. ун-ту ім. Петра Могили. Миколаїв, 2017.

3. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник інженерної академії України:* часопис. Київ, 2016. Вип. 3. С. 105–108.

4. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. Вип. 1. С. 5–10.

5. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Побудова примітивів строгого стійкого кодування мінімальної складності. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2018. Вип. 1. С. 21–26.

6. Рудницький В. М., Лада Н. В., Федотова-Півень І. М., Пустовіт М. О., Нестеренко О. Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Системи управління, навігації та зв'язку:* зб. наук. праць ПНТУ ім. Юрія Кондратюка. 2018. Вип. 6 (52). С. 113–115.

7. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики*. Харків, 2014. Вип. 168. С. 53–58.

8. Нестеренко О. Б. Исследование двухразрядных операций, удовлетворяющих критерию строгого стойкого кодирования, при многораундовом криптографическом преобразовании. *Wschodnioeuropejskie Czasopismo Naukowe* (East European sci. journal). 2018. No. 11 (39), part 2. С. 20–28. (Варшава, Польща).

9. Криптографічне кодування: обробка та захист інформації: кол. монографія / під ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

10. Бабенко В. Г., Нестеренко О. Б., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації*: тези доп. Другої міжнар. наук.-техн. конф. (Черкаси – Тольятті, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

11. Зажома В. М., Нестеренко О. Б. Генерація псевдовипадкових послідовностей на основі фільтрації матричних операцій криптоперетворення. *Проблеми інформатизації:* тези доп. Третьої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2015. 84 с.

12. Зажома В. М., Нестеренко О. Б. Вдосконалений метод вбудовування стегоповідомлення на основі ключового елементу. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої міжнар. наук.-техн. конф. (Полтава – Баку – Кіровоград – Харків). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2015. 72 с.

13. Шувалова Л. А., Нестеренко О. Б. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування. *Проблеми інформатизації*: тези доп. Четвертої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. С. 97.

14. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування . *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

15. Пустовіт М. О., Нестеренко О. Б., Матяш П. В. Моделювання розпилених водяних струменів для комп'ютеризованих симуляторів з гасіння пожеж в будівлях. Техника и технология. *Актуальные научные проблемы. Рассмотрение, решение, практика.* Гданьск, 2015. С. 22.

16. Пустовіт М. О., Нестеренко О. Б., Жаврук П. С. Комп'ютерне моделювання розпорошених водяних струменів для симулятора припинення горіння. *Надзвичайні ситуації: безпека та захист:* матеріали всеукр. наук.-практ. конф. з міжнар. участю. Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2015. С. 311–314.

17. Нестеренко О. Б. Двораундове криптографічне кодування операціями зі строгим лавинним ефектом. *Проблеми та перспективи цивільного захисту:* матеріали міжнар. наук.-практ. конф. молодих учених (29–30 берез. 2017 р.). Харків: НУЦЗУ. С. 384.

18. Нестеренко О. Б. Вдосконалення систем моніторингу з надзвичайних ситуацій. *Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика).* Харків, 2014. С. 55.

ЗМІСТ

ВСТУП

Актуальність теми. Проблема захисту інформації завжди була, є і буде актуальною. На сьогоднішній день ця проблема стала принципово важливою для Державної служби України з надзвичайних ситуацій. Особливо велике значення має оперативність, достовірність і конфіденційність інформації для управління підрозділами в кризових ситуаціях, адже від них залежить безпека та життя людей.

За останні десятиліття значно зросла кількість робіт, пов'язаних із криптографією та криптоаналізом, які опубліковані у відкритих наукових виданнях. Накопичений значний теоретичний і практичний потенціал використовується не тільки для побудови, а і для злому криптосистем. Не зважаючи на всі ризики, криптографія на сьогоднішній день залишається найбільш ефективним і поширеним засобом інформації у кіберпросторі. Підтвердженням важливості розвитку криптографії є конкурси на стандарти криптографії, які постійно проводять як у нашій державі, так і в світі.

Важливий внесок у розвиток криптології та захисту інформації внесли такі вітчизняні та зарубіжні науковці, як К. Е. Шеннон, Дж. Л. Мессі, Б. Шнайєр, М. Хеллман, Ч. Г. Беннет, Б. У. Діффі, Р. Меркл, Н. Кобліц, А. Шамір, М. Мауер, І. Чанг, Р. Л. Рівест, Ж. Брассар, І. Д. Горбенко, А. М. Олексійчук, О. В. Гомонай, Р. А. Хаді, В. К. Усенко, В. М. Сидельніков, О. А. Логачов, С. О. Шестаков, А. Н. Фіонов, Б. Я. Рябко, Д. М. Голубчіков, У. Збінден, А. А. Молдовян, Л. В. Ковальчук та ін.

Не зважаючи на це, залишаються невирішеними багато задач, однією з яких є підвищення невизначеності результатів шифрування, особливо в криптосистемах, алгоритми яких використовують псевдовипадкові послідовності. Створення квантових комп'ютерів та стрімке збільшення хмарних сховищ вимагають застосування високошвидкісної потокової комп'ютерної криптографії, яка забезпечить максимальну невизначеність результатів шифрування.

Таким чином, можна констатувати, що тема дисертаційного дослідження «Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування» є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 20.12.13 №179 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014–2018 рр.», а саме – пп. 1.2.8.1 «Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії»; Постанови Президії НАНУ від 30.01.2019 №30 «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки», а саме – пп. 1.2.8.1 «Розроблення методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії»; 1.2.8.2 «Розроблення методів підвищення продуктивності систем асиметричної криптографії». Результати дисертаційної роботи включені в НДР «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР№ 0116U008714), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Основною метою дослідження є підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

– розроблення методу синтезу операцій криптографічного перетворення інформації, які забезпечують максимальну невизначеність результатів шифрування;

– розроблення методу синтезу операцій за критерієм строгого стійкого кодування мінімальної складності;

– удосконалення методу синтезу програмних та апаратних засобів комп’ютерної криптографії для забезпечення підвищення невизначеності результатів шифрування.

Об'єкт дослідження – процеси комп’ютерного криптографічного захисту інформації.

Предмет дослідження – дослідження і синтез операцій криптографічного перетворення інформації за критерієм строгого кодування для систем потокового шифрування.

Методи дослідження. У процесі розробки методу синтезу операцій криптографічного перетворення інформації, які забезпечують максимальну невизначеність результатів шифрування, використовувався математичний апарат теорії інформації, теорії алгоритмів, теорії множин, криптографії, математичної логіки, методів дискретної математики, математичної статистики та комп’ютерного моделювання. Для розроблення методу синтезу операцій за критерієм строгого стійкого кодування мінімальної складності використовувались: теорія алгоритмів, теорії графів, криптографія, методи комп’ютерного моделювання, дискретної математики та математичної статистики. Для удосконалення методу синтезу програмних та апаратних засобів комп’ютерної криптографії для забезпечення підвищення невизначеності результатів шифрування використано теорії: інформації, ймовірності, алгоритмів, криптографії із застосуванням методів дискретної математики, комп’ютерного моделювання, обчислювального експерименту та математичної статистики.

Наукова новизна одержаних результатів. У процесі вирішення поставлених задач автором одержано такі результати:

1) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;

2) вперше розроблено метод синтезу операцій за критерієм строгого стійкого

кодування мінімальної складності на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;

3) набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування, шляхом застосування методів синтезу моделей операцій з новими властивостями, які забезпечили спрощення процесу синтезу програмних і апаратних криптографічних засобів і дозволили реалізувати синтез аналогічних засобів мінімальної складності без побудови таблиць істинності та мінімізації.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні розроблених методів до моделей, функціональних схем і програмних модулів для реалізації операцій потокового шифрування, які гарантовано забезпечують зміну кожного біта інформації з імовірністю одна друга.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS. Крім того, застосування цих послідовностей в імовірнісних моделях на прикладі інтегральної моделі розвитку і припинення пожежі забезпечило підвищення точності моделювання.

Акти впровадження результатів дисертаційного дослідження додатково підкреслюють практичну цінність роботи.

Реалізація. Дисертаційна робота виконувалася відповідно до планів НДР Черкаського інституту пожежної безпеки ім. Героїв Чорнобиля Національного Університету цивільного захисту України та Черкаського державного технологічного університету. Одержані в ній теоретичні й практичні результати використані та впроваджені у таких закладах:

– Черкаський державний технологічний університет на кафедрі інформаційної

безпеки та комп'ютерної інженерії – у матеріалах лекційних курсів «Основи криптографічного захисту інформації», «Комп'ютерні методи та засоби захисту інформації». Акт впровадження від 20.06.2017 р.;

–Приватне підприємство «Сенсорна Електроніка» – для забезпечення конкурентоспроможності та переваги над аналогами на ринках електронної техніки в частині пристроїв захисту інформації. Акт впровадження від 20.12.2018 р.

Особистий внесок здобувача. Усі нові результати дисертаційної роботи отримано автором самостійно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, автору належать: модифікація моделі ковзного шифрування [1], узагальнення результатів дослідження двохрозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту [2], встановлені закономірності для синтезу двохрозрядних операцій криптографічного кодування, які відповідають критерію ССК [3, 9, 13], технологія побудови вхідних даних для мінімізації моделі операцій які відповідають критерію ССК [4], моделі операцій ССК мінімальної складності [5, 12], моделі операцій, удосконалені та адаптовані для практичного застосування [6], моделі операцій, які відповідають критерію ССК [7, 10, 11], узагальнені моделі багатораундового ССК [14], генерація псевдовипадкових послідовностей із використанням операцій ССК [15, 16]. Результати, опубліковані в [8, 17, 18], отримані одноосібно.

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Другій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Тольятті, 2014), «Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика)» (Харків, 2014), Третій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2015), П'ятій міжнародній науково-практичній конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Полтава – Баку – Кіровоград, 2015), «Техника и технология. Актуальные научные проблемы.

Рассмотрение, решение, практика» (Гданьск / Gdańsk, 2015), Всеукраїнській науково-практичній конференції з міжнародною участю «Надзвичайні ситуації: безпека та захист» (Черкаси, 2015), Пятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2016), Міжнародній науково-практичній конференції молодих учених «Проблеми та перспективи цивільного захисту» (Харків, 2017), Шостій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2018).

Публікації. Основні результати дисертаційної роботи викладено в 18 друкованих працях, у тому числі: 7 статтях у наукових журналах і збірниках наукових праць, внесених до списку фахових видань України; 1 одноосібній статті в закордонному науковому виданні 1 колективній монографії; 9 тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях, а також науково-практичних конференціях і семінарах.

Структура і обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 161 сторінка. Основний зміст викладений на 155 сторінках, містить 49 таблиць, 4 рисунки. Список використаних джерел містить 115 найменувань. Робота містить 3 додатки.

РОЗДІЛ 1
АНАЛІЗ ЯКОСТІ СИСТЕМ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

1.1 Актуальність проведення аналізу якості криптографічних систем

Останні десятиліття характеризуються різким збільшенням кількості відкритих робіт з усіх питань криптології, а криптоаналіз стає однією з найбільш активно розвинених областей досліджень. Багато криптосистем, стійкість яких не викликала особливих сумнівів, виявилися успішно розкритими. При цьому розроблений великий арсенал математичних методів, що представляють прямий інтерес для криптоаналітика.

Відомо, що криптографічна стійкість базується на складності розв’язання таких математичних задач як факторизація великого цілого числа, розв’язок дискретного логарифма та інші [19-22]. Вони характеризуються субекспоненційною або експоненційною складністю розв’язання на сучасних комп’ютерах [21-23]. Очікувалося, що стійкість криптографічних систем буде надійно спиратися на нерозв'язність в реальному часі багатьох таких добре відомих задач [24-26] та що, напевно, з часом вдасться довести принципову нерозкриваність деяких криптосистем.

Але сподівання на досягнення доказової стійкості за допомогою зведення задач криптографії до добре відомих математичних задач [20, 21, 23] не виправдалися, а, скоріше, навпаки. Саме та обставина, що будь-яку задачу відшукання способу розкриття деякої конкретної криптосистеми можна переформулювати як привабливу задачку, при вирішенні якої вдається використовувати багато методів тієї ж теорії складності, теорії чисел і алгебри, призвело до розкриття багатьох криптосистем [26, 27, 32, 33]. На сьогоднішній день класичний «одноразовий блокнот» залишається єдиною, безумовно, стійкою системою шифрування [28, 29].

Ідеальне доведення стійкості деякої криптосистеми з відкритим ключем могло б полягати в доведенні того факту, що будь-який алгоритм розкриття цієї системи, що володіє незнехтовно малою вірогідністю її розкриття, пов'язаний з неприйнятно великим об'ємом обчислень [24-26, 30, 31]. І хоча жодна з відомих систем з відкритим ключем не задовольняє цьому сильному критерію стійкості, ситуацію не слід розглядати як абсолютно безнадійну. Було розроблено багато систем, щодо яких доведено, що їх стійкість еквівалентна складності рішення деяких важливих задач, які майже всіма розглядаються як вкрай складні, таких, наприклад, як відома задача розкладання цілих чисел [23, 27]. Зауважимо, що багато з розкритих криптосистем були отримані в результаті ослаблення цих імовірно стійких систем з метою досягнення більшої швидкодії [25, 26, 32, 33, 35]. Крім того, результати широких досліджень, що проводилися протягом останніх десяти років як в самій криптографії, так і в загальній теорії обчислювальної складності, дозволяють сучасному криптоаналітику набагато глибше зрозуміти, що ж робить його системи нестійкими [24, 26, 32, 33].

Здійснення криптоаналізу для давно існуючих і недавно розроблених криптоалгоритмів дуже актуальне, так як завчасно можна сказати, що даний криптоалгоритм нестійкий, і вдосконалити його або замінити новим [34, 36]. Для того, щоб виявляти нестійкі криптоалгоритми, необхідно весь час удосконалювати вже відомі методи криптоаналізу і знаходити нові.

Необхідність вдосконалення криптографічного захисту даних особливо гостро сьогодні постала з розвитком квантової криптографії [37, 38].

Розробка квантових алгоритмів створила сприятливий грунт для розвитку криптоаналізу, адже їх можливості значно перевищують можливості звичайних комп’ютерів. А це, в свою чергу, поставило під загрозу надійність криптосистем, стійкість яких базувалася на складності розв’язку певних математичних задач [37].

Саме це зумовило появу нового напряму досліджень під назвою “постквантова криптографія”, основною ціллю якої є створення нових класів стійких криптосистем [37-39].

Серед криптосистем, що вважаються стійкими до квантового криптоаналізу виділяють такі класи криптосистем [39]:

1. Криптографія на основі решіток.
2. Мультиваріативна криптографія.
3. Криптографія на основі геш-функцій.
4. Криптографія на основі кодів.
5. Криптографія ізогінеї суперсингулярних еліптичних кривих.
6. Симетрична криптографія.

Отже, проблема забезпечення криптографічної стійкості як для асиметричних криптоперетворень, так і для певних симетричних в умовах сьогодення постає дедалі гостріше.

1.2 Основні вимоги до криптографічних систем

Криптосистеми поділяються на симетричні і асиметричні (або з відкритим ключем) [30-33].

У симетричних криптосистемах для шифрування, і для розшифрування використовується один і той же ключ. У системах з відкритим ключем використовуються два ключі – відкритий і закритий (секретний), які математично пов'язані один з одним. Інформація шифрується за допомогою відкритого ключа, що доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення. Терміни розподіл ключів і керування ключами відносяться до процесів системи обробки інформації, суттю яких є вироблення і розподіл ключів між користувачами. Електронним цифровим підписом називається його криптографічне перетворення, що приєднуються до тексту, яке дозволяє при отриманні тексту іншим користувачем перевірити авторство і достовірність повідомлення [30-33, 40-45].

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги: висока продуктивність, простота,

захищеність і т.д. Програмна реалізація більш практична, допускає відому гнучкість у використанні [43-52].

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги [43-49, 52-55]:

- зашифроване повідомлення повинно піддаватися читанню тільки за наявності ключа;

- число операцій, необхідних для визначення використаного ключа шифрування за фрагментом зашифрованого повідомлення і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;

- число операцій, необхідних для розшифрування інформації шляхом перебору всіляких ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих (хмарних) обчислень), або вимагати неприйнятно високих витрат на ці обчислення;

- знання алгоритму шифрування не повинно впливати на надійність захисту;

- незначна зміна ключа повинно приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні одного і того ж вихідного тексту;

- незначна зміна вихідного тексту повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

- структурні елементи алгоритму шифрування повинні бути незмінними;

- додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

- довжина шифрованого тексту не повинна перевищувати довжину вихідного тексту;

- не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;

- будь-який ключ з множини можливих повинен забезпечувати надійний захист інформації;

- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

1.3 Визначення властивості “лавинного ефекту”

Лавинний ефект (avalanche) – це число символів, яке змінилося в шифртексті при зміні одного символу відкритого тексту [56, 57].

Однією з необхідних вимог при обчисленнні раундових ключів для зашифрування та розшифрування є забезпечення лавинного ефекту. Тобто значення кожного біту секретного ключа має впливати на значення кожного раундового ключа [52, 53, 55].

Строгий лавинний критерій можна формально визначити як рівну ймовірність зміни кожного вихідного біта при зміні одного вхідного біта [56, 57].

Відомий американський вчений К. Шеннон ввів поняття конфузія та дифузія як методів, що ускладнюють криптоаналіз. Згідно Шеннону [58]:

- дифузія – метод, при якому надлишковість у статистиці вхідних даних «розподіляється» по всій структурі вихідних даних. При цьому для статистичного аналізу потрібні більші об’єми вхідних даних. Дифузія веде до приховування структури відкритого тексту;
- конфузія – метод, при якому залежність ключа і вихідних даних робиться, за можливості, більш складною, зокрма, нелінійною. При цьому криптоаналітику стає складніше робити припущення про структуру ключа за вхідними даними, а також про вихідні дані, якщо відома частина ключа.

Лавинний ефект є наслідком хорошої конфузії та дифузії. Кількісно лавинний критерій, наприклад для S-блока підстановки, можливо визначити через коефіцієнт розповсюдження помилки як [57]

$$K_i(f) = \sum_{a_i} f(f(x) \oplus f(x \oplus e_i)) = 2^{\eta-1},$$

де η - розмірність компонентної функції S-блока підстановки.

Алгоритм криптографічного перетворення призначений для апаратної або програмної реалізації, задовольняє криптографічним вимогам і за своїми можливостями не накладає обмежень на ступінь секретності інформації, що захищається [59, 60].

До симетричного шифрування пред'являються такі вимоги [45-47, 52, 57, 58-61]:

- Відсутність лінійності (тобто умови f (a) xor f (b) = f (a xor b)), в іншому випадку полегшується застосування диференціального криптоаналізу до шифру.

- Повна втрата всіх статистичних закономірностей вихідного повідомлення. Для цього шифр повинен мати «ефект лавини».

Лавинний ефект проявляється в залежності всіх вихідних бітів від кожного вхідного біта [57-60]:

1. Криптографічний алгоритм задовольняє лавинному критерію, якщо при зміні одного біта вхідної послідовності, змінюється в середньому половина вихідних бітів.

2. Криптографічний алгоритм задовольняє строгому лавинному критерію, якщо при зміні одного біта вхідної послідовності, кожен біт вихідної послідовності змінюється з ймовірністю одна друга.

3. Криптографічний алгоритм відповідає критерію незалежності бітів, якщо при зміні будь-якого вхідного біта, будь-які два вихідних біта змінюються незалежно.

1.3.1 Властивості строгого лавинного ефекту і досконалості шифрів

Майже всі компоненти в схемах шифрування, включаючи S-блоки, перехідні функції станів, блокові шифри в цілому і т.д. є відображеннями простору n-мірних двійкових векторів у простір m-мірних двійкових векторів, при цьому часто n = m [20, 25].

Практично у всіх існуючих сьогодні архітектурах систем симетричного шифрування використовуються так звані вузли (таблиці) замін або S-блоки (S-box). Самі S-блоки представляють собою не що інше, як звичайні табличні підстановки. Вузли замін використовуються у самих різних криптосистемах – від криптографічних хешів до блокових ітеративних шифрів. При цьому, незважаючи на те, що увага приділяється в основному оборотним вузлам заміни, самі S-блоки такими бути не зобов'язані. Тобто, взагалі кажучи, вузол заміни – це деяке відображення, задане за допомогою таблиці значень. У більшості випадків вузли замін є єдиною нелінійної частиною шифру, і тому від стійкості методу їх створення, оцінки та використання цілком залежить стійкість шифру [24-27, 39-47, 52-55].

Власне, для опису невипадкових вузлів замін, які представляють собою так звані криптографічні примітиви, використовують особливі булеві функції [47]. Дані функції повинні відповідати певним критеріям, серед яких зобов'язані бути присутніми наступні властивості [65-67]:

- Властивість повноти.

Властивість повноти (completeness) формулюється правилом: кожен вихідний біт є нетривіальною функцією всіх вхідних бітів. Це дозволяє внести в криптосистему сувору залежність виходу шифру від всіх бітів ключа, що гарантує шифру криптостійкість, що визначається довжиною ключа. Неповнота шифру може привести до можливості поділу залежностей бітів виходу і входу на групи, що не залежать один від одного, в результаті чого криптоаналітику необхідно вирішити не одну складну задачу, а кілька простіших.

- Наявність лавинного ефекту.

Лавинний ефект (Avalanche Criterion – як розвиток властивості розсіювання) означає примусову зміну в середньому половини бітів виходу шифру при зміні хоча б одного біта входу. Відсутність лавинного ефекту призводить до появи великих еквівалентних ключів, що негативно позначається на фактичній криптостійкості шифру. Наявність же його робить вельми скрутним статистичний

аналіз виходу шифру і визначення ключа шифру за допомогою імовірнісних методів [56-58].

- Наявність їх комбінації як строгого лавинного ефекту.

Строгий лавинний ефект (Strict Avalanche Criterion, або SAC) досягається як компіляція властивостей повноти і лавинного ефекту, якщо кожен біт виходу шифру змінюється з ймовірністю при зміні одного біта входу. Число функцій для n змінних, що володіють таким ефектом, підраховано і дорівнює 2^{n-1}. Строгий лавинний ефект забезпечений також для тих функцій, для яких сума $f(x) \oplus f(x \oplus a)$ є збалансованою, тобто містить одиниць і нулів порівну, для всіх a з одним встановленим в одиницю бітом і іншими нулями [57, 58].

- Попарно незалежність всіх знаків виходу і оборотність як досконалість.

В іноземній літературі досконалість іноді називають також, як Bit Independence Criterion або BIC [55, 56, 59]. Наявність або відсутність досконалості криптографічних примітивів, використаних у шифрі, впливає на можливість витоку інформації при статистичних дослідженнях виходу шифру. У разі досконалості статистичні характеристики шифру наближаються за своїми значеннями до характеристик незалежних випадкових процесів, що безсумнівно істотно ускладнює криптоаналіз [62-64]. З моменту появи перших SP-мереж і потім після прийняття першого стандарту шифрування існуючі спочатку властивості повноти і лавинного ефекту помітно еволюціонували і стали властивостями строгого лавинного ефекту і досконалості [57].

Взагалі кажучи, ще команда розробників IBM наголошувала на деяких необхідних для S-блоків якостях (наслідуючи добру половину міркувань у Шеннона) [58, 62, 63]:

- нелінійну залежність вихідних бітів від вхідних;
- залежність будь-яких вхідних бітів від усіх вихідних;
- зміна половини вихідних бітів при зміні одного вхідного.

Ці властивості є не що інше, як визначення властивостей повноти і розсіювання, дані Клодом Шенноном [58].

Зрештою, після кількох десятків вдалих робіт у цій галузі, були колегіально сформульовані основні властивості вузлів замін [42-46, 57-63]:

- строгий лавинний ефект;
- біти виходу не повинні залежати один від одного;
- має існувати зворотне перетворення.

При дотриманні всіх трьох зазначених властивостей отримані S-блоки називають досконалими криптографічними перетвореннями. Приблизно в середині 90-х років виявилося, що необхідні набори функцій вже давно відомі в дискретній математиці і носять назву бент-функцій [67]. Багато досягнень у дослідженні бент функцій сьогодні благополучно перенесені в теоретичну область криптографії.

На сьогодні практично невідомі ефективні методи конструювання S блоків, які відповідають всім поставленим критеріям. Проте існує кілька алгоритмів, що дозволяють будувати ефективні вузли замін, стійкі проти більшості існуючих криптографічних атак [57].

Один з алгоритмів, використаних при створенні вузлів замін алгоритму CAST 256 [68], полягає у використанні бент-функції як функції, яка має наступну властивість: відстань Хеммінга від f до будь-якої аффінної функції у просторі функції над полем GF (2^m) є максимально можливим [69].

1.3.2 Критерії оцінки властивостей “лавинного ефекту”

Нехай $U^{(i)} = U \oplus E_i$, тобто бінарний вектор, отриманий інвертуванням i-ого біту вектора U. Тоді бінарний вектор $Y^{(i)} = F\left(U^{(i)}\right) \oplus F(U)$ називається лавинним вектором за компонентом i (де F – це функція шифрування). Для блочного шифру $U = X \parallel K$. Нехай для критеріїв, що розглядаються, розмірність вектора U дорівнює n, а для Y – дорівнює m.

Введемо наступні позначення потужності множини A: $\# A$.

Матриця залежностей має наступний вигляд: $a_{ij} = \#\left\{Y^{(i)}, y_j^{(i)}\right\}$. Ця матриця відображає залежність j-ого розряду вихідного вектора від i-ого розряду вхідного вектора.

Матриця відстаней має вигляд: $b_{ij} = \#\left\{Y^{(i)} \mid w\left(y^{(i)}\right) = j\right\}$, де w – функція ваги Хеммінга (число нерівних нулю елементів вектора).

Існує 4 критерія [34, 57, 59, 63], за якими пропонується перевіряти властивості розсіювання блочних алгоритмів:

1. Середнє число біт виходу,які змінюються при зміні одного біту вхідного вектора.

Це число оцінюється за формулою: $d_1 = \frac{1}{n}\sum_{i=1}^{n}\frac{\sum_{j=1}^{m} jb_{ij}}{N}$, где $N = \#U$.

2. Ступінь повноти перетворення: $d_2 = 1 - \frac{\#\left\{(i,j) \mid a_{ij} = 0\right\}}{nm}$.

3. Ступінь лавинного ефекту: $d_3 = 1 - \frac{\sum_{i=1}^{n}\left|\frac{1}{N}\sum_{j=1}^{m} 2jb_{ij} - m\right|}{nm}$.

4. Ступінь відповідності строгому лавинному критерію: $d_4 = 1 - \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left|\frac{2a_{ij}}{N} - 1\right|}{nm}$.

При дослідження дифузії, тобто впливу біт вхідного текста (відкритого) на перетворений текст (зашифрований), матриці залежностей та відстаней мають вигляд:

$$a_{ij} = \#\left\{\left(f\left(X^{(i)}, k\right)\right)_j \neq \left(f(X,k)\right)_j\right\},$$

$$b_{ij} = \#\left\{w\left(f\left(X^{(i)}, k\right) \oplus f(X,k)\right) = j\right\}.$$

При дослідженні конфузії, тобто впливу бітів ключа на перетворений текст (зашифрований), матриці залежностей та відстаней мають вигляд:

$$a_{ij} = \#\left\{\left(f\left(X, k^{(i)}\right)\right)_j \neq \left(f\left(X, k\right)\right)_j\right\},$$

$$b_{ij} = \#\left\{w\left(f\left(X, k^{(i)}\right) \oplus f\left(X, k\right)\right) = j\right\}.$$

Отже, з вище наведеного, можна зробити висновок, що чим більше лавинний ефект, тим вище надійність шифру.

1.4 Аналіз надійності та безпеки криптографічних систем

1.4.1 Поняття стійкості криптографічного алгоритму

Криптостійкістю називається характеристика шифру, що визначає його стійкість до розшифрування без знання ключа (тобто криптоаналіз) [40-43]. Є кілька показників криптостійкості, серед яких [25, 26, 30, 32]:

- кількість всіх можливих ключів;
- середній час, необхідний для успішної криптоаналітичної атаки того чи іншого виду [72].

Здатність криптосистеми протистояти атакам (активного чи пасивного) криптоаналітика називається стійкістю. Кількісно стійкість вимірюється як складність найкращого алгоритму, що приводить криптоаналітика до успіху з прийнятною ймовірністю [46, 49, 70, 71]. Залежно від цілей і можливостей криптоаналітика змінюється і стійкість. Розрізняють стійкість ключа (складність розкриття ключа найкращим відомим алгоритмом), стійкість безключового читання, імітостійкість (складність нав'язування хибної інформації найкращим відомим алгоритмом) і ймовірність нав'язування хибної інформації [44, 45, 48-53]. Це іноді зовсім різні поняття, не пов'язані між собою. Деякі криптосистеми, наприклад RSA, дозволяють нав'язувати неправдиву інформацію зі складністю, яка практично не залежить від стійкості ключа. Аналогічно можна розрізняти стійкість власне криптоалгоритму, стійкість протоколу, стійкість алгоритму генерації та розповсюдження ключів [48-53, 72].

Рівень стійкості залежить від можливостей криптоаналітика і від користувача. Так, розрізняють криптоаналіз на основі тільки шифрованого тексту, коли у криптоаналітика в розпорядженні тільки набір шифрограм і він не знає відкритих текстів, та криптоаналіз на основі відкритого тексту, коли криптоаналітик знає і відкриті, і відповідні шифровані тексти [26, 27, 30, 32, 33]. Оскільки криптоалгоритм зазвичай повинен бути досить універсальним, очевидним представляється вимога, щоб стійкість ключа не залежала від розподілу ймовірностей джерела повідомлень [24, 25]. У загальному випадку джерело повідомлень може виробляти "зручні" для порушника повідомлення, які можуть стати йому відомими. У цьому випадку говорять про криптоаналіз на основі спеціально обраних відкритих текстів [44-47]. Очевидно, що стійкість ключа відносно аналізу на основі вибраних текстів не може перевищувати стійкості відносно аналізу на основі відкритих текстів, а вона, в свою чергу, не може перевищувати стійкості відносно аналізу на основі шифрованих текстів [51-54, 74, 75]. Іноді розробником СЗІ допускається навіть, що ворожий криптоаналітик може мати доступ до криптосистеми, тобто бути «своїм». Зазвичай криптоалгоритми розробляють так, щоб вони були стійкими відносно криптоаналізу на основі спеціально обраних відкритих текстів [48-49].

Поняття «найкращого алгоритму» розкриття ключа у визначенні стійкості неконструктивно і допускає суб'єктивне тлумачення (для когось із розробників найкращим алгоритмом може бути простий перебір ключів). Мабуть, ні для одного з використовуваних криптоалгоритмів не визначений найкращий алгоритм розкриття ключа, тобто задача знаходження найкращого алгоритму є надзвичайно складною. Тому на практиці для оцінки стійкості користуються найкращим відомим або знайденим в ході досліджень алгоритмом розкриття. Таким чином, на практиці ніхто не може перешкодити здатному криптоаналітику знизити оцінку стійкості, придумавши новий, більш ефективний метод аналізу [27, 50, 72].

Створення нових ефективних методів розкриття ключа або іншого методу ослаблення криптоалгоритму може давати обізнаним особам великі можливості з нанесення шкоди користувачам, які застосовують даний криптоалгоритм.

Публікація або замовчування цих відомостей визначаються ступенем відкритості суспільства. Рядовий користувач системи безсилий перешкодити порушнику у розкритті його ключів [25-27, 75].

З викладеного випливає, що поняття «найкращого відомого» алгоритму неабсолютно: завтра може з'явитися новий більш ефективний алгоритм розкриття, який приведе до неприпустимого зниження стійкості криптоалгоритму [37-39]. З розвитком математики та засобів обчислювальної техніки стійкість криптоалгоритму може тільки зменшуватися. Для зменшення можливого збитку, викликаного несвоєчасною заміною криптоалгоритму, який втратив свою стійкість, бажана періодична перевірка стійкості криптоалгоритму. Для зниження ймовірності непередбачуваного «обвалу» знову розробленого криптоалгоритма необхідне проведення криптографічних досліджень [26, 43, 45].

Ефективність шифрування з метою захисту інформації залежить від збереження таємниці ключа і криптостійкості шифру [24, 29, 30, 32, 33, 46].

За стійкістю шифри діляться на три групи [27, 45, 88]:

- досконалі (абсолютно стійкі, теоретично стійкі) – шифри, свідомо не піддаються розкриттю (при правильному використанні). Розшифрування секретного повідомлення призводить до виникнення кількох осмислених рівноймовірних відкритих повідомлень;

- практично (обчислювально, достатньо) стійкі – шифри, розкриття яких за прийнятний час неможливе на сучасному або перспективному рівні обчислювальної техніки. Практична стійкість таких систем базується на теорії складності і оцінюється виключно на якийсь певний момент часу з двох позицій: обчислювальна складність повного перебору; відомі на даний момент слабкості (уразливості) і їх вплив на обчислювальну складність;

- нестійкі шифри.

Прийнято розрізняти криптоалгоритми за ступенем доказовості їх безпеки. Існують безумовно стійкі, доказово стійкі та ймовірно стійкі криптоалгоритми [46, 47, 60, 88]. Безпека безумовно стійких криптоалгоритмів заснована на доведених теоремах про неможливість розкриття ключа. Прикладом безумовно

стійкого криптоалгоритму є система з разовим використанням ключів (шифр Вернама) або система квантової криптографії, заснована на квантовомеханічному принципі невизначеності. Стійкість доказово стійких криптоалгоритмів визначається складністю розв'язання добре відомої математичної задачі, яку намагалися вирішити багато математиків і яка є загальновизнано складною. Прикладом можуть служити системи Діффі-Хеллмана або Рівеста-Шаміра-Адельмана, засновані на складностях відповідно дискретного логарифмування і розкладання цілого числа на множники. Імовірно стійкі криптоалгоритми засновані на складності рішення окремої математичної задачі, яка не зводиться до добре відомих задач і яку намагалися вирішити один або кілька людей. Прикладами можуть бути криптоалгоритми ГОСТ 28147-89, DES, FEAL [52, 70, 74, 75, 88].

