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

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___” _____ 2020р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 Прикладна математика
(код і назва)

на тему: Розпізнавачі "Калина"-подібних шифрів на основі їх алгебраїчних та структурних властивостей _____
_____
_____

Виконав (-ла): студент (-ка) 2 курсу, групи ФІ-81м.н.в.
(шифр групи)

Столович Михайло Вадимович _____ _____
(прізвище, ім’я, по батькові) (підпис)

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

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

ерській дисертації 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: другий (магістерський) за освітньо–професійною програмою

Спеціальність: 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
«___»_____20_ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Столович Михайло Вадимович
(прізвище, ім'я, по батькові)

1. Тема дисертації Розпізнавачі "Калина"-подібних шифрів на основі їх алгебраїчних та структурних властивостей _____
_____ ,
науковий керівник дисертації к.т.н. доцент Яковлєв Сергій Володимирович ___ ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____р. № _____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження інформаційні процеси в системах криптографічного захисту _____
_____

4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо–професійною програмою) моделі та методи криптоаналізу ланцюгів перетворень підпросторів симетричних блочних шифрів
_____
_____

5. Перелік завдань, які потрібно розробити: провести огляд опублікованих джерел за тематикою дослідження; дослідити новітні методи криптоаналізу лакцюгів перетворень підпросторів у застосувані до «Калина»-подібних шифрів; побудувати розпізнавачі калина-подібних шифрів;
_____

_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____
_____
_____

8. Консультанти розділів дисертації*

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

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	провести огляд опублікованих джерел за тематикою дослідження	вересень-жовтень 2018р.	
2	дослідити новітні методи криптоаналізу лакцюгів перетворень підпросторів у застосувані до «Калина»-подібних шифрів	жовтень 2018р.	
3	побудувати розпізнавачі калина-подібних шифрів	листопад-грудень 2018р.	

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Кваліфікаційна робота містить: 56 стор., 13 рисунків, 2 таблиці, 4 джерела.

У роботі було побудовано розпізнавачі за методом аналізу ланцюгових перетворень та проаналізовано стійкість Калина-подібних шифрів до криптоаналізу за методом ланцюгових перетворень. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є моделі та методи криптоаналізу ланцюгів перетворень підпросторів.

У роботі було побудовано розпізнавачі за методомо ланцюгових перетворень і методом нульової різниці для 5-раундових Калина-подібних шифрів. Також за методом неможливого інтеграла було побудовано 3-раундові розпізнавачі Калина-подібних шифрів.

ЛАНЦЮГОВІ ПЕРЕТВОРЕННЯ, КАЛИНА, НУЛЬОВА РІЗНИЦЯ, НЕМОЖЛИВИЙ ІНТЕГРАЛ

ABSTRACT

Qualification work contains: 56 pages, 13 figures, 2 tables, 4 sources.

In the work we built distinguishers based on subspace trail cryptanalysis for «Kalyna»-like cyphers. Also complexity of building such distinguishers was analyzed. The object of research is information processes in cryptographic protection systems. The subject of research is models and methods of subspace trail cryptanalysis.

In the work, distinguishers were constructed with the method of subspace trail cryptanalysis and the zero-difference method for 5-round «Kalyna»-like ciphers. Also 3-round Kalina-like cypher distinguishers were constructed with impossible mixture integral method.

SUBSPACE TRAIL CRYPTANALYSIS , KALYNA, ZERO-DIFFERENCE, IMPOSSIBLE INTEGRAL

ЗМІСТ

ВСТУП

Сучасні блокові шифри, такі як AES чи «Калина», стійкі до відомих методів криптоаналізу. Вони побудовані таким чином, щоб раундове перетворення із кожним новим раундом згладжувало структурні особливості вхідних текстів і шифртекст виглядав як випадкова послідовність. Тому зараз великий інтерес для дослідження становить аналіз структурних алгебраїчних властивостей таких шифрів.

Одним із методів криптоаналізу таких AES-подібних SP-мереж є аналіз ланцюгів перетворень підпросторів.

Актуальність дослідження. Актуальність даного дослідження полягає у тому, що останні результати дослідженнь ланцюгів перетворень підпросторів не застосовувалися до шифру «Калина». А так як аналіз ланцюгів перетворень підпросторів є новітнім методом аналізу шифрів, то актуально дослідити, стійкість шифру «Калина» до цього методу криптоаналізу.

Метою дослідження є проаналізувати стійкість та побудувати розпізнавачів для «Калина»-подібних шифрів. Для досягнення мети необхідно розв'язати **задачу дослідження**, яка полягає у побудові розпізнавачів «Калина»-подібних шифрів. Для розв'язання задачі необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) дослідити новітні методи криптоаналізу лакцюгів перетворень підпросторів у застосувані до «Калина»-подібних шифрів;

3) побудувати розпізнавачі калина-подібних шифрів;

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

Предметом дослідження є моделі та методи криптоаналізу ланцюгів перетворень підпросторів симетричних блочних шифрів.

При розв'язанні поставлених завдань використовувались такі *методи*

дослідження: теорії імовірностей, комбінаторного аналізу.

Наукова новизна отриманих результатів полягає в тому, що були застосувані новітні методи аналізу ланцюгів перетворень підпросторів для побудови розпізнавачів «Калина»-подібних шифрів.

Практичне значення результатів полягає в тому, що було досліджено структурні та алгебраїчні властивості «Калина»-подібних шифрів, що дозволить в подальшому покращити стійкість щифру «Калина».

Апробація результатів та публікації. Певні результати даної роботи були представлені на XVIII Науково-практичній конференції студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики"(12-13 травня 2020 р., м. Київ).

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

У данному розділі розглянемо, що таке SP-мережа, шифр «Калина». Також розглянемо модифікацію шифра «Калина», яку будемо застосовувати для побудови розпізнавачів.

Розглянемо теоретичні відомості із криптоаналізу на основі ланцюгів перетворення підпросторів, криптоаналізу нульової різниці та змішаного інтегрального методу.

1.1 SP-мережа та «Калина»-подібні шифри

SP-мережа – це ітеративний блоковий шифр виду:

$$E_K(X) = R_{K_r}(R_{K_{r-1}}(...(R_{K_0}(X))..),$$

де $K = (K_1, K_2, .., K_r) \in \Theta^{mr}$ – ключ шифрування, Θ^{mr} – ключовий простір одного блоку. Раундове перетворення R визначається наступним чином:

$$R : (V_t)^m \times (\Theta)^{mr} \to (V_t)^m,$$
$$R(X, K) = L(S_K(X)),$$

де $L : (V_t)^m \to (V_t)^m$ – лінійне відносно операції $\oplus$ перетворення, а $S_K(X)$ – функція, що описує рівень S-блоків залежних від ключа:

$$S_K(X) = (s_1(x_1, k_1), .., s_m(x_m, k_m)),$$

де $K = (K_1, K_2, .., K_r) \in \Theta^m$. Функції $s_i(x_i, k_i)$ повинні бути бієктивними при кожному фіксованому значенні ключа.

1.1.1 Шифр AES

Шифр AES – це американський стандарт блокового симетричного шифрування. Він має розмір блоку 128 біт та розмір ключа 128, 192, 256 біт.

Зашифрування Пряме перетворення алгоритму AES складається із наступних операцій:

1) Шар нелінійного бієктивного відображення (SubBytes):
На даному етапі ми застосовуємо до кожного байту матриці внутрішнього стану $G = (g_{i,j})$ підстановку $S : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}, k = 0, 1, 2, 3.$

2) Перестановка елементів (ShiftRows):
Дана операція виконує циклічний зсув вліво рядків матриці стану.

3) Лінійне перетворення (MixColumns):
Дана операція виконується наступним чином: кожен елемент матриці стану представляється як елемент $GF(2^4)$. Кожен елемент результуючої матриці стану отимується, як результат множення векторів довижини 4 над полем $GF(2^4)$.

1.1.2 Шифр «Калина»

Шифр «Калина» – це український стандарт блокового шифрування [1]. «Калина» є шифром, побудованим на схемі SP-мережі, структура якого подібна до структури AES.

Шифр розроблений вітчизняними спеціалістами, і в результаті конкурсу був обран стандартом України ДСТУ 7624:2014.

Шифр Калина має різну кількість ітерацій в залежності від розміру ключа і блоку. Побачити цю залежність можна в таблиці1.1.

Вхідні тексти записуються у вигляді матриці елементів з $\mathbb{F}_{2^8}$ розміру 8×2, 8×4, 8×8 відповідно. Далі будемо позначати матриці стану як $\mathbb{F}_{2^8}^{n \cdot m}$, де n – це кількість стовпчиків, а m – кількість рядків.

Таблиця 1.1 – Залежність кількості ітерацій від розміру блоку і довижини ключа

Розмір блоку	Довжина ключа	Кількість ітерацій
128	128	10
	256	14
256	256	14
	512	18
512	512	18

Базове перетворення виконує обробку вхідного блоку даних довжиною l бітів. Записуються та зчитуються байти матриці по стовпцях.

Зашифрування Алгоритм прямого перетворення шифру «Калина» складається з операцій:

1) Додавання раундового ключа за модулем 2^{64}:

Представимо цикловий ключ як матрицю розміром ідентичним розміру матриці стану. Будемо додавати раундовий ключ по стовпцям за модулем 2^{64}.

2) Шар нелінійного бієктивного відображення (SubBytes):

На даному етапі ми застосовуємо до кожного байту матриці внутрішнього стану $G = (g_{i,j})$ підстановку $S_k : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}, k = 0, 1, 2, 3$, де S_k підстановки наведені у ДСТУ.

3) Зсув елементів (ShiftRows):

Дана операція виконує циклічний зсув вправо рядків матриці стану. Кількість елементів зсуву залежить від номеру рядка та розміру блоку. Обчислюється за формулою $\delta_i = \lfloor i * l/512 \rfloor$.

4) Лінійне перетворення (MixColumns):

Дана операція виконується наступним чином: кожен елемент матриці стану представляється як елемент $GF(2^8)$, що утворено незвідним поліномом $f(x) = x^8 + x^4 + x^3 + x^2 + 1$. Кожен елемент результуючої матриці стану отимується, як результат множення векторів довижини 8 над полем $GF(2^8)$.

Таблиця 1.2 – Порядок операцій у алгоритмі «Калина»

# ітерації	Операції
0	Додаваня раундового ключа за модулем 2^{64}
$1 - -t - 1$	Шар нелінійного бієктивного відображення Перестановка елементів Лінійне перетворення Функція додавання циклового ключа за модулем 2
t	Шар нелінійного бієктивного відображення Перестановка елементів Лінійне перетворення Функція додавання циклового ключа за модулем 2^{64}

5) Функція додавання раундового ключа за модулем 2:
Раундовий ключ в нас представлен як матриця розміру $8 * C$. Під час цієї операції ми додаємо байти раундового ключа та байти матриці.

У таблиці 1.2 приведено порядок операції у алгоритмі шифра «Калина».

У роботі далі будемо розглядати модифіковану версію шифру, в якій немає вхідного та вихідного забілювання із ключем за модулем $\mathrm{mod}2^{64}$. Такі модифіковані шифри будемо позначати як Калина-128, Калина-256 та Калина-512 в залежності від розміру блоку.

1.2 Криптоаналіз на основі ланцюгів підпросторів

Представимо деякі теоретичні відомості з криптоаналізу ланцюгів підпросторів вхідних текстів SP-мереж. Даний метод використовує чітку структуру перетворень в SP-мережах, що дозволяє виявляти алгебраїчні властивості станів шифруючого перетворення.

Означення 1.1. Нехай R – це раундова функція ітеративного блокового шифру і нехай $(V_1, V_2, ..., V_{r+1})$ позначає послідновність $r + 1$ підпростора, де $dim(V_i) \leq dim(V_{i+1})$. Якщо для кожного $i = 1, ..., r$ та для будь-якого a_i існує a_{i+1} такий, що $R(V_i \oplus a_i) \subseteq V_{i+1} \oplus a_{i+1}$, тоді

$(V_1, V_2, ..., V_{r+1})$ – це ланцюг підпросторів довжини r для функції R

Нехай R^t позначає застосування t раундов із фіксованими ключами, тоді в термінах підпросторів $R^t(V_1 \oplus a_1) \subseteq V_{t+1} \oplus a_{t+1}$.

Визначемо типічні підпростори, які використовуються в данному методі.

Означення 1.2. Для $i \in I$, де I – це множина індексів стовпчиків:

– Стовпчиковий підпростір C_i визначається як $C_i = \langle e_{0,i}, e_{1,i}, ..., e_{j-1,i} \rangle$, де j – це кількість рядків у матриці стану

– Зсунутий підпростір D_i визначається як $D_i = ShiftRows^{-1}(C_i)$.

– Інверсивно-зсунутий підпростір ID_i визначається як $ID_i = ShiftRows(C_i)$

– Змішаний простір M_i визначається як $M_i = MixColumns(ID_i)$.

На рисунку 1.1 представлені приклади типічних підпросторів для шифру AES, а на рисунку 1.2 представлені приклади типічних підпросторів для шифру «Калина».

