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»
В.о. завідувача кафедри
__________ Сергій ЯКОВЛЄВ
«__» __________ 2023 р.

Магістерська дисертація

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

зі спеціальності: 113 Прикладна математика
на тему: **«Диференціально-обертальний криптоаналіз нелінійних вузлів LRX-криптосистем»**

Виконав:
студент II курсу, групи ФІ-12мн
Корж Нікіта Сергійович __________

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

Рецензент:
доцент кафедри ІБ, к.т.н.
Стьопочкіна Ірина Валеріївна __________

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент __________

Київ — 2023

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,
ОНП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
__________ Сергій ЯКОВЛЄВ
«__» __________ 2023 р.

ЗАВДАННЯ
на магістерську дисертацію

Студент: Корж Нікіта Сергійович

1. Тема роботи: «*Диференціально-обертальний криптоаналіз нелінійних вузлів LRX-криптосистем*», науковий керівник дисертації: доцент кафедри ММЗІ, к.т.н. Яковлєв Сергій Володимирович,

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

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

3. Об’єкт дослідження: Інформаційні процеси в системах криптографічного захисту інформації

4. Предмет дослідження: ARX- та LRX-системи та їх криптографічні властивості.

5. Перелік завдань: 1) провести огляд опублікованих джерел за тематикою дослідження; 2) уточнити відомі аналітичні вирази для ймовірностей RX-диференціалів функції модульного додавання на випадок зсуву більш ніж на один біт; 3) одержати аналітичні вирази для ймовірностей RX-диференціалів функцій, які реалізують логічні операції, що апроксимують модульне додавання.

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

7. Орієнтовний перелік публікацій: доповідь на XXI Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (11 – 12 травня 2023 р., м. Київ, Україна).

8. Дата видачі завдання: 10 вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2022 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-листопад 2022 р.	Виконано
3	Уточнення відомих аналітичних виразів для ймовірностей RX-диференціалів функції модульного додавання	Грудень 2022р. - Січень 2023р.	Виконано
4	Одержання аналітичного виразу для ймовірностей RX-диференціалів через операцію NORX	Лютий 2023р. - Березень 2023р.	Виконано
5	Одержання аналітичного виразу для ймовірностей RX-диференціалів через схожу операцію, яка також апроксимує модульне додавання	Квітень 2023р	Виконано
6	Оформлення магістерської дисертації	Травень 2023р.	Виконано

Студент ____________ Нікіта КОРЖ

Керівник ____________ Сергій ЯКОВЛЄВ

РЕФЕРАТ

Кваліфікаційна робота містить: 45 стор., 2 таблиці, 12 джерел.

Метою дослідження є розвиток методів криптоаналізу алгоритмів та протоколів легковагової криптографії.

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

Предметом дослідження є ARX- та LRX-системи та їх криптографічні властивості.

Було уточнено аналітичні вирази для ймовірностей проходження RX-диференціалів через операцію модульного додавання, які застосовні для будь-якої величини циклічного зсуву векторів на відміну від зсуву на один біт у Ашура і Лю. Ці результати розширюють можливості для проведення аналізу класичних ARX-криптосистем.

Було знайдено аналітичні вирази для імовірностей RX-диференціалів таких операцій та сформульовано умови їх неможливості. Показано, що для обох операцій RX-диференціали мають однакову умову неможливості, а значення імовірностей можливих диференціалів або співпадають, або відрізняються у константну кількість разів. Це дозволяє стверджувати, що обидві операції, які розглядались, забезпечують однаковий рівень стійкості до RX-аналізу.

ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, ОБЕРТАЛЬНИЙ КРИПТОАНАЛІЗ, ARX-КРИПТОСИСТЕМИ, NORX

ABSTRACT

The qualification work consists of: 45 pages, 2 tables, and 12 sources.

The **objective of the research** is to develop methods for cryptanalysis of lightweight cryptography algorithms and protocols.

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

The *subject of research* is ARX and LRX systems and their cryptographic properties.

Analytical expressions for the probabilities of RX-differentials passing through the operation of modular addition have been refined. These expressions are applicable for any value of cyclic shift in contrast to the one-bit shift in Ashur and Liu. These results expand the capabilities for conducting analysis on classical ARX-cryptosystems.

Analytical expressions for the probabilities of RX differentials for these operations have been found, and conditions for their impossibility have been formulated. It has been shown that for both operations, RX differentials have the same condition of impossibility, and the probabilities of possible differentials either coincide or differ by a constant factor. This allows us to conclude that both operations under consideration provide an equal level of resistance to RX analysis.