На жаль, безумовно стійкі криптосистеми незручні на практиці (системи з разовим використанням ключа вимагають великої захищеної пам'яті для зберігання ключів, системи квантової криптографії вимагають волоконно-оптичних каналів зв'язку і є дорогими, крім того, доказ їхньої безпеки йде з області математики в область фізики) [54,71, 88].

Перевагою доказово стійких алгоритмів є хороша вивченість задач, покладених в їх основу. Недоліком їх є неможливість оперативного доопрацювання криптоалгоритмів у разі появи такої необхідності, тобто жорсткість цих криптоалгоритмів. Підвищення стійкості може бути досягнуто збільшенням розміру математичної задачі або її заміною, що, як правило, тягне ланцюг змін не тільки в шифрувальній, але і суміжній апаратурі.

Імовірно стійкі криптоалгоритми характеризуються порівняно малою вивченістю математичної задачі, але проте мають велику гнучкість, що дозволяє не відмовлятися від алгоритмів, в яких виявлені слабкі місця, а проводити їх доопрацювання [60, 62-64, 88].

Задача забезпечення захищеного зв'язку включає в себе цілий комплекс проблем. Це задача забезпечення секретності та імітозахисту, розпізнавання (аутентифікації) і задача управління ключами, включаючи їх вироблення,

розподіл і доставку користувачам, а також їх оперативну заміну в разі потреби [73-75, 88].

Джерело повідомлень виробляє довільну інформацію (відкриті тексти) з якимось розподілом ймовірностей. Шифратор шифрує це повідомлення на конфіденційному (відомому тільки відправнику і одержувачу) ключі Z і переводить відкритий текст в шифрований текст або шифрограму (криптограму, шифротекст). Ключі виробляються джерелом ключів і по безпечних каналах розсилаються абонентом мережі зв'язку. Дешифратор розкриває прийняту шифрограму і передає одержувачу. Рандомізатор робить всі шифрограми несхожими одна на одну, навіть якщо вхідні повідомлення однакові. Вирішальний пристрій приймає рішення про те, чи є прийняте повідомлення автентичним, тобто виконує функцію імітозахисту. Операції шифрування і розшифрування можна описати так: Y = E (X), X = D (Y) [29, 32, 55, 79 , 88].

Для взаємної однозначності необхідно, щоб DE було одиничним перетворенням. Передбачається наявність у відправника і одержувача загального секретного ключа Z. Насправді, ключі у них не обов'язково однакові, але знання одного ключа, наприклад шифрування, дозволяє легко обчислити інший. Тому криптоалгоритми, що розглядаються, іноді називають симетричними, або одноключевими. Дана схема застосовується в тому випадку, якщо абоненти мережі довіряють один одному [81-88].

Автентичність і цілісність повідомлення забезпечуються його криптографічним перетворенням, що виконується за допомогою секретного ключа. Наприклад, якщо відправник передасть відразу і відкритий (не вимагає засекречування), і зашифрований тексти, то це дозволить одержувачу, який знає ключ, стверджувати, що текст при передачі по каналу зв'язку не був змінений, якщо результат розшифрування шифрограми збігається з відкритим текстом. Дійсно, випадковий збіг відповідних один одному відкритого тексту і шифрограми – практично неможлива подія. Цю пару міг скласти лише відправник, який знає секретний ключ. Звідси випливає і автентичність повідомлення (відправник ототожнюється з власником ключа). Насправді немає

необхідності передавати всю шифрограму, досить передати лише її частину, яка називається імітовставкою, яка повинна залежати від усього відкритого тексту. Тоді одержувач може на підставі отриманого тексту і ключа обчислити свою імітовставку і перевірити її відповідність отриманій [73-75, 79, 81-83, 88].

Для впізнання користувача використовується наступний діалог. Перевіряючий виробляє випадковий текст і посилає тому, кого потрібно упізнати, для шифрування. Упізнаваний шифрує цей текст і повертає перевіряючому. Той перевіряє відповідність шифрограми тексту. Правильну відповідь може скласти тільки власник секретного ключа, який ототожнюється з законним користувачем. Очевидно, що порушник, який прослуховує діалог, не зможе правильно зашифрувати новий текст і назватися користувачем. Винятком є аналогія відомого шахрайства, застосованого при грі в шахи поштою, коли порушник просто транслює відповіді і запити автентичним перевіряючому і тому, хто перевіряється, ведучи діалог одночасно з кожним із них. Принципова відмінність цієї системи від впізнання за паролем, де підслуховування дозволяє дізнатися секретний пароль і надалі скористатися цим, полягає в тому, що тут каналом зв'язку секретна інформація не передається. Ясно, що і якість шифрування, і імітостійкість, і стійкість впізнання можуть бути забезпечені, якщо покладене в основу криптоперетворення є стійким в сенсі розкриття ключа.

Криптографічні алгоритми зазвичай будуються з використанням простих і швидко виконуваних операторів декількох типів. Множина зворотних операторів, що перетворюють текст довжиною n біт в текст довжиною n біт, є елементами групи зворотних операторів за множенням (підстановок n-розрядних слів) [20, 22, 25]. Нехай f, g, h – зворотні оператори, тобто існують f^{-1}, g^{-1}, h^{-1}. Тому hgf – послідовне виконання операторів f, g, h – теж зворотний оператор (оператори виконуються справа наліво) зі зворотним оператором до цього добутку f^{-1}, g^{-1}, h^{-1}. Тому дешифратор виконує ті ж операції, що і шифратор, але в зворотному порядку, і кожен оператор розшифрування є зворотним до відповідного оператору шифрування. Деякі оператори є взаємно зворотними, тобто виконання підряд два рази деякої операції над текстом дає вихідний текст. У термінах теорії груп це

записується рівнянням $f^2 = e$, де e – одиничний оператор. Такий оператор називається інволюцією. Можна сказати, що інволюція являє собою корінь із одиниці. Прикладом інволюції є додавання за модулем два тексту з ключем [65, 66, 88].

Порушник може вирішувати такі завдання. Він може намагатися розкрити зашифровану інформацію, організувати вибіркове пропускання тієї чи іншої інформації, нарешті, він може намагатися змінити автентичну або нав'язати хибну інформацію. Принципова відмінність завдань засекречування і імітозахисту полягає в тому, що ключ засекречування має бути не доступний порушнику протягом терміну секретності інформації, який зазвичай набагато більше, ніж термін дії ключа і може складати десятки років. Ключ імітозахисту представляє інтерес для порушника тільки під час його дії. Тому і вимоги до нього пред'являються менш жорсткі, ніж до ключа засекречування [79-83].

Існує ще одне важливе застосування одноключової криптографії. Це здійснення одностороннього перетворення інформації. Таке перетворення називається хеш-функцією. Особливість цього перетворення полягає в тому, що пряме перетворення $y = h(x)$ обчислюється легко, а зворотне $x = h^{-1}(y)$ - важко. Взагалі кажучи, зворотне перетворення не є функцією, тому правильніше говорити про знаходження одного з прообразів для даного значення хеш-функції. В цьому випадку ключа, що розуміється як деяка конфіденційна інформація, немає. Однак стійкі хеш-функції, для яких прообраз за даним значенням функції важко знайти, реалізуються криптографічними методами і вимагають для обгрунтування стійкості проведення криптографічних досліджень. Типове застосування хеш-функції - створення стисненого образу для вихідного тексту такого, що знайти інший текст, що володіє таким же образом, обчислювально неможливо. Завдання створення стійкої хеш-функції виникає, наприклад, при цифровому підпису текстів [76-78].

Одне з можливих самостійних застосувань хеш-функцій – це впізнання користувача за допомогою ланцюжка виду $x, h(x), h(h(x)) = h^2(x), h^3(x), \ldots h^k(x)$.

Останнє значення ланцюжка $h^k(x)$ є контрольною інформацією для перевіряючого, а користувач знає $h^{k-1}(x)$ і пред'являє цю інформацію на вимогу перевіряючого. Перевіряючий обчислює h ($h^{k-1}(x)$) і порівнює з контрольною. Наступного разу цей користувач повинен пред'явити $h^{k-2}(x)$, а контрольною інформацією є $h^{k-1}(x)$ і т.д. Це цікаве рішення, запропоноване А. Конхеймом [80], однак має ряд недоліків. По-перше, користувачеві треба зберігати весь ланцюжок $h^i(x)$, що вимагає великого обсягу пам'яті, якщо число впізнавань може бути велике. По-друге, якщо у кожного користувача є кілька перевіряючих, то постає питання про синхронізацію перевіряючих за показниками останнього використаного значення $h^i(x)$, тобто потрібно канали зв'язку між кожною парою перевіряючих [79].

1.4.2 Атаки на асиметричну криптосистему

Ще одним великим класом криптографічних систем є так звані асиметричні або двохключові системи. Ці системи характеризуються тим, що для шифрування і для розшифрування використовуються різні ключі, пов'язані між собою певною залежністю. При цьому дана залежність така, що встановити один ключ, знаючи інший, з обчислювальної точки зору дуже важко [30,32, 52-55, 79-83].

Один з ключів (наприклад, ключ шифрування) може бути зроблений загальнодоступним, і в цьому випадку проблема отримання загального секретного ключа для зв'язку відпадає. Якщо зробити загальнодоступним ключ розшифрування, то на базі отриманої системи можна побудувати систему аутентифікації переданих повідомлень. Оскільки в більшості випадків один ключ з пари стає загальнодоступним, такі системи отримали також назву криптосистем з відкритим ключем.

Асиметричні алгоритми шифрування визначається трьома алгоритмами: генерації ключів, шифрування і розшифрування. Алгоритм генерації ключів відкритий, всякий може подати йому на вхід випадковий рядок r належної довжини і отримати пару ключів (k_1, k_2). Один з ключів (наприклад, k_1)

публікується, він називається відкритим, а другий, так званий секретний, зберігається в таємниці. Алгоритми шифрування E_{k_1} і розшифрування D_{k_2} такі, що для будь-якого відкритого тексту m: $D_{k_2}(E_{k_1}(m)) = m$. [32, 43-47]

Розглянемо тепер гіпотетичну атаку зловмисника на цю систему. Противнику відомий відкритий ключ k_1, але невідомий відповідний секретний ключ k_2. Противник перехопив криптограму d і намагається знайти повідомлення m, де $d = E_{k_1}(m)$. Оскільки алгоритм шифрування відкритий, противник може просто послідовно перебрати всі можливі повідомлення довжини n, обчислити для кожного такого повідомлення m_i криптограму $d_i = E_{k_1}(m_i)$ і порівняти d_i з d. Те повідомлення, для якого $d_i = d$ і буде шуканим відкритим текстом. Якщо повезе, то відкритий текст буде знайдений досить швидко. У гіршому ж випадку перебір буде виконаний за час порядку $2^n T(n)$, де T (n) – час, необхідний для шифрування повідомлення довжини *n*. Якщо повідомлення мають довжину близько 1000 бітів, то такий перебір нездійсненний на практиці ні на яких найпотужніших комп'ютерах [52-54].

Ми розглянули лише один з можливих способів атаки на криптосистему і найпростіший алгоритм пошуку відкритого тексту, який зазвичай називають алгоритмом повного перебору. Використовується також і інша назва: «метод грубої сили». Інший найпростіший алгоритм пошуку відкритого тексту – вгадування. Цей очевидний алгоритм вимагає невеликих обчислень, але спрацьовує з знехтовно малою ймовірністю (при великих довжинах текстів). Насправді противник може намагатися атакувати криптосистему різними способами і використовувати різні, більш витончені алгоритми пошуку відкритого тексту [47, 72, 82].

Крім того, зловмисник може спробувати відновити секретний ключ, використовуючи знання (в загальному випадку несекретні) про математичну залежність між відкритим і секретним ключами. Природно вважати криптосистему стійкою, якщо будь-який такий алгоритм вимагає практично нездійсненного обсягу обчислень або спрацьовує зі знехтовно малою

ймовірністю. При цьому противник може використовувати не тільки детерміновані, але і ймовірнісні алгоритми.) Це і є теоретико-складнісний підхід до визначення стійкості. Для його реалізації відносно того чи іншого типу криптографічних систем необхідно виконати наступне [84-86]:

1) дати формальне визначення системи даного типу;

2) дати формальне визначення стійкості системи;

3) довести стійкість конкретної конструкції системи даного типу.

Тут відразу ж виникає ряд проблем. По-перше, для застосування теоретико-складнісного підходу необхідно побудувати математичну модель криптографічного системи, що залежить від деякого параметра, так званого параметром безпеки, який може приймати як завгодно великі значення (зазвичай для простоти передбачається, що параметр безпеки може пробігати весь натуральний ряд).

По-друге, визначення стійкості криптографічного системи залежить від того завдання, яке стоїть перед противником, і від того, яка інформація про схему йому доступна. Тому стійкість систем доводиться визначати і досліджувати окремо для кожного припущення щодо противника.

По-третє, необхідно уточнити, який обсяг обчислень можна вважати «практично неможливим». Зі сказаного вище випливає, що ця величина не може бути просто константою, вона повинна бути представлена функцією від зростаючого параметра безпеки. Відповідно до тези Едмондс алгоритм вважається ефективним, якщо час його виконання обмежений деяким поліномом від довжини вхідного слова (в нашому випадку – від параметра безпеки). В іншому випадку говорять, що обчислення за даним алгоритмом практично нездійсненні. Зауважимо також, що самі криптографічні системи повинні бути ефективними, тобто всі обчислення, запропоновані тією або іншою схемою, повинні виконуватися за поліноміальний час.

По-четверте, необхідно визначити, яку ймовірність можна вважати знехтовно малою. У криптографії прийнято вважати такою будь-яку ймовірність,

яка для будь-якого полінома p і для всіх досить великих n не перевищує 1/p (n), де n – параметр безпеки [78-80].

Отже, при наявності всіх зазначених вище визначень, проблема обгрунтування стійкості криптографічного системи звелася до доказу відсутності поліноміального алгоритму, який вирішує завдання, що стоїть перед противником. Але тут виникає ще одна і вельми серйозна перешкода: сучасний стан теорії складності обчислень не дозволяє доводити зверхполіноміальні нижні оцінки складності для конкретних завдань даного класу. З цього випливає, що на даний момент стійкість криптографічних систем може бути встановлена лише з залученням будь-яких недоведених припущень. Тому основний напрямок досліджень полягає в пошуку найбільш слабких достатніх умов (в ідеалі – необхідних і достатніх) для існування стійких систем кожного з типів [78, 79].

В основному, розглядаються припущення двох типів – загальні (або теоретико-складнісні) і теоретико-числові, тобто припущення про складність конкретних теоретико-числових задач. Всі ці припущення в літературі зазвичай називаються криптографічними [86, 87].

З розглянутого вище випливає, що поняття стійкості криптосистеми багатогранно. Стійкість залежить не тільки від розробника, але і від особливостей використання даного криптоалгоритму в системі управління або зв'язку, від фізичної реалізації криптоалгоритму, а також від майбутніх успіхів математики та обчислювальної техніки. Адже криптосистема може експлуатуватися багато років, а необхідність зберігати в секреті протягом тривалого часу передану раніше відкритими каналами зв'язку інформацію може зробити необхідним прогнозувати розвиток науки і техніки на десятиліття [88].

1.4.3 Поняття надійності криптосистем

У сучасному програмному забезпеченні (ПЗ) криптоалгоритми широко застосовуються не тільки для задач шифрування даних [48-51, 70], але і для аутентифікації та перевірки цілісності [73-75]. На сьогоднішній день існують

добре відомі й апробовані криптоалгоритми (як з симетричними, так і несиметричними ключами), криптостійкість яких або доведена математично, або заснована на необхідності вирішення математично складної задачі (факторизації, дискретного логарифмування і т.п.). Таким чином, вони не можуть бути розкриті інакше, ніж повним перебором або рішенням зазначеної задачі.

З іншого боку, увесь час з'являється інформація про помилки або «дірки» в тій чи іншій програмній реалізації системи (в т.ч. тій, що застосовує криптоалгоритми), або про те, що вона була зламана (cracked). Це створює недовіру як до конкретних програм, так і до можливості взагалі захистити що-небудь криптографічними методами не тільки від кіберзлочинців, але і від простих хакерів.

Тому знання історії атак і "дірок" у криптосистемах, а також розуміння причин, через які вони мали місце, є однією з необхідних умов розробки захищених систем. Перспективним напрямком досліджень в цій області є аналіз успішно проведених атак або виявлених уразливостей в криптосистемах з метою їх узагальнення, класифікації та виявлення причин і закономірностей їх появи та існування [26, 45].

Можливо виділити наступні причини ненадійності програмної реалізації криптографічних систем [48, 50, 51, 72]:

1. Неможливість застосування стійких криптоалгоритмів;
2. Помилки в реалізації криптоалгоритмів;
3. Неправильне застосування криптоалгоритмів;
4. Людський фактор.

Причини ненадійності можна відобразити на наступною схемою (рис. 1).

Для сучасних криптографічних систем можна сформулювати такі вимоги щодо надійності [26, 27, 32, 70, 74, 75, 83, 84]:

- складність і трудомісткість процедур шифрування і розшифрування повинні визначатися в залежності від необхідного рівня захисту інформації (необхідно забезпечити надійний захист інформації);

Рис. 1 – Основні чинники ненадійності криптографічних програмних систем

- тимчасові і вартісні витрати на захист інформації повинні бути прийнятними при заданому рівні її секретності (витрати на захист не повинні бути надмірними);

- процедури шифрування і розшифрування не повинні залежати від довжини повідомлення;

- кількість всіх можливих ключів шифру має бути такою, щоб їх повний перебір за допомогою сучасних інформаційних технологій (в т.ч. і розподілених обчислень) був неможливий за прийнятне для противника час;

- будь-який ключ з множини можливих повинен забезпечувати надійний захист інформації;

- незначна зміна ключа повинно приводити до істотної зміни виду зашифрованого повідомлення;

- надмірність повідомлень, що вноситься в процесі шифрування, повинна бути якомога меншою (хорошим вважається результат, коли довжина шифрограми не перевищує довжину вихідного тексту);

- зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа.

1.5 Постановка задач досліджень

Як показав проведений аналітичний огляд сучасного стану систем захисту інформації, криптографічних систем та крипто аналізу криптографія залишається сьогоднішні найбільш ефективним і найбільш поширеним засобом захисту інформації. Не зважаючи на всі ризики комп’ютерна криптографія є основним засобом захисту інформації у кіберпросторі.

Розробкою нових та вдосконаленням існуючих крипто алгоритмів займається велике коло науковців та практиків. Не зважаючи на всі їхні здобутки, залишаються невирішеними багато задач, однією з яких є підвищення невизначеності результатів шифрування. Особливо актуальною є дана задача для в криптосистем в алгоритми яких використовують псевдовипадкові послідовності. Створення і розвиток

квантових комп'ютерів та стрімке збільшення хмарних сховищ вимагають застосування нових підходів які забезпечать створення високошвидкісної потокової комп'ютерної криптографії, та зможуть гарантувати досягнення максимальної невизначеності результатів шифрування.

На основі проведеного аналітичного огляду формулюються мета та задачі наукового дослідження.

Основною метою роботи є підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

– розроблення методу синтезу операцій криптографічного перетворення інформації, які забезпечують максимальну невизначеність результатів шифрування;

– розроблення методу синтезу операцій за критерієм строгого стійкого кодування мінімальної складності;

– удосконалення методу синтезу програмних та апаратних засобів комп'ютерної криптографії для забезпечення підвищення невизначеності результатів шифрування.

ВИСНОВКИ ДО РОЗДІЛУ 1

1. Проведений аналітичний огляд криптосистем показав необхідність та доцільністи проведення аналізу якості систем та вибору вимог для їх порівняння та оцінки.

2. Проводиться детельний огляд властивості "лавинного ефекту" та показники для його оцінки.

3. Розглядаються питання теоретичної та практичної оцінки надійності та безпеки криптографічних систем

4. На основі проведених досліджень формулюються мета та задачі дисертаційної роботи.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ДВОХРОЗРЯДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ

2.1. Аналіз двох розрядних операцій криптографічного перетворення по критерію строгого лавинного ефекту

Однією із характеристик криптографічних алгоритмів є лавинний ефект.

Лавинний ефект (англ. *Avalanche effect*) – поняття в криптографії, яке застосовується до блочних шифрів та хеш-функцій. Це важлива криптографічна властивість для шифрування, яка означає, що зміна значення малої кількості бітів у вхідному тексті або в ключі веде до великої кількості значень біт вихідної інформації. Іншими словами: зміна значення малої кількості бітів у вхідному тексті або в ключі, веде до «лавинної» зміни значень вихідних бітів шифротексту [93].

Термін «лавинний ефект» вперше був введений Х. Фейстелем в статті Cryptography and Computer Privacy, опублікованій в журналі Scientific American в травні 1978 року, хоча концептуальне поняття використовувалося ще Шенноном [89].

В алгоритмах з декількома проходами лавинний ефект зазвичай досягається завдяки тому, що на кожному проході зміна одного вхідного біта веде до зміни декількох вихідних бітів [89].

Для кількісної оцінки лавинного ефекту запропоновано використання строгого лавинного критерію (СЛК). Визначення СЛК вперше було дано С. Таваресом та А. Вебстером в роботі з дослідження S-блоків. Булеву функцію можна розглядати як частину структури S-блоків. Дизайн S-блоків, що задовольняють СЛК, був вивчений в роботах Адамса та С. Тавареса.

Криптографічний алгоритм задовольняє строгому лавинному критерію, якщо при зміні одного біта вхідної послідовності кожний біт вихідної послідовності змінюється з імовірністю одна друга [90].

$$\lambda_{слк} = 1/2 \tag{2.1}$$

Починаючи з 1990 року основні дослідження СЛК проводилися в контексті дослідження булевих функцій [90].

Булева функция $f(x)$, де x — вектор із n змінних, задовольняє СЛК, якщо при зміні одного із n вхідніх бітів вихідний біт змінюється з ймовірністю рівно $1/2$ [91, 92].

Розглянемо можливість отримання СЛК на прикладі операцій криптографічного перетворення інформації.

Криптографічна операція – це понумерований набір елементарних функцій які в сукупності забезпечують виконання криптографічного перетворення [94].

Елементарна функція – це функція криптографічного перетворення множини вхідних значень в одне вихідне значення [94].

Двохрозрядна операція криптографічного перетворення інформації – це операція яка включає в себе дві елементарні функції.

Проведемо аналіз двохрозрядних операцій криптографічного перетворення інформації по критерію строгого лавинного ефекту.

Повна множина дворозрядних операцій криптографічного перетворення інформації (криптографічного кодування) наведена в табл.2.1. [93].

Слід відмітити, що всі 24 операції криптографічного перетворення інформації побудовані на основі наступних 6 елементарних функцій:

$$f_3(x) = x_1; \tag{2.2}$$

$$f_5(x) = x_2; \tag{2.3}$$

$$f_6(x) = x_1 \oplus x_2; \tag{2.4}$$

$$f_9(x) = x_1 \oplus x_2 \oplus 1; \quad (2.5)$$

$$f_{10}(x) = x_2 \oplus 1; \quad (2.6)$$

$$f_{12}(x) = x_1 \oplus 1. \quad (2.7)$$

Таблиця 2.1

Повна група дворозрядних операцій криптографічного перетворення інформації

№	операція	№	операція	№	операція	№	операція
1	$F_{3,5} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	**7**	$F_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	**13**	$F_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	**19**	$F_{12,10} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
2	$F_{6,5} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$	**8**	$F_{6,10} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$	**14**	$F_{9,5} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$	**20**	$F_{9,10} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
3	$F_{3,6} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$	**9**	$F_{3,9} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	**15**	$F_{12,6} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	**21**	$F_{12,9} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
4	$F_{5,3} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	**10**	$F_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	**16**	$F_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	**22**	$F_{10,12} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
5	$F_{5,6} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$	**11**	$F_{5,9} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	**17**	$F_{10,6} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	**23**	$F_{10,9} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
6	$F_{6,3} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$	**12**	$F_{6,12} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$	**18**	$F_{9,3} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$	**24**	$F_{9,12} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

Дослідження елементарних функцій на відповідність СЛК може проходити в двох варіантах (або режимах):

- статичний режим, коли досліджуються на основі таблиці істинності зміни одного біта вхідної інформації і провіряється зміна результатів перетворення. Кількість змінених результатів повинна бути $1/2$ від загальної кількості отриманих в процесі перевірки результатів»
- динамічний режим, коли досліджуються на основі таблиці істинності зміни результатів виконання функцій при послідовній обробці повних наборів вхідних даних які відрізняються один від одного на один біт.

Дослідимо елементарну функцію (2.2) на відповідність СЛК в статичному режимі.

Нехай вхідні дані задані множиною $M(x) = \{00, 01, 10, 11\}$.

Результат виконання елементарної $f_3(x) = x_1$ на множині вхідних даних сформує множину $M(f_3(x)) = \{0, 0, 1, 1\}$.

При визначення СЛК будемо визначати зміну бітів вихідної послідовності $M(f_3(x))$, при зміні одного чи декількох біт вхідної послідовності $M(x)$.

Нехай буде інвертовано x_1 - перший біт вхідної послідовності. Тоді вхідна послідовність стане задана множиною $M(x_{\bar{1}}) = \{10, 11, 00, 01\}$, а результат виконання $f_3(x)$ сформує множину $M(f_3(x_{\bar{1}})) = \{0, 0, 1, 1\}$.

Визначимо кількість змін вихідної послідовності через кодову відстань за Хемінгом.

$$M(f_3(x) \oplus f_3(x_{\bar{1}})) = \{1, 1, 1, 1\} = \{1_4\}.$$

Визначимо $\lambda_{слк}$ через $M(f_3(x) \oplus f_3(x_{\bar{1}}))$.

$$\lambda_{слк}(f_3(x_{\bar{1}})) = 1. \qquad (2.8)$$

Нехай буде інвертовано x_2 - перший біт вхідної послідовності. Тоді вхідна послідовність стане задана множиною $M(x_{\bar{2}}) = \{01, 00, 11, 10\}$, а $M(f_3(x_{\bar{2}})) = \{0, 0, 1, 1\}$. Виходячи з множини $M(f_3(x_{\bar{2}}))$ отримаємо $M(f_3(x) \oplus f_3(x_{\bar{2}})) = \{0, 0, 0, 0\} = \{0_4\}$, а

$$\lambda_{слк}(f_3(x_{\bar{2}})) = 0. \qquad (2.9)$$

Якщо буде інвертовано перший (x_1) і другий (x_2) біти вхідної послідовності, тоді вхідна послідовність буде задана множиною $M(x_{\overline{1},\overline{2}}) = \{11, 10,\ 01, 00\}$, а $M(f_3(x_{\overline{1}\overline{2}})) = \{1, 1,\ 0,\ 0\}$.

Визначимо кількість змін вихідної послідовності через кодову відстань за Хемінгом $M(f_3(x) \oplus f_3(x_{\overline{1}\overline{2}})) = \{1, 1,\ 1,\ 1\} = \{1_4\}$. Виходячи з цього

$$\lambda_{слк}(f_3(x_{\overline{1}\overline{2}})) = 1. \qquad (2.10)$$

Вирази (2.8) – (2.10) дозволяють стверджувати, що елементарних функцій $f_3(x) = x_1$ не відповідає вимогам СЛК, тому що зміна одного з вхідних бітів, або обох вхідних бітів приводить до зміни всіх вихідних біт, або жоден з вихідних біт не буде змінено.

По аналогії проведемо дослідження елементарних функцій (2.3 – 2.7) на основі яких будуються операції криптографічного перетворення інформації. Результати дослідження елементарних функцій (2.2 – 2.7) по СЛК, на основі яких будуються двохрозрядні операції криптографічного перетворення інформації наведені в табл. 2.2. [2].

Таблиця 2.2.

Результати дослідження дворозрядних елементарних функцій для криптоперетворенні на СЛК

Вхідні дані														Інверсія x_1											
x_1	x_2	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$		$\overline{x}_1$	x_2	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$	
0	0	0	–	0	–	0	–	1	–	1	–	1	–	1	0	1	+	0	–	1	+	0	+	1	–	0	–
0	1	0	–	1	–	1	–	0	–	0	–	1	–	1	1	1	+	1	–	0	+	1	+	0	–	0	–
1	0	1	–	0	–	1	–	0	–	1	–	0	–	0	0	0	+	0	–	0	+	1	+	1	–	1	–
1	1	1	–	1	–	0	–	1	–	0	–	0	–	0	1	0	+	1	–	1	+	0	+	0	–	1	–
		0		**0**		**0**		**0**		**0**		**0**				**4**		**0**		**4**		**4**		**0**		**0**	
Інверсія x_2														Інверсія x_1 і x_2											
x_1	$\overline{x}_2$	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$		$\overline{x}_1$	$\overline{x}_2$	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$	
0	1	0	–	1	+	1	+	0	+	0	–	1	+	1	1	1	+	1	+	0	–	1	–	0	–	0	–
0	0	0	–	0	+	0	+	1	+	1	–	1	+	1	0	1	+	0	+	1	–	0	–	1	–	0	–
1	1	1	–	0	+	0	+	1	+	0	–	0	+	0	1	0	+	1	+	1	–	0	–	0	–	1	–
1	0	1	–	1	+	1	+	0	+	1	–	0	+	0	0	0	+	0	+	0	–	1	–	1	–	1	–
		0		**4**		**4**		**4**		**0**		**4**				**4**		**4**		**0**		**0**		**0**		**0**	

Як видно з табл. 2.2 жодна з елементарних функцій не може бути використана в крипто перетвореннях, які будуються на основі синтезованих двох розрядних операцій, тому що зміна одного з вхідних бітів, або обох вхідних бітів приводить до зміни всіх вихідних біт, або жоден з вихідних біт не буде змінено.

Виходячи з отриманих результатів можна зробити висновок, що двохрозрядні елементарні функції на основі яких будуються операції криптографічного перетворення інформації не відповідають вимогам СЛК, або двохрозрядні елементарні функції, які відповідають вимогам СЛК, не можуть бути використані при побудові операцій криптографічного перетворення інформації.

Розглянемо можливість використання елементарних функцій (2.2) – (2.7) для ефективної реалізації схем розгортки ключів. Для цього дослідимо дані елементарні функції на відповідність СЛК в динамічному режимі. Для цього знайдемо всі можливі варіанти послідовності вхідних значень для елементарних функцій, в яких кожне наступне значення порівняно з попереднім має кодову відстань по Хемінгу рівною 1. Слід відмітити, що наступним для останнього є перший елемент. Для цього розглянемо варіанти перестановок чотирьох елементів, наведених в табл. 2.3.

Таблиця 2.3

Варіанти перестановок чотирьох елементів

Перестановка		Перестановка		Перестановка		Перестановка	
1	a b c d	7	b a c d	13	c b a d	19	d b c a
2	a b d c	8	b a d c	14	c b d a	20	d b a c
3	a c d b	9	b c d a	15	c a d b	21	d c a b
4	a c b d	10	b c a d	16	c a b d	22	d c b a
5	a d b c	11	b d a c	17	c d b a	23	d a b c
6	a d c b	12	b d c a	18	c d a b	24	d a c b

Необхідність розгляду всіх варіантів перестановок покликана виключити можливу невідповідність СЛК.

Якщо припустити, що: a=00, b=01, c=10, d=11, тоді відстані по Хемінгу між елементами послідовності будуть наведені в табл. 2.4.

Підставимо відстані по Хемінгу між елементами послідовності (табл. 2.3), у варіанти перестановок елементів (табл. 2.2) визначимо варіанти послідовності вхідних значень для дослідження елементарних функцій. Отримані варіанти перестановок виділені сірим кольором в табл.2.5.

Таблиця 2.4

Відстані по Хемінгу між елементами послідовності

	a	**b**	**c**	**d**
a	**0**	**1**	**1**	**2**
b	**1**	**0**	**2**	**1**
c	**1**	**2**	**0**	**1**
d	**2**	**1**	**1**	**0**

Таблиця 2.5

Варіанти послідовності вхідних значень для дослідження елементарних функцій

Перестановка		**Перестановка**		**Перестановка**		**Перестановка**	
1	a b c d	**7**	b a c d	**13**	c b a d	**19**	d b c a
	1 2 1 2		**1 1 1 1**		**2 1 2 1**		**1 2 1 2**
2	a b d c	**8**	b a d c	**14**	c b d a	**20**	d b a c
	1 1 1 1		**1 2 1 2**		**2 1 2 1**		**1 1 1 1**
3	a c d b	**9**	b c d a	**15**	c a d b	**21**	d c a b
	1 1 1 1		**2 1 2 1**		**1 2 1 2**		**1 1 1 1**
4	a c b d	**10**	b c a d	**16**	c a b d	**22**	d c b a
	1 2 1 2		**2 1 2 1**		**1 1 1 1**		**1 2 1 2**
5	a d b c	**11**	b d a c	**17**	c d b a	**23**	d a b c
	2 1 2 1		**1 2 1 2**		**1 1 1 1**		**2 1 2 1**
6	a d c b	**12**	b d c a	**18**	c d a b	**24**	d a c b
	2 1 2 1		**1 1 1 1**		**1 2 1 2**		**2 12 1**

Дослідимо елементарні функції на СЛК з використанням перестановки №2, так як дана перестановка забезпечую послідовну зміну одного біта інформації на кожному з 4 циклів перетворення. Виходячи з даної постановки задачі СЛК для

схеми розгортки ключів буде визначатися як кількість змін вихідного символу на повній множині вхідних даних.

Результати дослідження елементарних функції на СЛК з використанням перестановки №2 представлені в табл. 2.6. Як видно з даної таблиці на перестановці №2 лише функції $f_5(x)$ і $f_{10}(x)$ відповідають СЛК. Проте слід відмітити, що для використання в схемі розгортки ключів елементарна функція повинні відповідати СЛК на всій множині визначених перестановок.

