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
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-науковою програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Побудова атаки усічених бумерангів на "Калина"-подібні шифри »**

Виконав: студент 2 курсу, групи ФІ-12мн
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 — 2023

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

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

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій Яковлєв
«__» _____ 2023 р.

ЗАВДАННЯ
на магістреську дисертацію

Студент: Мітрофанова Еліна Володимиріна

1. Тема роботи: «*Побудова атаки усічених бумерангів на "Калина"-подібні шифри* »,

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

затверджені наказом по університету №__ від «__» _____ 2023р.

2. Термін подання студентом роботи: «__» _____ 2023р.

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

4. Зміст роботи: побудова атаки усічених бумерангів на Калина-подібні шифри

5. Перелік ілюстративного матеріалу: презентація доповіді.

6. Дата видачі завдання: 10 вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	1 вересня - 15 жовтня 2022 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	1 жовтня – 1 грудня 2022 р	Виконано
3	Побудова атаки усічених бумерангів на 6-раундовий шифр Калина-512	1 грудня 2022 р - 17 січня 2023 р	Виконано
4	Побудова атаки усічених бумерангів на 6-раундовий шифр Калина-256, Калина-128	Лютий 2023р. - Березень 2023р.	Виконано
5	Аналіз отриманих результатів	Квітень 2023 р	Виконано
6	Оформлення роботи та підготовка презентації до захисту	Травень 2023 р	Виконано

Студент _____ Мітрофанова Е.В.

Керівник _____ Яковлєв С.В.

РЕФЕРАТ

Кваліфікаційна робота містить: 41 стор., 16 рисунків, 2 таблиці, 8 джерел.

Метою дослідження є уточнення методів оцінювання стійкості симетричних блокових шифрів до деяких класів атак.

Об'єктом дослідження інформаційні процеси в системах криптографічного захисту.

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

У даній роботі було побудовано атаки усічених бумерангів на шифр Калина-128, Калина-256, Калина-512 зі зменшеною кількістю раундів та одержано оцінки стійкості до даного класу атак.

АТАКА БУМЕРАНГІВ, УСІЧЕНІ ДИФЕРЕНЦІАЛИ, АТАКА УСІЧЕНИХ БУМЕРАНГІВ, AES, ШИФР КАЛИН.

ABSTRACT

The qualifying paper contains: 41 pages, 16 figures, 2 tables, 8 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 research is the resistance parameters of Kalina-like ciphers to the attack of truncated boomerangs.

In this work, attacks of truncated boomerangs on Kalina-128, Kalina-256, Kalina-512 ciphers with a reduced number of rounds were constructed and estimates of resistance to this class of attacks were obtained.

BOOMERANG ATTACK, TRUNCATED DIFFERENTIALS, TRUNCATED BOOMERANG ATTACK, AES, CIPHER KALYNA

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

V_n – множина n-бітових векторів.

$\oplus$– операція додавання за модулем 2(XOR)

AES - Advanced Encryption Standard

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

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

ВСТУП

Актуальність дослідження. Актуальність дослідження. На сьогоднішній день існує розмаїття методів криптоаналізу. Один із популярних методів - диференційний аналіз, був запропонований в 90-х роках ізраїльськими експертами Елі Біхамом і Аді Шамір для злому криптосистем, подібних до DES[1]. Диференційний аналіз швидко розвивався, з'явилося багато нових технік. Одна з них - усічені диференціали [2] та атака бумерангів [3].

Атака бумерангів є ще однією ефективною методикою в криптоаналізі. Вперше використовувалась для злому шифрів, які вважалися стійкими проти диференційних атак. Однак, нещодавно у роботі [4] було розглянуто нову версію цієї атаки - атаку усічених бумерангів, яка базується на усічених диференціалах, та застосована до блокового 6-раундового шифру AES.

Крім того, варто відзначити і український шифр "Калина". Дослідження його стійкості до диференційних атак показали, що можна встановити найменшу та максимальну кількість циклів, при яких шифр залишається стійким [5], а також час і пам'ять, які будуть використані при атаці. Проте серед розглянутих атак не було атаки усічених бумерангів.

У цій роботі більш детально буде розглянута атака-усічених бумерангів на Калина-подібні шифри зі зменшеною кількістю раундів та проаналізовано параметри стійкості до цієї атаки.

Метою дослідження є уточнення методів оцінювання стійкості симетричних блокових шифрів до деяких класів атак. Задача дослідження - побудова аналітичних оцінок стійкості Калина-подібних шифрів до атаки усічених бумерангів. До досягнення мети потрібно вирішити наступні завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) проаналізувати алгебрагічні властивості усічених диференціалів, схеми атаки бумерангів та атаки усічених бумерангів;

3) побудувати атаку усічених бумерангів на 6-раундовий шифр Калина-512 та з‘ясувати його стійкість до даної атаки;

4) побудувати атаку усічених бумерангів на 6-раундові шифри Калина-128 і Калина-256; порівняти стійкість цих шифрів з попередніми результатами для Калина-512.

Об’єктом дослідження інформаційні процеси в системах криптографічного захисту.

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

При розв’язанні поставлених завдань використовувались такі *методи дослідження*: комбінаторний аналіз, дискретная математика, диференційний аналіз.

Наукова новизна: побудовано атаки усічених бумерангів на шифр Калина-128, Калина-256, Калина-512 зі зменшеною кількістю раундів та одержано оцінки стійкості до даного класу атак.

Практичне значення. Результати даної роботи можуть бути використанні при аналізі існуючих та побудові нових Калина-подібних шифрів.

1 АТАКА УСІЧЕНИХ БУМЕРАНГІВ

У даному розділі розглянуто основні поняття, які стосуються усічених диференціалів, атаки бумерангів, усіченої атаки бумерангів, а також основні характеристики шифрів AES і Калина.

1.1 Диференційний аналіз. Усічені диференціали

Диференційний аналіз, запропонований ізраїльськими фахівцями у роботі [1], використовує пари зашифрованих текстів та відповідних розшифрованих текстів. В цьому аналізі досліджується, як змінюється різниця між зашифрованими текстами під час шифрування, а не процес самого шифрування

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 операції визначають конкретну статистику. Ми будемо досліджувати не сам процес шифрування тексту, а різницю між зашифрованими текстами, яка виникає під час шифрування.

Давайте розглянемо процес диференційного аналізу за наступною схемою:

1) Збираємо N пар повідомлень (x, x'), де $x = x' \circ \alpha$, разом з відповідними шифртекстами (y, y').

2) Для кожного потенційного ключа k_r, перетворюємо шифртекст (y, y') у повідомлення (x_{r-1}, x'_{r-1}) за допомогою відповідного ключа k_r.

3) Перевіряємо, чи виконується рівність $x'_{r-1} = x_{r-1} \bullet \beta$, де β - певний параметр.

4) Вибираємо ключ k_r, для якого рівність виконується найбільшу

кількість разів, як коректний ключ.

Отже, схема диференційного аналізу полягає у зборі пар повідомлень з певною різницею, перетворенні шифртекстів у повідомлення з допомогою потенційних ключів та перевірці рівності між повідомленнями та їхніми шифртекстами. Найкоректніший ключ обирається на основі того, який задовольняє рівність найбільшу кількість разів.

Усічені диференціали були запропоновані криптографом Елі Бієстером (Eli Biham) та математиком Аді Шамиром (Adi Shamir) в 1991 році як новий метод криптоаналізу, який може бути застосований до широкого спектру криптографічних функцій, включаючи хеш-функції та блочні шифри. Цей метод аналізу дозволяє знайти вразливості у криптографічних функціях, які можуть бути використані для атак на шифри та інші криптографічні протоколи. Визначимо усічені диференціали більш формально.

Означення 1.1. Нехай (α, β) диференціал і-того раунду. Якщо α' є підпослідовністю α, а β' є підпослідовністю β, то (α', β') називається усіченим диференціалом і-того раунду шифрування [4].

Будемо використовувати символ + для позначення операції XOR (додавання в $F_{2^u}^v$). Диференціал визначається різницею на вході $\Delta_{in} \in \{0,1\}^n$ та на виході $\Delta_{out} \in \{0,1\}^n$. Надалі будемо використовувати позначення $\Delta_{in} \xrightarrow[E]{p} \Delta_{out}$, коли існує диференціал з імовірністю $\overrightarrow{p}$, де $\overrightarrow{p}$ визначається так:

$$\overrightarrow{p} = Pr[\Delta_{in} \underset{E}{\rightarrow} \Delta_{out}] = Pr[E(P) + E(P + \Delta_{in}) = \Delta_{out}]. \qquad (1.1)$$

Оскільки E - перестановка, то $Pr[\Delta_{in} \underset{E}{\rightarrow} \Delta_{out}] = Pr[\Delta_{out} \xrightarrow[E^{-1}]{} \Delta_{in}]$.