DIFFERENTIAL CRYPTANALYSIS, ROTATIONAL CRYPTANALYSIS, ARX CRYPTOSYSTEMS, NORX

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

V_n — множина усіх двійкових векторів довжини n;

$x = (x_{n-1}, \ldots, x_1, x_0)$ та $y = (y_{n-1}, \ldots, y_1, y_0)$ — n-бітові двійкові вектори, $x_i, y_j \in \{0, 1\}$;

$\oplus$ — операція додавання за модулем 2 (XOR);

$\overrightarrow{x}$ — циклічний зсув вектору x на k бітів праворуч;

$x \ll 1 = SHL(x)$ — нециклічний зсув вектору x на 1 біт ліворуч;

$(I \oplus SHL)(x) = x \oplus SHL(x)$

$1_{x \preccurlyeq y}$ — характеристична функція, яка дорівнює одиниці тоді і тільки тоді, коли $x_i \leqslant y_i$ ддля будь-якого i;

$x \vee y$ — операція логічного АБО;

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

$mask = (0, \ldots, 0, 1, 0, \ldots, 1)$ — двійковий вектор з одиницями в позиціях $i = 0$ та $i = n - k$ і нулями в усіх інших позиціях;

$\overline{mask}$ — інверсія вектору $mask$;

$wt(x)$ — вага вектору x (кількість одиниць);

xdp^+ — ймовірність проходження диференціалу через операцію $+$;

xdp^h — ймовірність проходження диференціалу через операцію $h(x,y)$;

xdp^v — ймовірність проходження диференціалу через операцію $v(x,y)$;

$hdp^{\oplus}$ — ймовірність проходження диференціалу за операцією $h(x,y)$ через $\oplus$.

$vdp^{\oplus}$ — ймовірність проходження диференціалу за операцією $v(x,y)$ через $\oplus$.

rp^h, rp^v — ймовірність проходження пари обертання через апроксимуючі операції.

ВСТУП

Актуальність дослідження. Актуальність даного дослідження полягає у тому, що дослідження стійкості криптопримітивів є завжди актуальною задачею. Новий спосіб дослідження ARX-криптосистем був введений Ашуром і Лю у 2016, який називається RX-криптоаналізом. Даний метод комбінує техніки диференціального та обертального криптоаналізу на рівні аналітичних результатів.

Метою дослідження є розвиток методів криптоаналізу алгоритмів та протоколів легковагової криптографії. Для досягнення мети необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) уточнити відомі аналітичні вирази для ймовірностей RX-диференціалів функції модульного додавання на випадок зсуву більш ніж на один біт;

3) одержати аналітичні вирази для ймовірностей RX-диференціалів функцій, які реалізують логічні операції, що апроксимують модульне додавання.

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

Предметом дослідження є ARX- та LRX-системи та їх криптографічні властивості.

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

Наукова новизна отриманих результатів полягає у тому, що були знайдені аналітичні вирази для обчислення ймовірностей RX-диференціалів функцій, які апроксимують модульне додавання, що дозволяє провадити диференціально-обертальний криптоаналіз для широкого класу LRX-криптосистем.

Практичне значення. Одержані результати дозволяють провадити уточнений аналіз стійкості існуючих ARX- та LRX-криптосистем та створювати нові захищені системи такого типу.

Апробація результатів та публікації. Частину результатів даної роботи було представлено на XXI Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (11 – 12 травня 2023 р., м. Київ, Україна).

1 ДИФЕРЕНЦІАЛЬНО ОБЕРТАЛЬНИЙ КРИПТОАНАЛІЗ

У цьому розділі буде розглянуто диференціальний і обертальний криптоаналізи, а також RX-аналіз, введений Ашуром і Лю, який вони представили у своїй роботі. Будуть розглянуті результати застосування RX-аналізу до різних шифрів.

Будуть введені і детально розглянуті дві операції $h(x,y)$ та $v(x,y)$, які апроксимують модульне додавання, та як вони впливають на LRX - криптосистеми.

1.1 Диференціальний криптоаналіз

Диференціальний криптоаналіз - це загальний метод аналізу симетричних криптографічних примітивів, зокрема, блокових шифрів та хеш-функцій. Вперше він був оприлюднений у 1990 році Біамом та Шаміром [1, 2] з атаками на скорочені варіанти стандарту шифрування даних (DES), а в 1991 році була проведена перша атака на DES, яка була швидшою за вичерпний перебір ключів [3].

