НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___”_____20 _ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки : 113 «Прикладна математика»
(код і назва)

на тему: Криптографічні властивості S-блоків, які характеризують стійкість до атак бумерангів.

Виконав: студент __4__курсу, групи ФІ-62
(шифр групи)

Власенко Назар Миколайович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник Яковлєв Сергій Володимирович, к. т. н., доцент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут

Кафедра математичних методів захисту інформації

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки - 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою

М.М.Савчук

_____
(підпис) (ініціали, прізвище)

«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту

Власенко Назар Миколайович
(прізвище, ім'я, по батькові)

1. Тема роботи Криптографічні властивості S-блоків, які характеризують стійкість до атак бумерангу,
керівник роботи Яковлєв Сергій Володимирович, к. т. н., доцент ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____ р. № _____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____

4. Зміст роботи дослідження поведінки параметрів S-блоків, які характеризують стійкість до атак бумерангів. _____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____
_____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Узгодження теми дипломної роботи з керівником	01.09. – 01.10.	
2	Пошук та опрацювання інформації сумісної до теми диплому	01.10. – 01.12.	
3	Отримання нижніх оцінок рівномірності бумерангу для 2-раундової R-схеми	01.12. – 01.01.	
4	Експериментальна перевірка отриманих оцінок	01.01. – 10.03.	
5	Експериментальна перевірка розподілу значень елементів BCT	10.03. – 15.05.	
6	Оформлення роботи	15.05. – 04.06.	

Студент _____ Власенко Н.М.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Яковлєв С.В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Кваліфікаційна робота містить: 40 стор., 12 рисунків, 3 таблиці, 11 джерел.

Метою цього дослідження є уточнення моделей та методів криптоаналізу блокових шифрів, що дозволить розширити уявлення про використання базових криптографічних конструкцій для внесення нелінійності при проєктуванні нових шифрів та оцінити наслідки їх використання з точки зору стійкості до атак бумерангів. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є атаки бумерангів і параметри стійкості шифрів до цих атак.

У даній роботі було отримано та експериментально перевірено нижні оцінки для рівномірності бумерангу для S-блоків, які мають структуру R-схеми блокового шифрування. Також було експериментально перевірено розподіл коефіцієнтів таблиці бумерангової зв'язності для 8-бітових S-блоків, показано коректність цього розподілу вже для S-блоків вказаного розміру.

R-СХЕМА, BCT, BOOMERANG CONNECTIVITY TABLE, АТАКА БУМЕРАНГІВ

ABSTRACT

The qualifying paper contains: 40 pages, 12 figures, 3 tables, 11 sources.

The purpose of this investigation is to refine the models and methods of cryptanalysis of block ciphers, which will expand the idea of using basic cryptographic structures to bring nonlinearity in the design of new ciphers and assess the consequences of their use in terms of resistance to boomerang attacks. The object of the research is information processes in cryptographic protection systems. The subject of the research is boomerang attacks and resistance parameters to these attacks.

In this paper, the lower estimates for boomerang uniformity for S-blocks having the structure of the R-scheme of block encryption were obtained and experimentally verified. The distribution of the boomerang connectivity table coefficients for 8-bit S-blocks was also experimentally checked, and the correctness of this distribution was already shown for S-blocks of the specified size.

R-SCHEME, BCT, BOOMERANG CONNECTIVITY TABLE, BOOMERANG ATTACK

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$\oplus$ — операція побітового додавання

DDT — таблиця розподілів диференціалів (Difference Distribution Table)

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

$\|$ — операція приєднання двох векторів

β_S — рівномірість бумерангу S-блоку S

$\mathbb{F}_2^n$ — множина всіх бітових векторів довжини n

$Bin(i; n, p)$ — ймовірність біноміально розподіленої випадкової величини з параметрами n та p прийняти значення i

ВСТУП

Актуальність дослідження. Розробка та дослідження криптосистем ведеться доволі давно. Як наслідок, при їх побудові виникає потреба одержання певних оцінок стійкості до різного виду атак, аби точно стверджувати про доцільність використання тієї чи іншої криптосистеми. Незважаючи на доволі стрімкий розвиток криптографії й нині є напрямки, які слід розглянути більш детально. Одним з таких напрямків є аналіз стійкості криптосистем до атак бумерангів.

На початку 90-х років минулого століття Біхам та Шамір запропонували новий вид криптоаналізу на прикладі шифру DES[1]. На сьогодні відомо багато різноманітних технік диференціального криптоаналізу. Однією з таких є атака бумерангів [2], в основі якої лежить використання квартетів відкритих текстів та відповідних їм шифртекстів, а не пари, як це відбувається в класичному диференціальному аналізі.

Для внесення нелінійності при побудові блокових шифрів зазвичай використовують S-блоки. У цій роботі буде розглянуто випадок, коли таким S-блоком є 2-раундова R-схема, та зроблено висновки про доцільність використання цієї конструкції при побудові нових блокових шифрів з точки зору стійкості до атак бумерангів на основі одержаної нижньої оцінки бумерангової рівномірності для S-блоків, які мають зазначену структуру.

Метою дослідження є уточнення моделей та методів криптоаналізу блокових шифрів, що дозволить розширити уявлення про використання базових криптографічних конструкцій для внесення нелінійності при проєктуванні нових шифрів та оцінити наслідки їх використання з точки зору стійкості до атак бумерангів.

Задачею дослідження є дослідження поведінки параметрів S-блоків, які характеризують стійкість до атак бумерангів. Для

розв'язання задачі необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) побудувати аналітичні оцінки для значень «бумерангової» рівномірності для S-блоків, які мають структуру R-схеми блокового шифрування;

3) експериментально перевірити розбіжність між аналітичними оцінками та справжніми значеннями «бумерангової» рівномірності для S-блоків із різними алгебраїчними структурами;

4) перевірити гіпотезу про розподіл значень елементів таблиць бумерангової зв'язності на випадкових S-блоках.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є атаки бумерангів і параметри стійкості шифрів до цих атак.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи теорії імовірностей, математичної статистики, комбінаторного аналізу.

Наукова новизна отриманих результатів полягає у наступному:
1) вперше отримано аналітичні оцінки рівномірності бумерангу для 2-раундової збалансованої та незбалансованої R-схеми;
2) експериментально підтверджено, що одержаний в опублікованих джерелах розподіл значень елементів таблиці бумерангової зв'язності вже для S-блоків маленького розміру.

Практичне значення: одержані у роботі результати можна використовувати для створення нових та аналізу існуючих симетричних криптопримітивів.

Апробація результатів та публікації. Частину результатів даної роботи було доповідано на XVIII Науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики» (12-13 травня 2020 року, м.Київ).

1 АТАКА БУМЕРАНГІВ І ТАБЛИЦЯ БУМЕРАНГОВОЇ ЗВ'ЯЗНОСТІ

У даному розділі розглянуто основні поняття, які стосуються атаки бумерангів та новітнього інструменту для їх аналізу, так званої *таблиці бумерангової зв'язності* (Boomerang Connectivity Table, BCT).

1.1 Модель ітеративного шифру та статистичні атаки на останній раунд

Нехай X – множина відкритих текстів, Y – множина шифрованих текстів, K – ключовий простір, $\mathbb{F}_2^n = \{0,1\}^n$ – множина всіх n-бітових векторів. Тоді позначимо $f : X \times K \to Y$ – шифруюче перетворення таке, що:

(1) $\forall k \in K : \exists g : Y \times K \to X : \forall x \in X : g(f(x)) = x$;

(2) f - ефективно обчислюється.

У випадку, коли $X \equiv Y \equiv \{0,1\}^n$, будемо називати f блоковим шифром.

Нехай $F^{(1)}$, ... , $F^{(r)}$ – блокові шифри з однаковою множиною K. Тоді перетворення

$$E_k(x) = F_{k_r}^{(r)}(F_{k_{r-1}}^{(r-1)}(...(F_{k_1}^{(1)}(x)))),$$

де $k = (k_1, ..., k_r)$, будемо називати r-раундовим ітеративним блоковим шифром. Слід зазначити, що всюди надалі будемо вважати, що раундові ключі k_1, ... , k_r обираються випадково, рівномірно та незалежно один від одного. На Рис. 1.1 можемо спостерігати як виглядає ітеративний шифр із r раундів.

