НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«До захисту допущено»
В.о. завідувача кафедри
_____ Михайло САВЧУК
«__» _____ 2021 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика
на тему: **«Матричні співвідношення для параметрів, що характеризують стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу»**

Виконав: студент 4 курсу, групи ФІ-74
Шляхова Інна Олексіївна

Керівник: д.т.н.,проф.каф.ММЗІ Олексійчук А.М. _____

Консультант: _ _____

Рецензент: к.т.н., доц.кафедри ІБ Конюшок С.М. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2021

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність (освітня програма) — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Михайло САВЧУК
«__» _____ 2021 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Шляхова Інна Олексіївна

1. Тема роботи: «*Матричні співвідношення для параметрів, що характеризують стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу*»,

керівник: д.т.н.,проф.каф.ММЗІ Олексійчук А.М.,

затверджені наказом по університету №__ від «__» _____ 2021р.

2. Термін подання студентом роботи: 4 червня 2021р.

3. Вихідні дані до роботи: опубліковані джерела за тематикою дослідження.

4. Зміст роботи: під час дослідження було проведено огляд опублікованих джерел за тематикою дослідження; досліджено матричні співвідношення для параметрів, що характеризують стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу; з'ясові причини відсутності оцінок стійкості ітераційних блокових шифрів відносно дирефенціально-лінійних атак.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація доповіді.

6. Дата видачі завдання: 10 вересня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2020 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2020 р.	Виконано
3	Огляд диференціальних, лінійних та диференціально-лінійних атак	Листопад-грудень 2020 р.	Виконано
4	Дослідження та аналіз матричних співвідношенн для параметрів, що характеризують стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу	Січень-березень 2021 р.	Виконано
5	З'ясування причин відсутності оцінок стійкості блокових шифрів відносно диференціально-лінійних атак	Березень-травень 2021 р.	Виконано
6	Формулювання результатів дослідження	Травень-червень 2021 р.	Виконано

Студент _____ Шляхова І.О.

Керівник _____ Олексійчук А.М.

РЕФЕРАТ

Кваліфікаційна робота містить: 46 стор., 3 рисунки, 2 таблиці та 21 джерело.

Метою даної роботи є з'ясування причин, через які задача визначення стійкості ітеративних блокових шифрів відносно диференціально-лінійного криптоаналізу не розв'язана. Об'єктом дослідження є процеси перетворення інформації у ітеративних блокових шифрах, а предметод дослідження — методи оцінювання та обгрунтування стійкості ітеративних блокових шифрів до диференціально-лінійних методів криптоаналізу.

Наразі питання стійкості ітеративних блокових шифрів є важливим чинником під час побудови шифру, адже шифротекст повинен бути достатньо складним, аби протистояти атакам криптоаналітика, але не надто важким в обчисленнях.

У ході роботи були досліджені матриці, у позначеннях диференціально-лінійного криптоаналізу, за допомогою яких визначається стійкість ітеративних блокових шифрів до атак різного роду, а саме: лінійної, диференціальної та диференціально-лінійної атаки. Були досліджені певні взаємозв'язки та властивості матриць, які є причиною складності обгрунтування стійкості ітеративних блокових шифрів до диференціально-лінійних методів криптоаналізу.

БЛОКОВІ ШИФРИ, ДИФЕРЕНЦІАЛЬНО-ЛІНІЙНИЙ КРИПТОАНАЛІЗ, МАТРИЧНІ СПІВВІДНОШЕННЯ, СТІЙКІСТЬ

ABSTRACT

Qualification work contains: 46 pages, 3 figures, 2 tables and 21 sources.

The purpose of this work is to find out the reasons why the problem of determining the stability of iterative block ciphers with respect to differential-linear cryptanalysis is not solved. The object of research is the processes of information transformation in iterative block ciphers, and the research method — methods of assessing and justifying the stability of iterative block ciphers to differential-linear methods of cryptanalysis.

Currently,the issue of the iterative block ciphers stability is an important factor in building a cipher, because ciphertext must be complex enough to withstand the attacks of a cryptanalyst, but not too difficult to calculate.

In the course of the work, the matrices were studied, in the notation of differential-linear cryptanalysis, which determines the resistance of iterative block ciphers to attacks of various kinds, namely: linear, differential and differential-linear attacks. Certain relationships and properties of matrices, which are the reason of substantiation complexity of an iterative block ciphers stability against differential-linear methods of cryptanalysis, were studied.

BLOCK CIPHER, DIFFERENTIAL-LINEAR CRYPTOANALYSIS, MATRIX RELATIONS, STABILITY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$\oplus$ — операція побітового додавання

ВТ — відкритий текст

ШТ — шифрований текст

DES — (Data Encryption Standard) алгоритм блокового симетричного шифрування на основі мережі Фейстеля, створений у 1977 році.

AES — (Advanced Encryption Standard) алгоритм блокового симетричного шифрування на основі SP-мережі, розроблений у 1998 році.

ISO — (International Organization for Standardization) міжнародна організація зі стандартизації.

ВСТУП

Актуальність дослідження. Інформація займає чи не найбільшу нішу у нашому сучасному житті: література, соціальні мережі, державні документи тощо. Однак, якщо раніше люди, щоб відправити комусь повідомлення, прямували до пошти — то зараз ми маємо безліч месенджерів, електронних скриньок, соціальних мереж та інше. Із технічним розвитком великий спектр інформації перейшов у електронний формат (банківські перекази, книги, статті, особисті повідомлення, секретні документації, електронні документи). Але не вся інформація має право бути у загальному доступі, а отже її необхідно захищати від посторонніх людей і зловмисників.

Нині важливим напрямком у розвитку науки є забезпечення інформаційної безпеки. Саме цим питанням займається симетрична та асиметрична криптографія. Серед методів симетричної криптографії виділяють блокові шифри, які почали свій розвиток у 1949 році та продовжують розвиватися, не втрачаючи своєї актуальності. Поряд з процесом росту методів криптографії з'являються й методи криптоаналізу, які направлені на дешифрування повідомлень і розсекречення інформації та визначення стійкості шифрів відносно атак різного роду. Одним з таких методів є диференціально-лінійний криптографічний аналіз, який поєднує в собі диференціальну та лінійну атаки. Цей метод новий та недостатньо дослідженний. У даній роботі розглянута стійкість ітеративних блокових шифрів відносно диференціально-лінійних методів критографічного аналізу та проблеми, які з цим пов'язані.

Метою дослідження є з'ясування причин, через які досі задача визначення стійкості ітеративних блокових шифрів до диференціально-лінійного криптоаналізу не була розв'язана. Для досягнення мети необхідно розв'язати **задачу дослідження**, яка

полягає у дослідженні стійкості ітеративних блокових шифрів відносно диференціально-лінійних атак. Для розв'язання задачі необхідно вирішити такі **завдання дослідження**:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) дослідити матричні співвідношення для параметрів, що характеризують стійкість блокових шифрів відносно диференціально-лінійного методу криптоаналізу;

3) з'ясувати причин відсутності оцінок стійкості ітераційних блокових шифрів відносно дирефенціально-лінійних атак.

Об'єктом дослідження є процеси перетворення інформації в ітеративних блокових шифрах.

Предметом дослідження є методи оцінювання та обґрунтування стійкості ітеративних блочних шифрів до диференцільно-лінійних методів криптоаналізу.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної алгебри, методи лінійного та диференціального криптоаналізу, методи диференціально-лінійного криптоаналізу.

Наукова новизна отриманих результатів полягає у тому, що з'ясувати причин відсутності аналізу стійкості ітеративних блокових шифрів відносно диференціально-лінійного метода криптоаналізу не було проведено раніше.

Практичне значення результатів полягає у тому, що встановлені причини та труднощі, пов'язані з отриманням оцінок стійкості ітераційних блокових шифрів відносно дирефенціально-лінійних атак, схиляють до того, що існуючі методи не є ефективними для оцінування, і потрібно розглядати інші підходи для визначення стійкості шифрів.

1 ОГЛЯД ТЕОРЕТИЧНИХ МАТЕРІАЛІВ ЗА ЗАДАНОЮ ТЕМОЮ ДОСЛІДЖЕННЯ

У цьому розділі були визначені основні поняття та принципи побудови блокових шифрів, була детально розглянута SP-мережа з прикладом шифрування та мережа Фейстеля. Коротко описані міжнародні стандарти блокового шифрування за версією ISO.

1.1 Блокові шифри та принципи їхньої побудови

Блокові шифри — різновид симетричних шифрів, який оперує набіром блоків із n-кількістю біт із ВТ, тобто вони оброблюють дані блоками фіксованої довжини. Для всіх блоків шифрів використовується певний алгоритм шифрування, однак для кожного блоку виділяється свій ключ. На сьогоднішній день багато сучасних криптографічних алгоритмів базуються саме на блокових шифрах: DES, AES тощо.