Означення 1.3. Для I, множини індексів, нехай C_I, D_I, ID_I, M_I визначаються, як:

$$C_I = \bigoplus_{i \in I} C_i, \quad D_I = \bigoplus_{i \in I} D_i,$$
$$ID_I = \bigoplus_{i \in I} ID_i, \quad M_I = \bigoplus_{i \in I} M_i.$$

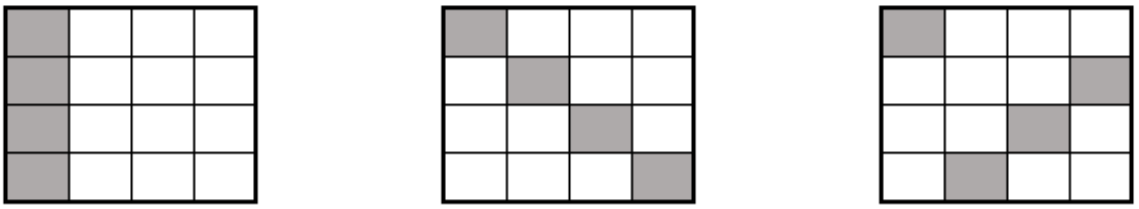

Рисунок 1.1 – Схематичне зображення елементів підпросторів C_0, D_0, ID_0 для шифру AES

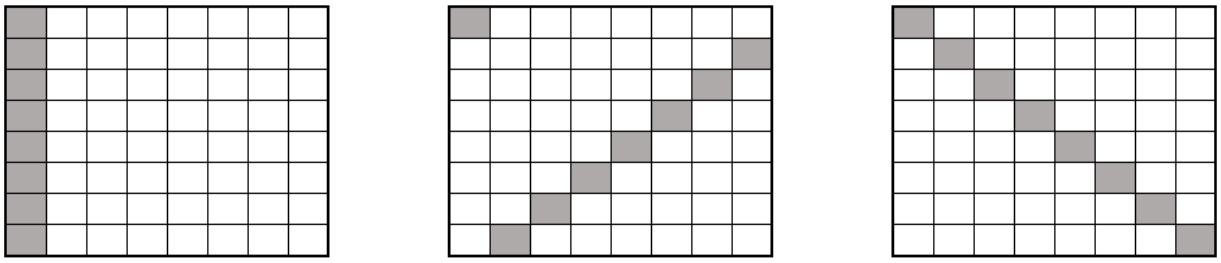

Рисунок 1.2 – Схематичне зображення елементів підпросторів C_0, D_0, ID_0 для шифру «Калина»

Ортогональне доповнення підпростору $D_I^\perp$ – це підпростір векторів, всі вектори в якому є ортогональними до всіх векторів у певному підпросторі D_I.

Теорема 1.1 ([2]). *Для множини індексів стовпчиків* $I \subset \{0, ..., j\}$ *та для кожного* $a \in D_I^\perp$, *існує єдиний елемент* $b \in C_I^\perp$, *так що* $R(D_I \oplus a) = C_I \oplus b$

Лема 1.1 ([2]). *Для усіх* $x, y \in \mathbb{F}_{2^8}^{n*m}$, *де* n – *це кількість стовпчиків матриці стану, а* m – *це кількість рядків, та для множини індексів* $I \subseteq \{0, .., n\}$ *справедлива така рівність:*

$$Pr\{R(x) \oplus R(y) \in C_I | x \oplus y \in D_I\} = 1.$$

Інакше кажучи, ми можемо зробити висновок, що для кожного $c \in C_I^\perp$, існує тільки один $d \in D_I^\perp$, такий що

$$R^{-1}(C_I \oplus c) = D_I \oplus d.$$

В загальному випадку,

$$\Pr\{R^{-1}(x) \oplus R^{-1}(y) \in D_I | x \oplus y \in C_I\} = 1.$$

Означення 1.4. Нехай X – це один із попередніх підпросторів C_I, D_I, ID_I, M_I. Нехай $x_0, ..., x_{n-1} \in F_{2^8}^{n*m}$ – це базис X. Нехай t є елементом якогось класу X, тобто $t \in X \oplus a$ для визначеного a. Ми

говоримо, що T згенерован змінними $(t^0, ..., t^{n-1})$, тобто $t \equiv (t^0, ..., t^{n-1})$ – тоді і тільки тоді $t = a \oplus \bigoplus_{i=0}^{n} t^i \cdot x_i$.

Розглянемо приклад для шифру AES. Нехай:

$$X = M_i \equiv \langle MC(e_{0,0}), MC(e_{3,1}), MC(e_{2,2}), MC(e_{1,3}) \rangle ,$$

та візьмемо елемент класу $p \in M_0 \oplus a$. Будемо казати, що p згенеровано змінними $p \equiv (p^0, p^1, p^2, p^3)$ тоді і тільки тоді, коли

$$p \equiv p^0 \cdot MC(e_{0,0}) \oplus p^1 \cdot MC(e_{1,3}) \oplus p^2 \cdot MC(e_{2,2}) \oplus p^3 \cdot MC(e_{3,1}) \oplus a.$$

Аналогічно, розглянемо приклад для шифру Калина. Нехай:

$$X = C_i \equiv \langle e_{0,i}, e_{1,i}, .., e_{7,i} \rangle ,$$

та візьмемо елемент класу $p \in C_0 \oplus a$. Будемо казати, що p згенеровано змінними $p \equiv (p^0, p^1, .., p^7)$ тоді і тільки тоді, коли

$$p \equiv p^0 \cdot e_{0,i} \oplus p^1 \cdot e_{1,i} \oplus .. \oplus p^7 \cdot e_{7,i} \oplus a.$$

1.3 Криптоаналіз нульової різниці

Наведемо короткі відомості про криптоаналіз нульовою різницею для 4-раундової SP-мережі.

Для вектора $v \in F_2^n$ та пари матриць $\alpha, \beta \in F_{2^8}^{n*m}$, де n – це кількість стовпчиків матриці стану, а m – кількість рядків, визначемо нову матрицю:

$$\rho^v(\alpha, \beta) = (\alpha_i * v_i \oplus \beta_i(v_i \oplus 1)), 0 \leq i < n,$$

де α_i та β_i – це колонки α та β відповідно.

Новий шифртекст отримується комбінуванням слов із двох матриць шифртекстів.

Теорема 1.2. *[4] Нехай* $\alpha, \beta \in F_{2^8}^{n*m}$ *та* $\alpha' = \rho^v(\alpha, \beta)$, $\beta' = \rho^v(\beta, \alpha)$.

Тоді

$$\nu(S \circ L \circ S(\alpha) \oplus S \circ L \circ S(\beta)) = \nu(S \circ L \circ S(\alpha') \oplus S \circ L \circ S(\beta')),$$

де $\nu(x)$ – це вектор-індикатор, котрий приймає значення 1, якщо слово x_i дорівнює нулю, та 0 в іншому випадку.

Теорему 1.2 можно представити у термінах криптоаналізу підпросторів таким чином. Нехай в нас є два відкритих текста з одного класу $p^0, p^1 \in D_I \oplus a$. Та:

$$c^0 = R^4(p^0), \quad p'^0 = R^{-4}(\rho(c^0, c^1)),$$
$$c^1 = R^4(p^1), \quad p'^1 = R^{-4}(\rho(c^1, c^0)).$$

Тоді із ймовірністю один виконується:$p'^0 \oplus p'^1 \in D_I$.

Наведемо визначення, що таке *super-Sbox*. Це визначення буде потрібно для доведення теореми та теорем з розділу 2.

Означення 1.5. Функцію *super-Sbox* визначемо як $super\text{-}Sbox(\cdot) = S - Box \circ AddRoundKey \circ MixColumns \circ S - Box(\cdot)$, де $\circ$ – це композиція функцій.

Наведемо доведення теореми, завдяки якій можливо побудувати змішаний інтегральний розпізнавач для AES.

Теорема 1.3. *([3]) Дано підпростір $C_0 \cap D_{0,3} \equiv \langle e_{0,0}, e_{1,0} \rangle \subseteq C_0$. Розглянемо два відкритих текста p^1 та p^2 з одного класу $C_0 \cap D_{0,3} \oplus a$ згенерованих $p^1 \equiv (z^1, w^1)$ та $p^2 \equiv (z^2, w^2)$ (де $z^i, w^i \in F_{2^8}, i = 1, 2$).*

Нехай $\tilde{p}^1, \tilde{p}^2 \in C_0 \oplus a \equiv \langle e_{0,0}, e_{1,0}, e_{2,0}, e_{3,0} \rangle$ – це два інших відкритих текста згенерованих

$$\tilde{p}^1 \equiv (z^1, w^1, \psi_0, \psi_1), \tilde{p}^2 \equiv (z^2, w^2, \psi_0, \psi_1)$$

або

$$\tilde{p}^1 \equiv (z^1, w^2, \psi_0, \psi_1), \tilde{p}^2 \equiv (z^2, w^1, \psi_0, \psi_1),$$

де $\psi_i, i = 0, 1$ можуть приймати будь-які значення з F_{2^8}.

Тоді

$$R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$$

виконується із ймовірністю 1 для 4-раундового AES незалежно від секретного ключа, S-box'ів та операції MixColumns.

Доведення.

Розглянемо дві пари текстів (p^1, p^2) та $(\tilde{p}^1, \tilde{p}^2)$ з одного класу $C_0 \cap D_{0,3} \oplus a$ для фіксованого a.

$$p^i \equiv a \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ w^i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ та } \tilde{p}^i \equiv a \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ w^{3-i} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

для $i = 1, 2$, тобто $p^i \equiv (z^i, w^i)$ та $\tilde{p}^i \equiv (z^i, w^{3-i})$.

Наша мета довести, що $R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$.

Так як $\Pr\{R^2(x) \oplus R^2(y) \in M_I | x \oplus y \in D_I\}$, то потрібно довести, що

$$R^2(p^1) \oplus R^2(p^2) \in D_J \Leftrightarrow R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) \in D_J.$$

Перш за все звернемо увагу, що

$$p^1 \oplus p^2 \in (C_0 \cap D_{0,3}) \subseteq D_{0,3},$$

та $R^2(x) \oplus R^2(y) \in M_{0,3}$.

Так як $M_{0,3} \cap D_J \neq \{0\}$ виконується тільки коли $|J| = 1$. то $R^2(x) \oplus R^2(y) \in D_{0,3}$ може відбутися, тільки коли $|J| = 1$.

2-раундове перетворення може буде переписано в термінах *super-Sbox*:

$$R^2 = AddRoundKey \circ MixColumns \circ ShiftRows \circ super\text{-}Sbox \circ ShiftRows(\cdot)$$

. Так як операції $ShiftRows$ та $MixColumns$ лінійні відносно наших змінних, то достатньо довести, що

$$\begin{aligned} &super\text{-}Sbox(q^1) \ \oplus \ super\text{-}Sbox(q^2) \in W_J \Leftrightarrow \\ &super\text{-}Sbox(\tilde{q}^1) \ \oplus \ super\text{-}Sbox(\tilde{q}^2) \in W_J, \end{aligned}$$

$$q^i = SR(p^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ 0 & 0 & 0 & w^i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ та}$$

$$\tilde{q}^i = SR(\tilde{q}^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ 0 & 0 & 0 & w^{3-i} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

де $i = 1, 2$ та множина W_J визначена, як $W_J := ShiftRows^{-1} \circ MixColumns^{-1}(D_J)$.

Так як кожна колонка q^1 та q^2 залежить від різних та незалежних змінних, *super-Sbox* обробляє кожну колонку незалежно, та операція $\bigoplus$ коммутативна, то з цього слідує, що $super\text{-}Sbox(q^1) \oplus super\text{-}Sbox(q^2) = super\text{-}Sbox(\tilde{q}^1) \oplus super\text{-}Sbox(\tilde{q}^2)$, з чого випливає твердження теореми. □

Висновки до розділу 1

У цьому розділі були розглянуто загальне визначення SP-мереж. Було надано опис шифрів AES та Калина. Були розглянуті теоретичні відомості для побудови розпізнавачів на основі аналізу ланцюгів підпросторових перетворень. Також були розглянуті теоретичні відомості з криптоаналізу за методом нульової різниці та за методом змішаного інтегрального криптоаналізу.

Було показано доведення базових теорем змішаного інтегрального криптоаналізу для побудови розпізнавача для шифру AES.

2 РОЗПІЗНАВАЧІ КАЛИНА-ПОДІБНИХ ШИФРІВ

У цьому розділі буде розглянуто алгоритми побудови розпізнавачів для Калина-подібних шифрів за допомогою аналізу ланцюгів перетворень підпросторів за методом змішаного інтегрального криптоаналізу та криптоаналізу нульової різниці.

Наша задача побудувати розпізнавачі для Калина-подібних шифрів за методом змішаного інтегрального криптоаналізу та криптоаналізом нульової різниці. Також ми отримаємо оцінку кількості текстів, які необхідні для побудови ефективного розпізнавача.

2.1 Побудова розпізнавачів для Калина-подібного шифрів за допомогою криптоаналізу нульової різниці

Принцип побудови розпізнавача[4] такий: ми шифруємо деяку кількість відкритих текстів і сподіваємость після першого раунду, що отриманий шифртекст буде належати до $D_K \cap C_0$, де K – це множина індексів. І будемо сприймати цей шифртекст, як вхід для 4-раундового шифру. Після цього будемо сподіватися із відповідною ймовірністю побачити збереження властивості нульової різниці для шифруючого перетворення.

2.1.1 Побудова розпізнавача для модифікованого 5-раундового шифру Калина-128

Для подальших обчислень нам знадобиться наступна лема.