Оскільки блокові шифри не є випадковими перетвореннями, то завжди будуть існувати статистики, які матимуть розподіл відмінний від рівномірного. Якщо знайдено певну особливість, виражену у статистичній

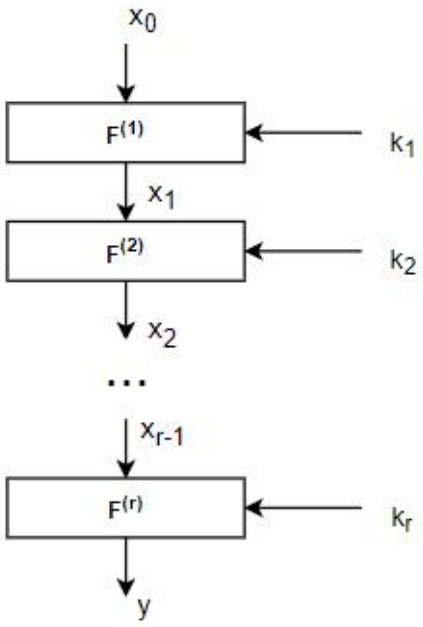

Рисунок 1.1 – r-раундовий ітеративний шифр

формі, розподіл якої відрізняється від рівномірного, то можна оцінити яким буде розподіл при умові, що значення ключа останнього раунду було вгадано вірно або ні. Звичайно, в першу чергу потрібно накопичити певну кількість відкритих текстів та відповідних їм шифрованих текстів. Розглянемо загальну схему статистичної атаки на ключ останнього раунду.

1. Знайти статистику $R_r(x, y)$, розподіл якої відрізняється від рівномірного. Як бачимо, вона залежить від кількості раундів.
2. Накопичити N пар (x, y) таких, що: $y = E_k(x)$, де k – фіксований, але невідомий.
3. Для кожного кандидата у k_r одержати x_{r-1} з y та обчислити вибірковий розподіл $\hat{R}_{r-1}(x, x_{r-1})$.
4. Якщо k_r вірне, то $\hat{R}_{r-1}$ відповідає R_{r-1}.

Зазначимо, що x_{r-1} на третьому кроці отримується завдяки розшифруванню y на ключі k_r на один раунд назад, тобто, якщо значення ключа вгадано вірно, то x_{r-1} отримано дійсно розшифруванням на один

раунд назад. Тоді вибірковий розподіл буде дорівнювати теоретичному. У випадку, якщо k_r обрано невірно, то фактично y було зашифровано на ще один раунд. Отже, маємо задачу розрізнення гіпотез, а саме задачу розрізнення розподілу $\hat{R}_{r-1}$ від рівномірного.

Зрозуміло, що з вибором ключа буде змінюватись і статистика, тобто для одного ключа статистика може мати один розподіл, а для іншого другий. Тому формулюється така гіпотеза.

Гіпотеза про еквівалентність ключів.

Майже для всіх k розподіли R_r несуттєво відрізняються.

Звідси маємо висновок, що замість того, щоб оцінювати розподіл R_r для всіх ключів, можна розглядати усереднений розподіл за всіма ключами.

Гіпотеза про рандомізацію значень.

Чим більше r, тим більше розподіл R_r наближається до рівномірного.

1.2 Атака бумерангів

Нехай $E_k(x) = E2_k(A_k(E1_k(x)))$, де $E1$, $E2$ – підшифри, A_k – афінне ключезалежне відображення. Будемо позначати через $D1$ та $D2$ розшифровуючі перетворення, які відповідають $E1$ та $E2$.

В атаці бумерангів шифр E розглядається як композиція двох підшифрів. Найважливішим у таких атаках є вибір підходящих характеристик для $E1$ та $E2$. Стандартне припущення полягає у тому, що такі характеристики можна обрати незалежно для $E1$ та $E2$. Хоча, як показав Мерфі, для шифрів на базі S-блоків дві незалежно обрані характеристики можуть бути несумісними, а отже, ймовірність генерування правильного квартету відкритих текстів може буті рівна нулеві.

Позначимо α, β, ϕ, $\gamma \in V_n$, де V_n – множина всіх n-бітових векторів.

Нехай також $\Pr\{\alpha \underset{E1}{\to} \beta\} = p_1$, $\Pr\{\beta \underset{D1}{\to} \alpha\} = p_2$, $\Pr\{\gamma \underset{D2}{\to} \phi\} = q$. Як

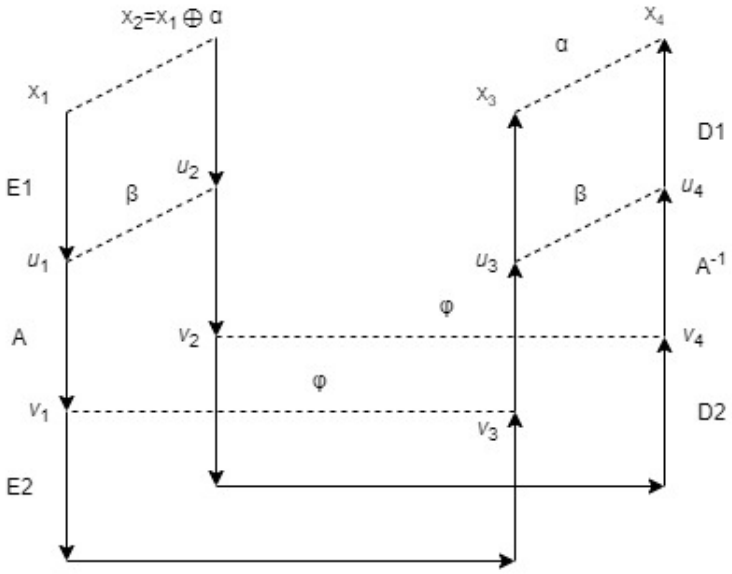

Рисунок 1.2 – Атака бумерангів

бачимо на Рис. 1.2, x_i – входи, $u_i = E1_k(x)$, $v_i = A_k(u_i)$, $y_i = E2_k(v_i)$. Після того, як були одержані y_1 та y_2, потрібно додати до них різницю γ. Постає питання про те, якою буде імовірність того, що x_3, x_4 (отримані внаслідок розшифрування відповідних y_i) також будуть мати різницю α. Легко бачити, що $u_1 \oplus u_2 = \beta$ з імовірністю p_1, $v_1 \oplus v_3 = \phi$ з імовірністю q, $v_2 \oplus v_4 = \phi$ з імовірністю q. Тоді, просумувавши всі v_i, отримаємо $v_1 \oplus v_2 \oplus v_3 \oplus v_4 = 0$. Далі має місце така лема.

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

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

то $u_1 \oplus u_2 \oplus u_3 \oplus u_4 = 0$.

Тоді $u_3 \oplus u_4 = \beta$, відповідно імовірність того, що x_3 та x_4 будуть мати різницю α, буде дорівнювати p_2.

Твердження 1.1 ([2],[3]). *Якщо всі події в позначеннях введених раніше є незалежними, то*

$$\Pr\{x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0\} = p_1 p_2 \hat{q},$$

де $\hat{q} = \sum_{\phi}(\Pr\{\gamma \underset{D2}{\to} \phi\} = q)$.

Необхідно зазначити, що атака працює, коли $p_1 p_2 \hat{q} >> \frac{1}{2^n}$, а E1 та E2 не повинні бути однаковими. Однак у даної атаки є суттєвий недолік, а саме, для проведення атаки потрібно вміти не лише шифрувати, але й розшифровувати.

1.3 Boomerang Connectivity Table

У роботі [4] автори запропонували поняття BCT та розглянули питання залежності двох характеристик у перетворенні A, коли воно представлене у вигляді одного S-блоку. Також ними було обговорено питання пошуку S-блоків з «хорошими» BCT. Перед тим як дати визначення BCT, слід визначити декілька інших понять.

Для n-бітового S-блоку $S : \{0,1\}^n \to \{0,1\}^n$, властивості для диференціального розподілу S зазвичай представляються у таблиці τ розміру $2^n \times 2^n$, яка називається *таблицею розподілів диференціалів* (Difference Distribution Table, DDT). Для довільних Δ_i, Δ_o значення

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

зберігається у відповідній комірці таблиці $\tau(\Delta_i, \Delta_o)$. Це значення показує, що вхідна різниця Δ_i розповсюджується до вихідної різниці Δ_o з імовірністю $\tau(\Delta_i, \Delta_o)/2^n$. Максимальне значення в такій таблиці (окрім першого рядка та стовпчика) називається диференціальною рівномірністю S-блока.

Для отримання диференціальних властивостей усього шифру слід

високоімовірнісних різниць шукається через ітерацію шифру, припускаючи, що S-блоки та інші операції на різних раундах поводяться незалежно. Однак у багатьох випадках може бути неможливо зробити це. Утім, коли так трапляється, атака бумерангів може бути застосована для отримання диференціальних властивостей різних сегментів шифру.

Як було зазначено, в атаці бумерангів шифруюче перетворення E є композицією двох підшифрів. Розглянемо випадок, коли вхідна різниця Δ_i визначена підшифром $E1$, а вихідна різниця ∇_0 підшифром $E2$. Тоді можна порахувати імовірність того, що для S-блоку S, для даної пари $(\Delta_i,\ \nabla_0)$, згенерується правильний квартет відкритих текстів. Вона обчислюється таким чином:

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

Тоді, подібно до DDT, можна оцінити такі імовірності для всіх пар $(\Delta_i,\ \nabla_0)$, записуючи отримані результати до таблиці.

