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

«На правах рукопису»
УДК 004.056.53

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

Магістерська дисертація

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

зі спеціальності: 113 Прикладна математика
на тему: **«Імовірності диференціалів LRX-перетворень спеціального виду»**

Виконав:
студент II курсу, групи ФІ-22мн
Галіца Олександр Олегович _____

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

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

Засвідчую, що у цій магістерській дисертації 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 — другий (магістерський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

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

ЗАВДАННЯ
на магістерську дисертацію

Студент: Галіца Олександр Олегович

1. Тема роботи: «*Імовірності диференціалів LRX-перетворень спеціального виду*», науковий керівник дисертації: доцент кафедри ММЗІ, к.т.н. 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 криптографічного захисту.

4. Предмет дослідження: LRX-перетворення та їхні криптографічні властивості.

5. Перелік завдань:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) проаналізувати нелінійні функції від двох аргументів та їхні криптографічні властивості;

3) отримати аналітичні вирази ймовірностей диференціалів для LRX-перетворень від трьох аргументів, узагальнити отримані результати.

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

7. Орієнтовний перелік публікацій: тези на XXII Міжнародній науково-практичній конференції «Шевченківська весна — 2024» (11 квітня 2024 р., м. Київ, Україна), доповідь 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).

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-жовтень 2023 р.	Виконано
3	Аналіз нелінійних булевих функцій від двох аргументів	Жовтень-грудень 2023 р.	Виконано
4	Одержання аналітичних виразів ймовірностей диференціалів для k-кратного логічного ТА	Грудень 2023 р. - січень 2024 р.	Виконано
5	Одержання аналітичних виразів ймовірностей диференціалів для кубічних нелінійних функцій спеціального виду	Січень 2024 р. - квітень 2024 р.	Виконано
6	Одержання диференціальних ймовірностей для функції мажоризації	Квітень 2024 р.	Виконано
7	Оформлення магістерської дисертації	Травень 2024 р.	Виконано

Студент _____ Олександр ГАЛІЦА

Керівник _____ Сергій ЯКОВЛЄВ

РЕФЕРАТ

Кваліфікаційна робота містить: 53 стор., 8 рисунків, 10 таблиць, 37 джерел.

Метою дослідження є розвиток диференціального криптоаналізу ARX- та LRX-криптосистем.

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

Предметом дослідження є LRX-перетворення та їхні криптографічні властивості.

У цій роботі було проаналізовано існуючі результати, що стосуються диференціального аналізу ARX- та LRX-криптосистем з акцентом на ймовірностях диференціалів нелінійних перетворень.

Деякі вже існуючі результати було узагальнено, зокрема було одержано ймовірності диференціалів для функції k-кратного логічного ТА, а також для функції мажоризації.

Було розглянуто множину кубічних нелінійних перетворень спеціального виду, проаналізовано їхню структуру, побудовано розбиття та одержано відповідні ймовірності диференціалів для усіх трьох класів цього розбиття.

ARX-КРИПТОСИСТЕМИ, LRX-ПЕРЕТВОРЕННЯ, ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ

ABSTRACT

The qualification contains: 53 pp., 8 figures, 10 tables, and 37 sources.

The purpose of the research is to develop a differential cryptanalysis of ARX- and LRX-cryptosystems.

The object of research is information processes in the systems of cryptographic protection systems.

The subject of research is LRX transformations and their cryptographic properties.

This paper analyzes the existing results related to the differential analysis of ARX- and LRX-cryptosystems with an emphasis on the probabilities of differentials of nonlinear transformations.

Some existing results were generalized, in particular, the probabilities of differentials for the function of k-fold logical AND, as well as for the majorization function were obtained.

The set of cubic nonlinear transformations of a special type was considered, their structure was analyzed, a partition was constructed, and the corresponding probabilities of differentials for all three classes of this partition were obtained.

ARX-CRYPTOSYSTEMS, LRX-TRANSFORMATIONS, DIFFERENTIAL CRYPTANALYSIS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$x \boxplus y$ — операція модульного додавання

$x \oplus y$ — операція побітового додавання (XOR)

$\neg x$, $\overline{x}$ — операція логічного НЕ

$x \wedge y$, $x\&y$, xy — операція логічного ТА

$x \vee y$ — операція логічного АБО

$x \mid y$ — операція заперечення логічного ТА (штрих Шеффера)

$x \downarrow y$ — операція заперечення логічного АБО (стрілка Пірса)

$x \to y$ — операція логічної імплікації

$x \leftarrow y$ — операція зворотної логічної імплікації

V_n — множина бітових векторів довжини n

$wt\,(x)$ — функція ваги вектору (кількість одиничних бітів в ньому)

ВСТУП

Актуальність дослідження. За останні кілька десятиліть малопотужні пристрої почали стрімко розповсюджуватись через зменшення габаритів та підвищення швидкодії, що призвело до заміщення класичних комп'ютерних систем ними в багатьох областях. Криптографія виявилась не готовою до цього, оскільки сучасні криптографічні стандарти надто обчислювально складні й ресурсів малопотужних пристроїв не вистачає для їхнього виконання.

ARX- та LRX-криптосистеми, що використовують лише елементарні операції, стали основою для побудови сучасних легких шифрів через свою надзвичайно високу швидкодію. Оскільки цей клас криптосистем є відносно новим, та нові методи ефективного криптоаналізу лише активно розробляються, є сенс розширювати та адаптувати існуючі методи аналізу, зокрема диференціальний криптоаналіз, для побудови атак та оцінювання стійкості.

Метою дослідження є розвиток диференціального криптоаналізу ARX- та LRX-криптосистем. Для досягнення мети необхідно розв'язати задачу, яка полягає в одержанні ймовірностей диференціалів для деяких нелінійних перетворень. Для розв'язання задачі необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) проаналізувати нелінійні функції від двох аргументів та їхні криптографічні властивості;

3) отримати аналітичні вирази ймовірностей диференціалів для LRX-перетворень від трьох аргументів, узагальнити отримані результати.

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

Предметом дослідження є LRX-перетворення та їхні криптографічні властивості.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи комбінаторного аналізу та дискретної математики, методи теорії ймовірностей, методи булевої алгебри.

Наукова новизна отриманих результатів полягає у одержанні ймовірностей диференціалів для ряду нових LRX-перетворень, які ще не розглядались до цього.

Практичне значення результатів полягає у тому, що їх можна використати для уточнення оцінок стійкості існуючих криптосистем, або для створення нових криптосистем, які використовуватимуть розглянуті перетворення, та для яких можна буде легко отримати оцінки стійкості від диференціального аналізу.

Апробація результатів та публікації. Результати даної роботи частково представлені на XXII Міжнародній науково-практичній конференції «Шевченківська весна — 2024» (11 квітня 2024 р., м. Київ, Україна) та 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).

1 ARX- І LRX-КРИПТОСИСТЕМИ ТА ЇХНІЙ ДИФЕРЕНЦІЙНИЙ АНАЛІЗ

Останні десятиліття все частіше почали використовуватися системи малопотужних пристроїв через зменшення собівартості й розмірів, збільшення співвідношення обчислювальних ресурсів до габаритів, та здатності спільно працювати над вирішенням деякої задачі. Прикладом може слугувати концепція «Інтернету речей» (IoT) — це мережа малих фізичних пристроїв та датчиків, які обмінюються між собою різною інформацією та, внаслідок цього, дозволяють автоматизувати певні побутові чи промислові процеси.

Сучасні криптографічні стандарти були незастосовні до малопотужних пристроїв через як громіздку фізичну реалізацію, яка виражається в кількості необхідних для побудови логічних вентилів, так і складну програмну реалізацію, для виконання якої не вистачає обчислювальних потужностей, тому, для вирішення гостро назрілих проблем захисту та цілісності інформації на подібних системах, Національний інститут стандартів та технологій США розпочав конкурс «Lightweight Cryptography» [30] у 2013 році, фіналістами якого стали криптосистеми, які, здебільшого, використовують лише елементарні операції, такі як додавання за модулем, побітове додавання тощо, які надзвичайно швидкі та легко фізично реалізовні.

Ці події стали одними з передумов для активного розвитку ARX-, а згодом і LRX-криптосистем, та створення нових видів криптоаналізу для пошуку вразливостей таких криптосистем.

1.1 ARX-криптосистеми

ARX-криптосистеми використовують лише невелику множину операцій, а саме додавання за модулем (Addition, зазвичай, модуль обирається виду 2^n), бітовий зсув (Rotation) та побітове додавання (XOR). Обчислювальна вартість цих для сучасних мікропроцесорів є крихітною, тому ARX-криптосистеми характеризуються значно вищою швидкодією в порівнянні з усіма іншими видами криптосистем, а стійкості до класичних видів криптоаналізу, таких як диференціальний та лінійний, вони досягають завдяки комбінації лінійних операцій (бітовий зсув та побітове додавання) та нелінійних (додавання за модулем). Розглянемо декілька відомих представників ARX-криптосистем.

1. Salsa20 — це потоковий шифр, розроблений Даніелем Бернштайном [16] та представлений на конкурсі eSTREAM [21], переможцем якого він і став у 2008 році. В основі лежить чверть-раундова функція (quarterround), схема роботи якої наведена на рис. 1.1, та яка має такий вид:

Нехай $y = (y_0, y_1, y_2, y_3)$, де $y_i \in V_{32}$, додавання здійснюється за модулем 2^{32}, тоді $quarterround\,(y) = (z_0, z_1, z_2, z_3)$, де

$$\begin{aligned} z_1 &= y_1 \oplus ((y_0 \boxplus y_3) \lll 7)\,, \\ z_2 &= y_2 \oplus ((z_1 \boxplus y_0) \lll 9)\,, \\ z_3 &= y_3 \oplus ((z_2 \boxplus z_1) \lll 13)\,, \\ z_0 &= y_0 \oplus ((z_3 \boxplus z_2) \lll 18)\,. \end{aligned}$$

В специфікації шифру Salsa20 Деніел Бернштайн пропонує використовувати 12 раундів, і на сьогодні найбільш успішний криптоаналіз був проведений в роботі [26]: автори показали, що атака відновлення 256-бітового ключа на 8-раундову модифікацію шифру Salsa20 може бути проведена з часовою складністю, оціненою в $2^{247.2}$, що є швидшим за перебір всього ключового простору; повний

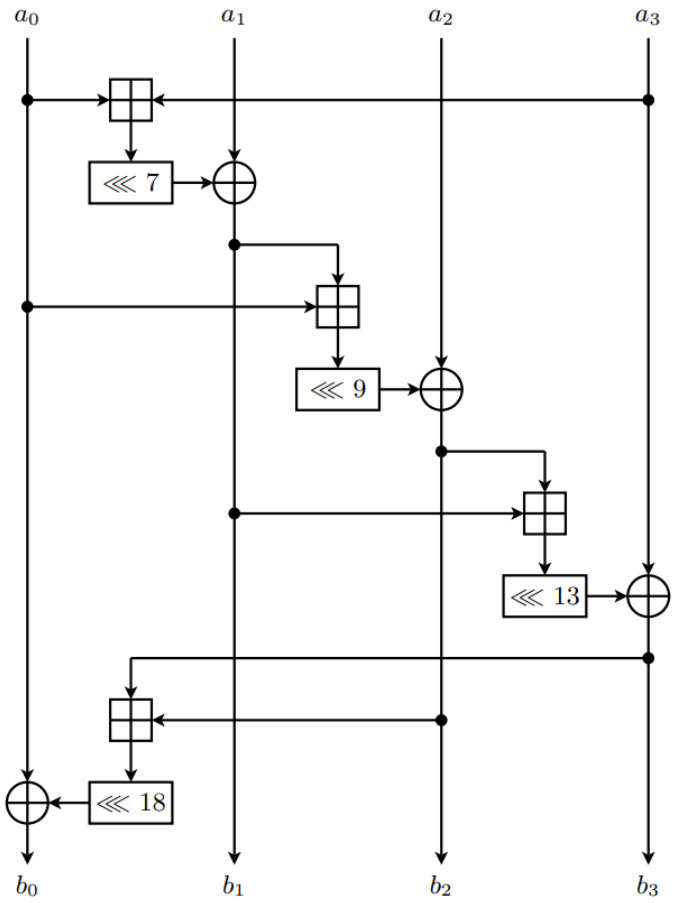


Рисунок 1.1 – Схема чверть-раундової функції шифру `Salsa20`

12-раундовий шифр досі не зламаний.

Що стосується диференціального криптоаналізу: в роботі [28] було запропоновано метод одержання оптимальних диференціальних характеристик наперед заданої ваги; в роботі [12] було розроблено так звану «гібридну модель» з певними припущеннями для теоретичної оцінки стійкості, та зробоено висновок, що 12 раундів в шифрі `Salsa20` достатньо для забезпечення 256-бітового рівня безпеки від диференціального криптоаналізу.

