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: **«Параметри стійкості фейстель-подібних шифрів до атак бумерангів »**

Виконав: студент 4 курсу, групи ФІ-73
Мітрофанова Еліна Володимиріна

Керівник: к. т. н., доцент кафедри ММЗІ Яковлєв С.В._____

Консультант: _ _____

Рецензент: _ _____

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: Мітрофанова Еліна Володимиріна

1. Тема роботи: «*Параметри стійкості фейстель-подібних шифрів до атак бумерангів* »,

керівник: к. т. н., доцент кафедри ММЗІ Яковлєв С.В.,

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: побудова аналітичних оцінок стікойсті фейстель-подібних схем до атакбумерангів та їх аналіз

5. Перелік ілюстративного матеріалу: 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	1 вересня - 1 жовтня 2020 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	1 жовтня – 1 грудня 2020 р	Виконано
3	Отримання параметрів стійкості для одного раунду R-схеми та схеми MISTY	1 грудня 2020 р - 17 січня 2021 р	Виконано
4	Отримання параметрів стійкості для двох раундів R-схеми та схеми MISTY	17 січня - 26 лютого 2021 р	Виконано
5	Уточнення нижньої границі рівномірності бумеранга для 3-раундової R-схеми та огляд атаки бумерангів на схему Лая-Мессі, 3-раундову схему MISTY	26 лютого - 20 березня 2021 р	Виконано
6	Огляд атаки бумерангів на схему Лая-Мессі	20 березня - 10 травня 2021 р	Виконано
7	Оформлення роботи та підготовка презентації до захисту	10 травня - 01 червня 2021 р	Виконано

Студент _____ Мітрофанова Е.В.

Керівник _____ Яковлєв С.В.

РЕФЕРАТ

Кваліфікаційна робота містить: 40 стор., 9 рисунків, 1 таблицю, 11 джерел. Метою цього дослідження є уточнення методів оціннювання стікойсті симетричних блокових шифрів до деяких класів атак. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є параметри стійкості фейстель-подібних шифрів до атаки бумерангів.

У даній роботі було отримано параметри стійкості до атаки бумерангів фейстель-подібних схем: 1-раундових, 2-раундових MISTY та R-схеми. Уточнено нижню оцінку для S-блоків, які мають констукцію 3-раундової R-схеми, а також була розглянута атака бумерангів на 3-раундову MISTY та схему Лая-Мессі.

АТАКА БУМЕРАНГІВ, BOOMERANG CONNECTIVITY TABLE, BCT, FEISTEL BOOMERANG CONNECTIVITY TABLE FBCT, R-СХЕМА, MISTY, СХЕМА ЛАЯ-МЕССІ

ABSTRACT

The qualifying paper contains: 40 pages, 12 figures, 3 tables, 11 sources. The purpose of this investigation is to refine methods of estimation of symmetry block ciphers to some classes of attacks. The object of the research is information processes in cryptographic protection systems. The subject of the research is resistance parameters of Feistel-like Ciphers for boomerang attacks.

In this work, the parameters of resistance to boomerangs attack of Feistel-like Ciphers were obtained for: 1-round, 2-round MISTY and R-schemes. The lower estimation for S-blocks was refined for S-blocks which have the construction of a 3-round R-scheme. Also the boomerang attack on the 3-round MISTY and the Lai-Messi scheme was considered.

BOOMERANG ATTACK, BOOMERANG CONNECTIVITY TABLE, BCT, FEISTEL BOOMERANG CONNECTIVITY TABLE FBCT, R-SHEME, MISTY, LAI-MASSEY SHEME

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

V_n – множина n-бітових векторів.

DDT – таблиця розподілів диференціалів (Difference Distribution Table)

BCT – таблиця бумерангової зв'язнсті (Boomerang Connectivity Table)

FBCT – таблиця фейстелевої бумерангової зв'язності (Feistel Boomerang Connectivity Table)

SPN (Substitution-Permutation network) – SP-мережа

ВСТУП

Актуальність дослідження. На сьогодняшній день існує багато різновидів криптоаналізу. Один із розповсюджених – диференційний аналіз, який вперше був хапропонован ще у 90-х роках ізраїльськими фахівцями Елі Біхамом і Аді Шамір для злому криптосистем, подібних DES[1]. Але DES виявився стійким до диференційного криптоаналізу, на відміну від деяких інших шифрів. Так, наприклад, вразливим виявився шифр FEAL.

Диференційний аналіз дуже стрімко став розвиватися, з'явилося багато нових технік. Однією з них є атака бумерангів[3]. Атака бумерангів була успішно застосована для злому шифрів, які до її появлення важалися стійкими до диференційних атак. У зв'язку з цим знадобився інстумент, який зміг би, як покращувати атаку, так і допомагати оцінити стійкість S-блоків до неї при побудові нових криптосистем. У 2018 для шифрів, заснованих на SP-мережі запропоновали поняття таблиці бумерангової зв'язності [6], пізніше представили аналог цієї таблиці для шифрв, S-блоки яких базуються на мережі Фейстеля [8].

У цій роботі більш детально розглянемо атаку на шифри, які побудовані на основі фейстель-подібних схем. Одержимо та проаналізуємо параметри стійкості раундових функцій даних шифрів до атаки бумерангів через відповідні параметри S-блоків та виявимо їх співвідношення вже з існуючими параметрами.

Метою дослідження є уточнення методів оціннювання стікойсті симетричних блокових шифрів до деяких класів атак. Задача дослідження - побудова аналітичних оцінок стікойсті фейстель-подібних схем до атак бумерангів

1) провести огляд опублікованих джерел за тематикою дослідження;

2) проаналізувати алгебрагічні властивості параметрів бумерангової зв'язності та фейстелевоібумеранговох зв'язності;

3) побудувати аналітичні співвідношення для R-схеми та схеми MISTY для одного, двох та трьох раундів;

4) побудувати нижню границю для бумерангової зв'язності для 3-раундової R-схеми.

Об'єктом дослідження інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є параметри стійкості фейстель-подібних шифрів до атаки бумерангів.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: комбінаторний аналіз, дискретная математика, абстактна алгебра. **Наукова новизна** одержані аналітичні вирази для параметри зв'язності для одного, двох раундів схеми MISTY та R-схеми, уточнено нижнб оцінку для бумерангової зв'язності 3-раундової R-схеми.

Практичне значення. Результати данної роботи можуть бути використанні при аналізі існуючих та побудові нових надійних фейстель-подібних схем та криптосистем, які використовують їх, в якості складових елементів.

Апробація результатів та публікації. Частину результатів данної роботи було оприлюднено на XIX Науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики» (13-14 травня 2021 року, м.Київ).

1 АТАКА БУМЕРАНГІВ І ТАБЛИЦЯ ФЕЙСТЕЛЕВОЇБУМЕРАНГОВОЇ ЗВ'ЯЗНОСТІ

У даному розділі розглянуто основні поняття, які стосуються атаки бумерангів, таблиці бумерангової зв'язності та новітнього аналогу цієї таблиці для мережі Фейстеля – таблиці фейстелевої бумерангової зв'язності (The Feistel Boomerang Connectivity Table, FBCT).

1.1 Диференційний аналіз

Диференційний аналіз був запропонован ізраільськими фахівцями у роботі [1]. У ньому розглядаються пари зашифрованих текстів та відповідних їм розшифрованих. Розглянемо схему диференційного аналізу, але перд цим введемо деякі поняття.

Нехай $\circ$ та $\bullet$ – оператори на множені V_n, де V_n – множина n-бітових векторів.

1) $< V_n, \circ >$ та $< V_n, \bullet >$ – абелеві групи;

2) нейтральний елемент – нулевий вектор.

Ці операціїї задають певну статистику. Будемо розглядати не те, як проходить шиифрувальний текст по шифру, а те, як проходить під час шифрування різниця між шифрувальними текстами. Розглянемо схему диференційного аналізу Нехай на вхід подаються два повідомлення x, x' з деякою різницею α.

1) Накопичуємо N пар (x, x') таких, що $x = x' \circ \alpha$ і відповідних їм шифртекстів (y,y').

2) Для кожного кандидата ключа у k_r, де

$$(y,y') \to (x_{r-1},x'_{r-1})$$

і перевіряємо, що виконується рівність $x'_{r-1} = x_{r-1} \bullet \beta$.

3) Коректне k_r – для якого рівність виконалась найбільше.

