НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 004.056.55:512.6

«До захисту допущено»
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2024 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Бумерангове перетворення S-блоків та його властивості за різними алгебраїчними операціями»**

Виконав:
студент IV курсу, групи ФІ-03
Буржимський Ростислав Володимирович _____

Керівник:
доцент кафедри ММЗІ, к. т. н., доцент
Яковлєв Сергій Володимирович _____

Рецензент:
посада, степінь, звання
Прізвище Ім'я По-батькові _____

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

Студент _____

Київ — 2024

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2024 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Буржимський Ростислав Володимирович

1. Тема роботи: «*Бумерангове перетворення S-блоків та його властивості за різними алгебраїчними операціями*», науковий керівник роботи: доцент кафедри ММЗІ, к. т. н., доцент Яковлєв Сергій Володимирович,

затверджені наказом по університету №__ від «__» _____ 2024 р.

2. Термін подання студентом роботи: «__» _____ 2024 р.

3. Об'єкт дослідження: інформаційні процеси в системах захисту інформації

4. Предмет дослідження: алгебраїчні та криптографічні властивості бумерангів та бумерангових перетворень S-блоків

5. Перелік завдань:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) ввести поняття бумерангового перетворення S-блоку та дослідити його алгебраїчні властивості;

3) ввести поняття бумерангової еквівалентності S-блоків;

4) описати класи еквівалентності та розробити алгоритм генерування класу еквівалентності за результатом бумерангового перетворення;

5) знайти аналітичний вид розподілів імовірностей диференціалів бумерангових перетворень.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація доповіді

7. Орієнтовний перелік публікацій: частину результатів даної роботи було представлено на XXII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (13 - 17 травня 2024 р., м. Київ, Україна) [12], XXII Міжнародній науково-практичній конференції «Шевченківська весна – 2024» (11 квітня 2024 р., м. Київ, Україна) [11].

8. Дата видачі завдання: 10 вересня 2023 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2023 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-грудень 2023 р.	Виконано
3	Отримано алгебраїчні властивості бумерангового перетворення	Січень 2024	Виконано
4	Описано структуру класів бумерангової еквівалентності за різними операціями та алгоритм генерування класу еквівалентності	Лютий-березень 2024	Виконано
5	Отримано аналітичний вигляд розподілів імовірностей диференціалів бумерангових перетворень	Квітень 2024	Виконано
6	Оформлення дипломної роботи	Травень 2024	Виконано

Студент _____ Ростислав БУРЖИМСЬКИЙ

Керівник _____ Сергій ЯКОВЛЄВ

РЕФЕРАТ

Кваліфікаційна робота містить: 53 стор., 8 рисунки, 1 таблиць, 12 джерел.

У даній роботі розглянуто основні алгебраїчні властивості бумерангового перетворення бієктивного S-блоку відносно довільної операції, яка утворює на множині двійкових векторів структуру абелевої групи. Введено поняття бумерангової еквівалентності S-блоків та класів бумерангової еквівалентності. Описано структуру класів еквівалентності при фіксованому значенні параметра бумерангового перетворення. За структурою класів еквівалентності для операції побітового додавання описано алгоритм генерування випадкової інволютивної перестановки без нерухомих точок. Розроблено алгоритм генерування класу еквівалентності за результатом бумерангового перетворення та знайдено оцінки часової та просторової складності. Знайдено аналітичний вид розподілів імовірностей диференціалів бумерангових перетворень.

S-БЛОК, АТАКА БУМЕРАНГІВ, КОЕФІЦІЄНТИ БУМЕРАНГОВОЇ ЗВ'ЯЗНОСТІ, БУМЕРАНГОВЕ ПЕРЕТВОРЕННЯ

ABSTRACT

The qualification work consists of: 53 pages, 8 figures, 1 table, 12 references.

This work examines the main algebraic properties of the boomerang transformation of a bijective S-box with respect to an arbitrary operation that forms an Abelian group structure on the set of binary vectors. The concept of boomerang equivalence of S-boxes and classes of boomerang equivalence is introduced. The structure of the equivalence classes is described for a fixed value of the boomerang transformation parameter. Based on the structure of the equivalence classes for the bitwise addition operation, an algorithm for generating a random involution permutation without fixed points is described. An algorithm for generating the equivalence class based on the result of the boomerang transformation is developed, and estimates of time and space complexity are found. The analytical form of the probability distributions of the boomerang transformation differentials is determined.

S-BOX, BOOMERANG ATTACK, BOOMERANG CONNECTIVITY COEFFICIENTS, BOOMERANG TRANSFORMATION

ЗМІСТ

Перелік умовних позначень, скорочень і термінів 7
Вступ 8
1 Методи диференціального аналізу та аналізу бумерангів для блокових шифрів 10
1.1 Диференціальний криптоаналіз та імовірності диференціалів 10
1.2 Зведення обчислення розподілу диференціальної ймовірності до комбінаторної задачі на графах 12
1.3 Атака бумерангів та її модифікація 16
1.4 Коефіцієнт бумерангової зв'язності та його властивості 19
Висновки до розділу 1 22
2 Дослідження бумерангового перетворення відносно різних операцій 23
2.1 Алгебраїчні властивості бумерангового перетворення 23
2.2 Бумерангова еквівалентність відносно операції побітового додавання 28
2.3 Бумерангова еквівалентність відносно операції додавання за модулем 2^n 30
2.4 Алгоритм відновлення класу S-блоків з точністю до еквівалентності та алгоритм генерування випадкової інволютивної перестановки без нерухомих точок 33
2.5 Розподіл диференціальних ймовірностей для інволютивних перестановок без нерухомих точок 43
Висновки до розділу 2 49
Висновки 51
Перелік посилань 52

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

V_n — множина всіх бітових векторів довжини n;

$\oplus$ — операція побітового додавання;

$+$ — операція додавання за модулем 2^n;

BCT — таблиця бумерангової зв'язності (Boomerang Connectivity Table);

DDT — таблиця розподілу диференціалів (Difference Distribution Table);

$\mathcal{I}^{(n)}$ — множина усіх n-бітних інволютивних відображень без нерухомих точок;

$\Pi^{(n)}$ — множина усіх бієктивних n-бітових відображень;

$DP^f_{\circ,\bullet}(\alpha,\beta)$ — ймовірність диференціалу (α,β) булевої функції f з вхідною операцією $\circ$ та вихідною $\bullet$;

$[P]$ — дужки айверсона: якщо $[P] = 1$, то P – істинне, інакше P – хибне;

$\Phi(2n)$ — кількість інволютивних відображень на множині потужності $2n$.

ВСТУП

Актуальність дослідження. Атака бумерангів вперше була запропонована Д. Вагнером в 1999 році [10], як новий підхід до диференціального криптоаналізу. Зокрема даний підхід має перевагу над класичними методами в тому, що розглядається проходження диференціалів окремих компонент шифру. За роки після публікації були зроблені покращення даного підходу [4, 5], що дали нові можливості для аналізу шифрів. Один з таких підходів — це коефіцієнт бумерангової зв'язності, що є параметром оцінки стійкості до такого типу атак. Це новий метод представлений вперше у 2018 році [3]. В основі оцінки цього метода є бумерангове перетворення S-блока, що досліджується в даній роботі.

Метою дослідження уточнення методів криптоаналізу на основі бумерангів для блокових шифрів. Для досягнення мети потрібно виконати такі завдання дослідження:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) ввести поняття бумерангового перетворення S-блоку та дослідити його алгебраїчні властивості;

3) ввести поняття бумерангової еквівалентності S-блоків;

4) описати класи еквівалентності та розробити алгоритм генерування класу еквівалентності за результатом бумерангового перетворення;

5) знайти аналітичний вид розподілів імовірностей диференціалів бумерангових перетворень.

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

Предметом дослідження є алгебраїчні та криптографічні властивості бумерангів та бумерангових перетворень S-блоків.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, теорії імовірностей,

теорії складності алгоритмів, комбінаторного аналізу.

Наукова новизна отриманих результатів полягає у формалізації поняття бумерангового перетворення S-блоку відносно різних алгебраїчних операцій. Вперше одержано алгебраїчні та криптографічні властивості, зокрема розподіл бумерангових перетворень. Вперше введено поняття бумерангової еквівалентності, описано класи еквівалентності S-блоків та наведено алгоритм відновлення класу еквівалентності.

Практичне значення одержаних результатів: оцінювати стійкість блокових шифрів до узагальнень та модифікацій атак бумерангів. Як допоміжний факт побудовано ефективний алгоритм генерування випадкових інволюцій без нерухомих точок над множиною потужності 2^n.

Апробація результатів та публікації. Частину результатів даної роботи було представлено на XXII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (13 - 17 травня 2024 р., м. Київ, Україна) [12], XXII Міжнародній науково-практичній конференції «Шевченківська весна – 2024» (11 квітня 2024 р., м. Київ, Україна) [11].

1 МЕТОДИ ДИФЕРЕНЦІАЛЬНОГО АНАЛІЗУ ТА АНАЛІЗУ БУМЕРАНГІВ ДЛЯ БЛОКОВИХ ШИФРІВ

В даному розділі, розглянуто такі поняття як диференціальний криптоаналіз, що вперше був представлений в роботах [1, 2], та його формальна теорія. Продемонстровано метод пошуку розподілу диференціальної ймовірності для випадкової перестановки. Розглянуто атаку бумерангів та її модифікацію. Введено поняття коефіцієнта бумерангової зв'язності, як параметра стійкості до атаки бумерангів. Також описано результати по розподілу коефіцієнта бумерангової зв'язності та математичного сподівання.

1.1 Диференціальний криптоаналіз та імовірності диференціалів

Для початку введемо наступні позначення $\circ$ та $\bullet$ — це операції над V_n, для яких виконується:

1. $\langle V_n, \circ\rangle$ та $\langle V_n, \bullet\rangle$ — абелеві групи;

2. нейтральний елемент — нульовий вектор.

У диференціальному криптоаналізі розглядається як під час шифрування проходить різниця α між двома відкритими текстами x_0 та $x_0^{'} = x_0 \circ \alpha$, які паралельно і незалежно один від одного подаються на вхід до r-раундової схеми шифрування.

Схема диференціального криптоаналізу

0. Знайти диференціали α та β, що $\Pr\{x_r^{'} = x_r \bullet \beta | x_0^{'} = x_0 \circ \alpha\} \gg \frac{1}{2^n}$;

1. Накопичуємо N пар $(x,x^{'})$ таких, що $x^{'} = x \circ \alpha$ і відповідних їм шифротекстів $(y,y^{'})$;

2. Для кожного кандидати у k_r розшифровується пара $(y,y^{'}) \xrightarrow{E_{k_r}^{-1}} (x,x^{'})$ і перевіряється рівність $x_{r-1}^{'} = x_{r-1} \bullet \beta$;

3. Коректне значення ключа k_r — для якого рівність виконалася найбільшу кількість разів.

Зауваження. В якості статистики використовується індикаторна функція: $R_{r-1} = [x'_{r-1} = x_{r-1} \bullet \beta | x'_0 = x_0 \circ \alpha]$.

Перейдемо до розгляду формальної теорії диференціального криптоаналізу.

Означення 1.1. *Диференціалом* функції $f\colon V_n \to V_n$ називається довільна пара векторів $(\alpha, \beta) \in V_n^2$, з якою пов'язана така подія: пара входів на функцію f з різницею α відносно операції $\circ$ переходить у пару виходів із різницею β відносно операції $\bullet$.

Означення 1.2. *Імовірність диференціала* (α,β) булевої функції f за операціями $(\circ,\bullet)$ визначається як:

$$DP^f_{\circ,\bullet}(\alpha,\beta) = \frac{1}{2^n} \cdot \#\{x \in V_n : f(x \bullet \alpha) = f(x) \bullet \beta\}$$

У випадку, якщо $DP^f_{\circ,\bullet}(\alpha,\beta) = 0$, то (α,β) називають неможливим диференціалом

Означення 1.3. *Максимальна ймовірність* для операцій $(\circ,\bullet)$ та диференціала (α,β) булевої функції f визначається як:

$$MDP_{\circ,\bullet}(f) = \max_{\alpha \neq 0, \beta} DP^f_{\circ,\bullet}(\alpha,\beta)$$

Наведемо основні властивості диференціальних ймовірностей.

1. $\forall f\colon DP^f_{\circ,\bullet}(0,0) = 1$;
2. $\forall \beta\colon DP^f_{\circ,\bullet}(0,\beta) = [\beta = 0]$;
3. $\forall \alpha\colon DP^f_{\circ,\bullet}(\alpha,0) = [\alpha = 0]$, якщо f є бієктивною (ін'єктивною);
4. $\forall \alpha\colon \sum\limits_{\beta} DP^f_{\circ,\bullet}(\alpha,\beta) = 1$;
5. $\forall \beta\colon \sum\limits_{\alpha} DP^f_{\circ,\bullet}(\alpha,\beta) = 1$, якщо f є бієктивною;
6. $\forall \alpha \neq 0, \beta \neq 0\colon MDP_{\circ,\bullet}(f) \geqslant \frac{1}{2^n - 1}$.