Усічена різниця визначається множиною вхідних різниць D_{in} та множиною вихідних різниць D_{out}. Використаємо позначення $D_{in} \xrightarrow[E]{p} D_{out}$ для позначення існування усіченої різниці з ймовірністю $\overrightarrow{p}$, визначеної

як:

$$\overrightarrow{p} = \underset{\Delta_{in} \in D_{in}}{\text{Avg}} \Pr[E(P) + E(P + \Delta_{in}) \in D_{out}] \tag{1.2}$$

Також визначимо ймовірність зворотніх усічених диференціалів

$$\overleftarrow{p} = \underset{\Delta_{out} \in D_{out}}{\text{Avg}} \Pr[E^{-1}(P) + E^{-1]}(P + \Delta_{out}) \in D_{in}] \tag{1.3}$$

На рисунку 1.1 наведено приклад усіченого диференційного аналізу на трьох раундах AES з відповідно 4, 1 та 4 активними S-Box у кожному раунді. У цьому усіченому диференційному аналізі D_{in} відповідає векторному простору елементів, які мають нулі на всіх діагоналях, окрім головної. D_{out} - це векторний простір станів, які зворотньо через операцію MixColumns мають значення 0 на кожній протилежній діагоналі, окрім головної.

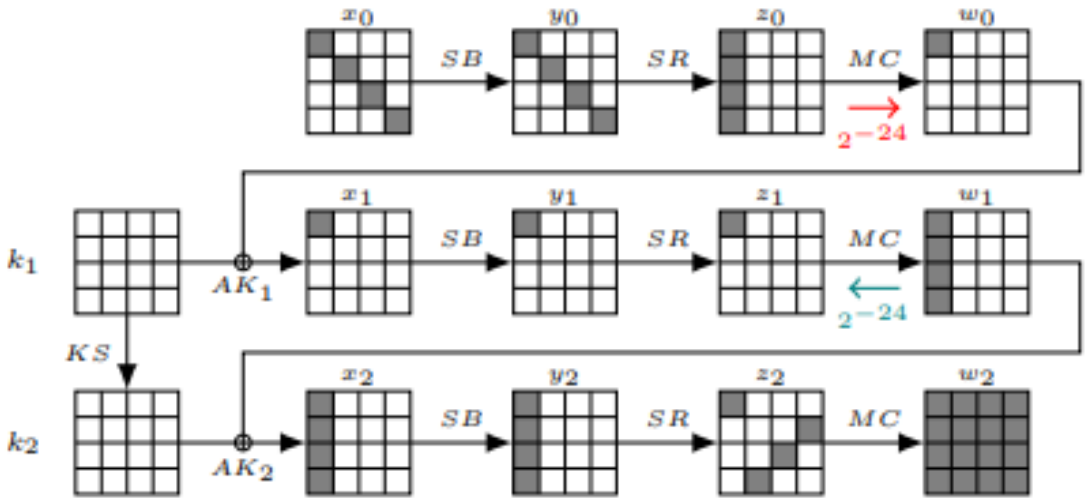


Рисунок 1.1 – Приклад усіченого диференціального аналізу на 3-раундовому AES.

Отже, $D_{in} = D_{out} = 2^{64}$. Імовірність усіченого диференціала $\overrightarrow{p} = 2^{-24}$, а зворотня ймовірність $\overleftarrow{p} = 2^{-24}$.

1.2 Атака бумерангів

Атака бумерангів (англ. Boomerang attack) - це одна з криптоаналітичних атак на блочні шифри, яка була вперше описана криптографом Девідом Вагнером[2] в 1999 році. Ця атака зазвичай використовується для підвищення швидкості атаки на блочний шифр з довільною довжиною блоку та розміром ключа.

Атака бумерангів базується на знаходженні певного числа побітових різниць, які можуть відбуватися в двох різних шифротекстах за умови, що відповідні частини відкритого тексту є ідентичними. Ці різниці можуть бути використані для підвищення швидкості знаходження ключа, оскільки вони дозволяють скоротити кількість можливих ключів, які необхідно перевірити.

Для проведення атаки бумерангів зазвичай використовують дві фази. Перша фаза полягає у виборі деякої кількості відкритих текстів та їх шифротекстів. Друга фаза полягає у пошуку побітових різниць між двома шифротекстами, які можуть бути використані для знаходження ключа. Ці різниці можуть бути знайдені за допомогою криптоаналітичних методів, таких як метод лінійних апроксимацій або метод диференціалів.

Після знаходження побітових різниць атакувач може згенерувати нову пару відкритого тексту та шифротексту, яка містить ці різниці. Ця нова пара може бути використана для перевірки можливих ключів, які задаються функцією шифрування.

Розглянемо дану атаку більш детально. Атакуючий розкладає повний шифр E на два підшифри E_0 (верхня частина) та E_1 (нижня частина), з $E = E_1 \circ E_0$, із високими ймовірностями диференціалів на E_0 та E_1 (ймовірності p та q), позначені $\Delta_{in} \xrightarrow[E_0]{p} \Delta_{out}$ та $\nabla_{in} \xrightarrow[E_1]{q} \nabla_{out}$.

Атака проходить наступним чином:

1) Генеруються пари відкритого тексту $(P, P^{'})$ такі, що $P + P^{'} = \Delta_{in}$, шифруються та отримаються відповідні шифртексти

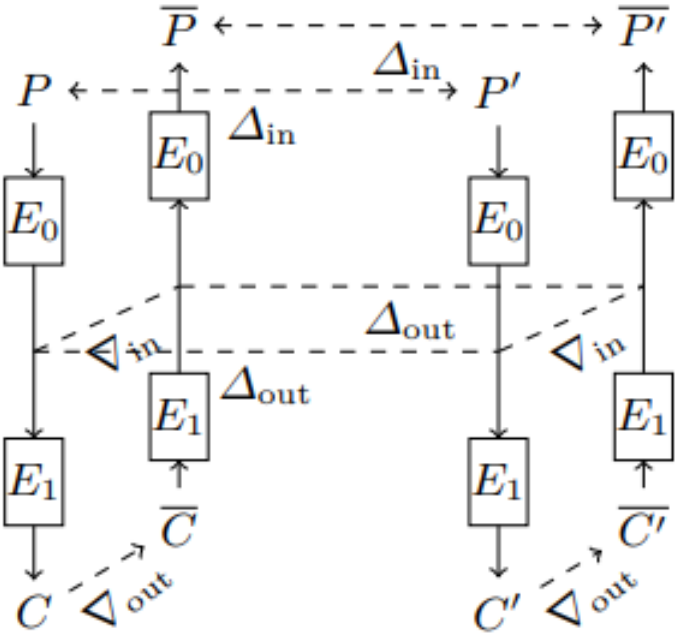


Рисунок 1.2 – Атака бумерангів

$(C, C') = (E(P), E(P'))$.

2) Зсуваються пари шифртекстів у нові пари $(\overline{C}, \overline{C'}) = (C + \nabla_{out}, C' + \nabla_{out})$ та запитуємо їх дешифрування $(\overline{P}, \overline{P'}) = (E^{-1}(\overline{C}), E^{-1}(\overline{C'}))$.

3) Пошук пари $\overline{P} + \overline{P'} = \Delta_{in}$.

Аналіз атаки. $E_0(P) = E_1^{-1}(C)$, тому що $E = E_1 \circ E_0$. $E_0(\overline{P}) + E_0(\overline{P'}) = E_1^{-1}(\overline{C}) + E_1^{-1}(\overline{C'}) + E_0(P) + E_1^{-1}(C) + E_0(P') + E_1^{-1}(C')$. Крім того, диференціали в E_0 і E_1 означають, що:

$$Pr[E_0(P) + E(P') = \Delta_{out}] = p$$

$$Pr[E_1^{-1}(C) + E_1^{-1}(\overline{C}) = \nabla_{in}] = q$$

$$Pr[E_1^{-1}(C') + E_1^{-1}(\overline{C'}) = \nabla_{in}] = q$$

Коли три події задовольняються, ми отримуємо $E_0(P)+E_0(P') = \Delta_{out}$ та з додатковою ймовірністю p, $P+P' = \Delta_{in}$. Нарешті, припускаючи, що всі події незалежні, ми обчислюємо ймовірність шляху бумеранга p_b як нижню

межу ймовірності відношення бумеранга $P + P' = \Delta_{in}$

$$Pr[E^{-1}(E(P) + \nabla_{out}) + E^{-1}(E(P + \Delta_{in}) + \nabla_{out}) = \Delta_{in}] \geqslant p_b = p^2 \times q^2.$$

Рисунок 1.2 показує конструкцію квартету бумерангу. Коли $p^2 \times q^2 \gg 2^{-n}$ це дає розпізнавальний аналіз шифру, використовуючи $O(p^{-2} \times q^{-2})$ квартетів, оскільки ймовірність виявлення квартету дорівнює 2^{-n} для випадкової перестановки. У більшості випадків аналіз розпізнавання може бути перетворений на відновлення ключа, використовуючи залежності ключа в розпізнавальному аналізі.

Атака бумерангів була успішно використана для аналізу багатьох блочних шифрів, включаючи DES, AES, Serpent, Blowfish та інші. Наприклад, атака бумерангів використовувалась для підвищення швидкості атаки на середньовеликі версії блочних шифрів DES та AES.