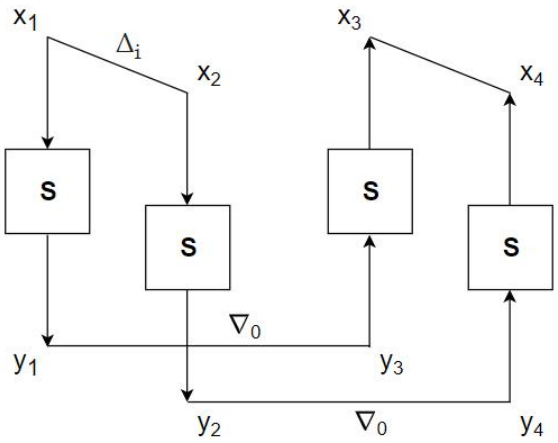

Рисунок 1.3 – Розповсюдження Δ_i до ∇_0

Таблиця, яка зберігає ці результати й називається таблицею бумерангової зв'язності (Boomerang Connectivity Table, BCT). Складність генерування такої таблиці для n-бітового S-блоку становить $O(2^{3n})$, що є більшим за $O(2^{2n})$ для DDT [4].

Зауваження. Максимальна ймовірність у BCT така ж, як і в DDT.

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 1.4 – DDT для s-блоку PRESENT

Автори приводять відмінність BCT від DDT на прикладі S-блоку блокового шифру PRESENT (див. Рис. 1.4 та Рис. 1.5). Визначимо *бумерангову рівномірність* S як максимальне значення $\beta_S(\Delta_i, \nabla_o)$ для нетривіальних значень Δ_i та ∇_o ($\Delta_i \neq 0$, $\nabla_o \neq 0$):

$$\beta_S = \max_{\Delta_i \neq 0, \nabla o \neq 0} \beta_S(\Delta i, \nabla_o).$$

Як і з однорідністю для таблиці розподілів диференціалів, чим менша бумерангова рівномірність, тим краще з точки зору стійкості шифру.

Однією з відмінностей BCT та DDT є те, що сумісність або несумісність різниці входу та різниці виходу визначається одразу ж (якщо відповідний запис у BCT дорівнює нулеві, то різниці несумісні, а отже, як було зазначено, ймовірність генерування правильного квартету також дорівнює нулеві). Варто зазначити, що неможливо однозначно перетворити BCT на DDT та навпаки.

BCT дає можливість більш коректно оцінити ймовірності

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 1.5 – BCT для s-блоку PRESENT

генерування правильного квартету відкритих текстів в атаках бумерангів. BCT корисно розглядати не лише як інструмент покращення атаки. При створенні нових блокових шифрів розглядається багато варіантів S-блоків, а BCT також дозволяє оцінити здатність S-блоку протистояти атакам бумерангу. Тому її можна застосовувати і при побудові нових шифрів.

1.4 Властивості BCT деяких відомих конструкцій

Для побудови великих S-блоків у криптографії часто використовують специфічні конструкції, наприклад схеми блокового шифрування маленького розміру без ключів. У [5] автори дослідили поведінку таких легковагових конструкцій у контексті атак бумерангу, оцінюючи рівномірності бумерангу для кожної з них. У дослідженні фігурують наступні конструкції: 3-раундова схема Фейстеля, 3-раундова схема Лая-Мессі та 3-раундова (збалансована та незбалансована)

MISTY (див. Рис.1.6).

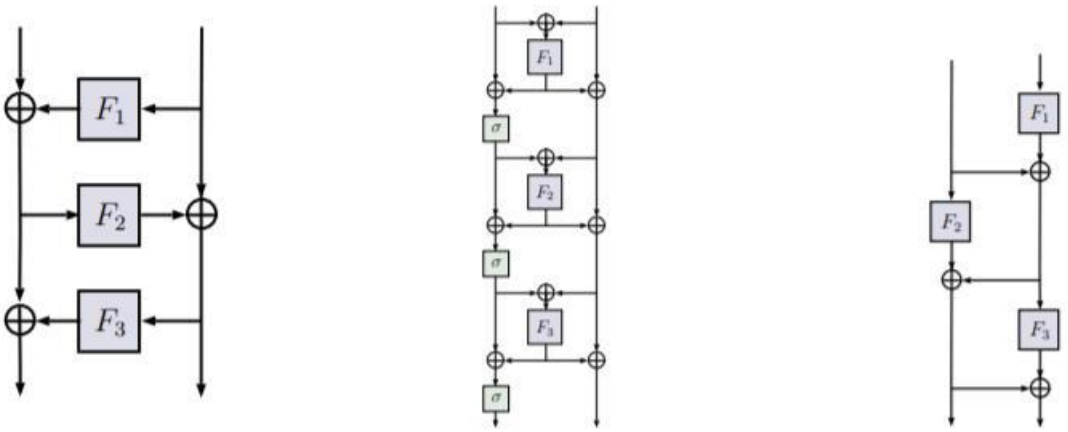

Рисунок 1.6 – Зліва направо: 3-раундова схема Фейстеля, 3-раундова схема Лая-Мессі та 3-раундова MISTY

Раніше шифри ZUC та Scream використовували S-блоки, які побудовані на основі схеми Фейстеля. У кожному з них вона мала 3-раундову структуру. Дослідження показали, що з усіх розглянутих у статті конструкцій, схема Фейстеля має найгіршу оцінку рівномірності бумерангу, відповідно і стійкість до атак бумерангів.

Нехай $F_1, F_3 : \mathbb{F}_2^m \to \mathbb{F}_2^n$ та $F_2 : \mathbb{F}_2^m \to \mathbb{F}_2^n$ – внутрішніх функції, тоді для будь-якого $b \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ було отримано значення рівномірності бумерангу: $\beta_S(b, b) = 2^{n+m}$, де $S : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n \times \mathbb{F}_2^m$ – 3-раундова схема Фейстеля. Щодо схеми Лая-Мессі, то була отримана оцінка: $\beta_S(a_1, b) = 2^{2n}$, де $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ – 3-раундова схема Лая-Мессі з внутрішніми функціями $F_1, F_2, F_3 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ та $a \in \mathbb{F}_2^n (a \neq 0), a_1 = (a, a), b = (\sigma(a), \sigma(b)) \in (F_2^n)^2$.

Хоча на практиці використовується переважно незбалансована MISTY, у зазначеному дослідженні окремо було розглянуто випадок із збалансованою схемою. Варто зазначити, що отримані результати стосуються оригінального шифру MISTY1 [6], а також 8-бітового S-блоку шифру Fantomas [7]. Отже, наведемо рівномірности бумерангу для наведених конструкцій.

Нехай $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ – 3-раундова збалансована мережа MISTY та нехай $F_1, F_2, F_3 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ – її внутрішні функції, які є бієктивними. Тоді рівномірність бумерангу обмежена знизу значенням: $\beta_S \geq 2^n \beta_{F_2}$. Як

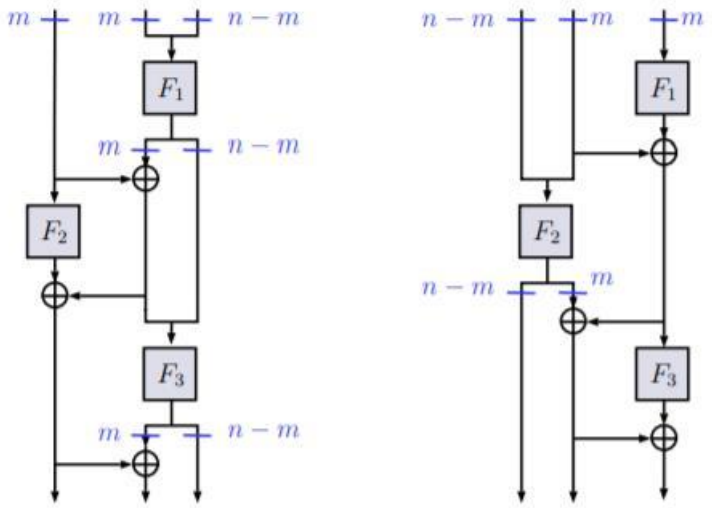

Рисунок 1.7 – Незбалансована мережа MISTY

бачимо, на нижню оцінку рівномірності впливає лише одна з трьох внутрішніх функцій, а саме функція другого раунду. Надалі ці висновки, отримані аналітичним шляхом, будуть перевірені у ході розв'язку задач, поставлених у даній роботі. Рівномірність бумерангу незбалансованої MISTY, зображеної на Рис.1.7, обмежена знизу значеннями $2^n \beta_{F_2}$ та $2^n \beta_{F_2|_{\mathbb{F}_2^m}}$ для випадку зліва та випадку справа відповідно.