1.2 Атака бумерангів

Наприкінці 90-х років Серж Водне (Serge Vaudenay), французький криптограф, розробив шифр COCONUT98 та надав доказ безпеки цього шифру до диференційного аналізу [2]. Пізніше Девід Вагнер опублікував наукову роботу, у якій запропонував новий вид диференційного аналізу – атаку бумерангів [3]. Він успішно застосував дану атаку для злому COCONUT98 та інших шифрів, які до цього вважалися стійкими до "класичного"диференційного аналізу.

Атака бумерангів розглядає алгоритм шифрування $E_k(x)$ як композицію двох підшифрі: $E_k(x) = E2_k(A_k(E1_k(x)))$, де A_k – це афінне відображення. $D1$, $D2$ – розшифровуючи перетворення до $E1$ та $E2$; $\alpha, \beta, \gamma, \phi \in V_n$ – це деякі різниці. [3]

$$Pr\left\{\alpha \underset{E1}{\longrightarrow} \beta\right\} = p_1,\ \ Pr\left\{\beta \underset{D1}{\longrightarrow} \alpha\right\} = p_2,\ \ Pr\left\{\gamma \underset{D2}{\longrightarrow} \phi\right\} = q.$$

Також ми будемо розглядати: x_i – входи, $u_i = E1_k(x_i)$ – результат шифрування, $v_i = A_k(u_i)$ – результат проходження через афінну функцію, $y_i = E2_k(v_i)$ – шифртекст. Постає питання, яка імовірність того, що шифртексти x_3 та x_4 також будуть мати різницю α .

Якщо подивитися на рисунок 2.2, то можна побачити, що $u_1 \oplus u_2 = \beta$ із імовірністю p_1, $v_1 \oplus v_3 = \phi$ з імовірністю q, $v_2 \oplus v_4 = \phi$ з імовірністю q.

Лема 1.1. *Якщо A — невироджена афінна булева функція і*

$$A(u_1) \oplus A(u_2) \oplus A(u_3) \oplus A(u_4) = 0$$

$$u_1 \oplus u_2 \oplus u_3 \oplus u_4 = 0 \Rightarrow u_3 \oplus u_4 = \beta \Rightarrow Pr\{x_3 \oplus x_4 = \alpha\} = p_2$$

$$\Rightarrow v_1 \oplus v_2 \oplus v_3 \oplus v_4 = 0.$$

Твердження 1.1. *Якщо всі події є незалежними, то*

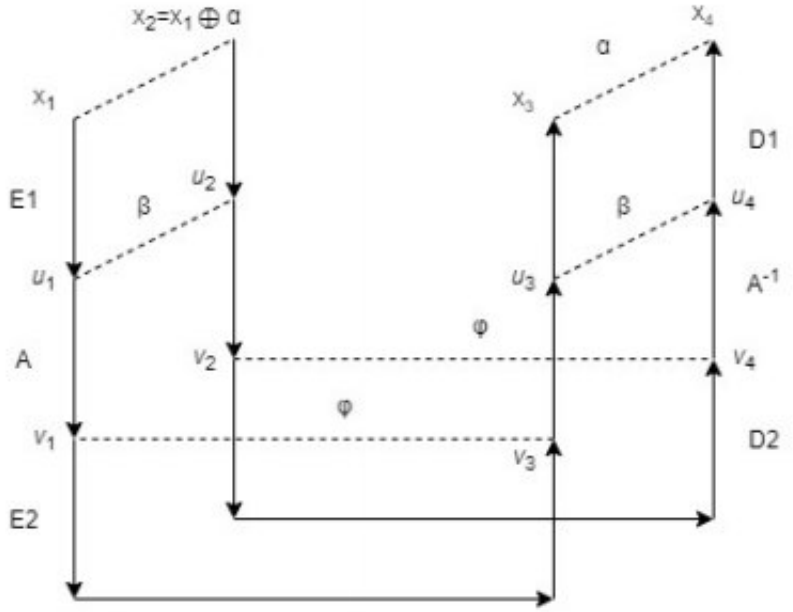

Рисунок 1.1 – Атака бумерангів

$$Pr\left\{x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0\right\} = p_1 p_2 \hat{q},\ де\ \hat{q} = \sum_{\phi} Pr\left\{\gamma \xrightarrow[D2]{} \phi\right\} = q$$

Зауваження.

– Атака працює, якщо $p_1 p_2 \hat{q} \geqslant \frac{1}{2^n}$.

– E1 та E2 не повинні бути однаковими.

– Мерфі показав приклад, коли ймовірність генерування правильного квартету відкритих шифрів дорівнює нулеві [4]. Протилежний феномен, а саме відмінності, які трапляються з імовірністю вищою, ніж очікувалося, також було представлено Бірюковим і Ховратовічем [5].

– Суттєвий недолік данної атаки полягає в тому, що це атака з адаптивним вибором відкрітих тексті та шифртекстів, тобто потрібно вміти не тільки шифрувати, але й розшифровувати.

Після опублікування роботи Вагнера з'явилося декілька модифікацій атаки бумернга : прямоугольна атака rectangle attack

1.3 Boomerang Connectivity Table

Для правильного врахування зв'язку між зашифрованими повідомленнями в атаці бумерангів використовується таблиця бумерангової зв'язності (Boomerang Connectivity Table, BCT), яка була представлена у роботі [6]. Таблиця бумерангової зв'язності за своєю структорою схожа з однією добре відомих таблиць – таблицею розподілів диференціалів (Difference Distribution Table, DDT).

Таблиця розподілу диференціалів має розмір $2^n \times 2^n$ та зберігає представлення властивостей диференціального розподілу для n-бітового S-блоку $S : \{0,1\}^n \to \{0,1\}^n$. Для довільних Δ_i, ∇_0 обчислюється

$$\#\{x \in \{0,1\}^n : S(x) \oplus S(x \oplus \Delta_i) = \Delta_0\}.$$

У відповідній комірці таблиці зберігається значення $\tau(\Delta_i,\Delta_0)$, яке

Δ_i \ Δ_o	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
a	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
b	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
c	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
d	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
e	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
f	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Рисунок 1.2 – DDT для s-блоку PRESENT

показує, що вхідна різниця Δ_i розповсюджується до вихідної різниці Δ_0 з імовірністю $\tau(\Delta_i,\Delta_0)/2^n$.

Замість того, щоб дивитися на властивість раунду в цілому, тобто на функцію, яка зазвичай має 64 або 128 бітів, було запропоновано звести проблему до тієї, яку можемо легко вивчити при завданні їй невеликого розміру: незалежне вивчення кожного S-блоку S. В той час як таблиця розподілення диференціалів описує різні властивості кожного S-блоку, з яких виводяться характеристики раунду, таблиця бумерангової зв'язності дає ймовірність перемикання бумеранга на кожен S-блок, з якого виводиться один з раундів.

Δ_i \ ∇_o	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	0	4	4	0	16	4	4	4	4	0	0	4	4	0	0
2	16	0	0	6	0	4	6	0	0	0	2	0	2	2	2	0
3	16	2	0	6	2	4	4	2	0	0	2	2	0	0	0	0
4	16	0	0	0	0	4	2	2	0	6	2	0	6	0	2	0
5	16	2	0	0	2	4	0	0	0	6	2	2	4	2	0	0
6	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
7	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
8	16	4	0	2	4	0	0	2	0	2	0	4	0	2	4	8
9	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
a	16	0	2	2	0	4	0	0	6	0	2	0	0	6	2	0
b	16	2	0	0	2	4	0	0	4	2	2	2	0	6	0	0
c	16	0	6	0	0	4	0	6	2	2	2	0	0	0	2	0
d	16	2	4	2	2	4	0	6	0	0	2	2	0	0	0	0
e	16	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
f	16	8	0	0	8	0	0	0	0	0	0	8	0	0	8	16

Рисунок 1.3 – BCT для s-блоку PRESENT

Перейдемо до визначення таблиці бумерангової зв'язності. Завдамо деяке перетворення E, яке є композицією двох підшифрів. Кожна комірка BCT буде зберігати ймовірність того, що для S, для кожної пари (Δ_i,∇_0), де Δ_i – вхідна різниця визначена підшифром E_1, а ∇_0 – вихідна різниця

визначена підшифром E_2. Ці значення обчислюються за формулою:

$$\#\{x \in \{0,1\}^n : S^{-1}(S(x) \oplus \nabla_0) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_0)\}/2^n.$$

Таблиця, яка буде зберігти результат обчислення для кожної пари (Δ_i, ∇_0) і буде називатися таблицею бумерангової зв‘язності. Визначимо більш формально.