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 – Приклад BCT для S-блоку шифра PRESENT

Однак, на щастя, існують методи захисту від атак бумерангів. Один з таких методів - це побудова BCT(Boomerang Connectivity Table)[3]. BCT таблицю можна побудувати за допомогою різних методів, наприклад, методу обчислення кореляційних імунітетів або методу лінійних апроксимацій. Результатом є таблиця, що містить відстані між раундами алгоритму, що дозволяє оцінити стійкість алгоритму до атак бумерангу. Розробники криптографічних алгоритмів можуть використовувати BCT таблицю для оцінки потенційних уразливостей свого алгоритму та для його вдосконалення з метою збільшення стійкості до атак бумерангу.

Також варто зазначити, що є аналогічний інструмент FBCT для шифрів, S-блоки яких базуються на мережі Фейстеля.

	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 1.4 – Приклад FBCT

1.3 Блокові шифри AES та Калина

Advanced Encryption Standard (AES) є стандартом шифрування, що використовується для захисту конфіденційної інформації в різних сферах. Шифр був прийнятий в 2001 році як заміна стандарту DES (Data Encryption Standard) [7]. Основна особливість AES полягає в його здатності шифрувати дані з високою швидкістю та надійністю.

AES використовує ключ довжиною 128, 192 або 256 біт. Для шифрування використовується ітеративний алгоритм, що працює з блоками даних довжиною 128 біт.

Алгоритм складається з 10, 12 або 14 раундів (залежно від довжини ключа). Кожен раунд складається з п'яти етапів:

1) SubBytes - полягає в заміні кожного байту згідно з S-блоком. Цей етап допомагає зберегти властивості дифузії та збурює будь-які структури, які можуть бути видимі у вихідному тексті.

2) ShiftRows - виконує циклічний зсув рядків блоку. Це забезпечує те, що жоден байт не зберігає своє положення у вихідному тексті.

3) MixColumns - змішує колонки блоку. Цей етап забезпечує додаткову дифузію та зменшує можливість атак на шифр.

4) AddRoundKey - полягає в додаванні ключа раунду до блоку. Це забезпечує додаткову безпеку та забезпечує те, що жоден біт вхідного тексту не може бути виведений з блоку без знання ключа.

5) KeyExpansion. Останній етап полягає в розширенні ключа. Ключ розширюється до розміру, який необхідний для виконання шифрування.

Шифр Калина є українським блочним шифром з відкритим кодом, розроблений у 2015 році [8] і призначений для заміни старішого стандарту шифрування, відомого як ГОСТ 28147-89. Шифр Калина використовує блок довжиною 128 бітів і має 10 раундів для 128-бітового ключа, 14 раундів для 256-бітового ключа та 18 раундів для 512-бітового ключа. Кожен раунд складається з таких же етапів, як і раунд шифру AES, але з

деякими відмінностями.

Таблиця 1.1 – Основні характеристики для AES та Калина

Характеристика	**AES**	**Калина**
Розмір блоку	128 біт	128, 256 або 512 біт
Кількість раундів	10/12/14	10/14/15
Розмір ключа	128, 192 або 256 біт	128, 256 або 512 біт

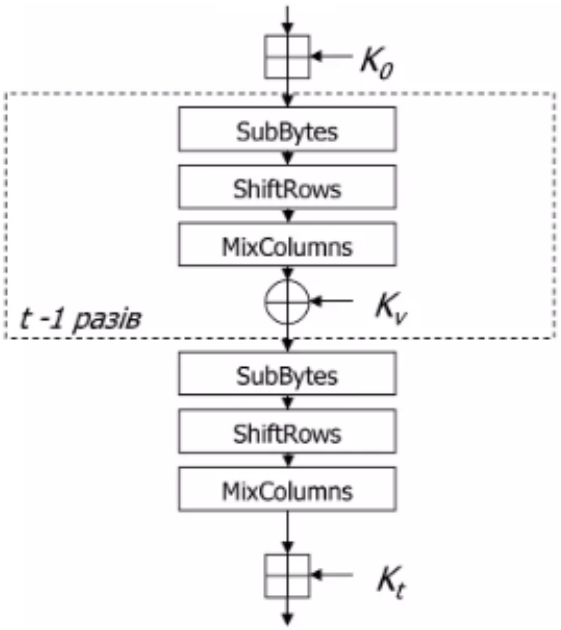
У шифрі AES операція ShiftRows виглядає наступним чином: перший рядок залишається без змін, другий рядок зсувається на один байт вліво, третій рядок зсувається на два байти вліво, а четвертий рядок зсувається на три байти вліво.

У шифрі Калина операція ShiftRows набагато більш складна. Блок даних у шифрі Калина поділяється на 8 рядків по 8 байтів у кожному. Операція ShiftRows змінює взаємне розташування байтів у кожному рядку відповідно до вектора зсувів, який залежить від номеру рядка та номеру раунду. У першому раунді всі вектори зсувів рівні нулю, а у наступних раундах вони обчислюються відповідно до формул, які включають у себе операції над полями Галуа.

Отже, хоча обидва шифри використовують операцію ShiftRows, реалізації цієї операції в них досить різні.

Шифри AES та Калина є досить стійкими та безпечними. Обидва шифри мають відомі результати стійкості, які були отримані після численних криптоаналітичних атак та перевірок.

Одна з останніх атак, яка була проведена на шифр AES - атака усічених бумерангів на 6-раундовий AES [6], аналіз та результати якої будуть розглянуті надалі.



$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ$$
$$\circ \left(\prod_{v=1}^{t-1} \left(\kappa_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi_l' \right) \right) \circ \eta_l^{(K_0)}$$

Рисунок 1.5 – Схема шифрування Калина

1.4 Атака усічених бумерангів

Атака усічених бумерангів (англ. "Truncated Differential Attack") - це криптографічна атака на блочний шифр, яка заснована на використанні диференціального аналізу і зменшенні розміру повідомлення, що аналізується. Для проведення атаки усічених бумерангів зловмисник повинен вибрати дві пари блоків повідомлень, які відрізняються в декількох бітах, і обчислити різницю між результатами шифрування цих пар блоків. Потім зловмисник здійснює пошук інших пар блоків, які відрізняються в тих самих бітах, що і попередні пари. Ці пари блоків повідомлення називаються "бумерангами". Якщо знайдеться достатня кількість бумерангів, то можна скласти їх у цепочки і використати для отримання значень ключа шифрування.

Атака усічених бумерангів є досить ефективною, особливо якщо шифр використовується зі слабкими ключами. Однак, вона вимагає великої кількості обчислювальних ресурсів і попередньої підготовки для знаходження достатньої кількості бумерангів.

Розглянемо більш формально схему атаки. Введемо дві усічені різниці $D_{in}^0 \xrightarrow[E_0]{p} D_{out}^0$ і $D_{in}^1 \xrightarrow[E_0]{p} D_{out}^1$ з імовірностями $\overrightarrow{p}$, $\overleftarrow{p}$ та $\overleftarrow{q}$ відповідно на E_0 та E_1. Припустимо, що D_{in}^0 - це векторне підпростір $\{0,1\}^n$ та $0 \notin D_{out}^0$. Атака усіченого бумеранга виконується наступним чином [6]:

1) Обирається випадковий відкритий текст P_0 та робиться запит на шифрувальний оракул на структурі $P_0 + D_{in}^0$; для кожного $i \in D_{in}^0$, ми визначаємо $P_i = P_0 + i$ та $C_i = E(P_i)$.

2)Для кожного шифртексту C_i, робиться запит на оракул розшифрування на множині $C_i + D_{out}^1$: для кожного $j \in D_{out}^1$, знаходять $\overline{C_i}^j = C_i + j$ та $\overline{P_i}^j = E^{-1}(\overline{C_i}^j)$.

3)Підраховується кількість пар $(\overline{P_i}^j, \overline{P_{i'}}^{j'})$ з умовою $\overline{P_i}^j + \overline{P_{i'}}^{j'} \in D_{in}^0$ (та $i \neq i', j \neq j'$). Це можна зробити ефективно, проектуючи значення відкритого тексту на ортогональне доповнення D_{in}^0 у $\{0,1\}^n$, шукаючи колізії.

4)Якщо потрібно, повторюються кроки $1-3$ з різними структурами відкритого тексту.

Аналіз атаки. Будемо вважати, що потенційний квартет $(P, P', \overline{P}, \overline{P'})$ відповідає квартету зашифрованих текстів $(C, C', \overline{C}, \overline{C'})$, де $P + P' \in D_{in}^0$ та $C + \overline{C}$, $C' + \overline{C}' \in D_{out}^1$. Отримаємо:

$$Pr[E_0(P) + E(P') \in D_{out}^0] = \overrightarrow{p}$$

$$Pr[E_1^{-1}(C) + E_1^{-1}(\overline{C}) \in D_{in}^1] = \overleftarrow{q}$$

$$Pr[E_1^{-1}(C') + E_1^{-1}(\overline{C'}) \in D_{in}^1] = \overleftarrow{q}$$

Згідно аналізу сендвіч-атаки (де $E_m = id$) визначаємо імовірність бумерангової зв'язності:

$$r = Pr\left[E_0(\overline{P} + E_0(\overline{P'}) \in D_{out}^0 \,\middle|\, \begin{array}{r} E_0(P) + E_0(P') \in D_{out}^0 \\ E_1^{-1}(C) + E_1^{-1}(C') \in D_{in}^1 \\ E_1^{-1}(C') + E_1^{-1}(\overline{C'}) \in D_{in}^1 \end{array}\right]$$

Якщо чотири події виконуються, має місце $\overline{P}+\overline{P'} \in D_{in}^0$ з додатковою ймовірністю $\overleftarrow{p}$. Аналіз усіченого бумерангу є тим же, що й запропоновано Вагнером [2], але наша атака є більш загальною зі структурами на обох сторонах.