Основною ідеєю диференціального криптоаналізу є аналіз відмінностей між вхідними та вихіднимим повідомленнями під час шифрування або інших криптографічних операцій. Замість того, щоб досліджувати окремі біти повідомлень, цей метод аналізує зміни відмінностей між двома повідомленнями та їх вплив на вихідні дані.

Цікавим є той факт, що диференціальний криптоаналіз був відомий розробникам DES, і сам шифр був створений для того, щоб протистояти цій потужній атаці [3]. Це пояснює, чому критерії побудови шифру трималися у секреті. Більшість з них стали відомими з розвитком диференціального криптоаналізу і пізніше були підтверджені розробниками.

Як диференціальна, так і лінійні атаки, не становлять великої загрози для реальних застосунків, оскільки вимагають для аналізу більше 2^{40} текстів. Для прикладу, для лінійної атаки необхідно зашифрувати 2^{43} відомих текстів за одним секретним ключем. Якщо користувач буде змінювати ключ кожні 2^{35} блоків, ймовірність успішної атаки стане мізерною. У випадку диференціальної атаки потрібно 2^{47} відкритих текстів, хоча атака все одно буде працювати, величезна кількість вибраних відкритів текстів робить атаку непрактичною.

1.2 Обертальний криптоаналіз

За останні десятиліття з'явилася величезна кількість симетричних примітивів, що використовують модульне додавання, побітове XOR та циклічні зсуву. Хоча модульне додавання часто наближається за допомогою операції XOR (виключне АБО), для випадкових вхідних даних ці операції є досить різними.

Обертальний криптоаналіз (англ. *rotational cryptoanalysis*) є специфічним типом криптоаналізу, оскільки він можу бути застосований лише до ARX-криптосистем. Даний метод криптоаналізу був запропонований Д. Ховратовичем та І. Ніколічем у [4] (хоча схожі методи аналізу використовувалися і раніше).

Основна ідея обертального криптоаналізу запозичена із статистичних атак на останні раунди блокових шифрів, зокрема, диференціального криптоаналізу, однак тут використовується «різниця» за унарною операцією, яка є своєрідною властивістю цього методу.

Означення 1.1. Парою обертання називається наступна пара векторів $(x, \overrightarrow{x})$, де $x \in \mathbb{F}_{2^n}$, $\overrightarrow{x} = x \ggg k$ — циклічний зсув на k-бітів.

Сутність обертального криптоаналізу полягає в дослідженні змін, які відбуваються із парами обертання при проходженні через ARX-схему, де нас найбільше цікавить випадок, коли пара обертання зберігається при проходженні.

Лема 1.1 (Даум, 5).

$$rp^+(k) = \Pr\{\overrightarrow{x+y} = \overrightarrow{x} + \overrightarrow{y}\} = \frac{1}{4}\left(1 + 2^{k-n} + 2^{-k} + 2^{-n}\right).$$

З даної леми випливає наступний наслідок:

Наслідок 1.1. *Для великих n та маленьких k випливають наступні ймовірності:*
1) Якщо $k = 1$, то $\Pr\{\overrightarrow{x+y} = \overrightarrow{x} + \overrightarrow{y}\} = 0.375$.
2) Якщо $k = 2$, то ймовірність буде дорівнювати 0.313.
3) При $k = 3$ ймовірність буде 0.281.

Можна зробити висновок, що пара обертання проходить через модульне додавання лише з деякою ймовірністю, однак ця ймовірність має доволі велике значення.

Твердження 1.1 (Ховратович, Ніколіч). *Нехай ARX-схема S містить лише операції побітового додавання, модульного додавання (ізольовані) та циклічного зсуву, тоді, за припущенням марковської поведінки йморвірностей, довільна пара обертання буде зберігатись після проходження схеми S із ймовірністю, близькою до ймовірності*

$$rp^S(k) = \Pr\{S(\overrightarrow{x}) = \overrightarrow{S(x)}\} \approx (rp^+(k))^q,$$

де q — кількість модульних додавань у схемі.

У ідеї обертального криптоаналізу є великий мінус, який полягає у тому, що він перестає працювати, якщо ARX-схема використовує модульне або побітове додавання із константами. Наприклад, це звичайна ситуація у геш-функціях. І, як наслідок маємо, що ймовірність проходження пари обертання через додавання із константами вкрай мала, що зводить нанівець весь аналіз.