Означення 1.1. Нехай $S : \{0,1\}^n \to \{0,1\}^n$ – бієктивна функція, $\Delta_i, \nabla_0 \in \{0,1\}^n$. *Таблиця бумерангової зв'язності (BCT)* для S – таблиця розміром $2^n \times 2^n$, у якій значення для кожної (Δ_i, ∇_0) позиції задається як

$$BCT(\Delta_i, \nabla_0) = \#\{x \in \{0,1\}^n : S^{-1}(S(x) \oplus \nabla_0) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_0) = \Delta_i\}.$$

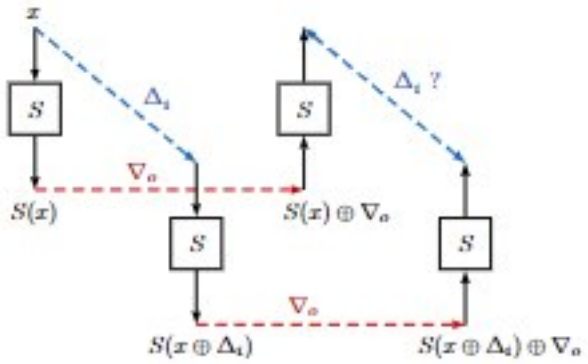

Рисунок 1.4 – Значення BCT (Δ_i, ∇_0) відповідає кількості входів x, які повертають бумеранг за 1 раунд.

Властивості BCT.

1) $BCT^S[0,\nabla_0] = BCT^S[\Delta_i, 0] = 2^n$.
2) $BCT^{S^{-1}}[\Delta_i,\nabla_0] = BCT^S[\nabla_0,\Delta_i]$.
3) $BCT^S[\Delta_i, \nabla_0]$ – парне число.
4) Якщо існують λ, $\mu : V_n \to V_n$ – невиродженні афінні перетворення;

$g(x) = \lambda(S(\mu(x)))$

$$\Rightarrow BCT^g[\Delta_i,\nabla_0] = BCT^S[\mu(\Delta_i), \lambda^{-1}(\nabla_0)]$$

.

Так само, як S-блок із таблицею розподілу диференціалів з малими коефіцієнтами забезпечує стійкість до диференційних атак, так S-блок з таблицею бумерангової зв'язності з невеликими коефіцієнтами не дозваляє зловмиснику створити ефективні атаки у стилі бумеранга.

Підсумовуючи, можна сказати що BCT допомагає спростити аналіз складності, зберігаючи і об'єднуючи різні ймовірності переключения S-блоків шифра в одній таблиці.

1.4 The Feistel Boomerang Connectivity Table

Таблиця бумерангвої зв'язності була розглянута лише для шифрів, S-блоки яких базуються на SP-мережі, тому у роботі [8] запропонували аналог цієї таблиці для шифрів, побудованих на мережі Фейстеля – таблицю фейстелевої бумерангової зв'язності (The Feistel Boomerang Connectivity Table, FBCT)

Нехай $S : \{0,1\}^n \to \{0,1\}^n$ та Δ_i, $\nabla_0 \in F_n^2$. Тоді FBCT для S – це таблиця розміром $2^n \times 2^n$, яка містить значення кожної пари(Δ_i, ∇_0), що обчислюються за формулою:

$$\#\{x \in \{0,1\}^n : S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_0) \oplus S(x \oplus \Delta_i \oplus \ \nabla_0) = 0\}$$

Після того, як таблиця побудована, імовірність того, що бумеранг повернеться протягом одного раунду схеми Фейстеля, буде твором відповідних коефіцієнтів FBCT розділенної на 2^n.

Неважко побачити, що формула для FBCT відповідає кількості разів похідної порядку 2 відносно Δ_i, ∇_0 векторної логічної функції

Таблиця фейстелевої бумерангової зв'язності має певні властивості:

1) *симетричність:*

$$0 \leqslant \Delta_i,\nabla_0 \leqslant 2^n - 1, FBCT(\nabla_0,\Delta_i) = FBCT(\Delta_1,\nabla_0);$$

2) *фіксованні значення:*

а) перший рядок: $0 \leqslant \nabla_0 \leqslant 2^n - 1, FBCT(0,\nabla_0) = 2^n$;

б) перший стовпчик: $0 \leqslant \Delta_i \leqslant 2^n - 1, FBCT(\Delta_i,0) = 2^n$;

в) діагональ: $0 \leqslant \Delta_i \leqslant 2^n - 1, FBCT(\Delta_i,\Delta_i) = 2^n$;

3) кратність: $0 \leqslant \Delta_i, \nabla_0 \leqslant 2^n - 1, FBCT(\Delta_i,\nabla_0) \equiv 0 \mod 4$.

4) еквівалентність:

$$0 \leqslant \Delta_i,\nabla_0 \leqslant 2^n - 1, FBCT(\Delta_i,\nabla_0) = FBCT(\Delta_i,\Delta_i \oplus \nabla_0).$$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	16	0	0	0	0	0	0	0	0	8	8	0	0	0	0
2	16	0	16	0	0	0	0	0	0	0	0	8	0	0	0	0
3	16	0	0	16	8	8	8	8	0	0	0	0	0	0	0	0
4	16	0	0	8	16	0	0	8	0	0	0	0	0	0	0	0
5	16	0	0	8	0	16	8	0	0	0	0	0	0	0	0	0
6	16	0	0	8	0	8	16	0	0	0	0	0	0	0	0	0
7	16	0	0	8	8	0	0	16	0	0	0	0	0	0	0	0
8	16	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0
9	16	0	8	0	0	0	0	0	0	16	0	8	0	0	0	0
a	16	8	0	0	0	0	0	0	0	0	16	8	0	0	0	0
b	16	8	8	0	0	0	0	0	0	8	8	16	0	0	0	0
c	16	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0
d	16	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0
e	16	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0
f	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16

Рисунок 1.5 – Приклад FBCT

Нехай S – майже ідеальна нелінійна функція(almost perfect non-liniar, APN), якщо похідна функції S у точці Δ_i не має рішень або має тільки два рішення для будь-якої $\Delta_i \neq 0$.

Теорема 1.1. *S є APN функцією тоді та тільки тоді, коли для $\Delta_i, \nabla_0 : 1 \leqslant \Delta_i \neq \nabla_0 \leqslant 2^n - 1$ виконується:*

$$FBCT(\Delta_i,\nabla_0) = 0$$

Тобто S називають майже ідеальною нелінійною функцією тоді, коли всі коефіцієнти $FBCT$ дорівнюють нулю, окрім першого стовпчика, першого рядка та діагоналі.

Наслідок 1.1. *Прямим наслідком цієї теореми є те, що будь-яка не-APN-функція має ненульовий коефіцієнт у позиції, яка не знаходиться в першому рядку, першому стовпці або діагоналі її $FBCT$, тому, зокрема, фейстелева бумерангова рівномірність вище або дорівнює 4.*

При вивченні S-блоків часто використовуються різні види еквівалентності, серед яких є лінійна, аффінна, розширена та CCZ-еквівалентність. Ці різні концепції відіграють важливу роль для класифікації наборів S-блоків, через головні криптографічні властивості: диференційність, лінійність та іноді алгебраїчний степінь. У роботі [8] дослідили вищезгадані типи еквівалентності для таблиці фейстелевої бумерангової зв'язності та порівнянняли з BCT.

Рівномірності бумеранга зберігається при	FBCT	BCT
афінної еквівалентності	+	+
расширенної афінної еквівалентності	+	-
CZZ-еквівалентності	-	-
інверсії	-	-

Дивлячись на таблицю можна зробити висновок, що "гарний"S -блок для SPN буде "гарним"і для схеми Фейстеля.

1.5 Поняття бумерангової рівномірності

У 2018 році Бура та Канто (Boura, Canteaut) ввели параметр для характиристики криптографічних S-блоків, який називається *рівномірність бумеранга*(Boomerang uniformity) [7]. Цей параметр дозволяє оцінити ефективність атак бумерангів до введених S-блоків. Рівномірність бумеранга для SPN шифрів визначається як максимальне значення, яке не стоїть не у першому стовпці, не у першому рядку.