1.5. ChaCha20 — це потоковий шифр, який є ідеологічним спадкоємцем `Salsa20`, розроблений тим же Даніелем Бернштайном [15]: він використовує ті ж принципи, на яких був побудований шифр `Salsa20`, проте раундова функція *quarterround* має дещо інший вигляд (рис. 1.2):

Нехай $y = (y_0, y_1, y_2, y_3)$, де $y_i \in V_{32}$, додавання здійснюється за

модулем 2^{32}, тоді $quarterround\,(y) = (z_0, z_1, z_2, z_3)$, де

$$\begin{aligned}
b_0 &= x_0 \boxplus x_1, \\
b_3 &= (x_3 \boxplus b_0) \lll 16, \\
b_2 &= x_2 \boxplus b_3, \\
b_1 &= (x_1 \boxplus b_2) \lll 12, \\
z_0 &= b_0 \boxplus b_1, \\
z_3 &= (b_3 \boxplus z_0) \lll 8, \\
z_2 &= b_2 \boxplus z_3, \\
z_1 &= (b_1 \boxplus z_2) \lll 7.
\end{aligned}$$

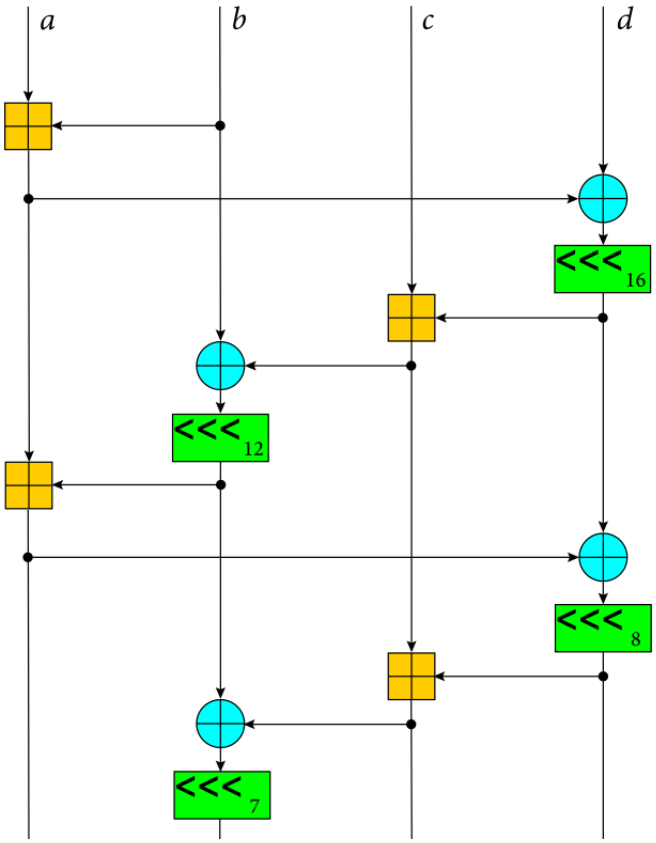


Рисунок 1.2 – Схема чверть-раундової функції шифру `ChaCha20`

Основною ціллю Д. Бернштайна було збільшити розсіювання, яке вносить один раунд, без сповільнення (або навіть пришвидшення) процесу шифрування. Шифр `ChaCha20` у свій час став настільки хорошою

альтернативою існуючим стандартам шифрування, що був включений у багато криптографічних бібліотек та протоколів, таких як `TLS`, `OpenSSH` та `QUIC`.

Найуспішніший криптоаналіз було проведено в роботі [17]: автори побудували атаку на 6-раундову модифікацію `ChaCha` з часовою складністю в $2^{99.48}$; і хоча цей результат є це суттєвим покращенням відносно вже побудованих атак (зменшення складності на 2^{40}), це не становить загрози для використання шифру, зважаючи на те, що специфікація шифру `ChaCha` передбачає використання 20-ти раундів. Є й інші роботи, де будуються атаки на `ChaCha20` з більшою кількістю раундів, зокрема автори роботи [18] зосереджуються на 7-раундовій `ChaCha`, пропонуючи атаку зі складністю $2^{221.95}$, що на порядки складніше за атаки на 6 раундів. Знову слід згадати й про роботу [12]: автори стверджують, що згідно їхнього моделювання 12 раундів повинно бути достатньо для забезпечення 256-бітового рівня безпеки, і 20 раундів є надлишком, якого можна було би позбутися для підвищення швидкодії.

2. LEA (Lightweight Encryption Algorithm) — блоковий шифр, розроблений в Південній Кореї в 2013 році, та прийнятий в подальшому в якості національного стандарту [20]. Раундова функція, схема якої наведена на рис. 1.3, має такий вид:

Нехай $x = (x_0, x_1, x_2, x_3)$, $x_i \in V_{32}$, додавання здійснюється за модулем 2^{32}, $k_j^i, j \in \overline{0,5}$ — раундові ключі, отримані за допомогою алгоритму розкладу ключів, тоді раундова функція `LEA` $f_i(x) = (y_0, y_1, y_2, y_3)$, де:

$$\begin{aligned} y_0 &= \left(\left(x_0 \oplus k_0^i\right) \boxplus \left(x_1 \oplus k_1^i\right)\right) \lll 9, \\ y_1 &= \left(\left(x_1 \oplus k_2^i\right) \boxplus \left(x_1 \oplus k_3^i\right)\right) \lll 9, \\ y_2 &= \left(\left(x_2 \oplus k_4^i\right) \boxplus \left(x_2 \oplus k_5^i\right)\right) \lll 9, \\ y_3 &= x_0. \end{aligned}$$

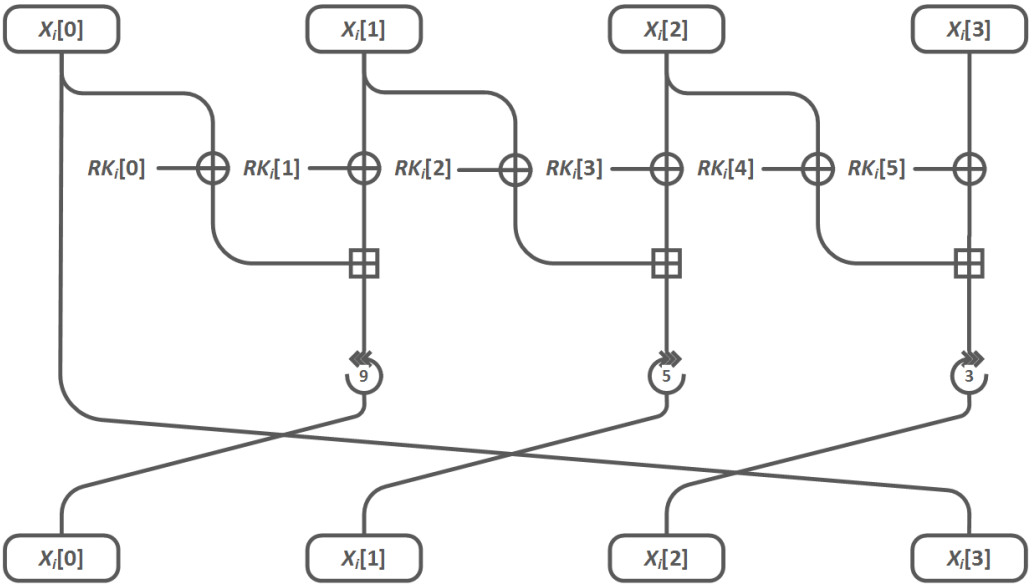


Рисунок 1.3 – Схема раундової функції шифру `LEA`

Найуспішніший криптоаналіз шифру `LEA` на сьогодні викладено в роботі [11]. Автори цієї роботи використовують методи диференціально-лінійного криптоаналізу, побудовано атаки на всі три модифікації шифру `LEA` — на 17 раундів `LEA-128` зі складністю $2^{82.9}$, на 17/18 раундів `LEA-192` зі складністю $2^{82.9}/2^{189.63}$, та на 17/18 раундів`LEA-256` зі складністю $2^{82.9}/2^{189.63}$ відповідно.

Слід згадати і про роботу [33], спрямовану виключно на диференціальний аналіз шифру `LEA`: в ній автори, використовуючи вже згаданий механізм пошуку оптимальних диференціалів [28], одержали нові 12-ти/13-ти раундові диференціальні характеристики з імовірностями $2^{-103.19}/2^{-123.79}$ відповідно.

3. Speck — блоковий шифр, опублікований Агенством національної безпеки в США в 2013 році [4], яке намагалася створити новітню та безпечну криптосистему, здатну виконуватися на різноманітних пристроях «Інтернету речей», зберігаючи при цьому прийнятний рівень захисту. Раундова функція, схема якої наведена на рис. 1.4, має такий

вид:

$$\begin{aligned} R_k(x,y) &= (f_k(x,y), f_k(x,y) \oplus (y \lll \beta)), \\ f_k(x,y) &= ((x \ggg \alpha) \boxplus y) \oplus k, \end{aligned}$$

де α/β дорівнюють 7/2 або 8/3 відповідно, в залежності від розміру вхідного блоку.

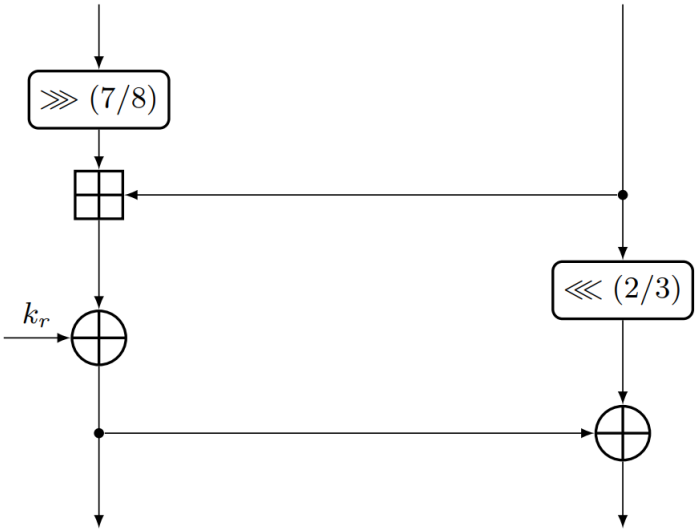


Рисунок 1.4 – Схема раундової функції шифру `Speck`

Розробники `Speck` передбачили різні режими роботи: шифр здатний працювати з розмірами блоку в 32, 48, 64, 96 та 128 бітів, а також з довжинами ключів в 64, 72, 96, 128, 144, 192 та 256 бітів. Оскільки `Speck` був запропонований АНБ та просувався як національний стандарт, багато криптоаналітиків по всьому світу розпочали його дослідження, і, станом на сьогодні, побудовано теоретичні атаки відновлення ключа, ефективніші за повний перебір ключового простору, на всі режими роботи. Ці атаки, хоч і розглядаються для зменшеної кількості раундів, побудовані для модифікацій, коли ця кількість зменшується лише на 25-30%, і такі шифри не вважаються надійними, оскільки є висока ймовірність, що вони будуть повністю зламані при наступному технологічному стрибку, або при відкритті нових методів криптоаналізу.

Найефективніші атаки на Speck були побудовані саме з використанням методів диференціального криптоаналізу, найкращі результати на сьогодні було отримано в роботі [22], кількість раундів, на які проводились атаки, та відповідну часову складність наведено в таблиці 1.1.

Таблиця 1.1 – Атаки відновлення ключа на шифр Speck

Режим роботи	Кількість раундів	Часова складність
32/64	14/22	$2^{60.58}$
48/72	16/22	$2^{71.78}$
48/96	17/22	$2^{95.78}$
64/96	19/26	$2^{92.28}$
64/128	20/27	$2^{125.34}$
96/96	20/28	$2^{95.75}$
96/144	21/29	$2^{143.13}$
128/128	23/32	$2^{124.95}$
128/192	24/33	$2^{174.53}$
128/256	25/34	$2^{238.53}$

Варта уваги й робота [5], автори якої запропонували більш ефективний алгоритм знаходження оптимальних диференціалів шляхом використання методів штучного інтелекту, зокрема «Single Player Monte-Carlo Tree Search», що, в деяких випадках, дозволило їм пришвидшити пошук в десятки разів відносно інших існуючих методів.

1.2 LRX-криптосистеми

На противагу ARX-, також розроблялися і LRX-криптосистеми, які замість модульного додавання — найскладнішої операції в трійці A-R-X — використовували деякі інші нелінійні логічні операції.

1. NORX — це блоковий шифр, який побудовано з використанням

конструкції криптографічної «губки», представлений на конкурсі CAESAR [2]. Оскільки шифр використовує класичну схему «губки», ключовим елементом для криптоаналізу тут є базова перестановка (один з основних компонентів в схемі «губки»), а точніше — введена розробниками функція G, яка застосовується парелельно до перемішаних частин вхідного блоку.

Одна з основних цілей, які собі ставили автори NORX при виборі функції G, було уникнення використання додавання за модулем, тому в якості нелінійної компоненти була використана така його апроксимація (рис. 1.5):

$$f(x) = (x \oplus y) \oplus ((x \wedge y) \lll 1).$$

Перетворення такого виду імітує додавання за модулем з бітом переносу, завдяки нециклічному зсуву, а також, окрім нелінійності, забезпечує ще й додаткове розсіювання бітів.