Лема 2.1. *Для будь-яких підпросторів C_I та D_J та множин*

індексів I, J для Калина-128 вірно наступне твердження:

$$\begin{aligned} Pr(x \in (C_I \cap D_J) | x \in C_I) &= (2^{-8})^{2*|I|-|I|*|J|}, \\ Pr(x \in (C_J \cap D_I) | x \in D_I) &= (2^{-8})^{2*|I|-|I|*|J|}. \end{aligned}$$

Розглянемо випадок, коли шифртекст після першого раунда шифрування належить до $D_K \cap C_0$, де $|K| = 1$. Після першого раунда шифрування подія

$$R(p^i) \oplus R(p^j) \in D_K \cap C_0,$$

де $|K| = 1$, відбудеться з ймовірністю $((2^4 - 1) + (2^4 - 1)) \cdot (2^{-8}) = 30 \cdot 2^{-8}$. В нас для нульового стовпчика матрциі стану $(2^4 - 1) = 15$ варіантів заповнення перших 4-ьох байтів, що відповідає належності матриці стану до простору D_0, та $(2^4 - 1) = 15$ варіантів для останніх 4-ьох байтів, що відповідає належності до простору D_1. Кожний варіант D_K згідно леми 2.1 має ймовірність $2^{-8^{(2 \cdot 1 - 1 \cdot 1)}} = 2^{-8}$. Якщо ми відповідно до теореми 1.2 змінимо значення стовпчиків шифртекстів, то

$$\begin{aligned} R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) &\in D_K, \\ R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) &\in D_K \cap C_L, \end{aligned}$$

де із ймовірністю $2 \cdot 2^{-8}$ $|L| = 1$.

Це означає, що, згідно леми 2.1, після ще одного раунда розшифрування два нових відкритих текста p'^j, p'^i будуть належати простору D_L із ймовірністю $30 \cdot 2^{-8} \cdot 2 \cdot 2^{-8} = 30 \cdot 2^{-15} \approx 2^{-10}$. Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.1.

Алгоритм побудови розпізнавача для модифікованого шифру Калина із розміром блоку 128

Після обрахунків маємо, що Ймовірність того, що пара відкритих текстів $p'^j \oplus p'^i$ належить до C_L, де $|L| = 1$, дорівнює 2^{-10}.

Ймовірність, що пара випадкових відкритих текстів $p'^j \oplus p'^i$ належить

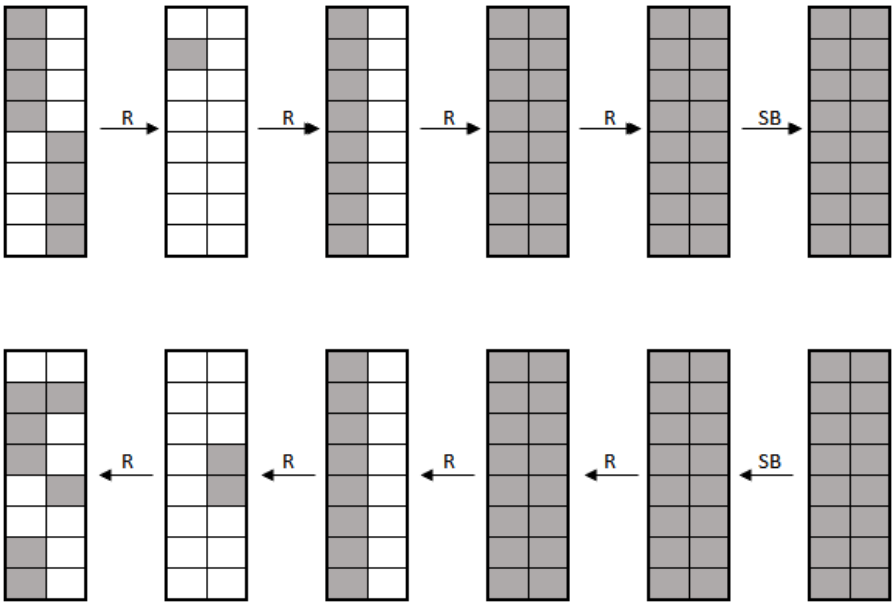

Рисунок 2.1 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 128 при $|K| = 1$

до C_L, де $|L| = 1$, дорівнює $\approx 2^{-63}$.

Загалом, кількість потрібних текстів дорівнює 2^{12}.

Алгоритм роботи розпізнавача буде виглядати таким чином:

Algorithm 2.1 5-раундовий розпізнавач Калина-128

Ensure: 1 якщо перетворення – це Калина-128, 0 – інакше
Зашифруємо 2^6 відкритих випадкових текстів з простору D_0;
Згенеруємо усі можливі пари відкритих текстів, яких 2^{11};
Шифруємо усі пари відкритих текстів. Після шифрування методом заміни стовпчиків матриці стану 1.2 для кожної пари маємо 2 додаткових шифртекста;
for all Пар шифртекстів c^i, c^j **do**
  $p'^i = R^{-5}(c^i)$;
  $p'^j = R^{-5}(c^j)$;
  if $p'^j \oplus p'^i \in D_L$, де $|L| = 1$ **then**
    return 1
  end if
end for
return 0

2.1.2 Побудова розпізнавача для модифікованого 5-раундового шифру Калина-256

Для побудови розпізнавача для 5-раундового шифру Калина-256 потрібно розглянути три випадки після першого раунда шифрування:

1) шифртекст належить до $D_K \cap C_0, |K| = 1$;

2) шифртекст належить до $D_K \cap C_0, |K| = 2$;

3) шифртекст належить до $D_K \cap C_0, |K| = 3$.

За аналогією до Калини-128 для обчислень нам знадобиться наступна лема.

Лема 2.2. *Для будь-яких підпросторів C_I та D_J та множин індексів I, J для Калина-256 вірно наступне твердження:*

$$\begin{aligned} Pr(x \in (C_I \cap D_J) | x \in C_I) &= (2^{-8})^{4*|I|-|I|*|J|}, \\ Pr(x \in (C_J \cap D_I) | x \in D_I) &= (2^{-8})^{4*|I|-|I|*|J|}. \end{aligned}$$

Розрахунки для $|K| = 1$ Аналогічно до Калини-128, будемо розглядати пару відкритих текстів з одного класу $p^i, p^j \in D_I \oplus a$. Ймовірність події $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, де $|K| = 1$ дорівнює $4 \cdot (2^2 - 1) \cdot 2^{-48}$. 4 варіанта, на вибір пари байтів, які належать якомусь з D_i, $(2^2 - 1)$ варіантів активних байтів в обраній парі, та за лемою2.2 ймовірність однієї такої події дорівнює 2^{-48}.

Відповідно до теореми 1.2, після заміни значення стовпчиків шифртекстів подія:

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \in D_K \cap C_L,$$

відбувається із ймовірністю $4 \cdot (2^2 - 1) \cdot 2^{-8}$, коли $|L| = 3$.

Згідно леми 2.2, після ще одного раунда розшифрування два нових відкритих текста p'^j, p'^i будуть належати простору D_L із ймовірністю $144 \cdot 2^{-56}$. Урізана диференціальна характеристика, використана в цьому

випадку, зображена на рисунку 2.2.

Розрахунки для $|K| = 2$

Розглянемо випадок, коли різниця двох відкритих текста $p^i, p^j \in D_I \oplus a$ після раунду шифрування належить до $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, де $|K| = 2$. Ймовірність цієї події дорівнює $C_4^2 \cdot (2^2 - 1)^2 \cdot 2^{-32} = 6 \cdot 9 \cdot 2^{-32}$. 6 варіантів, на вибір двох пар байтів, які належать двом $D_I, |I| = 2$, $(2^2 - 1)^2$ варіантів активних байтів в обраних парах, та за лемою2.2 ймовірність одної події дорівнює 2^{-32}.

Знову відповідно до теореми 1.2, змінимо значення стовпчиків шифртекстів. Подія

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \in D_K \cap C_L,$$

коли $|L| = 3$, відбудеться із ймовірністю $4 \cdot (2^2 - 1)^2 \cdot 2^{-16}$.

Це означає, що, згідно леми 2.2, після ще одного раунда розшифрування два нових відкритих текста p'^j, p'^i будуть належати D_L із ймовірністю $6 \cdot 9 \cdot 2^{-32} \cdot 4 \cdot (2^2 - 1)^2 \cdot 2^{-16} = 27 \cdot 9 \cdot 2^3 \cdot 2^{-48} = 243 \cdot 2^{-45}$.

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.3.

Розрахунки для $|K| = 3$

Для двох відкритих текстів $p^i, p^j \in D_I \oplus a$ ймовірність, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$ дорівнює $C_4^3 \cdot (2^2 - 1)^3 \cdot 2^{-32} = 4 \cdot 27 \cdot 2^{-32}$. 4 варіанта, на вибір двох пар байтів, які належать трьом $D_I, |I| = 3$, $(2^2 - 1)^3$ варіантів активних байтів в обраних парах, та за лемою2.2 ймовірність одної події дорівнює 2^{-16}.

Відповідно до теореми 1.2 ймовірність того, що :

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \in D_K \cap C_L,$$

коли $|L| = 3$, після заміни значення стовпчиків шифртекстів дорівнює $4 \cdot (2^2 - 1)^3 \cdot 2^{-24}$.

Після ще одного раунда розшифрування два нових відкритих текста

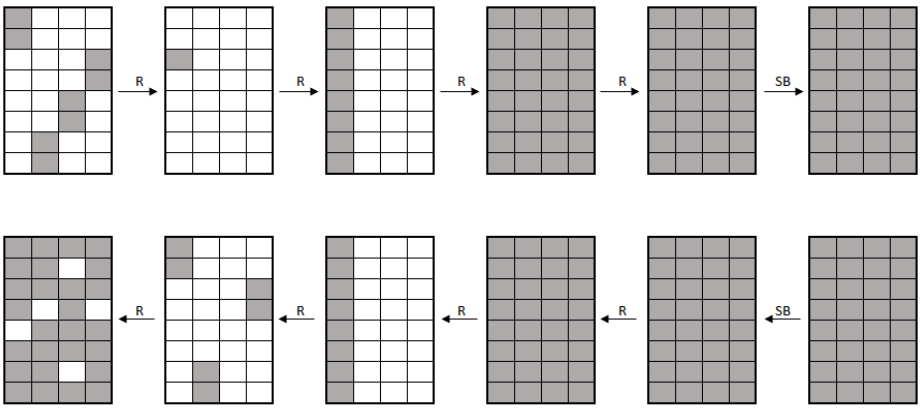

Рисунок 2.2 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 256 при $|K| = 1$

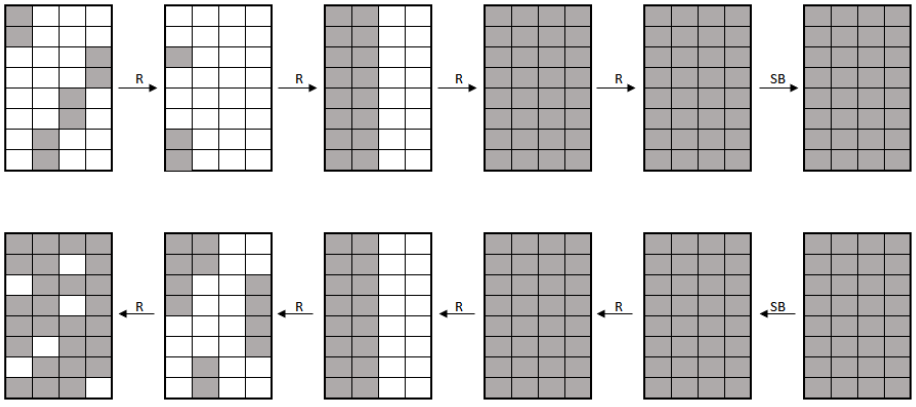

Рисунок 2.3 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 256 при $|K| = 2$

p'^j, p'^i будуть лежати в одному просторі D_L із ймовірністю $4 \cdot 27 \cdot 2^{-32} \cdot 4 \cdot 27 \cdot 2^{-24} = 27^2 \cdot 2^{-52}$.

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.4.

Алгоритм роботи розпізнавача для модифікованого шифру Калина із розміром блоку 256

Ймовірність, що пара відкритих текстів $p'^j \oplus p'^i$ належить до C_L дорівнює $27^2 \cdot 2^{-52} + 243 \cdot 2^{-45} + 144 \cdot 2^{-56} \approx 2^{-37}$.

Випадкова пара відкритих текстів $p'^j \oplus p'^i$ належить простору C_L, де $|L| = 1$, із ймовірністю $\approx 2^{-127}$.

Кількість потрібних текстів повинна перевищувати 2^{39}.

Алгоритм роботи розпізнавача буде виглядати таким чином:

Algorithm 2.2 5-раундовий розпізнавач Калина-256

Ensure: 1 якщо перетворення – це Калина-256, 0 – інакше
Зашифруємо 2^{19} відкритих випадкових текстів з простору D_0;
Згенеруємо усі можливі пари відкритих текстів, яких 2^{37};
Шифруємо усі пари відкритих текстів. Після шифрування методом заміни стовпчиків матриці стану 1.2 для кожної пари маємо 7 додаткових шифртекста;
for all Пар шифртекстів c^i, c^j **do**
  $p'^i = R^{-5}(c^i)$;
  $p'^j = R^{-5}(c^j)$;
  if $p'^j \oplus p'^i \in D_L$, де $|L| = 3$ **then**
    return 1
  end if
end for
return 0

2.1.3 Побудова розпізнавача для модифікованого 5-раундового шифру Калина-512

Аналогічно до Калини-128 і Калини-256 ми розглянемо 7 випадків, коли шифртекст належить до $D_K \cap C_0$, де $|K| = 1, .., 7$.