Означення 1.2.

$$max_{\Delta_i \neq 0, \nabla_0 \neq 0} BCT(\Delta_i, \nabla_0).$$

Означення 1.3. Бумерангова рівномірність для схеми Фейстеля.

$$max_{\Delta_i \neq 0, \nabla_0 \neq 0, \Delta_i \neq \nabla_0} FBCT(\Delta_i, \nabla_0).$$

У таблиці фейстелевої бумерангової зв'язності діагональ завжди еквівалентна 2^n, тому ці значення були вилучені. З точки зору розробки шифрів на основі схеми Фейстеля, краще використовувати S-блоки з невеликою рівномірністю бумеранга. Цієї мети можна досягти лише за допомогою APN-функції, як була розглянута у попередньому підрозділі.

У випадку з BCT зазначили, що рівномірность бумеранга S і його зворотнє те ж саме [8]. У схемі Фейстеля S-блоки не обов'язково повинні бути оборотними (найбільш відомим прикладом в цій категорії є DES). У досліджинні показали, що для оборотнього S-блоку можна знайти деякі окремі випадки, для яких ця властивість зберігається. Наприклад, для функцій APN, оскільки зворотнє також є майже ідеальною нелінійною функцією. Проте, в загальному випадку ця властивість не виконується.

1.6 Параметри стійкості до атаки бумерангів дяких фейстель-подібних схем

У роботі [7] представлені результати для нижньої границі бумерангової рівномірності 3-раундових схеми Фейстеля, MISTY, Лая-Мессі. Більш детально зупинимося на фейстель-подібних схемах, але спочатку розглянемо основні поняття. Схема Фейстеля була представлена в журналі«SciAm» Горстом Фейстелем ще у 1973 році. Один раунд схеми Фейстеля має вид

$$\Phi(x,y) = (y,F(x)).$$

Раундова функція в схемі Фейстеля є інвалютивно: розшифрування та зашифрування проводиться однаковою процедурою лише із зворотнім порядком раундових ключів. MISTY – схема блокового шифрування, створена на основі схеми Фейстеля у 1995 році [10]. Один раунд схеми MISTY має вид

$$\Phi(x,y) = (y,y \oplus F(x)).$$

Схема Лая-Мессі впреше була представлена у [11]. "Класичний"раунд схеми представляється як:

$$\Phi(x,y) = (x \oplus F(x \oplus y), y \oplus F(x \oplus y)).$$

У схемі Лая-Мессі в якості перемішуючого елемента використовується ортоморфізм σ, щоб уникнути ось такого співвідношення:

$$x_L \oplus x_R = y_L \oplus y_R,$$

де (x_L, x_R) – вхідне повідомлення, а (y_L, y_R) – вихідне повідомлення. Тоді один раунд можна перезаписати як

$$\Phi(x,y) = (\sigma(x \oplus F(x \oplus y)), y \oplus F(x \oplus y)).$$

Для збалансованої 3-раундової MISTY показили, що на нижню оцінку рівномірності бумерангу буде впливати лише функція другого раунду:

$$\beta_S \geqslant 2^n \cdot \beta_{F_2},$$

де $F_1, F_2, F_3 : \{0,1\}^n \to \{0,1\}^n$ – внутрішні перетворення. Для

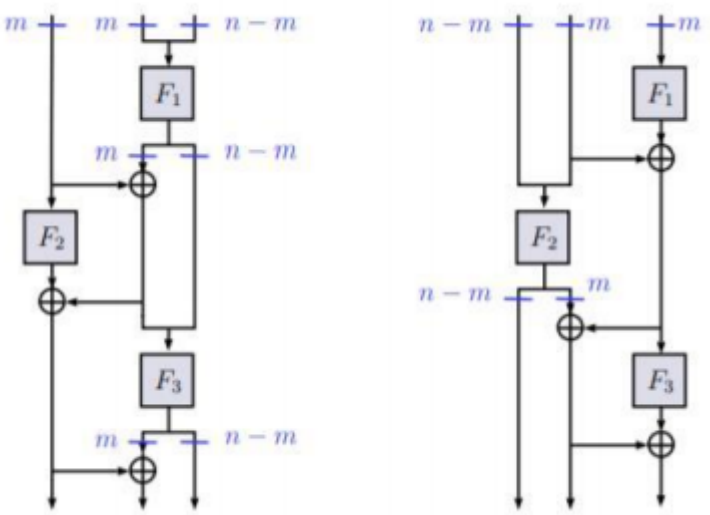

Рисунок 1.6 – Незбалнсована схема MISTY

незбалансованої 3-раундової MISTY, зображеної зліва на Рисунку 1.6, показали, що бумерангова рівномірність обмеженена значенням $2^n\beta_{F_2}$, а для зображеної зправа – $2^n\beta_{F_2|_{F_2^m}}$.

Для схеми Лая-Мессі (див. Рисунок 1.7) була отримана така оцінка

$$\beta_S(a_1, b) = 2^{2n}, a_1 = (a,a), b = (\sigma(a), \sigma(b)) \in (F_2^n)^2, b \in \{0,1\}^n \to \{0,1\}^n$$

R-схема є іншим аналогом схеми Фейстеля. Один раунд R-схеми має вид

$$\Phi(x,y) = (y \oplus F(x), F(x)).$$

У докладі [7] не було представлено оцінки рівномірності для R-схеми, цей пробіл буде усунено у другому розділі цієї роботи. Також повернемося до оцінки рівномірності декількох раундів MISTY.

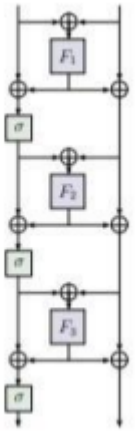

Рисунок 1.7 – 3х-раундова схема Лая-Мессі

Висновки до розділу 1

Отже, у першому розділі були розглянуті основні теоретичні відомості, що стосуються атаки бумерангів, таблиці бумерангової зв'язності для SPN шифів та її аналогу для шифрів на основі схеми Фейстеля, таблиці фейстелевої бумерангової зв'язності. Наведено основні визначення, властивості даних таблиць та їх порівняння. Також розглянуто поняття бумерангової рівномірності і її нижні оцінки для деяких фейстель-подібних схем.

2 ПАРАМЕТРИ СТІЙКОСТІ ДЛЯ СХЕМИ MISTY ТА R-СХЕМИ ДО АТАКИ БУМЕРАНГІВ

У даній частині буде розглянуто атаку бумерангів на фейстель-подібні шифри. Буде проведен аналіз параметрів стійкості для одного та двох раундів схеми MISTY, R-схеми до атаки бумерангів через відповідні параметри S-блоків та виявлення їх зв'язку вже з відомим для нас парамтерамом BCT. Також Частина результатів, які будуть викладатися надалі, була оприлюднена у [9].

2.1 Параметри стійкості 1-раундової та 2-раундової MISTY

Розглянемо схему MISTY із блоком довжини n, де n парне. Будемо позначати через Φ один раунд схеми MISTY, а внутрішнє перетворення через F. Тоді параметр BCT одного раунду схеми MISTY буде виражатися згідно наступного твердження.

Твердження 2.1.

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F}[\beta_L;\gamma_L \oplus \gamma_R] \cdot 2^{n/2}.$$

Доведення. Нехай на вхід подаються повідомлення, блоки яких поділені на праву та ліву частини:

$$\begin{aligned} M_1 &= (x_L, x_R), \\ M_2 &= (x_L \oplus \beta_L, x_R \oplus \beta_R), \\ M_1' &= (x_L', x_R'), \\ M_2' &= (x_L' \oplus \beta_L, x_R' \oplus \beta_R), \end{aligned}$$

де β_L – різниця між лівими частинами блоків повідомлень, а β_R – між правими. Різниця між зашифрованими лівими частинами – γ_L, правими –

γ_R. Розглянемо атаку бумеранга на схему MISTY для повідомлень M_1, M_2, M'_1, M'_2 (див. Рисунок 2.1). Отримаємо систему рівнянь:

$$\begin{cases} \gamma_L = x_R \oplus x'_R, \\ \gamma_R = x_R \oplus F(x_L) \oplus x'_R \oplus F(x'_L), \\ \gamma_L = x_R \oplus \beta_R \oplus x'_R \oplus \beta_R, \\ \gamma_R = x_R \oplus \beta_R \oplus x'_R \oplus \beta_R \oplus F(x_L \oplus \beta_L) \\ \qquad\qquad\qquad\qquad \oplus F(x'_L \oplus \beta_L). \end{cases}$$