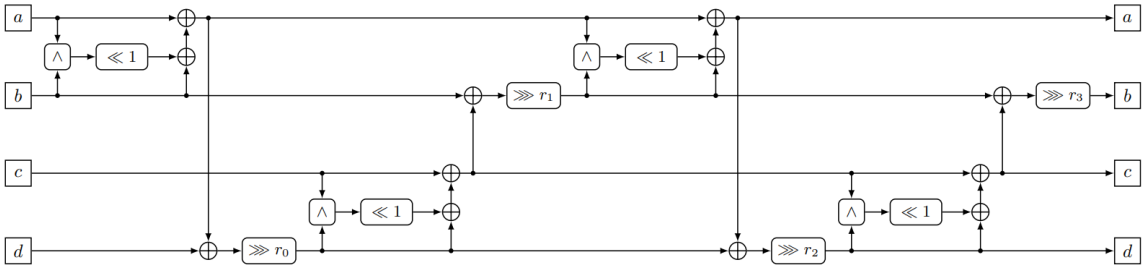


Рисунок 1.5 – Базова перестановка шифру NORX

2. Simon — це блоковий шифр, що використовує схему Фейстеля, який разом зі Speck був опублікований Агенцією національної безпеки США, та який є більш оптимальним з точки зору простоти апаратної реалізації [4]. Раундова функція, зображена на рис 1.6, має такий вид:

$$\begin{aligned} R_k(x, y) &= ((y \oplus f(x) \oplus k), x), \\ f(x) &= ((x \lll 1) \wedge (x \lll 8)) \oplus (x \lll 2). \end{aligned}$$

Як і Speck, Simon дозволяє використовувати ціле різноманіття як

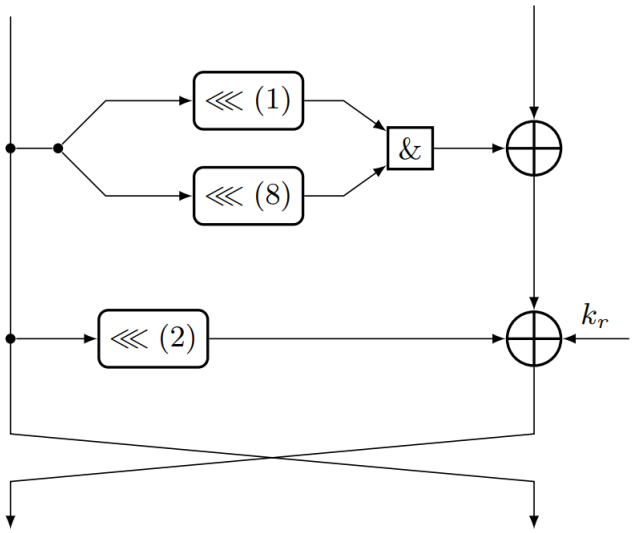


Рисунок 1.6 – Схема раундової функції шифру `Simon`

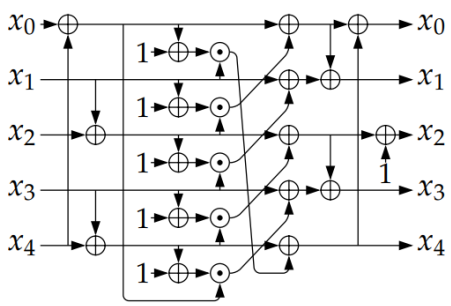
довжин ключів, так і розмірів вхідних блоків, проте, на відміну від `Speck`, найбільш вдалі атаки на шифр `Simon` були побудовані, використовуючи методи лінійного криптоаналізу. Останні результати в цьому напрямі викладені в роботі [10] та наведені в таблиці 1.2, де часова складність обчислена у кількості додавань та шифрувань. І знову, як і зі шифром `Speck`, атаки були побудовані на кількість раундів, що становить 65-70% від загальної кількості, що ставить під загрозу використання `Simon`.

3. Ascon — це блоковий шифр, переможець конкурсів `CAESAR` [9] та `Lightweight Cryptography` [32], а також, як і `NORX`, побудований з використанням конструкції «губки» [19]. Базова перестановка складається з трьох шарів: шару додавання з константою (використовує побітове додавання), шару заміни, що забезпечує перемішування, та лінійного шару, відповідального за розсіювання, структура останніх двох наведена на рис. 1.7.

Одна з причин обрання шифру `Ascon` в якості стандарту легкої криптографії був факт, що `Ascon` до цього став переможцем конкурсу `CAESAR` і був глибоко досліджений світовими криптоаналітиками. Було багато спроб побудувати атаки відновлення

Таблиця 1.2 – Атаки відновлення ключа на шифр `Simon`

Режим роботи	Кількість раундів	Часова складність
32/64	23/32	$2^{61.84}A + 2^{56}E$
48/72	24/36	$2^{67.89}A + 2^{65.34}E$
48/96	25/36	$2^{89.89}A + 2^{88.28}E$
64/96	30/42	$2^{93.62}A + 2^{88.13}E$
64/128	31/44	$2^{119.62}A + 2^{120}E$
96/96	37/52	$2^{67.94}A + 2^{88}E$
96/144	38/54	$2^{98.94}A + 2^{136}E$
128/128	49/68	$2^{87.77}A + 2^{120}E$
128/192	51/69	$2^{155.77}A + 2^{184}E$
128/256	53/72	$2^{239.77}A + 2^{248}E$



$$x_0 \leftarrow \Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$
$$x_1 \leftarrow \Sigma_1(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$
$$x_2 \leftarrow \Sigma_2(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$$
$$x_3 \leftarrow \Sigma_3(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$
$$x_4 \leftarrow \Sigma_4(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$$

Рисунок 1.7 – Схема шару заміни та нелінійного шару в базовій перестановці `Ascon`

ключа на `Ascon` з використанням усіх найсучасніших технік, і максимальна кількість раундів, для якої вдалося побудувати атаку, ефективнішу за повний перебір ключового простору, це 7 раундів. Найкращі атаки, метод криптоаналізу, що вони використовують, та їхня складність, наведено в таблиці 1.3.

Таблиця 1.3 – Атаки відновлення ключа на шифр `Simon`

Метод криптоаналізу	Кількість раундів	Часова складність	Джерело
Атака кубів	7/12	$2^{72.4}$ або $2^{104.7}$	[23]
Атака кубів	7/12	$2^{103.9}$	[24]
Диф.-лінійний	5/12	$2^{31.44}$	[34]
Атака усічених диф.	5/12	2^{58} або $2^{127.99}$	[35]

1.3 Диференціальний аналіз

Диференціальний аналіз і сьогодні залишається потужним видом криптоаналізу, стійкість до якого є однією з обов'язкових умов, що розглядаються при побудові сучасних блокових шифрів. Диференціальний аналіз «відкрив» (насправді, він був відомий працівникам Агенства національної безпеки США ще в 1970-х роках, але тримався в секреті [13]) Аді Шамір у кінці 1980-их років, побудувавши атаки на тодішній стандарт шифрування `DES`, а також `FEAL`, `Khafre`, `Lucifer` тощо, які були швидші за повний перебір усього ключового простору [6].

Диференціальний криптоаналіз — це, перш за все, атака на основі обраного відкритого тексту (модель, при якій зловмисник може отримувати шифротекст для довільного відкритого тексту). Мета диференціального криптоаналізу полягає у дослідженні, як різниця між спотвореним та вихідним блоками вхідного тексту впливатиме на різницю у шифротекстах. Зловмисник досліджує різниці у відповідних шифроктекстах, стараючись виявити якісь статистичні закономірності. Очікується, що деякі пари вхідних та вихідних різниць будуть частіше траплятися за інші, що дозволить будувати атаки по відновленню ключа, оскільки такий шифр буде відрізнюваний від випадкової перестановки.

Різниці можна розглядати за різними операціями, але зазвичай вони розглядаються за операцією побітового додавання $\oplus$. Базовою одиницею

диференціального криптоаналізу є так званий *диференціал.*

Означення 1.1. Нехай $f : V_n^k \to V_m$, $n, k, m \in \mathbb{N}$, тоді *диференціал* f — це довільний $k+1$-вектор $(\alpha_1, \alpha_2, ..., \alpha_k \to \gamma)$, $\alpha_i \in V_n, \gamma \in V_m$, де α_i відображають відповідні різниці на вході, а γ — різницю на виході.

Тоді можна ввести основну обчислювальну характеристику диференціалів, різниці розглядатимемо за операцією $\oplus$.

Означення 1.2. *Імовірність диференціалу* $(\alpha_1, \alpha_2, ..., \alpha_k \to \gamma)$ *перетворення* f *за операцією побітового додавання* (або XOR Differential Probability) визначається таким чином:

$$xdp^f(\alpha_1, \alpha_2, ..., \alpha_k \to \gamma) =$$
$$= \Pr_{x_1,...,x_k}\{f(x_1 \oplus \alpha_1, x_2 \oplus \alpha_2, \ldots, x_k \oplus \alpha_k) = f(x_1, x_2, \ldots, x_k) \oplus \gamma\}.$$

Традиційно, сучасні блокові шифри будуються на основі схеми Фейстеля, або `SP`-мережі, де нелінійність забезпечується так званим `S`-блоком (`Substitution`-блок), яка виконує роль деякої підстановки. Загалом, `S`-блок — це деяке перетворення, яке перетворює вхід довжини `n` на вихід довжини `m`, $n, m \in \mathbb{N}$.

Через те, що зазвичай розмір входу `S`-блоку є невеликим, для до вхідного блоку шифру застосовується паралельно кілька `S`-блоків, і потім вихід розсіюється лінійним шаром. Невеликий розмір `S`-блоку дає можливість порахувати таблицю розподілу різниць.

Означення 1.3. *Таблиця розподілу різниць перетворення* f *за операцією побітового додавання* (або Difference Distrubution Table) — таблиця, що показує ймовірнісний розподіл усіх можливих пар вхідних та вихідних різниць за операцією $\oplus$.

Властивості сучасних блокових шифрів, зокрема незалежність `S`-блоків, дозволяють обчислювати диференціальні характеристики, маючи ймовірності диференціалів для нелінійних частин шифру.

Означення 1.4. *r-раундова диференціальна характеристика* Ω

шифру E — послідовність бітових векторів $(\omega_1, \omega_2, \ldots, \omega_r)$, що розглядається як послідовність зміни між раундами під час шифрування.

Деякі сімейства блокових шифрів володіють доказовою стійкістю від диференціального аналізу, яка зводиться до підрахунку таблиці розподілу різниць та обчислення ймовірностей усіх диференціальних характеристик, з яких можна обчислити теоретичну складність найбільш потужної атаки, та зробити висновок про (не)застосовність цього методу криптоаналізу.

Якщо повернутись до ARX-криптосистем, то тут, зазвичай, побудувати таблицю розподілу різниць є надто складною задачею, оскільки навіть для $f : V_{32} \times V_{32} \to V_{32}$ це вимагало б 2^{96} бітів пам'яті, для 48 та 64 бітів — це взагалі нереалізовна в найближчому майбутньому задача, тому потрібно було застосувати якісь нові, більш оптимізовані підходи й техніки.

Загалом, криптоаналіз ARX-криптосистем розпочався з роботи Ліпмаа і Моріаі [25]. Оскільки різниці розглядаються за операцією побітового додавання, то єдиною операцією, яка спричинює не лінійні різниці — це додавання за модулем, і в цій роботі було вперше отримано аналітичні вирази ймовірностей диференціалів для операції модульного додавання.

Теорема 1.1. *Нехай* $(\alpha, \beta \to \gamma)$ — *довільний диференціал,* $\alpha, \beta, \gamma \in V_n$, *тоді справедливі такі твердження:*

1) $xdp^{\boxplus}(\alpha, \beta \to \gamma) \neq 0$ *тоді та тільки тоді, коли виконується таке рівняння:*

$$eq(\alpha \lll 1, \beta \lll 1, \gamma \lll 1) \wedge (\alpha \oplus \beta \oplus \gamma \oplus (\beta \lll 1)) = 0;$$

2) Якщо $xdp^{\boxplus}(\alpha, \beta \to \gamma) \neq 0$, *то*

$$xdp^{\boxplus}(\alpha, \beta \to \gamma) = \left(\frac{1}{2}\right)^{wt(\neg eq(\alpha \lll 1, \beta \lll 1, \gamma \lll 1))},$$

де $eq(x, y, z)$ — *це вектор рівності бітів:*

$$\forall i \in \overline{1, n} : eq(x, y, z)_i = 1 \iff x_i = y_i = z_i.$$

Отримання точних виразів для модульного додавання дозволило обчислювати ймовірності диференціальних характеристик та будувати, або принаймні намагатись будувати деякі атаки. Також слід зауважити, що Ліпмаа та Моріаі не лише обчислили ймовірності диференціалів, а й навели логарифмічний за часом алгоритм для знаходження «гарних» (в сенсі з високою диференціальною ймовірністю, проте не обов'язково найвищою) диференціалів.

Також варто згадати про роботу Бірюкова й Велічкова [8], в якій вони спробували подолати проблему обчислення таблиці розподілу різниць, а саме запропонували обчислювати часткову таблицю розподілу різниць, що міститиме лише такі диференціали, ймовірності яких вищі за деяку наперед задану межу.

Складність диференціального аналізу ARX-шифрів полягає в тому, що модульне додавання, на відміну від побітового, спричинює появу бітів переносу.