Зауваження. На початку дослідження диференціального криптоаналізу популярною операцією для дослідження імовірності

диферецiалiв була операцiя побiтового додавання. У такому випадку диференцiальну ймовiрнiсть можна задати через похiдну булевої функцiї за напрямком

$$DP^f_{\oplus}(\alpha,\beta) = \frac{1}{2^n} \cdot \#\{x \in V_n \colon D_\alpha(f(x)) = \beta\}.$$

Тодi для даної операцiї можна було виконувати швидке обчислення диференцiальних ймовiрностей. Замiсть перебору трьох параметрiв x,α,β, достатньо перебирати лише параметри x,α, таким чином потрiбно зробити $T(n) = 2^{2n}$ крокiв i виділити просторової пам'яті $S(n) = 2^n$

Означення 1.4. Нехай $S \colon V_n \to V_n$, $(a,b) \in V_n^2$. Тоді DDT для S задається таблицею $2^n \times 2^n$, у якій запис позицій для диференцiалу (a,b) задається як:

$$DDT_S(a,b) = \#\{x \in V_n \colon \ S(x) \oplus S(x \oplus \alpha) = \beta\}.$$

1.2 Зведення обчислення розподiлу диференцiальної ймовiрності до комбiнаторної задачi на графах

Розглянемо метод, що був запропонований в статтi [6]. Його суть полягає у тому, щоб розглядати проблему пошуку розподiлу диференцiальної ймовiрності, як комбiнаторну задачу на графi: порахувати кiлькiсть вiдображень зi збереженням ребер мiж двома визначеними орiєнтованими графами.

Означення 1.5. Для групи $\langle V_n, \otimes \rangle$ порядку 2^n i нетривiального диференцiала α iснує вiдповiдний орiєнтований граф, що позначається як $D_\alpha = (V_n, E_\alpha)$. Такий граф називається рiзницевим графом вiдносно операцiї $\otimes$.

Множина ребер графа D_α визначена як $E_\alpha = \{(u,v) \in V_n^2 \mid u \otimes (v)^{-1} = \alpha\}$, тобто мiж вершинами (u,v) iснує дуга, якщо вершини мають рiзницю α за операцiєю $\otimes$.

З властивості замкненості груп випливає, що кожна вершина різницевого графа породженого α має одне вхідне і вихідне ребро. Отже, дуги в різницевому графі утворюють замкнені ланцюги. Також з теореми Лагранжа випливає, що D_α містить $\frac{2^n}{\operatorname{ord}\alpha}$ неперетинних циклів довжини $\operatorname{ord}\alpha$.

Означення 1.6. Нехай $D_\alpha = (V_n,E_\alpha)$ і $D_\beta = (V_n,E_\beta)$ — різницеві орієнтовані графи, що породжуються різницями $\alpha,\beta \in V_n$. Для перестановки $\pi \in \Pi^{(n)}$ визначимо величину, що позначає кількість дуг з різницею α, які під дією перестановки переходять у дугу з різницею β:

$$d_{\otimes,\pi}(D_\alpha,D_\beta) = \#\{(u,v) \in E_\alpha \mid (u',v') \in E_\beta, \pi(u) = u', \pi(v) = v'\}$$

З означення випливає, що дана величина буде описувати імовірність диференціалу (α,β) для перестановки π:

$$d_{\otimes,\pi}(D_\alpha,D_\beta) = 2^n \cdot DP_\otimes(\pi,\alpha,\beta).$$

Також з отриманих означень, можна сформувати теорему, що описує розподіл диференціальної ймовірності для деякої абелевої групи та диференціалів цієї групи.

Теорема 1.1. *Для будь-якої абелевої групи G і елементів $\alpha,\beta \in G$, ймовірність $\Pr(2^n \cdot DP_\otimes(\pi,\alpha,\beta) = t)$ залежить лише від t, $\operatorname{ord} G = \#G$, $a = \operatorname{ord}\alpha$ і $b = \operatorname{ord}\beta$. Для $a = 2^r, b = 2^s, 1 \leqslant r \leqslant n, 1 \leqslant s \leqslant n$ і $1 \leqslant t \leqslant 2^n$:*

$$p_t(\#G,a,b) = \Pr(2^n \cdot DP_\otimes(\pi,\alpha,\beta) = t \mid \pi \in_R \Pi^{(n)}).$$

Нехай α,β елементи $\langle V_n,\otimes\rangle$, $D_\alpha = (V,E_\alpha)$ і $D_\beta = (V,E_\beta)$ відповідні різницеві графи. Для кожної дуги $uv \in E_\alpha$ позначимо множину перестановок, що поєднують різницеві графи, утворені різницями α та β.

$$A_{uv} = \{\pi \in \Pi^n \mid (\pi(u),\pi(v)) \in E_\beta\}.$$

Тоді за формулою включень та виключень кількість таких π, що

переводять рівно t дуг з D_α в D_β значення можна визначити як

$$P_t = \sum_{i=0}^{2^n-t} (-1)^i C_{t+i}^i S_{t+i}, \quad S_k = \sum_{\mathcal{Y} \subseteq E_\alpha, |\mathcal{Y}|=k} \left| \bigcap_{uv \in \mathcal{Y}} A_{uv} \right|.$$

Тоді розподіл диференціальної ймовірності обчислюється як:

$$p_t(\#G,a,b) = \frac{P_t}{2^n!}$$

Для абелевої групи $\langle V_n, \oplus \rangle$ було показано, що

$$P_{2t} \sim (C_{2^{n-1}}^t)^2 \cdot 2^t \cdot t! \cdot \frac{(2^{n-1}-t)!}{e^{1/2}}$$

Також для диференціалів порядку 2 показано, що $p_{2t}(2^n,2,2)$ асимптотично збігатиметься до розподілу Пуассона, що описується такою лемою.

Лема 1.1. *Якщо $t \in o(2^{n/2})$ при $n \to \infty$, тоді*

$$p_{2t}(2^n,2,2) = \frac{e^{-\frac{1}{2}}}{2^t \cdot t!} \cdot (1 + O((t+1)^2/2^n))$$

У випадку операції побітового додавання пошук значення P_t значно спрощується, тому що порядок різниць α та β дорівнює 2, і множини A_{uv} є незалежними в тому плані, що uv є єдиним ребром, яке інцидентне до u та v. Для загальної групової операції $\otimes \neq \oplus$ більшість елементів групи α матимуть порядок $\alpha > 2$, і, таким чином, породять різницевий граф, для якого існують множини $A_{u_1v_1}$, $A_{u_2v_2}$, де $v_1 = u_2$. Залежність між множинами A_{uv} значно ускладнює вирази для P_t. В наступній лемі буде описано розподіл для вхідної різниці з порядком 2 та вихідної різниці з порядком 4.

Лема 1.2. *Для $n \geqslant 2$ та $0 \leqslant t \leqslant 2^{n-1}$*

$$p_t(2^n,2,4) = \frac{1}{2^n} \cdot \sum_{i=0}^{2^{n-1}-t} (-1)^k C_{t+i}^i S_{t+i},$$

де для $0 \leqslant k \leqslant 2^{n-1}$,

$$S_k = \left(\sum_{i=\lceil k/2 \rceil}^{\min(k,2^{n-2})} C_{2^{n-2}}^{i} C_i^{k-i} \cdot 2^{3i} \right) \cdot C_{2^{n-1}}^{k} \cdot k! \cdot (2^n - 2k)!.$$

Як можна побачити, значення S_k має громіздки аналітичний запис, що ускладнює зведення розподілу диференціальної ймовірності до уже відомого розроділу. Для полегшення пошуку S_k було запропоновано застосувати апроксимацію цього значення. Головна ідея полягає в тому, щоб розглядати S_k не у термінах збереження ребер, а розкласти на терміни збереження вершин. Множина з k ребер інцидентна хоча б k вершинам і максимум $2k$ вершинам. Позначимо $p(\mathcal{Y})$ — кількість вершин, що інцидентні ребрам з множини $\mathcal{Y}$, де $k \leqslant p(\mathcal{Y}) \leqslant 2k$. Для $k \leqslant j \leqslant 2k$, визначимо

$$\phi(k,j) = \sum_{\mathcal{Y} \subseteq E_\alpha, |\mathcal{Y}|=k, p(\mathcal{Y})=j} |\{\pi | \pi(\mathcal{Y}) \subseteq E_\beta\}|.$$

Тоді S_k можна визначити такою сумою

$$S_k = \sum_{j=k}^{2k} \phi(k,j).$$

Було показано, що насправді $\phi(k,2k)$ домінує над усіма іншими доданками в термінах відображення незв'язних ребер D_α в незв'язні ребра D_β. Тоді S_k можна наблизити значенням $\phi(k,2k)$. Наведемо лему, яка описує значення S_k при наближенні.

Лема 1.3. *Нехай $n \geqslant 0, a = 2^r, b = 2^s, 1 \leqslant r \leqslant n$ та $2 \leqslant s \leqslant n$. Тоді*

$$S_k = \frac{2^n!}{k!} \cdot (1 + O(k^2/2^n)), \text{ для } k \in o(2^{n/2}), n \to \infty.$$

Використавши таке наближення, автори в статті змогли показати, що для диференціалів порядок, яких більш як два, розподіл диференціальної ймовірності буде розподілом Пуассона з параметром 1.

Лема 1.4. *Нехай* $a > 2$ *або* $b > 2$ *та* $t \in o(2^{n/2}/2)$, *тоді*

$$p_t(2^n,a,b) = \frac{e^{-1}}{t!} \cdot (1 + O((t+1)^2)/2n).$$

З леми 1.2 та леми 1.4 можна сформувати, теорему, що буде описувати розподіл диференціальної ймовірності для абелевої групи.

Теорема 1.2. *Нехай* $(V_n, \otimes)$ — *абелева група порядку* 2^n *і* $(\alpha,\beta) \in V_n^2$ *нетривіальні диференціали. Якщо* $\pi \in_R \Pi^{(n)}$ *і* $t = o(2^{n/2})$, *то*

$$Pr\left\{DP^{\pi}_{\otimes}(\alpha,\beta) = \frac{t}{2^{n-1}}\right\} \sim e^{-\frac{1}{2}} \cdot \frac{1}{2^t \cdot t!}, \qquad \textit{якщо } \operatorname{ord}\alpha = \operatorname{ord}\beta = 2$$

$$Pr\left\{DP^{\pi}_{\otimes}(\alpha,\beta) = \frac{t}{2^{n}}\right\} \sim e^{-1} \cdot \frac{1}{t!}, \qquad \textit{в інших випадках}$$

Наслідок 1.1.

1. $\mathbb{E}[DP_{\circ}(\alpha,\beta)] \sim \frac{1}{2^n}$;

2. $\sigma[DP_{\circ}(\alpha,\beta)] \sim \frac{\eta}{2^n}$, *де* $\eta = \sqrt{2}$, *якщо* $\operatorname{ord}\alpha = \operatorname{ord}\beta = 2$, *інакше* $\eta = 1$.

Тобто у випадку, коли диференціали мають порядок два, тоді апроксимації ймовірності диференціалів мають відхилення в $\sqrt{2}$ більше за інші випадки. Тоді такі апроксимації, для яких порядок диференціалів дорівнює 2, матимуть вищі ймовірності.

1.3 Атака бумерангів та її модифікація

Атака бумерангів — це новий підхід до використання теорії диференціального криптоаналізу, що був опублікований Д. Вагнером у статті 1999 [10]. Розглядається декомпозиція шифру E на два підшифра E_1 та E_0, при цьому $E_1 \neq E_0$, та досліджується диференціальне поширення компонент шифру, що є перевагою над класичними методами. Атака базується на чотирьох відкритих текстах розбитих на пари з фіксованою різницею α та відповідними шифротекстами з фіксованою

різницею δ. Під час шифрування припускається, що вхідна різниця α під дією E_0 переде в β з ймовірністю p, тоді як різниця γ перейде в δ під дією E_1 з ймовірністю q, аналогічні ймовірності будуть при розшифруванні. Тоді загальна ймовірність поширення диференціалів, зображених на рис. 1.1, описується як:

$$Pr\{E^{-1}(E(x) \oplus \delta) \oplus E^{-1}(E(x \oplus \alpha) \oplus \delta) = \alpha\} = p^2 q^2.$$

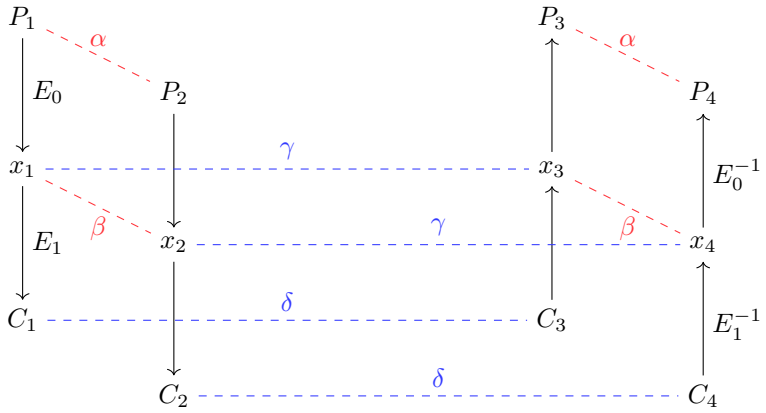

Рисунок 1.1 – схема атаки бумерангів

В даній атаці найважливішою частиною вважається вибір відповідних диференціальних характеристик для E_0 та E_1. Стандартне припущення про незалежність обраних диференціальних характеристик виявилося некоректним. Зокрема, Мерфі в статті [8] вказав, що для шифрів на основі S-блоків дві незалежно обрані характеристики можуть бути залежними, таким чином ймовірність створення правильного квартету буде нульовою.