Дослідження елементарних функцій для операцій криптоперетворення інформації на множині визначених перестановок наведена в табл. 2.7.

Таблиця 2.6

Результати дослідження елементарних функцій на СЛК з використанням перестановки №2

Вхідні дані								Результати перестановки №2							
	$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$		$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$
a	00	0	0	0	1	1	1	a	00	0	0	0	1	1	1
b	01	0	1	1	0	0	1	b	01	0	1	1	0	0	1
c	10	1	0	1	0	1	0	d	11	1	1	0	1	0	0
d	11	1	1	0	1	0	0	c	10	1	0	1	0	1	0
		1	3	2	2	3	1			1	2	3	3	2	1

Таблиця 2.7

Результати дослідження елементарних функцій на СЛК в динамічному режимі

Результати перестановки №2								Результати перестановки №3							
	$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$		$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$
a	00	0	0	0	1	1	1	a	00	0	0	0	1	1	1
b	01	0	1	1	0	0	1	c	10	1	0	1	0	1	0
d	11	1	1	0	1	0	0	d	11	1	1	0	1	0	0
c	10	1	0	1	0	1	0	b	01	0	1	1	0	0	1
		1	2	3	3	2	1			2	1	3	3	1	4
Результати перестановки №7								Результати перестановки №12							
	$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$		$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$
b	01	0	1	1	0	0	1	b	01	0	1	1	0	0	1
a	00	0	0	0	1	1	1	d	11	1	1	0	1	0	0
c	10	1	0	1	0	1	0	c	10	1	0	1	0	1	0
d	11	1	1	0	1	0	0	a	00	0	0	0	1	1	1
		1	2	3	3	2	1			2	1	3	3	1	2
Результати перестановки №16								Результати перестановки №17							

	$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$		$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$
c	10	1	0	1	0	1	0	c	10	1	0	1	0	1	0
a	00	0	0	0	1	1	1	d	11	1	1	0	1	0	0
b	01	0	1	1	0	0	1	b	01	0	1	1	0	0	1
d	11	1	1	0	1	0	0	a	00	0	0	0	1	1	1
		2	1	3	3	1	2			1	2	3	3	2	1
Результати перестановки №20								Результати перестановки №21							
	$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$		$x_1\ x_2$	$f_3(x)$	$f_5(x)$	$f_6(x)$	$f_9(x)$	$f_{10}(x)$	$f_{12}(x)$
d	11	1	1	0	1	0	0	d	11	1	1	0	1	0	0
b	01	0	1	1	0	0	1	c	10	1	0	1	0	1	0
a	00	0	0	0	1	1	1	a	00	0	0	0	1	1	1
c	10	1	0	1	0	1	0	b	01	0	1	1	0	0	1
		2	1	3	3	1	2			1	2	3	3	2	1

Аналіз табл. 2.7 показав, що елементарні функції на основі яких будуються операції криптографічного перетворення інформації, як самостійні операції недоцільно використовувати в схемах розгортки ключів, так як вони не відповідають СЛК на повній множині вибраних перестановок.

Проведене дослідження показало, що СЛК не доцільно використовувати для оцінки елементарних функцій і операцій криптографічного перетворення, так як даний критерій відображає вплив незначної зміни бітів ключа, або бітів інформації на результат шифрування. Даний критерій не дозволяє оцінити придатність елементарної функції для реалізації в операції криптографічного перетворення інформації, а також не дає можливості оцінити результат реалізації самої операції крипто перетворення.

2.2. Аналіз двох розрядних операцій криптографічного перетворення по критерію строгого стійкого кодування

Для якісної оцінки придатності використання операцій криптографічного перетворення інформації в крипто алгоритмах, по аналогії з лавинним ефектом введемо поняття стійкого кодування (СК). Стійке кодування – поняття, яке буде

застосовуватися для блочних і потокових шифрів і буде означати, що незалежно від зміни кількості біт у вхідному текст, чи ключі, в процесі перетворення буде змінена значна кількість біт вхідного тексту[3, 9].

Для кількісної оцінки стійкого кодування по аналогії з строгим лавинним критерієм запропоновано використання критерію строгого стійкого кодування (ССК) [9].

Криптографічний алгоритм, або операція криптографічного перетворення інформації задовольняє критерію строгому строгого стійкого кодування, якщо не залежно від ключа крипто алгоритму, або від вибраної операції криптографічного перетворення інформації кожний біт вихідної послідовності змінюється відносно вхідної інформації з імовірністю одна друга [3]..

$$\lambda_{ссk} = 1/2 \tag{2.11}$$

Виходячи з сформульованого визначення ССК доцільно досліджувати або криптоалгоритми, або операції криптографічного перетворення інформації. Досліджувати окремі елементарні функції, якщо це функції декількох змінних не представляється можливим, тому що в процесі їх виконання буде отримано лише один біт вихідної інформації, при декількох вхідних бітах, і $\lambda_{ссk}$ не буде розрахована.

Закономірним стає питання, чи можливо гарантовано отримати криптоалагоритми, які задовольняють вимогам критерію ССК. Правильну відповідь на дане запитання можна отримати лише отримавши операції які відповідають вимогам критерію ССК. На сьогоднішній день операції криптографічного перетворення не досліджувались на відповідність критерію ССК. Розглянемо можливість досягнення ССК на прикладі дворозрядних операцій криптографічного кодування наведених в табл. 2.1.

Нехай вхідні дані задані множиною $M(x) = \{00, 01, 10, 11\}$.

Результати виконання операції $F_{3,5}(x)$ на множині вхідних даних сформують множину $M(F_{3,5}(x)) = \{00, 01, 10, 11\}$.

Визначимо кількість змін вихідної послідовності через кодову відстань за Хемінгом для множини вхідних даних (множина кількості змін в словах вхідної інформації):

$$M(x \oplus M(F_{3,5}(x)) = \{0, 0, 0, 0\}.$$

Визначимо множину $\lambda_{сск}$ через $M(x \oplus M(F_{3,5}(x))$.

$$M(\lambda_{cck}(F_{3,5}) = \{0, 0, 0, 0\};$$

$$\lambda_{cck}(F_{3,5}(x)) = 0$$

Операції $F_{3,5}(x)$ не задовольняє критерію ССК.

Результати виконання операції $F_{6,5}(x)$ на множині вхідних даних сформують множину $M(F_{6,5}(x)) = \{00, 11, 10, 01\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{6,5}(x)) = \{0, 1, 0, 1\}$, а $M(\lambda_{cck}(F_{6,5}) = \{0, 1/2, 0, 1/2\}$; $\lambda_{cck}(F_{6,5}(x)) = 2/8 = 1/4$.

Операції $F_{6,5}(x)$ не задовольняє критерію ССК.

Результати виконання операції $F_{3,6}(x)$ на множині вхідних даних сформують множину $M(F_{3,6}(x)) = \{00, 01, 11, 10\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{3,6}(x)) = \{0, 0, 1, 1\}$, а $M(\lambda_{cck}(F_{3,6}) = \{0, 0, 1/2, 1/2\}$; $\lambda_{cck}(F_{3,6}(x)) = 1/4$.

Операції $F_{3,6}(x)$ не задовольняє критерію ССК.

Результати виконання операції $F_{5,3}(x)$ на множині вхідних даних сформують множину $M(F_{5,3}(x)) = \{00, 10,\ 01,\ 11\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{5,3}(x)) = \{0, 2,\ 2,\ 0\}$, а $M(\lambda_{cck}(F_{5,3}) = \{0, 2/2, 2/2, 0\}$; $\lambda_{cck}(F_{5,3}(x)) = 4/8 = 1/2$.

Не зважаючи на те, що $\lambda_{cck}(F_{5,3}(x)) = 1/2$, операції $F_{3,6}(x)$ не задовольняє критерію ССК, тому що при перетворення вхідних дворозрядних блоків інформації «00» і «11» не буде змінено жодного з вхідних бітів, а при перетворення вхідних блоків «01» і «10» буде змінено всі біти.

Результати виконання операції $F_{5,6}(x)$ на множині вхідних даних сформують множину $M(F_{5,6}(x)) = \{00, 11,\ 01,\ 10\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{5,6}(x)) = \{0, 1,\ 2,\ 1\}$, а $M(\lambda_{cck}(F_{5,6}) = \{0, 1/2, 2/2, 1/2\}$; $\lambda_{cck}(F_{5,6}(x)) = 4/8 = 1/2$.

Операції $F_{5,6}(x)$ не задовольняє критерію ССК, тому що при перетворення вхідного дворозрядних блока інформації «00» не буде змінено жодного з вхідних бітів, а при перетворенні вхідного блоку «01» буде змінено обидва біти інформації.

Результати виконання операції $F_{6,3}(x)$ на множині вхідних даних сформують множину $M(F_{6,3}(x)) = \{00, 10,\ 11,\ 01\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{6,3}(x)) = \{0, 2,\ 1,\ 1\}$, а $M(\lambda_{cck}(F_{6,3}) = \{0, 2/2, 1/2, 1/2\}$; $\lambda_{cck}(F_{6,3}(x)) = 4/8 = 1/2$.

Не зважаючи на те, що $\lambda_{cck}(F_{6,3}(x)) = 1/2$, операції $F_{6,3}(x)$ не задовольняє критерію ССК, тому що при перетворенні блоку інформації «00» не буде змінено

жодного з вхідних бітів, а при перетворенні вхідного блоку «01» буде змінено обидва біти інформації.

Результати виконання операції $F_{3,10}(x)$ на множині вхідних даних сформують множину $M(F_{3,10}(x)) = \{01, 00, 11, 10\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{3,10}(x)) = \{1, 1, 1, 1\}$, а $M(\lambda_{cck}(F_{3,10}) = \{1/2, 1/2, 1/2, 1/2\}$; $\lambda_{cck}(F_{3,10}(x)) = 1/2$.

Операції $F_{3,10}(x)$ задовольняє критерію ССК, тому що при перетворенні будь якого блоку вхідної інформації не буде змінено кожен другий біт.

Результати виконання операції $F_{6,10}(x)$ на множині вхідних даних сформують множину $M(F_{6,10}(x)) = \{01, 10, 11, 00\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{6,10}(x)) = \{1, 2, 1, 2\}$, а $M(\lambda_{cck}(F_{6,10}) = \{1/2, 2/2, 1/2, 2/2\}$; $\lambda_{cck}(F_{6,10}(x)) = 4/8 = 1/2$.

Операції $F_{6,10}(x)$ не задовольняє критерію ССК, тому що при перетворенні блоків вхідної інформації «01» і «11» буде змінено обидва біти.

Результати виконання операції $F_{3,9}(x)$ на множині вхідних даних сформують множину $M(F_{3,9}(x)) = \{01, 00, 10, 11\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{3,9}(x)) = \{1, 1, 0, 0\}$, а $M(\lambda_{cck}(F_{3,9}) = \{1/2, 1/2, 0, 0\}$; $\lambda_{cck}(F_{3,9}(x)) = 4/8 = 1/2$.

Операції $F_{3,9}(x)$ не задовольняє критерію ССК, тому що при перетворенні блоків вхідної інформації «10» і «11» не буде змінено жодного біта.

Результати виконання операції $F_{5,12}(x)$ на множині вхідних даних сформують множину $M(F_{5,12}(x)) = \{01, 11, 00, 10\}$. Тоді множина кількості

змін в словах вхідної інформації буде, $M(x \oplus M(F_{5,12}(x)) = \{1, 1, 1, 1\}$, а $M(\lambda_{cck}(F_{5,12}) = \{1/2, 1/2, 1/2, 1/2\}$; $\lambda_{cck}(F_{5,12}(x)) = 1/2$.

Операції $F_{5,12}(x)$ задовольняє критерію ССК, тому що при перетворенні будь якого блоку вхідної інформації не буде змінено кожен другий біт.

Результати виконання операції $F_{5,9}(x)$ на множині вхідних даних сформують множину $M(F_{5,9}(x)) = \{01, 10, 00, 11\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{5,9}(x)) = \{1, 2, 1, 0\}$, а $M(\lambda_{cck}(F_{5,9}) = \{1/2, 2/2, 1/2, 0\}$; $\lambda_{cck}(F_{5,9}(x)) = 4/8 = 1/2$.

Операції $F_{5,9}(x)$ не задовольняє критерію ССК, тому що при перетворенні блока вхідної інформації «01» буде змінено два біти, а при перетворенні блоку і «11» жодний біт не буде змінено.

Результати виконання операції $F_{6,12}(x)$ на множині вхідних даних сформують множину $M(F_{6,12}(x)) = \{01, 11, 10, 00\}$. Множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{6,12}(x)) = \{1, 1, 0, 2\}$.

Тоді $M(\lambda_{cck}(F_{6,12}) = \{1/2, 1/2, 0, 2/2\}$; $\lambda_{cck}(F_{6,12}(x)) = 4/8 = 1/2$.

Операції $F_{6,12}(x)$ не задовольняє критерію ССК, тому що при перетворенні блока вхідної інформації «11» буде змінено два біти, а при перетворенні блоку і «10» жодний біт не буде змінено.

Результати виконання операції $F_{12,5}(x)$ на множині вхідних даних сформують множину $M(F_{12,5}(x)) = \{10, 11, 00, 01\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{12,5}(x)) = \{1, 1, 1, 1\}$, а $M(\lambda_{cck}(F_{12,5}) = \{1/2, 1/2, 1/2, 1/2\}$; $\lambda_{cck}(F_{12,5}(x)) = 1/2$.

Операції $F_{12,5}(x)$ задовольняє критерію ССК, тому що при перетворенні будь якого блоку вхідної інформації не буде змінено кожен другий біт.

Результати виконання операції $F_{9,5}(x)$ на множині вхідних даних сформують множину $M(F_{9,5}(x)) = \{10,\ 01,\ 00,\ 11\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{9,5}(x)) = \{1, 0,\ 1,\ 0\}$, а $M(\lambda_{cck}(F_{9,5}) = \{1/2, 0, 1/2, 0\}$; $\lambda_{cck}(F_{9,5}(x)) = 1/2$.

Операції $F_{9,5}(x)$ не задовольняє критерію ССК, тому що при перетворенні блоків вхідної інформації «01» і «11» жодний біт не буде змінено.

Результати виконання операції $F_{12,6}(x)$ на множині вхідних даних сформують множину $M(F_{12,6}(x)) = \{10,\ 11,\ 01,\ 00\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{12,6}(x)) = \{1, 1,\ 2,\ 2\}$, а $M(\lambda_{cck}(F_{12,6}) = \{1/2, 1/2, 2/2, 2/2\}$; $\lambda_{cck}(F_{12,6}(x)) = 6/8 = 3/4$.

Операції $F_{12,6}(x)$ не задовольняє критерію ССК.

Результати виконання операції $F_{10,3}(x)$ на множині вхідних даних сформують множину $M(F_{10,3}(x)) = \{10,\ 00,\ 11,\ 01\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{10,3}(x)) = \{1, 1,\ 1,\ 1\}$, а $M(\lambda_{cck}(F_{10,3}) = \{1/2, 1/2, 1/2, 1/2\}$; $\lambda_{cck}(F_{10,3}(x)) = 1/2$.

Операції $F_{10,3}(x)$ задовольняє критерію ССК, тому що при перетворенні будь якого блоку вхідної інформації не буде змінено кожен другий біт.

Результати виконання операції $F_{10,6}(x)$ на множині вхідних даних сформують множину $M(F_{10,6}(x)) = \{10,\ 01,\ 11,\ 00\}$. Тоді множина кількості

змін в словах вхідної інформації буде, $M(x \oplus M(F_{10,6}(x)) = \{1, 0, 1, 2\}$, а $M(\lambda_{cck}(F_{10,6}) = \{1/2, 0, 1/2, 2/2\}$; $\lambda_{cck}(F_{10,6}(x)) = 4/8 = 1/2$.

Операції $F_{10,6}(x)$ не задовольняє критерію ССК, тому що при перетворенні блока вхідної інформації «11» буде змінено два біти, а при перетворенні блоку «01» жодний біт не буде змінено.

Результати виконання операції $F_{9,3}(x)$ на множині вхідних даних сформують множину $M(F_{9,3}(x)) = \{10, 00, 01, 11\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{9,3}(x)) = \{1, 1, 2, 0\}$, а $M(\lambda_{cck}(F_{9,3}) = \{1/2, 1/2, 2/2, 0\}$; $\lambda_{cck}(F_{9,3}(x)) = 4/8 = 1/2$.

Операції $F_{9,3}(x)$ не задовольняє критерію ССК, тому що при перетворенні блока вхідної інформації «10» буде змінено два біти, а при перетворенні блоку «11» жодний біт не буде змінено.

Результати виконання операції $F_{12,10}(x)$ на множині вхідних даних сформують множину $M(F_{12,10}(x)) = \{11, 10, 01, 00\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{12,10}(x)) = \{2, 2, 2, 2\}$, а $M(\lambda_{cck}(F_{12,10}) = \{2/2, 2/2, 2/2, 2/2\}$; $\lambda_{cck}(F_{12,10}(x)) = 8/8 = 1$.

Операції $F_{12,10}(x)$ не задовольняє критерію ССК.

Результати виконання операції $F_{12,9}(x)$ на множині вхідних даних сформують множину $M(F_{12,9}(x)) = \{11, 10, 00, 01\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{12,9}(x)) = \{2, 2, 1, 1\}$, а $M(\lambda_{cck}(F_{12,9}) = \{2/2, 2/2, 1/2, 1/2\}$; $\lambda_{cck}(F_{12,9}(x)) = 6/8 = 3/4$.

Операції $F_{12,9}(x)$ не задовольняє критерію ССК.

Результати виконання операції $F_{10,12}(x)$ на множині вхідних даних сформують множину $M(F_{10,12}(x)) = \{11,\ 01,\ 10,\ 00\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{10,12}(x)) = \{2, 0,\ 0,\ 2\}$, а $M(\lambda_{cck}(F_{10,12}) = \{2/2, 0, 0, 2/2\}$; $\lambda_{cck}(F_{12,9}(x)) = 4/8 = 1/2$.

Операції $F_{10,12}(x)$ не задовольняє критерію ССК, тому що при перетворення вхідних дворозрядних блоків інформації «01» і «10» не буде змінено жодного з вхідних бітів, а при перетворення вхідних блоків «00» і «11» буде змінено всі біти.

Результати виконання операції $F_{10,9}(x)$ на множині вхідних даних сформують множину $M(F_{10,9}(x)) = \{11,\ 00,\ 10,\ 01\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{10,9}(x)) = \{2, 1,\ 0,\ 1\}$, а $M(\lambda_{cck}(F_{10,9}) = \{2/2, 1/2, 0, 1/2\}$; $\lambda_{cck}(F_{10,9}(x)) = 4/8 = 1/2$.

Операції $F_{10,9}(x)$ не задовольняє критерію ССК, тому що при перетворенні блока вхідної інформації «00» буде змінено два біти, а при перетворенні блоку і «10» жодний біт не буде змінено.

Результати виконання операції $F_{9,12}(x)$ на множині вхідних даних сформують множину $M(F_{9,12}(x)) = \{11,\ 01,\ 00,\ 10\}$. Тоді множина кількості змін в словах вхідної інформації буде, $M(x \oplus M(F_{9,12}(x)) = \{2, 0,\ 1,\ 1\}$, а $M(\lambda_{cck}(F_{9,12}) = \{2/2,\ 0, 1/2, 1/2\}$; $\lambda_{cck}(F_{9,12}(x)) = 4/8 = 1/2$.

Операції $F_{9,12}(x)$ не задовольняє критерію ССК, тому що при перетворенні блока вхідної інформації «00» буде змінено два біти, а при перетворенні блоку і «01» жодний біт не буде змінено.

Слід відмітити, що для всіх 24 двохрозрядних операцій криптографічного перетворення характерні наступні властивості:

- множина значень $M(F_{i,j}(x))$ включає в себе перестановку двійкових значень цифр від 0 до 3;
- кількість блоків вихідної інформації які відповідають вимогам ССК в множині вихідних блоків може бути 0, 2 або 4;

кількість блоків вихідної інформації які не відповідають вимогам ССК в множині вихідних блоків може бути 0, 2 або 4.

На основі проведених досліджень було встановлено, що серед 24 двохрозрядних операцій криптографічного перетворення лише 4 операції відповідають вимогам критерію ССК [9]

$$F_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \tag{2.12}$$

$$F_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \tag{2.13}$$

$$F_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \tag{2.14}$$

$$F_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} \tag{2.15}$$

Визначення операцій які відповідають вимогам критерію ССК дозволяють провести їх детальне дослідження, і зробити спробу встановлення для них загальних залежностей, а також запропонувати гіпотезу для розробки методів синтезу операцій за критерієм ССК.

2.3. Дослідження двохрозрядних операцій криптографічного перетворення які відповідають вимогам критерію строгого стійкого кодування

Розглянемо більш детально операції криптографічного перетворення, які відповідають вимогам критерію ССК (2.12 – 2.15). Таблиці істинності даних операцій наведено в табл. 2.8 [9].

Таблиця 2.8

Таблиці істинності даних операцій які відповідають вимогам критерію ССК

Вхідна інформація		Результати перетворення вхідної інформації							
		$F_{3,10}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$		$F_{12,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$		$F_{10,3}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$		$F_{5,12}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	
0	0	0	1	1	0	1	0	0	1
0	1	0	0	1	1	0	0	1	1
1	0	1	1	0	0	1	1	0	0
1	1	1	0	0	1	0	1	1	0

Аналіз табл. 2.8 показав наступне:

- двох розрядні операції, які відповідають вимогам критерію ССК, в одній з двох елементарних функцій мають операцію інверсії ($F_{3,10}(x)$ та $F_{5,12}(x)$ мають інверсну другу елементарну функцію; $F_{12,5}(x)$ та $F_{10,3}(x)$ мають інверсну першу елементарну функцію;
- елементарні функції в операціях є простими (залежать лише від одної змінної) і використовуються в прямій послідовності ($F_{3,10}(x)$ і $F_{12,5}(x)$), або в оберненій ($F_{10,3}(x)$ і $F_{5,12}(x)$);
- якщо елементарні функції в операціях використовуються в прямій послідовності по буде інвертований один з двох розрядів в елементарній функції перетворення якого присутня операція інверсії;
- якщо елементарні функції в операціях використовуються в оберненій послідовності по буде інвертовано по половині біт в першому розряді і в

другому розряді не залежно від розміщення елементарної функції перетворення якій присутня операція інверсії.

Дослідимо варіанти застосування

Розглянемо варіанти застосування операцій, які відповідають вимогам критерію ССК. Дані варіанти можна поділити на три групи в основі яких лежать наступні підходи:

- з однораундовим застосуванням операцій криптографічного перетворення, які відповідають вимогам критерію ССК;
- з двохраундовим застосуванням операцій криптографічного перетворення, які відповідають вимогам критерію ССК;
- з багатораундовим застосуванням операцій криптографічного перетворення, які відповідають вимогам критерію ССК.

При однораундрму застосуванню операцій криптографічного перетворення, які відповідають вимогам критерію ССК (2.12 – 2.15) на фінальній стадії шифрування криптосистема забезпечить відповідність вимогам критерію ССК.

Визначимо відповідність результатів шифрування при двохраундовому застосуванні операцій з ССК на фінальній стадії крипто перетворення. Так як дві випадково вибрані операції криптоперетворення, які відповідають вимогам критерію ССК виконуються послідовно, а всі двох розрядні операції представляють собою математичну групу [Жиляэв], тоді існує третя операція результат виконання якої співпаде з результатом послідовного виконання двох попередніх операцій.

Визначимо результуючу операцію перетворення інформації на фінальній стадії крипто перетворення. Для цього підставимо у вираз, яким описана операція перетворення в другому раунді, вираз, яким описана операція перетворення в першому раунді.

Якщо першому раунді виконувалась $F_{3,10}(x) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{3,10}(x) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{3,10}(F_{3,10}(x)) = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = F_{3,5}(x)$

Операція $F_{3,5}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча операція $F_{3,12}(F_{3,10}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}=F_{12,10}(x)$.

Операція $F_{12,10}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча операція $F_{10,3}(F_{3,10}(x))=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}=F_{5,3}(x)$.

Операція $F_{5,3}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{5,12}(F_{3,10}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}=F_{10,12}(x)$.

Операція $F_{10,12}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, а в другому раунді також операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{3,10}(F_{12,5}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}=F_{12,10}(x)$

Операція $F_{12,10}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, а в другому раунді також операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча операція $F_{12,5}(F_{12,5}(x))=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}=F_{3,5}(x)$

Операція $F_{3,5}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, а в другому раунді також операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча операція $F_{10,3}(F_{12,5}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}=F_{10,12}(x)$

Операція $F_{10,12}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, а в другому раунді також операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{5,12}(F_{12,5}(x))=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}=F_{5,3}(x)$

Операція $F_{5,3}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, а в другому раунді також операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{3,10}(F_{10,3}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}=F_{10,12}(x)$

Операція $F_{10,12}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, а в другому раунді також операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча операція $F_{12,5}(F_{10,3}(x))=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}=F_{5,3}(x)$

Операція $F_{5,3}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, а в другому раунді також операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча операція $F_{10,3}(F_{10,3}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}=F_{12,10}(x)$

Операція $F_{12,10}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, а в другому раунді також операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{5,12}(F_{10,3}(x))=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}=F_{3,5}(x)$

Операція $F_{3,5}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{3,10}(F_{5,12}(x))=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}=F_{5,3}(x)$

Операція $F_{5,3}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча операція $F_{12,5}(F_{5,12}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}=F_{10,12}(x)$

Операція $F_{10,12}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча операція $F_{10,3}(F_{5,12}(x))=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}=F_{3,5}(x)$

Операція $F_{3,5}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, а в другому раунді також операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча операція $F_{5,12}(F_{5,12}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}=F_{12,10}(x)$

Операція $F_{12,10}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

На основі проведених досліджень можна стверджувати, що при двохраундовому застосуванні операцій з ССК на фінальній стадії крипто перетворення, результати шифрування не будуть відповідати вимогам критерію ССК. Це означає що при повторному використанні перетворення з максимальною невизначеністю його результатів, результати шифрування погіршаться.

2.4. Дослідження багатораундового застосування двохрозрядних операцій криптографічного перетворення які відповідають вимогам критерію строгого стійкого кодування

Розглянемо трьохраундове застосування операцій криптографічного перетворення, які відповідають вимогам критерію ССК. Для цього узагальнимо результати дослідження двохраундового застосування операцій з ССК і зведемо їх в таблицю моделей (табл. 2.9) [8, 9].

Таблиця 2.9

Моделі двохраундового застосування операцій з ССК

Операція першого раунду шифрування	Операція другого раунду шифрування			
	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$
$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$

Як видно з табл. 2.9 результати двораундового шифрування будуть співпадати з результатами однораундового шифрування за допомогою чотирьох операцій:

$$F_{3,5}(x) = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{2.16}$$

$$F_{12,10}(x) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \tag{2.17}$$

$$F_{5,3}(x) = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \tag{2.18}$$

$$F_{10,12}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \tag{2.19}$$

Якщо в криптоалгориммі операції (2.12 – 2.15) застосовуються рівномірно, а також послідовності вибору даних операцій на кожному раунді шифрування не залежать одна від другої, то результуючі операції (2.16 – 2.19) будуть розподілені рівномірно з ймовірністю 1/4 [8].Ймовірності результатів двохраундового застосування операцій крипторeретворення з ССК на фінальній стадії шифрування наведені в табл. 2.10.

Таблиця 2.10

Ймовірності результатів двохраундового застосування операцій крипторeретворення з ССК на фінальній стадії шифрування

Перший раунд	операція	$F_{3,10}(x) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10,3}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x) = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
	ймовірність	1/4	1/4	1/4	1/4
Другий раунд	операція	$F_{3,10}(x) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10,3}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x) = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
	ймовірність	1/4	1/4	1/4	1/4
Результат перетворення	операція	$F_{3,5}(x) = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{5,3}(x) = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
	ймовірність	1/4	1/4	1/4	1/4

Для визначення відповідності результатів трьохраундового застосування операцій криптографічного перетворення з ССК, вимогам критерію ССК, достатньо дослідити результати перетворення моделей двохраундового застосування операцій з ССК на останньому раунді шифрування.

Якщо модель операції реалізації двохраундного шифрування буде $F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ а в третьому раунді буде операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{3,10}(F_{3,5}(x))=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}=F_{3,10}(x)$

Операція $F_{3,10}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ а в третьому раунді буде операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча модель операції буде $F_{12,5}(F_{3,5}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}=F_{12,5}(x)$

Операція $F_{12,5}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ а в третьому раунді буде операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{10,3}(F_{3,5}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}=F_{10,3}(x)$

Операція $F_{10,3}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ а в третьому раунді буде операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{5,12}(F_{3,5}(x))=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=F_{5,12}(x)$

Операція $F_{5,12}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{3,10}(F_{12,10}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}=F_{12,5}(x)$

Операція $F_{12,5}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча модель операції буде $F_{12,5}(F_{12,10}(x))=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}=F_{3,10}(x)$

Операція $F_{3,10}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{10,3}(F_{12,10}(x))=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=F_{5,12}(x)$

Операція $F_{2,12}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{5,12}(F_{12,10}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}=F_{10,3}(x)$

Операція $F_{10,3}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$ а в третьому раунді буде операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{3,10}(F_{5,3}(x))=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=F_{5,12}(x)$

Операція $F_{5,12}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$ а в третьому раунді буде операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча модель операції буде $F_{12,5}(F_{5,3}(x))=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}=F_{10,3}(x)$

Операція $F_{10,3}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$ а в третьому раунді буде операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{10,3}(F_{5,3}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}=F_{12,5}(x)$

Операція $F_{12,5}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$ а в третьому раунді буде операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{5,12}(F_{5,3}(x))=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}=F_{3,10}(x)$

Операція $F_{3,10}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{3,10}(F_{10,12}(x))=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=F_{10,3}(x)$

Операція $F_{10,3}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, тоді результуюча модель операції буде $F_{12,5}(F_{10,12}(x))=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=F_{5,12}(x)$

Операція $F_{5,12}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{10,3}(F_{10,12}(x))=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}=F_{3,10}(x)$

Операція $F_{3,10}(x)$, і як наслідок, результат шифрування буде відповідати вимогам критерію ССК.

Якщо модель операції реалізації двохраундного шифрування буде $F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ а в третьому раунді буде операція $F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$, тоді результуюча модель операції буде $F_{5,12}(F_{10,12}(x))=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}=F_{12,5}(x)$

Операція $F_{12,5}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Зведемо результати досліджень трьохраундового застосування операцій з ССК до таблиці моделей застосування операцій з ССК (табл.. 2.11) [8].

Таблиця 2.11

Моделі трьохраундового застосування операцій з ССК

Операція третього раунду шифрування	Модель двохраундового застосування операцій			
	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$
$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$
$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$

На основі проведених досліджень можна стверджувати, що при трьохраундовому застосуванні операцій з ССК на фінальній стадії крипто перетворення, результати шифрування будуть відповідати вимогам критерію ССК. Підтвердженням цього служать моделі трьохраундного застосування операцій, які співпадають з операціями (2.12 – 2.15). Це означає, що знову буде досягнута максимальна невизначеність результатів при використанні двох розрядних операцій які відповідають критерію ССК [8].

Розрахуємо ймовірності результатів трьохраундового застосування операцій крипторeретворення з ССК на фінальній стадії шифрування.

Для розрахунку ймовірностей зробимо наступні припущення, яким відповідають високоякісні крипто алгоритми [8]:

- в третьому раунді криптоперетворення операції (2.12 – 2.15) застосовуються рівномірно;
- послідовність вибору даних операцій в даному раунді, не залежить від послідовностей вибору операцій для перших двох раундів, і як наслідок не залежить від послідовностей моделей двохраундового шифрування

Результати розрахунку ймовірностей наведені в табл. 2.12.

Таблиця 2.12

Ймовірності результатів трьохраундового застосування операцій крипторeретворення з ССК на фінальній стадії шифрування

Двох-Раундрва модель	операція	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
	ймовірність	1/4	1/4	1/4	1/4
Третій раунд	операція	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
	ймовірність	1/4	1/4	1/4	1/4
Результат перетво-рення	операція	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$
	ймовірність	1/4	1/4	1/4	1/4

Як видно з табл. 2.12 результуючі операції (2.12 – 2.15) будуть розподілені рівномірно з ймовірністю $1/4$.

Використавши табл. 2.9 і табл. 2.10 можна довести що при непарній кількості раундів застосуванні двох розрядних операцій з ССК на фінальній стадії крипто перетворення, результати шифрування будуть відповідати вимогам критерію ССК, а при парній кількості раундів не будуть відповідати вимогам даного критерію.

ВИСНОВКИ ДО РОЗДІЛУ 2

Досліджено двохрозрядні елементарні функції придатні для криптографічного перетворення інформації на відповідність критерію строгого лавинного ефекту. Встановлено, що елементарні функції придатні для крипто перетворення не відповідають критерію строгого лавинного ефекту, а сам критерій строгого лавинного ефекту не доцільно використовувати при оцінці якості елементарних функцій і операцій з яких будуються крипто алгоритми.

Для оцінки якості елементарних функцій і операцій з яких будуються крипто алгоритми запропоновано критерій строгого стійкого кодування, який полягає в досягненні максимальної невизначеності результатів шифрування. Визначено чотири дворозрядні операції, які відповідають критерію строгого стійкого кодування.

Встановлено що при випадковому використанні дворозрядниї операцій крипто перетворення, які відповідають критерію строгого стійкого кодування, в якості криптоалгоритму, повторне його застосування не приводить до покращення результатів перетворення, а при непарній кількості раундів невизначеність результатів погіршується.

Результати розділу опубліковані [2, 3, 8, 9].

РОЗДІЛ 3
МЕТОД СИНТЕЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ СТРОГОГО СТІЙКОГО КОДУВАННЯ

3.1 Синтез дворозрядних операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування

Проблема забезпечення необхідного рівня захисту інформації є досить складною, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів та застосування специфічних методів і засобів, а створення цілісної системи організаційних заходів та застосування специфічних методів і засобів захисту інформації. [4, 24].