Взагалі, $E_1^{-1}(C) + E_1^{-1}(\overline{C})E_1^{-1}(C')$ належать D_{in}^1, тому вони будуть рівні з імовірністю $|D_{in}^1|^{-1}$ і це передбачає, що $E_0(\overline{P}) + E_0(\overline{P'}) \in D_{out}^0$; отже $r \geq |D_{in}^1|^{-1}$. Більш того, якщо D_{in}^1 та D_{out}^0 векторні простори, то $\sum E_0(P) + E_0(P') + E_0(\overline{P}) + E_0(\overline{P}') \in D_{in}^1$; зокрема $\sum \in D_{out}^0$ з імовірністю $|D_{out}^0 \cap D_{in}^1|/|D_{in}^1$; це означає $E_0(\overline{P}) + E_0(\overline{P}') \in D_{out}^0$, отже $r \geq |D_{out}^0 \cap D_{in}^1|/|D_{in}^1|$.

Припускаємо, що всі події незалежні, кожен квартет $(P_i, P_{i'}, \bar{P}_i^j, \bar{P}_{i'}^{j'})$ визначається парою $(i,j),(i',j')$, йде по усіченому сліду бумеранга з імовірністю p_b і випадковим чином задовольняє $\bar{P}_i^j + \bar{P}_{i'}^{j'} = D_{in}^0$ з імовірністю $p_\$$:

$$p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q^2} \cdot r \quad r = |D_{in}^1|^{-1}$$
$$p_\$ = |D_{in}^0|/2^n$$

Припускаємо, що ймовірність бумеранга може бути апроксимована як $p_b + p_S$. Ми розрізняємо шифр E від випадкової перестановки, коли очікувана кількість квартетів (квартетів з $\overline{P_{i'j'}} + \overline{P_{i'j'}} \in D_{in}^0$) є значно вищою для E, ніж для випадкової перестановки. Ми визначаємо відношення сигнал-шум:

$$\sigma = \frac{p_b}{p_\$} \tag{1.4}$$

Коли $\sigma \geqslant 1$, ми отримуємо розпізнавальний алгоритм за допомогою $Q = O(p_b^{-1})$ квартетів. Більш точно з $Q = \mu \cdot p_b^{-1}$ (де μ - мала константа) очікується, що з шифром E залишиться μ квартетів, порівняно з $\mu \cdot \sigma^{-1}$ квартетів у випадку випадкової перестановки. Розпізнавальний алгоритм, що виявляє наявність хоча б одного квартета, має успішність $1 - e^{-\mu}$.

Коли σ менше, нам потрібно зібрати велику кількість квартетів та

порівняти очікувану кількість квартетів q_b для E та $q_\$$ для випадкової перестановки:

$$q_b = Q \times (p_S + p_b) = Q \times p_s(1 + \sigma)$$

$$q_S = Q \times p_\$$$

З теореми 1.1 можемо визначити $Q = O(p_\$^{-1}\sigma^{-2}) = O(p_b^{-1}\sigma^{-1})$.

Теорема 1.1. *Нехай X та Y - розподіли, і припустимо, що подія e відбувається в X з ймовірністю p та в Y з ймовірністю $p(1+q)$. Тоді для невеликих p та q, достатньо $O(\frac{1}{pq^2})$ вибірок, щоб відрізнити X від Y зі сталим успіхом [5].*

Використовуючи $Q = c \times p_b^{-1}\sigma^{-1}$ з маленькою константою c і встановленням порогу в $Q \times p_\$(1 + \sigma/2)$, розпізнавач має успішний шанс $\Phi(\sqrt{c/2})$, де Φ є кумулятивною функцією розподілу стандартного нормального розподілу.

Якщо Q менше ніж кількість квартетів в повній структурі $(|D_i^0 n|^2 |D_{out}^1|^2/2)$, то будуть використовуватись часткові структури тільки з $\sqrt{2Q}$ елементів. Завершуємо побудову розпізнавального алгоритму з постійною ймовірністю успіху з наступною складністю за кількістю квартетів, часом, даними та пам'яттю:

$$T = D = \max(\sqrt{2Q}, 2Q \times |D_{in}^0|^{-1} |D_{out}^1|^{-1} \tag{1.5}$$

$$Q = O\left(\max\left(p_b^{-1}, \sigma^{-1} p_b^{-1}\right)\right) \tag{1.6}$$

$$M = \min(D, |D_{in}^0||D_{out}^1|) \tag{1.7}$$

В роботі [6] було розглянуто атаку усічених бумерангів на прикладі 6-раундового шифру AES. В якості D_{in}^0 та D_{out}^1 розглядались такі матриці, в яких всі елементи нульові окрім елементів на головній діагонали. D_{out}^0 - вихідні матриці у форматі як зазначино на малнюку 1.5, D_{out}^1 - матриці, в яких на всіх діагоналях нулі окрім головної антидіагоналі. З цього було отримано наступні параметри:

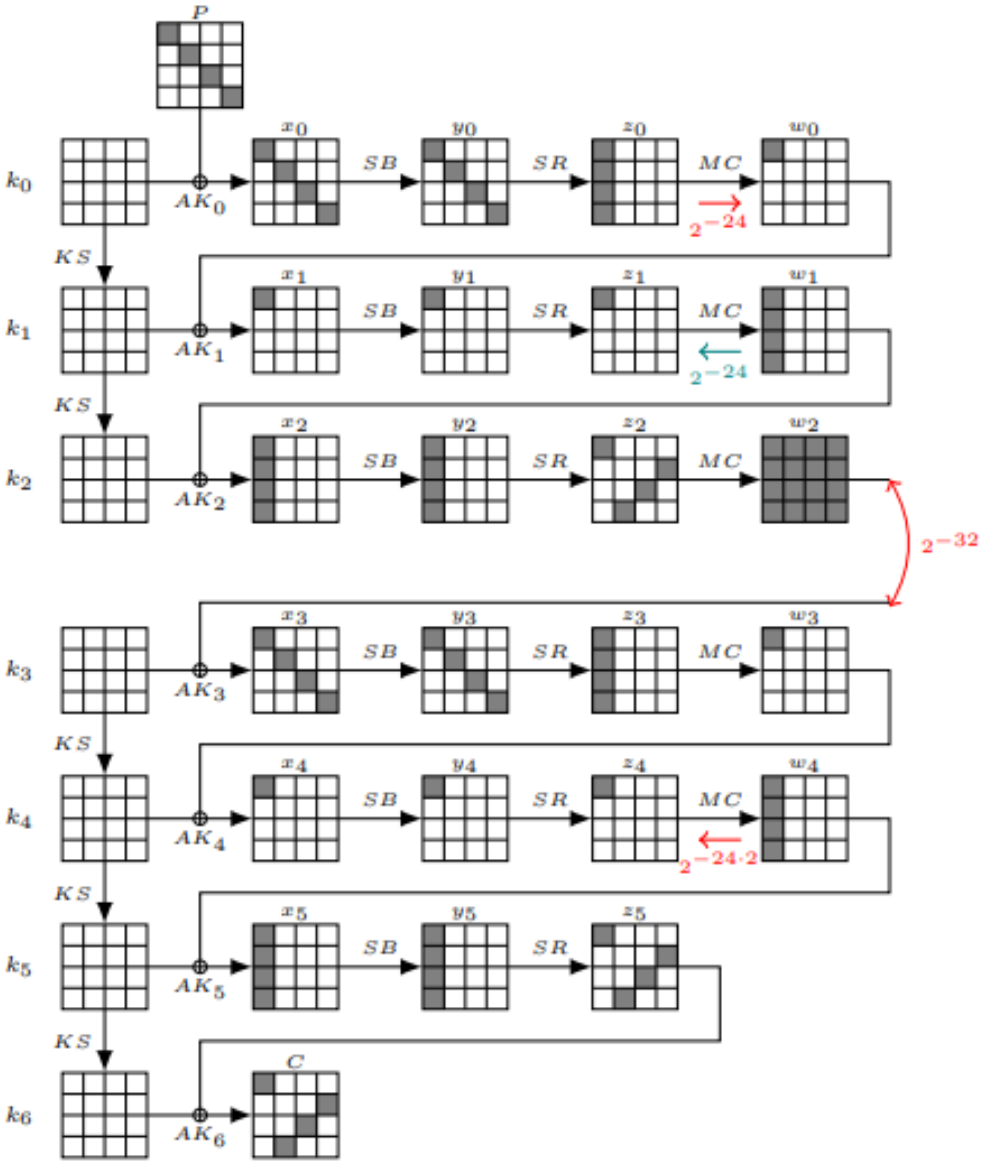


Рисунок 1.6 – Усічений слід бумеранга на 6-раундовому AES

$$|D^0_{in}| = |D^0_{out}| = 2^{32} \quad \vec{p} = 2^{-24} \quad \overleftarrow{p} = 2^{-24}$$
$$|D^1_{in}| = |D^1_{out}| = 2^{32} \quad \vec{p} = 2^{-24} \quad \overleftarrow{p} = 2^{-24}$$