Необхідно зазначити, що всі повідомлення, шифротексти та ключі — бітові рядки.

Означення 1.1. Блоковий шифр — це перетворення виду

$$E_k : V_n \times K \to V_n, \tag{1.1}$$

де V_n — n-бітові рядки, які ми трактуємо як вхідні повідомлення (ВТ), K — множина ключів (зазвичай це множина бітових рядків іншої довжини), V_n — множина всіх ШТ.

Принципи побудови та властивості блокового шифрування:

– відображення E_k має бути бієктивним для всіх $k \in K \Rightarrow \forall k : D_k \equiv E_k^{-1}$, де D_k — повідомлення (ВТ);

– ключі мають бути оптимальної довжини: достатньо короткі, щоб

ними було зручно користуватися, але достатньо довгими, щоб не постраждала стійкість;

– принципи Шеннона, такі як розсіювання та перемішування повинні виконуватись;

– шифри повинні відповідати криптографічним властивостям стійкості (наприклад, нелінійність, кореляційний імунітет, лавинні ефекти тощо);

– шифрування виконується ітеративно, на рисунку 1.1 наведена загальна схема шифрування, де $(k_1,\ k_2,\ \ldots\ ,\ k_r) = KS(k)$ — результат ключового розкладу, F — раундове шифруюче перетворення,

$$Y = E_k(x) = F_{k_r}(F_{k_{r-1}}(...F_{k_1}(x)...)); \tag{1.2}$$

– перетворення має бути оберненим самому до себе (інволютивним), це означає, що:

$$\forall x : \varphi(\varphi(x)) = x; \tag{1.3}$$

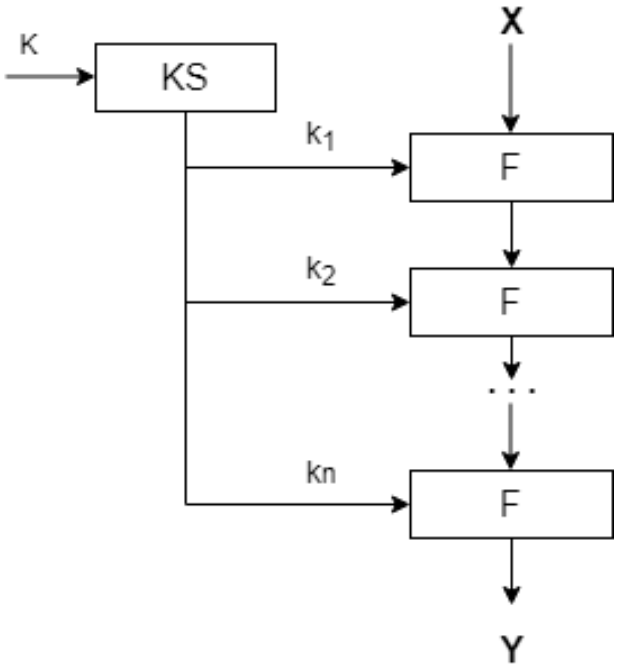

Рисунок 1.1 – Загальна схема ітеративного бловокого шифру.

Шифрування виконується наступним чином. Нехай K буде випадковим двійковим ключем деякої заданої довжини. K використовується для побудови N *раундових ключів*, які в свою чергу позначаються як K^1, K^2, ..., K^N. Набір раундових ключів (K^1, K^2, ..., K^N) — це ключовий розклад, який побудований з K шляхом певних фіксованих, загальноприйнятих алгоритмів.

Раундова функція, назвемо її f, приймає на вхід два параметри: раундовий ключ K^r та поточний стан, який ми назвемо w^{r-1}. Наступний стан буде визначатись таким чином: $w^r = f(w^{r-1}, K^r)$. Початковим станом w^0 буде ВТ, який подається на вхід, x. ШТ y отримується шляхом ітераційних перетворень ВТ x після N раундів шифру. Отже, порядок шифрування відбувається наступним чином:

$$x \to w^0$$
$$f(w^0, K^1) \to w^1$$
$$f(w^1, K^2) \to w^2$$
$$\dots$$
$$f(w^{N-1}, K^N) \to w^N$$
$$w^N \to y$$

Для того, щоб можна було розшифрувати, функція f має бути ін'єктивною, тобто: $\forall w, y : f^{-1}(f(w, y), y) = w$. А отже, розшифрування буде виконуватись наступним чином:

$$y \to w^N$$
$$f^{-1}(w^N, K^N) \to w^{N-1}$$
$$\dots$$
$$f^{-1}(w^2, K^2) \to w^1$$
$$f^{-1}(w^1, K^1) \to w^0$$
$$w^0 \to x$$

1.2 SP-мережа

SP-мережа (або *Substitution–Permutation Network*, SPN) — це клас блокових шифрів, що складаються з раундів, у яких повторюються серії математичних операцій. Основою агоритму AES є SP-мережа. Раунди шифрування мають структуру зображену на рисунку 1.2, кожен з яких складається з трьох етапів: додавання ключа, нелінійна заміна бітів та лінійна перестановка бітів. Розшифрування виконується у зворотньому напрямку.

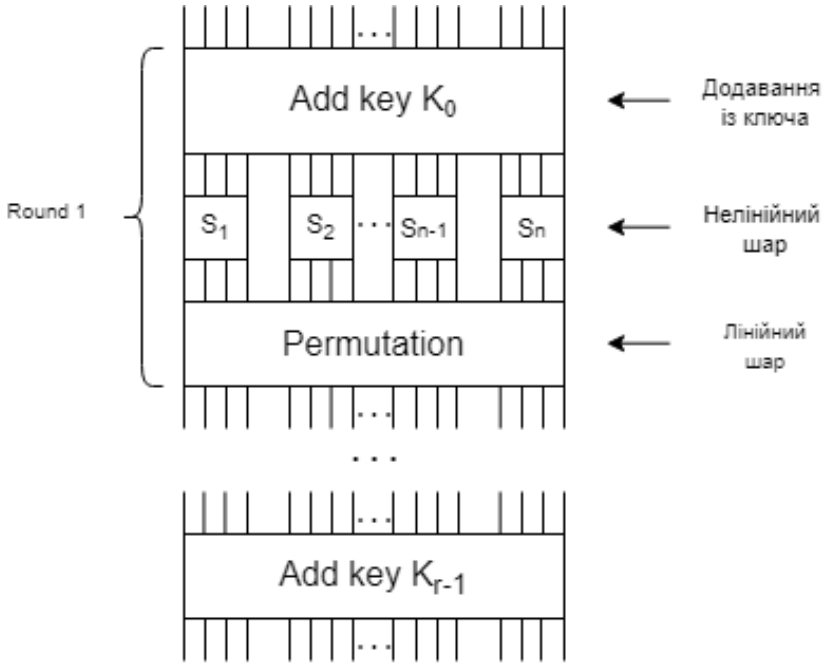

Рисунок 1.2 – Загальна схема шифрування SP-мережі.

Розглянемо детальніше принцип роботи SP-мережі. Нехай l та m є цілими натуральними числами. ВТ та ШТ будуть двійковими векторами довжини lm (тобто, lm довжина блоку шифру). SP-мережа складається з двох компонентів, які ми будемо позначати як π_s π_p:

$$\pi_s : \{0,1\}^l \to \{0,1\}^l,$$

що є перестановкою 2^l бітових рядків довжини l та

$$\pi_p : \{0,\ldots,lm\} \to \{0,\ldots,lm\},$$

що являє собою також перестановку цілих чисел від 1 до lm.

Перестановка π_s називається *S-блоком*. Використовується *для заміни* l бітів на інший набір бітів довжини l, в той час як π_p використовується для *перестановки* lm бітів, змінюючи їх порядок. Розглядаючи lm-бітний двійковий рядок, скажімо $x = (x_1, x_2, \ldots, x_{lm})$, ми можемо розцінювати x як конкатенацію з m l-бітних підрядків, які позначимо $x_{<1>}, x_{<2>}, \ldots, x_{<m>}$. Таким чином,

$$x = x_{<1>} \parallel x_{<2>} \parallel \cdots \parallel x_{<m>}, \text{ де}$$

$$x_{<i>} = (x_{(i-1)l+1}, x_{(i-1)l+2}, \ldots, x_{il}),\ i = \overline{1, m}$$

SP-мережа складається з N раундів, в кожному з яких (окрім останього) виконується m замін, використовуючи π_s, після чого йде перестановка π_p. Перед кожною операцією заміни буде відбуватися додавання раундового ключа. Зазвичай, це проста операція XOR. Розглянемо алгоритм шифрування SP-мережі. На вході ми маємо ВТ x, на виході маємо отримати ШТ y.

Алгоритм 1.1. [5]

Вхід: x, π_s, π_p, (K^1, K^2, ..., K^{N+1}).