Перше та третє рівняння системи тотожньо рівні. У другому та четвертому

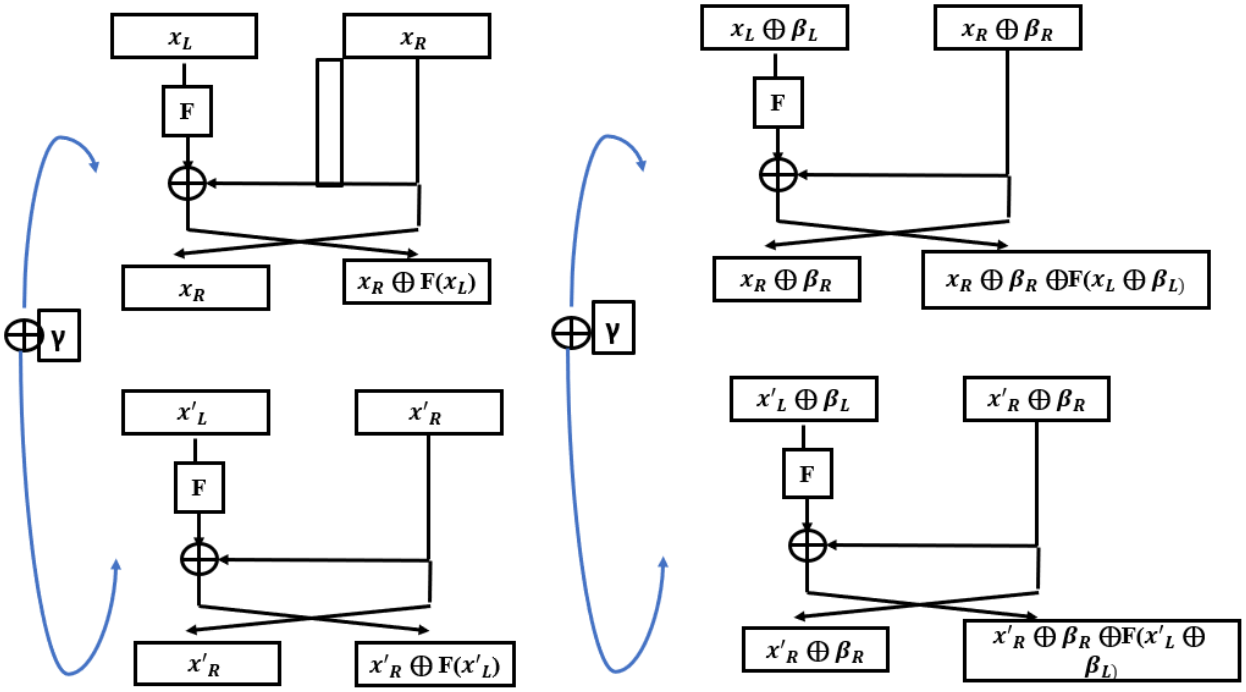

Рисунок 2.1 – Атака бумерангів на схему MISTY

рівняннях замість $x_R \oplus x'_R$ підставляємо γ_L та окремо розглядаємо систему з цих двох рівнянь:

$$\begin{cases} \gamma_L \oplus \gamma_R = F(x_L) \oplus F(x'_L), \\ \gamma_L \oplus \gamma_R = F(x_L \oplus \beta_L) \oplus F(x'_L \oplus \beta_L) \end{cases}$$

Позначимо $\gamma_L \oplus \gamma_R$ як $\Delta\gamma$. Виразимо x'_L з першого рівняння та $x'_L \oplus \beta_L$

з другого:

$$\begin{cases} x'_L = F^{-1}(F(x_L) \oplus \Delta\gamma), \\ x'_L \oplus \beta_L = F^{-1}(F(x_L \oplus \beta_L) \oplus \Delta\gamma). \end{cases}$$

Робимо $\oplus$ останніх двох рівнянь та отримуємо співвідношення:

$$F^{-1}(F(x_L) \oplus \Delta\gamma) \oplus F^{-1}(F(x_L \oplus \beta_L) \oplus \Delta\gamma) = \beta_L. \tag{2.1}$$

Значення x_R не впливає на розв'язок системи та може бути довільним. Неважко помітити, що (2.1) має вид BCT. Звідки маємо:

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F}[\beta_L;\gamma_L \oplus \gamma_R] \cdot 2^{n/2},$$

де BCT^F вказує на кількість усіх розв'язків x_L, а $2^{n/2}$ — на кількість усіх розв'язків x_R. Твердження доведено. □

Параметр стійкості 2-раундової MISTY так само виражається через BCT.

Твердження 2.2.

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F_2}[\beta_R;\gamma_L \oplus \gamma_R] \cdot 2^{n/2},$$

де F_2 – внутрішнє перетворення другого раунду.

Доведення. Це твердження доводиться аналогічно до твердження 2.1. Через F_1 позначимо функцію першого раунду, а через F_2 функцію другого раунду. Після атаки бумеранга на два раунди схеми MISTY отримаємо систему рівнянь.

$$\begin{cases} \gamma_L = x_R \oplus F_1(x_L) \oplus x'_R \oplus F_1(x'_L), \\ \gamma_R = x_R \oplus F_1(x_L) \oplus F_2(x_R) \oplus x'_R \oplus F_1(x'_L) \oplus F_2(x'_R), \\ \gamma_L = x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L) \oplus x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L), \\ \gamma_R = x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L) \oplus F_2(x_R \oplus \beta_R) \oplus \\ \qquad\qquad\qquad\qquad x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L) \oplus F_2(x'_R \oplus \beta_R). \end{cases}$$

Бачимо, що друге рівняння містить у собі перше рівняння, а четверте містить у собі третє. Після відповідних замін система зменшеться до двох рівнянь.

$$\begin{cases} F_2(x_R) \oplus F_2(x'_R) = \gamma_L \oplus \gamma_R, \\ F_2(x_R \oplus \beta_R) \oplus F_2(x'_R \oplus \beta_R) = \gamma_L \oplus \gamma_R. \end{cases}$$

Виразимо x'_R з першого рівняння та $x'_R \oplus \beta_R$ з другого:

$$\begin{cases} x'_R = F_2^{-1}(F_2(x_R) \oplus \gamma_R \oplus \gamma_L), \\ x'_R \oplus \beta_R = F_2^{-1}(F_2(x_R \oplus \beta_R) \oplus \gamma_R \oplus \gamma_L) \end{cases}$$

Робимо $\oplus$ останніх двох рівнянь й отримаємо співвідношення:

$$\beta_R = F_2^{-1}(F_2(x_R) \oplus \gamma_R \oplus \gamma_L) \oplus F_2^{-1}(F_2(x_R \oplus \beta_R) \oplus \gamma_R \oplus \gamma_L).$$

Простежуємо закономірність з рівнянням для таблиці бумерангової зв'язності та у результаті маємо такий вираз:

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F_2}[\beta_R;\gamma_L \oplus \gamma_R] \cdot 2^{n/2}.$$

Вираз BCT^{F_2} вказує на кількість усіх розв'язків x_L, а $2^{n/2}$ — на кількість усіх розв'язків x_R. Твердження доведено. □

2.2 Параметри стійкості 1-раундової й 2-раундової R-схеми

Аналогічні результати для параметрів стікойсті мають місце і для R-схеми. Для одного раунду розглядаємої схеми виведено наступне твердження.

Твердження 2.3.