Так як $D^0_{out} \cap D^1_{in} = \{0\}$, в нас є $r = |D^1_{in}|^{-1}$, то наведений вище аналіз

дає наступні параметри:

$$p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q^2} \cdot r = 2^{-128} \quad \sigma = -2^{-32}$$
$$p_\$ \ = 2^-96 \qquad\qquad\qquad\quad Q = c * 2^{160}$$

Algorithm 1. Truncated boomerang distinguisher on 6-round AES

$q \leftarrow 0$
for $0 \leq s < 2^{35}$ **do** ▷ 2^{35} structures
  $P_0 \leftarrow \$$
  for $i \in \mathcal{D}_{\text{in}}^0$ **do** ▷ Iterate over the main diagonal
    $C_i \leftarrow E(P_0 + i)$
    for $j \in \mathcal{D}_{\text{out}}^1$ **do** ▷ Iterate over the main anti-diagonal
      $\overline{P_i}^j \leftarrow E^{-1}(C_i + j)$
      Store $\overline{P_i}^j$ in a hash table indexed by three diagonals
  Count collisions in the hash table, and increment q
if $q > 2^{66} + 2^{33}$ **then**
  return AES
else
  return $

Рисунок 1.7 – Алгоритм

Використовуючи c = 4 і формули рівнянь (4), (5) і (6), ми отримуємо розпізнавач зі складністю:

$$T = D = 2^{99} \quad M = 2^{64}$$

Розпізнавач детально описано в алгоритмі 1.7. Він виконує 2^{67} запитів на шифрування та 2^{99} на розшифрування, для загальної складності даних $D = 2^{67} + 2^{99} \approx 2^{99}$. Загалом маємо $Q = 2^{35} \times 2^{64} \times 2^{64}/2 = 2^{162}$ квартетів $(P_i, P_i', \overline{P_i}^j, \overline{P_{i'}}^{j'})$, так що очікувана кількість квартетів, що залишається:

$$q_\$ = Q \times 2^{-96} = 2^{66} \quad q_E = Q \times (2^{-96} + 2^{-128}) = 2^{66} + 2^{34}$$

Розпізнавач повертає правильну відповідь з імовірністю

$$\Phi = \sqrt{c/2} = 0.84.$$

Отже, опубліковані результати вказують на те, що 6-раундовий шифр AES, який раніше вважався стійким до атак типу бумерангу, може бути підданий успішній атакі з використанням усічених бумерангів. Це вказує на потенційну слабкість шифру на меншій кількості раундів та необхідність збільшення числа раундів для забезпечення більшої стійкості проти таких атак. Дані результати підкреслюють важливість подальшого дослідження та розробки криптографічних алгоритмів, які забезпечують високий рівень безпеки від нових атак, включаючи атаки типу бумерангу.

На даний момент не було проведено усіченої атаки бумерангів на шифр Калина. Це є актуальною задачею, яка була досліджена та більш детально розглянута в другому розділі.

Висновки до розділу 1

Отже, у першому розділі були розглянуті основні теоретичні відомості, що стосуються усічених диференціалів, атаки усічених бумерангів, основні властивості та схеми шифрування блокових шифрів AES і Калина.

Також детально була розглянута атака усічених бумерангів на 6-раундовий AES.

2 АТАКА УСІЧЕНИХ ДИФЕРЕНЦІАЛІВ НА КАЛИНА-ПОДІБНІ ШИФРИ

В даній главі буде побудовано атаки усічених бумерангів на шифр Калина-128, Калина-256, Калина-512 зі зменшеною кількістю раундів і та одержано оцінки стійкості до даного класу атак. Також буде проведено порівняльний аналіз для отриманих результатів та виявлено, яка з представлений конструкцій забезпечує більшу криптографічну стійкість для даного виду атак.

2.1 Атака усічених бумерангів на 6-раундовий шифр Калина-512

Розглянемо атаку усічених бумерангів на 6-раундовий шифр Калина-512 з модифікацією додавання ключа. Детальна схема атки представлена на рисунку 2.3.

Розкладаємо шифр E на композицію двох підшифрів E_0, який відповідає першим трьом раундам та E_1, який відповидає другим трьом раундам. В якості вхідної різниці D^0_{in} було використовано множину з матриць, які мають нулі на всіх діагоналях, крім головної антидіагоналі.

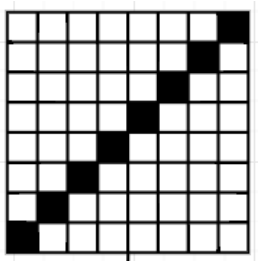


Рисунок 2.1 – Множина D^0_{in} для Калина-512

В якості вихідної різниці D^1_{out} розглядається множина, яка

складається з матриць, де всі елменти дорівнюють нулю, крім головної діагоналі, як зазначено на рисунку 2.2.

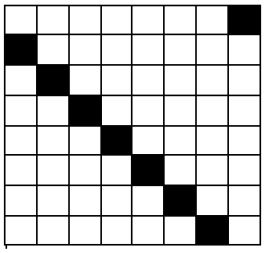


Рисунок 2.2 – Множина D^1_{out} для Калина-512

На першому раунді шифрування перехід після операції MixColumns з матриці, яка складається з одного ненульового стовпчика у матрицю, де тільки один елемент є ненульовим, відбувається з імовірністю $\overrightarrow{p}$. Імовірність зворотнього переходу на другому раунді при розшифрувані - $\overleftarrow{p}$. Всі інші переходи на перших трьох раундах будуть однозначні, так як перетворення MixColumns підібрано таким чином, що мінімальна кількість можливих ненульових байтів на вході і на виході обмежена знизу; для шифру Калина це не менше дев'яти.

Аналогічно для 4-6 раундів імовірність переходу при зашифрувані будемо позначати як $\overrightarrow{q}$, тоді зворотня імовірність $-\overleftarrow{q}$.

Множини D^0_{in} і D^0_{out} повністю співпадають. D^0_{out} буде складатись з матриць, які мають вигляд матриці w_2 на рисунку 2.3.

Отже, потужності даних множин та імовірності $\overrightarrow{p}, \overleftarrow{p}, \overrightarrow{q}, \overleftarrow{q}$ будуть мати наступні значення:

$$|D^0_{in}| = |D^0_{out}| = 2^{64} \quad \overrightarrow{p} = 2^{-56} \quad \overleftarrow{p} = 2^{-56}$$
$$|D^1_{in}| = |D^1_{out}| = 2^{64} \quad \overrightarrow{q} = 2^{-56} \quad \overleftarrow{q} = 2^{-56}$$

Припускаючи, що всі події незалежні, кожен квартет $(P_i, P_{i'}, \bar{P}^j_i, \bar{P}^{j'}_{i'})$