1. Визначаємо наш ВТ x як w^0 ($x \to w^0$).
2. Для r від 1 до $N-1$ виконуємо:
   2.1. $w^{r-1} \oplus K^r \to u^r$.
   2.2. Для i від 1 до m виконуємо:

2.2.1 $\pi_s(u^r_{<i>}) \to v^r_{<i>}$.

   2.3 $(v^r_{\pi_p(1)}, v^r_{\pi_p(2)}, \ldots, v^r_{\pi_p(lm)}) \to w^r$.

3. $w^{N-1} \oplus K^N \to u^N$.
4. Для i від 1 до m виконуємо:
   4.1 $\pi_s(u^N_{<i>}) \to v^N_{<i>}$.
5. $v^N \oplus K^{N+1} \to y$.

Вихід: y.

У Алгоритмі 1.1 u^r — вхідні данні для *S-блоку*, а v^r — вихідні данні з нього на раунді r. w^r отримуємо з v^r шляхом застосування перестановки π_p, після чого u^{r+1} рахуємо XORом w^r та раундового ключа K^{r+1}. В останьому раунді перестановка π_p не застосовується. Таким чином, алгоритм шифрування можна використовувати як алгоритм для розшиврування ШТ, якщо змінити порядок раундових ключів та *S-блоки* замінити оберненими.

Варто також звернути увагу, що першою та останньою операцією в SP-мережі є додавання ключа, що називається «відбілюванням», і це розглядається як корисний спосіб запобігти тому, щоб зловмисник почав виконувати операції шифрування або дешифрування, якщо ключ йому невідомий.

Розглянемо невеликий приклад роботи конкретної SP-мережі.

Приклад 1.1. Нехай $l = m = 4$, $N = 2$, а π_s визначаються наступним чином, де вхідні дані x записуються в шістнадцядковій системі обчислення:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_s(x)$	7	3	E	1	A	8	0	F	6	B	2	D	9	4	5	C

таким самим чином визначаємо аблицю для пестановки π_p:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_p(x)$	2	6	12	13	1	8	10	14	3	7	9	16	4	5	11	15

Для того, щоб завершити опис SP-мережі, необхідно задати алгоритм побудови раундових ключів. Наприклад, починаємо з 24-бітного ключа:

$$K = (k_1, k_2, \ldots, k_{24}) \in \{0,1\}^{24}$$

Для $1 \leqslant r \leqslant 3$ визначаємо K^r таким чином, щоб від складався з 16

послідовних біт з , починаючи з k_{4r-3}. Всі дані представлені у двійковому записі. Нехай,

$$K = 0101\ 0010\ 1101\ 1111\ 0110\ 1011$$

таким чином ми отримуємо наступні раундові ключі:

$$k_1 = 0101\ 0010\ 1101\ 1111$$

$$k_2 = 0010\ 1101\ 1111\ 0110$$

$$k_3 = 1101\ 1111\ 0110\ 1011$$

а відкритий текст буде мати наступний вигляд:

$$x = 0011\ 0100\ 1110\ 0101$$

Наступні кроки будуть виконуватись за Алгоритмом 1.1 та визначеними функціями π_s та π_p. В результаті отримуємо:

$$w^0 = 0011\ 0100\ 1110\ 0101$$

$$K^1 = 0101\ 0010\ 1101\ 1111$$

$$u^1 = 0110\ 0110\ 0011\ 1010$$

$$v^1 = 0000\ 0000\ 0001\ 0010$$

$$w^1 = 0000\ 0000\ 0010\ 0001$$

$$K^2 = 0010\ 1101\ 1111\ 0110$$

$$u^2 = 0010\ 1101\ 1101\ 0111$$

$$v^2 = 1110\ 0100\ 0100\ 1111$$

$$K^3 = 1101\ 1111\ 0110\ 1011$$

$$y = 0011\ 1011\ 0010\ 0100$$

SP-мережі мають кілька привабливих особливостей. По-перше, дизайн простий і дуже ефективний як в апаратному, так і в програмному забезпеченні. У програмному забезпеченні зазвичай *S-блоки* реалізуються у вигляді пошукової таблиці.

SP-мережа у Прикладі 1.1 не є безпечною, якщо з будь-якої іншої причини, крім довжини ключа (32 біти), яка є достатньо малою, був можливий вичерпний пошук ключа. Але можуть бути розроблені SP-мережі з більшою кількістю раундів, зі складнішими функціями та довшим ключем, які б мали більшу стійкість до різних атак.

1.3 Схема Фейстеля

Схема Фейстеля, або шифр Фейстеля, названа на честь Хорста Фейстеля, який її розвобир під час роботи в IBM [1]. Він та його колега Дон Копперсміт опублікували шифр під назвою Люцифер у 1973 році, що було першим публічним прикладом шифру, що використовує структуру Фейстеля. Пізніше, на основі шифру Люцифер був розроблений шифр DES, який був визнаний як національний стандарт шифрування у 1977 році. Раундове шифрування схеми Фейстеля зображене на рисунку 1.3.

У схемі Фейстеля кожен стан u^i розділений на дві частини рівної довжини: L^i та R^i (похідні від left та right). Раундова функція має наступний вигляд: $f(L^{i-1}, R^{i-1}, K^i)$, де

$$L^i = R^{i-1}$$
$$R^i = L^{i-1} \oplus f(R^i - 1, K^i)$$

Тобто, на вході в алгоритм шифрування ВТ x ділиться на дві частини однакової довжини. Раундова функція f, яка залежить від раундового ключа K^i, застосовується для однієї половини вхідного тексту, потім за допомогою операції XOR додається до другої половини. Після цього блоки тексту міняються місцями. У останньому раунді шифрування зміна місцями половин зашиврованого повідомлення відбувається двічі.

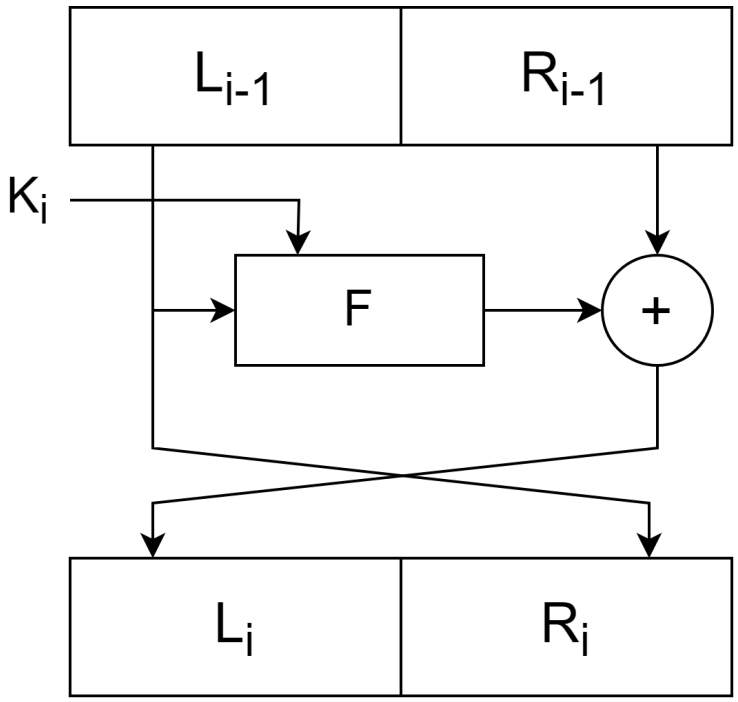

Рисунок 1.3 – Схема раундового шифрування у шифрі Фейстеля.

Мережа Фестеля має наступні властивості. Те, що у одному раунді шифрується лише половина повідомлення, є гарною властивістю, адже реалізація функції від $n/2$ бітів є кращою та ефективнішою, ніж функція від n бітів, де n — довжина повідомлення. Як і у SP-мережі, схема Фейстеля є інволютивною: процедура розшифрування відрізняється від процедури шифрування лише порядком раундових ключів.

1.4 Міжнародні стандарти блокових шифрів

Стандарти вкрай необхідні в сучасном житті, щоб забезпечувати бажані характеристики виробів чи послуг, такі як якість, безпеку, надійність, ефективність та інше. Якщо вироби, частини машини й прилади працюють добре, і безпечно, то це часто відбувається тому, що вони задовольняють вимогам стандартів. І організацією, відповідальною за багато тисяч стандартів, що приносять користь всьому світу, є ISO (*International Organization for Standardization*).

Міжнародна організація зі стандартизації (ISO) — це найбільший у світі розробник і видавець міжнародних стандартів. В даний час у світі діє близько 2000 різних стандартів, випущених Міжнародною організацією стандартизації, які застосовуються як у вузькоспеціалізованих областях, так і в міжнаціональному масштабі. Зокрема, вищезгадана система ISO/IEC 18033-3 використовується в якості стандартів блочних шифрів, які були визначені у 2005 році, переглядались у 2020, і станом на 2021 рік є актуальними[11]. Серед цих шифрів є:

– 64-бітові блочні шифри: TDEA, MISTY1, CAST-128, HIGHT;

– 128-бітові блочні шифри: AES, Camellia, SEED.