Висновки до розділу 1

Отже, на сьогодні досліджені властивості деяких відомих конструкцій, які характеризують стійкість до атак бумерангів. Однак деякі результати залишаються не підтвердженими експериментально. Також є конструкції, властивості BCT яких є невідомими, що не дає змоги давати оцінку ефективності їх використання для побудови нових S-блоків. Однією з таких є R-схема, яку і буде розглянуто у даній роботі.

2 АНАЛІТИЧНІ ГРАНИЦІ РІВНОМІРНОСТІ БУМЕРАНГУ ДЛЯ R-СХЕМИ БЛОКОВОГО ШИФРУВАННЯ

У цьому розділі буде розглянуто 2-раундову R-схему у випадках, коли вона має збалансований та незбалансований вигляд, отримано нижні оцінки рівномірності бумерангу для S-блоків із зазначеною структурою. Це дозволить порівняти R-схему із вже дослідженими структурами та зробити висновки про її переваги та недоліки відносно них. Також отримані результати дадуть можливість оцінити чи є доцільним використання R-схеми для побудови нових S-блоків з точки зору стійкості до атак бумерангів. Частина результатів у даному розділі була доповідана у [8].

2.1 Оцінка рівномірності бумерангу для R-схеми

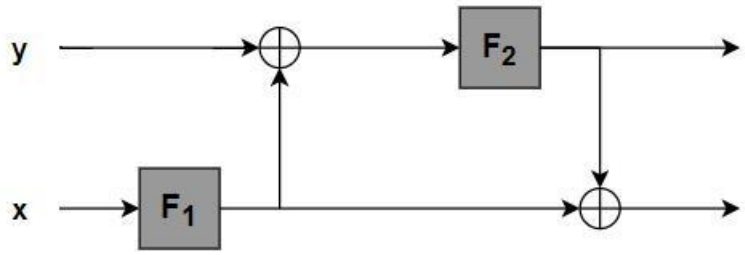

Рисунок 2.1 – 2-раундова R-схема

Нехай $R : \mathbb{F}_2^n \times \mathbb{F}_2^n$. R-схемою будемо називати таке відображення R, що для довільних $x \parallel y \in \mathbb{F}_2^n$ $R(x, y) = (F(x) \oplus y) \parallel F(x)$, де F – внутрішня функція. Далі досліджувалися випадки, коли R-схема має збалансований та незбалансований вигляд, тобто у першому варіанті x та y мають однаковий розмір (див. Рис. 2.1), у другому – різний (див Рис. 2.3).

Обидві внутрішні функції F_1, F_2 мають бути бієктивними, щоб уся конструкція була перестановкою. Як буде видно далі, нижня границя рівномірності бумерангу залежить від особливостей її внутрішніх підфункцій.

Нехай $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ – 2-раундова збалансована R-схема, та нехай $F_1, F_2 : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ – бієктивні відображення, які є внутрішніми функціями S. Тоді має місце така теорема.

Теорема 2.1. *Для бумерангової рівномірності введеного S-блоку S справедливе співвідношення:*

$$\beta_S \geq 2^n \beta_{F_1}.$$

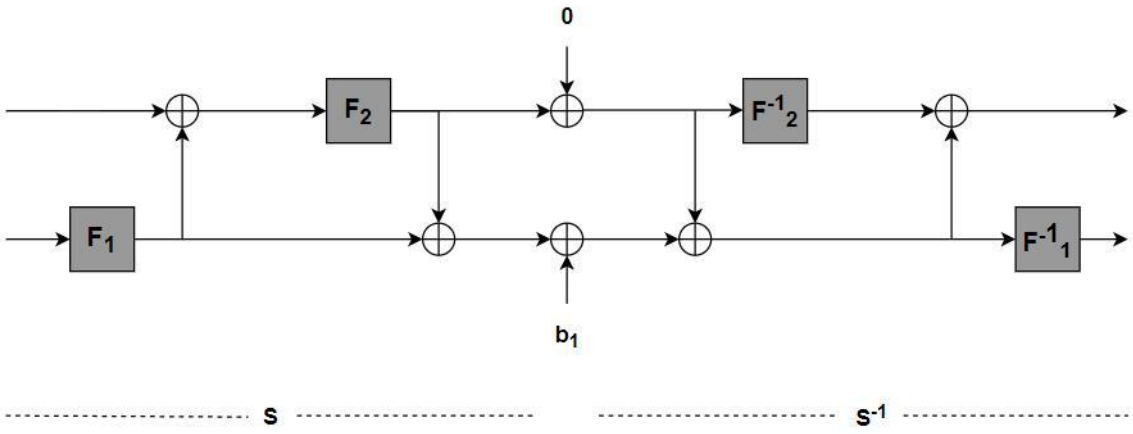

Рисунок 2.2 – Функція $S_b(x, y) = S^{-1}(S(x, y) \oplus b)$, де S – це 3-раундова R-схема (випадок $b = (b_1, b_1)$)

Доведення. Нехай $S_b(x, y) = S^{-1}(S(x, y) \oplus b)$, де $x, y \in \mathbb{F}_2^n$, $b \in (F_2^n)^2$ (див. рис.2.2). При такому перетворенні S_b з [5] маємо:

$$\beta_S(a, b) = \#\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \colon S_b(x, y) \oplus S_b((x, y) \oplus a) = a\},$$

де $a \in (F_2^n)^2$. Якщо рівномірність бумерангу F_1 це β_{F_1}, то за означенням

$\exists (a_1, b_1) \in (\mathbb{F}_2^n)^2$ така, що $\beta_{F_1}(a_1, b_1) = \beta_{F_1}$. Якщо $a = (a_1, 0)$, $b = (b_1, b_1)$, то

$$\beta_S(a, b) \;=\; \#\{(x, y) \;\in\; \mathbb{F}_2^n \times \mathbb{F}_2^n \colon S_b(x, y) \oplus S_b(x \oplus a_1, y) \;=\; (a_1, 0)\}.$$

Оскільки $b = (b_1, b_1)$, то можемо спростити:

$$S_b(x, y) = (F_1^{-1}(F_1(x) \oplus b_1), y \oplus b_1).$$

Отже, маємо:

$$\begin{aligned} &S_b(x, y) \oplus S_b(x \oplus a_1, y) = \\ &\quad = (F_1^{-1}(F_1(x) \oplus b_1) \oplus F_1^{-1}(F_1(x \oplus a_1) \oplus b_1), y \oplus b_1 \oplus y \oplus b_1) = \\ &\qquad\qquad = (F_1^{-1}(F_1(x) \oplus b_1) \oplus F_1^{-1}(F_1(x \oplus a_1) \oplus b_1), 0). \end{aligned}$$

Звідси випливає, що множина всіх розв'язків рівняння

$$S_b(x, y) \oplus S_b(x \oplus a_1, y) = (a_1, 0)$$

складається з усіх таких пар (x, y), де y – будь-яке, а x належить множині A, де

$$A = \{x \in \mathbb{F}_2^n \colon F_1^{-1}(F_1(x) \oplus b_1) \oplus F_1^{-1}(F_1(x \oplus a_1) \oplus b_1) = a_1\}.$$

Тоді $|A| = \beta_{F_1}(a_1, b_1) = \beta_{F_1}$. Робимо висновок, що рівномірність бумерангу збалансованої R-схеми з бієктивними внутрішніми функціями обмежена знизу значенням $2^n \beta_{F_1}$. □

Для незбалансованої R-схеми було розглянуто два випадки, коли більша «гілка» знаходиться зліва, а менша – справа та навпаки.

Нехай

$$S_1 : \mathbb{F}_2^m \times \mathbb{F}_2^n \to \mathbb{F}_2^m \times \mathbb{F}_2^n, \quad S_2 : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n \times \mathbb{F}_2^m$$

– незбалансовані 2-раундові R-схеми. Якщо S_1 – це конструкція зліва на Рис.2.3, то справедлива така теорема:

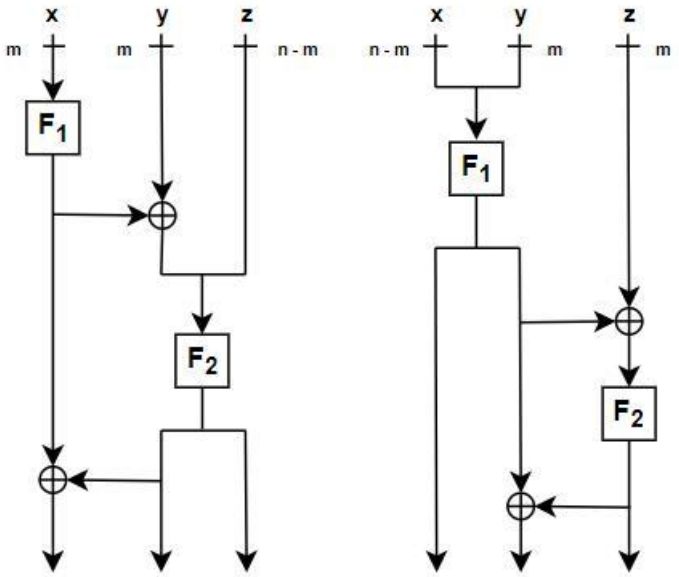

Рисунок 2.3 – Два типи незбалансованої 2-раундової R-схеми (зліва – S_1, справа – S_2)

Теорема 2.2. *Для введеної конструкції S_1 рівномірність бумерангу обмежена таким чином:*

$$\beta_{S_1} \geq 2^n \beta_{F_1}$$

.