Особливо важливим є захист інформації в комп'ютерних системах та мережах. Щоб гарантувати високий ступінь захисту інформації, необхідно постійно вирішувати складні науково-технічні завдання розробки та вдосконалення засобів її захисту [99].

Широке застосування комп'ютерних технологій та постійне збільшення обсягу інформаційних потоків викликає постійне зростання вимог до криптографії [70, 100]. Тому актуальною є розробка криптографічних алгоритмів захисту інформації, які забезпечать максимальну криптостійкість.

Побудова алгоритмів комп'ютерної криптографії базується на використанні операцій криптографічного перетворення інформації. Проте помимо синтезу операцій крипто перетворення актуальною є також задача визначення операцій використання яких буде мати більший ефект, порівняно з іншими.

Побудова операцій, які забезпечують строге стійке кодування, приведе до підвищення якості криптографічних алгоритмів та швидкості їх реалізації, іншими словами забезпечить досягнення максимальної невизначеності результатів шифрування при мінімальних затратах.

В попередніх дослідженнях проведено аналіз повної групи дворозрядних криптографічних операцій [95, 101, 102]. Узагальнено дослідження груп математичних операцій матричного криптографічного перетворення та розширеного матричного криптографічного перетворення.

Встановлено, що критерію ССК відповідає лише незначна частина операцій. Серед дворозряних операцій їх лише чотири [3, 4]. Виходячи з цього, стає актуальною задача побудови операцій криптографічного перетворення, які відповідають критерію ССК, з більшою розрядністю.

В попередніх дослідженнях визначено підмножину дворозрядних операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування. При використанні даних операцій операції на фінальній стадії шифрування досягається максимальна невизначеність зашифрованої інформації. Проте пошук даних операцій (2.12 – 2.15) проводився на основі повного перебору 24 операцій, які складають множину дворозрядних операцій криптографічного перетворення [96].

Для операцій криптографічного перетворення інформації з розрядністю більше двох провести аналіз на строге стійке кодування на основі перебору неможливо, тому що кількість трирозрядних операцій – вісім факторіал, що дорівнює 40320 операцій [97], а кількість чотири розрядних операцій шістнадцять факторіал. Провести аналіз чотирьохрозрядних операцій практично не реалізуєма задача.

Виходячи з цього можна стверджувати що задача синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування в повному обсязі не вирішена.

Розглянемо інші підходи крім перебору для синтезу операцій за критерієм ССК. Існуючі 24 дворозрядні операції криптографічного перетворення модна розглядати як математичний синтез 24 таблиць підстановки, тобто повної група таблиць підстановки, які будуються на основі перестановок 4 слів двохбітової вхідної інформації [97].

Відповідно до визначення ССК кожний біт вихідної послідовності змінюється відносно вхідної інформації з імовірністю одна друга. Для дворозрядних операцій криптографічного перетворення, і відповідних їм таблиць підстановки це означає що з двох біт вхідних даних, один з бітів, і тільки один, буде змінено на протилежне значення. Дане твердження може бути модифіковане наступним: над всіма дророзрядними блоками вхідних даних і вихідних результатів повинна бути відстань по Хемінгу рівна 1.

Одним з найбільш простих засобів побудови кодів з заданою відстанню по Хемінгу базується на використанні таблиць відстаней по Хемінгу [98]. Так як ми будемо будувати дворозрядні кодові перетворення, то використаємо таблицю відстаней по Хемінгу наведену табл. 3.1 [98].

Таблиця 3.1

Таблиця х відстаней за Хемінгом

	0	**1**	**2**	**3**
0	0	1	1	2
1	1	0	2	1
2	1	2	0	1
3	2	1	1	0

В заголовках рядків і стовпців табл. 3.1 наведені десяткові значення вхідних даних і результатів виконання в четвірковій системі числення, а на перетині – мінімальна кодова відстань між даними результатами.

Для побудови методу синтезу операцій за критерієм ССК на основі табл. 3.1 побудуємо таблицю вибору варіантів побудови операцій криптоперетворення (таблиць підстановок) з відстанню по Хемінгу рівною 1. Для цього необхідно з табл. 3.1 видалити інформаційну надмірність відносно кодів підстановки з відстанню по Хемінгу рівною 1.

На першому етапі видалення надмірності забілимо в таблиці всі відстані по Хемінгу, які не дорівнюють 1. Результати виконання першого етапу наведені в табл. 3.2.

На другому етапі видалення надмірності замінимо в клітинках в яких вказана відстань по Хемінгу 1, на значення рядків, в яких знаходяться дані

клітинки, і отримаємо проміжну таблицю вибору варіантів підстановки (табл. 3.3) [4].

Таблиця 3.2

Відкоригована таблиця відстаней за Хемінгом

	0	**1**	**2**	**3**
0		1	1	
1	1			1
2	1			1
3		1	1	

Таблиця 3.3

Проміжна таблиця вибору варіантів підстановки

	0	**1**	**2**	**3**
0		0	0	
1	1			1
2	2			2
3		3	3	

На третьому етапі, на основі проміжної таблиці вибору варіантів підстановки побудуємо таблицю вибору варіантів підстановки, для цього видалимо з таблиці заголовок рядків та пусті клітинки, як такі, що втратили інформативність.

В результаті виконання третього етапу буде побудована таблиця вибору варіантів підстановки в червінковій системі числення (табл.3.4)

Таблиця 3.4

Таблиця вибору варіантів підстановки

0	**1**	**2**	**3**
1	0	0	1
2	3	3	2

В табл. 3.4 в заголовках стовпчиків (перший рядок) наведені значення кодів цифр які кодуються при побудові таблиці підстановки. В інших рядках наведені значення кодів цифр, якими кодуються коди відповідних цифр першого рядка при побудові таблиці підстановки.

Так як, таблиця підстановки може будуватися на основа перестановки, необхідно враховувати однозначний взаємозв’язок вхідних і вихідних кодів в

таблиці підстановок. Іншими словами значення цифр, якими кодуються коди в таблиці перестановок не повинні повторятися.

Побудова таблиць підстановок на основі табл. 3.4 проводиться наступним чином:

- Цифру 0 можна закодувати цифрами 1, або 2. Нехай 0 закодуємо як 1;
- Цифру 1 можна закодувати цифрами 0, або 3. Нехай 1 закодуємо як 0;
- Цифру 2 можна закодувати цифрами 0, або 3. Так як цифра 0, на попередніх кроках кодування використана, то цифра 2 кодується цифрою 3;
- Цифру 3 можна закодувати цифрами 1, або 2. Так як цифра 1, на попередніх кроках кодування використана, то цифра 3 кодується цифрою 2.

В результаті виконання запропонованого алгоритму кодування, буде отримана таблиця підстановки в четвірковій системі числення:

$$0 \to 1; \quad 0 \to 1; \quad 0 \to 1; \quad 0 \to 1.$$

Результати побудови таблиць двох розрядних підстановок в четвірковій системі числення, які задовольняють критерію ССК, наведені в табл.3.5.

Таблиця 3.5

Результати побудови таблиць двох розрядних підстановок, які задовольняють критерію ССК

	0	**1**	**2**	**3**
1	1	0	3	2
2	1	3	0	2
3	2	0	3	1
4	2	3	0	1

Для синтезу дворозрядних операцій криптографічного перетворення які відповідають критерію ССК на основі побудови таблиць двох розрядних підстановок, необхідно дані таблиць перевести з червіркової системи числення в двійкову та провести мінімізацію елементарних функцій на основі яких будуть скомпоновані операції криптографічного перетворення.

Результати синтезу двохрозрядних операцій криптографічного перетворення, які відповідають вимогам критерію ССК наведені в табл.3.6.

Як видно з табл..3.6. в результаті мінімізації таблиць підстановок, було отримано 4 двохрозрядні операції криптографічного перетворення, які співпали з операціями (2.12 – 2.15) [9].

Таблиця3 6

Результати синтезу двох розрядних операцій криптографічного перетворення, які відповідають вимогам критерію ССК

Варіанти вхідних даних			Варіанти вихідних даних для побудови операцій											
			1			2			3			4		
0	0	0	**1**	0	1	**1**	0	1	**2**	1	0	**2**	1	0
1	0	1	**0**	0	0	**3**	1	1	**0**	0	0	**3**	1	1
2	1	0	**3**	1	1	**0**	0	0	**3**	1	1	**0**	0	0
3	1	1	**2**	1	0	**2**	1	0	**1**	0	1	**1**	0	1
Результати побудови операцій			$F_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$			$F_{5,12} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$			$F_{10,3} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$			$F_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$		

Використавши таблицю кодових відстаней за Хемінгом для побудови операцій криптографічних перетворень, які відповідають критерію ССК, відповідно до приведеного прикладу, була отримана можливість коректної побудови операцій без необхідності проведення дослідження на основі повного перебору з повної множини операцій.

3.2 Синтез чотирьохрозрядних операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування

Синтез чотирьохрозрядних операцій криптографічного перетворення які відповідають критерію ССК, проведемо по аналогії з синтезом двохрозрядних операцій з врахуванням особливосте, пов’язаних із збільшенням розрядності та потужності кодів.

Так як ми будемо будувати чотирьохрозрядні кодові перетворення, то використаємо таблицю відстаней по Хемінгу для чотирьохрозрядних кодів наведену табл. 3.7 [98, 102, 103].

Таблиця 3.7

Таблиця мінімальних кодових відстаней за Хемінгом для чотирьохрозрядних кодів

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	1	1	2	1	2	2	3	1	2	2	3	2	3	3	4
1	1	0	2	1	2	1	3	2	2	1	3	2	3	2	4	3
2	1	2	0	1	2	3	1	2	2	3	1	2	3	4	2	3
3	2	1	1	0	3	2	2	1	3	2	2	1	4	3	3	2
4	1	2	2	3	0	1	1	2	2	3	3	4	1	2	2	3
5	2	1	3	2	1	0	2	1	3	2	4	3	2	1	3	2
6	2	3	1	2	1	2	0	1	3	4	2	3	2	3	1	2
7	3	2	2	1	2	1	1	0	4	3	3	2	3	2	2	1
8	1	2	2	3	2	3	3	4	0	1	1	2	1	2	2	3
9	2	1	3	2	3	2	4	3	1	0	2	1	2	1	3	2
10	2	3	1	2	3	4	2	3	1	2	0	1	2	3	1	2
11	3	2	2	1	4	3	3	2	2	1	1	0	3	2	2	1
12	2	3	3	4	1	2	2	3	1	2	2	3	0	1	1	2
13	3	2	4	3	2	1	3	2	2	1	3	2	1	0	2	1
14	3	4	2	3	2	3	1	2	2	3	1	2	1	2	0	1
15	4	3	3	2	3	2	2	1	3	2	2	1	2	1	1	0

В заголовках рядків і стовпців табл. 3.1 наведені десяткові значення вхідних даних і результатів виконання в четвірковій системі числення, а на перетині –кодова відстань між даними результатами. Так як синтезуються чотирьох розрядні операції які відповідають критерію ССК, то при їх виконанні з 4 біт інформації повинно бути змінено 2.

Виходячи з цього, в табл. 3.7 нас цікавлять лише клітинки з відстанню по Хемінгу 2. Побудуємо відкориговану таблицю відстаней за Хемінгом для синтезу чотирьох розрядних операцій (табл.3.8).

На основі табл. 3.8 побудуємо проміжну таблицю вибору варіантів підстановки (табл.3.9)

На основі табл.3.8 побудуємо таблицю вибору варіантів підстановки (табл.3.10) [9].

Для синтезу чотирьох розрядної операції яка відповідає критерію ССК, на основі табл. 3.11 по аналогії з синтезом двох розрядних операцій побудуємо таблицю підстановок.

Таблиця 3.8

Відкоригована таблиця відстаней за Хемінгом

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0				2		2	2			2	2		2			
1			2		2			2	2			2		2		
2		2			2			2	2			2			2	
3	2					2	2			2	2					2
4		2	2					2	2					2	2	
5	2			2			2			2			2			2
6	2			2		2					2		2			2
7		2	2		2							2		2	2	
8		2	2		2							2		2	2	
9	2			2		2					2		2			2
10	2			2			2			2			2			2
11		2	2					2	2					2	2	
12	2					2	2			2	2					2
13		2			2			2	2			2			2	
14			2		2			2	2			2		2		
15				2		2	2			2	2		2			

Таблиця 3.9

Проміжна таблиця вибору варіантів підстановки

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0				0		0	0			0	0		0			
1			1		1			1	1			1		1		
2		2			2			2	2			2			2	
3	3					3	3			3	3					3
4		4	4					4	4					4	4	
5	5			5			5			5			5			5
6	6			6		6					6		6			6
7		7	7		7							7		7	7	
8		8	8		8							8		8	8	
9	9			9		9					9		9			9
10	10			10			10			10			10			10
11		11	11					11	11					11	11	
12	12					12	12			12	12					12
13		13			13			13	13			13			13	
14			14		14			14	14			14		14		
15				15		15	15			15	15		15			

Таблиця 3.10

Таблиця вибору варіантів підстановки

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Побудова таблиць підстановок на основі табл. 3.4 проводиться наступним чином:

- Цифру 0 можна закодувати кодами цифр 3, 5, 6, 9, 10 або 12. Нехай 0 закодуємо кодом цифри 3. Тоді $m_0^* = \{3\} \in M_0 = \{3, 5, 6, 9, 10, 12\}$ де M_0 – множина кодів (представлень), які може приймати цифра 0, m_0^* – вибране значення коду для представлення цифри 0 із множини M_0. Тоді множину вибраних значень для цифр 0 позначимо M_0^*;
- Цифру 1 можна закодувати кодами цифр 2, 4, 7, 8, 11 або 13. Нехай 1 закодуємо кодом цифри 2. Тоді $m_1^* = \{2\} \in M_1 = \{2, 4, 7, 8, 11, 13\}$ за умови $m_1^* \notin M^* = \{3\}$ де M_1 – множина кодів, які може приймати цифра 1, m_1^* – вибране значення коду для цифри 1. Тоді множину вибраних значень для цифр 0 і 1 позначимо: $M^* = M_0^* \cup m_1^* = \{3, 2\}$.
- Цифру 2 можна закодувати цифрами 1, 4, 7, 8, 11 або 14. Нехай 2 закодуємо цифрою 1. Тоді $m_2^* = \{1\} \in M_2 = \{1, 4, 7, 8, 11, 14\}$ де M_2- множина значень, які може приймати цифра 2, m_2^* –вибране значення коду тдля цифри 2. Тоді множину вибраних значень для цифр 0 – 2 позначимо: $M^* = M_1^* \cup m_2^* = m_0^* \cup m_1^* \cup m_2^* = \{3, 2, 1\}$.
- Виберемо код для представлення цифри 3 за наступних умов $m_3^* = (m_3 \in M_3 = \{0, 5, 6, 9, 10, 15\}) \wedge (m_3 \notin M_2^* = \{3, 2, 1\})$. Даній умові відповідає

будь який код із множини M_3. Нехай $m_3^* = \{1\}$, тоді $M^* = M_2^* \cup m_3^* = m_0^* \cup m_1^* \cup m_2^* = \cup m_3^* = \{3, 2, 1, 0\}$;

- Код цифри 4 нехай буде представлений кодом цифри 7, $m_4^* = \{7\}$, так як $m_4^* = \{7\} = (m_4 \in M_4 = \{1, 2, 7, 8, 13, 14\}) \wedge (m_4 \notin M_3^* = \{3, 2, 1, 0\})$, тоді $M^* = M_3^* \cup m_4^* = \{3, 2, 1, 0, 7\}$;
- Вибрану для побудови операції крипто перетворення таблицю підстановки яка буде включати коди всіх цифр (0 – 15) можна отримати на основі виразу:

$$M^* = M_4^* \cup \bigcap_{i=5}^{15} m_i^* = (m_i \in M_i) \wedge (m_i \notin M_{i-1}^*). \quad (3.1)$$

На основі виразу (3.1) можна побудувати модель побудови таблиці підстановок для синтезу чорирьохрозрядної операції криптоперетворення яка відповідає критерією ССК:

$$M^* = \bigcap_{i=0}^{15} m_i^* = (m_i \in M_i) \wedge (m_i \notin M_{i-1}^*) \quad (3.2)$$

Один із варіантів побудованої таблиці підстановок, з виділеною послідовністю вибраних кодів цифр наведено в табл. 3.11 [9].

Таблиця 3.11

Вибір варіанта побудови операції яка відповідає критерію ССК (варіант 1.1)

	Цифри, які шифруються															
Варіанти заміни	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
	5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
	6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
	9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
	10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
	12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Впорядкована множина M^* може розглядатися як таблиці підстановки так і таблиця істинності для синтезу операції на основі мінімізації. Результати мінімізації варіанта операції криптоперетворення за критерієм ССК наведено в табл. 3.12.

Таблиця 3.12

Результати синтез операції яка відповідає критерію ССК (варіант 1.1),

Синтез операції (варіант 1.1)										
Вхідні дані					**Вихідні дані**					**Модель операції**
цифра	**код**				**цифра**	**код**				
0	0	0	0	0	**3**	0	0	1	1	$F_{1.1}(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$
1	0	0	0	1	**2**	0	0	1	0	
2	0	0	1	0	**1**	0	0	0	1	
3	0	0	1	1	**0**	0	0	0	0	
4	0	1	0	0	**7**	0	1	1	1	
5	0	1	0	1	**6**	0	1	1	0	
6	0	1	1	0	**5**	0	1	0	1	
7	0	1	1	1	**4**	0	1	0	0	
8	1	0	0	0	**11**	1	0	1	1	
9	1	0	0	1	**10**	1	0	1	0	
10	1	0	1	0	**9**	1	0	0	1	
11	1	0	1	1	**8**	1	0	0	0	
12	1	1	0	0	**15**	1	1	1	1	
13	1	1	0	1	**14**	1	1	1	0	
14	1	1	1	0	**13**	1	1	0	1	
15	1	1	1	1	**12**	1	1	0	0	

На основі виразу (3.2) побудуємо ще одну таблицю підстановок і на її основі синтезуємо чорирьохрозрядну операцію криптоперетворення яка відповідає критерією ССК. Варіант побудованої таблиці підстановок, з виділеною послідовністю вибраних кодів цифр наведено в табл. 3.13[9].

Таблиця 3.13

Вибір варіанта побудови операції яка відповідає критерію ССК (варіант 1.2)

	Цифри, які шифруються															
Варіанти заміни	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
	5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
	6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
	9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
	10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
	12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Результати мінімізації варіанта таблиці підстановок (табл.3.13) для операції криптоперетворення за критерієм ССК наведено в табл. 3.14 [9].

Таблиця 3.14

Результати синтез операції яка відповідає критерію ССК (варіант1. 2)

Синтез операції (варіант 2)										
Вхідні дані					**Вихідні дані**					**Модель операції**
цифра	**код**				**цифра**	**код**				
0	0	0	0	0	**12**	1	1	0	0	$F_{1.2}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_4 \end{bmatrix}$
1	0	0	0	1	**13**	1	1	0	1	
2	0	0	1	0	**14**	1	1	1	0	
3	0	0	1	1	**15**	1	1	1	1	
4	0	1	0	0	**7**	0	1	1	1	
5	0	1	0	1	**6**	0	1	1	0	
6	0	1	1	0	**5**	0	1	0	1	
7	0	1	1	1	**4**	0	1	0	0	
8	1	0	0	0	**11**	1	0	1	1	
9	1	0	0	1	**10**	1	0	1	0	
10	1	0	1	0	**9**	1	0	0	1	
11	1	0	1	1	**8**	1	0	0	0	
12	1	1	0	0	**0**	0	0	0	0	
13	1	1	0	1	**1**	0	0	0	1	
14	1	1	1	0	**2**	0	0	1	0	
15	1	1	1	1	**3**	0	0	1	1	

Наступним етапом дослідження є узагальнення отриманих результатів синтезу операцій.

3.3 Метод синтез операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування та оцінка результатів його реалізації

3.3.1 Метод синтез операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування

Отримані результати дослідження синтезу чорирьохрозрядних операцій крипто перетворення, які відповідають критерією ССК дозволяють сформулювати метод синтезу операцій криптоперетворення за критерієм ССК в загальному випадку. При побудові методу необхідно враховувати можливість подальшої автоматизації процесу побудови таблиць підстановок, а також можливість використання програмних засобів мінімізації дискретних автоматів для автоматизованого синтезу операцій крипто перетворення.

Сутність методу полягає в наступному [4]:

1. Визначається розрядність операції крипто перетворення, яка співпадає з кількістю елементарних функцій в операції і є парним числом: $n = 2 \cdot k; \quad k \in N$.
2. Будується таблиця мінімальних кодових відстаней за Хемінгом $2^n \times 2^n$;
3. Будується таблиця варіантів підстановки кодів перетворення шляхом послідовної реалізації:
   - відкоригованої таблиці відстаней за Хемінгом, в якій залишені лише відстані за Хемінгом рівні k;
   - проміжної таблиці вибору варіантів підстановки, в якій залишені відстані за Хемінгом рівні k замінені номерами рядків, в яких вони знаходяться
   - таблицю вибору варіантів підстановки, щляхом видалення незадіяних комірок;
4. Визначаються значення кодів від 0 до $2^n - 1$ так, щоб не було повторення кодів шляхом послідовної реалізації $M^* = \bigcap_{i=0}^{2^n-1} m_i^* = (m_i \in M_i) \wedge (m_i \notin M_{i-1}^*)$;
5. Перевіряється коректність отриманого варіанта таблиці підстановки, за рахунок виявлення можливих помилок та допущених при побудові таблиці. При програмній реалізації даний пункт дозволяє контролюати як результати побудови таблиці так і наявність збоїв комп'ютерної техніки;
6. На основі отриманої таблиці підстановок будується таблиці істинності n-розрядної операції криптоперетворення яка відповідає критерією ССК:
7. На основі таблиці істинності мінімізується n-розрядна математична модель операції криптоперетворення яка відповідає критерією ССК.

Перевіримо коректність запропонованого методу шляхом синтезу декількох операцій крипто перетворення з заданими характеристиками, за умови $n = 4; \quad k = 2$.

Варіант побудованої таблиці підстановок, з виділеною послідовністю вибраних кодів цифр наведено в табл. 3.15.

Таблиця 3.15

Вибір варіанта побудови операції яка відповідає критерію ССК (варіант 1.3)

	Цифри, які шифруються															
Варіанти заміни	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
	5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
	6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
	9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
	10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
	12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Таблиця істинності і результати мінімізації варіанта таблиці підстановок (табл.3.15) для операції криптоперетворення за критерієм ССК наведено в табл. 3.16.

Таблиця 3.16

Результати синтез операції яка відповідає критерію ССК (варіант 1.3)

Синтез операції (варіант 1.3)										Модель операції
Вхідні дані					**Вихідні дані**					
цифра	**код**				**цифра**	**код**				
0	0	0	0	0	**5**	0	1	0	1	$F_{1.3}(x) = \begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_4 \\ \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2 \cdot x_4 \vee x_1 \cdot x_3 \cdot \bar{x}_4 \\ \bar{x}_1 \cdot \bar{x}_2 \cdot x_4 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_4 \vee \\ \vee x_1 \cdot \bar{x}_2 \cdot x_3 \cdot \bar{x}_4 \\ \bar{x}_1 \cdot \bar{x}_3 \cdot x_4 \vee \bar{x}_2 \cdot \bar{x}_3 \cdot \bar{x}_4 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \vee x_1 \cdot x_3 \cdot \bar{x}_4 \end{bmatrix}$
1	0	0	0	1	**7**	0	1	1	1	
2	0	0	1	0	**4**	0	1	0	0	
3	0	0	1	1	**6**	0	1	1	0	
4	0	1	0	0	**2**	0	0	1	0	
5	0	1	0	1	**9**	1	0	0	1	
6	0	1	1	0	**3**	0	0	1	1	
7	0	1	1	1	**11**	1	0	1	1	
8	1	0	0	0	**1**	0	0	0	1	
9	1	0	0	1	**0**	0	0	0	0	
10	1	0	1	0	**15**	1	1	1	1	
11	1	0	1	1	**8**	1	0	0	0	
12	1	1	0	0	**10**	1	0	1	0	
13	1	1	0	1	**14**	1	1	1	0	
14	1	1	1	0	**13**	1	1	0	1	
15	1	1	1	1	**12**	1	1	0	0	

Наступний варіант побудованої таблиці підстановок, з виділеною послідовністю вибраних кодів цифр наведено в табл. 3.17.

Таблиця 3.17

Вибір варіанта побудови операції яка відповідає критерію ССК (варіант 1.4)

	Цифри, які шифруються															
Варіанти заміни	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
	5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
	6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
	9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
	10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
	12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12

Результати мінімізації варіанта таблиці підстановок (табл.3.17) для операції криптоперетворення за критерієм ССК наведено в табл. 3.18.

Отримані результати тестування процесу синтезу операцій крипто перетворення за критерієм ССК дозволяють константувати про коректну розробку методу синтезу операцій, який на відміну від існуючих забезпечує побудову таблиць істинності операцій, які відповідають критеріє ССК.

Таблиця 3.18

Результати синтез операції яка відповідає критерію ССК (варіант1. 4)

Синтез операції (варіант 1.4)										
Вхідні дані					**Вихідні дані**					**Модель операції**
цифра	**код**				**цифра**	**код**				
0	0	0	0	0	**9**	1	0	0	1	$F_{1.4}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$
1	0	0	0	1	**11**	1	0	1	1	
2	0	0	1	0	**8**	1	0	0	0	
3	0	0	1	1	**10**	1	0	1	0	
4	0	1	0	0	**1**	0	0	0	1	
5	0	1	0	1	**3**	0	0	1	1	
6	0	1	1	0	**0**	0	0	0	0	
7	0	1	1	1	**2**	0	0	1	0	
8	1	0	0	0	**13**	1	1	0	1	
9	1	0	0	1	**15**	1	1	1	1	
10	1	0	1	0	**12**	1	1	0	0	
11	1	0	1	1	**14**	1	1	1	0	
12	1	1	0	0	**5**	0	1	0	1	
13	1	1	0	1	**7**	0	1	1	1	
14	1	1	1	0	**4**	0	1	0	0	
15	1	1	1	1	**6**	0	1	1	0	

Розроблений метод дозволяє автоматизувати процес побудови таблиць підстановок для синтезу операції криптоперетворення за критерієм ССК.

3.3.2 Результати реалізації методу синтезу операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування

Спираючись на отриманий досвід синтезу операцій криптографічного перетворення які відповідають критерію ССК, можна стверджувати, що синтезувати навіть не операції, а таблиці підстановки для побудови операцій в ручному режимі неможливо.

Для отримання первинної інформації про особливості побудови операцій, які досліджуються необхідно провести обчислювальний експеримент. При проведенні експерименту обмежмося моделюванням лише чотирьох розрядних операцій, які відповідають критерію ССК. Фрагмент зведених результатів моделювання таблиць підстановок для синтезу чотирьох розрядних операцій, які відповідають критерію ССК наведено в табл. 3.19.

Таблиця 3.19

Фрагмент зведених результатів моделювання таблиць підстановок для синтезу чотирьох розрядних операцій, які відповідають критерію ССК

№	Коди цифр для таблиць підстановок															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
2.1	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
2.2	3	2	1	0	7	6	5	4	11	10	9	13	15	14	8	12
2.3	3	2	1	0	7	6	5	4	11	10	9	14	15	8	13	12
2.4	3	2	1	0	7	6	5	4	11	10	12	8	15	14	13	9
2.5	3	2	1	0	7	6	5	4	11	10	12	13	15	14	8	9
2.6	3	2	1	0	7	6	5	4	11	10	12	14	15	8	13	9
2.7	3	2	1	0	7	6	5	4	11	10	15	8	9	14	13	12
2.8	3	2	1	0	7	6	5	4	11	10	15	13	9	14	8	12
2.9	3	2	1	0	7	6	5	4	11	10	15	14	9	8	13	12
2.10	3	2	1	0	7	6	5	4	11	12	9	8	15	14	13	10
2.11	3	2	1	0	7	6	5	4	11	12	9	13	15	14	8	10
2.12	3	2	1	0	7	6	5	4	11	12	9	14	15	8	13	10
2.13	3	2	1	0	7	6	5	4	11	12	15	8	9	14	13	10
2.14	3	2	1	0	7	6	5	4	11	12	15	8	10	14	13	9
2.15	3	2	1	0	7	6	5	4	11	12	15	13	9	14	8	10
2.16	3	2	1	0	7	6	5	4	11	12	15	13	10	14	8	9
2.17	3	2	1	0	7	6	5	4	11	12	15	14	9	8	13	10
2.18	3	2	1	0	7	6	5	4	11	12	15	14	10	8	13	9
2.19	3	2	1	0	7	6	5	4	11	15	9	8	10	14	13	12
2.20	3	2	1	0	7	6	5	4	11	15	9	13	10	14	8	12
2.21	3	2	1	0	7	6	5	4	11	15	9	14	10	8	13	12

2.22	3	2	1	0	7	6	5	4	11	15	12	8	9	14	13	10
2.23	3	2	1	0	7	6	5	4	11	15	12	8	10	14	13	9
2.24	3	2	1	0	7	6	5	4	11	15	12	13	9	14	8	10
2.25	3	2	1	0	7	6	5	4	11	15	12	13	10	14	8	9
2.26	3	2	1	0	7	6	5	4	11	15	12	14	9	8	13	10
2.27	3	2	1	0	7	6	5	4	11	15	12	14	10	8	13	9
2.28	3	2	1	0	7	6	5	4	13	10	9	8	15	14	11	12
2.29	3	2	1	0	7	6	5	4	13	10	9	14	15	8	11	12
2.30	3	2	1	0	7	6	5	4	13	10	9	14	15	11	8	12
2.31	3	2	1	0	7	6	5	4	13	10	12	8	15	4	11	9
2.32	3	2	1	0	7	6	5	4	13	10	12	14	14	15	11	9
2.33	3	2	1	0	7	6	5	4	13	10	12	14	15	11	8	9
2.34	3	2	1	0	7	6	5	4	13	10	15	8	9	14	11	12
2.35	3	2	1	0	7	6	5	4	13	10	15	14	9	8	11	12
2.36	3	2	1	0	7	6	5	4	13	10	15	14	9	11	8	12
2.37	3	2	1	0	7	6	5	4	13	12	9	8	15	14	11	10
2.38	3	2	1	0	7	6	5	4	13	12	9	14	15	8	11	10
2.39	3	2	1	0	7	6	5	4	13	12	9	14	15	11	8	10
2.40	3	2	1	0	7	6	5	4	13	12	15	8	9	14	11	10
2.41	3	2	1	0	7	6	5	4	13	12	15	8	10	14	11	9
2.42	3	2	1	0	7	6	5	4	13	12	15	14	9	8	11	10
2.43	3	2	1	0	7	6	5	4	13	12	15	14	9	11	8	10
2.44	3	2	1	0	7	6	5	4	13	12	15	14	10	8	11	9
2.45	3	2	1	0	7	6	5	4	13	12	15	14	10	11	8	9
2.46	3	2	1	0	7	6	5	4	13	15	9	8	10	14	11	12
2.47	3	2	1	0	7	6	5	4	13	15	9	14	10	8	11	12
2.48	3	2	1	0	7	6	5	4	13	15	9	14	10	11	8	12
2.49	3	2	1	0	7	6	5	4	13	15	12	8	9	14	11	10
2.50	3	2	1	0	7	6	5	4	13	15	12	8	10	14	11	9
2.51	3	2	1	0	7	6	5	4	13	15	12	14	9	8	11	10
2.52	3	2	1	0	7	6	5	4	13	15	12	14	9	11	8	10
2.53	3	2	1	0	7	6	5	4	13	15	12	14	10	8	11	9
2.54	3	2	1	0	7	6	5	4	13	15	12	14	10	11	8	9
2.55	3	2	1	0	7	6	5	4	14	10	9	8	15	11	13	12
2.56	3	2	1	0	7	6	5	4	14	10	9	13	15	8	11	12
2.57	3	2	1	0	7	6	5	4	14	10	9	13	15	11	8	12
2.58	3	2	1	0	7	6	5	4	14	10	12	8	15	11	13	9
2.59	3	2	1	0	7	6	5	4	14	10	12	13	15	8	11	9
2.60	3	2	1	0	7	6	5	4	14	10	12	13	15	11	8	9
2.61	3	2	1	0	7	6	5	4	14	10	15	8	9	11	13	12
2.62	3	2	1	0	7	6	5	4	14	10	15	13	9	8	11	12
2.63	3	2	1	0	7	6	5	4	14	10	15	13	9	11	8	12
2.64	3	2	1	0	7	6	5	4	14	12	9	8	15	11	13	10
2.65	3	2	1	0	7	6	5	4	14	12	9	13	15	8	11	10
2.66	3	2	1	0	7	6	5	4	14	12	9	13	15	11	8	10
2.67	3	2	1	0	7	6	5	4	14	12	15	8	9	11	13	10
2.68	3	2	1	0	7	6	5	4	14	12	15	8	10	11	13	9
2.69	3	2	1	0	7	6	5	4	14	12	15	13	9	8	11	10
2.70	3	2	1	0	7	6	5	4	14	12	15	13	9	11	8	10
2.71	3	2	1	0	7	6	5	4	14	12	15	13	10	8	11	9

2.72	3	2	1	0	7	6	5	4	14	12	15	13	10	11	8	9
2.73	3	2	1	0	7	6	5	4	14	15	9	8	10	11	13	12
2.74	3	2	1	0	7	6	5	4	14	15	9	13	10	8	11	12
2.75	3	2	1	0	7	6	5	4	14	15	9	13	10	11	8	12
2.76	3	2	1	0	7	6	5	4	14	15	12	8	9	11	13	10
2.77	3	2	1	0	7	6	5	4	14	15	12	8	10	11	13	9
2.78	3	2	1	0	7	6	5	4	14	15	12	13	9	8	11	10
2.79	3	2	1	0	7	6	5	4	14	15	12	13	9	11	8	10
2.80	3	2	1	0	7	6	5	4	14	15	12	13	10	8	11	9
2.81	3	2	1	0	7	6	5	4	14	15	12	13	10	11	8	9

Якщо $M_{2.1}^{*} = \{3,2,1,0,6,5,4,11,10,9,8,15,14,13,12\}$ то за результатами мінімізації таблицю підстановок буде описано:

$$F_{2.1}(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$$

Перевіримо відповідність отриманого аналітичного опису операції вимогам ССК.