TDEA. Цей блоковий шифр був розроблений Уітфілдом Діффі, Мартіном Хеллманом та Уолтом Тачманном у 1987 році на основі алгоритму DES. Даний шифр побудований за схемою Фейстеля. TDEA також ще називають Triple DES, 3DES або TDES. Швидкість його роботи втричі нижча, ніж швидкість DES, але усувається головний недолік — коротка довжина ключа, через який шляхом повного перебору можна дешифрувати повідомлення. Шифрування TDEA виконується за схемою Фейстеля на трьох ключах, кожен з яких довжиною в 56 бітів, які можуть бути незалежні між собою, співпадати або серез них буде лише одна пара однакових ключів. Варіант, коли три ключа не мають співпадінь між собою є найбільш надійним. На кожному ключі виконується по 16 раундів.

MISTY1. Даний блоковий шифр розробив Міцуру Міцуї з командою спеціалістів для компанії Mitsubishi Electric у 1995 році. Розшифровується як Mitsubishi Improved Security Technology. Шифрування відбувається за схемою Фейстеля, де довжина ключа складає 128 біт, а довжина блоку — 64 біт. Кількість раундів может бути будь-якою, але має бути кратною чотирьом, хоча рекомендується використовувати 8 раундів шифрування. MISTY1 був одним з обраних алгоритмів, які шифрують 64-бітні блоки, у европейському проекті NESSIE.

CAST-128. Алгоритм був створений Карлайлом Адамсом та Стаффордом Таваресом у 1996 році. Даний шифр складається з 12 або 16 раундів шифрування на основі мережі Фейстеля. Розмір блоку становить 64 біт, а довжина ключа может бути від 40 до 128 біт, але має бути кратною 8. Якщо довжина ключа перевищує 80 біт, використовують 16 раундів шифрування. Є три різні типи раундових функцій, які схожі між собою, але відрізняються застосовуваними операціями: додавання, віднімання або XOR. Використовується у багатьох продуктах, зокрема, за замовчуванням як шифр у деяких версіях GPG і PGP. Він також був схвалений для використання урядом Канади.

HIGHT. Розроблений південнокорейськими криптографами у 2006 році. Довжина ключа дорвнює 128 біт, а довжина блоку 64. Реалізація даного алгоритму не потребує великих апаратних ресурсів, щоб його було легко застосовувати у обчислювальних приладах, таких як датчик в USN або RFID-мітка. HIGHT має 32-раундову ітераційну структуру, яка є варіантом узагальненої мережі Фейстеля. Визначною особливістю цього шифру є те, що він складається з простих операцій, таких як XOR, додавання за модулем 2^8 і циклічний зсув вліво.

AES. Цей блоковий шифр був запропонований бельгійськими криптографами Вінсентом Рейменом та Джоаном Даменом на конкурсі NIST на заміну шифру DES і став переможцем. AES (Advanced Encryption Standard) також відомий під назвою Rijndael. Розмір блоку дорівнює 128 біт, а довжина ключа може бути 128, 192 або 256 біт. В залежності від довжии ключа, кількість раундів буде 10, 12 або 14 відповідно. Працює на основі SP-мережі. На кожному раунді застосовуються такі операції: AddRoundKey (додавання раундового ключа), SubBytes (ненілійна заміна), ShiftRows (перестановка бітів у стані), MixColumns (лінійна заміна). У останьому раунді лінійна заміна не виконується. Даний алгоритм має ефективну реалізацію на різних архітектурах.

Camellia. Алгоритм був розроблений у 2000 році японськими компаніями Mitsubishi Electric та NTT для європейського конкурсу NESSIE та став фіналістом. Як структуру, використовує мережу Фейстеля з 18 або 24 раундами та довжиною блоку в 128 біт. Довжина ключа залежить від кільності раундів: 128 біт (для 18 раундів шифрування) та 192 або 256 біт (для 24 раундів). Раундова функція використовує нелінійне перетворення, блок лінійного розсіювання кожні 16 циклів (побайтова операція XOR) і байтову перестановку.

SEED. Даний шифр був створений Корейським агентством інформаційної безпеки (KISA) у 1998 році.Він широко використовується в промисловості Південної Кореї, але рідко зустрічається десь ще. Він набув популярності в Кореї, тому що 40-бітове шифрування не вважалося досить надійним, тому Корейське агентство інформаційної безпеки розробило свій власний стандарт. SEED є мережею Фейстеля з довжиною ключа в 128 біт та блоком розміром у 128-біт. Шифрування виконується за 16 раундів.

Висновки до розділу 1

Серед усього різноманіття алгоритмів та методів криптографічного захисту виділяються ітеративні блокові шифри, які будуються на основі SP-мережі або схеми Фейстеля. Їм характерний певний ряд позитивних властивостей: розшифрування не потребує окремої схеми чи процедури, тому що виконується у зворотньому напрмку від процедури зашифрування; алгоритми ітеративного блокового шифрування можуть бути реалізовані як на пристроях з певним обмеженням у ресурсах, так і на приладах, які цих обмежень не мають, що говорить про їх універсальність; не мають надскладної будови для реалізації; є 7 ітеративних блокових шифрів, що входять до списку міжнародних стандартів за версією ISO. Усі ці фактори вказують на ефективність та актуальність даного виду шифрування. Підсумовуючи вище написане,

можна зробити висновок, що розвиток та аналіз ітеративних блокових шифрів є важливим та перспективним.

2 ДИФЕРЕНЦІАЛЬНО-ЛІНІЙНИЙ КРИПТОАНАЛІЗ

У розділі 2 були розглянуті три види статистичних атак: диференціальна, лінійна та диференціально-лінійна. Були описані два алгоритма для диференціально-лінійних атак та досліджені результати стійкійкості певних ітеративних шифрів відносно даного виду атак.

2.1 Лінійний криптоаналіз

Лінійний криптоаналіз був розроблений японським криптографом Міцуру Мацуї для криптоаналізу шифру FEAL у 1992 році[13]. Після цього Мацуї опублікував атаку на тогочасний стандарт шифрування DES[14].

Лінійний криптоаналіз — особливий різновид атаки на симетричні шифри, спрямований на відновлення невідомого ключа шифрування, по відомим відкритим повідомленнями і відповідним їм шифротекстам. Ціль даного метода полягає у пошуку можливості заміни складної булевої функції, що описує нелінійне перетворення, на просту лінійну функцію. Якщо лінійні залежності вдається знайти, то за допомогою статистичних даних можна знайти деякі біти ключа.

Для проведення криптоаналізу необхідно знати структуру шифра, а також мати достатній набір статистичних даних, що складаються з пар (ШТ-ВТ), отриманих на одному й тому ж невідомому криптоаналітику ключі. В подальшому буде проводитись аналіз не початкого шифру, а його лінійне наближення, яке;

1) простіше вихідного шифру та легше піддається аналізу;

2) може виявитись вдалим та дозволить звести проблему криптоаналізу вихідного шифру до аналізу його модифікації — з деякою, нехай і досить великою, похибкою.

2.1.1 Лінійне наближення

Нехай $< x, y >= x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$ — скалярний добуток двійкових векторів за модулем 2.

Розглянемо дейкий алгоритм блочного шифрування з r раундами. Нехай, P — ВТ, C — ШТ, K — ключ.

Означення 2.1. Лінійним наближенням шифра називається:

$$L :< P, \alpha > \oplus < C, \beta >=< K, \gamma >, \tag{2.1}$$

яке виконується з ймовірністю $1/2 + \varepsilon$, де $\varepsilon \neq 0$. Величина ε називається **переважанням** лінійного співвідношення. Для вдалого криптоаналіза модуль переважанням має бути якомога більшим.

Вектори α, β, γ називаються **масками**. Маски нам дозволяють обрати с якими саме бітами з ШТ, ВТ та ключа ми будемо працювати. Для того, щоб виявити, з якими α, β, γ нам варто працювати, звичайний перебір комбінацій не підходить, адже доведеться перебирати на багато більше ніж ключів.

Лінійне наближення шукають за допомогою метода «від простого до складного»: аналізуючи окремі компоненти шифру, починаючи з S-блоку, і поетапно переходячи до наближення всього шифру.

2.1.2 Алгоритми лінійних атак

Для знахоження бітів ключа за відомими ВТ та ШТ є два алгоритма, які розробив Міцуру Мацуї [15].

Алгоритм 2.1. Визначення одного біта ключа.