Лема 2.3. *Для будь-яких підпросторів C_I та D_J та множин*

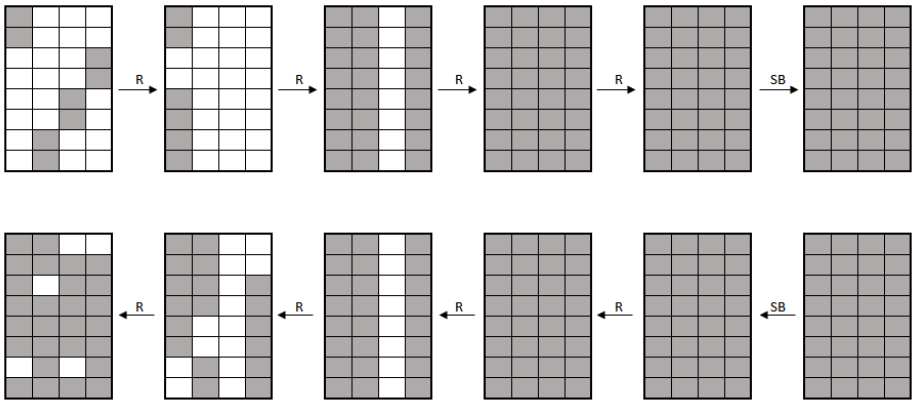

Рисунок 2.4 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 256 при $|K| = 3$

індексів I, J для Калина-512 вірно наступне твердження:

$$Pr(x \in (C_I \cap D_J) | x \in C_I) = (2^{-8})^{8*|I|-|I|*|J|},$$
$$Pr(x \in (C_J \cap D_I) | x \in D_I) = (2^{-8})^{8*|I|-|I|*|J|}.$$

Розрахунки для $|K| = 1$

Ймовірність події, що після першого раунда шифрування різниця належить до $D_K \cap C_0$, дорівнює $C_8^1 \cdot 2^{-8^{8 \cdot 1 - 1 \cdot 1}} = 8 \cdot 2^{-56}$. 8 варіантів на вибір активного байта у нульовому стовпчику. В даному випадку обирання активного байта у стовпчику це теж саме, що і обирання індекса зсунутого підпростору D_i. Обраховуючи ймовірність а лемою2.3, отримаємо ймовірність однієї події 2^{-56}.

Змінивши значення стовпчиків шифртекстів подія

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \ \in \ D_K \cap C_L,$$

де $|L| = 7$, відбувається із ймовірністю $8 * 2^{-8}$. Згідно леми 2.3, після ще одного раунда розшифрування відкриті тексти p'^j, p'^i будуть належати простору D_L із ймовірністю $8 \cdot 2^{-56} \cdot 8 \cdot 2^{-8} = 2^{-58}$.

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.5.

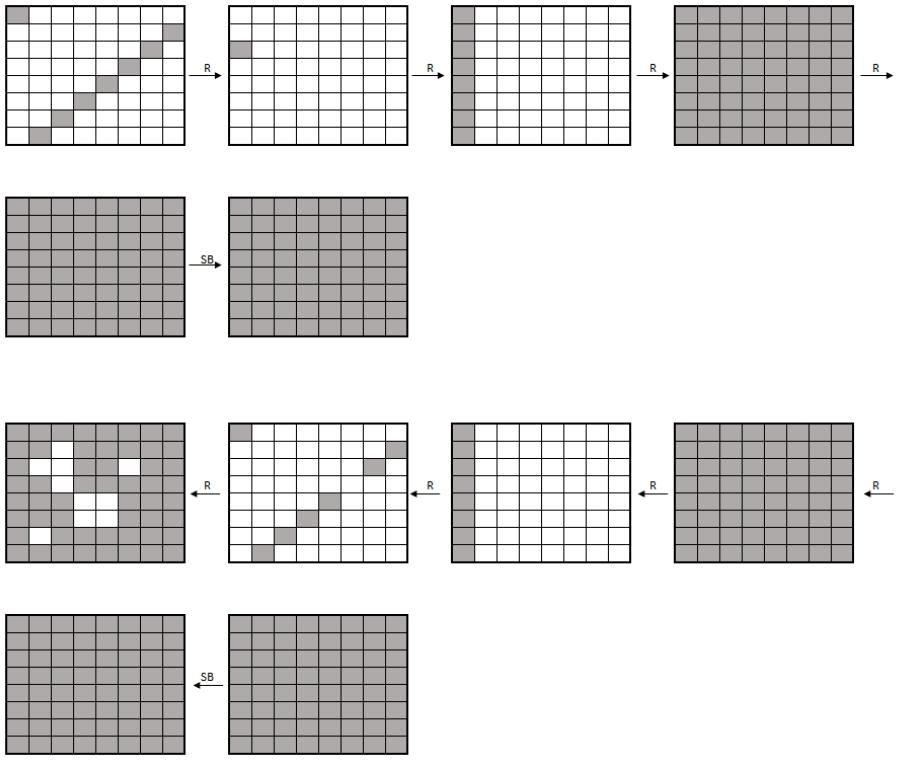

Рисунок 2.5 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 1$

Розрахунки для $|K| = 2$

Після першого раунда шифрування Ймовірність події, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, дорівнює $C_8^2 \cdot 2^{-8^{8\cdot 1-2\cdot 1}} = 28 \cdot 2^{-48}$. Ймовірність однієї події, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$ дорівнює 2^{-48}. І таких подій в нас може відбутися 28 – це кількість варіантів на вибір двох активних байтів у стовпчику матриці стану.

З ймовірністю $8 * 2^{(-8)^{8\cdot 2-7\cdot 2}} = 8 \cdot 2^{-16}$ та згідно теореми 1.2 відбувається подія

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \ \in \ D_K \cap C_L,$$

де $|L| = 7$.

Це означає, що, згідно леми 2.3, після ще одного раунда розшифрування два нових відкритих текста належать класу $p'^j \oplus p'^i \in D_L \oplus a$ із ймовірністю $28 \cdot 2^{-48} \cdot 8 \cdot 2^{-16} = 7 \cdot 2^{-59}$.

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.6.

Розрахунки для $|K| = 3$

Після першого раунда шифрування Ймовірність події, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, дорівнює $C_8^3 \cdot 2^{-8^{8\cdot1-3\cdot1}} = 56 \cdot 2^{-40}$. $C_8^3 = 28$ варіантів на вибір трьох активних байтів, що відповідає обиранню трьох індексів просторів D_i. За лемою2.3 ймовірність однієї такої події дорівнює 2^{-40}.

Якщо ми відповідно до теореми 1.2 змінемо значення стовпчиків шифртекстів, то

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \in D_K \cap C_L,$$

де $|L| = 7$ із ймовірністю $8 * 2^{(-8)^{8\cdot3-7\cdot3}} = 8 \cdot 2^{-24}$.

Розшифрувавши ще один раз шифртексти, ми отримаємо два відкритих текста p'^j, p'^i, які будуть в одному класі $D_L \oplus a$ із ймовірністю $56 \cdot 2^{-40} \cdot 8 \cdot 2^{-24} = 7 \cdot 2^{-58}$.

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.7.

Розрахунки для $|K| = 4$

Розглядаючи випадок, коли $R(p^i) \oplus R(p^j) \in D_K \cap C_0$ при $|K| = 4$, можна обрахувати, що ймовірність цієї події дорівнює дорівнює $C_8^4 \cdot 2^{-8^{8\cdot1-4\cdot1}} = 70 \cdot 2^{-32}$. $C_8^4 = 70$ варіантів на вибір чотирьох байтів, що належать D_K. ймовірність однієї такої комбінації просторів D_i дорівнює 2^{-32}.

Подія

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \in D_K \cap C_L,$$

де $|L| = 7$ відбувається із ймовірністю $8 * 2^{(-8)^{8\cdot4-7\cdot4}} = 8 * 2^{-32}$.

Розшифровуючи шифртексти ще один раунд, два нових відкритих текста лежать у просторі D_L із ймовірністю $70 \cdot 2^{-32} \cdot 8 \cdot 2^{-32} = 35 \cdot 2^{-60}$.

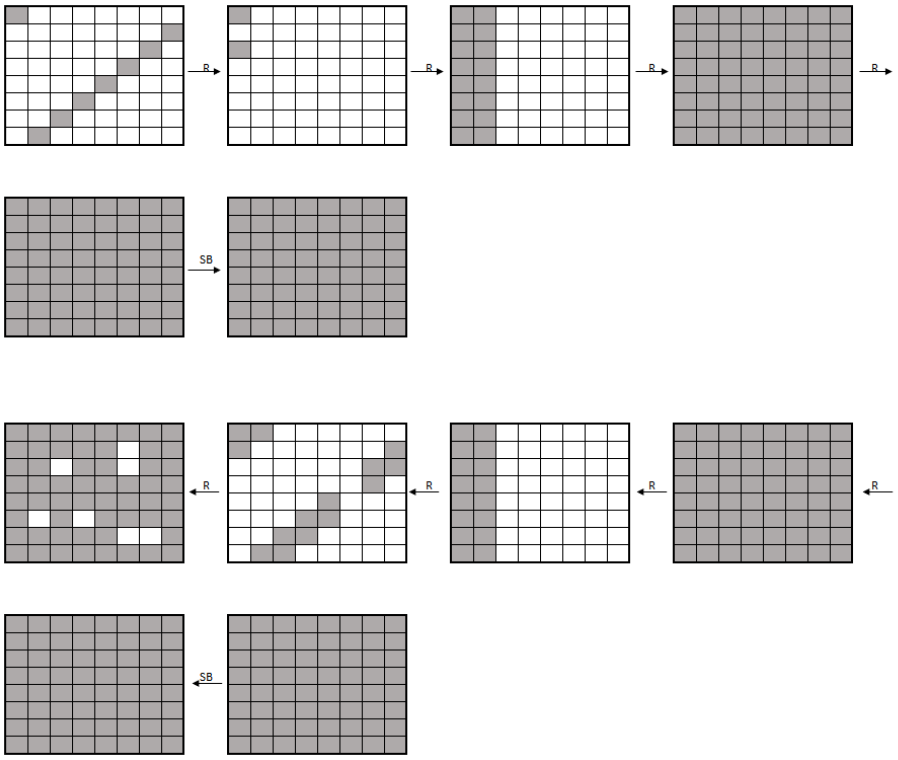

Рисунок 2.6 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 2$

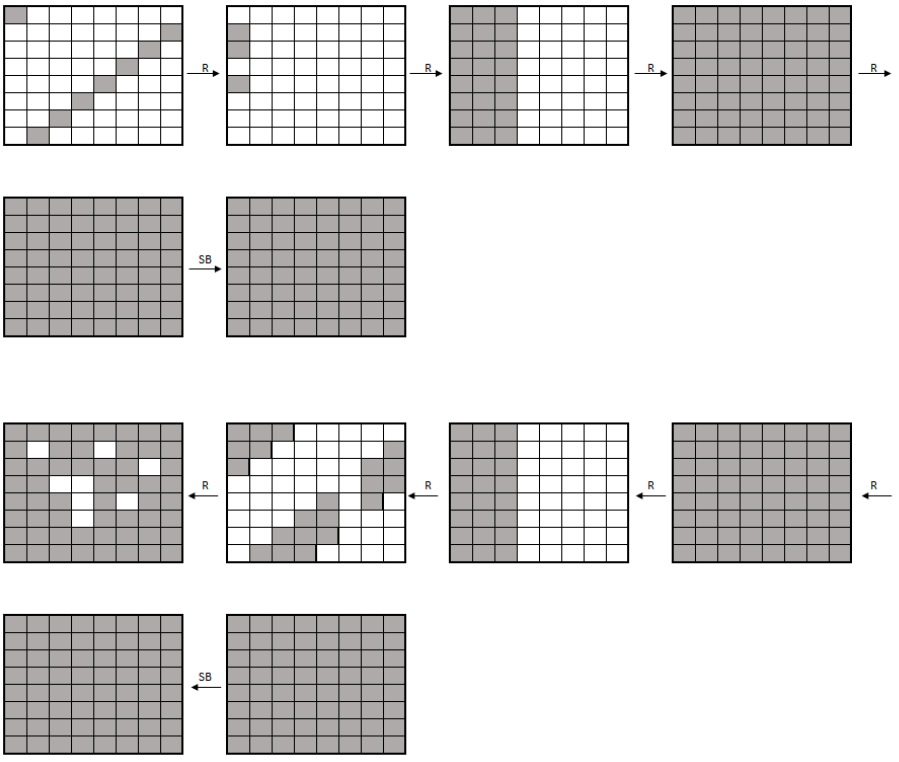

Рисунок 2.7 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 3$

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.8.

Розрахунки для $|K| = 5$

Ймовірність події, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, згідно леми 2.3, дорівнює $C_8^5 * 2^{-8^{8\cdot1-5\cdot1}} = 56 \cdot 2^{-24}$. В нас є 56 варіантів на вибір п'яти D_i, що відповідає п'яти активним байтам, Ймовірність однієї події дорівнює 2^{-24}.