Результати виконання операції $F_{2.1}(x)$ на множині вхідних даних сформують множину:

$$M(F_{2.1}(x)) = M_{2.1}^{*} = \{3,2,1,0,6,5,4,11,10,9,8,15,14,13,12\}.$$

Тоді множина кількості змін в словах вхідної інформації буде: $M(x \oplus M(F_{2.1}(x)) = \{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$

Визначимо значення ССК:

$$M(\lambda_{cck}(F_{2.1}) = \{2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4, 2/4\};$$

$$\lambda_{cck}(F_{2.1}(x)) = 32/64 = 1/2.$$

Якщо $M_{2.2}^{*} = \{3,2,1,0,6,5,4,11,10,9,13,15,14,8,12\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.2}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot x_3 \cdot x_4 \\ x_3 \oplus 1 \\ \bar{x}_4(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot \bar{x}_2 \cdot x_3 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.2}(x)) = 1/2.$$

Якщо $M^*_{2.3} = \{3,2,1,0,6,5,4,11,10,9,14,15,8,13,12\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.3}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot x_3 \cdot x_4 \\ \bar{x}_3(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot \bar{x}_2 \cdot x_4 \\ x_4 \oplus 1 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.3}(x)) = 1/2$$

Якщо $M^*_{2.4} = \{3,2,1,0,6,5,4,11,10,12,8,15,14,13,9\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.4}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot x_3 \cdot \bar{x}_4 \\ x_3 \oplus 1 \\ \bar{x}_4(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot x_2 \cdot x_3 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.4}(x)) = 1/2$$

Якщо $M^*_{2.5} = \{3,2,1,0,6,5,4,11,10,12,13,15,14,8,9\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.5}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot \bar{x}_2 \cdot x_3 \\ x_3 \oplus 1 \\ \bar{x}_4(\bar{x}_1 \vee \bar{x}_2) \vee x_1 \cdot x_3 \cdot x_4 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.5}(x)) = 1/2$$

Якщо $M^*_{2.6} = \{3,2,1,0,6,5,4,11,10,12,14,15,8,13,9\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.6}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot \bar{x}_2 \cdot x_3 \\ \bar{x}_3(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot \bar{x}_2 \cdot x_4 \\ \bar{x}_4(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot x_2 \cdot x_3 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.6}(x)) = 1/2$$

Якщо $M^*_{2.7} = \{3,2,1,0,6,5,4,11,10,15,8,9,14,13,12\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.7}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee x_4) \vee x_1 \cdot x_3 \cdot \bar{x}_4 \\ \bar{x}_3(\bar{x}_1 \vee x_4) \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_4 \\ x_4 \oplus 1 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.7}(x)) = 1/2$$

Якщо $M^*_{2.8} = \{3,2,1,0,6,5,4,11,10,15,13,9,14,8,12\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.8}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee x_4) \vee x_1 \cdot \bar{x}_2 \cdot x_3 \\ \bar{x}_3(x_1 \vee x_4) \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_4 \\ \bar{x}_4(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot \bar{x}_2 \cdot x_3 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.8}(x)) = 1/2$$

Якщо $M^*_{2.9} = \{3,2,1,0,6,5,4,11,10,15,14,9,8,13,12\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.9}(x) = \begin{bmatrix} x_1 \\ \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \\ x_4 \oplus 1 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.9}(x)) = 1/2$$

Якщо $M^*_{2.10} = \{3,2,1,0,6,5,4,11,12,9,8,15,14,13,10\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.10}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot \bar{x}_3 \cdot x_4 \\ \bar{x}_3(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot x_2 \cdot x_4 \\ x_4 \oplus 1 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.10}(x)) = 1/2$$

Якщо $M^*_{2.11} = \{3,2,1,0,6,5,4,11,12,9,13,15,14,8,10\}$, то операція крипто перетворення буде описана виразом:

$$F_{2.11}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_3) \vee x_1 \cdot \bar{x}_2 \cdot x_4 \\ \bar{x}_3(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot x_2 \cdot x_4 \\ \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_3 \cdot \bar{x}_4 \vee x_1 \cdot \bar{x}_2 \cdot x_3 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.11}(x)) = 1/2$$

Якщо $M^*_{2.12} = \{3,2,1,0,6,5,4,11,12,9,14,15,8,13,10\}$, то операція крипто перетворення буде описана виразом:

$$F_{1.12}(x) = \begin{bmatrix} x_1 \\ x_2(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot \bar{x}_2 \cdot x_4 \\ \bar{x}_3(\bar{x}_1 \vee \bar{x}_4) \vee x_1 \cdot x_3 \cdot x_4 \\ x_4 \oplus 1 \end{bmatrix}$$

Операція відповідає вимогам значення ССК, так як:

$$\lambda_{cck}(F_{2.12}(x)) = 1/2$$

Наведені приклади підтверджують підтверджують коректність реалізації розробленого методу синтез операцій криптографічного перетворення які відповідають критерію ССК, а отримані за допомогою даного методу моделі створюють теоретичне і практичне підґрунтя для подальших досліджень.

3.4 Дослідження багатораундового застосування операцій криптографічного перетворення які відповідають вимогам критерію строгого стійкого кодування

3.4.1 Дослідження двохраундового застосування чотирьохозрядних операцій криптографічного кодування за критерієм ССК

Подальші дослідження були направлені на встановлення залежності зміни ССК багатораундному застосуванні синтезованих операцій. При проведенні дослідження скористаємося підгодом, наведеним в підрозділі 2.4 при дослідженні двохоперендних операцій. Крім того обмежимося чотирима чотирьохрозрядними операціями ($F_{1.1}(x)$ - $F_{1.4}(x)$) та трьома раундами криптографічного перетворення.

Так як повна множина операцій досліджувати не може, тому проведемо дослідження на прикладах таблиць підстановки з подальшою формалізацію моделей та визначенням кількісних і якісних оцінок.

Якщо першому раунді виконувалась $F_{1.1}(x)$, а в другому раунді також операція $F_{1.1}(x)$, тоді результуюча операція буде задана як

$$F_{1,1}(F_{1,1}(x)) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = F_{1.1/1.1}(x) \tag{3.3}$$

Операція $F_{1.1/1.1}(x)$, і як наслідок, результат шифрування не буде відповідати вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{1.1}(x)$, а в другому раунді операція $F_{1.2}(x)$, тоді результуюча операція буде задана моделлю:

$$F_{1,2}(F_{1,1}(x)) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \oplus 1 \\ x_1 \oplus x_2 \oplus x_4 \oplus 1 \end{bmatrix} = F_{1.2/1.1}(x)\,. \tag{3.4}$$

Для перевірки коректності моделі необхідно підставити в $F_{1.2}(x)$, значення виходів моделі $F_{1.1}(x)$.

Для дослідження відповідності операції $F_{1.2/1.1}(x)$ вимогам критерію ССК, побудуємо таблицю істинності. Дана таблиця наведена в табл. 3.20.

Як видно з таблиці істинності операції що досліджується (табл. 3.20)

$$M(F_{1.2/1.1}(x)) = M^*_{1.2/1.1} = \{15,14,13,12,4,5,6,7,8,9,10,11,3,2,1,0\}\,.$$

Тоді множина кількості змін в словах вхідної інформації буде: $M(x \oplus M(F_{1.2/1.1}(x)) = \{4,4,4,4,0,0,0,0,0,0,0,0,4,4,4,4\}$

Визначимо значення ССК:

$$M(\lambda_{cck}(F_{1.2/1.1}) = \{4/4, 4/4, 4/4, 4/4, 0/4, 0/4, 0/4, 0/4, 0/4, 0/4, 0/4, 0/4, 4/4, 4/4, 4/4, 4/4\};$$

$$\lambda_{cck}(F_{1.2/1.1}(x)) = 32/64 = 1/2$$

Таблиця 3.20

Результати побудови таблиці істинності операції $F_{1.2/1.1}(x)$

Модель операції	Таблиця істинності операції									
	Вхідні дані					Вихідні дані				
	цифра	код				цифра	код			
$F_{1.2/1.1}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \oplus 1 \\ x_1 \oplus x_2 \oplus x_4 \oplus 1 \end{bmatrix}$	**0**	0	0	0	0	**15**	1	1	1	1
	1	0	0	0	1	**14**	1	1	1	0
	2	0	0	1	0	**13**	1	1	0	1
	3	0	0	1	1	**12**	1	1	0	0
	4	0	1	0	0	**4**	0	1	0	0
	5	0	1	0	1	**5**	0	1	0	1
	6	0	1	1	0	**6**	0	1	1	0
	7	0	1	1	1	**7**	0	1	1	1
	8	1	0	0	0	**8**	1	0	0	0
	9	1	0	0	1	**9**	1	0	0	1
	10	1	0	1	0	**10**	1	0	1	0
	11	1	0	1	1	**11**	1	0	1	1
	12	1	1	0	0	**3**	0	0	1	1
	13	1	1	0	1	**2**	0	0	1	0
	14	1	1	1	0	**1**	0	0	0	1
	15	1	1	1	1	**0**	0	0	0	0

Операції $F_{1.2/1.1}(x)$ не задовольняє критерію ССК, тому що при перетворенні блоків вхідної інформації 0 – 3 та 12 – 15 буде змінено всі чотири біти, а при перетворенні інших блоків жодний біт не буде змінено.

Знайдемо результуючу операцію, якщо в першому раунді виконувалась операція $F_{1.1}(x)$, а в другому раунді операція $F_{1.3}(x)$.

Знайдемо результуючу операцію за допомогою побудови результуючої таблиці підстановок з її подальшою мінімізацією.

Побудована результуюча таблиця підстановок наведена в табл..3.21.

Як видно з таблиці істинності операції що досліджується (табл. 3.21)

$$M(F_{1.3/1.1}(x)) = M^*_{1.3/1.1} = \{6,4,7,5,11,3,9,2,8,15,0,1,12,13,14,10\}.$$

Тоді множина кількості змін в словах вхідної інформації буде: $M(x \oplus M(F_{1.3/1.1}(x)) = \{2,2,2,2,4,2,4,2,0,2,2,2,0,0,0,2\}$

Визначимо значення ССК:

$$M(\lambda_{cck}(F_{1.3/1.1}) = \{2/4, 2/4, 2/4, 2/4, 4/4, 2/4, 4/4, 2/4, 0/4, 2/4, 2/4, 2/4, 0/4, 0/4, 0/4, 4/4\};$$

$$\lambda_{cck}(F_{1.3/1.1}(x)) = 28/64 = 7/16$$

Таблиця 3.21

Результуюча таблиця підстановок ($F_{1.3/1.1}(x)$)

Вхідні дані					Перший раунд					Другий раунд					Вихідні дані				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**3**	0	0	1	1	**5**	0	1	0	1	**6**	0	1	1	0
1	0	0	0	1	**2**	0	0	1	0	**7**	0	1	1	1	**4**	0	1	0	0
2	0	0	1	0	**1**	0	0	0	1	**4**	0	1	0	0	**7**	0	1	1	1
3	0	0	1	1	**0**	0	0	0	0	**6**	0	1	1	0	**5**	0	1	0	1
4	0	1	0	0	**7**	0	1	1	1	**2**	0	0	1	0	**11**	1	0	1	1
5	0	1	0	1	**6**	0	1	1	0	**9**	1	0	0	1	**3**	0	0	1	1
6	0	1	1	0	**5**	0	1	0	1	**3**	0	0	1	1	**9**	1	0	0	1
7	0	1	1	1	**4**	0	1	0	0	**11**	1	0	1	1	**2**	0	0	1	0
8	1	0	0	0	**11**	1	0	1	1	**1**	0	0	0	1	**8**	1	0	0	0
9	1	0	0	1	**10**	1	0	1	0	**0**	0	0	0	0	**15**	1	1	1	1
10	1	0	1	0	**9**	1	0	0	1	**15**	1	1	1	1	**0**	0	0	0	0
11	1	0	1	1	**8**	1	0	0	0	**8**	1	0	0	0	**1**	0	0	0	1
12	1	1	0	0	**15**	1	1	1	1	**10**	1	0	1	0	**12**	1	1	0	0
13	1	1	0	1	**14**	1	1	1	0	**14**	1	1	1	0	**13**	1	1	0	1
14	1	1	1	0	**13**	1	1	0	1	**13**	1	1	0	1	**14**	1	1	1	0
15	1	1	1	1	**12**	1	1	0	0	**12**	1	1	0	0	**10**	1	0	1	0

Результуюча операція, не відповідає вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{1.1}(x)$, а в другому раунді також операція $F_{1.4}(x)$, тоді результуюча операція.буде

$$F_{1.4}(F_{1,1}(x)) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} = F_{1.4/1.1}(x) \cdot \qquad (3.5)$$

Для дослідження відповідності операції $F_{1.4/1.1}(x)$ вимогам критерію ССК, побудуємо таблицю істинності. Дана таблиця наведена в табл. 3.22.

Як видно з таблиці істинності операції що досліджується (табл. 3.22)

$$M(F_{1.4/1.1}(x)) = M^*_{1.4/1.1} = \{10,8,11,9,2,0,3,1,14,12,15,13,6,4,7,5\}.$$

Таблиця 3.22

Результати побудови таблиці істинності операції $F_{1.4/1.1}(x)$

Модель операції	Таблиця істинності операції									
	Вхідні дані					Вихідні дані				
	цифра	код				цифра	код			
$F_{1.4/1.1}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	**0**	0	0	0	0	**10**	1	0	1	0
	1	0	0	0	1	**8**	1	0	0	0
	2	0	0	1	0	**11**	1	0	1	1
	3	0	0	1	1	**9**	1	0	0	1
	4	0	1	0	0	**2**	0	0	1	0
	5	0	1	0	1	**0**	0	0	0	0
	6	0	1	1	0	**3**	0	0	1	1
	7	0	1	1	1	**1**	0	0	0	1
	8	1	0	0	0	**14**	1	1	1	0
	9	1	0	0	1	**12**	1	1	0	0
	10	1	0	1	0	**15**	1	1	1	1
	11	1	0	1	1	**13**	1	1	0	1
	12	1	1	0	0	**6**	0	1	1	0
	13	1	1	0	1	**4**	0	1	0	0
	14	1	1	1	0	**7**	0	1	1	1
	15	1	1	1	1	**5**	0	1	0	1

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.4/1.1}(x)) = \{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$$

$$\lambda_{cck}(F_{1.4/1.1}(x)) = 1/2$$

Операції $F_{1.4/1.1}(x)$ задовольняє критерію ССК

Якщо першому раунді виконувалась $F_{1.2}(x)$, а в другому раунді операція $F_{1.1}(x)$, тоді результуюча операція буде задана як

$$F_{1,1}(F_{1,2}(x)) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \oplus 1 \\ x_1 \oplus x_2 \oplus x_4 \oplus 1 \end{bmatrix} = F_{1.1/1.2}(x) = F_{1.2/1.1}(x) \qquad (3.6)$$

Операція $F_{1.1/1.2}(x)$, як і операція $F_{1.2/1.1}(x)$ (3.4) не відповідають вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{1.2}(x)$, а в другому раунді операція $F_{1.2}(x)$, тоді результуюча операція буде задана моделлю:

$$F_{1,2}(F_{1,2}(x)) = \begin{bmatrix} x_2 \\ x_1 \\ x_3 \\ x_4 \end{bmatrix} = F_{1.2/1.2}(x) = F_{1.1/1.1}(x) \cdot$$

Операція $F_{1.2/1.2}(x)$, як і операція $F_{1.1/1.1}(x)$ (3.3) не відповідають вимогам критерію ССК.

Знайдемо результуючу операцію, якщо в першому раунді виконувалась операція $F_{1.2}(x)$, а в другому раунді операція $F_{1.3}(x)$.

Побудована результуюча таблиця підстановок наведена в табл..3.23.

Таблиця 3.23

Результуюча таблиця підстановок ($F_{1.3/1.2}(x)$)

Вхідні дані					**Перший раунд**					**Другий раунд**					**Вихідні дані**				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**12**	1	1	0	0	**5**	0	1	0	1	**10**	1	0	1	0
1	0	0	0	1	**13**	1	1	0	1	**7**	0	1	1	1	**14**	1	1	1	0
2	0	0	1	0	**14**	1	1	1	0	**4**	0	1	0	0	**13**	1	1	0	1
3	0	0	1	1	**15**	1	1	1	1	**6**	0	1	1	0	**12**	1	1	0	0
4	0	1	0	0	**7**	0	1	1	1	**2**	0	0	1	0	**11**	1	0	1	1
5	0	1	0	1	**6**	0	1	1	0	**9**	1	0	0	1	**3**	0	0	1	1
6	0	1	1	0	**5**	0	1	0	1	**3**	0	0	1	1	**9**	1	0	0	1
7	0	1	1	1	**4**	0	1	0	0	**11**	1	0	1	1	**2**	0	0	1	0
8	1	0	0	0	**11**	1	0	1	1	**1**	0	0	0	1	**8**	1	0	0	0
9	1	0	0	1	**10**	1	0	1	0	**0**	0	0	0	0	**15**	1	1	1	1
10	1	0	1	0	**9**	1	0	0	1	**15**	1	1	1	1	**0**	0	0	0	0
11	1	0	1	1	**8**	1	0	0	0	**8**	1	0	0	0	**1**	0	0	0	1
12	1	1	0	0	**0**	0	0	0	0	**10**	1	0	1	0	**5**	0	1	0	1
13	1	1	0	1	**1**	0	0	0	1	**14**	1	1	1	0	**7**	0	1	1	1
14	1	1	1	0	**2**	0	0	1	0	**13**	1	1	0	1	**4**	0	1	0	0
15	1	1	1	1	**3**	0	0	1	1	**12**	1	1	0	0	**6**	0	1	1	0

Як видно з таблиці істинності операції що досліджується (табл. 3.23)

$$M(F_{1.3/1.2}(x)) = M^*_{1.3/1.2} = \{10,14,13,12,11,3,9,2,8,15,0,1,5,7,4,6\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.3/1.2}(x)) = \{2,4,4,4,4,2,4,2,0,2,2,2,2,2,2,2\}$$

Визначимо значення ССК:

$$\lambda_{cck}(F_{1.3/1.2}(x)) = {}^{40}\!/_{64} = {}^{5}\!/_{8}$$

Результуюча операція, не відповідає вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{1.2}(x)$, а в другому раунді операція $F_{1.4}(x)$, тоді результуюча операція буде

$$F_{1.4}(F_{1,2}(x)) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus 1 \end{bmatrix} = F_{1.4/1.2}(x) \cdot$$

Для дослідження відповідності операції $F_{1.4/1.2}(x)$ вимогам критерію ССК, побудуємо таблицю істинності (табл.3.24.)

Таблиця 3.24

Результати побудови таблиці істинності операції $F_{1.4/1.2}(x)$

Модель операції	**Таблиця істинності операції**									
	Вхідні дані					**Вихідні дані**				
	цифра	**код**				**цифра**	**код**			
$F_{1.4/1.2}(x) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus 1 \end{bmatrix}$	**0**	0	0	0	0	**5**	0	1	0	1
	1	0	0	0	1	**7**	0	1	1	1
	2	0	0	1	0	**4**	0	1	0	0
	3	0	0	1	1	**6**	0	1	1	0
	4	0	1	0	0	**2**	0	0	1	0
	5	0	1	0	1	**0**	0	0	0	0
	6	0	1	1	0	**3**	0	0	1	1
	7	0	1	1	1	**1**	0	0	0	1
	8	1	0	0	0	**14**	1	1	1	0
	9	1	0	0	1	**12**	1	1	0	0
	10	1	0	1	0	**15**	1	1	1	1
	11	1	0	1	1	**13**	1	1	0	1
	12	1	1	0	0	**9**	1	0	0	1
	13	1	1	0	1	**11**	1	0	1	1
	14	1	1	1	0	**8**	1	0	0	0
	15	1	1	1	1	**10**	1	0	1	0

Як видно з таблиці істинності операції що досліджується (табл. 3.24)

$$M(F_{1.4/1.2}(x)) = M^*_{1.4/1.2} = \{5,7,4,6,2,0,3,1,14,12,15,13,9,11,8,10\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.4/1.2}(x)) = \{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$$

$$\lambda_{cck}(F_{1.4/1.2}(x)) = 1/2$$

Операції $F_{1.4/1.2}(x)$ задовольняє критерію ССК.

Знайдемо результуючу операцію, якщо в першому раунді виконувалась операція $F_{1.3}(x)$, а в другому раунді операція $F_{1.1}(x)$.

Побудована результуюча таблиця підстановок наведена в табл..3.25.

Таблиця 3.25

Результуюча таблиця підстановок ($F_{1.1/1.3}(x)$)

Вхідні дані					Перший раунд					Другий раунд					Вихідні дані				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**5**	0	1	0	1	**3**	0	0	1	1	**6**	0	1	1	0
1	0	0	0	1	**7**	0	1	1	1	**2**	0	0	1	0	**4**	0	1	0	0
2	0	0	1	0	**4**	0	1	0	0	**1**	0	0	0	1	**7**	0	1	1	1
3	0	0	1	1	**6**	0	1	1	0	**0**	0	0	0	0	**5**	0	1	0	1
4	0	1	0	0	**2**	0	0	1	0	**7**	0	1	1	1	**1**	0	0	0	1
5	0	1	0	1	**9**	1	0	0	1	**6**	0	1	1	0	**10**	1	0	1	0
6	0	1	1	0	**3**	0	0	1	1	**5**	0	1	0	1	**0**	0	0	0	0
7	0	1	1	1	**11**	1	0	1	1	**4**	0	1	0	0	**8**	1	0	0	0
8	1	0	0	0	**1**	0	0	0	1	**11**	1	0	1	1	**2**	0	0	1	0
9	1	0	0	1	**0**	0	0	0	0	**10**	1	0	1	0	**3**	0	0	1	1
10	1	0	1	0	**15**	1	1	1	1	**9**	1	0	0	1	**12**	1	1	0	0
11	1	0	1	1	**8**	1	0	0	0	**8**	1	0	0	0	**11**	1	0	1	1
12	1	1	0	0	**10**	1	0	1	0	**15**	1	1	1	1	**9**	1	0	0	1
13	1	1	0	1	**14**	1	1	1	0	**14**	1	1	1	0	**13**	1	1	0	1
14	1	1	1	0	**13**	1	1	0	1	**13**	1	1	0	1	**14**	1	1	1	0
15	1	1	1	1	**12**	1	1	0	0	**12**	1	1	0	0	**15**	1	1	1	1

Як видно з таблиці істинності операції що досліджується (табл. 3.25)

$$M(F_{1.1/1.3}(x)) = M^*_{1.1/1.3} = \{6,4,7,5,1,10,0,8,2,3,12,11,9,13,14,15\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.1/1.3}(x)) = \{2,2,2,2,2,4,2,4,2,2,2,0,2,0,0,0\}$$

Визначимо значення ССК:

$$\lambda_{cck}(F_{1.1/1.3}(x)) = 28/64 = 7/16$$

Результуюча операція, не відповідає вимогам критерію ССК.

Знайдемо результуючу операцію, якщо в першому раунді виконувалась операція $F_{1.3}(x)$, а в другому раунді операція $F_{1.2}(x)$.

Результуюча таблиця підстановок наведена в табл..3.26.

Як видно з таблиці істинності операції що досліджується (табл. 3.26)

$$M(F_{1.2/1.3}(x)) = M^*_{1.2/1.3} = \{6,4,7,5,14,10,15,8,13,12,3,11,9,2,1,0\}.$$

Таблиця 3.26

Результуюча таблиця підстановок ($F_{1.2/1.3}(x)$)

Вхідні дані					Перший раунд					Другий раунд					Вихідні дані				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**5**	0	1	0	1	**12**	1	1	0	0	**6**	0	1	1	0
1	0	0	0	1	**7**	0	1	1	1	**13**	1	1	0	1	**4**	0	1	0	0
2	0	0	1	0	**4**	0	1	0	0	**14**	1	1	1	0	**7**	0	1	1	1
3	0	0	1	1	**6**	0	1	1	0	**15**	1	1	1	1	**5**	0	1	0	1
4	0	1	0	0	**2**	0	0	1	0	**7**	0	1	1	1	**14**	1	1	1	0
5	0	1	0	1	**9**	1	0	0	1	**6**	0	1	1	0	**10**	1	0	1	0
6	0	1	1	0	**3**	0	0	1	1	**5**	0	1	0	1	**15**	1	1	1	1
7	0	1	1	1	**11**	1	0	1	1	**4**	0	1	0	0	**8**	1	0	0	0
8	1	0	0	0	**1**	0	0	0	1	**11**	1	0	1	1	**13**	1	1	0	1
9	1	0	0	1	**0**	0	0	0	0	**10**	1	0	1	0	**12**	1	1	0	0
10	1	0	1	0	**15**	1	1	1	1	**9**	1	0	0	1	**3**	0	0	1	1
11	1	0	1	1	**8**	1	0	0	0	**8**	1	0	0	0	**11**	1	0	1	1
12	1	1	0	0	**10**	1	0	1	0	**0**	0	0	0	0	**9**	1	0	0	1
13	1	1	0	1	**14**	1	1	1	0	**1**	0	0	0	1	**2**	0	0	1	0
14	1	1	1	0	**13**	1	1	0	1	**2**	0	0	1	0	**1**	0	0	0	1
15	1	1	1	1	**12**	1	1	0	0	**3**	0	0	1	1	**0**	0	0	0	0

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.2/1.3}(x)) = \{2,2,2,2,2,4,2,4,2,2,2,0,2,4,4,4\}$$

Визначимо значення ССК:

$$\lambda_{cck}(F_{1.2/1.3}(x)) = 32/64 = 1/2$$

Результуюча операція, не відповідає вимогам критерію ССК так як не забезпечує гарантовано перетворення всіх слів таблиці підстановки з максимальною невизначеністю.

Знайдемо результуючу операцію, якщо в першому раунді виконувалась операція $F_{1.3}(x)$, а в другому раунді операція $F_{1.3}(x)$.

Результуюча таблиця підстановок наведена в табл..3.27.

Як видно з таблиці істинності операції (табл. 3.27)

$$M(F_{1.3/1.3}(x)) = M^*_{1.3/1.3} = \{9,11,2,3,4,0,6,8,7,5,12,1,15,13,14,10\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.3/1.3}(x)) = \{2,2,0,0,0,2,0,4,4,2,2,2,2,0,0,2\}$$

Таблиця 3.27

Результуюча таблиця підстановок ($F_{1.3/1.3}(x)$)

Вхідні дані					Перший раунд					Другий раунд					Вихідні дані				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**5**	0	1	0	1	**5**	0	1	0	1	**9**	1	0	0	1
1	0	0	0	1	**7**	0	1	1	1	**7**	0	1	1	1	**11**	1	0	1	1
2	0	0	1	0	**4**	0	1	0	0	**4**	0	1	0	0	**2**	0	0	1	0
3	0	0	1	1	**6**	0	1	1	0	**6**	0	1	1	0	**3**	0	0	1	1
4	0	1	0	0	**2**	0	0	1	0	**2**	0	0	1	0	**4**	0	1	0	0
5	0	1	0	1	**9**	1	0	0	1	**9**	1	0	0	1	**0**	0	0	0	0
6	0	1	1	0	**3**	0	0	1	1	**3**	0	0	1	1	**6**	0	1	1	0
7	0	1	1	1	**11**	1	0	1	1	**11**	1	0	1	1	**8**	1	0	0	0
8	1	0	0	0	**1**	0	0	0	1	**1**	0	0	0	1	**7**	0	1	1	1
9	1	0	0	1	**0**	0	0	0	0	**0**	0	0	0	0	**5**	0	1	0	1
10	1	0	1	0	**15**	1	1	1	1	**15**	1	1	1	1	**12**	1	1	0	0
11	1	0	1	1	**8**	1	0	0	0	**8**	1	0	0	0	**1**	0	0	0	1
12	1	1	0	0	**10**	1	0	1	0	**10**	1	0	1	0	**15**	1	1	1	1
13	1	1	0	1	**14**	1	1	1	0	**14**	1	1	1	0	**13**	1	1	0	1
14	1	1	1	0	**13**	1	1	0	1	**13**	1	1	0	1	**14**	1	1	1	0
15	1	1	1	1	**12**	1	1	0	0	**12**	1	1	0	0	**10**	1	0	1	0

Визначимо значення ССК:

$$\lambda_{cck}(F_{1.3/1.3}(x)) = {}^{34}\!/_{64} = {}^{17}\!/_{32}$$

Результуюча операція, не відповідає вимогам критерію ССК.

Знайдемо таблицю підстановки результуючої операції, якщо в першому раунді виконувалась $F_{1.3}(x)$, а в другому раунді операція $F_{1.4}(x)$.

Таблиця істинності результуючої операції наведена в табл.3.28.

Як видно з табл. 3.28

$$M(F_{1.4/1.3}(x)) = M^{*}_{1.4/1.3} = \{3,2,1,0,8,15,10,14,11,9,6,13,12,4,7,5\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.4/1.3}(x)) = \{2,2,2,2,2,2,2,2,2,0,2,2,0,2,2,2\}$$

$$\lambda_{cck}(F_{1.4/1.3}(x)) = {}^{28}\!/_{64} = {}^{7}\!/_{16}$$

Операції $F_{1.4/1.3}(x)$ не задовольняє критерію ССК.

Таблиця 3.28

Результуюча таблиця підстановок ($F_{1.4/1.3}(x)$)

Вхідні дані					Перший раунд					Другий раунд					Вихідні дані				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**5**	0	1	0	1	**9**	1	0	0	1	**3**	0	0	1	1
1	0	0	0	1	**7**	0	1	1	1	**11**	1	0	1	1	**2**	0	0	1	0
2	0	0	1	0	**4**	0	1	0	0	**8**	1	0	0	0	**1**	0	0	0	1
3	0	0	1	1	**6**	0	1	1	0	**10**	1	0	1	0	**0**	0	0	0	0
4	0	1	0	0	**2**	0	0	1	0	**1**	0	0	0	1	**8**	1	0	0	0
5	0	1	0	1	**9**	1	0	0	1	**3**	0	0	1	1	**15**	1	1	1	1
6	0	1	1	0	**3**	0	0	1	1	**0**	0	0	0	0	**10**	1	0	1	0
7	0	1	1	1	**11**	1	0	1	1	**2**	0	0	1	0	**14**	1	1	1	0
8	1	0	0	0	**1**	0	0	0	1	**13**	1	1	0	1	**11**	1	0	1	1
9	1	0	0	1	**0**	0	0	0	0	**15**	1	1	1	1	**9**	1	0	0	1
10	1	0	1	0	**15**	1	1	1	1	**12**	1	1	0	0	**6**	0	1	1	0
11	1	0	1	1	**8**	1	0	0	0	**14**	1	1	1	0	**13**	1	1	0	1
12	1	1	0	0	**10**	1	0	1	0	**5**	0	1	0	1	**12**	1	1	0	0
13	1	1	0	1	**14**	1	1	1	0	**7**	0	1	1	1	**4**	0	1	0	0
14	1	1	1	0	**13**	1	1	0	1	**4**	0	1	0	0	**7**	0	1	1	1
15	1	1	1	1	**12**	1	1	0	0	**6**	0	1	1	0	**5**	0	1	0	1

Якщо першому раунді виконувалась $F_{1.4}(x)$, а в другому раунді операція $F_{1.1}(x)$, тоді результуюча операція буде задана як

$$F_{1,1}(F_{1,4}(x)) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} = F_{1.1/1.4}(x) = F_{1.4/1.1}(x)$$

Операція $F_{1.1/1.4}(x)$, як і операція $F_{1.4/1.1}(x)$ (3.5) відповідають вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{1.4}(x)$, а в другому раунді операція $F_{1.2}(x)$, тоді результуюча операція буде задана моделлю:

$$F_{1,2}(F_{1,4}(x)) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_4 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix} = F_{1.2/1.4}(x) \cdot$$

Для дослідження відповідності операції $F_{1.2/1.4}(x)$ вимогам критерію ССК, побудуємо таблицю істинності (табл.3.28.)

Таблиця 3.28

Результати побудови таблиці істинності операції $F_{1.2/1.4}(x)$

Модель операції	Таблиця істинності операції									
	Вхідні дані					Вихідні дані				
	цифра	код				цифра	код			
$F_{1.2/1.4}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_4 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$	**0**	0	0	0	0	**10**	1	0	1	0
	1	0	0	0	1	**8**	1	0	0	0
	2	0	0	1	0	**11**	1	0	1	1
	3	0	0	1	1	**9**	1	0	0	1
	4	0	1	0	0	**13**	1	1	0	1
	5	0	1	0	1	**15**	1	1	1	1
	6	0	1	1	0	**12**	1	1	0	0
	7	0	1	1	1	**14**	1	1	1	0
	8	1	0	0	0	**1**	0	0	0	1
	9	1	0	0	1	**3**	0	0	1	1
	10	1	0	1	0	**0**	0	0	0	0
	11	1	0	1	1	**2**	0	0	1	0
	12	1	1	0	0	**6**	0	1	1	0
	13	1	1	0	1	**4**	0	1	0	0
	14	1	1	1	0	**7**	0	1	1	1
	15	1	1	1	1	**5**	0	1	0	1

Як видно з таблиці істинності операції що досліджується (табл. 3.28)

$$M(F_{1.2/1.4}(x)) = M^*_{1.2/1.4} = \{10,8,11,9,13,15,12,14,1,3,0,2,6,4,7,5\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.2/1.4}(x)) = \{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$$

$$\lambda_{cck}(F_{1.2/1.4}(x)) = 1/2$$

Операції $F_{1.2/1.4}(x)$ задовольняє критерію ССК

Знайдемо результуючу операцію, якщо в першому раунді виконувалась операція $F_{1.4}(x)$, а в другому раунді операція $F_{1.3}(x)$.