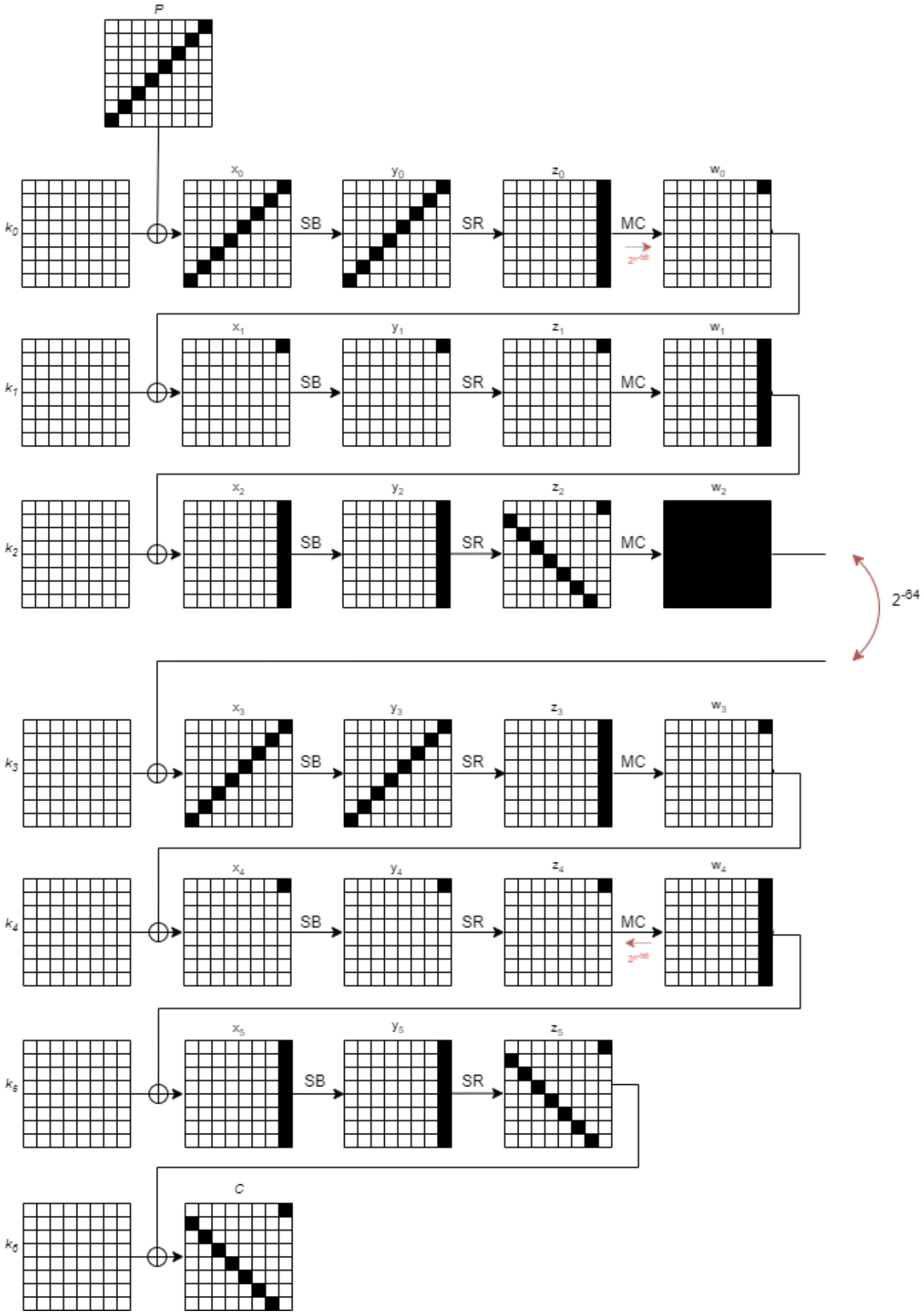


Рисунок 2.3 – Атака усічених бумерангів на 6-раундовий шифр Калина-512

визначається парою $(i,j),(i',j')$, йде по усіченому сліду бумеранга з імовірністю p_b і випадковим чином задовольняє $\bar{P}_i^j + \bar{P}_{i'}^{j'} = D_{in}^0$ з імовірністю $p_\$$:

$$p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q^2} \cdot r \quad r = |D_{in}^1|^{-1}$$
$$p_\$ = |D_{in}^0|/2^n$$

Так як $D_{out}^0 \cap D_{in}^1 = \{0\}$, у нас є $r = |D_{in}^1|^{-1}$, тому було отримано наступні параметри:

$$p_b = 2^{-56} \cdot 2^{-56} \cdot (2^{-56})^2 \cdot (2^{64})^{-1} = 2^{-288}$$
$$p_\$ = 2^{64}/2^{512} = 2^{-448}$$

Параметр p_b вказує на ймовірність, з якою усічена атака бумерангів буде успішною при виконанні певних передумов. Високе значення p_b вказує на більшу ймовірність успіху атаки, тоді як низьке значення свідчить про меншу ймовірність успіху.

Імовірність бумеранга може бути апроксимована як $p_b + p_\$$, тоді параметр сигнал-шум буде дорівнювати:

$$\sigma = \frac{p_b}{p_\$} = 2^{-288}/2^{-448} = 2^{160}.$$

У контексті атак усічених бумерангів, корисний сигнал відповідає певному вигляду усіченого шляху, тобто послідовності раундів шифру, що забезпечує можливість успішного проведення атаки. Небажаний шум, з іншого боку, описує випадковість атаки, яка може виникати з великої кількості випадкових проміжних значень, що виникають під час атаки. Якщо значення сигнал-шум більше одиниці, то це означає, що сигнал (кількість коректно працюючих квартетів) більше, ніж шум (кількість некоректно працюючих квартетів). Це зменшує кількість потенційних "шумових"квартетів, які можуть дати помилкові результати, і дозволяє

фокусуватись на меншій кількості квартетів під час атаки усічених бумерангів.

Так як, $\sigma \gg 1$, то потрібно буде проаналізувати значно менше квартетів, а саме

$$Q = \mu \cdot p_b^{-1}.$$

Зазначимо, що константа μ дорівнює чотирьом, тоді

$$Q = 2^{290}.$$

Використовуючи формули 1.5 - 1.7 обчислимо час, дані та пам'ять, які буде затрачено при побудові розпізнавального алгоритму.

$$T = D = \max(\sqrt{2Q}, 2Q \times |D_{in}^0|^{-1}|D_{out}^1|^{-1} = 2^{163},$$

$$M = \min(D, |D_{in}^0||D_{out}^1|) = 2^{128}.$$

,

Побудуємо атаку усічених диференціалів для модифікацій шифру Калина з меншою довжиною ключа та порівняємо параметри Q, T, D, M з тими, що було отримано вище.

2.2 Атака усічених бумерангів на 6-раундовий шифр Калина-256

Перейдемо до атаки усічених бумерангів на 6-раундовий шифр Калина-256.

В якості множин з вхідними та вихідними різницями будемо розглядати такі D_{in}^0, D_{in}^1($D_{in}^0 = D_{in}^1$) та D_{out}^1, які складаються з матриць, в яких кожен стовпчик має два ненульових значення та мають структуру зазначену на рисунку 2.4.

На загальній схемі шифрування зображеній на рисунку 2.6 матриця w_2, яка належить множені D_{out}^0, позначена сірим кольором. Така нотація

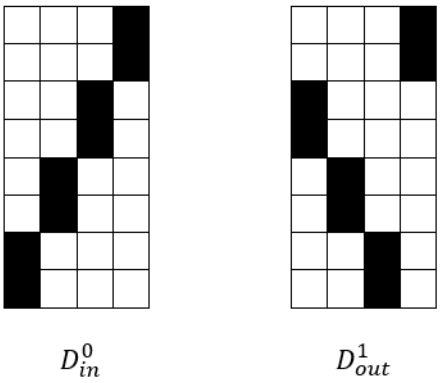


Рисунок 2.4 – Множини D^0_{in} та D^1_{out} для Калина-256

була введена, щоб зазначити, що матриця z_2 після застосування опереції MixColumns не обов'язково перейде в повністю ненульову матрицю. Множина D^0_{out} складається з матриць розміром 8 на 4, кожний стовпчик якої буде мати, як мінімум, 7 ненульових байтів, але розташування цих байтів може бути довільним.

Розглянемо перший стовпчик матриці z_2, в ньому два ненульових елемента, значить після застосування операції MixColumns матриця w_2 повинна мати не менше семи ненульових елементів.

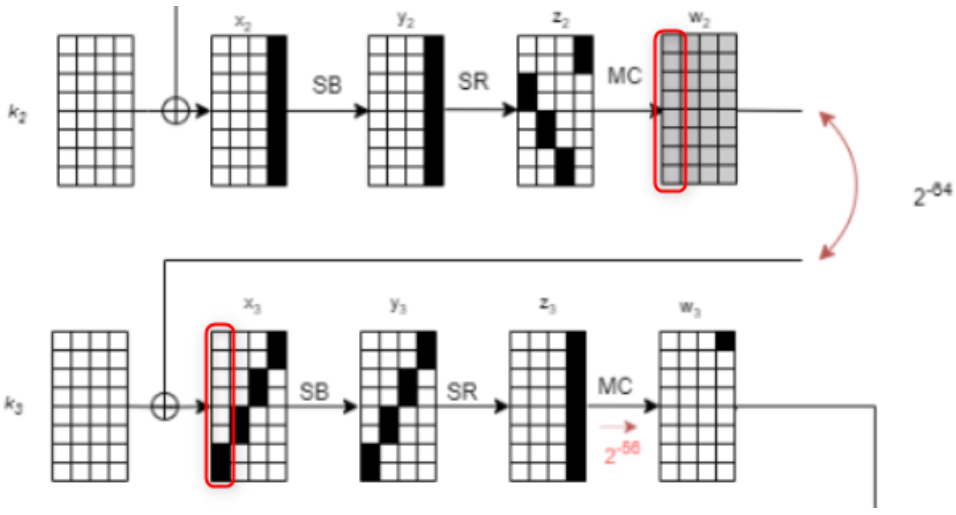


Рисунок 2.5 – Перетворення матриць після операції MixColumns для Калина-256

Відповідно в двох стовпчиках, виділених на рисунку 2.5 червоним

кольором, обов'язково знайдеться байт, який в x_3 буде нульовим, а в w_2 ненульовим, що вказує нам на те, що $D^0_{out} \cap D^1_{in} = \{0\}$.

Потужності даних множин і ймовірності $\overrightarrow{p}, \overleftarrow{p}, \overrightarrow{q}, \overleftarrow{q}$ будуть мати наступні значення:

$$\begin{aligned} |D^0_{in}| &= 2^{64} & \overrightarrow{p} &= 2^{-56} & \overleftarrow{p} &= 2^{-56} \\ |D^1_{in}| &= |D^1_{out}| = 2^{64} & \overrightarrow{q} &= 2^{-56} & \overleftarrow{q} &= 2^{-56} \end{aligned}$$

Вище було зазначино, що множини D^0_{out} та D^0_{in} не перетинаються, тому $r = |D^1_{in}|^{-1}$.