Для коригування методу аналізу бумерангів після зауважень Мерфі у статтях [4, 5] було запропоновано модифіковану атаку, що зображена на рис. 1.2, яка узагальнювала залежності диференціальних характеристик. Структура атаки відносно атаки бумерангів змінилася в тому що розглядається композиція E на 3 компоненти, $E(x) = E_1(E_m(E_0(x))$ та описали диференціальні характеристики для E_m.

Нехай (x_1,x_2,x_3,x_4) та (y_1,y_2,y_3,y_4) вхідні та вихідні четвірки текстів для E_m, де $y_i = E_m(x_i)$. Диференціальна характеристика E_0 визначає для E_m вхідну різницю β, а саме $x_1 \oplus x_2 = x_3 \oplus x_4 = \beta$, E_1 визначає для E_m вихідну різницю γ, тобто $y_1 \oplus y_3 = y_2 \oplus y_4 = \gamma$. Тоді значення r можна визначити таким чином:

$$r = \Pr\{(x_3 \oplus x_4) = \beta \,|\, (x_1 \oplus x_2) = \beta, (y_1 \oplus y_3) = \gamma, (y_2 \oplus y_4) = \gamma\}. \quad (1.1)$$

Загальна ймовірність поширення диференціалів зображених на рис 1.2 для шифру E визначається як:

$$Pr\{E^{-1}(E(P_1) \oplus \delta) \oplus E^{-1}(E(P_1 \oplus \alpha) \oplus \delta) = \alpha\} = p^2q^2r.$$

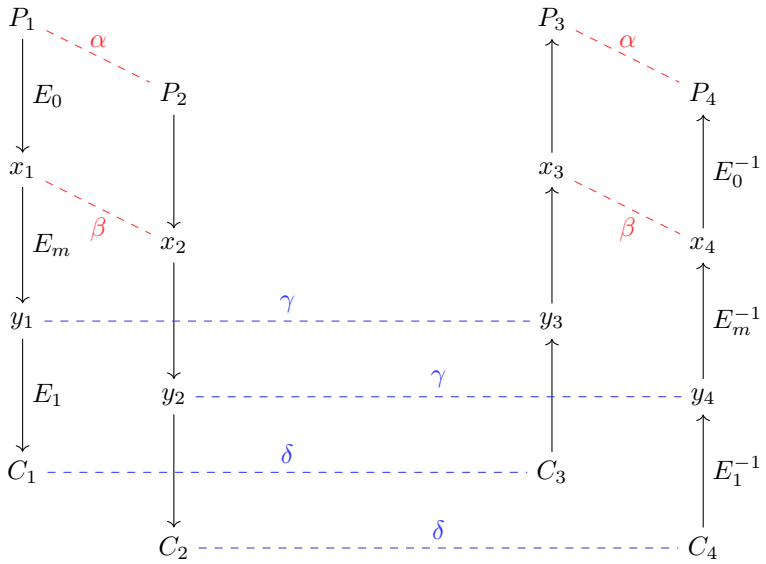

Рисунок 1.2 – схема узагальненої атаки бумерангів

Серед властивостей такого типу атаки можна виділити декілька. Для того, щоб шифр E відрізнити від ідеального шифру потрібно обрати близько $\frac{1}{(pq)^2r}$ адаптивних відритих текстів або шифротекстів та величина $p^2q^2r \gg \frac{1}{2^n}$. Недоліком даної атаки це те, що треба вміти не лише шифрувати, але й розшифровувати.

1.4 Коефіцієнт бумерангової зв'язності та його властивості

В 2018 році була опублікована стаття [3], що надала можливість обраховувати ймовірність (рівняння 1.1) генерації квартету зображеного на рис. 1.3 на окремому рівні. Також було показано взаємозв'язок атаки бумерангів з таблицею диференціальних ймовірностей.

На рис 1.3 розглядається випадок коли вхідний диференціал a до S-блоку визначаються підшифром E_0, а вихідний підшифром E_1. Важливе зауваження, що якщо зафіксувати вхідний диференціал, то всі значення у квартеті будуть фіксованими. Оскільки генерація правої частини квартету — це ймовірнісна подія для обчислення якої нам знадобиться наступний інструмент.

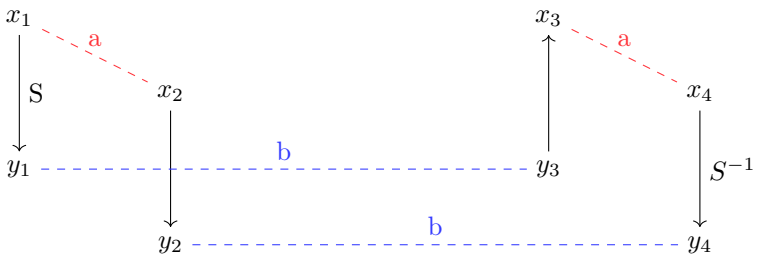

Рисунок 1.3 – обчислення r, коли E_m — це шар S-блоків

Означення 1.7. Нехай $S\colon V_n \to V_n$ — бієктивне відображення. Тоді таблиця бумерангової зв'язності (англ. Boomerang Connectivity Table) для S задається таблицею $2^n \times 2^n$, у якій запис позицій для диференціалу (a,b) визначається таким чином:

$$BCT_S(a,b) = \#\{x \in V_n\colon\ S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}.$$

Будь-яке значення в першому рядку та першому стовпці BCT дорівнює 2^n. Такий перехід з ймовірністю 1 можна описати за допомогою схеми перемикання сходинки (англ. Ladder switch), зображеної на рис. 1.4a. У випадку, якщо $a \neq 0$ і $b = 0$, можна побачити, що для будь-якого

x_1 і $x_2 = x_1 \oplus a$ маємо їхні образи y_1, y_2 після застосування S-блоку. Якщо $b = 0$, це значить, що ніяких модифікацій для шифротекстів застосовано не було. Тоді до y_1, y_2 застосуємо S^{-1} та отримаємо x_1, x_2 з ймовірністю 1. Аналогічно буде для випадку коли $a = 0$ і $b \neq 0$.

Тепер розглянемо зв'язок BCT і DDT, це можна зробити за допомогою схеми перемикання S-блоку (англ. S-box switch), зображеної на рис. 1.4б. Якщо для (a,b_0) $DDT_S(a,b_0) \neq 0$, тоді взявши $b_1 = b_0$ $BCT_S(a,b_1)$ набуває також значення, що й $DDT_S(a,b_0)$. На рис 1.4(б) припускається, що два входи $x_1, x_2 = x_1 \oplus a$ відображаються на $y_1 \oplus y_2 = b_0$ з ймовірністю p. Встановивши $b_0 = b_1$, тоді образи обчислюються як $y_3 = y_1 \oplus b_0$ та $y_4 = y_2 \oplus b_0$. Тоді це буде просто зміна місцями y_1 і y_2 після застосування S^{-1} на виході отримаємо пару (x_2,x_1).

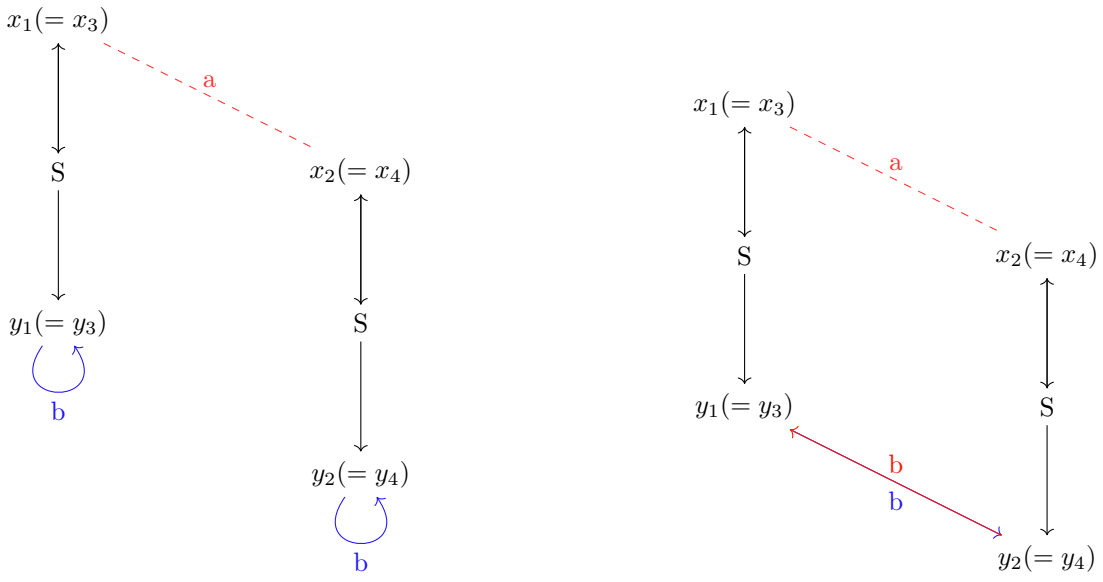

Рисунок 1.4 – (а) — перемикання сходинки , (б) — перемикання S-блоку

З отриманих вище тверджень можна узагальнити основні властивості для BCT як:

1. $BCT_S(0,b) = BCT_S(a,0) = 2^n$;
2. $BCT_s(a,b) = 0$, тоді диферецiали (a,b) є несумісними;
3. $\forall a,b \in V_n$: $BCT_S(a,b) = BCT_{S^{-1}}(b,a)$;

4. $\forall a,b \in V_n$: $BCT_S(a,b)$ — парне число ;

5. $\forall (a,b) \in V_n^2$: $BCT_S(a,b) \geqslant DDT_S(a,b)$;

6. Нехай $S_b = S^{-1}(S(x) \oplus b)$, тоді $BCT_S(a,b) = 2^n DP_{\oplus}^{S_b}(a,a)$.

Означення 1.8. Нехай $S\colon V_n \to V_n$ — бієктивне відображення; для будь-якої пари різниць $(a,b) \in V_n^2$ *коефіцієнт бумерангової зв'язності* за операцією побітового додавання визначається як:

$$\delta_{\oplus}^S(a,b) \;=\; \frac{1}{2^n} \cdot \#\{x \;\in\; V_n\colon S^{-1}(S(x \oplus a) \oplus b) \oplus S^{-1}(S(x) \oplus b) \;=\; a\}.$$

Теорема 1.3. *Нехай S випадково рівноімовірно обрана перестановка на V_n, тоді розподіл коефіцієнта бумерангової зв'язності для диференціалів $a,b \in V_n\backslash\{0\}$ моделюється двома випадковими і незалежними випадковими величинами $\xi_1 \sim Bin(2^{n-1}, \frac{1}{2^n-1})$ та $\xi_2 \sim Bin(2^{2n-2} - 2^{n-1}, \frac{1}{(2^n-1)^2})$.*

$$Pr\{\delta_{\oplus}^S(a,b) = c\} = \sum_{2i_1+4i_2=c} Pr\{\xi_1 = i_1\} \cdot Pr\{\xi_2 = i_2\}$$

Для $t = (2^n-1)^2$, математичне сподівання буде набувати наступного вигляду:

$$\mathbb{E}[\delta_{\oplus}^S] = \sum_{c=0}^{2^n} c\Big(\Big(\sum_{i=0}^{c} Pr\{\delta_{\oplus}^S(a,b) = i\}\Big)^t - \Big(\sum_{i=0}^{c-2} Pr\{\delta_{\oplus}^S(a,b) = i\}\Big)^t\Big)$$

Як можна побачити з таблиці 1.1 очікуване значення коефіцієнту бумерангової зв'язності зростає повільно із ростом n і воно буде значно менше за 2^n.

n	$\mathbb{E}(\delta_{\oplus}^S)$	$\frac{\mathbb{E}(\delta_{\oplus}^S)}{2^n}$	n	$\mathbb{E}(\delta_{\oplus}^S)$	$\frac{\mathbb{E}(\delta_{\oplus}^S)}{2^n}$	n	$\mathbb{E}(\delta_{\oplus}^S)$	$\frac{\mathbb{E}(\delta_{\oplus}^S)}{2^n}$	n	$\mathbb{E}(\delta_{\oplus}^S)$	$\frac{\mathbb{E}(\delta_{\oplus}^S)}{2^n}$
4	11.6	0.725	6	16.3	0.254	8	20.2	0.079	10	23.9	0.023
5	14.2	0.443	7	18.3	0.143	9	22.1	0.043	11	25.7	0.013

Таблиця 1.1 – мат. сподівання коефіцієнта бумерангової зв'язності для n-бітної перестановки

Висновки до розділу 1

У даному розділу був проведений аналіз опублікованих джерел за тематикою диференціального аналізу та аналізу бумерангів. Зокрема було описано поняття диференціала та його імовірності. Наведено основні властивості диференціальних ймовірностей. Досліджено результати статті [6], що дозволяють шукати розподіл диференціалів для випадкової перестановки. Також в цій статті було показано, що для випадків, коли диференціали мають порядок рівний 2, величини будуть розподілені в $\sqrt{2}$ разів краще.