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F}[\beta_L;\gamma_R] \cdot 2^{n/2}.$$

Доведення. Подібно попереднім доказам для схеми MISTY розглянемо атаку бумеранга на R-схему для повідомлень M_1, M_2, M'_1, M'_2

з тими ж різницями (див. Рисунок 2.2). У результаті отримаємо систему рівнянь:

$$\begin{cases} \gamma_L = x_R \oplus F(x_L) \oplus x'_R \oplus F(x'_L), \\ \gamma_R = F(x_L) \oplus F(x'_L), \\ \gamma_R = F(x_L \oplus \beta_L) \oplus F(x'_L \oplus \beta_L), \\ \gamma_L = x_R \oplus \beta_R \oplus F(x_L \oplus \beta_L) \oplus \\ \qquad x'_R \oplus \beta_R \oplus F(x'_L \oplus \beta_L). \end{cases}$$

Якщо виразити $x_R \oplus x'_R$ з першого рівняння системи і підставити у

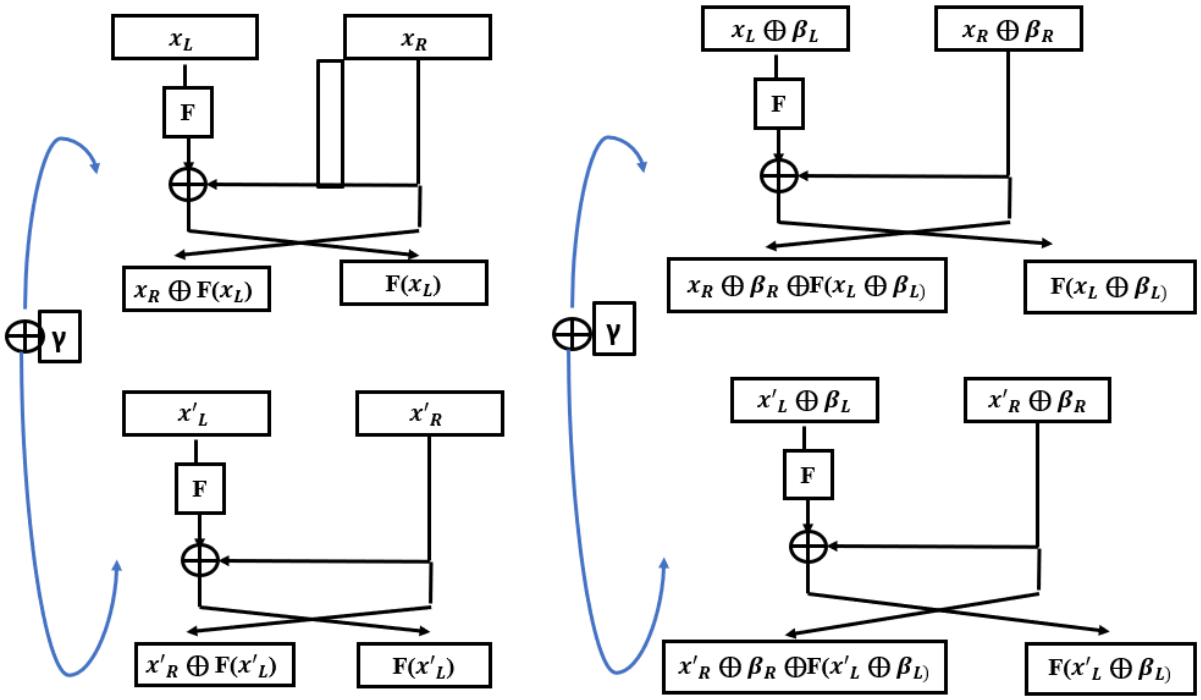

Рисунок 2.2 – Атака бумерангів на R-схему

четверте, то воно зведеться до рівності другого та третього. Тому розглянемо окремо друге та третє рівняння:

$$\begin{cases} \gamma_R = F(x_L) \oplus F(x'_L), \\ \gamma_R = F(x_L \oplus \beta_L) \oplus F(x'_L \oplus \beta_L). \end{cases}$$

Отримуємо вирази для x'_L та $x'_L \oplus \beta_L$:

$$\begin{cases} x'_L = F^{-1}(F(x_L) \oplus \gamma_R), \\ x'_L \oplus \beta_L = F^{-1}(F(x_L \oplus \beta_L) \oplus \gamma_R). \end{cases}$$

Складаємо ці два рівняння. Унаслідок маємо:

$$F^{-1}(F(x_L) \oplus \gamma_R) \oplus F^{-1}(F(x_L \oplus \beta_L) \oplus \gamma_R) = \beta_L.$$

Останнє співвідношення порівнюємо з BCT, як це було зроблено для схеми MISTY, і отримуємо:

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F}[\beta_L;\gamma_R] \cdot 2^{n/2}.$$

де BCT^F вказує на кількість усіх розв'язків x_L, а $2^{n/2}$ — на кількість усіх розв'язків x_R. Твердження доведено. □

Перейдемо до параметра стійкості до атаки бумерангів 2-раундової R-схеми.

Твердження 2.4.

$$BCT^{\Phi}[\beta;\gamma] = BCT^{F_1}[\beta_L;\gamma_L \oplus \gamma_R] \cdot 2^{n/2}.$$

Доведення. Після застосування атаки маємо:

$$\begin{cases} \gamma_L = F_1(x_L) \oplus F_2(x_R \oplus F_1(x_L)) \oplus F_1(x'_L) \oplus F_2(x'_R \oplus F_1(x'_L)), \\ \gamma_R = F_2(x_R \oplus F_1(x_L)) \oplus F_2(x'_R \oplus F_1(x'_L)), \\ \gamma_L = F_1(x_L \oplus \beta_L) \oplus F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \\ \quad \oplus F_1(x'_L \oplus \beta_L) \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L)), \\ \gamma_R = F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L)) \end{cases}$$

Підставляємо γ_R замість $F_2(x_R \oplus F_1(x_L)) \oplus F_2(x'_R \oplus F_1(x'_L))$ у перше рівняння та замість $F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L))$ – γ_L у третє

$$\begin{cases} \gamma_L = F_1(x_L) \oplus F_1(x'_L) \oplus \gamma_R, \\ \gamma_L = F_1(x_L \oplus \beta_L) \oplus F_1(x'_L \oplus \beta_L) \oplus \gamma_R. \end{cases}$$

$$\begin{cases} x'_L = F_1^{-1}(F_1(x_L) \oplus \gamma_R \oplus \gamma_L), \\ x'_L \oplus \beta_L = F_1^{-1}(F_1(x_L \oplus \beta_R) \oplus \gamma_R \oplus \gamma_L) \end{cases}$$

Складаємо останні два рівняння і отримаємо нове співвідношення:

$$\beta_L = F_1^{-1}(F_1(x_L) \oplus \gamma_R \oplus \gamma_L) \oplus F_1^{-1}(F_1(x_L \oplus \beta_L) \oplus \gamma_R \oplus \gamma_L).$$

Знов таки можемо переписати отриманий вираз через BCT.

$$BCT^{\Phi}[\beta; \gamma] = BCT^{F_1}[\beta_L; \gamma_L \oplus \gamma_R] \cdot 2^{n/2}.$$

Твердження доведено. □

2.3 Атака бумерангів на 3-раундові R-схему, MISTY

Застосувавши атаку бмерангів для 3-раундові MISTY, отримаємо

$$\begin{cases} \gamma_L = x_R \oplus F_1(x_L) \oplus F_2(x_R) \oplus x'_R \oplus F_1(x'_L) \oplus F_2(x'_R), \\ \gamma_R = x_R \oplus F_1(x_L) \oplus F_2(x_R) \oplus F_3(x_R \oplus F_1 x_L \oplus \\ \qquad\qquad x'_R \oplus F(x'_L) \oplus F(x'_R) \oplus F_3(x'_R \oplus F_1 x'_L), \\ \gamma_L = x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L) \oplus F_2(x_R \oplus \beta_R) \oplus \\ \qquad\qquad x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L) \oplus F_2(x'_R \oplus \beta_R), \\ \gamma_R = x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L) \oplus F_2(x_R \oplus \beta_R) \oplus F_3(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \\ \qquad x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L) \oplus F_2(x'_R \oplus \beta_R) \oplus F_3(x'_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L). \end{cases}$$

Знов таки система з чотирьох рівнянь зводиться до двох, бо перше рівняння міститься у другому. а третє – у четвертому.

$$\begin{cases} F_3(x_R \oplus F_1(x_L)) \oplus F_3(x'_R \oplus F_1(x'_L)) = \gamma_L \oplus \gamma_R, \\ F(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \oplus F(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L)) = \gamma_L \oplus \gamma_R \end{cases}$$

Введемо заміну

$$\begin{aligned} \delta &= F_1(x_L \oplus \beta_L) \oplus F_1(x_L), \\ \delta' &= F_1(x'_L \oplus \beta_L) \oplus F_1(x'_L), \\ y &= x_R \oplus F_1(x_L), \\ y &= x'_R \oplus F_1(x'_L). \end{aligned}$$

Кількість $x_L = DDT^{F_1}[\beta_L, \delta]$, а кількість $x'_L = DDT^{F_1}[\beta_L, \delta']$, де DDT – це вже відомий для нас парметр, який можна обчислити.