Отримаємо значення для імовірностей

$$p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q^2} \cdot r = 2^{-56} \cdot 2^{-56} \cdot (2^{-56})^2 \cdot (2^{64})^{-1} = 2^{-288}$$
$$p_\$ = 2^{64}/2^{256} = 2^{-192}$$

Апраксимуємо імовірність бумеранга як $p_b + p_S$, та отримаємо співвідношення сигнал-шум:

$$\sigma = \frac{p_b}{p_S} = 2^{-288}/2^{-192} = 2^{-96}$$

В даному випадку сігма вже не буде значно більше одиниці, тому нам потрібно буде розглядати більшу кількість квартетів для аналізу.

$$Q = c \times p_b^{-1} \cdot \sigma^{-1}$$

Замість c підставляємо константу, яка дорівнює чотирьом.

$$Q = 4 \times 2^{288} \times 2^{96} = 2^{386}.$$

Знайдемо час та пам'ять, які будуть використані побудови розпізнавача.

$$T = D = \max(\sqrt{2Q}, 2Q \times |D^0_{in}|^{-1} |D^1_{out}|^{-1}$$

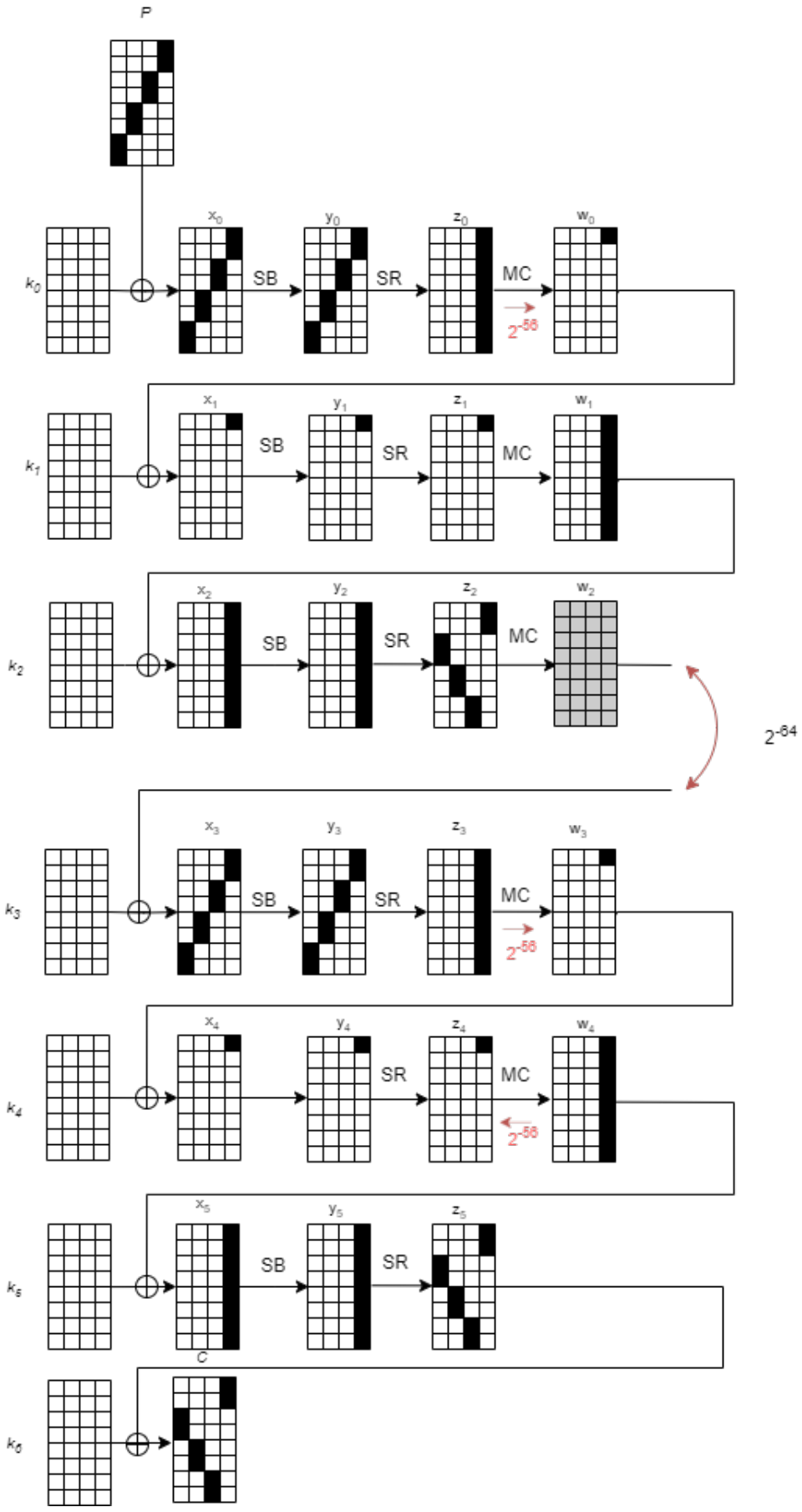


Рисунок 2.6 – Атака усічених бумерангів на 6-раундовий шифр Калина-256

$$M = \min(D, |D^0_{in}||D^1_{out}|)$$

З цього слідують наступні результати:

$$T = D = 2^{259}, M = 2^{128}.$$

В даному випадку атака є менш ефективною, ніж для Калина-512, так як кількість квартетів, які потрібно буде проаналізувати, приймає значення більше за повний перебір.

2.3 Атака усічених бумерангів на 6-раундовий шифр Калина-128

Перейдемо до атаки усічених бумерангів на 6-раундовий шифр Калина-128.

В якості вхідної різниці для атаки усічених бумерангів на 6-раундовий шифр Калина-128 з модифікацією додавання ключа була використана структура виду, яка зазначена на малюнку 2.7. Множини D^0_{in} і D^1_{in} повністю співпадають.

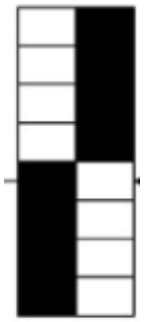


Рисунок 2.7 – Вхідна різниця для Калина-128

Множина D^0_{out} складається з матриць, в яких, як мінімум п'ять ненульових байтів в кожному стовпчику, ці байти можуть бути розташовани випадковим чином. Розглянемо рисунок 2.8: $w_2 \in D^0_{out}$, $x_3 \in D^1_{in}$. В матриці виду w_2 в кожному стовпчику може бути не більше

трьох нульових елементів. В матриці виду x_3 в кожному стовпчику завжди є чотири нульових елемента, тобто завжди знайдеться нульовий елемент, який буде в x_3, але не буде в w_2. З цього можемо зробити висновок, що множини D^0_{out} іD^1_{in} не перетинаються.

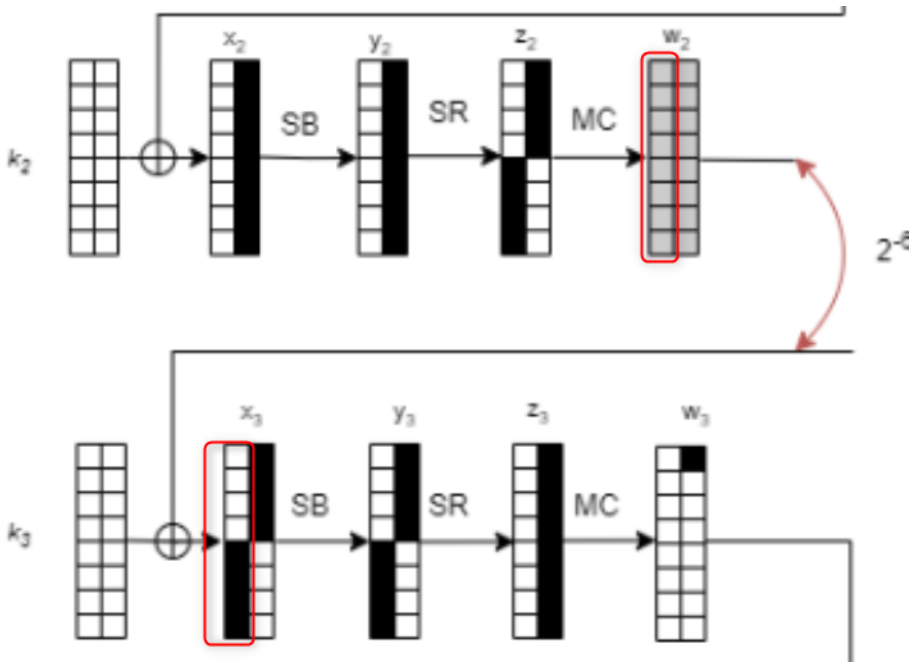


Рисунок 2.8 – Множини D^0_{out} s і D^1_{in} в Калина-128

Для даної конструкції потужності множин D^0_{in}, D^1_{in}, D^1_{out} та ймовірності $\vec{p}$, $\overleftarrow{p}$ $\vec{q}$, $\overleftarrow{q}$ будуть мати такі ж самі значення, що і для попередніх модифікацій.

$$|D^0_{in}| = 2^{64} \qquad \vec{p} = 2^{-56} \quad \overleftarrow{p} = 2^{-56}$$
$$|D^1_{in}| = |D^1_{out}| = 2^{64} \quad \vec{q} = 2^{-56} \quad \overleftarrow{q} = 2^{-56}$$

За відомими для нас формулами було отримано результати для p_b та $p_\$$.