Розглянуто атаку бумерангів, що описана в статті [10], наведено структуру атаки та ймовірність диференціального поширення шифра. Також в статті [8] було описано, що атака мала недоліки в припущенні незалежності диференціальних характеристик двох компонент шифру, що в деяких випадках зводило ймовірність генерування квартету до нуля. Зокрема в статтях [4, 5] ці недоліки були виправлені та було покращено атаку розбивши шифр на три компоненти, де посередині був шар S-блоків. Також у модифікації було описано ймовірність генерації диференціального поширення середнього шару. В статті [3] був представлений BCT, що дозволяє обчислювати ймовірність поширення диференціалів в середній компоненті розбитого шифру. Також в статті [9] був наведений розподіл коефіцієнту бумерангової зв'язності для випадкової перестановки над множиною V_n.

2 ДОСЛІДЖЕННЯ БУМЕРАНГОВОГО ПЕРЕТВОРЕННЯ ВІДНОСНО РІЗНИХ ОПЕРАЦІЙ

У даному розділі розглянуто основні алгебраїчні властивості бумерангового перетворення бієктивного S-блоку відносно довільної операції, яка утворює на множині двійкових векторів структуру абелевої групи. Введено поняття бумерангової еквівалентності S-блоків та класів бумерангової еквівалентності. Доведено, що для параметрів порядку 2 образи бумерангового перетворення є інволюціями без нерухомих точок; для інших параметрів вичерпно описано циклову структуру образу. Досліджено розбиття множини S-блоків на класи еквівалентності при зафіксованому параметрі бумерангового перетворення для операцій побітового додавання та модульного додавання. Описано алгоритм відновлення класу бумерангового перетворення з точністю до еквівалентності. Отримано розподіл диференціальної ймовірності для інволютивних відображень без нерухомих точок. Результати, які будуть наведені далі, були опубліковані в роботах [12, 11].

2.1 Алгебраїчні властивості бумерангового перетворення

Означення 2.1. Нехай $S\colon V_n \to V_n$ — бієктивне відображення, $\otimes$ — така операція, що $\langle V_n, \otimes\rangle$ є абелевою групою. Бумерангове перетворення S-блока S з параметром b для операції $\otimes$ позначається таким чином:

$$S_{\otimes,b} = S^{-1}(S(x) \otimes b).$$

Перелічимо основні знайдені властивості бумерангових перетворень S-блоків відносно операції $\otimes$.

Лема 2.1. *Для усіх $b \in V_n$ відображення $S_{\otimes,b}(x)$ є бієктивним.*

Доведення. Для початку покажемо, що $S_{\otimes,b}$ — ін'єктивне відображення. Для цього потрібно показати, що

$$\forall x_1,x_2 : x_1 \neq x_2 \Rightarrow S_{\otimes,b}(x_1) \neq S_{\otimes,b}(x_2).$$

Проведемо доведення від супротивного. Нехай $S_{\otimes,b}(x_1) = S_{\otimes,b}(x_2)$, тоді розпишемо детальніше наведену рівність

$$S^{-1}(S(x_1) \otimes b) = S^{-1}(S(x_2) \otimes b).$$

Оскільки S — бієктивне відображення, тоді до лівої та правої частини застосуємо відображення S, і тоді отримаємо

$$S(x_1) \otimes b = S(x_2) \otimes b.$$

Бумерангове перетворення задане відносно абелевої групи, тоді додамо до лівої та правої частини рівності b^{-1} та отримаємо, що

$$S(x_1) = S(x_2).$$

Звідси отримаємо суперечність з тим, що S — ін'єктивне відображення, а дана рівність суперечить означенню ін'єктивності.

Для перевірки, що $S_{\otimes,b}$ — сюр'єктивне відображення потрібно показати, що

$$\forall y \in V_n \; \exists x \in V_n : S_{\otimes,b}(x) = y.$$

Розпишемо для початку наведену рівність:

$$S^{-1}(S(x) \otimes b) = y.$$

Застосуємо відображення S до обох сторін рівності

$$S(S^{-1}(S(x) \otimes b)) = S(y).$$

Оскільки S — бієктивне відображення, тоді $S(S^{-1}(x)) = x$, застосувавши

дану властивість отримаємо

$$S(x) \otimes b = S(y).$$

Тобто початкову умову вдалося звести до вигляду

$$\forall y \in V_n \; \exists x \in V_n : S(x) \otimes b = S(y).$$

З того, що S — сюр'єктивне відображення, тоді уся множина V_n є досяжною для кожного входу та операція $\otimes$ утворює абелеву групу, тобто для b існує рівно одне значення $S(x)$, щоб виконувалася рівність, тобто отримана умова буде виконуватися для кожного y.

Оскільки $S_{\otimes,b}$ — сюр'єктивне та ін'єктивне відображення, одержуємо, що $S_{\otimes,b}$ — бієкція. □

Лема 2.2. *Якщо* $\operatorname{ord} b = 2$*, тоді* $S_{\otimes,b}$ *— інволютивне відображення:*

$$\forall x \in V_n \colon S_{\otimes,b}(S_{\otimes,b}(x)) = x.$$

Доведення. Потрібно показати, що $\forall x \in V_n$ виконується наступна рівність $S_{\otimes,b}(S_{\otimes,b}(x)) = x$. Розпишемо дану рівність, використавши властивість бієктивного відображення, що $\forall x \in V_n : S(S^{-1}(x)) = x$.

$$S_{\otimes,b}(S_{\otimes,b}(x)) = S^{-1}(\underbrace{S(S^{-1}(S(x) \otimes b))}_{S(x)\otimes b} \otimes b) = S^{-1}(S(x) \otimes b \otimes b).$$

Оскільки порядок елемента групи b рівний 2, тоді $b \otimes b = e$, а перетворення набуває такого вигляду:

$$S^{-1}(S(x) \otimes e) = S^{-1}(S(x)) = x.$$

Тобто отримали те, що потрібно було довести. □

Наслідок 2.1. *Для усіх* $b \in V_n \backslash \{0^n\}$ *відображення* $S_{\oplus,b}(x)$ *є інволютивним без нерухомих точок.*

Лема 2.3. *Для довільних $b_1 \neq b_2$ справедливо:*

$$\forall x \in V_n \colon S_{\otimes,b_1}(x) \neq S_{\otimes,b_2}(x).$$

Доведення. Проведемо доведення від супротивного. Нехай $\exists x \in V_n : S_{b_1}(x) = S_{b_2}(x)$. Розпишемо дану рівність

$$S^{-1}(S(x) \otimes b_1) = S^{-1}(S(x) \otimes b_1).$$

Застосуємо до лівої та правої частини рівності відображення S і властивість бієктивності $\forall x \in V_n : S(S^{-1}(x)) = x$.

$$S(x) \otimes b_1 = S(x) \otimes b_2 \Rightarrow S(x) \otimes (S(x))^{-1} \otimes b_1 = b_2 \Rightarrow b_1 = b_2.$$

Отримали суперечність з умовою, що $b_1 \neq b_2$.

□

Лема 2.4. *Якщо e — нейтральний елемент абелевої групи $\langle V_n, \otimes \rangle$, то $S_{\otimes,e}(x) \equiv x$. Якщо $b \neq e$, то бумерангове перетворення $S_{\otimes,e}(x)$ не має нерухомих точок, тобто*

$$\forall b \neq e \forall x \in V_n \colon S_{\otimes,b}(x) \neq x.$$

Доведення. Для початку розглянемо випадок, коли $b = e$. Розпишемо бумерангове перетворення з параметром e за операцією $\otimes$

$$\forall x \in V_n : S_{\otimes,e}(x) = S^{-1}(S(x) \otimes e).$$

Оскільки e — нейтральний елемент, тоді $S(x) \otimes e = S(x)$. Також відомо, що для бієктивного відображення S виконується властивість: $\forall x \in V_n : S^{-1}(S(x)) = x$. Тоді бумерангове перетворення буде набувати такого вигляду:

$$\forall x \in V_n : S_{\otimes,e}(x) = x.$$

Перейдемо до розгляду випадку, коли $b \neq e$. Проведемо доведення

від супротивного. Нехай

$$\exists b \neq e \exists x \in V_n \colon S_{\otimes,b}(x) = x.$$

Розпишемо бумерангове перетворення $S_{\otimes,b}(x)$:

$$S^{-1}(S(x) \otimes b) = x.$$

Застосуємо до обох частин рівності відображення S та отримаємо:

$$S(x) \otimes b = S(x).$$

Додамо до лівої та правої частини $(S(x))^{-1}$ та отримаємо $b = e$, що суперечить заданій умові. □

Лема 2.5. *Якщо $S(x)$ — лінійне відображення, то $S_{\otimes,,b}(x)$ належить класу афінних відображень.*

Доведення. Оскільки S - лінійне відображення, тоді S^{-1} також лінійне відображення. Застосуємо до бумерангового перетворення таку властивість лінійності відображення, що для $\forall x,y \in V_n : S(x \otimes y) = = S(x) \otimes S(y)$.

$$S_{\otimes,b}(x) = S^{-1}(S(x) \otimes b) = S^{-1}(S(x)) \otimes S^{-1}(b) = x \otimes S^{-1}(b).$$

□

Розглянемо бумерангове перетворення відносно операції модульного додавання. Структура підстановки $S_{+,b}$ описується такою лемою.

Лема 2.6. *Якщо* $\operatorname{ord} b = 2^k$, $1 \leqslant k \leqslant n$, *тоді $S_{+,b}(x)$ містить рівно 2^{n-k} циклів довжини 2^k.*

Доведення. Оскільки $\langle V_n, + \rangle$ — циклічна група, тоді за теоремою про властивість циклічних груп існує єдина циклічна підгрупа порядку 2^k. З умови нам відомо, що $\operatorname{ord} b = 2^k$, тоді b є генератором даної підгрупи. Позначимо $H = \langle b \rangle$; за теоремою Лагранжа кількість різних

класів суміжності, породжених підгрупою H, обчислюється як $[V_n\colon H] = \frac{|V_n|}{|H|} = 2^{n-k}$. Усі ці класи суміжності попарно не перетинаються та замкнені відносно додавання до кожного з них елемента b.

Покажемо замкненість відносно додавання елемента b. Для елементу $g \in V_n$ його клас суміжності за підгрупою H описується як

$$g + H = \{g + h : h \in H\} = \{g, g + b, g + 2b, \ldots, g + (2^k - 1)b\}.$$

З асоціативності операції додавання за модулем і замкненості циклічної групи H випливає, що додавання b до будь-якого елемента класу суміжності дає елемент з цього ж класу.

Задамо деяке розбиття множини бітових векторів довжини n: $V_n = V_n^1 \sqcup V_n^2 \sqcup \cdots \sqcup V_n^{2^{n-k}}$, де $|V_n^i| = 2^k$, тоді S можна представити як сукупність 2^{n-k} відображень $S_i\colon V_n^i \to K_i$, де $i = \overline{1, 2^{n-k}}$ і множини K_i — усі класи суміжності відносно H. Оскільки класи суміжності є замкненими відносно додавання b, то $\forall x \in V_n^i\colon S(x) + b \in K_i$. Відповідно, відображення $S_{+,b}^i$ буде діяти як $V_n^i \to V_n^i$ і замкнене на цих множинах. З леми 2.1 та леми 2.4 маємо, що таке відображення є бієктивним і не має нерухомих точок, тому воно фактично є циклом довжини 2^k. Отже, усі 2^{n-k} відображень $S_{+,b}^i$ є циклами довжини 2^k, що доводить твердження леми. □

2.2 Бумерангова еквівалентність відносно операції побітового додавання

Введемо поняття бумерангової еквівалентності.

Означення 2.2. S-блоки $S, F\colon V_n \to V_n$ вважаються *бумерангово еквівалентними за операцією* $\otimes$ *та вектором* $b \in V_n$, якщо $\forall x \in V_n : S_{\otimes,b}(x) = F_{\otimes,b}(x)$.