Побудована результуюча таблиця підстановок наведена в табл..3.29.

Як видно з таблиці істинності операції що досліджується (табл. 3.29)

$$M(F_{1.3/1.4}(x)) = M^*_{1.3/1.4} = \{0,8,1,15,7,6,5,4,14,12,10,13,9,11,2,3\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.3/1.4}(x)) = \{0,2,2,2,2,2,2,2,2,2,0,2,2,2,2,2\}$$

Таблиця 3.29

Результуюча таблиця підстановок ($F_{1.3/1.4}(x)$)

Вхідні дані					Перший раунд					Другий раунд					Вихідні дані				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**9**	1	0	0	1	**5**	0	1	0	1	**0**	0	0	0	0
1	0	0	0	1	**11**	1	0	1	1	**7**	0	1	1	1	**8**	1	0	0	0
2	0	0	1	0	**8**	1	0	0	0	**4**	0	1	0	0	**1**	0	0	0	1
3	0	0	1	1	**10**	1	0	1	0	**6**	0	1	1	0	**15**	1	1	1	1
4	0	1	0	0	**1**	0	0	0	1	**2**	0	0	1	0	**7**	0	1	1	1
5	0	1	0	1	**3**	0	0	1	1	**9**	1	0	0	1	**6**	0	1	1	0
6	0	1	1	0	**0**	0	0	0	0	**3**	0	0	1	1	**5**	0	1	0	1
7	0	1	1	1	**2**	0	0	1	0	**11**	1	0	1	1	**4**	0	1	0	0
8	1	0	0	0	**13**	1	1	0	1	**1**	0	0	0	1	**14**	1	1	1	0
9	1	0	0	1	**15**	1	1	1	1	**0**	0	0	0	0	**12**	1	1	0	0
10	1	0	1	0	**12**	1	1	0	0	**15**	1	1	1	1	**10**	1	0	1	0
11	1	0	1	1	**14**	1	1	1	0	**8**	1	0	0	0	**13**	1	1	0	1
12	1	1	0	0	**5**	0	1	0	1	**10**	1	0	1	0	**9**	1	0	0	1
13	1	1	0	1	**7**	0	1	1	1	**14**	1	1	1	0	**11**	1	0	1	1
14	1	1	1	0	**4**	0	1	0	0	**13**	1	1	0	1	**2**	0	0	1	0
15	1	1	1	1	**6**	0	1	1	0	**12**	1	1	0	0	**3**	0	0	1	1

Визначимо значення ССК:

$$\lambda_{cck}(F_{1.3/1.4}(x)) = 28/64 = 7/16$$

Результуюча операція, не відповідає вимогам критерію ССК.

Якщо першому раунді виконувалась $F_{1.4}(x)$, а в другому раунді також операція $F_{1.4}(x)$, тоді результуюча операція буде

$$F_{1.4}(F_{1,4}(x)) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix} = F_{1.4/1.4}(x) \cdot$$

Для дослідження відповідності операції $F_{1.4/1.4}(x)$ вимогам критерію ССК, побудуємо таблицю істинності (табл.3.30).

Як видно з таблиці істинності операції що досліджується (табл. 3.30)

$$M(F_{1.4/1.4}(x)) = M^*_{1.4/1.4} = \{15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x \oplus M(F_{1.4/1.4}(x)) = \{4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4\}$$

$$\lambda_{cck}(F_{1.4/1.4}(x)) = 1$$

Таблиця 3.30

Результати побудови таблиці істинності операції $F_{1.4/1.4}(x)$

Модель операції	Таблиця істинності операції									
	Вхідні дані					Вихідні дані				
	цифра	код				цифра	код			
$F_{1.4/1.4}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$	**0**	0	0	0	0	**15**	1	1	1	1
	1	0	0	0	1	***14***	1	1	1	0
	2	0	0	1	0	***13***	1	1	0	1
	3	0	0	1	1	***12***	1	1	0	0
	4	0	1	0	0	***11***	1	0	1	1
	5	0	1	0	1	***10***	1	0	1	0
	6	0	1	1	0	***9***	1	0	0	1
	7	0	1	1	1	***8***	1	0	0	0
	8	1	0	0	0	***7***	0	1	1	1
	9	1	0	0	1	***6***	0	1	1	0
	10	1	0	1	0	***5***	0	1	0	1
	11	1	0	1	1	***4***	0	1	0	0
	12	1	1	0	0	***3***	0	0	1	1
	13	1	1	0	1	***2***	0	0	1	0
	14	1	1	1	0	***1***	0	0	0	1
	15	1	1	1	1	***0***	0	0	0	0

Операції $F_{1.4/1.4}(x)$ задовольняє критерію ССК.

Узагальнимо результати дослідження двохраундового застосування операцій з ССК [8]. ($F_{1.1}(x)$ - $F_{1.4}(x)$) і зведемо їх до таблиці моделей (табл. 3.31), виділивши кольором результуючі перетворення які відповідають ССК.

Таблиця 3.31

Узагальнені результати дослідження двохраундового застосування операцій з ССК

Операція першого раунду шифрування	Операція другого раунду шифрування			
	$F_{1.1}(x)$	$F_{1.2}(x)$	$F_{1.3}(x)$	$F_{1.4}(x)$
$F_{1.1}(x)$	$F_{1.1/1.1}(x)=F_{1.2/1.2}(x)$	$F_{1.2/1.1}(x)=F_{1.1/1.2}(x)$	$F_{1.3/1.1}(x)$	$F_{1.4/1.1}(x)=F_{1.1/1.4}(x)$
$F_{1.2}(x)$	$F_{1.1/1.2}(x)=F_{1.2/1.1}(x)$	$F_{1.2/1.2}(x)=F_{1.1/1.1}(x)$	$F_{1.3/1.2}(x)$	$F_{1.4/1.2}(x)$
$F_{1.3}(x)$	$F_{1.1/1.3}(x)$	$F_{1.2/1.3}(x)$	$F_{1.3/1.3}(x)$	$F_{1.4/1.3}(x)$
$F_{1.4}(x)$	$F_{1.1/1.4}(x)=F_{1.4/1.1}(x)$	$F_{1.2/1.4}(x)$	$F_{1.3/1.4}(x)$	$F_{1.4/1.4}(x)$

Як видно з табл 3.31 результати двохраундового застосування чотирьох розрядних операцій по критерію ССК відрізняються від застосування двохрозрядних операцій тим, що в данному випадку після другого раунду можливе повторне досягнення ССК.

3.4.2 Дослідження трьохраундового застосування чотирьохозрядних операцій криптографічного кодування за критерієм ССК

Подальші дослідження були направлені на встановлення залежності зміни ССК при трьохраундному застосуванні операцій, які відповідають даному критерію [8, 14].

При використанні в перших двох раундах чотирирьох чотирьохрозрядних операцій ($F_{1.1}(x)$ - $F_{1.4}(x)$) серед 16 результуючих операцій перекодування, наведених в табл. 3.31, 13 операцій унікальні. Необхідно встановити значення ССК, при перетворенні, в нашому випадку, 13 результатів перекодування, додатковим перекодуванням операціями $F_{1.1}(x)$ – $F_{1.4}(x)$. На основі отриманих результатів необхідно буде зробити загальні висновки. Проте, для статистичної оцінки зміни ймовірності досягнення ССК, для нашого прикладу необхідно враховувати перекодування всих 16 результатів двохраундового кодування.

Якщо результуюче перетворення перших двох раундів є $F_{1.1/1.1}(x)$, а в третьому раунді виконувалась операція $F_{1.1}(x)$, тоді результуюча операція буде $F_{1.1}(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$, яка відповідає вимогам ССК.

Якщо результуюче перетворення перших двох раундів є $F_{1.1/1.1}(x)$, а в третьому раунді виконувалась операція $F_{1.2}(x)$, тоді результуюча операція буде $F_{1.2}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_4 \end{bmatrix}$, яка відповідає вимогам ССК.

Якщо результуюче перетворення перших двох раундів є $F_{1.1/1.1}(x)$, а в третьому раунді виконувалась операція $F_{1.3}(x)$, тоді результуюча операція буде

$$F_{1.3}(x)=\begin{bmatrix} x_1\cdot x_2 \vee x_1\cdot x_3 \vee x_2\cdot x_4 \\ \bar{x}_1\cdot\bar{x}_2 \vee x_1\cdot x_2\cdot x_4 \vee x_1\cdot x_3\cdot\bar{x}_4 \\ \bar{x}_1\cdot\bar{x}_2\cdot x_4 \vee \bar{x}_1\cdot x_2\cdot x_3 \vee x_1\cdot x_2\cdot\bar{x}_3 \vee \bar{x}_1\cdot x_2\cdot\bar{x}_4 \vee \\ \vee x_1\cdot\bar{x}_2\cdot x_3\cdot\bar{x}_4 \\ \bar{x}_1\cdot\bar{x}_3\cdot x_4 \vee \bar{x}_2\cdot\bar{x}_3\cdot\bar{x}_4 \vee \bar{x}_1\cdot x_2\cdot x_3 \vee x_1\cdot x_3\cdot\bar{x}_4 \end{bmatrix}$$, яка відповідає вимогам ССК.

Якщо результуюче перетворення перших двох раундів є $F_{1.3/1.1}(x)$, а в третьому раунді виконувалась операція $F_{1.1}(x)$, тоді знайдемо таблицю підстановок результуючої операції (табл.3.32).

Таблиця 3.32

Результуюча таблиця підстановок ($F_{1.1/1.3/1.1}(x)$)

Вхідні дані					**Другий раунд**					**Третій раунд**					**Вихідні дані**				
цифра	**код**				**цифра**	**код**				**цифра**	**код**				**цифра**	**код**			
0	0	0	0	0	**6**	0	1	1	0	**3**	0	0	1	1	**5**	0	1	0	1
1	0	0	0	1	**4**	0	1	0	0	**2**	0	0	1	0	**7**	0	1	1	1
2	0	0	1	0	**7**	0	1	1	1	**1**	0	0	0	1	**4**	0	1	0	0
3	0	0	1	1	**5**	0	1	0	1	**0**	0	0	0	0	**6**	0	1	1	0
4	0	1	0	0	**11**	1	0	1	1	**7**	0	1	1	1	**8**	1	0	0	0
5	0	1	0	1	**3**	0	0	1	1	**6**	0	1	1	0	**0**	0	0	0	0
6	0	1	1	0	**9**	1	0	0	1	**5**	0	1	0	1	**10**	1	0	1	0
7	0	1	1	1	**2**	0	0	1	0	**4**	0	1	0	0	**1**	0	0	0	1
8	1	0	0	0	**8**	1	0	0	0	**11**	1	0	1	1	**11**	1	0	1	1
9	1	0	0	1	**15**	1	1	1	1	**10**	1	0	1	0	**12**	1	1	0	0
10	1	0	1	0	**0**	0	0	0	0	**9**	1	0	0	1	**3**	0	0	1	1
11	1	0	1	1	**1**	0	0	0	1	**8**	1	0	0	0	**2**	0	0	1	0
12	1	1	0	0	**12**	1	1	0	0	**15**	1	1	1	1	**15**	1	1	1	1
13	1	1	0	1	**13**	1	1	0	1	**14**	1	1	1	0	**14**	1	1	1	0
14	1	1	1	0	**14**	1	1	1	0	**13**	1	1	0	1	**13**	1	1	0	1
15	1	1	1	1	**10**	1	0	1	0	**12**	1	1	0	0	**9**	1	0	0	1

Як видно з таблиці істинності операції що досліджується (табл. 3.32)

$$M(F_{1.1/1.3/1.1}(x))=M^{*}_{1.1/1.3/1.1}=\{5,7,4,6,8,0,10,1,11,12,3,2,15,14,13,9\}.$$

Тоді множина кількості змін в словах вхідної інформації буде:

$$M(x\oplus M(F_{1.1/1.3/1.1}(x))=\{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$$

$$\lambda_{cck}(F_{1.1/1.3/1.4}(x))=1/2$$

Результуюча операція відповідає вимогам критерію ССК.

Результуюче перетворення перших двох раундів є $F_{1.3/1.1}(x)$, в третьому раунді виконувалась операція $F_{1.2}(x)$. Знайдемо результуюче значення критерію ССК:

$$M^*_{1.2/1.3/1.1} = \{5,7,4,6,8,15,10,14,11,3,12,13,0,1,2,9\}.$$

Тоді $M(x \oplus M(F_{1.2/1.3/1.1}(x)) = \{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$

$$\lambda_{cck}(F_{1.2/1.3/1.4}(x)) = 1/2$$

Результуюче перетворення відповідає вимогам критерію ССК.

Результуюче перетворення перших двох раундів є $F_{1.3/1.1}(x)$, в третьому раунді виконувалась операція $F_{1.3}(x)$. Знайдемо результуюче значення критерію ССК:

$$M^*_{1.3/1.3/1.1} = \{3,2,11,9,8,6,0,4,1,12,5,7,10,14,13,15\}.$$

Тоді $M(x \oplus M(F_{1.3/1.3/1.1}(x)) = \{2,2,2,2,2,2,2,2,2,2,4,2,2,2,2,0\}$

$$\lambda_{cck}(F_{1.3/1.3/1.4}(x)) = 1/2$$

Результуюче перетворення не відповідає вимогам критерію ССК.

Результуюче перетворення перших двох раундів є $F_{1.3/1.1}(x)$, в третьому раунді виконувалась операція $F_{1.4}(x)$. Знайдемо результуюче значення критерію ССК:

$$M^*_{1.4/1.3/1.1} = \{0,1,2,3,14,10,15,8,13,6,0,11,9,7,4,12\}.$$

Тоді $M(x \oplus M(F_{1.3/1.3/1.1}(x)) = \{0,0,0,0,2,4,2,4,2,4,2,0,2,2,2,2\}$

$$\lambda_{cck}(F_{1.4/1.3/1.4}(x)) = 28/64 = 7/16$$

Якщо результуюче перетворення перших двох раундів є $F_{1.1/1.2}(x)$, а в третьому раунді виконувалась операція $F_{1.1}(x)$, тоді результуюча операція буде $F_{1.2}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_4 \end{bmatrix}$, яка відповідає вимогам ССК.

Якщо результуюче перетворення перших двох раундів є $F_{1.1/1.2}(x)$, а в третьому раунді виконувалась операція $F_{1.2}(x)$, тоді результуюча операція буде

$F_{1.1}(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$, яка відповідає вимогам ССК.

Якщо результуюче перетворення перших двох раундів було $F_{1.1/1.2}(x)$. В третьому раунді виконувалась операція $F_{1.3}(x)$, тоді результуюча таблиця підстановок буде:

$$M^*_{1.3/1.1/1.2}=\{12,13,14,10,2,9,3,11,1,0,15,8,6,4,7,5\}$$

Тоді $M(x \oplus M(F_{1.3/1.1/1.2}(x))=\{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$

$$\lambda_{cck}(F_{1.3/1.1/1.2}(x))=1/2$$

Результуюче перетворення не відповідає вимогам критерію ССК.

Якщо результуюче перетворення перших двох раундів є $F_{1.1/1.2}(x)$, а в третьому раунді виконувалась операція $F_{1.4}(x)$, тоді результуюча операція буде

$F_{1.4/1.1/1.2}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_4 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$, яка відповідає вимогам ССК.

Якщо результуюче перетворення перших двох раундів було $F_{1.3/1.2}(x)$. В третьому раунді виконувалась операція $F_{1.1}(x)$, тоді результуюча таблиця підстановок буде:

$$M^*_{1.1/1.3/1.2}=\{9,13,14,15,8,0,10,1,11,12,3,2,6,4,7,5\};$$

$$M(x \oplus M(F_{1.1/1.3/1.2}(x))=\{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\}$$

$\lambda_{cck}(F_{1.1/1.3/1.2}(x))=1/2$. Відповідає вимогам ССК

Якщо результуюче перетворення перших двох раундів було $F_{1.3/1.2}(x)$. В третьому раунді виконувалась операція $F_{1.2}(x)$, тоді результуюча таблиця підстановок буде:

$$M^{*}_{1.2/1.3/1.2} = \{9,2,1,0,8,15,10,14,11,3,12,13,6,4,7,5\};$$

$$M(x \oplus M(F_{1.2/1.3/1.2}(x)) = \{2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2\};$$

$$\lambda_{cck}(F_{1.2/1.3/1.2}(x)) = 1/2 .$$ Відповідає вимогам ССК

Якщо результуюче перетворення перших двох раундів було $F_{1.3/1.2}(x)$. В третьому раунді виконувалась операція $F_{1.3}(x)$, тоді результуюча таблиця підстановок буде:

$$M^{*}_{1.3/1.3/1.2} = \{9,2,1,0,8,15,10,14,11,3,12,13,6,4,7,5\};$$

$$M(x \oplus M(F_{1.3/1.3/1.2}(x)) = \{4,2,2,2,2,2,2,2,2,2,4,2,2,2,2,2\};$$

$$\lambda_{cck}(F_{1.3/1.3/1.2}(x)) = 9/16 .$$ Не відповідає вимогам ССК

Якщо результуюче перетворення перших двох раундів було $F_{1.3/1.2}(x)$. В третьому раунді виконувалась операція $F_{1.4}(x)$, тоді результуюча таблиця підстановок буде:

$$M^{*}_{1.4/1.3/1.2} = \{9,2,1,0,8,15,10,14,11,3,12,13,6,4,7,5\};$$

$$M(x \oplus M(F_{1.4/1.3/1.2}(x)) = \{2,2,2,2,2,4,2,4,2,4,2,0,4,4,4,4\};$$

$$\lambda_{cck}(F_{1.4/1.3/1.2}(x)) = 11/16 .$$ Не відповідає вимогам ССК

По аналогії побудуємо останні 56 трьохраундових перетворень інформації операціями, які відповідають вимогам критерію ССК, та визначимо відповідність ССК результуючого перетворення. Результати дослідження зведені в табл.3.33. По аналогії з табл. 3.31, виділивши кольором результуючі перетворення які відповідають вимогам ССК.

Таблиця 3.33

Узагальнені результати дослідження трьохраундового застосування операцій з ССК ($F_{1.1}(x)$ - $F_{1.4}(x)$)

Операція першого раунду шифрування	**Операція другого раунду шифрування**			
	$F_{1.1}(x)$	$F_{1.2}(x)$	$F_{1.3}(x)$	$F_{1.4}(x)$
$F_{1.1/1.1}(x)$	$F_{1.1/1.1/1.1}(x)$	$F_{1.2/1.1/1.1}(x)$	$F_{1.3/1.1/1.1}(x)$	$F_{1.4/1.1/1.1}(x)$
$F_{1.2/1.1}(x)$	$F_{1.1/1.2/1.1}(x)$	$F_{1.2/1.2/1.1}(x)$	$F_{1.3/1.2/1.1}(x)$	$F_{1.4/1.2/1.1}(x)$
$F_{1.3/1.1}(x)$	$F_{1.1/1.3/1.1}(x)$	$F_{1.2/1.3/1.1}(x)$	$F_{1.3/1.3/1.1}(x)$	$F_{1.4/1.3/1.1}(x)$
$F_{1.4/1.1}(x)$	$F_{1.1/1.4/1.1}(x)$	$F_{1.2/1.4/1.1}(x)$	$F_{1.3/1.4/1.1}(x)$	$F_{1.4/1.4/1.1}(x)$
$F_{1.1/1.2}(x)$	$F_{1.1/1.1/1.2}(x)$	$F_{1.2/1.1/1.2}(x)$	$F_{1.3/1.1/1.2}(x)$	$F_{1.4/1.1/1.2}(x)$
$F_{1.2/1.2}(x)$	$F_{1.1/1.2/1.2}(x)$	$F_{1.2/1.2/1.2}(x)$	$F_{1.3/1.2/1.2}(x)$	$F_{1.4/1.2/1.2}(x)$
$F_{1.3/1.2}(x)$	$F_{1.1/1.3/1.2}(x)$	$F_{1.2/1.3/1.2}(x)$	$F_{1.3/1.3/1.2}(x)$	$F_{1.4/1.3/1.2}(x)$
$F_{1.4/1.2}(x)$	$F_{1.1/1.4/1.2}(x)$	$F_{1.2/1.4/1.2}(x)$	$F_{1.3/1.4/1.2}(x)$	$F_{1.4/1.4/1.2}(x)$
$F_{1.1/1.3}(x)$	$F_{1.1/1.1/1.3}(x)$	$F_{1.2/1.1/1.3}(x)$	$F_{1.3/1.1/1.3}(x)$	$F_{1.4/1.1/1.3}(x)$
$F_{1.2/1.3}(x)$	$F_{1.1/1.2/1.3}(x)$	$F_{1.2/1.2/1.3}(x)$	$F_{1.3/1.2/1.3}(x)$	$F_{1.4/1.2/1.3}(x)$
$F_{1.3/1.3}(x)$	$F_{1.1/1.3/1.3}(x)$	$F_{1.2/1.3/1.3}(x)$	$F_{1.3/1.3/1.3}(x)$	$F_{1.4/1.3/1.3}(x)$
$F_{1.4/1.3}(x)$	$F_{1.1/1.4/1.3}(x)$	$F_{1.2/1.4/1.3}(x)$	$F_{1.3/1.4/1.3}(x)$	$F_{1.4/1.4/1.3}(x)$
$F_{1.1/1.4}(x)$	$F_{1.1/1.1/1.4}(x)$	$F_{1.2/1.1/1.4}(x)$	$F_{1.3/1.1/1.4}(x)$	$F_{1.4/1.1/1.4}(x)$
$F_{1.2/1.4}(x)$	$F_{1.1/1.2/1.4}(x)$	$F_{1.2/1.2/1.4}(x)$	$F_{1.3/1.2/1.4}(x)$	$F_{1.4/1.2/1.4}(x)$
$F_{1.3/1.4}(x)$	$F_{1.1/1.3/1.4}(x)$	$F_{1.2/1.3/1.4}(x)$	$F_{1.3/1.3/1.4}(x)$	$F_{1.4/1.3/1.4}(x)$
$F_{1.4/1.4}(x)$	$F_{1.1/1.4/1.4}(x)$	$F_{1.2/1.4/1.4}(x)$	$F_{1.3/1.4/1.4}(x)$	$F_{1.4/1.4/1.4}(x)$

На основі результатів наведених в табл..3.31 і 3.33 можна стверджувати, що при використанні операцій крипто перетворення гарантована відповідність вимогам критерію ССК, буде лише в результатів першого раунду шифрування. Застосування будь якої кількості раундів перетворення не гарантує максимальної невизначеності результатів, за винятком випадку застосування двох розрядних операцій і непарної кількості раундів перетворення [14].

ВИСНОВКИ ДО РОЗДІЛУ 3

На основі дослідження двох розрядних операції, які відповідають критерію строгого стійкого кодування, а також таблиць мінімальних кодових відстаней по

Хетінгу, запропоновано принципи синтезу операцій за критерієм ССК, та синтезовано повну множину даних двох розрядних операцій.

Перевірено та уточнено запропонований порядок синтезу операцій, які відповідають вимогам ССК, на прикладі чотирьох розрядних операцій. Встановлено, що процес синтезу операцій може бути автоматизованим на основі таблиці вибору варіантів підстановки шляхом перебору з наступною фільтрацією на коректність таблиць підстановки.

Розроблено метод синтезу операцій криптографічного перетворення які відповідають критерію строгого стійкого кодування адаптований до автоматизованого застосування шляхом програмної реалізації. Перевірено коректність програмної реалізації методу на прикладі синтезу чотирьох розрядних операцій та проведена оцінка результатів його реалізації. Представлення даних операцій дискретними моделями забезпечує мінімальний час їх реалізації як на апаратному так і на програмному рівні. Крім того, слід відмітити, що дані операції забезпечать заміну таблиць підстановок дискретними моделями, що значно знизить вимоги до обсягу пам’яті спеціалізованих обчислювальних систем, оскільки втрачається необхідність збереження великої кількості таблиць перестановок.

Можливість синтезу великої кількості операцій криптографічного перетворення за критерієм строгого стійкого кодування забезпечує можливість вибирати моделі невеликої складності, які забезпечать криптографічне перетворення інформації з меншим часом при тих самих характеристиках результатів перетворення.

На основі випадково вибраних результатів синтезу операцій було встановлено, що при використанні даних операцій крипто перетворення, гарантована відповідність вимогам критерію ССК, буде лише в результатів першого раунду шифрування. Застосування будь якої кількості раундів перетворення не гарантує максимальної невизначеності результатів, за винятком випадку застосування двох розрядних операцій і непарної кількості раундів перетворення.

Результати розділу опубліковані [3, 4, 8, 9, 14].

РОЗДІЛ 4
МЕТОД СИНТЕЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ МІНІМАЛЬНОЇ СКЛАДНОСТІ ЗА КРИТЕРІЄМ СТРОГОГО СТІЙКОГО КОДУВАННЯ

4.1 Моделювання чотирьох розрядних операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування

Дослідимо криптографічні перетворення які отримані за допомогою розробленого методу синтезу операцій криптографічного перетворення, які відповідають критерію строгого стійкого кодування, на основі мінімальної відстані за Хеммінгом [103]. В процесі дослідження встановлено наступне [5]:

- представлення даних операцій дискретними моделями забезпечує мінімальний час їх реалізації на апаратному та програмному рівні
- моделі операцій забезпечать заміну таблиць підстановок дискретними моделями, що значно знизить вимоги до обсягу пам’яті спеціалізованих обчислювальних систем, оскільки втрачається необхідність збереження великої кількості таблиць перестановок.
- можливість синтезу великої кількості операцій криптографічного перетворення за критерієм строгого стійкого кодування забезпечує можливість вибирати для реалізації крипто перетворень моделі різної складності, що в свою чергу забезпечить можливість варіативності обчислювальної складності алгоритмів.

Для систем потокового шифрування доцільно використовувати операції крипто перетворення які відповідають як критерію ССК, так і мають невелику складність (за кількістю операцій), адже складність математичної моделі крипто операції прямо пропорціональна часу її реалізації [104]. Синтезувавши дані операції для реалізації потокових шифрів, будуть створені умови для підвищення якості шифрування за рахунок досягнення максимальної невизначеності

результатів перетворення при збереженні швидкості перетворення, яка є основною перевагою потокових шифрів над блоковими.

Як показано в [3] для чотирьох розрядних операцій криптографічного перетворення інформації неможливо на основі перебору провести аналіз на строге стійке кодування, із за великої кількості операцій, навіть при автоматизованому синтезі достатньо проблематично виділити операції які мають найменшу, або близьку до найменшої складність, крім відповідності вимогам ССК. Виходячи з цього можна стверджувати, що застосування методу синтезу операцій криптографічного перетворення, які відповідають критерію строгого стійкого кодування, на основі мінімальної відстані за Хеммінгом, не ефективно.

При дослідженні двох розрядних операцій криптографічного перетворення інформації, які гарантовано забезпечують зміну половини бітів вхідної інформації (2.12 – 2.15) було встановлено, що всі вони будуються на основі перестановок двох розрядів та інверсії одного з розрядів [2]. Серед досліджених чотирьох розрядних операцій криптографічного перетворення, операції $F_{1.1}(x)$ та $F_{1.4}(x)$ також побудовані на основі перестановок та інверсій.

Якщо складність операції визначати через кількість входів логічних елементів функціональної схеми її реалізації, або кількістю мулевих операцій, які реалізують математичну модель, то серед множини операцій мінімальну складність мають операції, побудовані на основі перестановок. Проте серед цих операцій відсутні операції які відповідають вимогам ССК. Операції, які відповідають вимогам ССК, та побудовані на основі перестановок та інверсії половину розрядів мають найменшу складність, а значить мінімальну для сукупності всіх операцій, які синтезуються в даній роботі.

Проте для встановлення залежностей між перестановками та інверсіями які в сукупності забезпечать досягнення критерію ССК необхідно отримати додаткові дані на основі обчислювального експерименту. Під час експерименту перевіримо на відповідність критерію ССК чотирьох розрядних операцій синтезованих на повній перестановок чотирьох розрядів в поєднанні з повною множиною інверсій результатів перестановок.

В результаті обчислювального експерименту отримано 42 чотирьох розрядні операції мінімальної складності, які відповідають вимогам ССК.

Розглянемо і проаналізуємо дані операції для встановлення взаємозв'язків між перестановками та інверсіями для розробки методу синтезу аналогічних операцій довільної розрядності.

$$F_{1\epsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \end{bmatrix} \tag{4.1}$$

В операції (4.1) перестановки розрядів відсутні, проте інвертовані два розряди 1 і 2 з чотирьох.

$$F_{2\epsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix} \tag{4.2}$$

В операції (4.2) перестановки розрядів також відсутні, проте інвертовані 1 і 3 розряди.

$$F_{3\epsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.3}$$

В операції (4.3) перестановки розрядів також відсутні, проте інвертовані 1 і 4 розряди.

$$F_{4\epsilon} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix} \tag{4.4}$$

В операції (4.4) відсутні перестановки розрядів, інвертовані 2 і 3 розряди.

$$F_{5\epsilon} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.5}$$

В операції (4.5) відсутні перестановки розрядів, інвертовані 2 і 4 розряди.

$$F_{6\epsilon} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.6}$$

В операції (4.6) відсутні перестановки розрядів, інвертовані 3 і 4 розряди.

Шість операцій (4.1 – 4.6) складають групу операцій в яких відсутні перестановки розрядів, але присутні всі набори інверсій двох розрядів з чотирьох буде визначатися як:

$$k_{4,0p} = C_4^2$$

де $C_4^2 = \dfrac{4!}{2!\cdot(4-2)!} = 6$.

Розглянемо наступну групу операцій.

$$F_{7\varepsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \\ x_2 \end{bmatrix} \tag{4.7}$$

В операції (4.7) переставлені другий з четвертим розряди, а після цього інвертовані перший і другий розряди. Необхідно відмітити, що інвертовано один з переставлених розрядів і не переставлений розряд.

$$F_{8\varepsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_4 \\ x_3 \\ x_2 \oplus 1 \end{bmatrix} \tag{4.8}$$

В операції (4.8), також, переставлені другий з четвертим розряди, а після цього інвертовані перший і четвертий розряди. Необхідно відмітити, що інвертовано один з переставлених розрядів і не переставлений розряд. Операція (4.7) відрізняється від (4.8) тим що в них інвертуються різні разряди серед переставлених.

$$F_{9\varepsilon} = \begin{bmatrix} x_1 \\ x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \end{bmatrix} \tag{4.9}$$

$$F_{10\varepsilon} = \begin{bmatrix} x_1 \\ x_4 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \end{bmatrix} \tag{4.10}$$

В операціях (4.9) і (4.10), на відміну від операцій (4.7) і (4.8) інвертовано інший не переставлений розряд.

Наступну групу операцій, складають чотири операції, в яких переставлені місцями третій та четвертий розряди.

$$F_{11\varepsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_4 \\ x_3 \end{bmatrix} \tag{4.11}$$

$$F_{12\varepsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix} \tag{4.12}$$

$$F_{13\varepsilon} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} \tag{4.13}$$

$$F_{14\varepsilon} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix} \tag{4.14}$$

На основі виразів (4.7 – 4.10) та виразів (4.11 – 4.14) можна зробити висновок, для чотирьох розрядних операцій, для того, щоб вони відповідали вимогам ССК, при наявності перестановки двох розрядів, повинні інвертуватися два розряди з яких один не переставлений, а інший переставлений.

Для доведення даного висновку, перевіримо інші групи операцій, в яких переставлено два розряди.

Якщо переставлені другий і третій розряди, тоді за результатами експерименту було отримано чотири операції.

$$F_{15\varepsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \end{bmatrix} \tag{4.15}$$

$$F_{16\varepsilon} = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \end{bmatrix} \tag{4.16}$$

$$F_{17\varepsilon} = \begin{bmatrix} x_1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.17}$$

$$F_{18\varepsilon} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.18}$$

У виразах (4.15, 4.16) інвертовано перший не переставлений та другий і третій переставлені розряди відповідно. Вирази (4.17, 4.18) відрізняються від (4.15, 4.16) тим, що в них інвертовано замість першого не переставленого розряду четвертий не переставлений розряд.

Якщо переставлені перший і другий розряди, тоді за результатами експерименту було отримано чотири операції

$$F_{19\varepsilon} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix} \tag{4.19}$$

$$F_{20\epsilon} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.20}$$

$$F_{21\epsilon} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix} \tag{4.21}$$

$$F_{22\epsilon} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.22}$$

У виразах (4.19 – 4.22) інвертовано по одному не переставленому та по одному переставленому розрядах.

Якщо переставлені перший і третій розряди, тоді також за результатами експерименту було отримано чотири операції.

$$F_{23\epsilon} = \begin{bmatrix} x_3 \oplus 1 \\ x_2 \oplus 1 \\ x_1 \\ x_4 \end{bmatrix} \tag{4.23}$$

$$F_{24\epsilon} = \begin{bmatrix} x_3 \oplus 1 \\ x_2 \\ x_1 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.24}$$

$$F_{25\text{є}} = \begin{bmatrix} x_3 \\ x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_4 \end{bmatrix} \tag{4.25}$$

$$F_{26\text{є}} = \begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix} \tag{4.26}$$

Дана група операцій (4.23 – 4.26) також підтверджує висновок, що для забезпечення вимогам ССК, чотирьох розрядна операція повинна мати по одному інвертованому переставленому розряду, та по одному інвертованому не переставленому розряду.