Якщо ми відповідно до теореми 1.2 змінемо значення стовпчиків шифртекстів, то

$$\begin{aligned} R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) &\in D_K \\ R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) &\in D_K \cap C_L, \end{aligned}$$

де $|L| = 7$ із ймовірністю $8 * 2^{(-8)^{8\cdot5-7\cdot5}} = 8 \cdot 2^{-40}$. Це означає, що, згідно леми 2.3, після ще одного раунда розшифрування два нових відкритих текста p'^j, p'^i будуть лежати в просторі D_L із ймовірністю $56 \cdot 2^{-24} \cdot 8 \cdot 2^{-40} = 7 \cdot 2^{-58}$.

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.9.

Розрахунки для $|K| = 6$

По аналогії, після першого раунда шифрування Ймовірність події, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, дорівнює $C_8^6 * 2^{-8^{8\cdot1-6\cdot1}} = 28 \cdot 2^{-16}$. В нас є 28 варіантів на вибір шести активних байтів, та за лемою2.3 ймовірність одної події дорівнює 2^{-16}.

Відповідно до теореми 1.2 змінемо значення стовпчиків шифртекстів. Подія, що

$$R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) \in D_K \cap C_L,$$

де $|L| = 7$, відбудеться з ймовірністю $8 * 2^{(-8)^{8\cdot6-7\cdot6}} = 8 \cdot 2^{-48}$.

Очевидним є те, що, згідно леми 2.3, після п'ятого раунда розшифрування два нових відкритих текста $p'^j \oplus p'^i \in D_L \oplus a$ із ймовірністю $28 \cdot 2^{-16} \cdot 8 \cdot 2^{-48} = 7 \cdot 2^{-59}$.

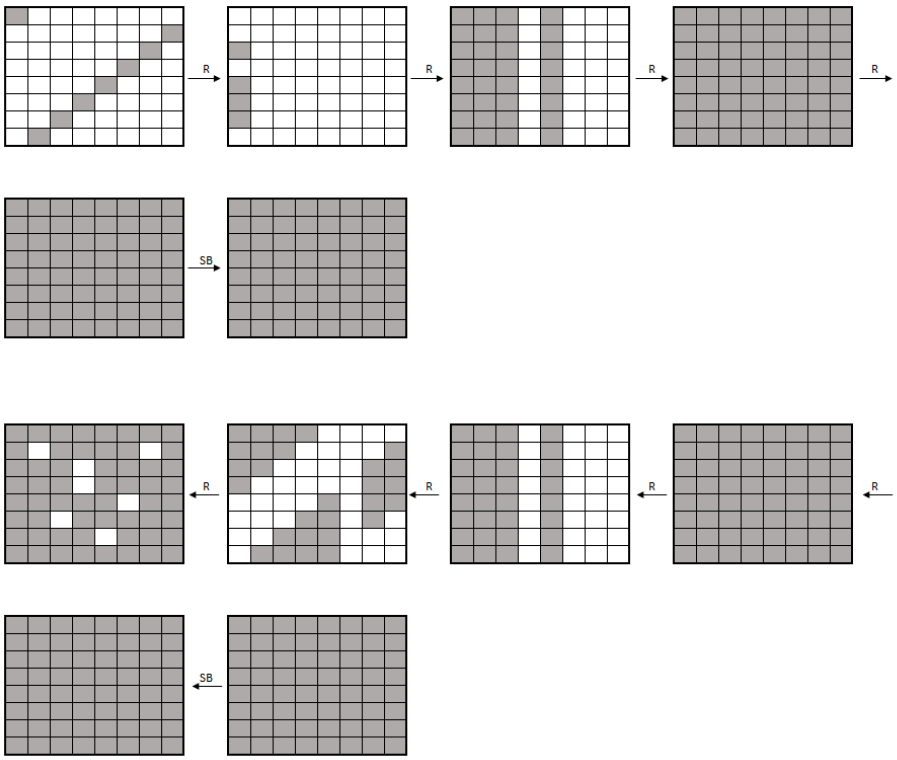

Рисунок 2.8 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 4$

Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.10.

Розрахунки для $|K| = 7$

Після першого раунда шифрування Ймовірність події, що $R(p^i) \oplus R(p^j) \in D_K \cap C_0$, дорівнює $C_8^7 * 2^{-8^{8\cdot 1-7\cdot 1}} = 8 \cdot 2^{-8}$. 8 варіантів на вибір семи активних байтів, та за лемою2.3 ймовірність одної події дорівнює 2^{-8}.

Якщо ми відповідно до теореми 1.2 змінемо значення стовпчиків шифртекстів, то

$$\begin{aligned} R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) &\in D_K \\ R^{-4}(\rho^v(c^i, c^j)) \oplus R^{-4}(\rho^v(c^j, c^i)) &\in D_K \cap C_L, \end{aligned}$$

де $|L| = 7$ із ймовірністю $8 * 2^{(-8)^{8\cdot 7-7\cdot 7}} = 8 \cdot 2^{-56}$. Це означає, що, згідно леми 2.3, після ще одного раунда розшифрування два нових відкритих

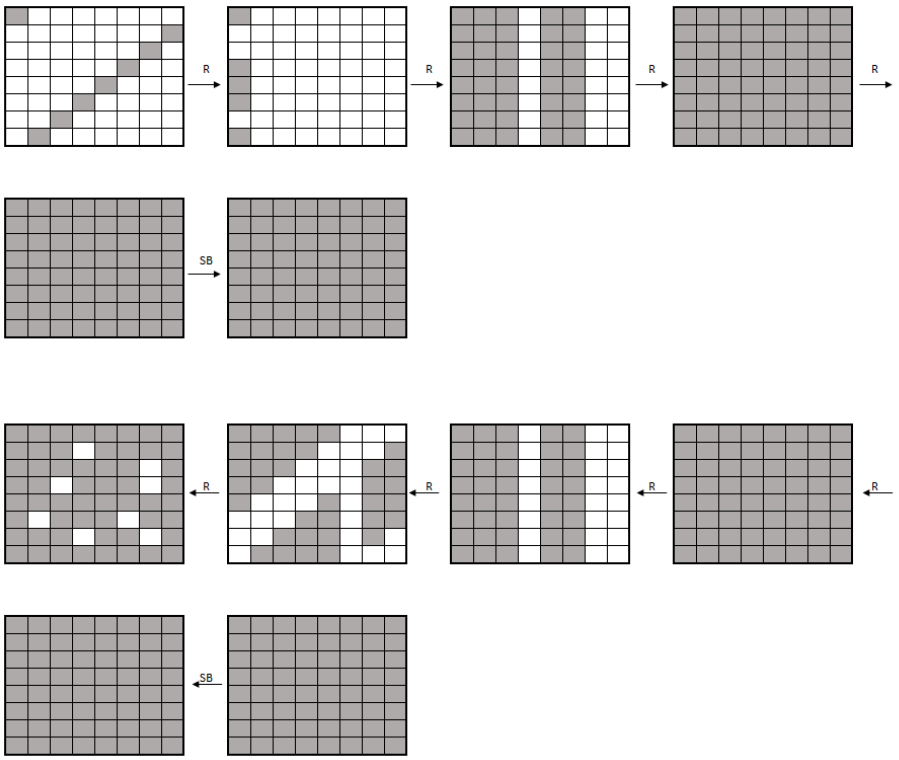

Рисунок 2.9 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 5$

текста p'^j, p'^i будуть лежати в просторі D_L із ймовірністю $8 \cdot 2^{-8} \cdot 8 \cdot 2^{-56} = 2^{-58}$. Урізана диференціальна характеристика, використана в цьому випадку, зображена на рисунку 2.11.

Алгоритм побудови розпізнавача для модифікованого шифру Калина із розміром блоку 512

Ймовірність, що пара відкритих текстів $p'^j \oplus p'^i$ належить до C_L дорівнює $2^{-58} + 7 \cdot 2^{-59} + 7 \cdot 2^{-58} + 35 \cdot 2^{-60} + 7 \cdot 2^{-58} + 7 \cdot 2^{-59} + 2^{-58} \approx 2^{-53}$

Ймовірність, що пара випадкових відкритих текстів $p'^j \oplus p'^i$ належить до C_L дорівнює $\approx 2^{-253}$.

Задля того, щоб ймовірність успіху була більше 0.95, обрахуємо кількість необхідних текстів. Кількість необхідних текстів дорівнює 2^{55}.

Алгоритм роботи розпізнавача буде виглядати таким чином:

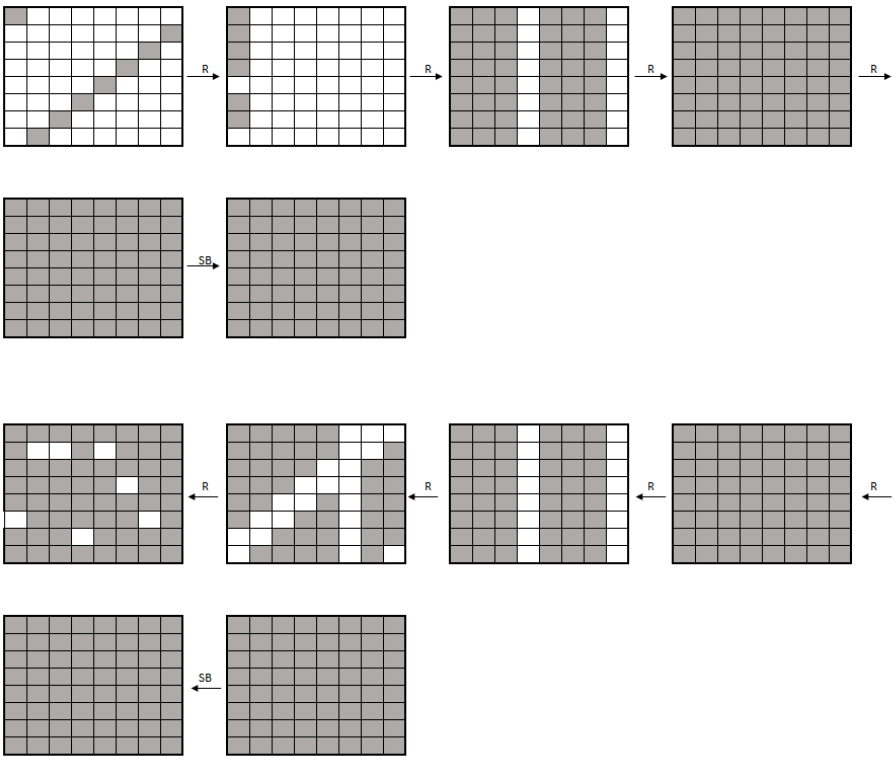

Рисунок 2.10 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 6$

Algorithm 2.3 5-раундовий розпізнавач Калина-512

Ensure: 1 якщо перетворення – це Калина-512, 0 – інакше
Зашифруємо 2^{26} відкритих випадкових текстів з простору D_0;
Згенеруємо усі можливі пари відкритих текстів, яких 2^{51};
Шифруємо усі пари відкритих текстів. Після шифрування методом заміни стовпчиків матриці стану 1.2 для кожної пари маємо 29 додаткових шифртекста;
for all Пар шифртекстів c^i, c^j **do**
  $p'^i = R^{-5}(c^i)$;
  $p'^j = R^{-5}(c^j)$;
  if $p'^j \oplus p'^i \in D_L$, де $|L| = 7$ **then**
    return 1
  end if
end for
return 0

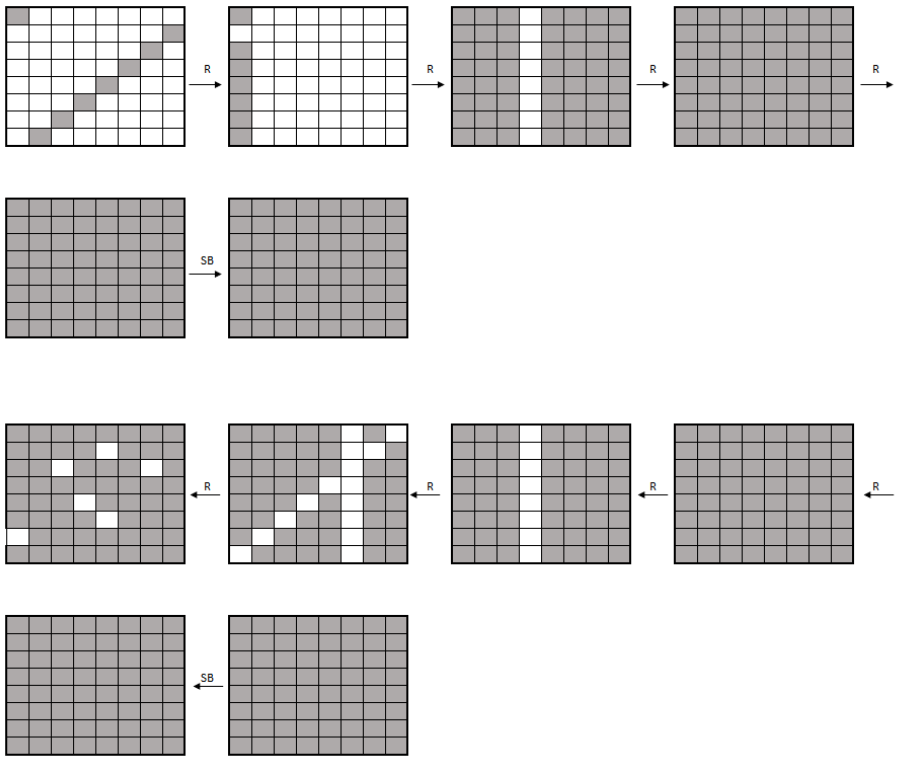

Рисунок 2.11 – Приклад перетворення вхідного підпростора для модифікованого шифру Калина із розміром блоку 512 при $|K| = 7$

2.2 Неможливий змішаний інтегральний розпізавач

Зазвичай, розпізнавачі шифрів будуються на збереженнія якоїсь властивості вхідного масиву даних. Неможливий змішаний інтегральний розпізнавач будується на основі того факту, що тексти при шифруванні не можуть мати деякі властивості (з цього і назва "неможливий").