Означення 2.3. *Класом бумерангової еквівалентності* $[S]$

відображення $S \in \Pi^{(n)}$ відносно операції $\otimes$ є множина:

$$[S] = \{F \in \Pi^{(n)} : \forall x \in V_n, S_{\otimes,b}(x) = F_{\otimes,b}(x)\}.$$

Для початку розглянемо, якого вигляду може набувати бумерангове перетворення S-блоку відносно заданої операції з фіксованим значенням b. Якщо розглянути абелеву групу $\langle V_n, \oplus\rangle$, то усі елементи, окрім нейтрального, будуть мати порядок, який дорівнює 2. Тоді з леми 2.4 та леми 2.2 випливає, що дане перетворення є інволютивним без нерухомих точок. Розіб'ємо множину входів на дві рівнопотужні підмножини $V_n = X \sqcup Y$, де $X = \{x_1,x_2,\ldots,x_{2^{n-1}}\}$, $Y = \{y_1,y_2,\ldots,y_{2^{n-1}}\}$ та

$$S_{\oplus,b}(X) = Y, \qquad S_{\oplus,b}(Y) = X.$$

Відповідно, без обмеження загальності, $S_{\oplus,b}$ можна описати як підстановку у такий спосіб:

$$S_{\oplus,b} = \begin{pmatrix} x_1 & x_2 & \ldots & x_{2^{n-1}} & y_1 & y_2 & \ldots & y_{2^{n-1}} \\ \\ y_1 & y_2 & \ldots & y_{2^{n-1}} & x_1 & x_2 & \ldots & x_{2^{n-1}} \end{pmatrix}.$$

Детальніше розглянемо бумерангове перетворення на підмножині входів X. Для $i = \overline{1, 2^{n-1}}$ маємо

$$S_{\oplus,b}(x_i) = y_i \Rightarrow S(x_i) \oplus b = S(y_i) \Rightarrow S(x_i) \oplus S(y_i) = b.$$

Отримане співвідношення можна записати як систему рівнянь

$$\begin{cases} S(x_1) \oplus S(y_1) = b \\ S(x_2) \oplus S(y_2) = b \\ \vdots \\ S(x_{2^{n-1}}) \oplus S(y_{2^{n-1}}) = b \end{cases} \tag{2.1}$$

Усі розв'язки заданої системи будуть утворювати клас бумерангової

еквівалентності, що породжує задане $S_{\oplus,b}$. Потужність такого класу еквівалентності визначається так: оберемо пару значень $(t_1,t_2) \in V_n^2$ таких, що $t_1 \oplus t_2 = b$. Оскільки розглядається, що S — бієктивне відображення, тоді цю пару або симетричну їй можна підставити лише в одне з 2^{n-1} рівнянь. Таких симетричних пар існує 2^{n-1}, і дані пари будуть утворювати різні розв'язки, тому множина розв'язків складається з перестановки пар описаного виду та обиранням однієї пари з двох. Таким чином, потужність будь-якого класу бумерангової еквівалентності буде визначатися як

$$|[S]| = 2^{2^{n-1}} \cdot (2^{n-1})!.$$

Оскільки S-блоки розглядаються як n-бітні бієктивні відображення, тоді розділивши потужність таких відображень на потужність класу бумерангової еквівалентності буде отримана загальна кількість таких класів, що описують усі образи бумерангового перетворення:

$$|S/\sim| = \frac{2^n!}{2^{2^{n-1}} \cdot (2^{n-1})!}.$$

Як відомо, наведене значення дорівнює кількості інволютивних відображень без нерухомих точок на множині з 2^n елементів. Звідси випливає, що будь-яка інволюція без нерухомих точок є образом бумерангового перетворення відносно операції побітового додавання для цілого класу S-блоків.

2.3 Бумерангова еквівалентність відносно операції додавання за модулем 2^n

Розглянемо бумерангове перетворення S-блоків відносно операції додавання за модулем 2^n. Будемо вважати, що $\operatorname{ord} b = 2^k$, де $1 \leqslant k \leqslant n$. З леми 2.6 відомо, що у такому випадку відображення $S_{+,b}$ розпадається на цикли довжини 2^k, тому бумерангове перетворення S-блоку можна задати

як 2^{n-k} різних відображень.

Розіб'ємо множину входів $V_n = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_{2^{n-k}}$, де $X_i = \{x_0^{(i)}, x_1^{(i)}, \ldots, x_{2^k-1}^{(i)}\}$. Тоді, як і в попередньому розділі, без обмеження загальності, можна описати $S_{+,b}$ як сукупність підстановок виду

$$S_{+,b}^i = \begin{pmatrix} x_0^{(i)} & x_1^{(i)} & \ldots & x_{2^k-2}^{(i)} & x_{2^k-1}^{(i)} \\ x_1^{(i)} & x_2^{(i)} & \ldots & x_{2^k-1}^{(i)} & x_0^{(i)} \end{pmatrix}.$$

Розпишемо детальніше задане $S_{+,b}$ перетворення; для $i = \overline{1, 2^{n-k}}$, $j = \overline{0, 2^k - 1}$ маємо

$$S_{+,b}^i \left(x_j^{(i)} \right) = x_{(j+1) \bmod 2^k}^{(i)}.$$

Повторюючи дії, аналогічні випадку побітового додавання, одержуємо такі співвідношення для довільних i, j:

$$S\left(x_{(j+1) \bmod 2^k}^{(i)} \right) - S\left(x_j^{(i)} \right) = b.$$

Наведені співвідношення можна розглядати як сукупність з 2^{n-k} систем, кожна з яких має 2^k рівнянь:

$$\begin{cases} S(x_1^{(i)}) - S(x_0^{(i)}) = b \\ S(x_2^{(i)}) - S(x_1^{(i)}) = b \\ \vdots \\ S(x_{2^k-1}^{(i)}) - S(x_{2^k-2}^{(i)}) = b \\ S(x_0^{(i)}) - S(x_{2^k-1}^{(i)}) = b \end{cases}$$

Дані рівняння є лінійними відносно $+$, тому наведену систему можна

записати у матричному вигляді; матрицею цієї системи буде

$$A = \begin{pmatrix} -1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & -1 \end{pmatrix}$$

Як можна побачити, сума перших $2^k - 1$ рядків матриці дорівнює останньому рядку зі зміною знаку, тому систему можна переписати, прибравши останнє рівняння:

$$\begin{cases} S(x_1^{(i)}) - S(x_0^{(i)}) = b \\ S(x_2^{(i)}) - S(x_1^{(i)}) = b \\ \vdots \\ S(x_{2^k-1}^{(i)}) - S(x_{2^k-2}^{(i)}) = b \end{cases}$$

Якщо одне зі значень системи зафіксувати, тоді дана система матиме єдиний розв'язок. Усього значень, що можна зафіксувати, існує 2^n, тобто кількість розв'язків підсистеми залежить від кількості можливих значень для фіксування. Враховуючи те, що S — бієктивне відображення, то отримані розв'язки підсистеми не можна використовувати для фіксування в іншій підсистемі, тому наступна підсистема матиме на 2^k менше значень і так кількість можливих значень буде зменшуватися для кожної наступної підсистеми. Оскільки дані розв'язки описують клас бумерангової еквівалентності, тому потужність

такого класу дорівнює

$$|[S]| = \prod_{i=0}^{2^{n-k}-1} (2^n - i \cdot 2^k) = 2^{k \cdot 2^{n-k}} \cdot (2^{n-k})!.$$

У випадку $\operatorname{ord} b = 2$ можна засвідчитися, що потужність класу бумерангової еквівалентності буде збігатися з потужністю класу еквівалентності відносно операції $\oplus$, оскільки в такому випадку класи еквівалентності будуть описувати інволютивні перестановки без нерухомих точок.

Також розділивши потужність n-бітових бієктивних відображень на потужність класу еквівалентності, отримаємо значення, що описує кількість відображень, які мають 2^{n-k} циклів довжини 2^k, а саме

$$|S/\sim| = \frac{2^n!}{2^{k \cdot 2^{n-k}} \cdot (2^{n-k})!}.$$

Відповідно, як і у випадку побітового додавання, будь-яке перетворення такої циклової структури є образом бумерангового перетворення відносно модульного додавання для цілого класу S-блоків.

2.4 Алгоритм відновлення класу S-блоків з точністю до еквівалентності та алгоритм генерування випадкової інволютивної перестановки без нерухомих точок

Опишемо алгоритм, що буде відновлювати клас S-блоків з точністю до еквівалентності. Такий алгоритм можна розбити на два під алгоритми: розв'язування підсистеми при певному фіксованому значенні та рекурсивний перебір можливих значень для фіксування підсистем. З леми 2.6 маємо, що $S_{+,b}$ можна представити у вигляді набору підстановок з циклом довжини 2^k. Тоді на вхід алгоритму можна подати $S_{+,b}$ як

матрицю циклів :

$$S_{+,b} = \begin{pmatrix} x_0^1 & x_1^1 & \dots & x_{2^k-1}^1 \\ x_0^2 & x_1^2 & \dots & x_{2^k-1}^2 \\ \vdots & \vdots & \dots & \vdots \\ x_0^{2^{n-k}} & x_1^{2^{n-k}} & \dots & x_{2^k-1}^{2^{n-k}} \end{pmatrix}$$

Для початку опишемо алгоритм розв'язання підсистеми, який зображений на рис. 2.1. Кожне рівняння зв'язане таким чином:

$$i = \overline{0,2^{n-k}-1} : S(x_i^{(j)}) - S(x_{i-1}^{(j)}) = b.$$

Як можна побачити значення $S(x_i^{(j)})$ залежить від попереднього. Якщо для початкового фіксування обрати значення $S(x_0^{(j)})$, тоді вираз можна переписати як:

$$i = \overline{1,2^{n-k}-1} : S(x_i^{(j)}) = S(x_{i-1}^{(j)}) + b.$$

Алгоритм має приймати на вхід: цикл бумерангового перетворення, S-блок, що відновлюється, значення, що залишилися для фіксування, щоб на кожному кроці викреслювати вже використані елементи при розв'язанні підсистеми та параметр бумерангового перетворення. На виході алгоритм повертає частково відновлений S-блок та значення для фіксування в наступних підсистемах.

Загальний алгоритм відновлення, зображений на рис. 2.2, є рекурсивним. На кожному рівні рекурсії потрібно перебирати можливі значення для фіксування в залежності від обраних значень у попередніх викликах. Тому для кожного нового виклику потрібно створювати новий список значень для фіксування без 2^k значень, що були використані на даному рівні. Рекурсія завершиться після перебору останнього циклу $S_{+,b}$. Також для спрощення запису на усіх рівнях рекурсії список для

Алгоритм 2.1 subSystem

Вхід: $x = \{x_0, x_1, \ldots, x_{2^k}\}$, $recoveryS$, $index$, b
Вихід: $recoveryS$, $index$
1: **for** $i = 1$ **to** $2^{n-k} - 1$ **do**
2: $\quad recoveryS[s[i]] \leftarrow b + recoveryS[s[i-1]]$
3: $\quad index \leftarrow index \backslash \{b + recoveryS[s[i-1]]\}$
4: **end for**
5: **return** $recoveryS$, $index$

Рисунок 2.1 – Алгоритм розв'язання підсистеми при фіксованому значенні

накопичення відновлених S-блоків вважається доступним і не потребує копіювання.

Алгоритм 2.2 Recovery

Вхід: $class = \varnothing$, $S_{+,b}$, $j = 0$, $index = \{0,1,\ldots 2^n - 1\}$, $recoveryS = \{0,0,\ldots,0\}$, b
Вихід: $class$
1: **if** $j = 2^{n-k}$ **then**
2: $\quad class \leftarrow class \cup \{recoveryS\}$
3: $\quad$ **return**
4: **end if**
5: $s \leftarrow S_b[j]$
6: **for** each i **in** $index$ **do**
7: $\quad recoveryS[s[0]] \leftarrow i$
8: $\quad index_{copy} \leftarrow index \backslash \{i\}$
9: $\quad index_{copy} \leftarrow subSystem(s, recoveryS, index_{copy}, b)$
10: $\quad Recovery(class, S_{b,+}, j+1, index_{copy}, recoveryS, b)$
11: **end for**

Рисунок 2.2 – Алгоритм відновлення класу S-блоків з точністю до еквівалентності

Даний алгоритм також застосовний до операції побітового додавання. Для цього потрібно в алгоритм розв'язання підсистеми замінити операцію додавання за модулем 2^n на операцію побітового додавання та на вхід $S_{\oplus,b}$ буде подаватися, як матриця циклів довжини 2.

Оскільки такий алгоритм — рекурсивний, то його часову та

просторову складність можна описати, як такі рекурентні співвідношення:

$$T(2^n) = 2^n \cdot T(2^n - 2^k) + 2^k;$$
$$S(2^n) = 2^n \cdot S(2^n - 2^k) + 2^n;$$
$$T(0) = S(0) = 0.$$

Лема 2.7. *Розв'язком рекуренти часової складності є така сума:*

$$T(2^n) = 2^k \sum_{i=0}^{2^{n-k}-1} (2^k)^i \cdot (2^{n-k})^{\underline{i}}.$$

Доведення. Розглянемо дерево рекурсії на рис 2.3. Корінь дерева має вартість 2^k і він має 2^n нащадків, кожен з них має таку ж вартість. Кожен з нащадків буде мати на 2^k менше нащадківч від кількості батьківської вершини. Тоді кількість вершин на певному рівні визначається, як добуток кількості усіх попередніх рівнів. Просумувавши по усім рівнях дерева отримаємо, що часова складність визначається як:

$$T(2^n) = \sum_{i=0}^{2^{n-k}-1} 2^k \cdot \prod_{j=0}^{i} (2^n - j \cdot 2^k) = 2^k \sum_{i=0}^{2^{n-k}-1} 2^{ik} \cdot (2^{n-k})^{\underline{i}}.$$

Доведемо отримане значення $T(2^n)$ методом математичної індукції. Для зручності введемо такі заміни: $a = 2^k, b = 2^n$. Тоді рекуренту запишемо як:

$$T(b) = b \cdot T(b-a) + a = a \sum_{i=0}^{b/a-1} a^i \cdot (a/b)^{\underline{i}}.$$

База математичної індукції $b = a$:

$$T(a) = a \cdot T(a-a) + a = a,$$
$$T(a) = a \sum_{i=0}^{0} a^i \cdot (b/a)^{\underline{i}} = a.$$