Доведення. Почнемо з доведення для S_1. Дамо означення для функції

$$\begin{aligned} S_b \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2^{n-m} &\to \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2^{n-m}, \\ (x, y, z) &\mapsto S^{-1}(S(x, y, z) + b). \end{aligned}$$

У цьому випадку внутрішня функція F_1 є перестановкою над $\mathbb{F}_2^m$, а F_2 – перестановка над $\mathbb{F}_2^n$. Для n-бітового вектору позначимо через $left$ його ліві m бітів та через $right$ його праві $n - m$ бітів. Також позначимо значення трійки (x, y, z) після i раундів для обох варіантів незбалансованої R-схеми як (l_i, m_i, r_i). Нехай $(l_0, m_0, r_0) = (x, y, z)$.

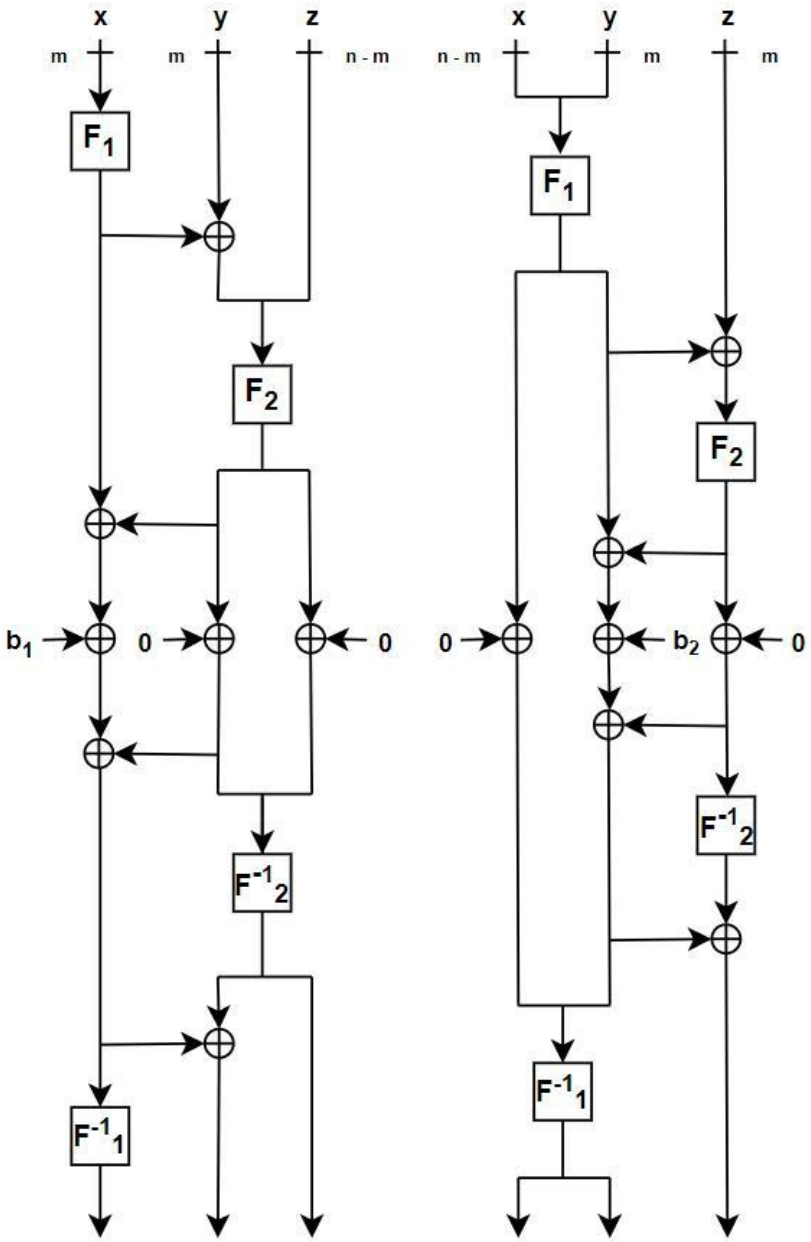

Рисунок 2.4 – Функції $S_b(x) = S^1(S(x) + b)$ для $x \in \mathbb{F}_2^m \times \mathbb{F}_2^n$ (зліва) та для $x \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ (справа), де S – 2-раундова незбалансована R-схема

Тоді

$$(l_1, m_1, r_1) = (F_1(x), F_1(x) \oplus y, z);$$
$$(l_2, m_2, r_2) = (F_1(x) \oplus F_2((F_1(x) \oplus y) \parallel z)_{left}, F_2((F_1(x) \oplus y) \parallel z)_{left},$$
$$F_2((F_1(x) \oplus y) \parallel z)_{right}).$$

Нехай $b = (b_1, b_2, b_3) \in \mathbb{F}_2^{n+m}$ таке, що $b_1 \neq 0$, $b_2 = 0, b_3 = 0$, де $b_1, b_2 \in \mathbb{F}_2^m$

та $b_3 \in \mathbb{F}_2^{n-m}$. Тоді, починаючи з $(l_2 \oplus b_1, m_2 \oplus b_2, r_2 \oplus b_3)$, отримуємо

$$(l_3, m_3, r_3) = (F_1(x) \oplus b_1, F_1(x) \oplus y, z);$$
$$(l_4, m_4, r_4) = (F_1^{-1}(F_1(x) \oplus b_1), y \oplus b_1, z).$$

Отже, для заданого b маємо

$$S_b(x, y, z) = (F_1^{-1}(F_1(x) \oplus b_1), y \oplus b_1, z).$$

Тоді для $a = (a_1, 0, 0), b = (b_1, 0, 0) \in \mathbb{F}_2^m \times F_2^m \times F_2^{n-m}$ отримуємо

$$S_b(x, y, z) \oplus S_b(x \oplus a_1, y, z) = (F_1^{-1}(F_1(x) \oplus b_1) \oplus F_1^{-1}(F_1(x \oplus a_1) \oplus b_1),$$
$$y \oplus b_1 \oplus y \oplus b_1, z \oplus z).$$

За означенням $\beta_{S_1}(a, b) = 2^n \beta_{F_1}(a_1, b_1)$. Для будь-якого $x \in A$, де

$$A = \{x \in \mathbb{F}_2^m \colon (F_1^{-1}(F_1(x) \oplus b_1) \oplus F_1^{-1}(F_1(x \oplus a_1) \oplus b_1) = a_1\}$$

маємо

$$S_b(x, y, z) \oplus S_b(x \oplus a_1, y, z) = (a_1, 0, 0).$$

Обираючи a_1, b_1 такі, що $\beta_{S_1}(a, b) = \beta_{F_1}$ робимо висновок, що рівномірність бумерангу обмежена знизу значенням $2^n \beta_{F_1}$. □

Якщо S_2 – це конструкція справа на Рис.2.4, то маємо результат, який є дуже схожим на попередній, але його також слід розглянути задля повноти дослідження. Отже, справедлива така теорема:

Теорема 2.3. *Для введеної конструкції S_1 рівномірність бумерангу обмежена таким чином:*

$$\beta_{S_2} \geq 2^n \beta_{F_1|_{\mathbb{F}_2^m}}$$

.