1. Знайти лінійне наближення L для бітів ВТ, ШТ та ключа, що виконуються з ймовірністю $p = 1/2 + \varepsilon$, яка досить вильно відрізняється від $1/2$.

2. При невідомому фіксованому ключі K взяти N пар ВТ та відповідному їм ШТ. Враховуючи знак ε виконати розрізнення двох простих статистичних гіпотез: чи виконується співвідношення для даного невідомого ключа K чи ні. А саме:

2.1. Для кожної пари (P, C) статистики розрахувати значення лівою части співвідношення L. Нехай позначати відповідну кількість пар статистики будуть N_0 та N_1, для який ліва частина співвідношення буде дорівнювати 0 та 1 відповідно. Таким чином $N_0 + N_1 = N$.

2.2. Вважаємо, що

$$< K, \gamma >= \begin{cases} 0, & \text{якщо}(N_0 - N_1) \cdot \varepsilon > 0 \\ 1, & \text{в інших випадках} \end{cases}$$

2.2. Підбираємо секретний ключ відповідно до отриманого співвідношення.

Однак більшої популярності набув покращений алгоритм пошуку лінійної залежності, що дозволяє за допомогою лінійного наближення знаходити кілька бітів ключа.

Нехай C_i позначає проміжний ШТ, де $i = \overline{0, r}$, і виконуються співвідношення $C_0 = P, C_r = C$.

Алгоритм 2.2. Визначення кількох бітів ключа.

1. Визначаємо лінійне співвідношення L' для бітів проміжних ШТ C_1, C_{r-1} і ключа , який виконується з імовірністю $p = 1/2 + \varepsilon'$, яка досить сильно відрізняється від $1/2$. Число ε' називається **теоретичним переважанням** співвідношення L'.

Нехай співвідношення L' має вигляд

$$< a, C_1 > \oplus < b, C_{r-1} >=< d, K >$$

Ліва частина цього співвідношення залежить лише від бітів ШТ і не залежить від ключа.

2. При фіксованому невідомому ключі скласти статистику із N пар ВТ та ШТ. Нехай це будуть пари

$$(P^{(1)}, C^{(1)}),\ (P^{(2)}, C^{(2)}),\ \ldots,\ (P^{(N)}, C^{(N)})$$

3. Нехай K' буде позначати таку мінімальну частину ключа K, знаючи яку, можна знайти значення комбінації $< a, C_1 >$ по відомому ШТ C. Для того, щоб визначати, які біти ключа K мають міститися в K', достатньо проаналізувати перший раунд шифрування та ті біти ключа, від який істотно залежать біти ШТ C_1, що входять в комбінацію $< a, C_1 >$ з ненульовими коефіцієнтами. Аналогічно, нехай K'' — така мінімальна частину ключа K, знаючи яку, можна однозначно знайти значення лінійної комбінації $< b, C_{r-1} >$ за відомомим ШТ C.
Біти ключа, що входять в $K' \cup K''$, називаються **активними**.

4. Виконати перебір по всім можливим варіантам частини $K' \cup K''$. Для кожної фіксованої частини $K' \cup K''$ зробити наступні дії:

4.1. Для кожної пари $P^{(i)}, C^{(i)}$ з використанням частин ключа K', K'' розрахувати значення $< a, C_1 > \oplus < b, C_{r-1} >$. Нехай серед N пар рівно для N_0 пар це значення виявилось ріним нулю, для N_1 — рівним одиниці. $N_0 + N_1 = N$

4.2. Розрахувати **експериментальне переважання** (це величина $\widetilde{\varepsilon}$), що визначається рівністю $1/2 + \widetilde{\varepsilon} = N_0/N$.

5. Частини ключів $K' \cup K''$, для яких отримане експериментальне переважання, що достатньо сильно відрізняється від теоретичного переважання, вважається невірним. Частини ключа, що залишились, заносяться у масив. Як правило, для коректної роботи алгоритму вводять **припустиму похибка** δ, що визначає можливу різницю між переважаннями. Якщо $|\varepsilon' - \widetilde{\varepsilon}| \leqslant \delta$, то відмінність допустима, інакше частина ключа $K' \cup K''$ вважається невірною.

6. Для кожної допустимої частини ключа $K' \cup K''$ шляхом перебору відбудовують біти ключа K, що залишилися.

2.2 Диференціальний криптоаналіз

Відкриття диференціального криптоаналізу зазвичай приписують Елі Біхаму та Аді Шаміру, які опублікували ряд атак проти різних блокових шифрів та хеш-функцій, включаючи теоретичну слабкість в алгоритмі DES, у кінці 1980-х років[16].

Диференціальний криптоаналіз заснований на вивченні перетворення різниць між шифрованими значеннями на різних раундах шифрування. Це атака у відкритому тексті, яка спирається на ідею про те, що фіксована різниця вхідних даних, з великою ймовірністю, може генерувати певну різницю на виході. Під час шифрування пари ВТ із заданою побітовою різницею та спостерігаючи за тим, які ключові біти пропонуються вихідною різницею, можна визначити ключові біти. Даний вид криптоаналізу належить до статистичних атак. Експлуатація диференціальних атак довга, адже потребує велику кількість раундів. Розглянемо детальніше алгоритм диференційного криптоаналізу.

Алгоритм 2.3. Основна ідея.

1. Пара векторів $(\alpha, \beta)_i$ називається **і-м диференціалом шифра**, якщо пара ВТ, які відрізняються на векторα, після i раундів шифрування може перейти в пару ШТ, які відрізняються на вектор β. Імовірність і-го диференціала

$$P_{(\alpha,\beta)_i} = P\{\Delta C_i = \beta | \Delta P = \alpha\}$$

2. Обираємо найбільш ймовірний $(r-1)$-й диференціал (α, β).

3. При фіксованому невідомому ключі K складаємо статистику із N четвірок $\{P,\ P',\ C,\ C'\}$ таких, що $\Delta P = \alpha$.

4. Припускаємо, що $\Delta C_{r-1} = \beta$. Для трійки ΔC_{r-1}, C, C' знаходимо список можливих значень ключа K.

5. Ключ, який зустрічається в таких списках найбільш часто, можем вважати основним рішенням.

2.3 Загальний опис диференціально-лінійного криптоаналізу

Не дивлячись на те, що виключення довгих диференціалів та лінійних наближень здається достатнім для того, щоб зробити шифр стійким до диференціальних та лінійних атак, виявилося, що у багатьох випадках короткі характеристики та наближення також можуть бути використані для розбиття шифру. Прикладом даного криптоаналізу стала диференціально-лінійна атака.

Вперше цю атаку описали Ленгфорд та Хеллман у 1994 році. Принцип роботи її полягає у тому, що ШТ E розділяють на два підшифра E_0 та E_1 та об'єднують диференціальну характеристику для E_0 із лінійним приближенням для E_1 у атаку на весь шифр E. Працює наступним чином.

Припустимо, що ми маємо диференціал $\triangle_I \rightarrow_p \triangle_O$ для E_0 та лінійне наближення $\lambda_I \rightarrow_q \lambda_O$ для E_1. Для того, щоб відрізнити E від випадкової перестановки, супротивник розглядає пари відкритого тексту з різницею введення $\triangle_I$ та для кожної пари перевіряє, чи відповідають відповідні шифротексти щодо рівноправності маски λ_O.

Візьмемо різну пару ВТ та позначимо як P та P', пару ШТ як C та C', а проміжні значення E_0 та E_1 через X та X'. Під час атаки виконуються поєднуються такі наближення:

– значення $C \cdot \lambda_O$ та $C' \cdot \lambda_O$ співвідносяться з $X \cdot \lambda_I$ та $X' \cdot \lambda_I$ відповідно лінійним наближенням E_1;

– значення $X \cdot \lambda_I$ та $X' \cdot \lambda_I$ співвідносяться як наслідок диференціала для E_0.

Як наслідок, $C \cdot \lambda_O$ корелює з $C' \cdot \lambda_O$.

2.4 Побудова диференціально-лінійної атаки на блоковий шифр

Введемо необхідні позначення. Нехай $\sigma(V_n)$ буде симетричною групою підстановок на $V_n = \{0,1\}^n$, де n є натуральним числом. Для $\alpha = (\alpha_1, \ldots, \alpha_n)$ та $\beta_1, \ldots, \beta_n$, які належать множині V_n визначимо наступні операції:

$$\alpha\beta = \alpha_1\beta_1 \oplus \cdots \oplus \alpha_n\beta_n$$

$$\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \ldots, \alpha_n \oplus \beta_n)$$

2.4.1 Диференціально-лінійна атака спрямована на відновлення бітів ключа

Розглянемо блоковий шифр $\Im$ з множиною відкритих текстів $X = V_n$, множиною ключів $K = V_m$ та сім'єю шифрувальних перетворень $(F_k : k \in K)$. Вважається, що при проведенні атаки супротивник має доступ до оракула F_k з невідомим (вибраним випадково рівноймовірно з множини K) ключем k.