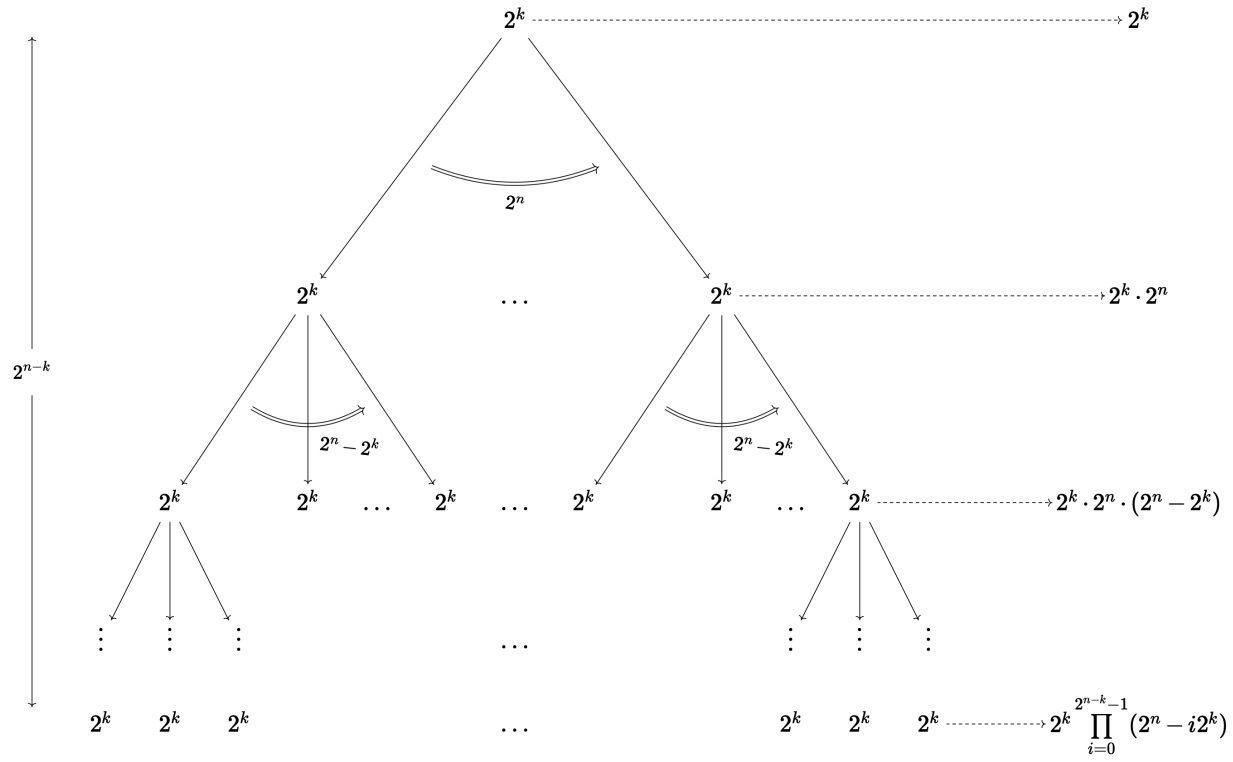

Рисунок 2.3 – Дерево рекурсії $T(2^n)$

Крок математичної індукції $b = b + a$:

$$T(a+b) = (a+b) \cdot T(b) + a = a \cdot (a+b) \sum_{i=0}^{b/a-1} a^i \cdot (b/a)^{\underline{i}} + a.$$

Потрібно показати, що таке значення буде зводитися до

$$T(a+b) = a \sum_{i=0}^{b/a} a^i \cdot (b/a+1)^{\underline{i}}.$$

Прирівняємо ці два значення:

$$a \sum_{i=0}^{b/a} a^i \cdot (b/a+1)^{\underline{i}} = a \cdot (a+b) \sum_{i=0}^{b/a-1} a^i \cdot (b/a)^{\underline{i}} + a.$$

Зведемо ліву частину до вигляду правої.

$$a\sum_{i=0}^{b/a} a^i \cdot (b/a+1)^{\underline{i}} = a + a\sum_{i=1}^{b/a} a^i \cdot (b/a+1)^{\underline{i}} = a + a \cdot (b/a+1)\sum_{i=1}^{b/a} a^i \cdot (b/a)^{\underline{i-1}} =$$
$$= (a+b)\sum_{i=0}^{b/a-1} a^{i+1} \cdot (b/a)^{\underline{i}} = a + a \cdot (a+b)\sum_{i=0}^{b/a-1} a^i (b/a)^{\underline{i}} + a.$$

Тобто отримали те, що потрібно було показати. □

Лема 2.8. *Розв'язком рекуренти просторової складності є така сума:*

$$S(2^n) = \sum_{i=0}^{2^{n-k}-1} 2^{ki} \cdot (2^n - i \cdot 2^k) \cdot (2^{n-k})^{\underline{i}}.$$

Доведення. Розглянемо дерево рекурсії на рис 2.4. Корінь дерева має вартість 2^n і він має 2^n нащадків, кожен з них має вартість на 2^k меншу. Кількість вершин на кожному рівні визначається аналогічно як і у випадку часової складності, але вартість вершин в даному випадку не стала і зменшується на 2^k від попереднього рівня. Просумувавши по усім рівнях дерева отримаємо, що просторова складність визначається як:

$$S(2^n) = \sum_{i=0}^{2^{n-k}-1} (2^n - i \cdot 2^k) \prod_{j=0}^{i} (2^n - j \cdot 2^k) = \sum_{i=0}^{2^{n-k}-1} 2^{ik} \cdot (2^n - i \cdot 2^k) \cdot (2^{n-k})^{\underline{i}}.$$

Доведемо отримане значення $S(2^n)$ методом математичної індукції. Для зручності введемо такі заміни: $a = 2^k, b = 2^n$. Тоді рекуренту запишемо як:

$$S(b) = b \cdot S(b-a) + b = \sum_{i=0}^{b/a-1} (b - i \cdot a) \cdot a^i \cdot (b/a)^{\underline{i}}.$$

База математичної індукції $b = a$:

$$S(a) = a \cdot S(a-a) + a = a,$$
$$S(a) = \sum_{i=0}^{0} (a - i \cdot a) a^i (1)^{\underline{i}} = a.$$

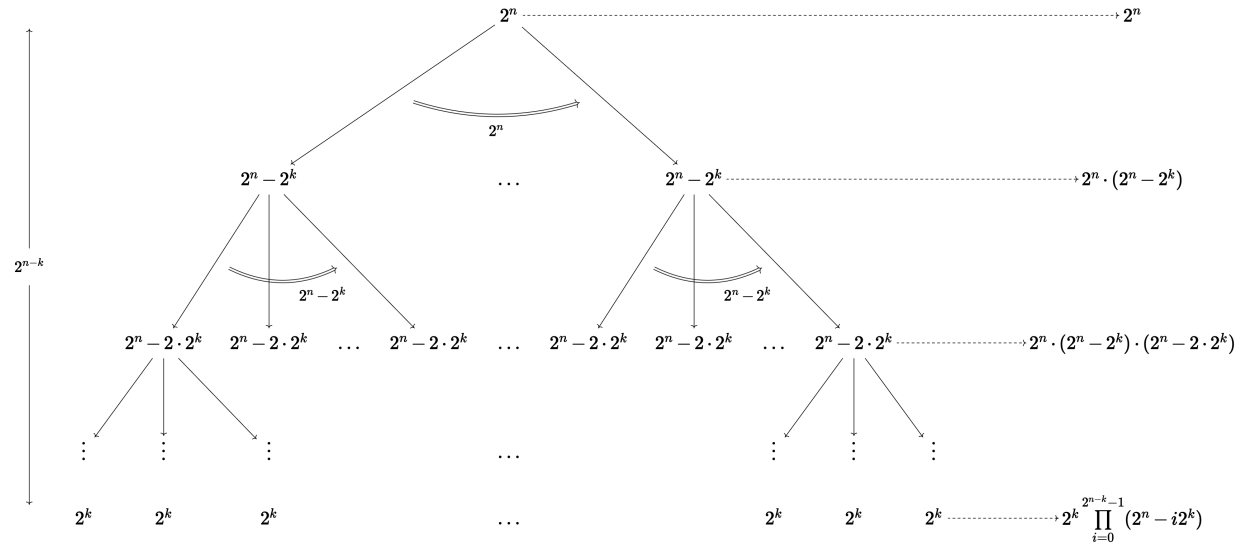

Рисунок 2.4 – Дерево рекурсії $S(2^n)$

Крок математичної індукції $b = b + a$:

$$S(b + a) = (b + a) \cdot S(b) + (b + a).$$

Потрібно показати, що таке значення буде дорівнювати

$$(b + a)S(b) + (b + a) = \sum_{i=0}^{b/a} (b + a - i \cdot a) \cdot a^i \cdot (b/a)^{\underline{i}}.$$

Покажемо, що праву частину можна звести до лівої:

$$\sum_{i=0}^{b/a} (b + a - i \cdot a) \cdot a^i \cdot (b/a)^{\underline{i}} = (b + a) + \sum_{i=1}^{b/a} a^i \cdot (b + a - i \cdot a) \cdot (b/a + 1)^{\underline{i}} =$$

$$= (a + b) + \frac{b + a}{a} \sum_{i=1}^{b/a} (b + a - i \cdot a) \cdot a^i (b/a)^{\underline{i-1}} =$$

$$= (a + b) + \frac{b + a}{a} \sum_{i=0}^{b/a-1} (b + a - i \cdot a - a) \cdot a^{i+1} \cdot (b/a)^{\underline{i}} =$$

$$= (a + b) + (a + b) \sum_{i=0}^{b/a-1} (b - i \cdot a) \cdot a^i \cdot (b/a)^i = (a + b) \cdot S(b) + (a + b).$$

□

Розглянемо, яку асимптотичну оцінку матимуть рекуренти часової та просторової складності.

Лема 2.9. *Асимптотична оцінка часової складності визначається як:*

$$T(2^n) = O(2^k \cdot 2^{n\cdot(2^{n-k}+1)}).$$

Доведення. З леми 2.7 маємо, що часова складність описується такою сумою:

$$T(2^n) = 2^k \sum_{i=0}^{2^{n-k}-1} (2^k)^i \cdot (2^{n-k})^{\underline{i}}.$$

Спадний факторіал можна обмежити зверху значенням $(2^{n-k})^i$. Тоді суму можна переписати як:

$$T(2^n) = 2^k \sum_{i=0}^{2^{n-k}-1} (2^k)^i \cdot (2^{n-k})^i = 2^k \sum_{i=0}^{2^{n-k}-1} (2^n)^i = 2^k \frac{2^{n\cdot 2^{n-k}} - 1}{2^n - 1}.$$

Розглянемо детальніше отримане значення:

$$\lim_{n\to\infty} \frac{2^{n\cdot 2^{n-k}} - 1}{(2^n - 1)(2^{n\cdot(2^{n-k}+1)} - 2^n)} = \lim_{n\to\infty} \frac{2^n(2^{n\cdot 2^{n-k}} - 1)}{(1 - \frac{1}{2^n})(2^{n\cdot(2^{n-k}+1)} - 2^n)} = \lim_{n\to\infty} \frac{1}{1 - \frac{1}{2^n}} = 1.$$

Значення $\frac{2^{n\cdot 2^{n-k}}-1}{2^n-1}$ еквівалентне $2^{n\cdot(2^{n-k}+1)} - 2^n$. Тоді $T(2^n) = O(2^k \cdot 2^{n\cdot(2^{n-k}+1)})$. □

Лема 2.10. *Асимптотична оцінка просторової складності визначається як:*

$$S(2^n) = O(2^k \cdot 2^{n\cdot(2^{n-k}+3)}).$$

Доведення. З леми 2.8 маємо, що просторова складність описується такою сумою:

$$S(2^n) = \sum_{i=0}^{2^{n-k}-1} 2^{ki} \cdot (2^n - i \cdot 2^k) \cdot (2^{n-k})^{\underline{i}}.$$

Скористаємося обмеженням спадного факторіала з доведення леми 2.9.

Тоді сума набуватиме такого виду:

$$S(2^n) = \sum_{i=0}^{2^{n-k}-1} (2^n)^i \cdot (2^n - i \cdot 2^k) = 2^n \sum_{i=0}^{2^{n-k}-1} (2^n)^i - 2^k \sum_{i=0}^{2^{n-k}-1} i \cdot (2^n)^i =$$
$$= \frac{2^n(2^{n\cdot 2^{n-k}} - 1)}{2^n - 1} - \frac{2^n(2^k + 2^{n\cdot(2^{n-k}+1)} - 2^{n\cdot 2^{n-k}+k} - 2^{n\cdot 2^{n-k}})}{(2^n-1)^2}$$
$$= \frac{2^n((2^n-1)(2^{n\cdot 2^{n-k}} - 1) - 2^k - 2^{n\cdot(2^{n-k}+1)} + 2^{n\cdot 2^{n-k}+k} + 2^{n\cdot 2^{n-k}})}{(2^n-1)^2}$$
$$= \frac{2^n(2^{n\cdot(2^{n-k}+1)} - 2^n - 2^{n\cdot 2^{n-k}} + 1 - 2^k - 2^{n\cdot(2^{n-k}+1)} + 2^{n\cdot 2^{n-k}+k} + 2^{n\cdot 2^{n-k}})}{(2^n-1)^2}$$
$$= \frac{2^n(1 - 2^k - 2^n + 2^{n\cdot 2^{n-k}+k})}{(2^n-1)^2}.$$

Отримане значення аналогічно доведенню леми 2.9 буде еквівалентне значенню:

$$2^{4n}(2^k \cdot 2^{n\cdot(2^{n-k}-1)} - 1).$$

Тоді $S(2^n) = O(2^k \cdot 2^{n\cdot(2^{n-k}+3)})$.