Доведення. Дамо означення для функції

$$\begin{aligned} S_b\colon \mathbb{F}_2^{n-m} \times \mathbb{F}_2^m \times \mathbb{F}_2^m &\to \mathbb{F}_2^{n-m} \times \mathbb{F}_2^m \times \mathbb{F}_2^m, \\ (x, y, z) &\mapsto S^{-1}(S(x, y, z) + b). \end{aligned}$$

У цьому випадку внутрішня функція F_1 є перестановкою над $\mathbb{F}_2^n$, а F_2 – перестановка над $\mathbb{F}_2^m$. Для n-бітового вектору позначимо через $left$ його ліві $n-m$ бітів та через $right$ його праві m бітів. Значення трійки (x, y, z) після i раундів було позначено для обох випадків як (l_i, m_i, r_i). Початкове значення трійки $(l_0, m_0, r_0) = (x, y, z)$. Тоді

$$\begin{aligned} (l_1, m_1, r_1) &= (F_1(x \parallel y)_{left}, F_1(x \parallel y)_{right}, F_1(x \parallel y)_{right} \oplus z); \\ (l_2, m_2, r_2) &= (F_1(x \parallel y)_{left}, F_1(x \parallel y)_{right} \oplus F_2(F_1(x \parallel y)_{right} \oplus z), \\ &\qquad F_2(F_1(x \parallel y)_{right} \oplus z). \end{aligned}$$

Нехай $b = (b_1, b_2, b_3) \in \mathbb{F}_2^{n+m}$ таке, що $b_1 = 0$, $b_2 \neq 0, b_3 = 0$, де $b_1 \in \mathbb{F}_2^{n-m}$ та $b_2, b_3 \in \mathbb{F}_2^m$. Тоді, починаючи з $(l_2 \oplus b_1, m_2 \oplus b_2, r_2 \oplus b_3)$, отримуємо

$$\begin{aligned} (l_3, m_3, r_3) &= (F_1(x \parallel y)_{left}, F_1(x \parallel y)_{right} \oplus b_2, F_1(x \parallel y)_{right} \oplus z); \\ (l_4, m_4, r_4) &= (F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2)_{left}, F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2)_{right}, z \oplus b_2). \end{aligned}$$

Отже, для заданого b маємо

$$S_b(x, y, z) = (F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2)_{left}, F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2)_{right}, z \oplus b_2).$$

Тоді для $a = (0, a_2, 0), b = (0, b_2, 0) \in \mathbb{F}_2^m \times F_2^m \times F_2^{n-m}$ отримуємо

$$\begin{aligned} S_b(x, y, z) \oplus S_b(x, y \oplus a_2, z) = (&F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2)_{left} \oplus \\ &F_1^{-1}(F_1(x \parallel y \oplus a_2) \oplus 0 \parallel b_2)_{left}, F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2)_{right} \oplus \\ &F_1^{-1}(F_1(x \parallel y \oplus a_2) \oplus 0 \parallel b_2)_{right}, z \oplus b_2 \oplus z \oplus b_2). \end{aligned}$$

За означенням $\beta_{S_2}(a,b) = 2^n\beta_{F_1}(0 \parallel a_2, 0 \parallel b_2)$. Для будь-якого $x \parallel y \in A$, де

$$A = \{x \| y \in \mathbb{F}_2^n : \\ F_1^{-1}(F_1(x \parallel y) \oplus 0 \parallel b_2) \oplus F_1^{-1}(F_1(x \parallel y \oplus a_2) \oplus 0 \parallel b_2) = 0 \parallel a_2\}$$

маємо

$$S_b(x,y,z) \oplus S_b(x \oplus a_1, y, z) = (0, a_2, 0).$$

Обираючи такі a_2, b_2, що $\beta_{F_1}(0 \parallel a_2, 0 \parallel b_2) = \beta_{F_1|_{\mathbb{F}_2^m}}$ робимо висновок, що, дійсно, рівномірність бумерангу обмежена знизу значенням $2^n\beta_{F_1|_{\mathbb{F}_2^m}}$. □

Бачимо, що як при використанні збалансованої R-схеми так і при використанні незбалансованої R-схеми з наведеною кількістю раундів лише підфункція першого раунду впливає на значення нижньої границі рівномірності. Необхідно брати до уваги те, що це лише нижня оцінка, тобто справжнє значення рівномірності бумерангу може залежати від усіх підфункцій. Зазначимо, що отриманий результат подібний до відповідного для 3-раундової MISTY [5], в якому нижня оцінка бумерангової рівномірності для схеми залежала лише від відповідного параметру підфункції другого раунду шифрування.

2.2 Експериментальна перевірка аналітичних нижніх границь рівномірності бумерангу

Оскільки у цій роботі розглядалися 8-бітові S-блоки, то у якості внутрішніх раундових функцій у збалансованій R-схемі фігурують 4-бітові перестановки. Одна частина з них була одержана за допомогою генератора випадкових перестановок мови програмування Python. Для ста тисяч 4-бітових S-блоків, отриманих у результаті генерування, було пораховано рівномірності бумерангу та виявлено три класи перестановок (з рівномірністю 8, 10 та 16). Випадковим чином було обрано по одній перестановці з кожного класу. Решта S-блоків була запозичена зі статті

[9]. Для проведення експерименту використовувалися такі перестановки:

$$\text{K1} = (7, 9, 4, D, 0, 2, C, B, A, 8, 1, 6, E, 5, F, 3)$$
$$\text{K2} = (1, 9, 6, 5, B, E, 2, 8, 4, A, F, 3, 0, 7, C, D)$$
$$\text{K3} = (A, C, 3, 8, B, 7, D, 0, 4, 5, 1, F, E, 9, 6, 2)$$
$$\text{K4} = (E, A, F, 1, 0, D, 7, 4, 5, 2, 8, 6, 3, B, 9, C)$$
$$\text{K5} = (B, 0, D, E, 6, 4, 7, 9, 5, 1, C, 2, 8, F, A, 3)$$
$$\text{K6} = (1, C, 3, 8, 0, 6, E, D, F, B, 4, 5, 9, 2, A, 7)$$
$$\text{K7} = (E, 7, B, D, 8, 2, 5, 6, 3, 0, 1, C, F, 9, 4, A)$$
$$\text{K8} = (4, 3, A, B, D, E, 8, 5, 9, 1, 7, C, F, 2, 6, 0)$$
$$U8 = (E, B, F, 7, 1, D, 6, 3, 8, 0, 5, C, 2, 9, 4, A)$$
$$U10 = (C, 2, D, E, 1, 4, B, 6, 9, 12, 3, 5, 0, 7, 8, A)$$
$$U16 = (5, 1, 9, 8, E, 2, D, C, 3, 0, F, 6, A, 4, 7, B),$$

де U8 — S-блок із рівномірністю бумерангу 8, U10 — S-блок із рівномірністю бумерангу 10 та U16 — S-блок із рівномірністю бумерангу 16, K1, ... , K8 – S-блоки зі статті, які володіють хорошими властивостями стійкості до лінійного та класичного диференціального криптоаналізу.

У Теоремах 2.1, 2.2 та 2.3 було показано, що нижня оцінка рівномірності бумерангу залежить лише від підфункції першого раунду. Щоб перевірити чи це насправді так, було проведено наступний експеримент. Спочатку у якості обох внутрішніх функцій було обрано одну й ту ж перестановку. Було обчислено рівномірність бумерангу по черзі для U8, U10, U16. Далі було обрано у якості функції першого раунду перестановку з рівномірністю 8, а у якості функції другого раунду перестановку з рівномірністю 10, а потім навпаки. Для порівняння також було обчислено рівномірність бумерангу для 3-раундової R-схеми. Результати експерименту можна спостерігати у Таблицях 2.2 та 2.1.

Таблиця 2.1 – Рівномірності бумерангу для досліджуваних S-блоків

Структура S-блоку	Теоретична оцінка рівномірності	Справжнє значення рівномірності
2-раундова R-схема (у якості внутрішніх функцій виступає U8)	128	256
2-раундова R-схема (у якості внутрішніх функцій виступає U10)	160	256
2-раундова R-схема (у якості внутрішніх функцій виступає U16)	256	256
2-раундова R-схема (функція першого раунду – U8, функція другого раунду – U10)	128	256
2-раундова R-схема (функція першого раунду – U10, функція другого раунду – U8)	160	256
3-раундова R-схема (у якості внутрішніх функцій виступає U8)	-	128
3-раундова R-схема (у якості внутрішніх функцій виступає U10)	-	160
3-раундова R-схема (функція першого раунду – U8, решта підфункцій – U10)	-	160
3-раундова R-схема (функція першого раунду – U10, решта підфункцій – U8)	-	128
3-раундова MISTY (у якості внутрішніх функцій виступає U8)	128	128
3-раундова MISTY (у якості внутрішніх функцій виступає U10)	160	160
3-раундова MISTY (функція другого раунду – U8, решта підфункцій – U10)	128	128
3-раундова MISTY (функція другого раунду – U10, решта підфункцій – U8)	160	160

Таблиця 2.2 – Рівномірності бумерангу 4-бітових S-блоків стійких до лінійного криптоаналізу

Перестановка F	K1	K2	K3	K4	K5	K6	K7	K8
β_F	16	16	16	10	10	16	16	10

На прикладі перестановок K1,...,K8 можемо спостерігати, що наявність хороших властивостей, які характеризують стійкість до лінійного та класичного диференціального криптоаналізу абсолютно не гарантують стійкості до атак бумерангу. Більшість вказаних перестановок мають найгіршу рівномірність бумерангу з можливих.