Для доведення даного твердження необхідно розглянути останню із нерозглянутих парних перестановок. Переставлені місцями перший та четвертий розряди.

$$F_{27\text{є}} = \begin{bmatrix} x_4 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \end{bmatrix} \tag{4.27}$$

$$F_{28\text{є}} = \begin{bmatrix} x_4 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_1 \end{bmatrix} \tag{4.28}$$

$$F_{29\epsilon} = \begin{bmatrix} x_4 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \oplus 1 \end{bmatrix} \tag{4.29}$$

$$F_{30\epsilon} = \begin{bmatrix} x_4 \\ x_2 \\ x_3 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \tag{4.30}$$

Виразах (4.27 – 4.30) завершили представлення результатів моделювання чотирьох розрядних операцій з однією перестановкою двох розрядів та інверсіями. Наведена повна множина операцій підтверджує висновок, що якщо чотирьох розрядна операція має по одному інвертованому переставленому розряду, та по одному інвертованому не переставленому розряду то вона відповідає вимогам ССК.

Визначимо кількість груп чотирьох розрядних операцій в яких присутня одна парна перестановка.

Кількість груп даних операцій визначається на основі вибору варіантів перестановки на основі сполук без повторення $C_4^2 = \frac{4!}{2! \cdot (4-2)!} = 6$. Дана кількість груп встановлена за результатами експерименту.

Так як в кожній групі присутні чотири операції в яких інвертовано по одному переставленому та одному не переставленому розряду, тобто, по одному з двох розрядів в кожній підгрупі переставлених та не переставлених розрядів ($2 \cdot C_2^1 = 2\frac{2!}{1! \cdot (2-1)!} = 4$), що і показами результати експерименту.

Кількість чотирьох розрядних операцій які відповідають вимогам ССК в яких присутня одна парна перестановка буде визначатися:

$$k_{4,1p} = C_4^2 \cdot 2 \cdot C_2^1 = 2 \cdot C_2^1 \cdot C_4^2 = 24$$

Результати моделювання показали відсутність операцій на відповідність ССК при наявності перестановки трьох розрядів.

Розглянемо результати моделювання чотирьох розрядних операцій які відповідають вимогам ССК при наявності двох парних перестановок.

Розглянемо групу операцій в яких попарно переставлені перший і другий та третій і четвертий розряди:

$$F_{31\varepsilon} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} \tag{4.31}$$

$$F_{32\varepsilon} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix} \tag{4.32}$$

$$F_{33\varepsilon} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} \tag{4.33}$$

$$F_{34\varepsilon} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix} \tag{4.34}$$

На основі виразів (4.31 – 4.34) можна запропонувати гіпотезу, що для забезпечення вимогам ССК, чотирьох розрядна операція повинна мати по одному інвертованому розряду в кожній парній перестановці.

Наступну групу операцій складають операції в яких попарно переставлені перший і третій та другий і четвертий розряди:

$$F_{35\varepsilon} = \begin{bmatrix} x_3 \oplus 1 \\ x_4 \oplus 1 \\ x_1 \\ x_2 \end{bmatrix} \tag{4.35}$$

$$F_{36\varepsilon} = \begin{bmatrix} x_3 \oplus 1 \\ x_4 \\ x_1 \\ x_2 \oplus 1 \end{bmatrix} \tag{4.36}$$

$$F_{37\varepsilon} = \begin{bmatrix} x_3 \\ x_4 \oplus 1 \\ x_1 \oplus 1 \\ x_2 \end{bmatrix} \tag{4.37}$$

$$F_{38\varepsilon} = \begin{bmatrix} x_3 \\ x_4 \\ x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \tag{4.38}$$

Вирази (4.35 – 4.38) підтверджують гіпотезу, що чотирьох розрядна операція відповідає вимогам ССК, якщо має по одному інвертованому розряду в кожній парній перестановці.

Для забезпечення коректності гіпотези розглянемо останню групу із чотирьох операцій, отриману за результатами експерименту в яких попарно переставлені перший і четвертий та другий і третій розряди:

$$F_{39в} = \begin{bmatrix} x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_1 \end{bmatrix} \tag{4.39}$$

$$F_{40в} = \begin{bmatrix} x_4 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_1 \end{bmatrix} \tag{4.40}$$

$$F_{41в} = \begin{bmatrix} x_4 \\ x_3 \oplus 1 \\ x_2 \\ x_1 \oplus 1 \end{bmatrix} \tag{4.41}$$

$$F_{42в} = \begin{bmatrix} x_4 \\ x_3 \\ x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \tag{4.42}$$

Вирази (4.31 – 4.42) складають повну групу двох парних перестановок з однією інверсією к кожній парі переставлених біт. Так як інших варіантів двох парних перестановок чотирьох розрядів не існує то запропоновану гіпотезу, що для забезпечення вимогам ССК, чотирьох розрядна операція повинна мати по одному інвертованому розряду в кожній парній перестановці. можна вважати правильною для повної множини операцій.

Визначимо кількість груп чотирьох розрядних операцій в яких присутні дві парні перестановки. За результатами обчислювального експерименту встановлено що існує три групи даних операцій по чотири операції в кожній.

Визначимо через число сполук експериментально встановлену кількість груп чотирьох розрядних операцій в яких присутні дві парні перестановки.

Варіанти парних перестановок для побудови груп чотирьох розрядних операцій, які відповідають вимогам ССК, наведені в табл. 4.1.

Аналіз табл.4.1 показав, що визначити кількість груп чотирьох розрядних операцій в яких присутні дві парні перестановки можна на основі сполучень не з чотирьох елементів, а з трьох елементів ($C_3^1 = C_3^2 = 3$), тому, що перший елемент кортежу, який буде переставлятися завжди переставляється.

Таблиця 4.1

Варіанти парних перестановок для побудови груп чотирьох розрядних операцій, які відповідають вимогам ССК

№	Варіант парної перестановки				Кількість	
0	1	2	3	4	**1**	**10**
1	**2**	**1**	3	4	**6**	
2	**3**	2	**1**	4		
3	**4**	2	3	**1**		
4	1	**3**	**2**	4		
5	1	**4**	3	**2**		
6	1	2	**4**	**3**		
7	**2**	**1**	**4**	**3**	**3**	
8	**3**	**4**	**1**	**2**		
9	**4**	**3**	**2**	**1**		

В кожній групі присутні чотири операції в яких інвертовано по одному переставленому розряду в кожній підгрупі, елементи якої переставляються між собою ($2 \cdot C_2^1 = 4$), що і показами результати експерименту [4].

Кількість чотирьох розрядних операцій які відповідають вимогам ССК в яких присутні дві парні перестановки буде визначатися:

$$k_{4,2p} = C_3^2 \cdot 2 \cdot C_2^1 = 2 \cdot C_2^1 \cdot C_3^2 = 12$$

Загальна кількість чотирьох розрядних операцій які побудовані на основі перестановок і інверсій та відповідають вимогам ССК буде визначатися як:

$$k_{4,pi} = k_{4,0p} + k_{4,1p} = k_{4,2p} = C_4^2 + 2 \cdot C_2^1 \cdot C_4^2 + 2 \cdot C_2^1 \cdot C_3^2 = 6 + 24 + 12 = 42$$

$$k_{4,pi} = C_4^2 + 2 \cdot C_2^1 \cdot C_4^2 + 2 \cdot C_2^1 \cdot C_3^2 = C_4^2 + 2 \cdot C_2^1 \cdot (C_4^2 + C_3^2) \quad (4.43)$$

Отримані наукові результати дозволяють розробити метод синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм ССК.

4.2 Метод синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування

4.2.1 Розробка методу синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування

Двох розрядні операції криптографічного перетворення інформації відповідають вимогам ССК (2.12 – 2.15), будуються на основі інверсії половини біт як переставлених, так і не переставлених.

Основні отримані наукові результати, отримані при досліджені чотирьох розрядних операцій криптографічного перетворення (4.1 – 4.42), які необхідні для розробки методу синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм ССК полягають в наступному: досліджені чотирьох розрядниі операції криптографічного перетворення які відповідають вимогам ССК, та мають мінімальну будуються на основі:

- інверсії половини (двох) біт якщо відсутні перестановки;
- інверсії одного переставленого розряду та не переставленого розряду при наявності однієї парної перестановки;
- інверсії одного з двох розрядів в кожній парній перестановці, при наявності двох парних перестановок.

По аналогії з правилами синтезу чотирьох розрядних операцій криптографічного перетворення які мають мінімальну складність і відповідають вимогам критерієм ССК, сформулюємо правила синтезу аналогічних шести розрядних операцій:

- інверсії половини (трьох) біт якщо відсутні перестановки. Наприклад:

$$F_{1n} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \\ x_5 \oplus 1 \\ x_6 \end{bmatrix}, \qquad F_{2n} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \\ x_5 \oplus 1 \\ x_6 \end{bmatrix}, \qquad F_{3n} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \\ x_5 \\ x_6 \oplus 1 \end{bmatrix}; \quad (4.44)$$

- інверсії одного переставленого розряду та двох не переставлених розряді при наявності однієї парної перестановки.

Наприклад:

$$F_{4n} = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \\ x_5 \oplus 1 \\ x_6 \end{bmatrix}, \qquad F_{5n} = \begin{bmatrix} x_4 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \oplus 1 \\ x_5 \oplus 1 \\ x_6 \end{bmatrix}, \qquad F_{6n} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_5 \oplus 1 \\ x_4 \\ x_6 \oplus 1 \end{bmatrix}; \quad (4.45)$$

- інверсії одного переставленого розряду в кожній з двох парних перестановок та інверсії одного з не переставлених розрядів.

Наприклад:

$$F_{7n} = \begin{bmatrix} x_6 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \\ x_5 \oplus 1 \\ x_1 \end{bmatrix}, \qquad F_{5n} = \begin{bmatrix} x_4 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \oplus 1 \\ x_5 \oplus 1 \\ x_6 \end{bmatrix}, \qquad F_{9n} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \\ x_5 \oplus 1 \\ x_4 \\ x_6 \oplus 1 \end{bmatrix}; \quad (4.46)$$

- інверсії одного з двох розрядів в кожній парній перестановці, при наявності трьох парних перестановок.

Наприклад:

$$F_{10n} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \\ x_5 \oplus 1 \\ x_6 \end{bmatrix}, \qquad F_{11n} = \begin{bmatrix} x_4 \\ x_6 \oplus 1 \\ x_5 \\ x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \end{bmatrix}, \qquad F_{12n} = \begin{bmatrix} x_5 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_6 \\ x_1 \\ x_4 \oplus 1 \end{bmatrix}. \quad (4.47)$$

Аналіз показав, що всі наведені операції ($F_{1n} - F_{12n}$) відповідають вимогам критерію ССК.

Узагальнивши отримані результати дослідження сформулюємо метод синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм ССК: синтез операцій, які задовольняють критерію ССК і мають мінімальну складність проводиться на основі парних перестановок та інверсії, шляхом інверсії половини біт, за умови однієї інверсії в кожній парній перестановці.

Наведемо приклади операцій синтезованих даним методом:

- восьми бітові операції

$$F_{13n} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \\ x_5 \oplus 1 \\ x_6 \\ x_7 \oplus 1 \\ x_8 \end{bmatrix}, \qquad F_{14n} = \begin{bmatrix} x_4 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \oplus 1 \\ x_5 \oplus 1 \\ x_6 \\ x_8 \oplus 1 \\ x_7 \end{bmatrix}, \qquad F_{15n} = \begin{bmatrix} x_5 \oplus 1 \\ x_8 \\ x_4 \oplus 1 \\ x_3 \\ x_1 \\ x_7 \\ x_6 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \qquad F_{16n} = \begin{bmatrix} x_3 \\ x_7 \oplus 1 \\ x_1 \oplus 1 \\ x_4 \\ x_5 \oplus 1 \\ x_8 \oplus 1 \\ x_2 \\ x_6 \end{bmatrix} \quad (4.48)$$

- десяти бітові операції

$$F_{17n}=\begin{bmatrix} x_1\oplus 1\\ x_2\oplus 1\\ x_3\\ x_4\oplus 1\\ x_5\oplus 1\\ x_6\\ x_7\oplus 1\\ x_8\\ x_9\\ x_{10}\end{bmatrix},\quad F_{18n}=\begin{bmatrix} x_5\oplus 1\\ x_8\\ x_4\oplus 1\\ x_3\\ x_1\\ x_7\\ x_6\oplus 1\\ x_2\oplus 1\\ x_{10}\\ x_9\oplus 1\end{bmatrix},\quad F_{19n}=\begin{bmatrix} x_1\oplus 1\\ x_2\oplus 1\\ x_3\\ x_{10}\oplus 1\\ x_9\oplus 1\\ x_8\oplus 1\\ x_7\\ x_6\\ x_5\\ x_4\end{bmatrix},\quad F_{20n}=\begin{bmatrix} x_7\\ x_{10}\oplus 1\\ x_6\\ x_4\\ x_5\\ x_3\oplus 1\\ x_1\oplus 1\\ x_8\oplus 1\\ x_9\oplus 1\\ x_2\end{bmatrix} \quad (4.49)$$

Аналіз показав, що всі наведені операції ($F_{13n}-F_{20n}$) відповідають вимогам критерію ССК.

На основі розробленого методу оцінимо потужність множини синтезованих операцій.

4.2.2 Оцінка потужності груп синтезовних операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування

Уточнимо кількість операцій, які відповідають критерію строгого стійкого кодування синтезованих даним методом. При застосовуванні лише операції інверсії без застосування операцій перестановки можна отримати операції критерію строгого стійкого кодування кількість яких визначається наступним чином: для дворозрядного коду кількість операцій визначається за виразом C_2^1, для чотирирозрядного коду – C_4^2, для шістирозрядного коду – C_6^3, для n-розрядного коду при умові, що n парне число, – $C_n^{\frac{1}{2}n}$ [5].

Для чотирирозрядного коду при виконанні однієї перестановки кількість варіантів перестановок буде дорівнювати C_4^2, при цьому, відповідно до розробленого методу синтезу один із переставлених розрядів повинен бути інвертованим, тому кількість операцій з однією і тією ж перестановкою буде

збільшена в двічі, так як кожна з операцій відрізняється вибором розряду який інвертується. Кількість інверсій розрядів, які не переставлялися, для кожної перестановки, при одній перестановці менша від загальної кількості інверсій і дорівнюватиме C_2^1. Загальна кількість чотири розрядних операції з однією перестановкою визначається як $2 \cdot C_4^2 \cdot C_2^1$. Тоді для шести розрядного коду кількість операцій з однією перестановкою визначається як $2 \cdot C_6^2 \cdot C_4^2$ [5].

В загальному вигляді кількість n-розрядних операцій строгого стійкого кодування в яких присутня одна перестановки буде визначатись як добуток подвоєної кількості перестановкою двох розрядів $\left(2C_n^2\right)$, і кількість інверсій для кожної перестановки, яка розраховується як $C_{n-2}^{\frac{1}{2}(n-2)}$. Виходячи з цього кількість операцій строгого стійкого кодування, в яких присутня одна перестановка, визначається як: $2 \cdot C_n^2 \cdot C_{n-2}^{\frac{1}{2}(n-2)}$ [5].

По аналогії, кількість n -розрядних операцій строгого стійкого кодування в яких присутні дві перестановки буде визначатись як: $4 \cdot C_n^2 \cdot C_{n-2}^2 \cdot C_{n-4}^{\frac{1}{2}(n-4)}$

Виходячи з цього в загальному вигляді кількість операцій n-розрядного коду може бути розраховано за наступним виразом:

$$C = C_n^{\frac{1}{2}n} + 2^1 \cdot C_{n-2}^2 \cdot C_{n-2}^{\frac{1}{2}(n-2)} + 2^2 \cdot C_n^4 \cdot C_{n-2}^{\frac{1}{2}(n-2)} \cdot C_{n-4}^{\frac{1}{2}(n-4)} + \ldots + 2^k \cdot C_n^{2k} \cdot C_{n-2k}^{\frac{1}{2}(n-2k)},$$

при $0 < {}^{k \le \frac{1}{2}n}$ [5].

Отриманий вираз дозволяє зробити приблизну оцінку кількості операцій, що забезпечують строге стійке кодування, які отримані на основі запропонованого методу.

Проведемо точну оцінку потужності множини операцій, синтезованих на основі запропонованого методу на основі рекурентних послідовностей. Отримаємо залежність для розрахунку n - го члена послідовності [1, 105, 106]. Для встановлення залежності використаємо графічну інтерпретацію перестановок.

Отримати парні перестановки для побудови груп шести розрядних операцій, які відповідають вимогам ССК можливо на основі парних перестановок для побудови груп чотирьох розрядних операцій, які відповідають вимогам ССК. Для цього, побудуємо, для групи шести розрядних операцій, варіанти однієї парної перестановки, та доповнимо групу варіантом операцій без парних перестановок. Доповнення групи проводилось по аналогії з побудовою варіантів парних перестановок для груп чотирьох розрядних операцій (табл. 4.1.). Отримаємо 16 комбінацій, з яких одна не містить парної перестановки і 15 мають по одній парній перестановці ($C_6^2 = 15$). Дані варіанти побудови операцій наведені в табл. 4.3.

Якщо в добавлених двох розрядах, переставлених, чи не переставлених буде один інвертований один розряд, то кількість таких операцій відповідно до табл. 4.3. можливо розрахувати через кількість чотирьох розрядних операцій які побудовані на основі перестановок і інверсій та відповідають вимогам ССК.

$$k^*_{6,pi} = 2 \cdot k_{4,pi} \cdot (C_6^2 + 1) \qquad (4.50)$$

Таблиця 4.2

Варіанти однієї парної перестановки для побудови груп шести розрядних операцій, які відповідають вимогам ССК

№	Варіант парної перестановки						Кількість	
1	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**16**
2	**2**	**1**	**3**	**4**	**5**	**6**	**15**	
3	**3**	**2**	**1**	**4**	**5**	**6**		
4	**4**	**2**	**3**	**1**	**5**	**6**		
5	**5**	**2**	**3**	**4**	**1**	**6**		
6	**6**	**2**	**3**	**4**	**5**	**1**		
7	**1**	**3**	**2**	**4**	**5**	**6**		
8	**1**	**4**	**3**	**2**	**5**	**6**		
9	**1**	**5**	**3**	**4**	**2**	**6**		
10	**1**	**6**	**3**	**4**	**5**	**2**		
11	**1**	**2**	**4**	**3**	**5**	**6**		
12	**1**	**2**	**5**	**4**	**3**	**6**		
13	**1**	**2**	**6**	**4**	**5**	**3**		
14	**1**	**2**	**3**	**5**	**4**	**6**		
15	**1**	**2**	**3**	**6**	**5**	**4**		
16	**1**	**2**	**3**	**4**	**6**	**5**		

Множник 2 в виразі (4.50) показує, що загальна кількість операцій які відповідають вимогам ССК мають по одній інверсії в кожному з переставлених розрядів.

Проте вираз (4.50) не враховує операцій які відповідають вимогам ССК і не мають інверсій добавлених двох розрядах. Дану кількість операцій можна визначити через кількість парних перестановок та інверсій трьох в чотирьох розрядному коді: $k^{**}_{6,pi} = 1 \cdot k_{4|3,pi}$.

Таблиця 4.3

Варіанти парних перестановок для побудови груп шести розрядних операцій, які відповідають вимогам ССК

№	Варіант парної перестановки						Кількість		
1.1	**1**	**2**	3	4	5	6	**1**		
1.2	**1**	**2**	4	3	5	6			
1.3	**1**	**2**	5	4	3	6			
1.4	**1**	**2**	6	4	5	3	**6**	**10**	
1.5	**1**	**2**	3	5	4	6			
1.6	**1**	**2**	3	6	5	4			
1.7	**1**	**2**	3	4	6	5			
1.8	**1**	**2**	4	3	6	5			
1.9	**1**	**2**	5	6	3	4	**3**		
1.10	**1**	**2**	6	5	4	3			
2.1	**2**	**1**	3	4	5	6	**1**		
2.2	**2**	**1**	4	3	5	6			
2.3	**2**	**1**	5	4	3	6			
2.4	**2**	**1**	6	4	5	3	**6**	**10**	
2.5	**2**	**1**	3	5	4	6			
2.6	**2**	**1**	3	6	5	4			
2.7	**2**	**1**	3	4	6	5			
2.8	**2**	**1**	4	3	6	5			
2.9	**2**	**1**	5	6	3	4	**3**		
2.10	**2**	**1**	6	5	4	3			
3.1	**3**	2	**1**	4	5	6	**1**		
3.2	**3**	4	**1**	2	5	6			
3.3	**3**	5	**1**	4	2	6			
3.4	**3**	6	**1**	4	5	2	**6**	**10**	**160**
3.5	**3**	2	**1**	5	4	6			
3.6	**3**	2	**1**	6	5	4			
3.7	**3**	2	**1**	4	6	5			
3.8	**3**	4	**1**	2	6	5			
3.9	**3**	5	**1**	6	2	4	**3**		
3.10	**3**	6	**1**	5	4	2			
. . . . .									

16.1	1	2	3	4	**6**	**5**	**1**	**10**	
16.2	2	1	3	4	**6**	**5**	**6**		
16.3	3	2	1	4	**6**	**5**			
16.4	4	2	3	1	**6**	**5**			
16.5	1	3	2	4	**6**	**5**			
16.6	1	4	3	2	**6**	**5**			
16.7	1	2	4	3	**6**	**5**			
16.8	2	1	4	3	**6**	**5**	**3**		
16.9	3	4	1	2	**6**	**5**			
16.10	4	3	4	1	**6**	**5**			

Загальна кількість шести розрядних операцій які побудовані на основі перестановок і інверсій та відповідають вимогам ССК буде визначатися як

$$k_{6,pi} = k^{*}_{6,pi} + k^{**}_{6,pi} == 2 \cdot k_{4,pi} \cdot (C_6^2 + 1) + k_{4|3,pi} \qquad (4.51)$$

На основі виразу (4.51) модна визначити загальну залежність від розрядності кількості операцій, які побудовані на основі перестановок і інверсій, та відповідають вимогам ССК

$$k_{n,pi} = 2 \cdot k_{n,pi} \cdot (C_n^{n/2} + 1) + k_{n|(n/2+1),pi} \qquad (4.52)$$

Вираз (4.52) показує, що зі збільшенням розрядності, кількість операцій збільшується в комбінаторній залежності.

4.3 Застосування синтезованих операцій криптографічного перетворення інформації мінімальної складності за критерієм строгого стійкого кодування

4.3.1 Реалізація синтезованих операцій криптографічного перетворення інформації

Практична реалізація операцій крипто перетворення які відповідають вимогам ССК може бути виконана на програмному та апаратному рівнях. Як правило програмна реалізація крипто алгоритмів застосовується для блокового шифрування, а апаратна реалізація для потокового шифрування.

На сьогоднішній день подавляючи більшість мікроконтролерів, мікропроцесорів і процесорів комп'ютерних систем реалізують операції обробки інформаційних бітів в рамках обробки як мінімум байта інформації. Дане уточнення робить громіздкою, а як наслідок недостатньо швидкою і неефективною реалізацію операції які відповідають вимогам ССК на програмному рівні [6].

Виходячи з даного уточнення розглянемо апаратну реалізацію синтезованих операцій. Побудова функціональних схем пристроїв на основі синтезованих моделей операцій не викликає складностей [105-108]. Незначна складність дискретних моделей операцій не є непереборним фактором для побудови пристроїв, які реалізують по декілька операцій одночасно [109], при цьому вибір необхідної операції буде реалізовано на основі вибору необхідної команди.

Розглянемо реалізацію групи двохрозрядних операцій крипто перетворення які відповідають вимогам ССК. Синтез функціональної схеми пристрою проведемо за умови: якщо код команди буде «00» то необхідно реалізувати операцію (2.12); якщо «01» – операцію (2.13); якщо «10» – операцію (2.14); якщо «11» – операцію (2.15). Будувати функіональні схеми будемо по аналогії з пристроями для виконання логічних операцій криптографічного перетворення [110-112]. Функціональна схема пристрою наведене на рис. 4.1.

На рис. 4.1 позначено $x_1 - x_2$, $y_1 - y_2$, $k_1 - k_2$ перший та другий біти вхідних, вихідних даних та кодів команд відповідно.

Апаратну реалізацію чотирьох розрядних операцій розглянемо на прикладі операцій $F_{11\epsilon} - F_{14\epsilon}$, які описані моделями (4.11 –4.14). Синтез функціональної схеми пристрою проведемо за умови: якщо код команди буде «00» то необхідно реалізувати операцію (4.11); якщо «01» – операцію (4.12); якщо «10» – операцію (4.13); якщо «11» – операцію (4.14). Функціональна схема пристрою наведене на рис. 4.2

На рис. 4.2 позначено $x_1 - x_4$, $y_1 - y_4$, $k_1 - k_2$ відповідні біти вхідних і вихідних даних та кодів команд відповідно.

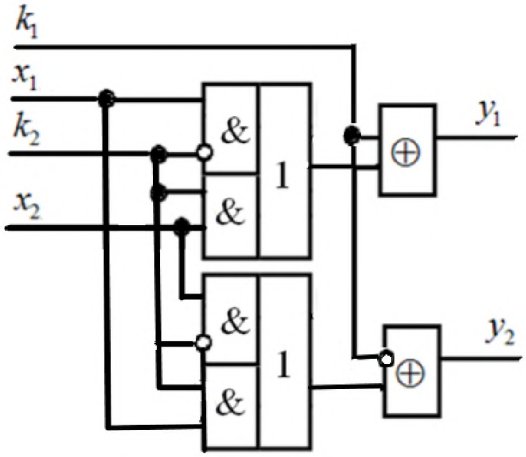

Рис. 4.1. Функціональна схема пристрою реалізації групи двохрозрядних операцій криптоперетворення які відповідають вимогам ССК.

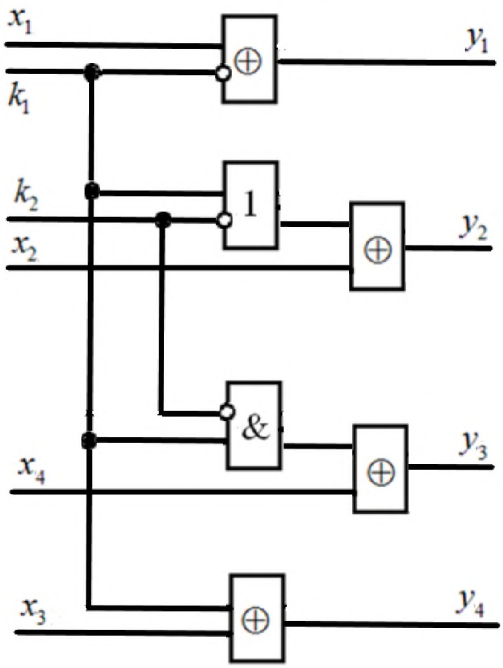

Рис. 4.2 Функціональна схема пристрою реалізації чотирьохрозрядних операцій криптоперетворення $F_{11є} - F_{14є}$, які відповідають вимогам ССК

По аналогії можливо будувати функціональні схеми пристроїв реалізації операцій криптоперетворення, які відповідають вимогам ССК довільної розрядності на основі синтезовиних моделей операцій.

Розглянемо можливість застосування синтезованих операцій та отриманих пристроїв при реалізації потокового шифрування.

4.3.2 Оцінка можливості застосування синтезованих операцій криптографічного перетворення інформації в потоковому шифруванні

Для оцінки можливості застосування операцій криптоперетворення які відповідають вимогам ССК розглянемо структурну схему потокового шифрування наведену на рис. 4.3 [113].

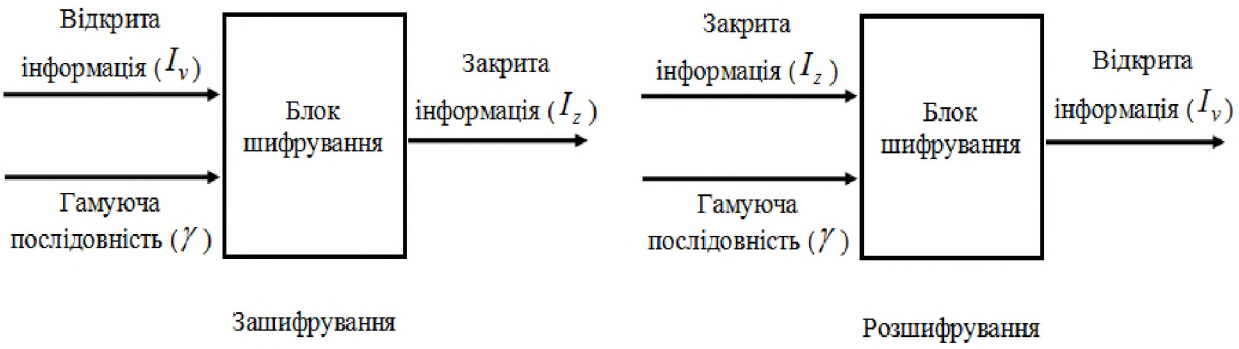

Рис. 4.3. Структурна схема потокового шифрування

В процесі зашифруваня відкрита інформація сумісно з гамуючою послідовністю поступають в блок шифрування де шляхом виконання над ними двохоперандної операції, яка має властивості операції додавання по модулю, формується закрита вихідна інформація. В процесі розшифруваня закрита інформація сумісно з ідентичною гамуючою послідовністю поступають в блок шифрування де шляхом виконання над ними двохоперандної операції, такою самою як і при за шифруванні, або аналогічною їй формується відкрита інформація, яка передавалася по закритому каналу зв’язку, або зберігалася в пам’яті комп’ютерної системи спеціального призначення.

Основна складність в застосуванні операцій криптоперетворення, які відповідають вимогам ССК полягає в тому, що дані операції однооперандні і виконують криптографічне преретворення, лише одного операнда, а саме вхідної

інформації без участі іншого (гамуючої послідовності), тому що він в операції відсутній

Проте в ряді досліджень показано, що групи однооперандних операцій можуть використовуватися в крипто примітивах шляхом їх випадкового вибору на основі гамуючої послідовності.

Оцінку можливості застосування синтезованих операцій в потокових шифрах проведемо на основі моделей двохрозрядних операцій криптоперетворення, які відповідають вимогам ССК. Для застосування в потокових шифрах з даних однооперандних операцій необхідно побудувати операцію по аналогії з операціями додавання по модулю два з точністю до перестановки які отримані в [114, 115]. Дані відомі двохоперандні операції наведені в наведені в табл. 4.4.

Необхідність побудови аналогічних операцій обумовлена тим, що застосування операцій, наведених в табл. 4.4, забезпечує підвищення стійкості і надійності потокового шифрування [2.9 – 2.10].

Виходячи з виразів (2.12 – 2.15) які описують двох розрядні однооперандні операції, необхідно побудувати двохоперандну операцію криптографічного перетворення. Дана операція забезпечить двохвохрозрядне строге стійке криптографічне кодування при потоковому шифруванні.

Таблиця 4.4

Група операцій додавання за модулем два з точністю до перестановки

$O_{1.1}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \\ x_{1.2} \oplus x_{2.2} \end{vmatrix}$	$O_{2.1}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \\ x_{1.2} \oplus x_{2.1} \end{vmatrix}$	$O_{3.1}^{\oplus} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \\ x_{1.1} \oplus x_{2.2} \end{vmatrix}$
$O_{1.2}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \\ x_{1.2} \oplus x_{2.2} \oplus 1 \end{vmatrix}$	$O_{2.2}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \\ x_{1.2} \oplus x_{2.1} \oplus 1 \end{vmatrix}$	$O_{3.2}^{\oplus} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \\ x_{1.1} \oplus x_{2.2} \oplus 1 \end{vmatrix}$
$O_{1.3}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \oplus 1 \\ x_{1.2} \oplus x_{2.2} \end{vmatrix}$	$O_{2.3}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \oplus 1 \\ x_{1.2} \oplus x_{2.1} \end{vmatrix}$	$O_{3.3}^{\oplus} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \oplus 1 \\ x_{1.1} \oplus x_{2.2} \end{vmatrix}$
$O_{1.4}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \oplus 1 \\ x_{1.2} \oplus x_{2.2} \oplus 1 \end{vmatrix}$	$O_{2.4}^{\oplus} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \oplus 1 \\ x_{1.2} \oplus x_{2.1} \oplus 1 \end{vmatrix}$	$O_{3.4}^{\oplus} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \oplus 1 \\ x_{1.1} \oplus x_{2.2} \oplus 1 \end{vmatrix}$

Випадковий вибір однооперандних операцій буде проводиться на основі команд перетворення, заданих гамуючою послідовністю, на основі моделі моделі:

$$O_{3\_10,12\_5,5\_12,10\_3} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} \tag{4.53}$$

Скористаемося технологією синтезу двохоперандних операцій крипто перетворення на основі однооперандних [2].

Для спрощення побудови операції, проведемо її в три етапи. На першому етапі побудуємо спрощену операцію, без врахування інверсій розрядів. Виходячи з (4.53) модель даної операція буду задана виразом:

$$O_{3\_5,3\_5,5\_3,5\_3} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases}.$$

Перетворемо дану операцію з врахуванням значень команд її реалізації в якості другого аргументу:

$$O_{3\_5,3\_5,5\_3,5\_3} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases}$$

Опраючись на отримані взаємоперетворення, операцію $O_{3\_5,3\_5,5\_3,5\_3}$ можна записати як:

$$O_{3\_5,3\_5,5\_3,5\_3} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \qquad (4.54)$$

На другому етапі синтезу побудуємо двохоперандну операцію обробки сигналів інверсії. Модель даної операції відповідно до (4.53) можна представити:

$$\overline{O}_{3\_10,12\_5,5\_12,10\_3} = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases}$$

Перетворемо операцію обробки сигналів інверсії з врахуванням значень команд реалізації в якості другого аргументу:

$$\overline{O}_{3\_10,12\_5,5\_12,10\_3} = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases}$$

Операцію $\overline{O}_{3\_5,3\_5,5\_3,5\_3}$ можна записати як:

$$\overline{O}_{3\_10,12\_5,5\_12,10\_3} = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{bmatrix} k_2 \\ \overline{k}_2 \end{bmatrix} \tag{4.55}$$

На основі додавання за модулем 2 поєднавши моделі (4.54) і (4.55) отримаємо операцію $O_{3\_10,12\_5,5\_12,10\_3}$

$$O_{3\_10,12\_5,5\_12,10\_3} = O_{3\_5,3\_5,5\_3,5\_3} \oplus \overline{O}_{3\_10,12\_5,5\_12,10\_3}$$

$$O_{3\_10,12\_5,5\_12,10\_3} = \begin{bmatrix} x_1 \cdot \overline{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \overline{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \overline{k}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \overline{k}_1 \oplus x_2 \cdot k_1 \oplus k_2 \\ x_1 \cdot \overline{k}_1 \oplus x_2 \cdot k_1 \oplus \overline{k}_2 \end{bmatrix} \tag{4.56}$$

Представимо операцію (4.56), як операцію обробки двох аргументів.

$$O_{3\_10,12\_5,5\_12,10\_3} = \begin{bmatrix} x_1 \cdot \overline{y}_1 \oplus x_2 \cdot y_1 \oplus y_2 \\ x_1 \cdot y_1 \oplus x_2 \cdot \overline{y}_1 \oplus \overline{y}_2 \end{bmatrix} \tag{4.57}$$

Отримана операція (4.57) забезпечує реалізацію строгого стійкого криптографічного кодування при її застосуванні в потокових шифрах, так як автоматично перетворює два розряди гамуючої послідовності в другий операнда, а також сумістно перетворює обидва операнда в зашифрований текст.