Замість $F_1(x_L \oplus \beta_L)$ підставимо $F_1(x_L) \oplus \delta$, а замість $F_1(x'_L \oplus \beta_L)$ підставимо $F_1(x'_L) \oplus \delta'$.

$$\begin{cases} F_3(y) \oplus F_3(y') = \gamma_L \oplus \gamma_R, \\ F(x_R \oplus \beta_R \oplus \delta \oplus F_1(x_L)) \oplus F(x'_R \oplus \beta_R \oplus \delta' \oplus F_1(x'_L)) = \gamma_L \oplus \gamma_R \end{cases}$$

Робимо відповідні заміни на y,y' у другому рівнянні.

$$\begin{cases} F_3(y) \oplus F_3(y') = \gamma_L \oplus \gamma_R, \\ F_3(y \oplus \beta_R \oplus \delta) \oplus F_3(y' \oplus \beta_R \oplus \delta') = \gamma_L \oplus \gamma_R \end{cases}$$

Виражаємо y', $y' \oplus \beta_R$.

$$\begin{cases} y' = F_3^{-1}(\gamma_L \oplus \gamma_R \oplus F_3(y)), \\ y' \oplus \beta_R \oplus \delta' = F_3^{-1}(\gamma_L \oplus \gamma_R \oplus F_3(y \oplus \beta_R \oplus \delta)) \end{cases}$$

Застосовуємо виняткову диз'юнкцію для рівнянь останньої системи.

$$\beta_R \oplus \delta' = F_3^{-1}(\gamma_L \oplus \gamma_R \oplus F_3(y)) \oplus F_3^{-1}(\gamma_L \oplus \gamma_R \oplus F_3(y \oplus \beta_R \oplus \delta)). \quad (2.2)$$

2.2 має певну схожість з парметром для BCT, але однозначну заміну неможливо зробити.

Розглядаємо атаку бумерангів для 3-раундової R-схеми.

$$\begin{cases} \gamma_L = F_2(x_R \oplus F_1(x_L)) \oplus F_3(F_1(x_L) \oplus F_2(x_R \oplus F_1(x_L))) \\ \quad \oplus F_2(x'_R \oplus F_1(x'_L)) \oplus F_3(F'_1(x_L) \oplus F_2(x'_R \oplus F_1(x'_L))), \\ \gamma_R = F_3(F_1(x_L) \oplus F_2(x_R \oplus F_1(x_L))) \oplus F_3(F_1(x'_L) \oplus F_2(x'_R \oplus F_1(x'_L))) \\ \gamma_L = F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \oplus F_3(F_1(x_L \oplus \beta_L) \oplus \\ F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L))) \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L)) \oplus \\ F_3(F'_1(x_L \oplus \beta_L) \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L))), \\ \gamma_R = F_3(F_1(x_L \oplus \beta_L) \oplus F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L))) \oplus \\ \qquad F_3(F_1(x'_L \oplus \beta_L) \oplus F_2(x'_R \beta_R \oplus F_1(x'_L \oplus \beta_L))). \end{cases}$$

$$\begin{cases} F_2(x_R \oplus F_1(x_L)) \oplus F_2(x'_R \oplus F_1(x'_L)) = \gamma_L \oplus \gamma_R, \\ F_2(x_R \oplus \beta_R \oplus F_1(x_L \oplus \beta_L)) \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L \oplus \beta_L)) = \gamma_L \oplus \gamma_R, \end{cases}$$

Використовуємо заміну, яка була введена для 3-раундової схеми MISTY: y, y', δ, δ'.

$$\begin{cases} F_2(y) \oplus F_2(y') = \gamma_L \oplus \gamma_R, \\ F_2(x_R \oplus \beta_R \oplus F_1(x_L) \oplus \delta \oplus F_2(x'_R \oplus \beta_R \oplus F_1(x'_L) \oplus \delta') = \gamma_L \oplus \gamma_R, \end{cases}$$

$$\begin{cases} F_2(y) \oplus F_2(y') = \gamma_L \oplus \gamma_R, \\ F_2(y \oplus \beta_R \oplus \delta) \oplus F_2(y' \oplus \beta_R \oplus \delta') = \gamma_L \oplus \gamma_R. \end{cases}$$

Виражаємо $y', y' \oplus \beta_R$.

$$\begin{cases} y' = F_2^{-1}(\gamma_L \oplus \gamma_R \oplus F_2(y)), \\ y' \oplus \beta_R \oplus \delta' = F_2^{-1}(\gamma_L \oplus \gamma_R \oplus F_2(y \oplus \beta_R \oplus \delta)). \end{cases}$$

$$\beta_R \oplus \delta' = F_2^{-1}(\gamma_L \oplus \gamma_R \oplus F_2(y)) \oplus F_2^{-1}(\gamma_L \oplus \gamma_R \oplus F_2(y \oplus \beta_R \oplus \delta)) \quad (2.3)$$

Положимо $\gamma_L = \gamma_R$, тоді 2.3 можна перезаписати як

$$\beta_R \oplus \delta' = F_2^{-1}(F_2(y)) \oplus F_2^{-1}(F_2(y \oplus \beta_R \oplus \delta)) = y \oplus y \oplus \beta_R \oplus \delta.$$

Бачимо, що y та β_R скорочуються, тому

$$\delta = \delta'$$

Повернемося до нашої заміни для δ, δ'.

$$\begin{cases} \delta = F_1(x_L \oplus \beta_L) \oplus F_1(x_L), \\ \delta' = F_1(x'_L \oplus \beta_L) \oplus F_1(x'_L). \end{cases}$$

x_R скоротилося, тому вона не впливає на разрешимость рішення. Так як дельти рівні, то прирівнюємо їх і покладаємо, що $x'_L = x_L + \epsilon$

$$F_1(x_L \oplus \beta_L) \oplus F_1(x_L) \oplus F_1(x_L \oplus \epsilon \oplus \beta_L) \oplus F_1(x_L \oplus \epsilon) = 0. \quad (2.4)$$

2.4 має вигляд FBCT. З цього робимо висновок, що x_L належить FBCT. Оскільки, завжди існують такі значення β_L і ϵ, при яких FBCT приймає максимальне значення, ми можемо поставити їх у якості початкового бумеранга, який ми аналізуємо. У результаті отримаємо, що найбільша кількість $x_L = maxFBCT$. Тоді справидливе наступне твердження.

Твердження 2.5.

$$maxBCT_\Phi \geqslant maxFBCT^{F_1} \cdot 2^{n/2}.$$

2.4 Атака бумерангів на схему Лая-Мессі

Розглядаємо атаку бумеранга на схему Лая-Мессі. По-перше, встановимо, що σ лінійна, тобто

$$\sigma(A \oplus B) = \sigma(A) \oplus \sigma(B).$$

На вхід подаються два повідомлення з блоками однакої довжини, які мають відповідні різниці між блоками β_L, β_R.

$$\begin{aligned} M_1 &= (x_L,x_R), \\ M_2 &= (x_L \oplus \beta_L, x_R \oplus \beta_R). \end{aligned}$$

Після одного раунду шифрування отримаємо зашифровані поввідомелння, які позначемо через M_1', M_2'.

$$M_1' = \sigma(x_L \oplus F(x_L \oplus x_R)), x_R \oplus F(x_L \oplus x_R)),$$
$$M_2' = \sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R)), x_R \oplus \beta_R \oplus F(x_L \oplus x_R \oplus \beta_R)).$$

Скадаємо відповідні частини зашифрованих повідомлень з різницями γ_L, γ_R.

$$M_1' \oplus \gamma = \sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L, x_R \oplus (x_L \oplus x_R)) \oplus \gamma_R,$$
$$M_2' \oplus \gamma = \sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R)) \oplus \gamma_L, x_R \oplus \beta_R \oplus$$
$$\oplus F(x_L \oplus x_R \oplus \beta_R)) \oplus \gamma_R).$$

Тепер разшифровуємо

$$E^{-1}(M_1' \oplus \gamma) = \sigma^{-1}(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L, x_R \oplus F(x_L \oplus x_R)) \oplus \gamma_R,$$
$$E^{-1}(M_2' \oplus \gamma) = \sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R)) \oplus \gamma_L, x_R \oplus \beta_R \oplus \gamma_R \oplus$$
$$\oplus F(x_L \oplus x_R \oplus \beta_R))).$$

Згідно схемі атаки бумеранга різниця між лівими частинами разширофаних повідомелнь буде дорівнювати β_L, а між правими β_R. Спочатку розглянемо суму лівих частин. Будемо покроково розкривати дужки, використовуючи лінійність ортоморфізма.