Означення 1.5. *Вектор бітів переносу* $carry\,(x, y)$ — це біти, які з'являються в процесі додавання за модулем, тобто

$$carry\,(x, y) = (x \boxplus y) \oplus x \oplus y.$$

Властивості додавання дозволяють представити вектор бітів переносу як рекурентну послідовність:

$$\begin{aligned} c_0 &= 0; \\ c_i &= (x_i \oplus y_i) \wedge (y_i \oplus z_i) \wedge (x_i \oplus z_i)\,, \end{aligned}$$

де $x, y \in V_n$ $c = carry\,(x, y)$, $i \in \overline{1, n-1}$.

Автори роботи [25] також сформулювали лему, яка пов'язує ймовірності диференціалів та відповідні біти переносу.

Лема 1.1. *Нехай* $(\alpha, \beta \to \gamma)$ *— диференціал,* $\alpha, \beta, \gamma \in V_n$*, тоді*

$$xdp^{\boxplus}\,(\alpha, \beta \to \gamma) = \Pr_{x,y}\left\{carry\,(x, y) \oplus carry\,(x \oplus \alpha, y \oplus \beta) = \alpha \oplus \beta \oplus \gamma\right\}.$$

Якщо раундовій функції є кілька додавань за модулем, то і бітів переносу з'являється декілька, і всі вони пов'язані один з одним, що значно ускладнює отримання аналітичних виразів ймовірностей диференціалів, необхідних для знаходження високоймовірнісних диференціальних характеристик.

Тому однією з передумов розвитку LRX-криптосистем (окрім як з міркувань швидкодії), як стверджували автори NORX — фактично, першого LRX-шифру — було бажання спростити криптоаналіз шляхом заміни модульного додавання деякою його нелінійною апроксимацією.

Операція логічного ТА $\wedge$ є нелінійною, має просту таблицю істинності та її легко апаратно реалізувати, тому більшість LRX-перетворень використовують або її, або деяке її ускладнення в якості нелінійного частини перетворення.

Вперше аналітичні вирази ймовірностей диференціалів для операції логічного ТА були отримані у роботі Бірюкова, Роя та Велічкова по криптоаналізу шифру Simon [7].

Теорема 1.2. *Нехай* $(\alpha, \beta \to \gamma)$ *— диференціал,* $\alpha, \beta, \gamma \in V_n$*, тоді*

$$xdp^{\wedge}(\alpha, \beta \to \gamma) = \\ = 2^{-n} \cdot \prod_{i=0}^{n-1} \left(\left(2 \cdot \overline{(\overline{\alpha_i} \wedge \overline{\beta_i} \wedge \overline{\gamma_i})} \right) \vee \overline{(\overline{\alpha_i} \wedge \overline{\beta_i})} \right) \wedge \overline{(\overline{\alpha_i} \wedge \overline{\beta_i} \wedge \gamma_i)}. \quad (1.1)$$

Також ними розглядалися диференціали виду $(\alpha, (\alpha \lll r) \to \gamma)$, $r \in N$: отримати аналітичні вирази для їхніх ймовірностей не вдалося, проте була сформульована гіпотеза, що для фіксованих α, γ ймовірність такого диференціалу може бути обчислена за час $\mathcal{O}(n)$.

Якщо повернутись до криптоаналізу шифру NORX, то в роботі [1], відштовхуючись від теорем 1.1 та 1.2, були сформульовані схожі формулювання для нелінійної функції G шифру NORX.

Теорема 1.3. *Нехай* $(\alpha, \beta \to \gamma)$ *— довільний диференціал,* $\alpha, \beta, \gamma \in V_n$*, тоді справедливі такі твердження:*

1) $xdp^G(\alpha, \beta \to \gamma) \neq 0 \iff (\alpha \oplus \beta \oplus \gamma) \wedge \overline{((\alpha \vee \beta) \ll 1)} = 0$*;*

2) Якщо $xdp^G(\alpha, \beta \to \gamma) \neq 0$*, тоді:*

$$xdp^G(\alpha, \beta \to \gamma) = \left(\frac{1}{2}\right)^{wt((\alpha \vee \beta) \ll 1)}.$$

Проте автори роботи також зрозуміли, що більш ефективно буде розглядати так звані f-диференціали замість класичних бітових різниць за операцією $\oplus$.

Означення 1.6. Нехай $f : V_n \times V_n \to V_n$, $\alpha, \beta, \gamma \in V_n$, тоді $(\alpha, \beta \to \gamma)$ буде f-диференціалом, якщо існують такі бітові вектори $x, y \in V_n$, що

$$f(x, \alpha) \oplus f(y, \beta) = f(x \oplus y, \gamma).$$

Якщо ж таких x, y не існує, то $(\alpha, \beta \to \gamma)$ — це неможливий f-диференціал.

Ймовірності таких диференціалів теж можна розглядати, відповідне позначення: $fdp^{\oplus}(\alpha, \beta \to \gamma)$.

Відповідно, якщо скористатись означенням 1.6 та виглядом функції G, отримаємо рівняння, аналіз якого дасть змогу отримати шукані f-диференціали.

$$\alpha \oplus \beta \oplus \gamma = ((x \wedge (\alpha \oplus \gamma)) \oplus (y \oplus (\beta \oplus \gamma))) \ll 1.$$

Тепер можна переформулювати теорему 1.3 в термінах f-диференціалів.

Теорема 1.4. *Нехай* $(\alpha, \beta \to \gamma)$ *— довільний диференціал,* $\alpha, \beta, \gamma \in V_n$*, тоді справедливі такі твердження:*

1) $Gdp^{\oplus}(\alpha, \beta \to \gamma) \neq 0$ *тоді та тільки тоді, коли справедливе таке рівняння:*

$$(\alpha \oplus \beta \oplus \gamma) \wedge \left(\left(\overline{\gamma \ll 1}\right) \oplus (\alpha \ll 1)\right) \wedge \left(\left(\overline{\beta \ll 1}\right) \oplus (\gamma \ll 1)\right) = 0;$$

2) Якщо $Gdp^{\oplus}(\alpha, \beta \to \gamma) \neq 0$*, тоді:*

$$Gdp^{\oplus}(\alpha, \beta \to \gamma) = \left(\frac{1}{2}\right)^{wt((\alpha \oplus \gamma) \vee (\beta \oplus \gamma) \ll 1)}.$$

Як можна побачити, під кожне конкретне перетворення є сенс розглядати різні за видом диференціали, оскільки диференціали, розглянуті за іншою операцією, можуть бути розподілені більш нерівномірно, що дасть можливість будувати ефективніші атаки.

Також у роботі [1] було запропоновано алгоритм `NODE` для знаходження диференціальних характеристик з наперед заданою вагою. З його допомогою авторами було знайдені декілька двораундових диференціальних характеристикик з ймовірністю 1 для 32- та 64-бітового варіантів функції G, рис. 1.8.

Differences				
δ_0	80000000	80000000	80000000	00000000
δ_1	00000000	00000001	80000000	00000000
δ_0	80000000	00000000	80000000	80000080
δ_1	80000000	00000000	00000000	00000000
δ_0	00000000	80000000	00000000	80000080
δ_1	80000000	00000001	80000000	00000000

Differences				
δ_0	8000000000000000	8000000000000000	8000000000000000	0000000000000000
δ_1	0000000000000000	0000000000000001	8000000000000000	0000000000000000
δ_0	8000000000000000	0000000000000000	8000000000000000	8000000000000080
δ_1	8000000000000000	0000000000000000	0000000000000000	0000000000000000
δ_0	0000000000000000	8000000000000000	0000000000000000	8000000000000080
δ_1	8000000000000000	0000000000000001	8000000000000000	0000000000000000

Рисунок 1.8 – Двораундові диференціальні характеристики для функції G

Висновки до розділу 1

У цьому розділі було окреслено передумови виникнення та розвитку `ARX`- та `LRX`-криптосистем, розглянуто ряд відомих `ARX`- та `LRX`-криптосистем і деякі їхні властистивості, також наведено їхні нелінійні перетворення.

Окрім цього детально розглянуто диференціальний аналіз та як він

працює, розглянуто особливості застосування диференціального аналізу до ARX- та LRX-криптосистем, а також викладено основні результати, що будуть використані у подальших обчисленнях.

2 ДИФЕРЕНЦІАЛЬНІ ЙМОВІРНОСТІ ДЕЯКИХ LRX-ПЕРЕТВОРЕНЬ

У цьому розділі буде розглянуто ряд LRX-перетворень, а саме логічне ТА, k-кратне логічне ТА, деякі кубічні функції спеціального виду, функція мажоризації та одержано ймовірності диференціалів для них.

2.1 Імовірності диференціалів логічного ТА

Як вже згадувалося, вперше аналітичні вирази ймовірностей диференціалів для операції логічного ТА були отримані в роботі [7]. Проте виявилося, що ці вирази можна переформулювати у більш зручному для обчислень вигляді, результат було отримані спільно з Сергієм Яковлєвим [37].

Теорема 2.1. *Для довільних $\alpha, \beta, \gamma \in V_n$ справедливі твердження:*
1) $xdp^{\wedge}(\alpha, \beta \to \gamma) \neq 0 \iff \overline{\alpha} \wedge \overline{\beta} \wedge \gamma = 0$;
2) якщо $xdp^{\wedge}(\alpha, \beta \to \gamma) \neq 0$, то

$$xdp^{\wedge}(\alpha, \beta \to \gamma) = 2^{-wt(\alpha \vee \beta)}.$$

Доведення. Розглянемо рівняння $(x \oplus \alpha)(y \oplus \beta) = xy \oplus \gamma$ побітово:

$$\begin{aligned} (x_i \oplus \alpha_i)(y_i \oplus \beta_i) &= x_i y_i \oplus \gamma_i; \\ \alpha_i y_i \oplus \beta_i x_i &= \alpha_i \beta_i \oplus \gamma_i. \end{aligned} \tag{2.1}$$

Позначимо через p_i імовірність виконання рівняння (2.1); оскільки усі біти обчислюються незалежно, то $xdp^{\wedge}(\alpha, \beta \to \gamma) = \prod_{i=0}^{n-1} p_i$.

Розглянемо усі можливі випадки значень параметрів α_i, β_i та γ_i, відповідні форми рівняння (2.1) та імовірності p_i для кожного випадку. Значення імовірностей наведено у таблиці 2.1.

Таблиця 2.1 – Рівняння (2.1) та ймовірність його виконання p_i при усіх можливих значеннях α_i, β_i, γ_i.

α_i	β_i	γ_i	рівняння	p_i
0	0	0	$0 = 0$	1
0	0	1	$0 = 1$	0
0	1	0	$x_i = 0$	1/2
0	1	1	$x_i = 1$	1/2
1	0	0	$y_i = 0$	1/2
1	0	1	$y_i = 1$	1/2
1	1	0	$x_i \oplus y_i = 1$	1/2
1	1	1	$x_i \oplus y_i = 0$	1/2

З таблиці 2.1 бачимо, що при умовах $\alpha_i = \beta_i = 0$ та $\gamma_i = 1$ рівняння не може виконуватись: $p_i = 0$; тому якщо у векторі $\overline{\alpha} \wedge \overline{\beta} \wedge \gamma$ хоча б один біт дорівнює 1, то $xdp^{\wedge}(\alpha, \beta \to \gamma) = 0$.

Якщо ж $xdp^{\wedge}(\alpha, \beta \to 0) \neq 0$, то при $\alpha_i = \beta_i = 0$ маємо $p_i = 1$, а в усіх інших випадках — $p_i = \frac{1}{2}$; тому $xdp^{\wedge}(\alpha, \beta \to \gamma) = 2^{-k}$, де k — кількість ненульових пар (α_i, β_i) або, що те саме, кількість одиничних бітів у векторі $\alpha \vee \beta$, з чого й випливає твердження теореми. □

2.2 Імовірності диференціалів для k-кратного логічного ТА

Теорема 2.1 може бути узагальнена для операції k-кратного логічного ТА, але для цього спочатку потрібно навести допоміжний факт.