Далі ми наведемо такі властивості для модифікованих шифрів Калина-128, Калина-256, Калина-512, та доведемо, що шифртекст не може мати даної властивості, якщо перетворення – це модифікована Калина. На основі цих властивостей ми побудуємо розпізнавач модифікованих шифрів Калина та оцінимо кількість текстів, якої потребує розпізнавач для ефективної роботи.

2.2.1 Неможливий змішаний розпізнавач для Калини-128

Лема 2.4. *Для будь-яких x, y та для будь-яких множин індексів $I, J \subseteq \{0,1\}$. $M_I \cap D_J = \{0\}$ тоді і тільки тоді, коли $|I| + |J| \leq 2$.*

Для того, щоб побудувати неможливий змішаний інтегральний розпізнавач для Калина-128, нам потрібно довести теорему аналогічну до теореми 1.3 для AES. Далі ми використаємо результат її задля того, щоб вивести властивість, якої не можуть мати шифртексти зашифровані за допомогою Калина-128.

Теорема 2.1. *Дано підпростір $A \equiv \langle e_{0,0}, e_{4,0} \rangle \subseteq C_0 \cap D_{0,1} \subseteq C_0$. Розглянемо два відкритих текста p^1 та p^2 з одного простору $A \oplus a$ згенерованої $p^1 \equiv (z^1, w^1)$ та $p^2 \equiv (z^2, w^2)$ (де $z^i, w^i \in F_{2^8}, i = 1, 2$). Нехай $\tilde{p}^1, \tilde{p}^2 \in C_0 \oplus a \equiv \langle e_{0,0}, ..., e_{7,0} \rangle$ – це два інших відкритих текста згенерованих*

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5),$$

або

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5),$$

де $\psi_i, i = 0, .., 5$ можуть приймати будь-які значення з F_{2^8}. Тоді

$$R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$$

виконується із ймовірністю 1 для 4-раундової Калини-128 незалежно від секретного ключа, S-Box'ів та операції MixColumns.

Доведення.

Розглянемо дві пари текстів (p^1, p^2) та $(\tilde{p}^1, \tilde{p}^2)$ з простору $A \oplus a$ для фіксованого a.

$$p^i \equiv a \oplus \begin{bmatrix} z^i & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ w^i & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ та } \tilde{p}^i \equiv a \oplus \begin{bmatrix} z^i & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ w^{3-i} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

для $i = 1, 2$, тобто $p^i \equiv (z^i, w^i)$ та $\tilde{p}^i \equiv (z^i, w^{3-i})$.

Мета довести $R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$

Так як $\Pr\{R^2(x) \oplus R^2(y) \in M_I | x \oplus y \in D_I\}$, то потрібно довести, що $R^2(p^1) \oplus R^2(p^2) \in D_J \Leftrightarrow R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) \in D_J$ Перш за все звернемо увагу, що $p^1 \oplus p^2 \in (C_0 \cap D_{0,1}) \subseteq D_{0,1}$, та $R^2(x) \oplus R^2(y) \in M_{0,1}$. Так як $M_{0,1} \cap D_J \neq \{0\}$ виконується тільки коли $|J| = 1$. то $R^2(x) \oplus R^2(y) \in D_{0,1}$ може відбутися, тільки коли $|J| = 1$.

2-раундове перетворення може буде переписано в термінах *super-Sbox*:

$$R^2 = ARK \circ MC \circ SR \circ \textit{super-Sbox} \circ SR(\cdot).$$

Так як операції SR та MC лінійні, то достатньо довести, що

$$\textit{super-Sbox}(q^1) \oplus \textit{super-Sbox}(q^2) \in W_J \Leftrightarrow \textit{super-Sbox}(\tilde{q}^1) \oplus \textit{super-Sbox}(\tilde{q}^2) \in W_J$$

,

$$q^i = SR(p^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & w^i \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ та } \tilde{q}^i = SR(\tilde{q}^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & w^{3-i} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},$$

де $i = 1, 2$ та множина W_J визначена, як $W_J := SR^{-1} \circ MC^{-1}(D_J)$.

Так як кожна колонка q^1 та q^2 залежить від різних та незалежних змінних, *super-Sbox* працює незалежно на кожній колонці та операція XOR коммутативна, то з цього слідує, що $super\text{-}Sbox(q^1) \oplus super\text{-}Sbox(q^2) = super\text{-}Sbox(\tilde{q}^1) \oplus super\text{-}Sbox(\tilde{q}^2)$, з якого слідує оригінальний тезіс. □

Змішаний інтегральний розпізнавач для 3-раундової Калина-128

Тепер ми можемо переписати теорему 2.1 у вигляді властивості нульової різниці.

Лема 2.5. *Дан підпростір* $A \equiv \langle e_{0,0}, e_{4,0} \rangle \subseteq C_0 \cap D_{0,1}$. *Розглянемо два відкритих текста* p^1 *та* p^2 *з одного простору* $A \oplus a$ *згенерованих* $p^1 \equiv (z^1, w^1)$ *та* $p^1 \equiv (z^1, w^2)$. *Нехай* $\tilde{p}^1, \tilde{p}^2$ – *це два інших відкритих текста, згерованих*

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5),$$

або

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}. *тоді* $R^2(p^1) \oplus R^2(p^2) \oplus R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) = 0$ *виконується з ймовірністю 1 для 2-раундової калини-128, незалежно від секретного ключа, SBox та MixColumns.*

На базі даної леми ми побудуємо 3-раундовий неможливий інтегральний розпізнавач.

З $R^2(p^1) \oplus R^2(p^2) \oplus R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) = 0$ випливає, що секретний ключ повинен задовольняти такій рівності

$$S\text{-}Box^{-1}(c^1_{j,l} \oplus k_{j,l}) \oplus S\text{-}Box^{-1}(c^2_{j,l} \oplus k_{j,l}) \oplus$$
$$S\text{-}Box^{-1}(\tilde{c}^1_{j,l} \oplus k_{j,l}) \oplus S\text{-}Box^{-1}(\tilde{c}^2_{j,l} \oplus k_{j,l}) = 0,$$

де $j = 0, .., 7, l = 0, 1$ Важним зауваженням є те, що існує щонайменше один ключ, який задовольняє рівності.

Лема 2.6. *Нехай* $\{c^1, c^2, \tilde{c}^1, \tilde{c}^2\}$ *- це множина шифртекстів, які є результатом 3-раундового шифрування* $\{p^1, p^2, \tilde{p}^1, \tilde{p}^2\}$. *З ймовірністю* 1 *існує як мінімум один ключ, що задовольняє рівності 2.2.1.*

Якщо не існує такого ключа, який задовольняє рівності, то перетворення – це не калина-128.

Мінусом даного методу є те, що нам потрібно шукати такий ключ. Тому, побудуємо розпізнавач, який буде працювати без необхідності підбирати ключ одного раунда. Наступна теорема показує цю властивість.

Теорема 2.2. *Нехай дан простор* $A \equiv \langle e_{0,0}, e_{0,4} \rangle \subseteq C_0 \cap D_{0,1}$. *Розглянемо два відкритих текста з одного простору* $p^1, p^2 \in A$, *згенерованої* $p^1 \equiv (z^1, w^1)$ *та* $p^2 \equiv (z^2, w^2)$. *Нехай* p^3, p^4 *– це два інших відкритих текста згенерованих*

$$p^3 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5), p^4 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5),$$

або

$$p^3 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5), p^4 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}.

Для усіх $i = 1, 2; j = 1, ..8$ *та для усіх пар* $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$, *умова*

$[R^3(p^\alpha) \oplus R^3(p^\beta)]_{i,j} = 0$ *та* $[R^3(p^\gamma) \oplus R^3(p^\delta)]_{i,j} \neq 0$

де $[\cdot]_{i,j}$ *означає байт в рядку* j *та стовпчику* i, *означає, що перетворення* R – *це не 3-раундова калина-128, незалежно від секретного ключа, сбоксів та матриці MixColumns.*

Доведення. Будемо доводити від супротивного. Нехай існує $i = 1, 2; j = 1, ..8$ та існує така пара з $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$, що $[R^3(p^\alpha) \oplus R^3(p^\beta)]_{i,j} = 0$ та $[R^3(p^\gamma) \oplus R^3(p^\delta)]_{i,j} \neq 0$.

За лемою 2.1, існує як мінімум один ключ k для 3-раундової Калини-128, що задовольняє рівняння. З того, що $[R^3(p^\alpha) = R^3(p^\beta)]_{i,j}$ следует $c^\alpha_{i,j} = c^\beta_{i,j}$, що вирожается в $S\text{-}Box^{-1}(c^\alpha_{i,j} \oplus k_{i,j}) \oplus S\text{-}Box^{-1}(c^\beta_{i,j} \oplus k_{i,j}) = 0$ згідно рівняння. $S\text{-}Box^{-1}(c^\gamma_{i,j} \oplus k_{i,j}) \oplus S\text{-}Box^{-1}(c^\delta_{i,j} \oplus k_{i,j}) = 0$ т.к. $[R^3(p^\gamma) = R^3(p^\delta)]_{i,j} \neq 0$,то $c^\gamma_{i,j} \neq c^\delta_{i,j}$, тобто $\forall k_{j,l} : S\text{-}Box^{-1}(c^\gamma_{i,j} \oplus k_{i,j}) \neq S\text{-}Box^{-1}(c^\delta_{i,j} \oplus k_{i,j})$ що є протиріччям із лемою 2.1. □

Алгоритм змішаного інтегрального розпізнавача для 3-раундової Калина-128

Ймовірність того, що випадково згенеровані тексти будуть мати властивість 2.2 дорівнює $1 - (1 - 2^{-8} * (1 - 2^{-8}))^{16*6} \approx 2^{-1.65}$ А ймовірність успіху розпізнавача дорівнює $1 - (1 - 2^{-1.65})^N$, де N – це кількість пар текстів. Для того, щоб ймовірність успіху була більша за 0.95, потрібно, щоб кількість пар $N \geq 8$. Якщо нам достатньо 8 пар текстів, то потрібно 5 різних текстів, бо $C^2_5 = 10 \geq 8$.

Введемо позначення для спрощення представлення алгоритму змішаного інтегрального розпізнавача:

$\Upsilon^{x,y}_{\Psi,\Phi} := \{p^1 = (x^1, y^1, \Psi, \Phi), p^2 = (x^2, y^2, \Psi, \Phi)\}.$

Algorithm 2.4 3-раундовий неможливий інтегральний розпізнавач Калини-128

Require: 5 $\Upsilon^{x,y}_{\Psi,\Phi} := \{p^1 = (x^1, y^1, \Psi, \Phi), p^2 = (x^2, y^2, \Psi, \Phi)\}$, де $p^1, p^2 \in C_0 \oplus a; p^1 \equiv (x^1, \psi_0, \psi_1, \psi_2, y^1, \psi_3, \psi_4, \psi_5), p^2 \equiv (x^2, \psi_0, \psi_1, \psi_2, y^2, \psi_3, \psi_4, \psi_5)$. та відповідні шифртексти після 3-ьох раундів.
Ensure: 1 якщо перетворення – це Калина-128, 0 – інакше
  for кожної двійки пар $[R^3(p^1), R^3(p^2)]$ та $[R^3(q^1), R^3(q^2)]$ **do**
    $\Upsilon^1 \equiv \{p^1, p^2\}$ та $\Upsilon^2 \equiv \{q^1, q^2\}$;
    for $i = 1, 2$ **do**
      for $j = 1, .., 8$ **do**
        if $[a \oplus b]_{i,k} = 0$ та $[c \oplus d]_{i,k} \neq 0$, де $(a, b, c, d) \in \{[R^3(p^1), R^3(p^2)], [R^3(q^1), R^3(q^2)]\}$, для усіх різних пар a, b, c, d **then**
          return 0
        end if
      end for
    end for
  end for
  return 1

2.2.2 Неможливий змішаний розпізнавач для Калини-256

Лема 2.7. *Для будь-яких x, y та для будь-яких множин індексів $I, J \subseteq \{0, 1, 2, 3\}$. $M_I \cap D_J = \{0\}$ тоді і тільки тоді, коли $|I| + |J| \leq 4$*

Аналогічно до Калини-128, щоб побудувати неможливий змішаний інтегральний розпізнавач для Калина-256, нам потрібно довести теорему аналогічну теорему до 2.1. Далі ми використаємо результат її задля того, щоб вивести властивість, якої не можуть мати шифртексти зашифровані за допомогою Калина-256.