Що стосується Теореми 2.1, то в результаті виконання експерименту неможливо однозначно стверджувати про залежність нижньої границі рівномірності бумерангу всієї конструкції від функції першого раунду, адже в усіх розглянутих випадках рівномірність 2-раундової R-схеми максимальна. Однак звідси можна зробити висновок, що, незважаючи на використання внутрішніх функцій з відносно низькою рівномірністю бумерангу, використання 2-раундової R-схеми не є доцільним для побудови S-блоків стійких до атак бумерангу. Згідно з наведеними в таблиці результатами, 3-раундова R-схема, хоча й має не максимальне, але все ще велике значення рівномірності бумерангу, також не може вважатися стійкою до атак бумерангів. Для того, щоб робити більш надійні твердження щодо стійкості саме 3-раундової R-схеми, властивості її BCT слід вивчити більш детально. Бачимо, що значення рівномірності 3-раундової мережі MISTY співпадає з аналітичними оцінками, знайденими у [5].

Висновки до розділу 2

Отже, у даному розділі було отримано аналітичні оцінки для нижньої границі рівномірності бумерангу для S-блоків, які мають структуру 2-раундової R-схеми (як збалансованої так і незбалансованої), показано, що ці оцінки залежать лише від рівномірності бумерангу внутрішньої функції першого раунду схеми. Було виявлено незалежність стійкості до атак бумерангів від стійкості до лінійного криптоаналізу. Також була експериментально перевірена розбіжність справжніх значень та аналітичних оцінок для R-схеми та мережі MISTY і показано, що істинні значення суттєво більші за нижні границі. Це каже про те, що їх не можна вважати точними. Звідси виникає питання про те, як взагалі розподілене значення рівномірності бумерангу та які значення очікуються від випадково згенерованого S-блоку. На це питання дається відповідь у наступному розділі.

3 ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА РОЗПОДІЛУ BCT

У цьому розділі буде розглянуто знайдений розподіл коефіцієнтів для таблиці BCT та експериментально перевірено його коректність. Ця інформація є вкрай важливою, адже переконавшись, що розподіл дійсно має запропонований вигляд, можна оцінювати рівномірність бумерангу, не прибігаючи до побудови великих таблиць BCT.

3.1 Загальні відомості про розподіл та результати експерименту

Інформація щодо вигляду розподілу коефіцієнтів DDT чи то BCT може бути корисна для того, щоб оцінити ймовірність того, що випадкова перестановка має «хороші» диференціальні (для DDT) або бумерангові (для BCT) властивості. У даній роботі експериментальним чином було перевірено розподіл коефіцієнтів BCT, знайдений авторами статті [10]. Перед тим як перейти безпосередньо до результатів, детально розглянемо запропоновану теорему з доведенням та твердження про альтернативне визначення BCT.

Твердження 3.1 (Альтернативне визначення BCT[11]). *Нехай $S \in \mathbb{F}_2^n$ – перестановка. Для будь-яких $a, b \in \mathbb{F}_2^n$ запис $\beta_S(a, b)$ у BCT перестановки S задається як кількість розв'язків у $F_2^n \times F_2^n$ такої системи рівнянь*

$$\begin{cases} S^{-1}(x \oplus b) \oplus S^{-1}(y \oplus b) = a, \\ S^{-1}(x) \oplus S^{-1}(y) = a. \end{cases} \tag{3.1}$$

Теорема 3.1 ([11]). *Якщо S – обрана випадковим чином перестановка над $\mathbb{F}_2^n$, то коефіцієнти її BCT $\beta_S(a, b)$, де $a, b \neq 0$,*

можуть розглядатися як незалежні однаково розподілені випадкові величини з таким розподілом:

$$\Pr\{\beta_S(a,b)=c\}=\sum_{2i_1+4i_2=c} P_1(i_1)P_2(i_2),$$

де i_1, i_2 – цілі невід'ємні числа, сума ведеться по всіх розв'язках рівняння $2i_1+4i_2=c$, P_1 та P_2 – розподіли випадкових величин такої форми:

$$P_1(i)=Bin(i;2^{n-1},\frac{1}{2^n-1}) \quad та \quad P_2(i)=Bin(i;2^{2n-2},\frac{1}{(2^n-1)^2})$$

Доведення. Для будь-яких $x,y\in\mathbb{F}_2^n$ таких, що $x\neq y$, позначимо множину

$$S_{x,y}=\{(x,y),(y,x),(x\oplus b,y\oplus b),(y\oplus b,x\oplus b)\},$$

потужність якої дорівнює 4, окрім випадку, коли $x\oplus y=b$. Тоді $S_{x,y}$ містить лише два елементи. Ці множини такі, що пара (x,y) є розв'язком системи, наведеної вище тоді та тільки тоді, коли всі елементи в $S_{x,y}$ також є розв'язками даної системи. Щоб довести цю теорему, множину всіх пар елементів в $\mathbb{F}_2^n$ було розбито на такі множини $S_{x,y}$.

Розглянемо таке відношення еквівалентності: $(x,y)\sim(x\prime,y\prime)$ тоді та тільки тоді, коли мультимножини $S_{x,y}$ та $S_{x\prime,y\prime}$ є ідентичними. Відповідні класи еквівалентності мають розмір 4, за винятком випадку, коли $x\oplus y=b$, у цьому разі вони містять 2 елементи. Всього є 2^{n-1} класи розміру 2. Оскільки є $2^n(2^n-1)$ упорядкованих пар елементів у $\mathbb{F}_2^n$, то отримуємо, що є $(2^n(2^n-1)-2\times 2^{n-1})/4$ класи потужності 4, тобто $2^{2n-2}-2^{n-1}$.

Тоді для того, щоб Система3.1 мала рівно c розв'язків, необхідно, щоб існувало i_1 розв'язків у класах розміру 4 та i_2 розв'язків в класах розміру 2, де $2i_1+4i_2=c$. Отримуємо

$$\Pr\{\beta_S(a,b)=c\}=\sum_{2i_1+4i_2=c} P_1(i_1)P_2(i_2),$$

де P_1 – це ймовірність того, що існує i_1 класів розміру 4, P_2 – це ймовірність

того, що існує i_2 класів розміру 2 таких, що є розв'язками системи. Тепер доведемо, що розподіли P_1 та P_2 такі, як зазначено у теоремі.

Розмір 2. У цьому випадку справедливо, що $y = x \oplus b$, отже обидва рівняння Системи3.1 співпадають. Припустимо, що $S^{-1}(x) \oplus S^{-1}(x \oplus b) = a$ виконується з ймовірністю $\frac{1}{2^n-1}$, так як $S^{-1}(x) \oplus S_{-1}(x \oplus b)$ може приймати яке завгодно значення в $\mathbb{F}_2^n/\{0\}$. Оскільки є 2^{n-1} таких пар, P_1 відповідає біноміальному розподілу 2^{n-1} повторами випробування Бернуллі з ймовірністю успіху $\frac{1}{2^n-1}$.

Розмір 4. Два рівняння системи 3.1 тепер незалежні. Використовуючи ті ж міркування, що і вище, припустимо, що кожна з рівнянь виконується з ймовірністю $\frac{1}{2^n-1}$. Оскільки є $2^{2n-2} - 2^{n-1}$ таких пар, P_2 відповідає біноміальному розподілу з параметрами $2^{2n-2} - 2^{n-1}$ та $\frac{1}{(2^n-1)^2}$. □

У доведенні використовувалися деякі модельні припущення, які не працюють на практиці, зокрема було припущено, що комірки ВСТ є незаєжними. Тому виникає потреба у експериментальній перевірці введеної гіпотези.

Перевірка виду розподілу проводилася за допомогою використання методів статистичного аналізу, а саме розв'язок поставленої задачі потребував перевірки статистичної гіпотези. Отже, на початку експерименту слід сформулювати гіпотезу. Введемо основну гіпотезу для даного випадку: H_0 – значення комірки у ВСТ має такий вигляд, як у Теоремі 3.1. Відповідно альтернативна гіпотеза полягає в тому, що значення комірки має будь-який інший розподіл. Звідси маємо задачу узгодження. У якості статистичного критерію було обрано відомий критерій хі-квадрат Пірсона, адже через його універсальність, критерій можна використовувати для даних будь-якої природи.

У якості випадкової величини розглядаємо значення комірки. Позначимо її через ξ. Введена випадкова величина може приймати значення в діапазоні від 0 до 255. Було проведено $n = 1000000$

незалежних випробувань. Тоді нехай

$$v_j = \sum_{i=1}^{n}(I(\xi_i = j)), j = 0, ..., 255,$$

– відповідні частоти результатів випробувань, $I(x = y)$ – індикаторна функція ($I(x = y) = 1$, якщо $x = y$, та $I(x = y) = 0$ у протилежному випадку).