$$\sigma^{-1}(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R \oplus$$
$$\oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus \sigma^{-1}(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus$$
$$\oplus F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R \oplus$$
$$\oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)) =$$
$$= \mathrm{x}_L \oplus F(x_L \oplus x_R) \oplus \sigma^{-1}(\gamma_L) \oplus \sigma^{-1}(F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R \oplus$$
$$\oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \oplus\sigma^{-1}(\gamma_L) \oplus$$
$$\oplus\sigma^{-1}(F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R \oplus F(x_L \oplus$$
$$\oplus\beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)) =$$
$$= \beta_L \oplus F(x_L \oplus x_R) \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \sigma^{-1}(F(\sigma(x_L \oplus F(x_L \oplus x_R))$$
$$\oplus\gamma_L \oplus x_R \oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus \sigma^{-1}(F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)$$
$$\oplus\gamma_L \oplus x_R \oplus \beta_R \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)).$$

Цей вираз буде дорівнювати β_L, якщо

$$F(x_L \oplus x_R) \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \sigma^{-1}(F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R$$
$$\oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus \sigma^{-1}(F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R$$
$$\oplus\beta_R \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)) = 0$$

Тепер робимо $\oplus$ для правих частин разшифрованих повідомелень.

$$x_R \oplus F(x_L \oplus x_R) \oplus \gamma_R \oplus F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R \oplus F(x_L \oplus x_R) \oplus \gamma_R))$$

$$\oplus x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_L \oplus F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)$$

$\oplus\gamma_L \oplus x_R \oplus \beta_R \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)) =$

$= \beta_R \oplus F(x_L \oplus x_R) \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L$

$\oplus x_R \oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R$

$\oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)).$

Цей вираз буде дорівнювати β_R, якщо

$$F(x_L \oplus x_R) \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R$$
$$\oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R$$
$$\oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)) = 0$$

Обидві умови дорівнюють нулеві, тому прирівняємо їх один до одного.

$$\sigma^{-1}(F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R \oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus$$
$$\sigma^{-1}(F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R))$$
$$\oplus F(\sigma(x_L \oplus F(x_L \oplus x_R)) \oplus \gamma_L \oplus x_R \oplus F(x_L \oplus x_R) \oplus \gamma_R)) \oplus F(\sigma(x_L \oplus \beta_L \oplus$$
$$F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R) \oplus F(x_L \oplus \beta_L \oplus x_R \oplus \beta_R) \oplus \gamma_R)) = 0$$

Для спрощення вигляду останнього виразу, введомо $y = x_R \oplus x_L$

$$\sigma^{-1}(F(\sigma(x_L \oplus F(y)) \oplus \gamma_L \oplus x_R \oplus F(y) \oplus \gamma_R)) \oplus \sigma^{-1}(F(\sigma(x_L \oplus \beta_L \oplus F(y \oplus \beta_L$$
$$\oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R \oplus F(y \oplus \beta_L \oplus \beta_R) \oplus \gamma_R)) \oplus F(\sigma(x_L \oplus F(y)) \oplus \gamma_L \oplus x_R$$
$$\oplus F(y) \oplus \gamma_R)) \oplus F(\sigma(x_L \oplus \beta_L \oplus F(x_L \oplus \beta_L \oplus \oplus x_R \oplus \beta_R)) \oplus \gamma_L \oplus x_R \oplus \beta_R) \oplus$$
$$\oplus F(y \oplus \beta_L \oplus \beta_R) \oplus \gamma_R)) = 0$$

На жаль, по останньому виразу неможливо зробити висновок на рахунок оцінкі стікойсті схеми Лая-Месіі та її зв'язку з параметром BCT або FBCT. Але отримане рівняння можна буде використовувати у майбутньому для уточнення властивостей або аналізу S-блоків на основі схеми Лая-Мессі.

Висновки до розділу 2

У даному розділі було розглянуто атаку бумерангів на S-блоки 1-го, 2-х раундів шифрування R-схеми та схеми MISTY. Виведені параметри стійкості для цих схем до атаки бумерангів та виявлено їх співвідношення з таблицею бумерангової зв'язності. Показано, що і для схеми MISTY, і для R-схеми параметри стійкості до атак бумерангів виражаються через відомий параметр бумерангової зв'язності внутрішніх перетворень. Також було уточнено аналітичну оцінку для нижньої границі рівномірності бумерангу для 3-раундової R-схеми та виведені співвідношення для 3-раундові схеми MISTY та 1-раундової схеми Лая-Мессі, які можуть буди використані для подальшого аналізу стійкості фейстель-подібних схем.

ВИСНОВКИ

У ході даної роботи був проведений аналіз опублікованих джерел за тематикою дослідження, який показав, що параметри стійкості до фейстель-подібних схем або щє не виведені, або потребують уточнення. Тому у цій роботі розглядалися S-блоки, які мають структуру одного або декількох раундів R-схеми, MISTY, схеми Лая-Мессі блокового шифрування.

Для конструкцій 1-раундової, 2-раундової R-схеми та MISTY були виведині точні оцінки та виявлено їх співвідношення вже с існуючим парметром BCT. Отримані результати показали, що для даних схем шифрування не потрібно вводити нові параметри, як це було зроблено для мережі Фейстеля. Виведені твердження вказують на те, що значення максимуму BCT для цих схем буде достатньо високим. Це свідчить про те, що шифри на основі представлених конструкцій можуть бути менш стійкими до атаки бумерангів. Більш того, можна помітити, що на параметр стійкості 2-раундової R-схеми буде впливати лише внутрішня функція першого раунду, а на параметри 2-раундової MISTY функція другого раунду. Отже, при побудові шифрів на цих схемах треба ретельно обирати зазначині раундові функції.

Також був проведен аналіз 3-раундових R-схеми, MISTY та одного раунду схеми Лая-Мессі. Під час якого отримано нижню оцінку для R-схеми. Виявилося, що дана оцінка залежить від FBCT, при умові, коли вихідні різниці однакові.

Результати роботи можуть бути використані для поширеного аналізу шифрів, S-блоки яких засновані на фейстель-подібних схемах, вивчення їх властивостей та побудови нових конструкцій, які будуть стійкими до атаки бумерангів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Eli Biham and Adi Shamir. Differential Cryptanalysis of the Data Encryption Standard. Berlin, Heidelberg: Springer-Verlag, 1993. isbn: 0387979301.

2. Serge Vaudenay (February 1998). Provable Security for Block Ciphers by Decorrelation (PostScript). 15th Annual Symposium on Theoretical Aspects of Computer Science (STACS '98). Paris: Springer-Verlag. pp. 249–275. Retrieved 26 February 2007.

3. David Wagner. "The Boomerang Attack". In: Fast Software Encryption. Ed. by Lars Knudsen. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 156–170. isbn: 978-3-540-48519-3.

4. Sean Murphy. The return of the cryptographic boomerang. IEEE Trans. Information Theory, 57(4):2517–2521, 2011

5. Alex Biryukov, Dmitry Khovratovich. Related-key Cryptanalysis of the Full AES-192 and AES-256

6. Carlos Cid et al. Boomerang Connectivity Table: A New Cryptanalysis Tool. Cryptology ePrint Archive, Report 2018/161. https://eprint.iacr.org/2018/ 161. 2018.

7. Shizhu Tian, Christina Boura, and L´eo Perrin. Boomerang Uniformity of Popular S-box Constructions. Cryptology ePrint Archive, Report 2019/1002.

8. Boukerrou, H., Huynh, P., Lallemand, V., Mandal, B., Minier, M. (2020). On the Feistel Counterpart of the Boomerang Connectivity Table: Introduction and Analysis of the FBCT. IACR Transactions on Symmetric Cryptology, 2020(1), 331-362.

9. Мітрофанова Е.В "Бумерангова зв'язність S-блоків зі структурою R-схеми блокового шифрування". In: Теоретичні і прикладні проблеми фізики, математики та інформатики. Київ : КПІ ім. Ігоря Сікорського: Видавництво «Політехніка», 2020, pp. 228–229. isbn: 978-966-622.

10. Mitsuru Matsui. “New block encryption algorithm MISTY”. In: Fast Software Encryption. Ed. by Eli Biham. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 54–68. isbn: 978-3-540-69243-0.

11. Vaudenay S. On the lai-massey scheme //International Conference on the Theory and Application of Cryptology and Information Security.Springer, Berlin, Heidelberg, 1999. P. 8-19.