Теорема 2.3. *Дано підпростір $A \equiv \langle e_{0,0}, e_{6,0} \rangle \subseteq C_0 \cap D_{0,3} \subseteq C_0$. Розглянемо два відкритих текста p^1 та p^2 з одного простору $A \oplus a$ згенерованої $p^1 \equiv (z^1, w^1)$ та $p^2 \equiv (z^2, w^2)$ (де $z^i, w^i \in F_{2^8}, i = 1, 2$). Нехай $\tilde{p}^1, \tilde{p}^2 \in C_0 \oplus a \equiv \langle e_{0,0}, e_{1,0}, e_{2,0}, e_{3,0}, e_{4,0}, e_{5,0}, e_{6,0}, e_{7,0} \rangle$ – це два інших відкритих текста згенерованих*

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^1, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^2, \psi_5),$$

або

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^2, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^1, \psi_5),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}. *Тоді*

$$R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$$

виконується із ймовірністю 1 для 4-раундової Калина-128 незалежно від секретного ключа, S-Box'ів та операції MixColumns.

Доведення.

Розглянемо дві пари текстів (p^1, p^2) та $(\tilde{p}^1, \tilde{p}^2)$ з простору $A \subseteq (C_0 \cap D_{0,3}) \oplus a$ для фіксованого a.

$$p^i \equiv a \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ w^i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ та } \tilde{p}^i \equiv a \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ w^{3-i} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

для $i = 1, 2$, тобто $p^i \equiv (z^i, w^i)$ та $\tilde{p}^i \equiv (z^i, w^{3-i})$.

Мета довести $R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$

Так як $\Pr\{R^2(x) \oplus R^2(y) \in M_I | x \oplus y \in D_I\}$, то потрібно довести, що $R^2(p^1) \oplus R^2(p^2) \in D_J \Leftrightarrow R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) \in D_J$ Перш за все звернемо увагу, що $p^1 \oplus p^2 \in (C_0 \cap D_{0,3}) \subseteq D_{0,3}$, та $R^2(x) \oplus R^2(y) \in M_{0,1}$. Так як $M_{0,3} \cap D_J \neq \{0\}$ виконується тільки коли $|J| = 1$. то $R^2(x) \oplus R^2(y) \in D_{0,3}$

може відбутися, тільки коли $|J| = 1$.

2-раундове перетворення може буде переписано в термінах *super-Sbox*:

$$R^2 = ARK \circ MC \circ SR \circ super\text{-}Sbox \circ SR(\cdot)$$

. Так як операції SR та MC лінійні, то достатньо довести, що $super\text{-}Sbox(q^1) \oplus super\text{-}Sbox(q^2) \in W_J \Leftrightarrow super\text{-}Sbox(\tilde{q}^1) \oplus super\text{-}Sbox(\tilde{q}^2) \in W_J$,

$$q^i = SR(p^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & w^i & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ та}$$

$$\tilde{q}^i = SR(\tilde{q}^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & w^{3-i} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

де $i = 1, 2$ та множина W_J визначена, як $W_J := SR^{-1} \circ MC^{-1}(D_J)$.

Так як кожна колонка q^1 та q^2 залежить від різних та незалежних змінних, *super-Sbox* працює незалежно на кожній колонці та операція XOR коммутативна, то з цього слідує, що $super\text{-}Sbox(q^1) \oplus super\text{-}Sbox(q^2) = super\text{-}Sbox(\tilde{q}^1) \oplus super\text{-}Sbox(\tilde{q}^2)$, з якого слідує оригінальний тезіс. □

Змішаний інтегральний розпізнавач для 3-раундової Калина-256

Теорема 2.3 може бути переписана, як властивість нульової різниці.

Лема 2.8. *Дан підпростір* $C_0 \cap D_{0,3} \equiv \langle e_{0,0}, e_{6,0} \rangle$. *Розглянемо два відкритих текста* p^1 *та* p^2 *з одного простору* $(C_0 \cap D_{0,3}) \oplus a$ *згенерованих* $p^1 \equiv (z^1, w^1)$ *та* $p^1 \equiv (z^1, w^2)$. *Нехай* $\tilde{p}^1, \tilde{p}^2$ *– це два інших відкритих текста, згерованих*

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^1, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^2, \psi_5),$$

або

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^2, \psi_5), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, w^1, \psi_5),$$

де $\psi_i, i = 0,..,5$ *можуть приймати будь-які значення з* F_{2^8}. *тоді* $R^2(p^1) \oplus R^2(p^2) \oplus R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) = 0$ *виконується з ймовірністю 1 для 2-раундової калини-128, незалежно від секретного ключа, SBox та MixColumns.*

На основі 2-раундової властивості вище ми побудуємо неможливу властивість для 3-раундової Калини-256.

З $R^2(p^1) \oplus R^2(p^2) \oplus R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) = 0$. випливає, що секретний ключ повинен задовольняти наступній рівності

$$S\text{-}Box^{-1}(c^1_{j,l} \oplus k_{j,l}) \oplus S\text{-}Box^{-1}(c^2_{j,l} \oplus k_{j,l}) \oplus$$
$$S\text{-}Box^{-1}(\tilde{c}^1_{j,l} \oplus k_{j,l}) \oplus S\text{-}Box^{-1}(\tilde{c}^2_{j,l} \oplus k_{j,l}) = 0,$$

де $j = 0,..,7, l = 0,..,3$ Важним зауваженням є те, що існує щонайменше один ключ, який задовольняє рівності.

Лема 2.9. *Нехай* $\{c^1, c^2, \tilde{c}^1, \tilde{c}^2\}$ *- це множина шифртекстів, які є результатом 3-раундового шифрування* $\{p^1, p^2, \tilde{p}^1, \tilde{p}^2\}$. *З ймовірністю* 1 *існує як мінімум один ключ, що задовольняє рівності.*

Якщо не існує такого ключа, який задовольняє рівності вище, то перетворення – це не калина-256. Проте знову, щоб не підбирати ключ одного раунда, ми виведемо властивість, яка не буде потребувати знання раундового ключа.

Теорема 2.4. *Нехай дан простор* $C_0 \cap D_{0,7} \equiv \langle e_{0,0}, e_{0,4} \rangle$. *Розглянемо два відкритих текста з одного простору* $p^1, p^2 \in (C_0 \cap D_{0,1})$, *згенерованої* $p^1 \equiv (z^1, w^1)$ *та* $p^2 \equiv (z^2, w^2)$. *Нехай* p^3, p^4 *– це два інших відкритих текста згенерованих*

$$p^3 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5), p^4 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5),$$

або

$$p^3 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5), p^4 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}.

Для усіх $i = 1, .., 4; j = 1, ..8$ *та для усіх пар* $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$, *умова*

$[R^3(p^\alpha) \oplus R^3(p^\beta)]_{i,j} = 0$ *та* $[R^3(p^\gamma) \oplus R^3(p^\delta)]_{i,j} \neq 0$

де $[\cdot]_{i,j}$ *означає байт в рядку* j *та стовпчику* i, *означає, що перетворення* R – *це не 3-раундова калина-128, незалежно від секретного ключа, сбоксів та матриці микколумнс.*

Доведення. Будемо доводити від супротивного. Нехай існує $i = 1, .., 4; j = 1, ..8$ та існує така пара з $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$, що $[R^3(p^\alpha) \oplus R^3(p^\beta)]_{i,j} = 0$ та $[R^3(p^\gamma) \oplus R^3(p^\delta)]_{i,j} \neq 0$.

За лемою 2.2, існує як мінімум один ключ k для 3-раундової Калини-256, що задовольняє рівняння. З того, що $[R^3(p^\alpha) = R^3(p^\beta)]_{i,j}$ следует $c^\alpha_{i,j} = c^\beta_{i,j}$, що вирожается в $S\text{-}Box^{-1}(c^\alpha_{i,j} \oplus k_{i,j}) \oplus S\text{-}Box^{-1}(c^\beta_{i,j} \oplus k_{i,j}) = 0$ згідно рівняння. $S\text{-}Box^{-1}(c^\gamma_{i,j} \oplus k_{i,j}) \oplus S\text{-}Box^{-1}(c^\delta_{i,j} \oplus k_{i,j}) = 0$ т.к. $[R^3(p^\gamma) = R^3(p^\delta)]_{i,j} \neq 0$,то $c^\gamma_{i,j} \neq c^\delta_{i,j}$, тобто $\forall k_{j,l} : S\text{-}Box^{-1}(c^\gamma_{i,j} \oplus k_{i,j}) \neq S\text{-}Box^{-1}(c^\delta_{i,j} \oplus k_{i,j})$ що є протиріччям із лемою 2.2. □

Алгоритм змішаного інтегрального розпізнавача для 3-раундової Калина-256

Ймовірність того, що випадково згенеровані тексти будуть мати властивість 2.4 дорівнює $1 - (1 - 2^{-8} * (1 - 2^{-8}))^{32*6} \approx 2^{-0.94}$. Ймовірність успіху розпізнавача для N пар текстів дорівнює $1 - (1 - 2^{-0.94})^N$, де N – це кількість пар текстів. Якщо ми хочемо, щоб ймовірність успіху була більша за 95%, то потрібна кількість пар більша за 5. Виходячи з цього, нам потрібно 4 різних текстів, бо $C^2_4 = 6 \geq 5$.

2.2.3 Неможливий змішаний розпізнавач для Калини-512

Лема 2.10. *Для будь-яких* x, y *та для будь-яких множин індексів* $I, J \subseteq \{0, .., 7\}$. $M_I \cap D_J = \{0\}$ *тоді і тільки тоді, коли* $|I| + |J| \leq 8$

Algorithm 2.5 3-раундовий неможливий інтегральний розпізнавач Калини-256

Require: 4 $\Upsilon^{x,y}_{\Psi,\Phi} := \{p^1 = (x^1, y^1, \Psi, \Phi), p^2 = (x^2, y^2, \Psi, \Phi)\}$, де $p^1, p^2 \in C_0 \oplus a; p^1 \equiv (x^1, \psi_0, \psi_1, \psi_2, y^1, \psi_3, \psi_4, \psi_5), p^2 \equiv (x^2, \psi_0, \psi_1, \psi_2, y^2, \psi_3, \psi_4, \psi_5)$. та відповідні шифртексти після 3-ьох раундів.
Ensure: 1 якщо перетворення – це Калина-256, 0 – інакше
  for кожної двійки пар $[R^3(p^1), R^3(p^2)]$ та $[R^3(q^1), R^3(q^2)]$ **do**
    $\Upsilon^1 \equiv \{p^1, p^2\}$ та $\Upsilon^2 \equiv \{q^1, q^2\}$;
    for $i = 1, .., 4$ **do**
      for $j = 1, .., 8$ **do**
        if $[a \oplus b]_{i,k} = 0$ та $[c \oplus d]_{i,k} \neq 0$, де $(a, b, c, d) \in \{[R^3(p^1), R^3(p^2)], [R^3(q^1), R^3(q^2)]\}$, для усіх різних пар a, b, c, d **then**
          return 0
        end if
      end for
    end for
  end for
  return 1

Відповідно до Калини-128 та Калини-256, побудуємо неможливий змішаний інтегральний розпізнавач для Калина-512. Для цього доведемо теорему аналогічну теорему до 2.1. Використаємо цей результат для виведення неможливої інтегральної властивості для шифру Калина-512.

Теорема 2.5. *Дано підпростір* $C_0 \cap D_{0,7} \equiv \langle e_{0,0}, e_{8,0} \rangle \subseteq C_0$. *Розглянемо два відкритих текста* p^1 *та* p^2 *з одного простору* $(C_0 \cap D_{0,71}) \oplus a$ *згенерованої* $p^1 \equiv (z^1, w^1)$ *та* $p^2 \equiv (z^2, w^2)$ *(де* $z^i, w^i \in F_{2^8}, i = 1, 2$*). Нехай* $\tilde{p}^1, \tilde{p}^2 \in C_0 \oplus a \equiv \langle e_{0,0}, e_{1,0}, e_{2,0}, e_{3,0}, e_{4,0}, e_{5,0}, e_{6,0}, e_{7,0} \rangle$ *– це два інших відкритих текста згенерованих*

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^1), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^2),$$

або

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^2), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^1),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}. *Тоді*

$$R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$$

виконується із ймовірністю 1 для 4-раундової Калина-128 незалежно від

секретного ключа, S-Box'ів та операції MixColumns.

Доведення.

Розглянемо дві пари текстів (p^1, p^2) та $(\tilde{p}^1, \tilde{p}^2)$ з простору $(C_0 \cap D_{0,7}) \oplus a$ для фіксованого a.

$$p^i \equiv a \oplus \begin{bmatrix} z^i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ w^i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ та } \tilde{p}^i \equiv a \oplus \begin{bmatrix} z^i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ w^i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

для $i = 1, 2$, тобто $p^i \equiv (z^i, w^i)$ та $\tilde{p}^i \equiv (z^i, w^{3-i})$.