Проблему з введенням у стан константи вдалось вирішити Ашуру і Лю у своїй роботі [6].

1.3 Обертальний криптоаналіз в контексті констант.

Відомо, що диференціальний критоаналіз розглядає різниці відкритих текстів та зашифрованих текстів за операцію $\oplus$. Дане твердження можна розглядати в контексті ARX-криптосистем, але виникає одна складність, яка полягає в тому, що потрібно визначати ймовірність проходження $\oplus$ - диференціалів через операцію модульного додавання, тобто, для функції f(x,y) = x + y та довільних трьох векторів α, β, γ необхідно обчислити $\Pr\{f(x \oplus \alpha, y \oplus \beta) = f(x,y) \oplus \gamma\}$.

Означення 1.2. $xdp^{+}(\alpha,\beta \to \gamma) = \Pr\{f(x\oplus\alpha, y\oplus\beta) = f(x,y)\oplus\gamma\} = \frac{1}{2^{2n}}\#\{(x,y) : (x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma\}$.

Ховратович і Ніколіч у своїй статті [4] показали, що $ARX - C$, тобто конструкція ARX з константою є повною. Це означає, що будь-яка функція може бути реалізована за допомогою операцій $ARX - C$. У більшості випадків константи вводяться у стан або за допомогою операції XOR, або за допомогою модулярного додавання. Коли константа C є обертально-інваріантною, тобто $C = C \ggg k$, для деякого k, XOR з константою не змінює обертальну властивість пари $(x, \overrightarrow{x})$. Однак, коли константа C не є обертально-інваріантною, властивості виводу потребують подальшої перевірки.

Загалом, коли константа C, яка не є обертально-інваріантною, додається до обертальної пари $(x, \overrightarrow{x})$, вихідна пара $(x \oplus C, \overrightarrow{x} \oplus C)$ більше не утворює обертальну пару. Якщо ця пара задана як вхідні дані для модульного додавання, основна формула в Леммі 1.2 для обчислення поширення властивості обертання більше не може використовуватися.

Лема 1.2. *Нехай* $\alpha, \beta, \gamma \in \mathbb{F}_{2^n}$ *є константами. Для незалежних рівномірних випадкових величин* $x, y \in \mathbb{F}_{2^n}$ *ймовірність* $x + y + 1 = ((x \oplus \alpha) + (y \oplus \beta)) \oplus \gamma$ *дорівнює*

$$1_{(I \oplus SHL)(\alpha\oplus\beta\oplus\gamma)\oplus 1 \preccurlyeq SHL((\alpha\oplus\gamma)|(\beta\oplus\gamma)} \cdot 2^{-|SHL((\alpha\oplus\gamma)|(\beta\oplus\gamma))|}.$$

Доведення. *Нехай* $\overline{x}$ *- побітове доповення до* $x \in \mathbb{F}_{2^n}$*. Маємо, що* $x + \overline{x} = -1$*, де* $-1 = 2^n - 1$*. Таким чином*

$$\overline{x} + \overline{y} = (-1 - x) + (-1 - y) = -x - y - 2.$$

Таким чином $\overline{x} + \overline{y} + 1 = -(x + y) - 1 = \overline{x + y} = (x + y) \oplus (-1)$*. Отже, рівняння* $x + y + 1 = (x \oplus \alpha) + (y \oplus \beta) \oplus \gamma$ *перетвореться на* $(x + y) \oplus (-1) = (\overline{x} \oplus \alpha) + (\overline{y} \oplus \beta) + \gamma$*, яке є еквівалентом наступного рівняння* $x + y = ((x \oplus \overline{\alpha}) + (y \oplus \beta)) \oplus \gamma$*, яке в свою чергу буде дорівнювати*

$$1_{(I \oplus SHL)(\alpha \oplus \beta \oplus \gamma) \oplus 1 \preccurlyeq SHL((\alpha \oplus \gamma)|(\beta \oplus \gamma)} \cdot 2^{-|SHL((\alpha \oplus \gamma)|(\beta \oplus \gamma))|}.$$

$\square$

Зауваження. Із доведення Леми 1.2 випливає, що

$$\Pr\{x + y + 1 = ((x \oplus \alpha) + (y \oplus \beta)) \oplus \gamma\} = xdp^+(\overline{\alpha},\overline{\beta} \to \overline{\gamma}).$$

Означення 1.3. Вектор рівності $eq(\alpha, \beta, \gamma)$ вказує позиції, на яких збігаються всі три вектори, й обчислюється за наступною формулою:

$$eq(\alpha,\beta,\gamma) = (\neg\alpha \oplus \beta) \wedge (\neg\alpha \oplus \gamma)$$

Наслідок 1.2. $eq(\alpha_i, \beta_i, \gamma_i) = 1$ *тоді і тільки тоді, коли* $\alpha_i = \beta_i = \gamma_i$.