Лема 2.1. *Нехай* $f(x_1, x_2, \ldots, x_k) = (x_1 \oplus \alpha_1) \cdot \ldots \cdot (x_k \oplus \alpha_k)$, $x_i, \alpha_i \in \{0, 1\}$, $i = \overline{1, n}$, *тоді:*

$$wt(f(x_1, x_2, \ldots, x_k)) = 1.$$

Доведення. Розглянемо таке рівняння:

$$(x_1 \oplus \alpha_1) \cdot (x_2 \oplus \alpha_2) \cdot \ldots \cdot (x_k \oplus \alpha_k) = 1. \tag{2.2}$$

З властивостей функції логічного ТА випливає, що рівняння (2.2) може бути переписане у вигляді системі лінійних рівнянь:

$$\begin{cases} x_1 \oplus \alpha_1 = 1 \\ x_2 \oplus \alpha_2 = 1 \\ \ldots \\ x_k \oplus \alpha_k = 1 \end{cases} \iff \begin{cases} x_1 = \alpha_1 \oplus 1 \\ x_2 = \alpha_2 \oplus 1 \\ \ldots \\ x_k = \alpha_k \oplus 1 \end{cases}$$

Тобто існує єдиний вектор $(y_1, y_2, \ldots, y_k) \in V_k$:

$$(y_1, y_2, \ldots, y_k) = (\alpha_1 \oplus 1, \alpha_2 \oplus 1, \ldots, \alpha_k \oplus 1),$$

такий, що $f(y_1, y_2, \ldots, y_k) = 1$, звідки й випливає рівність:

$$wt(f(x_1, x_2, \ldots, x_k)) = 1,$$

яка й доводить лему. □

Для більш компактного запису також можна ввести позначення x^α, $x, \alpha \in \{0, 1\}$:

$$x^\alpha = \begin{cases} x, \alpha = 0; \\ \overline{x}, \alpha = 1. \end{cases}$$

Це позначення легко узагальнюється і для багатобітових векторів:

$$x^\alpha = \left(x_{n-1}^{\alpha_{n-1}}, x_{n-2}^{\alpha_{n-2}}, \ldots, x_0^{\alpha_0}\right);\ x, \alpha \in V_n.$$

Теорема 2.2. *Нехай* $f(x_1, x_2, \ldots, x_k) = x_1 x_2 \cdot \ldots \cdot x_k$, $k \geqslant 2$, $x_i \in V_n$, *тоді для довільних* $\alpha_1, \ldots, \alpha_k, \gamma \in V_n$*:*

1) $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) \neq 0 \iff \overline{\alpha_1} \cdot \ldots \cdot \overline{\alpha_k} \cdot \gamma = 0$*;*

2) якщо $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) \neq 0$, *то:*

$$xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) = \left(\frac{1}{2^{k-1}}\right)^{wt(\alpha_1 \vee \ldots \vee \alpha_k)} \cdot \left(2^{k-1} - 1\right)^{wt((\alpha_1 \vee \ldots \vee \alpha_k) \wedge \overline{\gamma})}.$$

Доведення. Оскільки усі використані операції виконуються побітово, то ймовірності розглядатимуться для деякого i-того біту, а далі, користуючись незалежністю бітів, ми отримаємо відповідні ймовірності для усіх бітів. Для спрощення викладок порядковий індекс біту не вказуватиметься, тобто запис $x_1 \oplus x_2$ означатиме бітове додавання лише i-тих бітів векторів x_1 та x_2.

Формула для обчислення диференціальної ймовірності k-кратного застосування операції логічного ТА за операцією побітового додавання $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma)$ має такий вид:

$$\Pr_{x_1, x_2, \ldots, x_k}\{(x_1 \oplus \alpha_1)(x_2 \oplus \alpha_2)\ldots(x_k \oplus \alpha_k) = x_1 x_2 \ldots x_k \oplus \gamma\} =$$
$$= \Pr_{x_1, x_2, \ldots, x_k}\left\{\underbrace{x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}}_{f_2} = \underbrace{x_1 x_2 \ldots x_k}_{f_1} \oplus \gamma\right\} \quad (2.3)$$

Розділимо обчислення ймовірності (2.3) на два випадки, в залежності від значення γ. При $\gamma = 0$ потрібно проаналізувати, коли виконується наступна подія:

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} = x_1 x_2 \ldots x_k \,(f_2 = f_1). \quad (2.4)$$

Одразу видно, що при $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$ подія (2.4) перетворюється на тривіальну:

$$\Pr_{x_1, \ldots, x_k}\{x_1 x_2 \ldots x_k = x_1 x_2 \ldots x_k\} = 1,$$

інакше, з леми 2.1 випливає, що

$$\begin{cases} \exists! \left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right) : f_2\left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right) = 1; \\ \left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right) \neq (1, 1, \ldots, 1) = 1^k, \end{cases}$$

тобто для всіх бітових векторів $(y_1, y_2, \ldots, y_k) \in V_k$, які не дорівнюють $\left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right)$ та $\underbrace{(1, 1, \ldots, 1)}_{k}$, справедливе таке рівняння:

$$f_1(y_1, y_2, \ldots, y_k) = f_2(y_1, y_2, \ldots, y_k) = 0.$$

Таким чином, при $\gamma = 0$ ймовірність (2.3) приймає вигляд:

$$\begin{aligned} &\Pr_{x_1, x_2, \ldots, x_k}\left\{x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} = x_1 x_2 \ldots x_k\right\} = \\ &\qquad = \begin{cases} \frac{2^k - 2}{2^k} = \frac{2^{k-1} - 1}{2^{k-1}}, & (\alpha_1, \alpha_2, \ldots, \alpha_k) \neq (0, 0, \ldots, 0); \\ 1, & (\alpha_1, \alpha_2, \ldots, \alpha_k) = (0, 0, \ldots, 0). \end{cases} \end{aligned} \tag{2.5}$$

Якщо ж $\gamma = 1$, то потрібно проаналізувати ймовірність такої події:

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} = x_1 x_2 \ldots x_k \oplus 1 \ \ (f_2 = f_1 \oplus 1). \tag{2.6}$$

Одразу видно, що при $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$ подія (2.6) перетворюється на неможливу:

$$\Pr_{x_1, \ldots, x_k}\left\{x_1 x_2 \ldots x_k = x_1 x_2 \ldots x_k \oplus 1\right\} = 0,$$

інакше, з леми 2.1 випливає, що

$$\begin{cases} \exists! \left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) : f_2\left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) = 1; \\ \left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) \neq (1, 1, \ldots, 1) = 1^k, \end{cases}$$

отже лише для двох векторів значення функцій f_2 та $f_1 \oplus 1$ будуть мати

однакові значення:

$$\begin{cases} f_1\left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) \oplus 1 = 1; \\ f_2\left(1, 1, \ldots, 1\right) = f_1\left(1, 1, \ldots, 1\right) = 0. \end{cases}$$

Таким чином, при $\gamma = 1$ ймовірність (2.3) приймає вигляд:

$$\begin{aligned} &\Pr_{x_1,x_2,\ldots,x_k}\left\{x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_k^{\alpha_k} = x_1x_2\ldots x_k \oplus 1\right\} = \\ &\qquad = \begin{cases} \frac{2}{2^k} = \frac{1}{2^{k-1}}, & (\alpha_1, \alpha_2, \ldots, \alpha_k) \neq (0, 0, \ldots, 0); \\ 0, & (\alpha_1, \alpha_2, \ldots, \alpha_k) = (0, 0, \ldots, 0). \end{cases} \end{aligned} \tag{2.7}$$

Отже нульова ймовірність досягається лише за умови, коли $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$ та $\gamma = 1$, тому $xdp^f\left(\alpha_1, \ldots, \alpha_k \to \gamma\right) > 0$ тоді та тільки тоді, коли ця умова не виконується для жодного біту, що еквівалентно виконанню такої рівності:

$$\overline{\alpha_1} \cdot \overline{\alpha_2} \cdot \ldots \cdot \overline{\alpha_k} \cdot \gamma = 0.$$

Якщо ж $xdp^f\left(\alpha_1, \ldots, \alpha_k \to \gamma\right) > 0$, то, відштовхуючись від обчислених імовірностей (2.5) та (2.7) для окремих бітів, отримуємо шукану ймовірність:

$$\begin{aligned} &xdp^f\left(\alpha_1, \ldots, \alpha_k \to \gamma\right) = \\ &\qquad = \left(\frac{2^{k-1}-1}{2^{k-1}}\right)^{wt((\alpha_1 \vee \ldots \vee \alpha_k) \wedge \overline{\gamma})} \left(\frac{1}{2^{k-1}}\right)^{wt((\alpha_1 \vee \ldots \vee \alpha_k) \wedge \gamma)} = \\ &\qquad\qquad = \left(\frac{1}{2^{k-1}}\right)^{wt(\alpha_1 \vee \ldots \vee \alpha_k)} \left(2^{k-1}-1\right)^{wt((\alpha_1 \vee \ldots \vee \alpha_k) \wedge \overline{\gamma})}, \end{aligned}$$

що й доводить теорему. □

2.3 Імовірності диференціалів для нелінійних функцій від двох аргументів

Особливістю операції логічного ТА є те, що усі інші нелінійні двійкові операції від двох аргументів (а саме $\Omega_\star = \{\wedge, \vee, |, \downarrow, \rightarrow, \leftarrow\}$) можна виразити через неї. Також виявилося, що їхні диференціальні ймовірності є пов'язаними, і цей факт теж був досліджений спільно з Сергієм Яковлєвим [37], але для доведення цього твердження потрібно сформулювати ряд допоміжних лем — слід зазначити, що ми не претендуємо на їхнє авторство, адже ці міркування очевидним чином випливають з означень, проте введення цих лем є необхідним для формального доведення надалі сформульованих тверджень та теорем.

Лема 2.2. *Нехай* $f : (V_n)^k \to V_n$ *— довільна булева функція,* $n, k \in V_n$*, тоді для довільних* $\alpha_1, \alpha_2, \ldots, \alpha_k, \gamma \in V_n$ *справедлива така рівність:*

$$xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) = xdp^{f\oplus 1}(\alpha_1, \ldots, \alpha_k \to \gamma).$$

Доведення. Зафіксуємо деяку функцію f та розглянемо ймовірність диференціалу $(\alpha_1, \ldots, \alpha_k \to \gamma)$ для функції $g = f \oplus 1$:

$$xdp^g(\alpha_1, \ldots, \alpha_k \to \gamma) =$$
$$= \Pr_{x_1,x_2,\ldots,x_k}\{g(x_1 \oplus \alpha_1, x_2 \oplus \alpha_2, \ldots, x_k \oplus \alpha_k) = g(x_1, x_2, \ldots, x_k) \oplus \gamma\} \tag{2.8}$$

Підставивши $f \oplus 1$ в обидві частини підімовірнісного рівняння (2.8) замість g, отримаємо:

$$\Pr_{x_1,x_2,\ldots,x_k}\{f(x_1 \oplus \alpha_1, x_2 \oplus \alpha_2, \ldots, x_k \oplus \alpha_k) \oplus 1 = \\ = f(x_1, x_2, \ldots, x_k) \oplus 1 \oplus \gamma\},$$

а це дорівнює $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma)$, що й треба було довести. □

Не лише заперечення результату виконання функції, а й заперечення окремих аргументів функції теж не змінює її диференціальних ймовірностей.

Лема 2.3. *Нехай* $f : (V_n)^k \to V_n$ *— довільна булева функція,* $n, k \in V_n$*,* I *— одиничний вектор довжини* n*, тоді для довільних* $\alpha_1, \alpha_2, \ldots, \alpha_k, \gamma \in V_n$ *та функції* $g = f(x_1 \oplus I^{a_1}, x_2 \oplus I^{a_2}, \ldots, x_k \oplus I^{a_k})$*,* $a_i \in \{0, 1\}$*, справедлива така рівність:*

$$xdp^g(\alpha_1, \ldots, \alpha_k \to \gamma) = xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma).$$

Доведення. Зафіксуємо деяку функцію f та розглянемо ймовірність диференціалу $(\alpha_1, \ldots, \alpha_k \to \gamma)$ для функції g:

$$xdp^g(\alpha_1, \ldots, \alpha_k \to \gamma) =$$
$$= \Pr_{x_1, x_2, \ldots, x_k}\{g(x_1 \oplus \alpha_1, x_2 \oplus \alpha_2, \ldots, x_k \oplus \alpha_k) = g(x_1, x_2, \ldots, x_k) \oplus \gamma\} \tag{2.9}$$

Скориставшись взаємо'язком функції g з функцією f, з рівняння (2.9) отримаємо:

$$\Pr_{x_1, x_2, \ldots, x_k}\{f(x_1 \oplus I^{a_1} \oplus \alpha_1, x_2 \oplus I^{a_2} \oplus \alpha_2, \ldots, x_k \oplus I^{a_k} \oplus \alpha_k) =$$
$$= f(x_1 \oplus I^{a_1}, x_2 \oplus I^{a_2}, \ldots, x_k \oplus I^{a_k}) \oplus \gamma\} \tag{2.10}$$

Введемо k нових змінних $\widetilde{x_i} = x_i \oplus I^{a_i}$, $i \in \overline{1, k}$, тоді ймовірність (2.10) можна переписати як:

$$\Pr_{\widetilde{x_1}, \widetilde{x_2}, \ldots, \widetilde{x_k}}\{f(\widetilde{x_1} \oplus \alpha_1, \widetilde{x_2} \oplus \alpha_2, \ldots, \widetilde{x_k} \oplus \alpha_k) = f(\widetilde{x_1}, \widetilde{x_2}, \ldots, \widetilde{x_k}) \oplus \gamma\},$$

а це дорівнює $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma)$, що й треба було довести. □

Тепер ми можемо сформулювати твердження про зв'язок диференціальних ймовірностей булевих нелінійних перетворень від двох змінних з імовірностями диференціалів функції логічного ТА.

Твердження 2.1. *Для будь-яких* $\alpha, \beta, \gamma \in V_n$ *справедливі рівності*

$$xdp^{\star}(\alpha, \beta \to \gamma) = xdp^{\wedge}(\alpha, \beta \to \gamma),$$

де $\star \in \Omega_{\star}$.