Основною перевагою синтезованої операції (4.57) над моделлю строгого стійкого криптографічного кодування (4.53) є простота її реалізації як на апаратному так і програмному рівні. Тому що дана операція допускає вибір в якості операндів операнда, які складаються з двох біт, або з двох байт, або з двох слів і т.д..Один із ва варіантів алгоритму реалізації наведено на рис. 4.4.

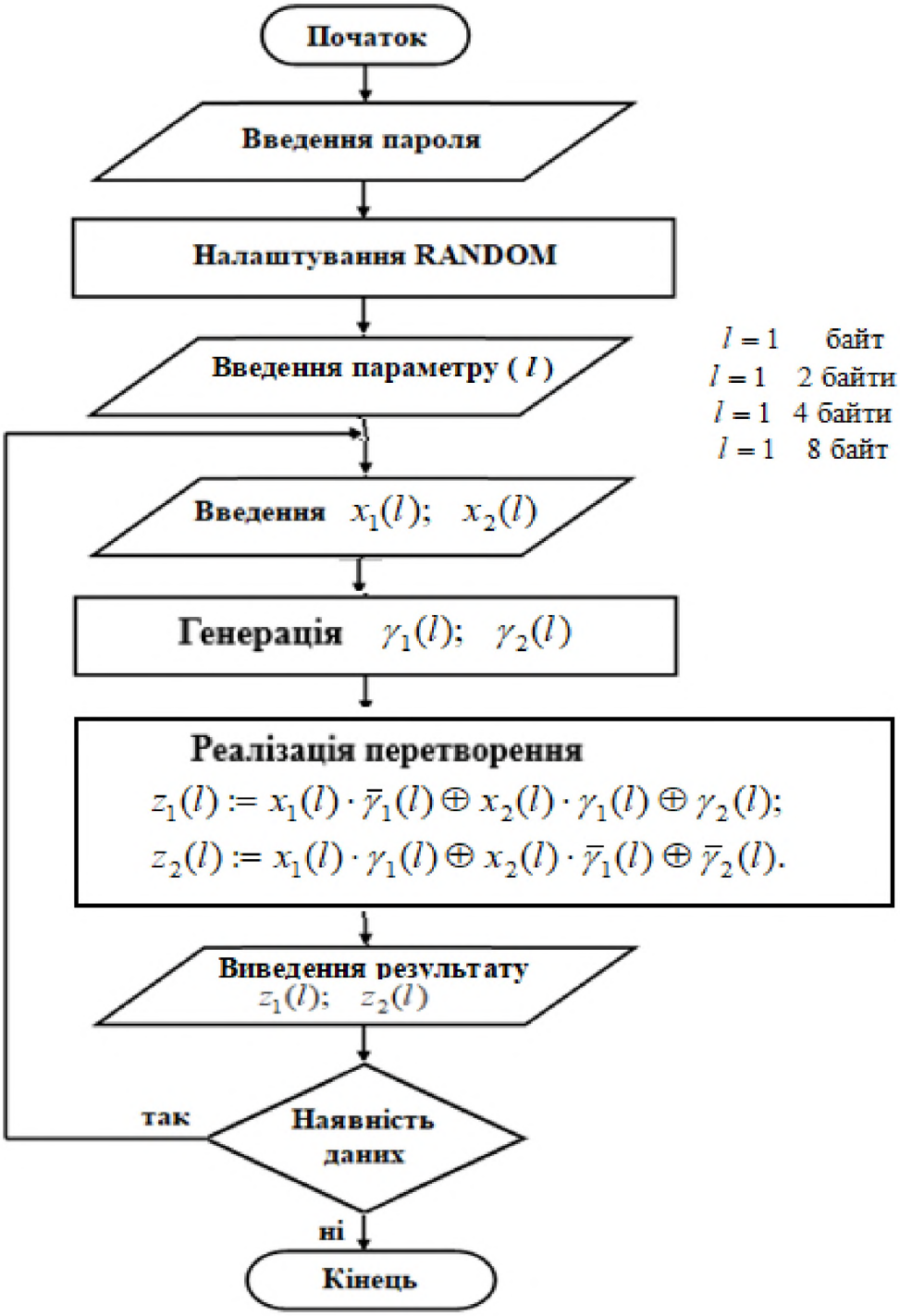

Рис. 4.4. Варіант алгоритму програмної реалізації шифрування

По аналогії можна побудувати двохоренандні операції довільної розрядності, наприклад чотири, вісім, шістнадцять розрядів, або іншої розрядності при наявності моделей одноперандних операцій даної розрядності які забезпечують відповідність вимогам ССК.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS [7, 11, 12]. Отримані результати дослідження можуть бути застосовані не тільки при побудові потокових систем шифрування. Застосування послідовностей які генеруються з використанням синтезованих операцій в імовірностних моделях, на прикладі інтегральної моделі розвитку і припинення пожежі, забезпечило підвищення точності моделювання [15, 16, 18].

ВИСНОВКИ ДО РОЗДІЛУ 4

На основі дослідження операції, які відповідають критерію строгого стійкого кодування було відмічено, що складність моделей відрізняється, а моделі операцій, які мають найменшу складність, складаються лише з перестановок і інверсій.

Відмічена особливість моделей була покладена в основу обчислювального експерименту, результати якого дозволили встановити обмеження та залежності між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності синтезованих моделей.

розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності сутність якого полягає в наступному: синтез операцій, які задовольняють критерію ССК і мають мінімальну складність, проводиться на основі парних перестановок та інверсії шляхом інверсії половини бітів, за умови однієї інверсії в кожній парній перестановці.

Для вирішення третьої наукової задачі були запропоновано використовувати синтезовані операції потокового шифрування, а саме – в блоці шифрування. Удосконалення методів синтезу програмно-апаратних засобів комп’ютерної криптографії полягає в побудові операцій криптоперетворення мінімальної складності без виконання етапів синтезу таблиць істинності та етапу мінімізації логічних функцій

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS, крім того, застосування даних послідовностей в імовірнісних моделях, на прикладі інтегральної моделі розвитку і припинення пожежі, забезпечило підвищення точності моделювання.

Результати розділу опубліковані [1-7, 10-12, 15, 16,18].

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування:

1) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом, для послідовного перетворення її в проміжну таблицю вибору варіантів підстановки та таблицю вибору варіантів підстановки для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;

2) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі узагальнення теоретичних і експериментальних досліджень, які забезпечили можливість використання лише операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;

3) набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування шляхом застосування методів синтезу моделей операцій із новими властивостями, які забезпечили спрощення синтезу програмних і апаратних криптографічних засобів. Синтез моделей операцій за критерієм строгого стійкого кодування мінімальної складності реалізовано без побудови таблиць істинності та етапу мінімізації булевих функцій, що значно спрощує побудову спеціалізованих програмно-апаратних засобів. Засоби, які синтезуються, забезпечують підвищення

ефективності криптографічних алгоритмів шляхом розширення множини операцій для їх побудови, а також забезпечують максимальну невизначеність результатів шифрування на основі гарантованої зміни кожного біта інформації з імовірністю одна друга;

4) практична цінність роботи полягає в доведенні розроблених методів до моделей, функціональних схем і програмних модулів для реалізації операцій потокового шифрування, синтезованих за критерієм строгого стійкого кодування. Основний практичний результаті роботи полягає в побудові операцій потокового шифрування, які гарантовано забезпечують зміну кожного біта інформації з ймовірністю одна друга, забезпечують максимальну невизначеність результатів шифрування.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS, крім того, застосування даних послідовностей в імовірнісних моделях, на прикладі інтегральної моделі розвитку і припинення пожежі, забезпечило підвищення точності моделювання.

Результати роботи впроваджено в приватному підприємстві «Сенсорна Електроніка», а також – у навчальний процес Черкаського державного технологічного університету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків: ХУПС ім. І. Кожедуба, 2015. С. 129–134.

2. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Аналіз дворозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту. *Наукові праці:* наук.-метод. журн. Чорномор. держ. ун-ту ім. Петра Могили. Миколаїв, 2017.

3. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник інженерної академії України:* часопис. Київ, 2016. Вип. 3. С. 105–108.

4. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. Вип. 1. С. 5–10.

5. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Побудова примітивів строгого стійкого кодування мінімальної складності. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2018. Вип. 1. С. 21–26.

6. Рудницький В. М., Лада Н. В., Федотова-Півень І. М., Пустовіт М. О., Нестеренко О. Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Системи управління, навігації та зв'язку:* зб. наук. праць ПНТУ ім. Юрія Кондратюка. 2018. Вип. 6 (52). С. 113–115.

7. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики*. Харків, 2014. Вип. 168. С. 53–58.

8. Нестеренко О. Б. Исследование двухразрядных операций, удовлетворяющих критерию строгого стойкого кодирования, при

многораундовом криптографическом преобразовании. *Wschodnioeuropejskie Czasopismo Naukowe* (East European sci. journal). 2018. No. 11 (39), part 2. С. 20–28. (Варшава, Польща).

9. Криптографічне кодування: обробка та захист інформації: кол. монографія / під ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

10. Бабенко В. Г., Нестеренко О. Б., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації*: тези доп. Другої міжнар. наук.-техн. конф. (Черкаси – Тольятті, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

11. Зажома В. М., Нестеренко О. Б. Генерація псевдовипадкових послідовностей на основі фільтрації матричних операцій криптоперетворення. *Проблеми інформатизації:* тези доп. Третьої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2015. 84 с.

12. Зажома В. М., Нестеренко О. Б. Вдосконалений метод вбудовування стегоповідомлення на основі ключового елементу. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П’ятої міжнар. наук.-техн. конф. (Полтава – Баку – Кіровоград – Харків). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2015. 72 с.

13. Шувалова Л. А., Нестеренко О. Б. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування. *Проблеми інформатизації*: тези доп. Четвертої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. С. 97.

14. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування . *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 14–16 листоп. 2018 р.).

Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

15. Пустовіт М. О., Нестеренко О. Б., Матяш П. В. Моделювання розпилених водяних струменів для комп'ютеризованих симуляторів з гасіння пожеж в будівлях. Техника и технология. *Актуальные научные проблемы. Рассмотрение, решение, практика.* Гданьск, 2015. С. 22.

16. Пустовіт М. О., Нестеренко О. Б., Жаврук П. С. Комп'ютерне моделювання розпорошених водяних струменів для симулятора припинення горіння. *Надзвичайні ситуації: безпека та захист:* матеріали всеукр. наук.-практ. конф. з міжнар. участю. Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2015. С. 311–314.

17. Нестеренко О. Б. Двораундове криптографічне кодування операціями зі строгим лавинним ефектом. *Проблеми та перспективи цивільного захисту:* матеріали міжнар. наук.-практ. конф. молодих учених (29–30 берез. 2017 р.). Харків: НУЦЗУ. С. 384.

18. Нестеренко О. Б. Вдосконалення систем моніторингу з надзвичайних ситуацій. *Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика).* Харків, 2014. С. 55.

19. Koblitz N., Algebraic Aspects of Cryptography, Springer-Verlag, Berlin, 1998. 215 p.

20. Коблиц Н. Курс теории чисел и криптографии. Москва: ТВП, 2001. 254 с.

21. Фомичев В. М. Дискретная математика и криптология: курс лекций. Москва: Диалог-МИФИ, 2003. 400 с.

22. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. Москва: МЦНМО, 2002. 104 с.

23. Cryptology and computational number theory, Proc. of Symp. in Appl. Math., v. 42, 1990.

24. Мао Венбо. Современная криптография: теория и практика / пер. с англ. Москва: Изд. дом «Вильямс», 2005. 768 с.: ил.; парал. тит. англ.

25. Ростовцев А. Г., Маховенко Е. Б. Теоретическая криптография. Москва: Профессионал, 2005. 490 с.

26. Черёмушкин А. В. Криптографические протоколы. Основные свойства и уязвимости. Москва: Изд. дом «Академия», 2009. 272 с.

27. Тилборг Х. К. А. ван. Основы криптологии: профессиональное руководство и интерактивный учебник. Москва: Мир, 2006. 471 с.

28. Жельников В. Криптография от папируса до компьютера. Москва: ABF, 1996. 335 с.

29. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография: учебник для вузов. Санкт-Петербург: Лань, 2000. 224 с.

30. Хорошко В. А., Чекатков А. А. Методи й засоби захисту інформації. Київ: Юніор, 2003. 504 с.

31. Саломаа А. Криптография с открытым ключом. Москва: Мир, 1996. 318 с.

32. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: підручник. Київ: ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.

33. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. Москва: Радио и связь, 2001. 376 с.

34. Дмитришин О. В. Методи і засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем: дис. ... канд. техн. наук: 05.13.05. Вінниця, 2012. 180 с.

35. Бабенко В. Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій: дис. ... канд. техн. наук: 05.13.21. Черкаси, 2009. 166 с.

36. Чечельницький В. Я. Методологія підвищення ефективності телекомунікаційних систем на основі інтеграції канального кодування та шифрування даних: дис. ... докт. техн. наук: 05.12.02. Одеса, 2013. 407 с.

37. Горбенко Ю. І., Ганзя Р. С. Аналіз шляхів розвитку криптографії після

появи квантових комп'ютерів. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/27194/1/8-40-48.pdf

38. Горбенко Ю. І., Ганзя Р. С. Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера. *Захист інформації:* науково-практичний журнал. Київ, 2014. Т. 16. № 2. С. 106–112.

39. Bernstein D., Buchmann J., Dahmen E. Post-quantum cryptography. Berlin: Springer, 2009. 246 p.

40. Основы криптографии: учеб. пособие / А. П. Алферов, А. К. Зубов, А. С. Кузьмин, А. В. Черемушкин; 2-е изд., испр. и доп. Москва: Гелиос АРВ, 2002. 480 с., ил.

41. Словарь криптографических терминов / под ред. Б. А. Погорелова и В. Н. Сачкова. Москва: МЦНМО, 2006. 94 с.

42. Жданов О. Н., Золотарев В. В. Методы и средства криптографической защиты информации: учеб. пособ. Красноярск: СибГАУ, 2007. 217 с.

43. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Москва: ТРИУМФ, 2002. 816 с.

44. Кузьминов Т. В. Криптографические методы защиты информации. Новосибирск: Наука, 1998. 185 с.

45. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры. Москва: Гелиос АРВ, 2005. 192 с.

46. Мухачев В. А., Хорошко В. А. Методы практической криптографии. Москва: Полиграф-Консалтинг, 2005. 209 с.

47. Чмора А. Л. Современная прикладная криптография. Москва: Гелиос АРВ, 2002. 244 с.

48. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособ. для вузов / [П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др.]. Москва: Радио и связь, 2000. 168 с.

49. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. Москва: ДМК Пресс, 2008. 544 с.

50. Крысин А. В. Информационная безопасность: практич. руководство.

Москва: СПАРРК; Киев: Век+, 2003. 320 с.

51. Панасенко С. П. Защита информации в компьютерных сетях: шифрование. *Мир ПК*. 2002. № 2. С. 70–73.

52. Фергюссон Н., Шнайер Б. Практическая криптография. Москва: Вильямс, 2005. 424 с.

53. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях. Москва: Научный мир, 2004. 172 с.

54. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. Москва: Горячая линия – Телеком, 2002. 175 с.

55. Goldreich O. Foundations of cryptography. Volume 1 (Basic tools). Vol. 2 (Basic applications). Cambridge University Press, Cambridge, United Kingdom, 2001 (v. 1), 2004 (v. 2).

56. Vergili I., Yücel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes. *Turk J Elec Engin*. 2001. T. 9. No. 2. C. 137–145.

57. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany, 2015. 100 с.

58. Шеннон К. Э.Теория связи в секретных системах. Работы по теории информации и кибернетике. Москва: ИЛ, 1963.

59. Menezes A. J., Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography, Pub. CRC Press, 1996. 816 p.

60. Бабаш А. В., Шанкин Г. П. Криптография / под ред. В. П. Шерстюка, Э.Л. Применко. Москва: СОЛОН-ПРЕСС, 2007. 512 с.

61. Beker H., Piper F., Cipher System, Northwood Books, 1982. 144 p.

62. Мельников В. В. Защита информации в компьютерных системах. Москва: Финансы и статистика – Электроинформ, 1997. 368 с.

63. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. Москва: Изд-во Агентства «Яхтсмен», 1996. 192 с.

64. Luby M. Pseudorandomness and cryptographic applications. Princeton

University Press, Princeton, New Jersey, 1996.

65. Логачев О. А., Ященко В. В., Сальников А. А. Булевы функции в теории кодирования и криптологии. Москва: МЦМНО, 2004. 469 с.

66. Агафонова И. В. Криптографические свойства нелинейных булевых функций: материалы семинара по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD». URL: http://www.dha.spb.ru/

67. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. Изд-во LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. 180 с.

68. Carlisle Adams. The CAST-256 Encryption Algorithm. URL: http://www.mavi1.org/web_security/cryptography/aes-testing/cast/cast-256.pdf

69. C. Adams H. M. Heys S. E. Tavares, and M. Wiener. An Analysis of the CAST-256 Cipher URL: //http://www.engr.mun.ca/~howard/PAPERS/cast256.pdf

70. Безбогов А. А., Яковлев А. Я., Шамкин В. Н. Криптографическая защита информации: учеб. пособие. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. 140 с.

71. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. Москва: Горячая линия-Телеком, 2001. 148 с.

72. Kocher P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. URL: http://citeseer.ist.psu.edu – Cryptography Research, Inc., San Francisco, USA.

73. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Москва: Наука, 2012. 552 с.

74. Барабанова М. И., Кияев В. И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: учеб. пособие. Санкт-Петербург: Изд-во СПбГУЭФ, 2010. 267 с.

75. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. Москва: ДМК Пресс, 2012. 592 с., ил.

76. Katz J., Lindell Y., Introduction to Modern Cryptography: Principles and Protocols – Chapman and Hall/CRC, 2007. 552 p.

77. Stinson D. R., Cryptography: Theory and Practice, CRC Press, 2007. 616 p.

78. Van Tilborg H.C.A., Jajodia S. Encyclopedia of Cryptography and Security. Springer, 2011. 1457 p.

79. Goldreich O. Foundations of Cryptography. Basic Applications, Cambridge University Press, 2004. 396 p.

80. Конхейм А. Г. Основы криптографии. Москва: Радио и связь, 1987.

81. Щербаков А. Ю., Домашев А. В. Прикладная криптография: использование и синтез криптографических интерфейсов. Москва: Русская Редакция, 2003. 416 с.

82. Масленников М. Практическая криптография. Санкт-Петербург: БХВ-Петербург, 2003. 464 с.

83. Столлингс В. Криптография и защита сетей: принципы и практика. 2-е изд. Москва: Вильяме, 2001. 672 с.

84. Васильева И. Н. Криптографические методы защиты информации: учеб. и практ. для академ. бакалавриата. Москва: Юрайт, 2018. 349 с.

85. Введение в криптографию / под общ. ред. В. В. Ященко. 4-е изд., доп. Москва: МЦНМО, 2012. 348 с.

86. Варновский Н. П. Криптография и теория сложности: матем. просв., сер. 3, 2. Москва: МЦНМО, 1998, С. 71–86.

85. Зубов А. Ю. Совершенные шифры. Москва: Гелиос АРВ, 2003. 160 с.

88. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: Теорія. Практика. Застосування: підруч. для ВНЗ. Харків: Форт, 2013. 880 с.

89. Richard A. Mollin. Codes: the guide to secrecy from ancient to modern times. Chapman & Hall/CRC, 2005. С. 142.

90. Thomas W. Cusick, Pantelimon Stanica, Pantelimon Stănică. Cryptographic Boolean Functions and Applications. Academic Press, 2009. С. 25.

91. Золотухин В. Ю., Чалкин Т. А. Разработка методики оценки зависимости криптостойкости алгоритма ГОСТ 28147-89 от выбранной ключевой информации Секция 2. Математические методы криптографии. (Сент. 2010). С. 20–21. URL: https://cyberleninka.ru/.../razrabotka-metodiki-otsenki-zavisimosti-riptostoykosti-alg...

92. URL: https://dic.academic.ru/dic.nsf/ruwiki/1312419

93. Криптографическое кодирование: методы и средства реализации: монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко, И. В. Миронец и др. Тольятти: Тольят. гос. ун-т., 2013. 196 с.

94. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку* : зб. наук. праць. Вип. 1 (21), т. 2. Київ: Центр. наук.-досл. ін-т навігації і управл., 2012. С. 170–173.

95. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України: науково-технічний журнал.* Харків: ХУПС ім. І. Кожедуба. 2011. Вип. 2(6). С. 112–114.

96. Криптографическое кодирование: методы и средства реализации (Ч. 2): монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко, Р. П. Мельник, С. В. Рудницкий, О. Г. Мельник. Харьков: Изд-во ООО «Щедрая усадьба плюс», 2014. 224 с.

97. Рудницький В. М., Бабенко В. Г. Властивості таблиць мінімальних кодових відстаней за Хеммінгом. *Сімнадцята наукова сесія Осередку Наукового товариства ім. Шевченка у Черкасах:* матеріали доповідей на засіданнях секцій і комісій (14-24 берез. 2007 р.) / за ред. В. В. Масненка. Черкаси: Осер. НТШ у Черк., 2007. С. 206–208.

98. Малець І. О. Роль та проблеми функціонування телекомунікаційних систем при надзвичайних ситуаціях. Електронний науковий архів Науково-технічної бібліотеки Національного університету «Львівська політехніка». 2011. URL: http://ena.lp.edu.ua.

99. Соколов В. Ю. Інформаційні системи і технології: навч. посіб. Київ: Вид-во ДУІКТ, 2010. 138 с.

100. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації:* зб. наук. праць. № 9 (107). Харків: ХУПС ім. І. Кожедуба, 2012.

С. 130–139.

101. Рудницький В. М., Миронець І. В. , Бабенко В. Г. Систематизація повної множини логічних функцій для криптографічного перетворення інформації. *Системи обробки інформації*: зб. наук. праць. Вип. 8 (98). Харків: ХУПС ім. І. Кожедуба, 2011. С. 184–188.

102. Квасников В. П. Рудницкий В. Н., Бабенко В. Г. Синтез таблиц минимальных кодовых расстояний по Хеммингу. *Електроніка та системи управління*. 2006. №3 (9). С. 47–52.

103. Хемминг Р. В., Гутера Р. С. Численные методы для научных работников и инженеров. Москва: Наука, 1968. 308 с.

104. Бабаш А. В. Шанкин Г. П. Криптография. Аспекты защиты. Москва: Солон-Р, 2002. 512 с.

105. Стахов А. П. Введение в алгоритмическую теорию измерений. Москва: Сов. радио,1972. 288 с.

106. Стахов А. П. Алгоритмическая теория измерений. *Новое в жизни, науке, технике. Сер. математика, кибернетика,* Москва: Знание, 1979. 64 с.

107. Прикладная теория цифровых автоматов / К. Г. Самофалов, А. М. Романкевич, В. Н. Валуйский, Ю. С. Каневский, М. М. Пиневич. Киев: Вища шк. Головное изд-во, 1987. 375 с.

108. Рудницкий В. Н. Теоретические основы синтеза высоконадежных отказоустойчивых дискретных устройств. *Збірник наукових праць ЦНДІ ЗС України*. 2005. № 3 (33). С. 192–198.

109. Киносита К., Асада К., Карацу О. Логическое проектирование СБИС /под ред. Л. В. Поспелова. Москва: Мир, 1988. 309 с.

110. Деклараційний патент на корисну модель 45917 Україна, МПК H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907998; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

111. Деклараційний патент на корисну модель 46617 Україна, МПК H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення

/ Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

112. Деклараційний патент на корисну модель 46618 Україна, МПК H03M 13/00. Пристрій для виконання логічних операцій криптографічного перетворення / Рудницький В.М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908001; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

113. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. Москва: Горяч. Линия-Телеком, 2005. 229 с.

114. Рудницький В. М., Лада Н. В., Козловська С. Г. Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання. *Сучасні інформаційні системи.* Харків: НТУ «ХПІ», 2018. Т. 2, № 4. С. 26–30.

115. Лада Н. В., Козловська С. Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. *Системи управління, навігації та зв'язку*: зб. наук. праць. Полтава: ПНТУ, 2018. Т. 1 (47). С. 127–130.

ДОДАТОК А

Список публікацій здобувача за темою дисертації

1. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків: ХУПС ім. І. Кожедуба, 2015. С. 129–134.

2. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Аналіз дворозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту. *Наукові праці:* наук.-метод. журн. Чорномор. держ. ун-ту ім. Петра Могили. Миколаїв, 2017.

3. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник інженерної академії України:* часопис. Київ, 2016. Вип. 3. С. 105–108.

4. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. Вип. 1. С. 5–10.

5. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Побудова примітивів строгого стійкого кодування мінімальної складності. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2018. Вип. 1. С. 21–26.

6. Рудницький В. М., Лада Н. В., Федотова-Півень І. М., Пустовіт М. О., Нестеренко О. Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Системи управління, навігації та зв'язку:* зб. наук. праць ПНТУ ім. Юрія Кондратюка. 2018. Вип. 6 (52). С. 113–115.

7. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики*. Харків, 2014. Вип. 168. С. 53–58.

8. Нестеренко О. Б. Исследование двухразрядных операций, удовлетворяющих критерию строгого стойкого кодирования, при многораундовом криптографическом преобразовании. *Wschodnioeuropejskie Czasopismo Naukowe* (East European sci. journal). 2018. No. 11 (39), part 2. С. 20–28. (Варшава, Польща).

9. Криптографічне кодування: обробка та захист інформації: кол. монографія / під ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

10. Бабенко В. Г., Нестеренко О. Б., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації*: тези доп. Другої міжнар. наук.-техн. конф. (Черкаси – Тольятті, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

11. Зажома В. М., Нестеренко О. Б. Генерація псевдовипадкових послідовностей на основі фільтрації матричних операцій криптоперетворення. *Проблеми інформатизації:* тези доп. Третьої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2015. 84 с.

12. Зажома В. М., Нестеренко О. Б. Вдосконалений метод вбудовування стегоповідомлення на основі ключового елементу. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої міжнар. наук.-техн. конф. (Полтава – Баку – Кіровоград – Харків). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2015. 72 с.

13. Шувалова Л. А., Нестеренко О. Б. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування. *Проблеми інформатизації*: тези доп. Четвертої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. С. 97.

14. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування . *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-

техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

15. Пустовіт М. О., Нестеренко О. Б., Матяш П. В. Моделювання розпилених водяних струменів для комп'ютеризованих симуляторів з гасіння пожеж в будівлях. Техника и технология. *Актуальные научные проблемы. Рассмотрение, решение, практика.* Гданьск, 2015. С. 22.

16. Пустовіт М. О., Нестеренко О. Б., Жаврук П. С. Комп'ютерне моделювання розпорошених водяних струменів для симулятора припинення горіння. *Надзвичайні ситуації: безпека та захист:* матеріали всеукр. наук.-практ. конф. з міжнар. участю. Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2015. С. 311–314.

17. Нестеренко О. Б. Двораундове криптографічне кодування операціями зі строгим лавинним ефектом. *Проблеми та перспективи цивільного захисту:* матеріали міжнар. наук.-практ. конф. молодих учених (29–30 берез. 2017 р.). Харків: НУЦЗУ. С. 384.

18. Нестеренко О. Б. Вдосконалення систем моніторингу з надзвичайних ситуацій. *Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика).* Харків, 2014. С. 55.

Відомості про апробацію результатів дисертації

1. Бабенко В. Г., Нестеренко О. Б., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації*: тези доп. Другої міжнар. наук.-техн. конф. (Черкаси – Тольятті, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10. – очна участь.

2. Зажома В. М., Нестеренко О. Б. Генерація псевдовипадкових послідовностей на основі фільтрації матричних операцій криптоперетворення. *Проблеми інформатизації:* тези доп. Третьої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2015. 84 с. – очна участь.

3. Зажома В. М., Нестеренко О. Б. Вдосконалений метод вбудовування стегоповідомлення на основі ключового елементу. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої міжнар. наук.-техн. конф. (Полтава – Баку – Кіровоград – Харків). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2015. 72 с. – заочна участь.

4. Шувалова Л. А., Нестеренко О. Б. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування. *Проблеми інформатизації*: тези доп. Четвертої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. С. 97. – очна участь.

5. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування . *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10. – очна участь.

6. Пустовіт М. О., Нестеренко О. Б., Матяш П. В. Моделювання розпилених водяних струменів для комп'ютеризованих симуляторів з гасіння пожеж в

будівлях. Техника и технология. *Актуальные научные проблемы. Рассмотрение, решение, практика.* Гданьск, 2015. С. 22. – заочна участь.

7. Пустовіт М. О., Нестеренко О. Б., Жаврук П. С. Комп'ютерне моделювання розпорошених водяних струменів для симулятора припинення горіння. *Надзвичайні ситуації: безпека та захист:* матеріали всеукр. наук.-практ. конф. з міжнар. участю. Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2015. С. 311–314. – очна участь.

8. Нестеренко О. Б. Двораундове криптографічне кодування операціями зі строгим лавинним ефектом. *Проблеми та перспективи цивільного захисту:* матеріали міжнар. наук.-практ. конф. молодих учених (29–30 берез. 2017 р.). Харків: НУЦЗУ. С. 384. – очна участь.

9. Нестеренко О. Б. Вдосконалення систем моніторингу з надзвичайних ситуацій. *Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика).* Харків, 2014. С. 55. – заочна участь.

«ЗАТВЕРДЖУЮ»
Ректор Черкаського
державного технологічного
університету

_____ О.О. Григор
«___» _____ 2017р.

АКТ
впровадження результатів дисертаційної роботи
Нестеренко Оксани Борисівни в навчальний процес
Черкаського державного технологічного університету

Комісія у складі: завідувача кафедри інформаційних технологій проектування д.т.н., доцента Прокопенко Т.О., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Федотової-Півень І.М., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Миронець І.В., розглянувши матеріали дисертаційного дослідження Нестеренко Оксани Борисівни, встановила наступне:

1. При підготовці бакалаврів за напрямом 6.170103 «Управління інформаційною безпекою» в курсі лекцій з дисциплін «Основи криптографічного захисту інформації» та «Криптографічні методи та засоби захисту інформації» використовуються результати дисертаційного дослідження, а саме:
   - метод синтезу операцій криптографічного перетворення інформації, які забезпечують максимальну невизначеність результатів шифрування;
   - метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності.
2. При виконанні курсових і кваліфікаційних робіт використовуються запропоновані методики синтезу прямих та обернених операцій розширеного матричного криптографічного перетворення.

Завідувач кафедри ІТП, д.т.н., доц. _____ Т.О. Прокопенко

Доцент кафедри ІБ та КІ, к.т.н., доц. _____ І.М.Федотова-Півень

Доцент кафедри ІБ та КІ, к.т.н., доц. _____ І.В. Миронець

ПРИВАТНЕ ПІДПРИЄМСТВО
"СЕНСОРНА ЕЛЕКТРОНІКА"

18029, Черкаси, вул. Олени Теліги, 7/69, тел.: (0472)66-26-97, Код ЄДРПОУ 33752446

від 18.09.2018 р. № 27/01

АКТ ВПРОВАДЖЕННЯ

дисертаційної роботи Нестеренко Оксани Володимирівна на тему «Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування»

Приватне підприємство «Сенсорна електроніка» займається розробкою та виробництвом елементів сенсорної та інших типів електроніки та систем на їх основі: датчиків різних фізичних величин, елементів та вузлів вимірювальної техніки, систем охорони, систем захисту інформації тощо.

Засоби синтезу операцій потокового шифрування, про які зазначається в дисертаційній роботі Нестеренко О.В., представляють для нашого підприємства значний інтерес, оскільки через їх значні переваги над аналогами вони будуть конкурентоспроможні на ринках електронної техніки в частині пристроїв захисту інформації.

Зокрема, інтерес представляє впровадження у вироби розробляємої техніки такі результати, отримані Нестеренко О.В.:

- метод синтезу операцій за критерієм строгого стійкого кодування, шляхом використання таблиць мінімальних відстаней по Хеммінгу;
- метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності, на основі використання операцій перестановки і гамування;
- методи синтезу програмно-апаратних засобів комп'ютерної криптографії на основі додаткового використання нової групи операцій синтезованих за критерієм строгого стійкого кодування.

Підприємство «Сенсорна електроніка» зацікавлене у провадженні результатів дисертаційного дослідження Нестеренко О.В., оскільки це призводить до підвищення невизначеності результатів потокового шифрування. Обсяги виробництва та терміни реалізації будуть визначені після завершення маркетингових досліджень.

Директор
ПП «Сенсорна електроніка» М. П. Мусієнко

ПРИВАТНЕ ПІДПРИЄМСТВО Сенсорна електроніка 33752446 УКРАЇНА м. ЧЕРКАСИ