Наступна теорема дозволяє обчислити ймовірність проходження $\oplus$ - диференціалів через операцію модульного додавання.

Теорема 1.1 (Ліпмаа, Моріаі)**.** *Для довільних n-бітних векторів* α*,* β*,* γ *виконуються такі твердження:*

1) $xdp^+(\alpha, \beta \to \gamma) > 0$ *тоді і тільки тоді, коли*

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

2) Якщо $xdp^{+}(\alpha, \beta \to \gamma) > 0$, *то* $xdp^{+}(\alpha, \beta \to \gamma) = 2^{-k}$, *де* $k = wt(\neg eq(\alpha \ll 1, \beta \ll 1, \gamma \ll 1))$.

Означення 1.4. Нехай α та β — деякі константи, тоді RX-парою будемо називати $(x \oplus \alpha, \overrightarrow{x} \oplus \beta)$.

Зауважимо, якщо α і β будуть дорівнювати нулю, то RX-пара стає звичайною парою обертання.

У роботі [6] Т. Ашур та Ю. Лю запропонували комбінований підхід до криптоаналізу ARX-криптосистем, так званий диференціально-обертальний криптоаналіз (або RX-аналіз), який поєднує ідеї диференціального та обертального криптоаналізу. У даному підході розглядаються та аналізуються зміни між текстами, які відрізняються не тільки циклічними зсувами, але й заданими побітовими різницями, що дозволяє успішно «протягувати» такі зміни через додавання із константами.

Теорема 1.2. *Нехай* $x, y \in \mathbb{F}_{2^n}$ *незалежні рівноймовірні випадкові величини. Нехай* α_1, β_1, α_2, β_2, Δ_1, Δ_2 *- константи в* $\mathbb{F}_{2^n}$. *Тоді*

$$\Pr\{\overrightarrow{(x \oplus \alpha_1) + (y \oplus \beta_1) \oplus \Delta_1} = (\overrightarrow{x} \oplus \alpha_2) + (\overrightarrow{y} \oplus \beta_2) \oplus \Delta_2\} =$$

$$1_{(I \oplus SHL)(\delta_1 \oplus \delta_2 \oplus \delta_3) \oplus 1 \preccurlyeq SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))} \cdot 2^{-|SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))|} \cdot 2^{-3} +$$
$$1_{(I \oplus SHL)(\delta_1 \oplus \delta_2 \oplus \delta_3) \preccurlyeq SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))} \cdot 2^{-|SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))|} \cdot 2^{-1.415},$$

де $\delta_1 = R(\alpha_1) \oplus L'(\alpha_2)$, $\delta_2 = R(\beta_1) \oplus L'(\beta_2)$, $\delta_3 = R(\Delta_1) \oplus L'(\Delta_2)$,

Автори одержали аналітичні вирази для імовірності проходження такого узагальненого диференціалу через операцію додавання за модулем, що надало можливість провадити аналіз ARX-криптосистем із використанням існуючих формалізованих методів.

У статті [7] автори розширили RX-криптоаналіз на AND-RX-шифри, які мають схожу парадигму побудови. Шифри AND-RX визначають як аналог шифрів ARX, в яких модульне додавання замінено на побітове AND. Шифри такого типу викликають інтерес завдяки блочному шифру Simon, за яким послідували інші шифри, подібні до Simon, такі як Simeck. Оскільки операції AND-RX у шифрах Simon є побітовими, то статистичні властивості окремих бітів залишаються незалежними від позиції біта.

Автори проаналізували розповсюдження RX-диференціалів через раунди AND-RX і розробили формулу, яка дозволяє порахувати ймовірність проходження RX-диференціалів через вказані операції. Вони досягли значних успіхів в аналізі стійкості відповідних шифрів, оскільки у більшості випадків, отримані розпізнавачі були найдовшими для відповідних варіантів Simeck.