Доведення. Таблицею істинності легко перевірити, що усі нелінійні функції від двох аргументів можна представити через логічне ТА:

$$\begin{aligned} x \vee y &= \overline{\overline{x} \wedge \overline{y}}, \\ x \mid y &= \overline{x \wedge y}, \\ x \downarrow y &= \overline{\overline{x} \wedge \overline{y}}, \\ x \to y &= \overline{x \wedge \overline{y}}, \\ x \leftarrow y &= \overline{\overline{x} \wedge y}. \end{aligned}$$

Користуючись 2.2 та 2.3, які стверджують, що всі перетворення, отримані через заперечення результату деякої функції, або заперечення аргументів функції, будуть еквівалентними цій функції в сенсі значення ймовірностей диференціалів, можна зробити висновок, що диференціальні ймовірності усіх нелінійних функцій від двох аргументів є однаковими. □

2.4 Імовірності диференціалів нелінійних кубічних функцій спеціального виду

Якщо розглянути перетворення такого виду:

$$\begin{aligned} g_{\circ,\bullet}(x, y, z) &= (x \circ y) \bullet z; \\ h_{\circ,\bullet}(x, y, z) &= x \circ (y \bullet z), \end{aligned}$$

де $\circ, \bullet \in \Omega_{\star}$, то ймовірності їхніх диференціалів, як і в твердженні 2.1, можуть бути виражені через диференціальні ймовірності

функції $f(x,y,z) = xyz$, але для доведення цього твердження нам знадобиться допоміжна лема.

Лема 2.4. *Нехай* $f : (V_n)^k \to V_n$ *— довільна булева функція,* $n,k \in V_n$, $g(x_1,x_2,\ldots,x_k) = f(x_1,x_2,\ldots,x_k) \oplus l(x_1,x_2,\ldots,x_k)$, *де* $l(x_1,x_2,\ldots,x_k)$ *— деяка лінійна за операцією* $\oplus$ *функція, тоді для довільних* $\alpha_1,\alpha_2,\ldots,\alpha_k,\gamma \in V_n$ *справедлива така рівність:*

$$xdp^g(\alpha_1,\ldots,\alpha_k \to \gamma) = xdp^f(\alpha_1,\ldots,\alpha_k \to \gamma \oplus l(\alpha_1,\alpha_2,\ldots,\alpha_k)).$$

Доведення. Зафіксуємо деяку функцію f, тоді ймовірність диференціалу $(\alpha_1,\ldots,\alpha_k \to \gamma)$ для функції g має вид:

$$xdp^g(\alpha_1,\ldots,\alpha_k \to \gamma) = \\ = \Pr_{x_1,x_2,\ldots,x_k}\{g(x_1\oplus\alpha_1, x_2\oplus\alpha_2,\ldots,x_k\oplus\alpha_k) = g(x_1,x_2,\ldots,x_k)\oplus\gamma\}. \quad (2.11)$$

Перепишемо підімовірнісне рівняння виразу (2.9) через функцію f:

$$f(x_1\oplus\alpha_1, x_2\oplus\alpha_2,\ldots,x_k\oplus\alpha_k) \oplus l(x_1\oplus\alpha_1, x_2\oplus\alpha_2,\ldots,x_k\oplus\alpha_k) = \\ = f(x_1,x_2,\ldots,x_k) \oplus l(x_1,x_2,\ldots,x_k) \oplus \gamma. \quad (2.12)$$

Оскільки функція l — лінійна, то:

$$l(x_1\oplus\alpha_1, x_2\oplus\alpha_2,\ldots,x_k\oplus\alpha_k) = \\ = l(x_1,x_2,\ldots,x_k) \oplus l(\alpha_1,\alpha_2,\ldots,\alpha_k). \quad (2.13)$$

Користуючись властивістю 2.13, з рівняння 2.12 отримуємо, що

$$f(x_1\oplus\alpha_1, x_2\oplus\alpha_2,\ldots,x_k\oplus\alpha_k) = f(x_1,x_2,\ldots,x_k) \oplus l(\alpha_1,\alpha_2,\ldots,\alpha_k) \oplus \gamma.$$

Тепер, повертаючись до рівняння (2.11), одержуємо шукану

ймовірність:

$$\begin{aligned}\Pr_{x_1,x_2,\ldots,x_k}\{f(x_1\oplus\alpha_1,x_2\oplus\alpha_2,\ldots,x_k\oplus\alpha_k)=\\ =f(x_1,x_2,\ldots,x_k)\oplus l(\alpha_1,\alpha_2,\ldots,\alpha_k)\oplus\gamma\}=\\ =xdp^f(\alpha_1,\alpha_2,\ldots,\alpha_k\to\gamma\oplus l(\alpha_1,\alpha_2,\ldots,\alpha_k)).\end{aligned}$$

□

Тепер ми можемо сформулювати теорему про зв'язок ймовірностей диференціалів кубічних функцій спеціального виду з множини Φ та 3-кратного логічного ТА, де

$$\Phi=\{g_{\circ,\bullet}(x,y,z)=(x\circ y)\bullet z, h_{\circ,\bullet}(x,y,z)=x\circ(y\bullet z)\mid\circ,\bullet\in\Omega_\star\}.$$

Теорема 2.3. *Нехай $f_1=xyz$, $f_2=xyz\oplus z$, $f_3=xyz\oplus x$, тоді для довільних $\alpha,\beta,\delta,\gamma\in V_n$, $f\in\Phi$:*

$$xdp^f(\alpha,\beta,\delta\to\gamma)=\begin{cases}xdp^{f_1}(\alpha,\beta,\delta\to\gamma)=\left(\frac{1}{4}\right)^{wt(\alpha\vee\beta\vee\delta)}\cdot 3^{wt(\alpha\vee\beta\vee\delta)\wedge\gamma};\\ xdp^{f_2}(\alpha,\beta,\delta\to\gamma)=\left(\frac{1}{4}\right)^{wt(\alpha\vee\beta\vee\delta)}\cdot 3^{wt(\alpha\vee\beta\vee\delta)\wedge(\gamma\oplus\delta)};\\ xdp^{f_3}(\alpha,\beta,\delta\to\gamma)=\left(\frac{1}{4}\right)^{wt(\alpha\vee\beta\vee\delta)}\cdot 3^{wt(\alpha\vee\beta\vee\delta)\wedge(\gamma\oplus\alpha)}.\end{cases}$$

Доведення. Емпіричним методом було встановленно, що розбиття множини Φ складається з трьох класів, «базисними» функціями для яких є f_1, f_2 та f_3. Усі три класи, та функції, що вони містять, наведено в таблицях А.1, А.2 та А.3. Покажемо процес зведення деяких перетворень з кожного класу до «базисної» функції, щоб показати, що перетворення в цих класах дійсно мають однакові диференціальні ймовірності:

1. $f_1=xyz$**:**

- $g_1(x,y,z)=(x\mid y)\downarrow z=xyz\oplus xy=xy\overline{z}=f_1(x,y,\overline{z})$,

звідки з леми 2.3 випливає, що $xdp^{g_1}(\alpha,\beta,\delta\to\gamma)=xdp^{f_1}(\alpha,\beta,\delta\to\gamma)$;

- $g_2(x,y,z) = x \mid (y \downarrow z)$:

$$g_2(x,y,z) = xyz \oplus xy \oplus xz \oplus x \oplus 1 = \\ = x(y \oplus 1)(z \oplus 1) \oplus 1 = f_1(x, \overline{y}, \overline{z}) \oplus 1,$$

звідки з лем 2.2 та 2.3 випливає, що $xdp^{g_2}(\alpha, \beta, \delta \to \gamma) = xdp^{f_1}(\alpha, \beta, \delta \to \gamma)$.

2. $f_2 = xyz \oplus z = \overline{xy} \cdot z$**:**

- $g_3(x,y,z) = (x \wedge y) \vee z$:

$$g_3(x,y,z) = \overline{xy} \cdot z \oplus xy = \overline{xy} \cdot z \oplus \overline{xy} \oplus 1 = \\ = \overline{xy} \cdot \overline{z} \oplus 1 = f_2(x,y,\overline{z}) \oplus 1,$$

звідки з лем 2.2 та 2.3 випливає, що $xdp^{g_3}(\alpha, \beta, \delta \to \gamma) = xdp^{f_2}(\alpha, \beta, \delta \to \gamma)$;

- $g_4(x,y,z) = (x \downarrow y) \downarrow z$:

$$g_4(x,y,z) = z(xy \oplus x \oplus y) \oplus (xy \oplus x \oplus y) = \\ = (xy \oplus x \oplus y)(z \oplus 1) = (x \vee y)\overline{z} = \\ = \overline{\overline{x} \cdot \overline{y}} \cdot \overline{z} = f_2(\overline{x}, \overline{y}, \overline{z}),$$

звідки з леми 2.3 випливає, що $xdp^{g_4}(\alpha, \beta, \delta \to \gamma) = xdp^{f_2}(\alpha, \beta, \delta \to \gamma)$.

3. $f_3 = xyz \oplus x = x \cdot \overline{yz}$**:**

- $g_5(x,y,z) = x \mid (y \vee z)$:

$$g_5(x,y,z) = xyz \oplus xy \oplus xz \oplus 1 = x(yz \oplus y \oplus z) \oplus 1 = \\ = x(y \vee z) \oplus 1 = x \cdot \overline{\overline{y} \cdot \overline{z}} \oplus 1 = f_3(x, \overline{y}, \overline{z}) \oplus 1,$$

звідки з лем 2.2 та 2.3 випливає, що $xdp^{g_5}(\alpha, \beta, \delta \to \gamma) = xdp^{f_3}(\alpha, \beta, \delta \to \gamma)$.

Застосувавши ці міркування для решти функцій можна показати, що

для довільних $\alpha, \beta, \delta, \gamma \in V_n,\ f \in \Phi$:

$$xdp^f(\alpha, \beta, \delta \to \gamma) = \begin{bmatrix} xdp^{f_1}(\alpha, \beta, \delta \to \gamma); \\ xdp^{f_2}(\alpha, \beta, \delta \to \gamma); \\ xdp^{f_3}(\alpha, \beta, \delta \to \gamma). \end{bmatrix}$$

Користуючись теоремою 2.2, отримуємо

$$xdp^{f_1}(\alpha, \beta, \delta \to \gamma) = \left(\frac{1}{4}\right)^{wt(\alpha \vee \beta \vee \delta)} \cdot 3^{wt(\alpha \vee \beta \vee \delta) \wedge \gamma}.$$

В свою чергу, $f_2(x, y, z) = f_1(x, y, z) \oplus z$, що дозволяє нам скористатись лемою 2.4 для отримання її диференціальних імовірностей:

$$xdp^{f_2}(\alpha, \beta, \delta \to \gamma) = xdp^{f_1}(\alpha, \beta, \delta \to \gamma \oplus \delta) = \left(\frac{1}{4}\right)^{wt(\alpha \vee \beta \vee \delta)} \cdot 3^{wt(\alpha \vee \beta \vee \delta) \wedge (\gamma \oplus \delta)}.$$

Аналогічні міркування застосовуємо і до $f_3(x, y, z) = f_1(x, y, z) \oplus x$, та отримуємо:

$$xdp^{f_3}(\alpha, \beta, \delta \to \gamma) = xdp^{f_1}(\alpha, \beta, \delta \to \gamma \oplus \alpha) = \left(\frac{1}{4}\right)^{wt(\alpha \vee \beta \vee \delta)} \cdot 3^{wt(\alpha \vee \beta \vee \delta) \wedge (\gamma \oplus \alpha)}.$$

□

Кілька диференціалів та їхні відповідні ймовірності для кожного класу для чотирьох-бітових перетворень наведемо в таблиці 2.2.

2.5 Диференціальні ймовірності функції мажоризації

Функція мажоризації $maj : (V_n)^3 \to V_n$ — це бітова функція від трьох аргументів:

$$maj(x, y, z) = xy \oplus yz \oplus xz.$$

Таблиця 2.2 – Диференціали та їх ймовірності для кубічних функції

Диференціал	p_{f_1}	p_{f_2}	p_{f_3}
$(\texttt{0x0}, \texttt{0x8}, \texttt{0x0} \to \texttt{0x8})$	0.75	0.25	0.75
$(\texttt{0x4}, \texttt{0x5}, \texttt{0x0} \to \texttt{0x5})$	0.5625	0.0625	0.1875
$(\texttt{0x1}, \texttt{0x0}, \texttt{0x1} \to \texttt{0x1})$	0.25	0.75	0.75
$(\texttt{0x1}, \texttt{0x0}, \texttt{0x2} \to \texttt{0x2})$	0.1875	0.5625	0.0625
$(\texttt{0x3}, \texttt{0x0}, \texttt{0x3} \to \texttt{0x1})$	0.0625	0.1875	0.5625
$(\texttt{0x1}, \texttt{0xD}, \texttt{0x1} \to \texttt{0x1})$	0.140625	0.421875	0.421875

Таблиця 2.3 – Таблиця істинності для функції мажоризації

x	y	z	$maj(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Функція мажоризації володіє рядом криптографічних особливостей: з її таблиці істинності 2.3 одразу видно, що вона є збалансованою, і ця властивість ускладнює проведення кореляційних атак. Також було доведено, що ця функція володіє оптимальною алгебраїчною імунністю [27], що, в свою чергу, ускладнює проведення алгебраїчних атак.