$$p_b = 2^{-56} \cdot 2^{-56} \cdot (2^{-56})^2 \cdot (2^{64})^{-1} = 2^{-288}$$
$$p_\$ = 2^{64}/2^{128} = 2^{-64}$$

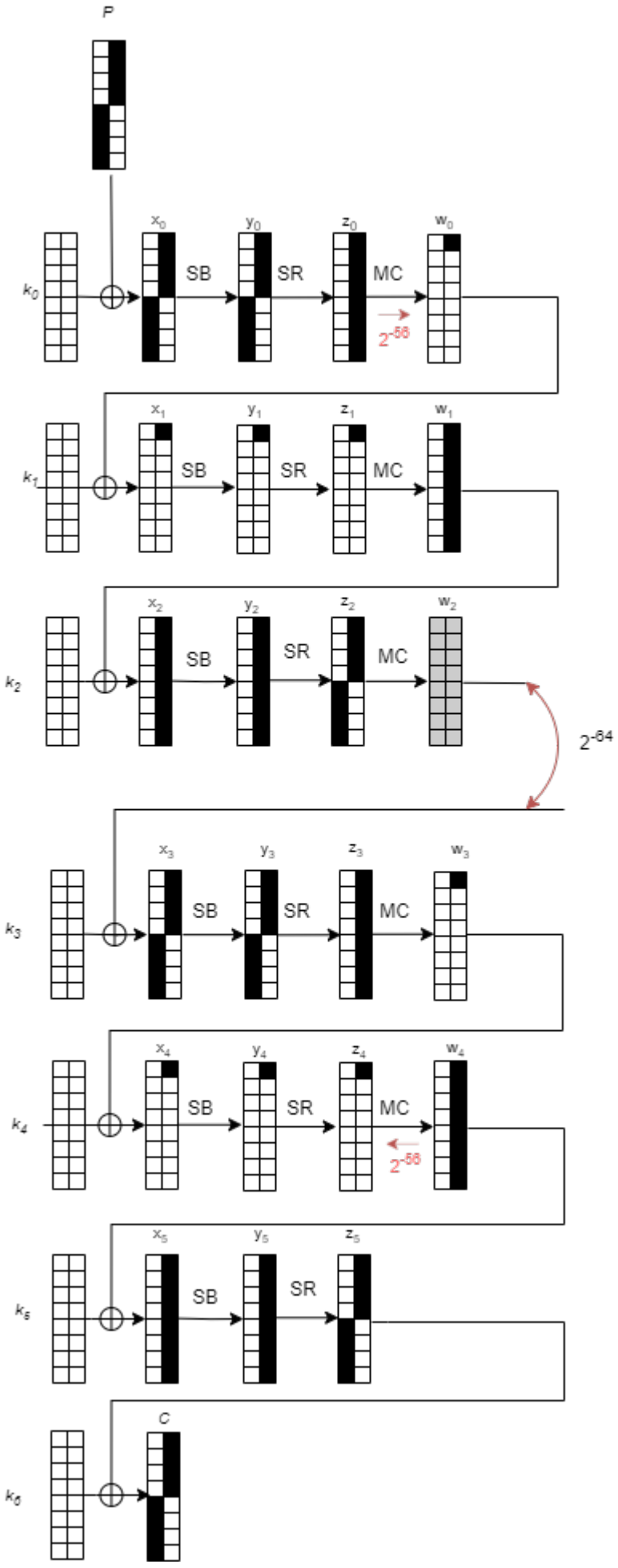


Рисунок 2.9 – Атака усічених бумерангів на 6-раундовий шифр

З цього виходить, що відношення сигнал-шум буде:

$$\sigma = \frac{p_b}{p_S} = 2^{-288}/2^{-64} = 2^{-224}$$

Так як σ дуже маленька, то нам потрібно кількість квартетів для аналізу вироховується по формулі:

$$Q = c \times p_b^{-1} \cdot \sigma^{-1}$$

При c = 4, отримаємо кількість квартетів

$$Q = 4 \cdot 2^{512} = 2^{514}.$$

Використовуючи формулу 1.5 було отримано значення T і D.

$$\begin{aligned} T = D &= \max(\sqrt{2Q}, 2Q \times |D_{in}^0|^{-1}|D_{out}^1|^{-1}) \\ &= \max(\sqrt{2^{515}}, 2 \cdot 2^{514} \times 2^{-64} \cdot 2^{-64}) = 2^{387}. \end{aligned}$$

.

Показник пам'яті в даному випадку буде приймати таке саме значення, що і для Калина-512, Калина -256.

$$M = \min(D, |D_{in}^0||D_{out}^1|) = 2^{128}$$

.

Також слід звернути увагу на те, що множини D_{in}^0 та D_{out}^0 будуть ідентичні. Ця властивість може надалі враховуватись при аналізі подібних конструкцій.

Висновки до розділу 2

У даному розділі було побудовано атаку усічених бумерангів для 6-раундових Калина-128, Калина-256, Калина-512. Виведені параметри

стійкості для цих шифрів до атаки усічених бумерангів.

Таблиця 2.1 – Результати атаки

Шифр	Q	T=D	M
Калина-128	2^{514}	2^{387}	2^{128}
Калина-256	2^{386}	2^{259}	2^{128}
Калина-512	2^{290}	2^{163}	2^{128}

Основною перевагою Калини-512 порівняно з Калиною-256 та Калиною-128 є більша довжина ключа. Це означає, що Калина-512 може забезпечити більшу криптографічну стійкість і міцніше захистити дані від атак з використанням brute force (грубої сили) або інших криптоаналітичних методів. Згідно з отриманими результатами атака усічених бумерангів вцілому не є ефективною для всіх трьох випадків, але для Калина-512 вона буде більш ефективною, так як параметри стійкості Q, T, D мають значення менше за повний перебір.

ВИСНОВКИ

У ході даної роботи був проведений детальний аналіз опублікованих джерел за тематикою дослідження, який показав, що ще не було проведено атаки усічених бумерангів для шифру Калина. Тому у цій роботі було побудовано атаки усічених бумерангів на шифр Калина-128, Калина-256, Калина-512 зі зменшеною кількістю раундів та одержано оцінки стійкості до даного класу атак.

Для конструкцій 6-раундового шифру Калина-128, Калина-256 та Калина-512 були отримані такі парамтери, як кількість квартетів, які потрібно буде розглянути при атаці, час та пам'ять, що будуть витрачені при побудові розпізнавального алгоритму.

Отримані результати вказують на те, що для всіх трьох випадків кількість квартетів, які потрібно буде проаналізовувати для проведення атаки є вельме великою. Для шифрів з довжиною ключа 128, 256 це значення більше за повний перебір, що вказує на нефективність даної атаки; при довжині ключа 512 атака буде більш ефективною, що є достатньо нетиповим, так як зазвичай кращі результати стійкості для інших атак показував шифр, який мав більшу довжину ключа. Аналогічний висновок можна зробити і для параметрів T, D.

Більш того, варто звернути увагу на значення параметра p_b для всіх трьох конструкцій, який вказує на імовірність успішного вибору різниці бумерангу з випадковою різницею, коли проводиться атака усічених бумерангів та порівняти з бутфорсом повідомлення. Отримані результати знов вказують нам на те, що розглянуті конструкції, особливо Калина-128, Калина-256, є стійкими до атаки усічених бумерангів.

Також вартно звернути увагу на те, що при атаці на 6-раундову Калину-128 множина вхідних різниць повністю співдає з множиною вихідних різниць.

Результати роботи можуть бути використані для поширеного

аналізу Калина-подібних шифрів, які будуть стійкими до атаки усічених бумерангів. Також варто зазначити, що для майбутнього аналізу можна првести аналогічну атаку, але для більшої кількісті раундів на Калина-подібні шифри та порівняти з існуючими вже результатами. Виявлення можливих слабкостей та розробка нових методів атаки можуть сприяти розробленю більш стійких криптографічних алгоритмів, що забезпечують безпеку інформації.

ПЕРЕЛІК ПОСИЛАНЬ

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

4. Knudsen L. Truncated and Higher Order Differentials / Lars R. Knudsen // Fast Software Encryption: Second International Workshop. Proceedings / Lars R. Knudsen. — Leuven, Belgium: Springer, 1994. — (Lecture Notes in Computer Science; вип. 1008). — С. 196 – 211.

5. Itsik Mantin and Adi Shamir. A practical attack on broadcast RC4. In Mitsuru Matsui, editor, FSE 2001, volume 2355 of LNCS, pages 152–164. Springer, Heidelberg, April 2002

6. Augustin Bariant and Gaëtan Leurent, Truncated Boomerang Attacks and Application to AES-based Ciphers, Cryptology ePrint Archive, Paper 2022/701

7. Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001.

8. Oliynykov, Roman; Gorbenko, Ivan; Kazymyrov, Oleksandr; Ruzhentsev, Victor; Kuznetsov, Oleksandr; Gorbenko, Yurii; Dyrda, Oleksandr; Dolgov, Viktor; Pushkaryov, Andrii; Mordvinov, Ruslan; Kaidalov, Dmytro (2015). A New Encryption Standard of Ukraine: The Kalyna Block Cipher

.