Також, в роботі була введена SMT модель, за якою були знайдені відповідні RX-характеристики. Оцінивши свою модель, автори отримали RX-харакатеристики до 20, 27 і 35 раундів з відповідними ймовірностями 2^{-26}, 2^{-42} та 2^{-54} для версій Simeck з розмірами блоків 32, 48 і 64 біти відповідно.

Цікавим результатом, який отримали автори, був результат, отриманий при застосуванні моделі до блочного шифру Simon. Була отримана RX-характеристика до 11 раудів з ймовірністю 2^{-24}. Більш того, було виявлено, що знайти хороші RX-характеристики в шифрі Simon складніше, ніж в шифрі Simeck. Застосувавши модель SAT/SMT до іграшкових прикладів, автори дійшли висновку, що саме різниця в розкладі ключів робить Simeck більш вразливим до RX-криптоаналізу, ніж Simon.

З часом, авторам статті [10] вдалось покращити результати атаки, які були опубліковані раніше. Вони представили SAT/SMT модель для RX-криптоаналізу ARX-примітивів. У роботі дану модель було застосовано до різних версій SPECK та було отримано кразі розрізнювачі, ніж ті, які були опубліковані раніше.

Для Speck32/64 були представлені розрізнювачі для 10, 11 і 12 раундів з відповідними їм ймовірностями $2^{-19.15}$, $2^{-22.15}$, $2^{-25.57}$, які працюють для класів слабких ключівв розміром $2^{28.10}$, $2^{18.68}$ та $2^{4.92}$. Для версії Speck48 було представлено декілька розрізнювачів, найдовший з яких працює за 15 раундів з ймовірністю $2^{-43.81}$.

Крім того, для всіх версій можна знайти свої компроміси, якщо по різному налаштовувати цільові функції для складності даних і розміру класу слабких ключів. Представлену у роботі модель можна легко використовувати для інших ARX-конструкцій.

В наступній представленій авторами роботі [8], було узагальнено ідею RX-криптоаналізу на AND-RX шифри і показано, що RX-диференціал має таку ж ймовірність розповсюдження, як і відповідний XOR-дифернеціал, що проходить через ту саму функцію.

Також, автори статті, для сімейств шифрів Simon, знайшли RX-характеристики для наступної кількості раундів: 14 раундів для Simon32/64; 14 і 15 раундів для Simon48 з розмірами ключів 72 і 96 відповідно; 16 раундів для всіх версій Simon64; 15 і 18 раундів для Simon96 з розмірами ключів 96 і 144 відповідно; 16, 20 і 22 раунди для Simon128 з розмірами ключів 128, 192, 256 відповідно.

Крім того, автори вперше представили процедуру використання RX-характеристик для атаки з відновленням ключа, яку застосували до 28-раундового блочного шифру Simeck64.

У статті [9] автори запропонували потужний комп'ютерний інструмент, який дозволяє прискорити та полегшити оцінку стійкості блокових шифрів проти RX-криптоаналізу. Представлений у роботі інстумент бере реалізацію блочного шифру і автоматично знаходить оптимальну RX-характеристику. У порівнянні з більшістю автоматизованих інструментів, які підтримують лише невелий набір примітивів, даний інстумент підтримує будь-який блочний ARX-шифр. Крім того, даний інструмент легко адаптується завдяки своїй модульній архітектурі. Однак, щоб розв'язувати SMT задачі за адекватний час, необхідно мати комп'ютер високого класу.

1.4 Операції, які апроксимують модульне додавання

NORX — схема автентифікованого шифрування з асоційованими даними (AEAD) [11], яка має досить сильні диференціальні та обертальні властивості, що робить її безпечною для використання в криптографічних схемах. Розробники шифру використали альтернативну концепцію побудови легковагових шифрів, яка називається LRX-дизайном, де «L» означає «Logic», тобто логічні операції. Вони запропонували замість модульного додавання використовувати спеціальну операцію, яка побудована лише з логічних операцій над двійковими векторами і тому реалізується швидше та ефективніше, але при цьому апроксимує операцію додавання, щоб зберегти певні криптографічні властивості.