□

Перейдемо до алгоритму генерування випадкових інволютивних перестановок без нерухомих точок. Для опису даного алгоритму було використано результати розділу 2.2, де описано структуру розбиття S-блоків на класи еквівалентності за операцією $\oplus$ та параметром b. Зокрема було показано, що образами перетворень є інволютивні відображення без нерухомих точок. Тоді генерування випадкових інволютивних перестановок без нерухомих точок може базуватися на генерації випадкової перестановки та застосування бумерангового перетворення з операцією $\oplus$ та деяким фіксованим значенням $b \neq 0$. Оскільки алгоритм працює для будь-якого ненульового b, оберемо найпростіше значення $b = 1$. Також з леми 2.6 маємо, що взявши в якості параметра бумерангового перетворення значення $b = 2^{n-1}$, що має $\mathrm{ord}_+ b = 2$, тоді алгоритм буде працювати з операцією додавання за модулем 2^n. Для генерування випадкової перестановки можна обрати

алгоритм Фішера-Йетса [7]. Алгоритм генерування зображено на рис 2.5.

Алгоритм 2.3 generateInvolutions

Вхід: n
Вихід: $randomI$
1: $S \leftarrow Fisher - YatesAlgorithm(2^n)$
2: **for** each x **in** $\{0,1,\ldots,2^n-1\}$ **do**
3: $\quad randomI(x) \leftarrow S_{\oplus,1}(x)$
4: **end for**
5: **return** $randomI$

Рисунок 2.5 – Алгоритм генерування випадкової інволютивної перестановки без нерухомих точок

Наведемо лему, що доводить коректність даного алгоритму.

Лема 2.11. *Нехай S-блоки рівномірно розподілені над множиною V_n, тоді образи бумерангового перетворення при фіксованому параметрі будуть рівномірно розподіленими на множині усіх інволюцій над множиною V_n*

Доведення. З результатів, одержаних в розділі 2.2 маємо, що множина S-блоків розбивається на рівнопотужні класи бумерангової еквівалентності, що породжують інволютивні відображення без нерухомих точок. Тобто, розподіл бумерангового перетворення буде дорівнювати сумі ймовірностей S-блоків, що породжують дане перетворення. За умовою відомо, що S-блоки рівноймовірні, тому розподіл бумерангового перетворення можна записати, як:

$$\forall \pi \in \mathcal{I}^n : \Pr\{\forall x \in V_n \colon S_b(x) = \pi(x)\} = \sum_{i=1}^{|[S]|} \frac{1}{2^n!} = \frac{|[S]|}{2^n!} = \frac{2^{2^{n-1}} \cdot (2^{n-1})!}{2^n!}.$$

Як можна побачити, отриманий розподіл описуватиме рівномірність інволютивних перестановок без нерухомих точок. □

2.5 Розподіл диференціальних ймовірностей для інволютивних перестановок без нерухомих точок

З отриманих результатів в розділі 2.2 випливає, що розподіли диференціальних ймовірностей бумерангового перетворення за операцією побітового додавання може розглядатися з випадковим обиранням рівномірно розподіленої інволютивної перестановки без нерухомих точок. Для отримання такого розподілу можна узагальнити результати описані в розділі 1.2 для операції побітового додавання та інволютивних перестановок без нерухомих точок.

Позначимо множину ребер $E_\alpha^\oplus$ різницевого графа породженого різницею α для операції побітового додавання. Таку множину ребер можна подати, як невпорядковані пари з різницею α:

$$E_\alpha^\oplus = \{\{u,v\} : u,v \in V_n, u \oplus v = \alpha\}.$$

Тоді з теореми 1.1 розподіл набуватиме такого вигляду:

$$p_t(\#G,a,b) = \Pr(2^n \cdot DP_\oplus(\pi,\alpha,\beta) = t \mid \pi \in_R \mathcal{I}^{(n)}) = \frac{P_t}{|\mathcal{I}^{(n)}|}.$$

Як нам відомо P_t обчислюється за формулою включень та виключень:

$$P_t = \sum_{i=0}^{2^{n-1}-t} (-1)^i C_{t+i}^i S_{t+i}, \quad S_k = \sum_{\mathcal{Y} \subseteq E_\alpha^\oplus, |\mathcal{Y}|=k} \left| \bigcap_{uv \in \mathcal{Y}} A_{uv} \right|.$$

Представлення значення S_k доволі не інтуїтивне, тому множину $\bigcap_{uv\in\mathcal{Y}} A_{uv}$ можна представити, як множину інволютивних перестановок такого виду: $\{\pi | \pi(\mathcal{Y}) \subseteq E_\beta^\oplus\}$. Тоді S_k можна переписати, як:

$$S_k = \sum_{\mathcal{Y} \subseteq E_\alpha^\oplus, |\mathcal{Y}|=k} |\{\pi | \pi(\mathcal{Y}) \subseteq E_\beta^\oplus\}|.$$

Представимо множину ребер $E_\alpha^\oplus$ як:

$$E_\alpha^\oplus = \{\{x_1,y_1\},\{x_2,y_2\},\ldots,\{x_{2^{n-2}},y_{2^{n-2}}\},\{x_1\oplus\beta,y_1\oplus\beta\},$$
$$\{x_2\oplus\beta,y_2\oplus\beta\},\ldots,\{x_{2^{n-2}}\oplus\beta,y_{2^{n-2}}\oplus\beta\}\}.$$

Тоді $\mathcal{Y}\subseteq E_\alpha^\oplus$ можна представити, як розбиття на множини $\mathcal{Y}_1$, що містить t множин вигляду $\{x,y\},\{x\oplus\beta,y\oplus\beta\}$, та $\mathcal{Y}_2$, що складається з $k-2t$ множин виду $\{x,y\}$ або $\{x\oplus\beta,y\oplus\beta\}$.

$$\mathcal{Y}_1 = \{\{x_1,y_1\},\ldots,\{x_t,y_t\},\{x_1\oplus\beta,y_1\oplus\beta\},\ldots,\{x_t\oplus\beta,y_t\oplus\beta\}\};$$
$$\mathcal{Y}_2 = \{\{x_1^*,y_1^*\},\ldots,\{x_{k-2t}^*,y_{k-2t}^*\}\}.$$

Таке представлення обумовлене властивістю інволютивності перестановки π та правилами, які діють при заповненні значення переходу. Наведемо леми, що опишуть усі можливі випадки для інволютивних перестановок без нерухомих точок, що переводять ребра множини $\mathcal{Y}$ в множину ребер з різницею β.

Лема 2.12. *Нехай $\{x,y\}\in\mathcal{Y}$, тоді вершини x та y не можуть переходити у вершини $\{x,y,x\oplus b,y\oplus b\}$.*

Доведення. Неможливість $\pi(x)\neq x$ випливає з означення π. Тоді розглянемо випадок $\pi(x)=y$, тоді $\pi(y)$ має дорівнювати $y\oplus b$, а такого бути не може, оскільки π інволютивне відображення. Для $\pi(y)=x$ аналогічно. □

Лема 2.13. *Нехай $\{x_1,y_1\},\{x_2,y_2\}\in\mathcal{Y}_1$, якщо $\pi(x_1)=x_2$, тоді ребра $\{x_2,y_2\},\{x_2\oplus\beta,y_2\oplus\beta\},\{x_1\oplus\beta,y_1\oplus\beta\}$ мають єдиний спосіб співставленням з ребрами, що мають різницю β:*

$$\begin{pmatrix} x_1 & y_1 & x_2 & y_2 & x_1\oplus b & y_1\oplus b & x_2\oplus b & y_2\oplus b \\ x_2 & x_2\oplus\beta & x_1 & x_1\oplus\beta & y_2 & y_2\oplus b & y_1 & y_1\oplus b \end{pmatrix}$$

Доведення. За умовою відомо, що $\pi(x_1)=x_2$, тоді $\pi(y_1)$ має

дорівнювати $x_2 \oplus \beta$.

$$\pi(x_1) = x_2 \qquad \pi(x_2) = x_1$$
$$\pi(y_1) = x_2 \oplus \beta \qquad \pi(x_2 \oplus \beta) = y_1$$

Тепер потрібно заповнити ребра $\{x_2,y_2\}$, $\{x_1 \oplus \beta, y_2 \oplus \beta\}$ та $\{x_2 \oplus \beta, y_2 \oplus \beta\}$ так, щоб вони переходили в ребро з різницею β. Розглянемо для початку ребро $\{x_2,y_2\}$. Відомо, що $\pi(x_2) = x_1$, тоді $\pi(y_2) = x_1 \oplus \beta$.

$$\pi(x_2) = x_1$$
$$\pi(y_2) = x_1 \oplus \beta \qquad \pi(x_1 \oplus \beta) = y_2$$

Можна побачити, що заповнюється значення для $\pi(x_1 \oplus \alpha \oplus \beta) = \pi(y_1 \oplus \beta) = y_2 \oplus \beta$. Тоді за інволютивністю $\pi(y_2 \oplus \beta) = y_1 \oplus \beta$ та $\pi(x_2 \oplus \beta) = y_1 \oplus \beta \oplus \beta = y_1$. Тобто вдалося показати, що заповнення одного значення x_1 буде визначати переходи інших 3 ребер.

□

Лема 2.14. *Нехай* $\{x_1^*,y_2^*\},\{x_2^*,y_2^*\} \in \mathcal{Y}_2$*, якщо* $\pi(x_1^*) = x_2^*$ *тоді існує єдиний спосіб співставити співставити ребро* $\{x_2^*, y_2^*\}$ *з ребром з різницею* β*:*

$$\begin{pmatrix} x_1^* & y_1^* & x_2^* & y_2^* & x_1^* \oplus \beta & x_2^* \oplus \beta \\ x_2^* & x_2^* \oplus \beta & x_1^* & x_1^* \oplus \beta & y_2^* & y_1^* \end{pmatrix}$$

Доведення. За умовою відомо, що $\pi(x_1^*) = x_2^*$, тоді $\pi(y_1^*)$ має дорівнювати $x_2^* \oplus \beta$.

$$\pi(x_1^*) = x_2^* \qquad \pi(x_2^*) = x_1^*$$
$$\pi(y_1^*) = x_2^* \oplus \beta \qquad \pi(x_2^* \oplus \beta) = y_1^*$$

Як можна побачити, що $\pi(x_2^*) = x_1^*$, тоді $\pi(y_2^*) = x_1^* \oplus \beta$. Оскільки множина $\mathcal{Y}_2$ обиралася таким чином, щоб вершини $x_1^* \oplus \beta$, $x_2^* \oplus \beta$ не

повинні переходити в ребра з різницею β, тому вони будуть заповнені значеннями y_1^* та y_2^*, а значення $y_1^* \oplus \beta$, $y_2^* \oplus \beta$ будуть заповнені довільним чином із збереженням умов перестановки π. □

Лема 2.15. *Нехай* $\{x,y\} \in \mathcal{Y}_1$ *та* $\{x^*,y^*\} \in \mathcal{Y}_2$, *якщо* $\pi(x) = y^*$, *тоді існує єдиний спосіб співставити ребра* $\{x \oplus \beta, y \oplus \beta, x^*, y^*\}$ *з ребрами, що мають різницю* β*:*

$$\begin{pmatrix} x & y & x^* & y^* & x \oplus b & y \oplus b & x^* \oplus b & y^* \oplus b \\ x^* & x^* \oplus \beta & x & x \oplus \beta & y^* & y_m^* \oplus b & y & y \oplus b \end{pmatrix}$$

Лема 2.16. *Нехай* $\{x_1,y_1\},\{x_1 \oplus \beta,y_1 \oplus \beta\} \in \mathcal{Y}_1$ *та* $\pi(x_1) = t_1$, *де вершини* t_1 *та* $t_1 \oplus \beta$ *не фігурують в множині ребер* $\mathcal{Y}$. *Тоді* $x_1 \oplus \beta$ *має такі ж обмеження для переходу в вершину, що міститься в ребрі різниці* β*:*

$$\begin{pmatrix} x_1 & y_1 & x_1 \oplus \beta & y_1 \oplus \beta & t_1 & t_1 \oplus \beta & t_2 & t_2 \oplus \beta \\ t_1 & t_1 \oplus \beta & t_2 & t_2 \oplus \beta & x_1 & y_1 & x_1 \oplus \beta & y_1 \oplus \beta \end{pmatrix}$$

Доведення. Якщо $\pi(x_2 \oplus \beta)$ буде переходити в вершини, що містять в $\mathcal{Y}$, то тоді це буде зводитися до випадків леми 2.13 або леми 2.15. Якщо $\{x^*,y^*\} \in \mathcal{Y}_2$, тоді значення $x^* \oplus \beta, y^* \oplus \beta$ немає в множині $\mathcal{Y}$, але якщо в них перевести тоді отримаємо також випадок з леми 2.15.