Отже, маємо вектор $\overline{v} = (v_0, ..., v_{255})$, по якому треба перевірити гіпотезу $H_0 : p = p^\circ$, де $p^\circ = (p_0^\circ, ..., p_{255}^\circ), p_i^\circ = Pr\{\xi = i\}$ – вектор ймовірностей, заданий за допомогою Теореми 3.1. У нашому випадку тестова статистика критерію Пірсона має такий вигляд:

$$\overset{\circ}{X}{}_n^2 = \sum_{j=0}^{255} \frac{(v_j - np_j^\circ)^2}{np_j^\circ}$$

Точний розподіл незручний для розрахунку критерію, але для великих вибірок наведена статистика має простий граничний розподіл, який не залежить від $\overline{p}^\circ$. Відомо, що для об'єму вибірки більшого за 50 можна використовувати граничний розподіл χ^2_{N-1} с хорошим наближенням.

Отже, сформулюємо критерій

$$H_0 \quad \text{відхиляється} \Leftrightarrow \{\overset{\circ}{X}{}_n^2 > \chi^2_{(1-\alpha)(N-1)}\},$$

де α – рівень значущості, N – максимальне значення, яке може приймати випадкова величина ξ, але оскільки згідно з порахованим вектором частот значення жодної комірки не було непарним, то у сумі враховувалися лише парні j. Через це у розрахунку теоретичного значення χ^2 значення N бралося рівним 128. У ході експерименту рівень значущості α обирався рівний 0.05, 0.01 та 0.001, а теоретичний розподіл апроксимувався пуассонівським. Необхідно також зазначити, що вибірка із мільйона перестановок була отримана за допомогою генератора випадкових перестановок мови програмування Python. Розглядався випадок для 8-бітових перестановок. Звідси маємо 65025 ітерацій

перевірки гіпотези для кожної з комірок. Результати експерименту можна спостерігати у Таблиці 3.1.

Таблиця 3.1 – Результати перевірки гіпотези про вид розподілу значення комірки BCT

Рівень значущості α	Теоретичне значення χ^2	Максимальне значення χ^2	Мінімальне значення χ^2	Кількість прийнятих гіпотез	Кількість відхилених гіпотез	Кількість аномальних значень χ^2	Кількість значень χ^2 менших за 10
0,05	154,01833927	21562,78306476	2,3195554	64575	450	21	1202
0,01	166,20243287			64799	226		
0,001	180,42350879			64883	142		

Бачимо, що у всіх трьох випадках статистичні тести підтверджують основну гіпотезу про вигляд розподілу. Зазначимо, що у процесі виконання експерименту було виявлено деякі аномальні значення тестової статистики, кількість яких відмічена у відповідному стовпчику таблиці. Під аномальними даними мається на увазі значення статистики, які є суттєво більшими за теоретичне значення χ^2. Бачимо, що поява таких аномалій є вкрай рідкою, але тим не менш потребує окремого вивчення надалі.

Оскільки 8-бітові S-блоки мають суттєве значення для сучасної криптографії, наведемо графік розподілу для S-блоку такого розміру на Рис. 3.1. По вигляду розподілу бачимо, що непарні значення є недосяжними.

З попередніх досліджень відомо, що математичне сподівання рівномірності бумерангу для 8-бітового S-блоку, обчислене за допомогою знайденого розподілу, дорівнює 20.2. На практиці ж бачимо, що для S-блоків, які мають структуру мережі MISTY або R-схеми, значення рівномірності бумерангу дорівнює щонайменше 128. Звідси можна зробити висновки, що S-блоки з аналітичною структурою скоріш за все будуть мати «погані» значення рівномірності бумерангу порівняно з випадковими S-блоками. Цей факт може бути використаний як індикатор того, що S-блок має внутрішню структуру.

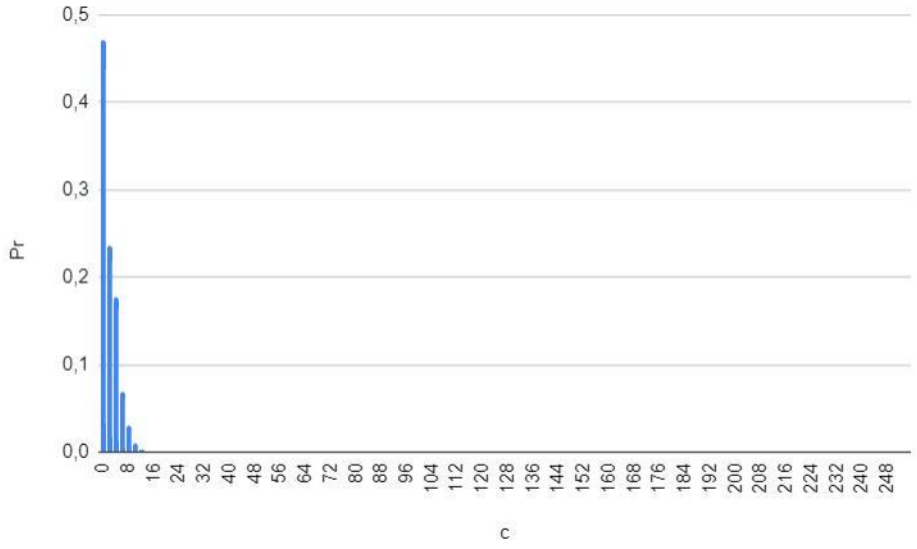

Рисунок 3.1 – Розподіл значень елементів BCT для 8-бітового S-блоку

Висновки до розділу 3

У даному розділі було розглянуто розподіл значень BCT та експериментально перевірено коректність тих припущень, які були зроблені при його побудові. Дійсно, прийняті модельні припущення є адекватними та виконуються навіть для не дуже великого розміру S-блоку.

ВИСНОВКИ

У ході виконання даної роботи був проведений аналіз опублікованих джерел за тематикою дослідження, який показав що питання про надійність класичних конструкцій у контексті стійкості до атак бумерангів залишається відкритим. Тому задля розширення уявлення про властивості таких конструкцій у роботі розглядалися S-блоки, які мають структуру 2-раундової R-схеми блокового шифрування. Для них було отримано нижні оцінки рівномірності бумерангу та експериментально перевірено чи вони співпадають зі справжніми значеннями. В результаті чого можна зробити висновок про доцільність використання зазначеної конструкції. Хоча й серед отриманих рівномірностей наявні не максимальні, але все ще високі значення, можна сміливо стверджувати, що 2-раундова чи то 3-раундов R-схема, незважаючи на структуру (збалансована або незбалансована), не має достатніх якостей, які б дозволяли їй розглядатися як фундамент для побудови нових S-блоків, стійких до атак бумерангів.

Також у роботі за допомогою методів статистичного аналізу було перевірено розподіл значень BCT, в результаті чого було підтверджено, що він дійсно відображає правдоподібні результати, незважаючи на всі модельні припущення, які були зроблені при його знаходженні. Отже, він може бути використаний на практиці для оцінки рівномірності бумерангу щонайменше для 8-бітових S-блоків.

Результати проведеного дослідження можуть бути використані надалі для аналізу та вивчення властивостей S-блоків, які використовують в якості своїх внутрішніх функцій 4-бітові перестановки.

ПЕРЕЛІК ПОСИЛАНЬ

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

[2] 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.

[3] Eli Biham, Orr Dunkelman, and Nathan Keller. "Related-Key Boomerang and Rectangle Attacks". In: *Advances in Cryptology – EUROCRYPT 2005*. Ed. by Ronald Cramer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 507–525. ISBN: 978-3-540-32055-5.

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

[5] Shizhu Tian, Christina Boura, and Léo Perrin. *Boomerang Uniformity of Popular S-box Constructions*. Cryptology ePrint Archive, Report 2019/1002. https://eprint.iacr.org/2019/1002. 2019.

[6] 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.

[7] Vincent Grosso et al. "LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations". In: *Fast Software Encryption*. Ed. by

Carlos Cid and Christian Rechberger. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 18–37. ISBN: 978-3-662-46706-0.

[8] Власенко Н.М. “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.

[9] Яковлєв С.В. “Збалансовані критерії якості довгострокових ключових елементів алгоритму шифрування ГОСТ 28147-89”. In: *Інформаційні технології та комп’ютерна інженерія.* 1 (14) (2009), С. 48–55.

[10] Xavier Bonnetain, Léo Perrin, and Shizhu Tian. *Anomalies and Vector Space Search: Tools for S-Box Analysis (Full Version)*. Cryptology ePrint Archive, Report 2019/528. https://eprint.iacr.org/2019/528. 2019.

[11] Kangquan Li et al. *New Results about the Boomerang Uniformity of Permutation Polynomials*. Cryptology ePrint Archive, Report 2019/079. https://eprint.iacr.org/2019/079. 2019.