Мета довести $R^4(p^1) \oplus R^4(p^2) \in M_J \Leftrightarrow R^4(\tilde{p}^1) \oplus R^4(\tilde{p}^2) \in M_J$

Так як $\Pr\{R^2(x) \oplus R^2(y) \in M_I | x \oplus y \in D_I\}$, то потрібно довести, що $R^2(p^1) \oplus R^2(p^2) \in D_J \Leftrightarrow R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) \in D_J$ Перш за все звернемо увагу, що $p^1 \oplus p^2 \in (C_0 \cap D_{0,7}) \subseteq D_{0,7}$, та $R^2(x) \oplus R^2(y) \in M_{0,7}$. Так як $M_{0,1} \cap D_J \neq \{0\}$ виконується тільки коли $|J| = 1$. то $R^2(x) \oplus R^2(y) \in D_{0,7}$ може відбутися, тільки коли $|J| = 7$.

2-раундове перетворення може буде переписано в термінах *super-Sbox*:

$$R^2 = ARK \circ MC \circ SR \circ \textit{super-Sbox} \circ SR(\cdot)$$

. Так як операції SR та MC лінійні, то достатньо довести, що $\textit{super-Sbox}(q^1) \oplus \textit{super-Sbox}(q^2) \in W_J \Leftrightarrow \textit{super-Sbox}(\tilde{q}^1) \oplus \textit{super-Sbox}(\tilde{q}^2) \in W_J$,

$$q^i = SR(p^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & w^i & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ та}$$

$$\tilde{q}^i = SR(\tilde{q}^i) \equiv SR(a) \oplus \begin{bmatrix} z^i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & w^{3-i} & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

де $i = 1, 2$ та множина W_J визначена, як $W_J := SR^{-1} \circ MC^{-1}(D_J)$.

Так як кожна колонка q^1 та q^2 залежить від різних та незалежних змінних, *super-Sbox* працює незалежно на кожній колонці та операція XOR коммутативна, то з цього слідує, що $super\text{-}Sbox(q^1) \oplus super\text{-}Sbox(q^2) = super\text{-}Sbox(\tilde{q}^1) \oplus super\text{-}Sbox(\tilde{q}^2)$, з якого слідує оригінальний тезіс. □

Змішаний інтегральний розпізнавач для 3-раундової

Калина-512

Переробимо теорему 2.5 у властивість нульової різниці.

Лема 2.11. *Дан підпростір* $C_0 \cap D_{0,7} \equiv \langle e_{0,0}, e_{7,0} \rangle$. *Розглянемо два відкритих текста* p^1 *та* p^2 *з одного простору* $(C_0 \cap D_{0,7}) \oplus a$ *згенерованих* $p^1 \equiv (z^1, w^1)$ *та* $p^1 \equiv (z^1, w^2)$. *Нехай* $\tilde{p}^1, \tilde{p}^2$ – *це два інших відкритих текста, згерованих*

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^1), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^2),$$

або

$$\tilde{p}^1 \equiv (z^1, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^2), \tilde{p}^2 \equiv (z^2, \psi_0, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, w^1),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}. *тоді* $R^2(p^1) \oplus R^2(p^2) \oplus R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) = 0$ *виконується з ймовірністю 1 для 2-раундової калини-128, незалежно від секретного ключа, SBox та MixColumns.*

З $R^2(p^1) \oplus R^2(p^2) \oplus R^2(\tilde{p}^1) \oplus R^2(\tilde{p}^2) = 0$. випливає, що секретний ключ повинен задовольняти наступній рівності

$$S\text{-}Box^{-1}(c^1_{j,l} \oplus k_{j,l}) \oplus S\text{-}Box^{-1}(c^2_{j,l} \oplus k_{j,l}) \oplus$$
$$S\text{-}Box^{-1}(\tilde{c}^1_{j,l} \oplus k_{j,l}) \oplus S\text{-}Box^{-1}(\tilde{c}^2_{j,l} \oplus k_{j,l}) = 0,$$

де $j, l = 0, .., 7$ Важним зауваженням є те, що існує щонайменше один ключ, який задовольняє рівності.

Лема 2.12. *Нехай* $\{c^1, c^2, \tilde{c}^1, \tilde{c}^2\}$ - *це множина шифртекстів, які є результатом 3-раундового шифрування* $\{p^1, p^2, \tilde{p}^1, \tilde{p}^2\}$. *З ймовірністю* 1 *існує як мінімум один ключ, що задовольняє рівності.*

Якщо не існує такого ключа, який задовольняє рівності, то перетворення – це не калина-128. Так як ми хочемо отримати розпізнач, який буде працювати без необхідності підбирати ключ одного раунда, то потрібно вивести цю властивість.

Теорема 2.6. *Нехай дан простор* $C_0 \cap D_{0,7} \equiv \langle e_{0,0}, e_{7,0} \rangle$. *Розглянемо два відкритих текста з одного простору* $p^1, p^2 \in (C_0 \cap D_{0,7})$, *згенерованої* $p^1 \equiv (z^1, w^1)$ *та* $p^2 \equiv (z^2, w^2)$. *Нехай* p^3, p^4 – *це два інших відкритих текста згенерованих*

$$p^3 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5), p^4 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5),$$

або

$$p^3 \equiv (z^1, \psi_0, \psi_1, \psi_2, w^2, \psi_3, \psi_4, \psi_5), p^4 \equiv (z^2, \psi_0, \psi_1, \psi_2, w^1, \psi_3, \psi_4, \psi_5),$$

де $\psi_i, i = 0, .., 5$ *можуть приймати будь-які значення з* F_{2^8}.

Для усіх $i = 1, .., 8; j = 1, ..8$ *та для усіх пар* $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$, *умова*

$[R^3(p^\alpha) \oplus R^3(p^\beta)]_{i,j} = 0$ *та* $[R^3(p^\gamma) \oplus R^3(p^\delta)]_{i,j} \neq 0$

де $[\cdot]_{i,j}$ *означає байт в рядку* j *та стовпчику* i, *означає, що перетворення* R – *це не 3-раундова калина-128, незалежно від секретного ключа, сбоксів та матриці микколумнс.*

Доведення. Будемо доводити від супротивного. Нехай існує $i = 1, .., 8; j = 1, ..8$ та існує така пара з $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$, що $[R^3(p^\alpha) \oplus R^3(p^\beta)]_{i,j} = 0$ та $[R^3(p^\gamma) \oplus R^3(p^\delta)]_{i,j} \neq 0$.

За лемою 2.3, існує як мінімум один ключ k для 3-раундової Калини-128, що задовольняє рівняння. З того, що $[R^3(p^\alpha) = R^3(p^\beta)]_{i,j}$ следует $c^\alpha_{i,j} = c^\beta_{i,j}$, що вирожается в $S\text{-}Box^{-1}(c^\alpha_{i,j} \oplus k_{i,j}) \oplus S\text{-}Box^{-1}(c^\beta_{i,j} \oplus k_{i,j}) = 0$ згідно рівняння. $S\text{-}Box^{-1}(c^\gamma_{i,j} \oplus k_{i,j}) \oplus S\text{-}Box^{-1}(c^\delta_{i,j} \oplus k_{i,j}) = 0$ т.к. $[R^3(p^\gamma) = R^3(p^\delta)]_{i,j} \neq 0$,то $c^\gamma_{i,j} \neq c^\delta_{i,j}$, тобто $\forall k_{j,l} : S\text{-}Box^{-1}(c^\gamma_{i,j} \oplus k_{i,j}) \neq S\text{-}Box^{-1}(c^\delta_{i,j} \oplus k_{i,j})$ що є протиріччям із лемою 2.3. □

Алгоритм змішаного інтегрального розпізнавача для 3-раундової Калина-512

Ймовірність того, що випадково згенеровані тексти будуть мати властивість 2.4 дорівнює $1 - (1 - 2^{-8} * (1 - 2^{-8}))^{32*6} \approx 2^{-0.47}$. Ймовірність

успіху розпізнавача для N пар текстів дорівнює $1-(1-2^{-0.47})^N$, де N – це кількість пар текстів. Якщо ми хочемо, щоб ймовірність успіху була більша за 95%, то потрібна кількість пар більша за 3. Виходячи з цього, нам потрібно 4 різних текстів, бо $C_4^2 = 6 \geq 3$.

Algorithm 2.6 3-раундовий неможливий інтегральний розпізнавач Калини-512

Require: 4 $\Upsilon^{x,y}_{\Psi,\Phi} := \{p^1 = (x^1, y^1, \Psi, \Phi), p^2 = (x^2, y^2, \Psi, \Phi)\}$, де $p^1, p^2 \in C_0 \oplus a; p^1 \equiv (x^1, \psi_0, \psi_1, \psi_2, y^1, \psi_3, \psi_4, \psi_5), p^2 \equiv (x^2, \psi_0, \psi_1, \psi_2, y^2, \psi_3, \psi_4, \psi_5)$. та відповідні шифртексти після 3-ьох раундів.
Ensure: 1 якщо перетворення – це Калина-512, 0 – інакше
  for кожної двійки пар $[R^3(p^1), R^3(p^2)]$ та $[R^3(q^1), R^3(q^2)]$ **do**
    $\Upsilon^1 \equiv \{p^1, p^2\}$ та $\Upsilon^2 \equiv \{q^1, q^2\}$;
    for $i = 1, .., 8$ **do**
      for $j = 1, .., 8$ **do**
        if $[a \oplus b]_{i,k} = 0$ та $[c \oplus d]_{i,k} \neq 0$, де $(a, b, c, d) \in \{[R^3(p^1), R^3(p^2)], [R^3(q^1), R^3(q^2)]\}$, для усіх різних пар a, b, c, d **then**
          return 0
        end if
      end for
    end for
  end for
  return 1

Висновки до розділу 2

У цьому розділі було наведено алгоритм побудови розпізнавача для «Калина»-подібних шифрів за допомогою ланцюгів підпросторових перетворень та криптоаналізу нульової різниці. Алгоритми розпізнавачів були побудовані для шифрів із розміром блоку 128, 256, 512 для п'яти раундів модифікованого шифру «Калина». Для розпізнавача 5-раундового шифру із розміром блоку 128 із ймовірністю успіху 95% потрібно 2^{12} відкритих текстів. Для модифікованого шифру «Калина» із розміром блоку 256 розпізнавач вимагає 2^{39} відкритих текстів, щоб ймовірність успіху була не менше 95%. Калина-512 для розпізнавача, побудованого за допомогою ланцюгів підпросторових перетворень, вимагає 2^{55} відкритих текстів із ймовірністю успіху 95%.

Для побудови розпізнавачів «Калина»-подібних шифрів за методом неможливого інтегрального аналізу було доведено необхідні теореми

аналогічні до віподпідних теорем для шифру AES. Алгоритми розпізнавачів були побудовані для шифрів із розміром блоку 128, 256, 512 для трьох раундів. Для розпізнавача 3-раундового шифру із розміром блоку 128 із ймовірністю успіху 95% потрібно 5 текстів. Для модифікованого шифру «Калина» із розміром блоку 256 та 512 потрібно 4 текста, щоб ймовірність успіху була більша за 95%.

ВИСНОВКИ

У ході даної роботи був проведений аналіз опублікованих джерел за тематикою аналізу лацнюгів перетворень підпросторів, криптоаналізу нульової різниці, неможливого та змішанного інтегрального криптоаналізу.

Було наведено алгоритм побудови розпізнавача для «Калина»-подібних шифрів за допомогою ланцюгів підпросторових перетворень та криптоаналізу нульової різниці. Алгоритми розпізнавачів були побудовані для шифрів із розміром блоку 128, 256, 512 для п'яти раундів модифікованого шифру «Калина». Для розпізнавача 5-раундового шифру із розміром блоку 128 із ймовірністю успіху 95% потрібно 2^{12} відкритих текстів. Для модифікованого шифру «Калина» із розміром блоку 256 розпізнавач вимагає 2^{39} відкритих текстів, щоб ймовірність успіху була не менше 95%. Калина-512 для розпізнавача, побудованого за допомогою ланцюгів підпросторових перетворень, вимагає 2^{55} відкритих текстів із ймовірністю успіху 95%.

Для побудови розпізнавачів «Калина»-подібних шифрів за методом неможливого інтегрального аналізу було доведено необхідні теореми аналогічні до віподпідних теорем для шифру AES. Алгоритми розпізнавачів були побудовані для шифрів із розміром блоку 128, 256, 512 для трьох раундів. Для розпізнавача 3-раундового шифру із розміром блоку 128 із ймовірністю успіху 95% потрібно 5 текстів. Для модифікованого шифру «Калина» із розміром блоку 256 та 512 потрібно 4 текста, щоб ймовірність успіху була більша за 95%.

Подальші напрямки дослідження повині бути спрямовані на підвищення ефективности використання структурних властивостей шифрів для методу неможливого інтегрального криптоаналізу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Oliynykov Roman, Gorbenko Ivan, Kazymyrov Oleksandr et al. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. Cryptology ePrint Archive, Report 2015/650. 2015. https://eprint.iacr.org/2015/650.

2. Grassi Lorenzo, Rechberger Christian, Rønjom Sondre. Subspace Trail Cryptanalysis and its Applications to AES. Cryptology ePrint Archive, Report 2016/592. 2016. https://eprint.iacr.org/2016/592.

3. Grassi Lorenzo. Mixture Differential Cryptanalysis and Structural Truncated Differential Attacks on round-reduced AES. Cryptology ePrint Archive, Report 2017/832. 2017. https://eprint.iacr.org/2017/832.

4. Bardeh Navid Ghaedi, Rønjom Sondre. Practical Attacks on Reduced-Round AES. Cryptology ePrint Archive, Report 2019/770. 2019. https://eprint.iacr.org/2019/770.