Алгоритм 2.4. Диференціально-лінійна атака на блоковий шифр.

1. Аналітик обирає ненульові вектори $\alpha, \beta, a \in V_n$.

2. Генерує незалежні в сукупності випадкові рівноймовірні ВТ $X_1, \ldots, X_t \in V_n$.

3. Обчислює для кожного ВТ пару ШТ $F_k(X_i)$, $F_k(X_i \oplus a)$, $i = \overline{1,t}$.

4. Відповідно для кожного ШТ обчислює значення $v_i = \alpha F_k(X_i) \oplus \beta F_k(X_i \oplus a)$, $i = \overline{1,t}$.

5. Відновити значення ключа $\psi(k)$ за послідовнісю $v_1, \ldots, v_t$, де $\psi : K \to \{0,1\}$.

Зауваження. Для того, щоб побудована атака була ефективною необхідно обирати вектори $\alpha, \beta, a \in V_n$ операцію $+$ та функцію ψ , виходячи з особливостей будови блокового шифру таким чином, аби випадкова послідовність $v_1, \ldots, v_t$ містила якомога більше інформації про значення секретного ключа.

Згідно з [7] можна визначати твердження відносно інформаційної складності даної атаки.

Твердження 2.1. *Найменший обсяг даних, необхідних для проведення на шифр* $\Im$ *диференціально-лінійної атаки (на основі векторів* $\alpha, \beta, a \in V_n$*, операції*$+$ *та функції* ψ*) з імовірністю помилки не більше ніж* $\sigma \in (0, 1/2)$*, задовольняє нерівності*

$$[21]t \geqslant \frac{(1-\sigma-h(\sigma))ln2}{|K|^{-1}\sum\limits_{k\in K}(2P_X\{\alpha F_k(X) = \beta F_k(X+a)\}-1)^2}\,, \tag{2.2}$$

де X – випадковий вектор з рівномірним розподілом ймовірностей на множині V_n, а $h(\sigma) = -\sigma log\sigma - (1-\sigma)log(1-\sigma)$.

2.4.2 Диференціально-лінійна розрізнювальна атака

Було розглянуто диференціально-лінійну атаку, яка має за мету відновлення невідомих бітів ключа на основі векторів $\alpha, \beta, a \in V_n$, операції $+$ та функції ψ. Існує й інша атака, а саме — розрізнювальна атака. Сенс її полягає у тому, щоб відрізнити шифр від випадкової підстановки на V_n за допомогою аналізу послідовності v_i ($v_i = \alpha F_k(X_i) \oplus \beta F_k(X_i \oplus a)$, $i = \overline{1,t}$). Для цього вводяться дві гіпотези: гіпотеза H_0 описує те, що оракул F(до якого криптоаналітик має доступ) з ймовірністю $1/2$ є реалізацією випадкової ріноймовірною підстановкою на множині V_n; гіпотеза H_1 про те, що оракул F з ймовірністю $1/2$ співпадає з шифрувальним перетворенням F_k шифру $\Im$ при невідомому ключі k, який вибран випадково рівноймовірно з множини K. Мета атаки

полягає у тому, щоб розрізнити ці дві гіпотези.

Алгоритм 2.5.

1. Криптоаналітик обирає ненульові вектори $\alpha, \beta, a \in V_n$.
2. Генерує випадкові незалежні в сукупновті рівноймовірні ВТ $X_1, \ldots, X_t \in V_n$.
3. Обчислює для кожного ВТ пару ШТ $F_k(X_i)$, $F_k(X_i \oplus a)$, $i = \overline{1,t}$.
4. Відповідно для кожного ШТ обчислює значення $v_i = \alpha F_k(X_i) \oplus \beta F_k(X_i \oplus a)$, $i = \overline{1,t}$.
5. За отриманою послідовністю $v_1, \ldots, v_t$ перевіряє умову виконання нерівності $v_1 + \cdots + v_t > C$ (величина $C > 0$ визначається зазделегіть). Якщо умова виконується, то гіпотеза H_0 вважається істинною, в іншому випадку приймається гіпотеза H_1.

Твердження 2.2. *Найменший обсяг даних, необхідних для проведення на шифр* $\Im$ *диференціально-лінійної атаки з імовірністю помилки не більше ніж* $\sigma \in (0, 1/2)$ *задовольняє нерівності [21]*

$$t \geqslant \frac{2(1 - h(\sigma))ln2}{|K|^{-1} \sum\limits_{k \in K} \triangle(P_k) + |\sigma(V_n)|^{-1} \sum\limits_{F \in \sigma(V_n)} \triangle(P_F)}, \tag{2.3}$$

де

$$\triangle(P_k) = (2P_X\{\alpha F_k(X) = \beta F_k(X + a)\} - 1)^2$$

$$\triangle(P_F) = (2P_X\{\alpha F(X) = \beta F(X + a)\} - 1)^2$$

2.5 Результати диференціально-лінійних атак на блокові шифри

Для того, щоб оцінити ефективність даного виду атак, необхідно розглянути побудовані диференціально-лінійні атаки на конкретні ітеративні блокові шифри. Можна виділити наступні результати дослідників.

DES. Для 8-раундового DES диференціально-лінійний метод став дуже ефективним. За допомогою цієї атаки можна відновити 10 бітів ключа з лише 512 обраними відкритими текстами та шанс на успіх скаладає 80%. Імовірність успіху може срости до 95%, використовувати 768 ВТ [17].

ARIA. Не зважаючи на те, що алгоритм стійкий до диференціальних та лінійних атак поодинці, він вразливий до диференціально-лінійної атаки[18].

CTC2. Для проведення атаки на даний алгоритм, необхідно 2^{142} обраних відкритих текстів та $2^{54.2}$ байтів пам'яті, що наразі з сучасною текхнікою не є можливим для раціонального використання. При цьому, імовірність відновити 255 біт ключа складає 99,9% [19].

Serpent. Атака застосовна до 11-раундового алгоритму з ключами розмірами 140–256 біт. Працює швидше, ніж повний перебір, і має рівень успіху 72,1%. Для атаки потрібно $2^{125.3}$ обраних відкритих текстів та 2^{60} байтів оперативної пам'яті [20].

Висновки до розділу 2

Двома центральними статистичними методами криптоаналізу блочних шифрів є диференційний криптоаналіз та лінійний криптоаналіз. Виходячи із особливостей даних атак, стійкість до цих двох криптоаналітичних прийомів стала центральним критерієм у конструкції блочноих шифрів. Не дивлячись на те, що виключення довгих диференціалів та лінійних наближень здається достатнім для того, щоб зробити шифр стійким до диференціальних та лінійних атак, виявилося, що у багатьох випадках короткі характеристики та наближення також можуть бути використані для розбиття шифру. Прикладом даного криптоаналізу є диференціально-лінійна атака. Даний вид криптоаналізу ділиться на два типи атак: розрізнювальна атака, метою якої є відрізнити шифр від випадкової підстановки, та атака, спрямована на відновлення

бітів ключа. Однозначну ефективності диференціально-лінійної атаки визначити складно. Лінійний та диференціальний аналізи поодинці є менше ефективними відносно минулого стандарту шифрування DES, який є цілковито не стійким до диференціально-лінійного методу криптоаналізу. Атаки на новіші шифри, такі як CTC2, Serpent мають менший успіх, адже потребують більшої кількості ресурсів, які не завжи є можливість отримати.

Вивчення та аналіз диференціально-лінійних атак на ітеративні блокові шифри є важливим методом для удосконалення шифрів, підвищення їх стікості та пошуку вразливостей.

3 СПІВВІДНОШЕННЯ МІЖ ПАРАМЕТРАМИ, ЩО ХАРАКТЕРИЗУЮТЬ ДИФЕРЕНЦІАЛЬНІ, ЛІНІЙНІ ТА ДИФЕРЕНЦІАЛЬНО-ЛІНІЙНІ ВЛАСТИВОСТІ БЛОКОВИХ ШИФРІВ

У розділі 3 були розглянуті та проаналізовані матричні співвідношення між параметрами, що характеризують диференціальні, лінійні та диференціально-лінійні властивості ітеративних блокових шифрів. Були визначені матричні характеристики, за допомогою яких можна визначити стійкість шифрів відносно диференціально-лінійного методу криптоаналізу, та з'ясовані причини відустності оцінок стійкості ітеративних блокових шифрів відповідно разглянутого виду криптографічного аналізу.

3.1 Коефіцієт кореляції

Означення 3.1. Коєфіцієнт кореляції, який зображає зв'язок між парою парою булевих функцій $f(x)$ та $g(x)$, що позначається як $C(f, g)$, визначається як

$$C(f, g) = 2 \cdot P\{f(x) = g(x)\} - 1 \tag{3.1}$$

Очевидно виводиться, що $C(f, g) = C(g, f)$. Якщо коєфіцієнт кореляції відмінний від нуля, то функціїї $f(x)$ та $g(x)$ називаються корельованими.