Хоча саме ці властивості розглядаються в першу чергу при виборі фільтрувальної функції для потокових шифрів (які зазвичай і є об'єктами кореляційних та алгебраїчних атак), функція мажоризації все ж рідко використовується в якості фільтрувальної функції через її не найвищий показний нелінійності [14]. Тим не менше, попри це вона була

використана в шифрі A5/1 [3]; в сучасних потокових криптосистемах її якщо й використовують, то хіба що в комбінації з іншими функціями, прикладом може слугувати шифр ACORN [36] (учасник конкурсу CAESAR). Окрім потокових шифрів, функція мажоризації використовується й у стандартах гешування SHA-1 та SHA-2 [31], а також в блоковому шифрі SHACAL-2 [29], який є фіналістом конкурсу NESSIE, та основою якого, власне, і являється SHA-2.

Властивості функції мажоризації роблять її кандидатом на використання в якості нелінійного перетворення в LRX-криптосистемах, тому сформулюємо теорему про її диференціальні ймовірності.

Теорема 2.4. *Для довільних* $\alpha, \beta, \delta, \gamma \in V_n$ *справедливі такі твердження:*

1) $xdp^{maj}(\alpha, \beta, \delta \to \gamma) \neq 0 \iff eq(\alpha, \beta, \delta, \overline{\gamma}) = 0$;

2) $xdp^{maj}(\alpha, \beta, \delta \to \gamma) \neq 0$, *то*

$$xdp^{maj}(\alpha, \beta, \delta \to \gamma) = \left(\frac{1}{2}\right)^{n - wt(eq(\alpha,\beta,\delta))}.$$

Доведення. Ймовірність диференціалу $xdp^{maj}(\alpha, \beta, \delta \to \gamma)$ має такий вид:

$$\Pr_{x,y,z}\{(x \oplus \alpha)(y \oplus \beta) \oplus (y \oplus \beta)(z \oplus \delta) \oplus (x \oplus \alpha)(z \oplus \delta) = \\ = xy \oplus yz \oplus xz \oplus \gamma\}.$$

Розглянемо i-тий біт підімовірнісного рівняння:

$$(x_i \oplus \alpha_i)(y_i \oplus \beta_i) \oplus (y_i \oplus \beta_i)(z_i \oplus \delta_i) \oplus (x_i \oplus \alpha_i)(z_i \oplus \delta_i) = \\ = x_i y_i \oplus y_i z_i \oplus x_i z_i \oplus \gamma_i,$$

розкривши дужки отримаємо:

$$x_i y_i \oplus \beta_i x_i \oplus \alpha_i y_i \oplus \alpha_i \beta_i \oplus y_i z_i \oplus \delta_i y_i \oplus \beta_i z_i \oplus$$
$$\oplus \beta_i \delta_i \oplus x_i z_i \oplus \delta_i x_i \oplus \alpha_i z_i \oplus \alpha_i \delta_i =$$
$$= x_i y_i \oplus y_i z_i \oplus x_i z_i \oplus \gamma_i,$$

звідки випливає, що

$$(\beta_i \oplus \delta_i)\, x_i \oplus (\alpha_i \oplus \delta_i)\, y_i \oplus (\alpha_i \oplus \beta_i)\, z_i = \alpha_i \beta_i \oplus \beta_i \delta_i \oplus \alpha_i \delta_i \oplus \gamma. \qquad (2.14)$$

Позначимо символом p_i імовірність виконання рівняння (2.14), значення p_i для всіх можливих наборів $\alpha_i, \beta_i, \delta_i, \gamma_i$ наведені у таблиці 2.4.

Таблиця 2.4 – Імовірності p_i виконання рівняння (2.14).

α_i	β_i	δ_i	γ_i	рівняння	p_i
0	0	0	0	$0 = 0$	1
0	0	0	1	$0 = 1$	0
0	0	1	0	$x_i \oplus y_i = 0$	1/2
0	0	1	1	$x_i \oplus y_i = 1$	1/2
0	1	0	0	$x_i \oplus z_i = 0$	1/2
0	1	0	1	$x_i \oplus z_i = 1$	1/2
0	1	1	0	$y_i \oplus z_i = 1$	1/2
0	1	1	1	$y_i \oplus z_i = 0$	1/2
1	0	0	0	$y_i \oplus z_i = 0$	1/2
1	0	0	1	$y_i \oplus z_i = 1$	1/2
1	0	1	0	$x_i \oplus z_i = 1$	1/2
1	0	1	1	$x_i \oplus z_i = 0$	1/2
1	1	0	0	$x_i \oplus y_i = 1$	1/2
1	1	0	1	$x_i \oplus y_i = 0$	1/2
1	1	1	0	$0 = 1$	0
1	1	1	1	$0 = 0$	1

З таблиці 2.4 бачимо, що ймовірність p_i дорівнює нулю тоді та

тільки тоді, коли $\alpha_i = \beta_i = \delta_i = \overline{\gamma_i}$, тому, якщо хоча б один біт у векторі $eq\,(\alpha, \beta, \delta, \overline{\gamma})$ є одиничним, то $xdp^{maj}\,(\alpha, \beta, \delta \to \gamma) = 0$, що доводить першу частину теореми.

Якщо $xdp^{maj}\,(\alpha, \beta, \delta \to \gamma) \neq 0$ та $\alpha_i = \beta_i = \delta_i$, то рівняння виконується завжди, інакше — з ймовірністю $1/2$, тому $xdp^{maj}\,(\alpha, \beta, \delta \to \gamma) = \left(\frac{1}{2}\right)^{n-k}$, де k — кількість одиничних бітів у векторі $eq\,(\alpha, \beta, \delta)$, з чого випливає друга частина теореми. □

Висновки до розділу 2

У даному розділі було переформульовано аналітичні вирази для функції логічного ТА, а також узагальнено цей результат для функції k-кратного логічного ТА. Також було показано, що усі інші нелінійні функції від двох аргументів можна звести до функції логічного ТА, й вони є еквівалентними в сенсі диференціальних ймовірностей.

Було розглянуто множину кубічних нелінійних функцій спеціального виду, проаналізовано її структуру, знайдено базисні елементи та одержано аналітичні вирази для ймовірностей диференціалів, а також встановлено зв'язок всіх цих виразів з диференціальними ймовірностями функції 3-кратного логічного ТА.

ВИСНОВКИ

У ході даної роботи було розглянуто сучасні ARX- та LRX-криптосистеми з акцентом на їхні нелінійні перетворення. Огляд існуючих криптосистем показав, що більшість LRX-перетворень використовують операцію логічного ТА (або деякі її ускладнення) в якості заміни додавання за модулем. Також було проаналізовано існуючі підходи й техніки до диференціального криптоаналізу ARX- та LRX-криптосистем, розглянуто підхід аналізу нестандартних диференціалів в роботі по криптоаналізу шифру `NORX`.

Було одержаного спрощені результати, еквівалентні вже існуючим, а саме ймовірності диференціалів для функції логічного ТА, проте виявилось, що цей результат ще й можна узагальнити для k-кратної функції логічного ТА.

Було розглянуто множину кубічних функцій спеціального виду, проаналізовано їхню структуру та зв'язок з функцією 3-кратного логічного ТА. Також було одержано аналітичні вирази ймовірності для функцій усіх класів, що розбивають цю множину, а також показано, як ці вирази зводяться до диференцільних ймовірностей 3-кратного логічного ТА.

Окрім цього, було розглянуто функцію мажоризації, її структуру та використання в криптографії. Також було одержано аналітичні вирази для її диференціальних ймовірностей.

Загалом, ймовірності диференціалів є основою, необхідною для проведення диференціального криптоаналізу, оскільки саме з їхньою допомогою шукаються високоймовірні диференціальні характеристики, які, в свою чергу, використовуються для побудови атак, тому знаходження диференціальних ймовірностей для перспективних LRX-перетворень має сенс, оскільки напрямок LRX-криптосистем лише починає свій розвиток.

Подальші дослідження можуть як продовжити існуючий шлях, тобто розгляд ще більш різноманітних LRX-перетворень, зокрема з залученням бітового зсуву (як циклічного, так і нециклічного), тому що такі перетворення в цій роботі не були розглянуті, так і більш практичні, такі як створення нових LRX-криптосистем, нелінійне перетворення яких буде обрано з врахуванням отриманих в цій роботі результатів.

ПЕРЕЛІК ПОСИЛАНЬ

[1] J.-P. Aumasson, P. Jovanovic та S. Neves. *Analysis of NORX: Investigating Differential and Rotational Properties*. Англ. 2014. DOI: 10.1007/978-3-319-16295-9_17. URL: https://eprint.iacr.org/2014/317.

[2] J.-P. Aumasson, P. Jovanovic та S. Neves. *Norx v3.0*. Англ. 2016. DOI: 10.1145/2744769.2747946. URL: https://competitions.cr.yp.to/round3/norxv30.pdf.

[3] E. Barkan, E. Biham та N. Keller. *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*. Англ. 2003. DOI: https://doi.org/10.1007/978-3-540-45146-4_35.

[4] R. Beaulieu та ін. *The SIMON and SPECK Families of Lightweight Block Ciphers*. Англ. 2013. DOI: 10.1145/2744769.2747946. URL: https://eprint.iacr.org/2013/404.

[5] E. Bellini та ін. *Monte Carlo Tree Search for automatic differential characteristics search: application to SPECK*. Англ. 2024. DOI: 10.1007/978-3-031-22912-1_17. URL: https://eprint.iacr.org/2024/126.

[6] E. Biham та A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Англ. 1993. DOI: 10.1007/978-1-4613-9314-6.

[7] A. Biryukov, A. Roy та V. Velichkov. *Differential Analysis of Block Ciphers SIMON and SPECK*. Англ. 2014. DOI: 10.1007/978-3-662-46706-0_28. URL: https://eprint.iacr.org/2014/922.

[8] A. Biryukov та V. Velichkov. *Automatic Search for Differential Trails in ARX Ciphers*. Англ. 2013. DOI: 10.1007/978-3-319-04852-9_12. URL: https://eprint.iacr.org/2013/853.

[9] *CAESAR submissions*. Англ. 2019. URL: https://competitions.cr.yp.to/caesar.html.

[10] H. Chen та X. Wang. *Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques*. Англ. 2015. URL: https://eprint.iacr.org/2015/666.

[11] Y. Chen, Z. Bao та H. Yu. *Differential-Linear Approximation Semi-Unconstrained Searching and Partition Tree: Application to LEA and Speck*. Англ. 2023. DOI: 10.1007/978-981-99-8727-6_8. URL: https://eprint.iacr.org/2023/1414.

[12] A. R. Choudhuri та S. Maitra. *Differential Cryptanalysis of Salsa and ChaCha – An Evaluation with a Hybrid Model*. Англ. 2016. URL: https://eprint.iacr.org/2016/377.

[13] Don Coppersmith. *The Data Encryption Standard (DES) and its strength against attacks*. Англ. 1994. DOI: 10.1147/rd.383.0243.

[14] T. W. Cusick. *Simpler proof for nonlinearity of majority function*. Англ. 2017. DOI: 10.1016/j.dam.2021.02.031. eprint: arXiv:1710.02034. URL: https://arxiv.org/abs/1710.02034.

[15] Daniel J. Bernstein. *ChaCha, a variant of Salsa20*. Англ. 2005. URL: https://cr.yp.to/chacha/chacha-20080128.pdf.

[16] Daniel J. Bernstein. *Salsa20 specification*. Англ. 2005. URL: https://cr.yp.to/snuffle/spec.pdf.

[17] S. Dey, H. K. Garai та S. Maitra. *Cryptanalysis of Reduced Round ChaCha- New Attack and Deeper Analysis*. Англ. 2023. DOI: 10.46586/tosc.v2023.i1.89-110. URL: https://eprint.iacr.org/2023/134.

[18] S. Dey та ін. *Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha*. Англ. 2022. DOI: 10.1007/978-3-031-07082-2_4. URL: https://eprint.iacr.org/2022/536.

[19] C. Dobraunig та ін. *Ascon v1.2*. Англ. 2019. URL: https://ascon.iaik.tugraz.at/specification.html.

[20] A. D. Dwivedi та G. Srivastava. *Differential Cryptanalysis in ARX Ciphers with specific applications to LEA*. Англ. 2018. DOI: 10.1007/978-3-662-46706-0_28. URL: https://eprint.iacr.org/2018/898.

[21] *eSTREAM: the ECRYPT Stream Cipher Project*. Англ. 2008. URL: https://competitions.cr.yp.to/estream.html.

[22] Z. Feng та ін. *Improved Differential Cryptanalysis on SPECK Using Plaintext Structures*. Англ. 2023. URL: https://eprint.iacr.org/2023/566.

[23] Kai Hu. *Improved Conditional Cube Attacks on Ascon AEADs in Nonce-Respecting Settings – with a Break-Fix Strategy*. Англ. 2024. URL: https://eprint.iacr.org/2024/743.

[24] Z. Li, X. Dong та X. Wang. *Conditional Cube Attack on Round-Reduced ASCON*. Англ. 2017. DOI: 10.13154/tosc.v2017.i1.175-202. URL: https://eprint.iacr.org/2017/160.