□

Теорема 2.1. *Значення* S_k *для інволютивних перестановок без нерухомих точок, можна обчислити як:*

$$S_k = \sum_{t=0}^{[k/2]} C_{2^{n-2}}^{t} \cdot C_{2^{n-2}-2t}^{k-2t} \cdot 2^{k-2t} \cdot \Psi(k,t), \text{ де}$$

$$\Psi(k,t) = \sum_{\substack{4i_1+2i_2+\\ +3i_3+2i_4+i_5=k}} \Bigg(4^{i_1+i_2+i_3+i_4} 2^{i_5} \cdot C_t^{2i_1} \cdot C_{t-2k}^{2i_2} \cdot C_{t-i_1}^{i_3} \cdot C_{k-2t-i_2}^{i_3} \cdot \Phi(2i_1) \cdot \Phi(2i_2)$$

$$C_{t-2k-i_2-i_3}^{i_5} C_{t-i_1-i_3}^{i_4} \cdot (2^{n-1} - 2k + 2t)^{\underline{2i_4+i_5}} \cdot i_3! \cdot \Phi(2^n - 2(k + i_3 + i_5 + 2i_4)) \Bigg).$$

Доведення. З описаних лем 2.12 – 2.16, зрозуміло, що пари мають між собою тісний взаємозв'язок. Тому з множини $\mathcal{Y}_1$ можна розглядати лише пари $\mathcal{Y}_1^{'} = \{\{x_1,y_1\},\ldots,\{x_t,y_t\}\}$, тому що ребра $\{x_i \oplus \beta, y_i \oplus \beta\}$ будуть визначатися залежно від заповнення цих ребер. Підрахунок підстановок π, що переводять множину $\mathcal{Y}$ в множину ребер з різницею β можна узагальнити як відображення ребер з перебором початкового заповнення вершин:

1) За лемою 2.13 зрозуміло, що можна обирати, які ребра з множини $\mathcal{Y}_1^{'}$ мають бути поєднані. Нехай потрібно поєднати $2i_1$ ребер в множині $\mathcal{Y}_1^{'}$. Тоді існує $C_t^{2i_1}$ способів обрати, які саме ребра з множини $\mathcal{Y}_1^{'}$ будуть пов'язані. Оскільки ребро не може бути поєднане саме з собою та поєднати можна поєднати лише два ребра, то таке поєднання описується інволютивними відображеннями без нерухомих точок. Також потрібно зазначити, щоб отримати всі можливі випадки заповнення зв'язаних ребер достатньо перебрати лише 4 значення для якоїсь з вершин. Тобто загалом виходить, що таких відображень буде

$$4^{i_1} \cdot C_t^{2i_1} \cdot \Phi(2i_1).$$

2) За лемою 2.14 аналогічно до попереднього пункту потрібно поєднувати ребра в множині $\mathcal{Y}_2$. Нехай потрібно поєднати $2i_2$. Така кількість буде описуватися інволюціями без нерухомих точок. Способів обрати ребра, що будуть поєднані: $C_{t-2k}^{2i_2}$ та 4 заповнення однієї з вершин для отримання усіх можливих перестановок. Тоді загальна кількість буде дорівнювати

$$4^{i_2} \cdot C_{t-2k}^{2i_2} \Phi(2i_2).$$

3) За лемою 2.15 можна розглядати відображення з множини $\mathcal{Y}_1^{'}$ в множину $\mathcal{Y}_2$. Нехай потрібно відобразити i_3 ребер. Такі відображення будуть бієктивними, тому кількість способів відобразити ребра дорівнює $i_3!$. Також потрібно обрати i_3 ребер з множини $\mathcal{Y}_1^{'}$ та $\mathcal{Y}_2$ та обрати з 4 значень, якими можна заповнити одну з вершин. Загальна кількість описується таким значенням:

$$4^{i_3} \cdot C_{t-i_1}^{i_3} \cdot C_{k-2t-i_2}^{i_3} \cdot i_3!.$$

4) В лемі 2.16 описується випадок, коли вершина ребра з множини $\mathcal{Y}_1$ переходить в ребро вершин, якого немає в множині $\mathcal{Y}$. Також можливий такий самий випадок переходу ребра для множини $\mathcal{Y}_2$. Нехай i_4 ребер з множини $\mathcal{Y}_1^{'}$ та i_5 ребра з множини $\mathcal{Y}_2$ перейдуть в ребро з такими вершинами. Тоді можна обирати i_4 значень з множини $\mathcal{Y}_1^{'}$. Не можна переходити в $2k$ вершин множини $\mathcal{Y}$ та ще $2(k-2t)$ значень, що не увійшли в множину $\mathcal{Y}_2$. Тоді загалом є $2^n - 4k + 4t$ вершин в які можна перейти. Усього способів заповнити усі $2i_4 + i_5$ ребер дорівнює

$$\prod_{i=0}^{2i_4+i_5} (2^n - 4k + 4t - 2i) = 2^{2i_4+i_5}(2^{n-1} - 2k + 2t)^{\underline{2i_4+i_5}}.$$

Загальна кількість способів перевести ребра буде дорівнювати:

$$C_{t-i_1-i_3}^{i_4} \cdot C_{t-2k-i_2-i_3}^{i_5} \cdot 2^{2i_4+i_5} \cdot (2^{n-1} - 2k + 2t)^{\underline{2i_4+i_5}}.$$

5) Також потрібно заповнені значення, що залишилися. Оскільки для цих значень немає обмежень при переході, то їх потрібно заповнити, як інволютивні відображення без нерухомих точок. Усього заповнено $2k$ значень множини $\mathcal{Y}$. Також є випадки, коли при переході були заповнені вершини, що не належать множині $\mathcal{Y}$. У випадку леми 2.14 для кожного поєднання ребер буде заповнено дві додаткові вершини, всього таких поєднань i_2, тоді буде заповнено $2i_2$ значень. Для леми 2.15 всього поєднань i_3, при цьому буде заповнено додаткові дві вершини, тобто

заповнено $2i_3$ значень. Для леми 2.16 обираючи $2i_4$ ребер, вершин додатково буде заповнено $4i_4$. Також такий випадок був описаний у пункті 4 для ребра з множини $\mathcal{Y}_2$, що заповнює ще $2i_5$ значень. Тобто залишилося $2^n - 2(k + i_2 + i_3 + 2i_4 + i_5)$ незаповнених значень вершин.

Зрозуміло, що повинні виконуватися такі умови $2i_1 + i_3 + i_4 = t$ та $2i_2 + i_3 + i_5 = k - 2t$. Якщо підставимо першу умову в другу, тоді отримаємо згортку, що описує кількість перестановок для фіксованого значення t.

$$\Psi(k,t) = \sum_{\substack{4i_1+2i_2+ \\ +3i_3+2i_4+i_5=k}} \Bigg(4^{i_1+i_2+i_3+i_4} 2^{i_5} \cdot C_t^{2i_1} \cdot C_{t-2k}^{2i_2} \cdot C_{t-i_1}^{i_3} \cdot C_{k-2t-i_2}^{i_3} \cdot \Phi(2i_1) \cdot \Phi(2i_2)$$

$$C_{t-2k-i_2-i_3}^{i_5} C_{t-i_1-i_3}^{i_4} \cdot (2^{n-1} - 2k + 2t)^{\underline{2i_4+i_5}} \cdot \cdot i_3! \Phi(2^n - 2(k + i_3 + i_5 + 2i_4)) \Bigg).$$

Також потрібно порахувати кількість підмножин $\mathcal{Y}$ при фіксованому t. Для початку оберемо t значень для того, щоб визначити множину $\mathcal{Y}_1$: $C_{2^{n-2}}^t$. Кількість способів визначити множину $\mathcal{Y}_2$ описується як: $C_{2^{n-2}-2t}^{k-2t} \cdot 2^{k-2t}$. Загальна $\mathcal{Y}$ кількість можна описати як суму по усім можливим t:

$$\sum_{t=0}^{[k/2]} C_{2^{n-2}}^t \cdot C_{2^{n-2}-2t}^{k-2t} \cdot 2^{k-2t}.$$

Значення S_k буде описуватися як:

$$\sum_{t=0}^{[k/2]} C_{2^{n-2}}^t \cdot C_{2^{n-2}-2t}^{k-2t} \cdot 2^{k-2t} \cdot \Psi(k,t).$$

□

Висновки до розділу 2

В даному розділі були продемонстровані алгебраїчні властивості бумерангового перетворення над абелевою групою; розглянуто, якого

виду набувають ці перетворення за операціями побітового додавання та додавання за модулем 2^n, введено поняття бумерангової еквівалентності S-блоків. Показано, що для операції побітового додавання потужність класів бумерангової еквівалентності буде однаковою при будь-якому значенні параметра бумерангового перетворення, а образами перетворення є інволюції без нерухомих точок. Зокрема спираючись на отримані результати було описано алгоритм генерування випадкової перестановки без нерухомих точок. У випадку модульного додавання потужність класів напряму залежить від порядку параметра бумерангового перетворення, а образи перетворення складаються з циклів однакового розміру. Також було описано алгоритм відновлення усіх прообразів бумерангового перетворення при фіксованому параметрі та знайдено оцінки часової та просторової складності. З отриманих алгебраїчних результатів вдалося узагальнити результати роботи [6] та отримати аналітичний вигляд розподілу диференціалів бумерангового перетворення для параметрів порядку 2.

ВИСНОВКИ

У ході даної роботи був проведений аналіз опублікованих джерел за тематикою диференціального аналізу та аналізу бумерангів. Зокрема було розглянуто поняття диференціалів та поняття імовірності диференціалів. Наведено основні властивості диференціальних ймовірностей. Розглянуто метод обрахунку розподілу диференціальної ймовірності як комбінаторну задачу перерахунку ребер різницевого графа, що переходять з різниці α в різницю β. Розглянуто коефіцієнт бумерангової зв'язності, як інструмент обрахунку ймовірності поширення диференціалів компоненти шифру в атаці бумерангів.

Було введено поняття бумерангового перетворення над операцією, яка утворює на множині двійкових векторів структуру абелевої групи. Отримано алгебраїчні властивості бумерангового перетворення над абелевою групою. Введено поняття бумерангової еквівалентності S-блоків. Показано, що для операції побітового додавання потужність класів бумерангової еквівалентності буде однаковою при будь-якому значенні параметра бумерангового перетворення. У випадку модульного додавання потужність класів напряму залежить від порядку параметра бумерангового перетворення. Також було описано алгоритм відновлення усіх прообразів бумерангового перетворення при фіксованому параметрі та знайдено оцінки часової та просторової складності. Результати обрахунку розподілу диференціальної ймовірності для випадкової перестановки було узагальнено для інволютивних перестановок без нерухомих точок та отримано аналітичне значення розподілу для диференціалів порядку 2.

У подальшій роботі планується покращити аналітичну форму розподілу для диференціалів порядку 2. Також розглянути випадки коли диференціали матимуть порядок понад два.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Eli Biham та Adi Shamir. «Differential cryptanalysis of DES-like cryptosystems». В: *Journal of Cryptology* 4.1 (1991), с. 3—72. DOI: 10.1007/BF00630563. URL: https://doi.org/10.1007/BF00630563.

[2] Eli Biham та Adi Shamir. «Differential Cryptanalysis of the Full 16-round DES». В: *Advances in Cryptology — CRYPTO' 92*. За ред. Ernest F. Brickell. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, с. 487—496. ISBN: 978-3-540-48071-6.

[3] Carlos Cid та ін. *Boomerang Connectivity Table: A New Cryptanalysis Tool*. Cryptology ePrint Archive, Paper 2018/161. 2018. URL: https://eprint.iacr.org/2018/161.

[4] Orr Dunkelman, Nathan Keller та Adi Shamir. *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*. Cryptology ePrint Archive, Paper 2010/013. 2010. URL: https://eprint.iacr.org/2010/013.

[5] Orr Dunkelman, Nathan Keller та Adi Shamir. «A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony». В: *Journal of Cryptology* 27.4 (2014), с. 824—849. DOI: 10.1007/s00145-013-9154-9.

[6] Philip Hawkes та Luke O'Connor. «XOR and Non-XOR Differential Probabilities». В: *Advances in Cryptology — EUROCRYPT '99*. За ред. Jacques Stern. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, с. 272—285. ISBN: 978-3-540-48910-8.

[7] Donald E. Knuth. *The art of computer programming. Volume 2, Seminumerical algorithms*. Addison-Wesley series in computer science and information processing; v. 2. Reading, Mass: Addison-Wesley, 1969, с. 139—140.

[8] Sean Murphy. «The Return of the Cryptographic Boomerang». В: *Information Theory, IEEE Transactions on* 57 (трав. 2011), с. 2517—2521. DOI: 10.1109/TIT.2011.2111091.

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

[10] David Wagner. «The Boomerang Attack». В: *Fast Software Encryption*. За ред. Lars Knudsen. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, с. 156—170. ISBN: 978-3-540-48519-3.

[11] Р.В Буржимський, С. В. Яковлєв та Л. О. Завадська. «Алгебраїчні властивості бумерангового перетворення S-блоків». В: *XXII Міжнародної науково-практичної конференції «Шевченківська весна – 2024» (11 квітня 2024 р., м. Київ, Україна), тези доповіді:* Київ: Київський національний університет імені Тараса Шевченка, 2024, с. 70. URL: https://probability.knu.ua/shv2024/ShV_2024.pdf.

[12] Буржимський Р.В. «Бумерангова еквівалентність S-блоків відносно різних алгебраїчних операцій». В: *XXII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (13 - 17 травня 2024 р., м. Київ, Україна) : матеріали конференції.* Київ: КПІ ім. Ігоря Сікорського, Видавництво «Політехніка», 2024, с. 194—197. ISBN: 978-3-540-48519-3. URL: http://conf.ipt.kpi.ua/2022/06/13/.