Вектор відбору w є бітовим вектором, який відбирає усі компоненті i із вектора, де $w_i = 1$. Аналогічно внутрішньому добутку векторів у лінійній алгебрі, лінійна комбінація компонентів вектора x, вибраним w, може бути виражена як $w^T x$, де степінь T позначає транспонування вектора w. Лінійна булева функція $w^T x$ повністю задається відповідним

вектором відбору w.

Нехай $\widehat{f}(x)$ буде дійсною функцією, яка дорівнює -1, при $f(x) = 1$ та відповідно 1, при $f(x) = 0$. Це можна виразити як $\widehat{f}(x) = (-1)^{f(x)}$. У цьому позначенні дійсна функція, що відповідає лінійній булевій функції $w^T x$, стає $(-1)^{w^T x}$. Побітова сума двох булевих функцій відповідає розрядному добутку їх дійсних аналогів, тобто:

$$\widehat{f(x) + g}(x) = \widehat{f}(x)\widehat{g}(x) \tag{3.2}$$

внутрішній добуток для функцій, що мають реальне значення визначається як:

$$< \widehat{f}(x), \widehat{g}(x) >= \sum_x \widehat{f}(x)\widehat{g}(x) \tag{3.3}$$

з цього випливає, що:

$$C(f(x), g(x)) = 2^{-n} < \widehat{f}(x), \widehat{g}(x) > \tag{3.4}$$

Дійсні функції, що відповідають лінійним булевим функціям, утворюють ортогональний базис відносно визначеного внутрішнього добутку:

$$< (-1)^{u^T x}, (-1)^{v^T x} >= 2^n \sigma(u + v), \tag{3.5}$$

де $\sigma(w)$ — дійсна функція дорівнює 1, якщо w нульвий вектор, і 0 в інших випадках. Представлення булевої функції щодо цієї основи називається її перетворенням Уолша-Адамара.

Зв'язок між перетворенням Уолша-Адамара булевої функції та її кореляцією з лінійними булевими функціями спочатку був встановлений в [8]. Якщо коєфіцієнти кореляції $C(f(x), w^T x)$ позначити як $\widehat{F}(x)$, то матимемо:

$$\widehat{f}(x) = \sum_w \widehat{F}(w)(-1)^{w^T x} \tag{3.6}$$

$$\widehat{F}(w) = 2^{-n} \sum_x \widehat{f}(x)(-1)^{w^t x} \tag{3.7}$$

$$\widehat{F}(w) = W(f(x)) \tag{3.8}$$

Отже, булева функція повністю задається набором коефіцієнтів кореляції з усіма лінійними функціями.

3.2 Матриця кореляції

Відображення $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ можна представити як m булевих функцій $(h_0, \dots h_{n-1})$. Кожна функція h_i має перетворення Уолша-Адамара H_i. Векторна функція з компонентами H_i позначається як $\widehat{H}$ і її можна вважати перетворенням Уолша-Адамара перетворення h. Як і у випадку булевих функцій, $\widehat{H}$ повністю визначає булеве перетворення h. Перетворення Уолша-Адамара будь-якої лінійної комбінації компонентів h визначається як

$$W(u^T h) = \bigotimes_{u_i=1} H_i \tag{3.9}$$

Усі коефіцієнти кореляції між лінійними комбінаціями вхідних бітів та вихідних бітів відображення h можуть бути розміщені у *кореляційній мартриці* C^h розмірністю $2^m \times 2^n$. Елемент C_{uw}, де u — це номер рядка, а w — стовпця, дорівнює $C(u^T h(x), w(x))$. Рядки матриці можна інтерпретувати як

$$(-1)^{u^T h(x)} = \sum_w C^h_{uw} (-1)^{w^T x} \tag{3.10}$$

3.3 Співвідношення між параметрами, що характеризують диференціальні, лінійні та диференціально-лінійні властивості блокових шифрів

Для будь-якої комутативної групової операції $+$ на множині $V_n = \{0,1\}^n$ та довільної підставновки $f \in \sigma(V_n)$ можна записати матриці $C_f = (C_f(\alpha,\beta))_{\alpha,\beta\in V_n}$, $L_f = (L_f(\alpha,\beta))_{\alpha,\beta\in V_n}$, $D_{f,+} = (D_{f,+}(\alpha,\beta))_{\alpha,\beta\in V_n}$, $A_{f,+} = (A_{f,+}(\alpha,\beta))_{\alpha,\beta\in V_n}$ [21], які мають наступний вигляд

$$C_f(\alpha,\beta) = 2^{-n}\sum_{x\in V_n}(-1)^{\alpha f(x)\oplus\beta x}, \alpha,\beta\in V_n \tag{3.11}$$

$$L_f(\alpha,\beta) = (2P_X\{\alpha X = \beta f(X)\} - 1)^2, \alpha,\beta\in V_n \tag{3.12}$$

$$D_{f,+}(\alpha,\beta) = P_X\{f(X+\alpha)\oplus f(X) = \beta\}, \alpha,\beta\in V_n \tag{3.13}$$

$$A_{f,+}(\alpha,\beta) = 2^{-n}\sum_{x\in V_n}(-1)^{\beta(f(x+\alpha)\oplus f(x))}, \alpha,\beta\in V_n \tag{3.14}$$

У матрицях (3.12) та (3.3) випадковий вектор X має рівномірний розподіл на множині V_n.

Матриця (3.11) є інтерпритованим представленням кореляційної матриці підстановки f, тобто, ця матриця відображає залежність між всіма бітами входу та всіма бітами виходу, а вектори α та β задають, які саме біти, відповидно виходу та входу, обираються.

З іншого боку матриця (3.12) є інакшою версією таблиці розподілу кореляційної імунності [10] перестановки f, що зображує внутрішній добуток між послідовністю кожної лінійної комбінації комопнентних функцій і кожною лінійною послідовністю. Дана матриця корисна для вивчення кореляційного імунітету, а також нелінійності кожної лінійної комбінації компонентних функцій.

Матриця (3.3) співпадає з таблицею розподілу різниць, у випадку коли $+ = \oplus$. Максимальні елементи цієї матриці, що містяться в її рядках

та стовпцях, характерицують стійкість шифру $\Im$ до диференціального методу криптоаналізу.

Матриця (3.14), також у випадку, коли $+ = \oplus$, співпадає з таблицею розподілу автокореляції підстановки f. Ця матриця вказує на автокореляцію всіх лінійних комбінацій компонентних функцій. Стійкість шифру $\Im$ протистояти диференціально-лінійному методу криптоаналізу(у випадку коли $\alpha = \beta$), характеризується найбільшим значенням квадратів елементів матриці (3.14), що розташовані у її рядках та стовпцях з ненульовими номерами.

Якщо $\Im$ ітераційтиний блоковий шифр з множиною ВТ та ШТ V_n, множиною ключів K та сім'єю шифрувальних перетворень $(F_k : k \in K)$, тоді матриці $C_\Im$, $L_\Im$, $D_{\Im,+}$ та $A_{\Im,+}$ визначаються як середні арифметичні за всіма ключами $k \in K$ значень матриць C_{Fk}, L_{Fk}, $D_{F_k,+}$ та $A_{F_k,+}$ відповідно.

Не складно помітити, що з формул (3.11) та (3.12) випливає перше співвідношення матриць, а саме [21]:

$$L_f(\alpha,\beta) = C_f(\beta,\alpha)^2, \alpha,\beta \in V_n \tag{3.15}$$

Дане співвідношення описує зв'язок між кореляційною матрицею та таблицею розподілу кореляційної імунності.

Є співвідношення між таблицею розподілу автокореляції та таблицею розподілу різниць. Нехай $H_n = ((-1)^{\alpha\beta})_{\alpha,\beta\in V_n}$ — матриця Адмара, тоді справедлива рівність, у випадку, коли $+ = \oplus$ [10] [21]:

$$A_{f,\oplus} = D_{f,\oplus}H_n = H_nL_f \tag{3.16}$$

Використовуючи ту саму матрицю Адамара H_n, $\Pi_f = (\sigma(f(\alpha),\beta))_{\alpha,\beta\in V_n}$ — підстановочну матрицю, що відповідає підстановці $f \in \sigma(V_n)$, де σ позначає символ Кронекера ($\sigma(f(\alpha),\beta) = 1$, якщо $f(\alpha) = \beta$ та $\sigma(f(\alpha),\beta) = 0$, якщо $f(\alpha) \neq \beta$) випливають наступні співвідношення [21]:

$$C_f = 2^{-n}H_n\Pi_f^TH_n \tag{3.17}$$

$$D_{f,\oplus} = 2^{-n} H_n L_f H_n, \tag{3.18}$$

де отримується з наведених означень, а було доведено в [12].