[25] H. Lipmaa та S. Moriai. *Efficient Algorithms for Computing Differential Properties of Addition*. Англ. 2001. DOI: https://doi.org/10.1007/3-540-45473-X_28. URL: https://eprint.iacr.org/2001/001.

[26] S. Maitra, G. Paul та W. Meier. *Salsa20 Cryptanalysis: New Moves and Revisiting Old Styles*. Англ. 2015. URL: https://eprint.iacr.org/2015/217.

[27] Pierrick Méaux. *On the Fast Algebraic Immunity of Majority Functions*. Англ. 2019. DOI: 10.1007/978-3-030-30530-7_5. URL: https://eprint.iacr.org/2019/999.

[28] N. Mouha та B. Preneel. *Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20*. Англ. 2013. URL: https://eprint.iacr.org/2013/328.

[29] S. Murphy, B. Preneel та ін. *The NESSIE Book: Final Report of European Project IST-1999-12324*. Англ. 2004, с. 555—557. URL: https://pure.royalholloway.ac.uk/en/publications/the-nessie-book-final-report-of-european-project-ist-1999-12324.

[30] NIST. *Lightweight Cryptography*. Англ. 2022. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

[31] NIST. *Secure Hash Standard (SHS)*. Англ. 2015. DOI: 10.6028/NIST.FIPS.180-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[32] NIST. *Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process*. Англ. 2023. URL: https://doi.org/10.6028/NIST.IR.8454.

[33] L. Song, Z. Huang та Q. Yang. *Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA*. Англ. 2016. DOI: 10.1007/978-3-319-40367-0_24. URL: https://eprint.iacr.org/2016/209.

[34] Cihangir Tezcan. *Analysis of Ascon, DryGASCON, and Shamash Permutations*. Англ. 2020. URL: https://eprint.iacr.org/2020/1458.

[35] Cihangir Tezcan. *Truncated, Impossible, and Improbable Differential Analysis of Ascon*. Англ. 2016. DOI: 10.5220/0005689903250332. URL: https://eprint.iacr.org/2016/490.

[36] Hongjun Wu. *ACORN: A Lightweight Authenticated Cipher (v3)*. Англ. 2016. URL: https://competitions.cr.yp.to/round3/acornv3.pdf.

[37] В: *Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених*. За ред. С. М. Пономаренко та ін. КПІ ім. Ігоря Сікорського. Видавництво «Політехніка», трав. 2024, с. 198—201. ISBN: 978-966-990-053-1.

ДОДАТОК А ВЕЛИКІ РИСУНКИ ТА ТАБЛИЦІ

Таблиця А.1 – Клас f_1 нелінійних функцій, $f_1(x, y, z) = xyz$

Функція	АНФ	Зведена f_1 форма
$(x \wedge y) \wedge z$	xyz	$f_1(x, y, z)$
$(x \wedge y) \mid z$	$xyz \oplus 1$	$f_1(x, y, z) \oplus 1$
$(x \wedge y) \to z$	$xyz \oplus xy \oplus 1$	$f_1(x, y, \overline{z}) \oplus 1$
$(x \mid y) \vee z$	$xyz \oplus xy \oplus 1$	$f_1(x, y, \overline{z}) \oplus 1$
$(x \mid y) \downarrow z$	$xyz \oplus xy$	$f_1(x, y, \overline{z})$
$(x \mid y) \leftarrow z$	$xyz \oplus 1$	$f_1(x, y, z) \oplus 1$
$(x \vee y) \vee z$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z$	$f_1(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$(x \vee y) \downarrow z$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z \oplus 1$	$f_1(\overline{x}, \overline{y}, \overline{z})$
$(x \vee y) \leftarrow z$	$xyz \oplus xz \oplus yz \oplus z \oplus 1$	$f_1(\overline{x}, \overline{y}, z) \oplus 1$
$(x \downarrow y) \wedge z$	$xyz \oplus xz \oplus yz \oplus z$	$f_1(\overline{x}, \overline{y}, z)$
$(x \downarrow y) \mid z$	$xyz \oplus xz \oplus yz \oplus z \oplus 1$	$f_1(\overline{x}, \overline{y}, z) \oplus 1$
$(x \downarrow y) \to z$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z$	$f_1(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$(x \to y) \vee z$	$xyz \oplus xy \oplus xz \oplus x \oplus 1$	$f_1(x, \overline{y}, \overline{z}) \oplus 1$
$(x \to y) \downarrow z$	$xyz \oplus xy \oplus xz \oplus x$	$f_1(x, \overline{y}, \overline{z})$
$(x \to y) \leftarrow z$	$xyz \oplus xz \oplus 1$	$f_1(x, \overline{y}, z) \oplus 1$
$(x \leftarrow y) \vee z$	$xyz \oplus xy \oplus yz \oplus y \oplus 1$	$f_1(\overline{x}, y, \overline{z}) \oplus 1$
$(x \leftarrow y) \downarrow z$	$xyz \oplus xy \oplus yz \oplus y$	$f_1(\overline{x}, y, \overline{z})$
$(x \leftarrow y) \leftarrow z$	$xyz \oplus yz \oplus 1$	$f_1(\overline{x}, y, z) \oplus 1$
$x \wedge (y \wedge z)$	xyz	$f_1(x, y, z)$
$x \wedge (y \downarrow z)$	$xyz \oplus xy \oplus xz \oplus x$	$f_1(x, \overline{y}, \overline{z})$
$x \mid (y \wedge z)$	$xyz \oplus 1$	$f_1(x, y, z) \oplus 1$
$x \mid (y \downarrow z)$	$xyz \oplus xy \oplus xz \oplus x \oplus 1$	$f_1(x, \overline{y}, \overline{z}) \oplus 1$
$x \vee (y \mid z)$	$xyz \oplus yz \oplus 1$	$f_1(\overline{x}, y, z) \oplus 1$
$x \vee (y \vee z)$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z$	$f_1(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$x \vee (y \to z)$	$xyz \oplus xy \oplus yz \oplus y \oplus 1$	$f_1(\overline{x}, y, \overline{z}) \oplus 1$
$x \vee (y \leftarrow z)$	$xyz \oplus xz \oplus yz \oplus z \oplus 1$	$f_1(\overline{x}, \overline{y}, z) \oplus 1$
$x \downarrow (y \mid z)$	$xyz \oplus yz$	$f_1(\overline{x}, y, z)$
$x \downarrow (y \vee z)$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z \oplus 1$	$f_1(\overline{x}, \overline{y}, \overline{z})$
$x \downarrow (y \to z)$	$xyz \oplus xy \oplus yz \oplus y$	$f_1(\overline{x}, y, \overline{z})$
$x \downarrow (y \leftarrow z)$	$xyz \oplus xz \oplus yz \oplus z$	$f_1(\overline{x}, \overline{y}, z)$
$x \to (y \mid z)$	$xyz \oplus 1$	$f_1(x, y, z) \oplus 1$
$x \to (y \vee z)$	$xyz \oplus xy \oplus xz \oplus x \oplus 1$	$f_1(x, \overline{y}, \overline{z}) \oplus 1$
$x \to (y \to z)$	$xyz \oplus xy \oplus 1$	$f_1(x, y, \overline{z}) \oplus 1$
$x \to (y \leftarrow z)$	$xyz \oplus xz \oplus 1$	$f_1(x, \overline{y}, z) \oplus 1$
$x \leftarrow (y \wedge z)$	$xyz \oplus yz \oplus 1$	$f_1(\overline{x}, y, z) \oplus 1$
$x \leftarrow (y \downarrow z)$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z$	$f_1(\overline{x}, \overline{y}, \overline{z}) \oplus 1$

Таблиця А.2 – Клас f_2 нелінійних функцій, $f_2(x, y, z) = xyz \oplus z$

Функція	АНФ	Зведена f_2 форма
$(x \wedge y) \vee z$	$xyz \oplus xy \oplus z$	$f_2(x, y, \overline{z}) \oplus 1$
$(x \wedge y) \downarrow z$	$xyz \oplus xy \oplus z \oplus 1$	$f_2(x, y, \overline{z})$
$(x \wedge y) \leftarrow z$	$xyz \oplus z \oplus 1$	$f_2(x, y, z) \oplus 1$
$(x \mid y) \wedge z$	$xyz \oplus z$	$f_2(x, y, z)$
$(x \mid y) \mid z$	$xyz \oplus z \oplus 1$	$f_2(x, y, z) \oplus 1$
$(x \mid y) \rightarrow z$	$xyz \oplus xy \oplus z$	$f_2(x, y, \overline{z}) \oplus 1$
$(x \vee y) \wedge z$	$xyz \oplus xz \oplus yz$	$f_2(\overline{x}, \overline{y}, z)$
$(x \vee y) \mid z$	$xyz \oplus xz \oplus yz \oplus 1$	$f_2(\overline{x}, \overline{y}, z) \oplus 1$
$(x \vee y) \rightarrow z$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus 1$	$f_2(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$(x \downarrow y) \vee z$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus 1$	$f_2(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$(x \downarrow y) \downarrow z$	$xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y$	$f_2(\overline{x}, \overline{y}, \overline{z})$
$(x \downarrow y) \leftarrow z$	$xyz \oplus xz \oplus yz \oplus 1$	$f_2(\overline{x}, \overline{y}, z) \oplus 1$
$(x \rightarrow y) \wedge z$	$xyz \oplus xz \oplus z$	$f_2(x, \overline{y}, z)$
$(x \rightarrow y) \mid z$	$xyz \oplus xz \oplus z \oplus 1$	$f_2(x, \overline{y}, z) \oplus 1$
$(x \rightarrow y) \rightarrow z$	$xyz \oplus xy \oplus xz \oplus x \oplus z$	$f_2(x, \overline{y}, \overline{z}) \oplus 1$
$(x \leftarrow y) \wedge z$	$xyz \oplus yz \oplus z$	$f_2(\overline{x}, y, z)$
$(x \leftarrow y) \mid z$	$xyz \oplus yz \oplus z \oplus 1$	$f_2(\overline{x}, y, z) \oplus 1$
$(x \leftarrow y) \rightarrow z$	$xyz \oplus xy \oplus yz \oplus y \oplus z$	$f_2(\overline{x}, y, \overline{z}) \oplus 1$

Таблиця А.3 – Клас f_3 нелінійних функцій, $f_3(x, y, z) = xyz \oplus x$

Функція	АНФ	Зведена f_3 форма
$x \wedge (y \mid z)$	$xyz \oplus x$	$f_3(x, y, z)$
$x \wedge (y \vee z)$	$xyz \oplus xy \oplus xz$	$f_3(x, \overline{y}, \overline{z})$
$x \wedge (y \rightarrow z)$	$xyz \oplus xy \oplus x$	$f_3(x, y, \overline{z})$
$x \wedge (y \leftarrow z)$	$xyz \oplus xz \oplus x$	$f_3(x, \overline{y}, z)$
$x \mid (y \mid z)$	$xyz \oplus x \oplus 1$	$f_3(x, y, z) \oplus 1$
$x \mid (y \vee z)$	$xyz \oplus xy \oplus xz \oplus 1$	$f_3(x, \overline{y}, \overline{z}) \oplus 1$
$x \mid (y \rightarrow z)$	$xyz \oplus xy \oplus x \oplus 1$	$f_3(x, y, \overline{z}) \oplus 1$
$x \mid (y \leftarrow z)$	$xyz \oplus xz \oplus x \oplus 1$	$f_3(x, \overline{y}, z) \oplus 1$
$x \vee (y \wedge z)$	$xyz \oplus yz \oplus x$	$f_3(\overline{x}, y, z) \oplus 1$
$x \vee (y \downarrow z)$	$xyz \oplus xy \oplus xz \oplus yz \oplus y \oplus z \oplus 1$	$f_3(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$x \downarrow (y \wedge z)$	$xyz \oplus yz \oplus x \oplus 1$	$f_3(\overline{x}, y, z)$
$x \downarrow (y \downarrow z)$	$xyz \oplus xy \oplus xz \oplus yz \oplus y \oplus z$	$f_3(\overline{x}, \overline{y}, \overline{z})$
$x \rightarrow (y \wedge z)$	$xyz \oplus x \oplus 1$	$f_3(x, y, z) \oplus 1$
$x \rightarrow (y \downarrow z)$	$xyz \oplus xy \oplus xz \oplus 1$	$f_3(x, \overline{y}, \overline{z}) \oplus 1$
$x \leftarrow (y \mid z)$	$xyz \oplus yz \oplus x$	$f_3(\overline{x}, y, z) \oplus 1$
$x \leftarrow (y \vee z)$	$xyz \oplus xy \oplus xz \oplus yz \oplus y \oplus z \oplus 1$	$f_3(\overline{x}, \overline{y}, \overline{z}) \oplus 1$
$x \leftarrow (y \rightarrow z)$	$xyz \oplus xy \oplus yz \oplus x \oplus y$	$f_3(\overline{x}, y, \overline{z}) \oplus 1$
$x \leftarrow (y \leftarrow z)$	$xyz \oplus xz \oplus yz \oplus x \oplus z$	$f_3(\overline{x}, \overline{y}, z) \oplus 1$