З формули випливає, що матриця C_f є ортогональною. З цього можна зробити висновок, що на підставі рівностей та матриці L_f та D_f є двічі стохастичними.

Для визначення стійкості ітеративного блокового шифру відносно диференціально-лінійної атаки необхідно надати оцінку максимальним значенням квадратів елементів таблиці розподілу автокореляції підстановки f, або $A_{f,+}(\alpha, \beta)$ у наведених вище позначеннях. Якщо повидитися на формулу (3.16) можна сказати, що матриця $A_{f,+}(\alpha, \beta)$ залежить від добутку таблиці розподілу різниць та матриці Адамара. Матриця $D_{f,+}(\alpha, \beta)$ є двічі стохастичною, що означає, що сума елементів будь-якого рядка або стовпця однакові.

Розглянемо матрицю H_n. Це матриця Адамара, у якої в першому рядку та першому стовпчику стоять одиниці, адже якщо α чи β дорівнюють нулю, то $(-1)^{\alpha\beta}$ не може приймати інших значень. Зазвичай, у матрицях чи таблицях, які використовують для криптографічного аналізу шифрів, перші рядки та перші стовпчики не використовують, бо вони не несуть у собі важливої інформації. У матриці H_n перший рядок та перший стовбець складається з одиниць, а сума елеметів у кожному рядку та кожному стовпчику дорівнює нулю..

3.4 Стійкість ітеративних блокових шифрів відносно диференціально-лінійного криптоаналізу

Для визначення стійкості ітеративних блокових шифрів відносно диференціально-лінійного криптоаналізу використовують методи, де для оцінки ефективності проведення атаки задають якісь умови чи властивості самого шифру. Однак немає обґрунтування стійкості відносно диференціально-лінійної атаки без евристичних методів аналізу. І цьому є

причина.

Щоб довести стійкість ітеративного блочного шифру відносно диференціально-лінійних атак необхідно дати оцінку найбільшим значенням квадратів елеметів матриці $A_{f,+}(\alpha, \beta)$. Для цього розглянемо описані раніше матриці, а саме $D_{f,+}(\alpha, \beta)$. Як вже було сказано, у даній матриці випадковий вектор X має рівномірний розподіл на множині V_n, з чого випливає, що члени матриці рівномірні, однакові. Шляхом множення цієї матриці на матрицю Адамара можна отримати матрицю $A_{f,+}(\alpha, \beta)$, за допомогою якої й необхідно визначити стійкість шифру до диференцільно-лінійних атак. Без припущень про природу шифру чи його властивості матриця $D_{f,+}(\alpha, \beta)$ не буде відображати вичерпної кількості інформації для аналізу, після множення її на матрицю Адамара H_n ситуація трохи зміниться, але не настільки, щоб провести доскональний аналіз для обґрунтування стікості. Отже, це і є причиною, через яку досі не було обґрунтовано стійкості ітеративних блочних шифрів до диференціально-лінійних атак.

Підсумовуючи вище сказане, можна також виділити той факт, що існуючі методи оцінки стійкості ітеративних блочних шифрів є не ефективними без евристичних методів аналізу. Отже, щоб обґрунтувати стійкість, необхідно застосовувати інші методи її отримання.

Висновки до розділу 3

Параметри, що характеризують диференціальні, лінійні та диференціально-лінійні властивості ітеративних блокових шифрів можна проаналізувати, використовуючи відповідні матриці. Параметри цих матриць характеризують стійкість шифру відповідним атакам. Досліждення виявило, що є певні співвідношення, між цими параметрами.

У загальному випадку, щоб довести стійкість ітеративного блочного шифру відносно диференціально-лінійних атак, необхідно дати оцінку

найбільшим значенням квадратів елеметів матриці $A_{f,+}(\alpha, \beta)$. Матриця $A_{f,+}(\alpha, \beta)$, що характеризує диференціально-лінійні властивості шифру, виражається через добуток двох матриць: матриці Адамара та матриці $D_{f,+}(\alpha, \beta)$, що співпадає з таблицею розподілу різниць. Тобто шляхом аналізу параметрів матриць, можна оцінити стійкість відносно диференціально-лінійного криптоаналізу. Проблемою є те, що без припущень про особливості шифру, оцінити параметри для обгрунтування стійкости існуючими методами не вдається, у зв'язку з особливостями матриці $D_{f,+}(\alpha, \beta)$, які були описані у розділі 3.

ВИСНОВКИ

Розвиток та аналіз ітеративних блокових шифрів є важливим та перспективним. Особливо аналіз стійкості алгоритмів до криптографічних атак. Двома центральними статистичними методами криптоаналізу блочних шифрів є диференційний криптоаналіз та лінійний криптоаналіз. Виходячи із особливостей даних атак, стійкість до цих двох криптоаналітичних прийомів стала центральним критерієм у конструкції блочних шифрів. Але стійкість до цих атак не виключає вразливості до більш складних методів, наприклад, диференціально-лінійного криптоаналізу.

У ході даної роботи був проведений аналіз опублікованих джерел за тематикою диференціально-лінійних атак на блокові шифри та матричних співвідношень для параметрів, що характеризують стійкість блокових шифрів відносно диференціального, лінійного та диференціально-лінійного методів криптоаналізу. Аналіз показав, що диференціальний та лінійний методи криптоаналізу досліджені у більшій мірі, навідміну від диференціально-лінійного криптоаналізу, який відносно більш новий. Для диференціально-лінійного криптоаналізу вже були виведені нижні оцінки інформаційної складності, однак обгрунтування стійкості шифру так і не було визначено. Були проаналізовані деякі матричні співвідношення параметрів та зроблені висновки щодо їх властивостей.

Метою було з'ясувати причину, через які не вдається обгрунтувати стійкість ітеративних блокових шифрів відносно диференціально-лінійних атак. Ця причина полягає у самих властивостях таблиці розподілу різниць та матриці Адамара, тому що саме через їх добуток можна виразити матрицю розподілу автокореляційної підстановки, елементи якої й мають визначати стійкість шифру до диференціально-лінійного методу криптоаналізу.

Для подальших дісліджень варто враховувати виведені властивості матричних співвідношень та досліджувати або вводити інші методи, щоб визначити стійкість шифру до диференціально-лінійних методів криптоаналізу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Horst Feistel. *Cryptography and Computer Privacy.* 1973.

2. Achiya Bar-On, Orr Dunkelman, Nathan Keller and Ariel Weizman. *DLCT: A New Tool for Differential-Linear Cryptanalysis.* 2019.

3. Kaisa Nyberg. *The Extended Autocorrelation and Boomerang Tables and Links Between Nonlinearity Properties of Vectorial Boolean Functions.* 2019.

4. Баричев С.Г., Серов Р.Е.. *Основы совеременной криптографии.* 2006.

5. Douglas R. Stinson. *Cryptography: Theory and Practice.* 1995.

6. Howard M. Heys. *A tutorial on linear and differential cryptanalysis.* 2002.

7. Anne Canteaut, Joëlle Roué. *Differential Attacks Against SPN: A Thorough Analysis.* 2015.

8. M.R.Z'aba, M.A.Maarof. *A survey on the cryptanalysis of the advanced encryption standard.* 2006.

9. Joan Daemen, René Govaerts and Joos Vandewalle. *Correlation Matrices.* 1994.

10. Xian-mo Zhang , Yuliang Zheng and Hideki Imai. *Relating Differential Distribution Tables to Other Properties of of Substitution Boxes.* 1997.

11. ISO [Електронний ресурс] / iso.org. — 2021. — Режим доступу: https://www.iso.org/standard/54531.html

12. Chabaud F., Vaudenay S. *Links between differential and linear cryptanalysis.* 1994.

13. Mitsuru Matsui, Atsuhiro Yamagishi. *A New Method for Known Plaintext Attack of FEAL Cipher.* 1992.

14. Mitsuru Matsui. *The First Experimental Cryptanalysis of the Data Encryption Standard.* 1994.

15. Mitsuru Matsui. *Linear Cryptanalysis Method for DES Cipher.* 1993.

16. Eli Biham, Adi Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* 1990.

17. Susan K., Langford M. and E. Hellman. *Differential-Linear Cryptanalysis.* 2001.

18. Wentan Yi, Jiongjiong Ren and Shaozhen Chen. *Multidimensional Differential-Linear Cryptanalysis of the ARIA Block Cipher.* 2016.

19. Jiqiang Lu. *A Methodology for Differential-Linear Cryptanalysis and Its Applications.* 2012.

20. Eli Biham, Orr Dunkelman and Nathan Keller. *Differential-Linear Cryptanalysis of Serpent.* 2003.

21. Олесійчук А.М. *Узагальнений диференціально-лінійний криптоаналіз блокових шифрів.* 2021.