Означення 1.5. Нелінійна операція h в шифрі $NORX$ є векторною булевою функцією, яка визначається наступним чином:

$$h(x,y) = x \oplus y \oplus ((xy) \ll 1).$$

Наступна лема є важливим кроком на шляху до знаходження розповсюдження диференціалів у $NORX$. Вона усуває залежінсть рівняння $f(x \oplus \alpha, y \oplus \beta) = f(x,y) \oplus \gamma$ від векторів x та y, тобто, за допомогою леми, можна дізнатися, чи є заданий кортеж (α, β, γ) XOR-диференціалом від операції $h(x,y)$ за константу кількість операцій.

Лема 1.3. *Для кожного XOR-диференціалу $(\alpha, \beta \to \gamma)$ нелінійної операції $h(x,y)$ із ненульовою ймовірністю задовольняється наступне рівняння:*

$$(\alpha \oplus \beta \oplus \gamma) \wedge (\neg((\alpha \vee \beta) \ll 1)) = 0.$$

Очевидно, що, якщо умова леми не буде виконана, то (α, β, γ) — є не можливим XOR-диференціалом операції $h(x,y)$.

Наступна лема дозволяє обрахувати ймовірність диференціалу відносно нелінійної операції h.

Лема 1.4. *Нехай δ— XOR-диференціал відносно операції $h(x,y)$ із ненульовою ймовірністю, тоді*

$$xdp^h(\delta) = 2^{-wt((\alpha \vee \beta) \ll 1)}.$$

Замість розгляду XOR-диференціалів, також можна аналізувати f-диференціали, який буде введено в наступному означенні.

Означення 1.6. Нехай $f : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ — векторна булева функція, α, β і γ — диференціали відносно f, тоді $(\alpha, \beta \to \gamma)$ називаємо f-диференціалом, якщо для векторів x, y довжиною n виконується наступна рівність:

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

У випадку, якщо таких n-бітних векторів не існує, то $(\alpha, \beta \to \gamma)$ є неможливим f-диференціалом.

Підставляючи в означення 1.6 операцію $h(x,y)$ отримаємо наступну рівність:

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

яке також може бути описане на рівні бітів:

$$\alpha_0 \oplus \beta_o \oplus \gamma_0 = 0$$
$$(\alpha_i \oplus \beta_i \oplus \gamma_i) \oplus (x_{i-1} \wedge (\alpha_{i-1} \oplus \gamma_{i-1})) \oplus (y_{i-1} \wedge (\beta_{i-1} \oplus \gamma_{i-1})), i > 0.$$

Лема 1.5. *Нехай $h(x,y)$ - нелінійна операція, тоді для кожного диференціалу в контексті визначення 1.6 виконується наступна рівність:*

$$(\alpha \oplus \beta \oplus \gamma) \wedge (\neg(\gamma \ll 1) \oplus (\alpha \ll 1)) \wedge (\neg(\beta \ll 1) \oplus (\gamma \ll 1)) = 0.$$

Лема 1.6. *Нехай $h(x,y)$ — нелінійна операція шифру $NORX$, α,β та γ — довільні n-бітні вектори, тоді*

$$hdp^{\oplus}(\alpha,\ \beta \to \gamma) = 2^{-wt(((\alpha \oplus \gamma) \vee (\beta \oplus \gamma)) \ll 1)}.$$

У своїй статті [11], автори представили не тільки детальний аналіз шифру $NORX$, а й презентували $NODE$-фреймворк, який дозволяє автоматизувати пошук XOR-диференціалів та XOR-характеристик.

У роботі [12] була представлена аналогічна операція, яка також апроксимує модульне додавання.

Означення 1.7. Нелійна операція v є векторною булевою функцією, яка визначається наступним чином:

$$v(x,y) = x \oplus y \oplus ((x \vee y) \ll 1) \oplus 1.$$

Якщо f є булевою функцію степеню n, то розглянути операції є квадратичними, а також, операції h та v втрачають деякі властивості, зокрема, вони не задовольняють властивості асоціативності, тому, їх можна використовувати для побудови ARX-криптосистем не як алгебраїчні операції, а як функції ускладнення, з якою вони добре справляються.

Наслідок 1.3. *Апроксимуючі операції зберігають комутативність, а наймолодший біт результату усіх операцій є афінною функцією від наймолодших бітів аргументів. Це означає, що заміна операції модульного додавання на іншу все одно потребує циклічних зсувів при побудові криптосистем.*

Теорема 1.3. *Для довільних n-бітних векторів α, β, γ виконуються такі твердження:*

1) $xdp^v(\alpha, \beta \to \gamma) > 0 \Leftrightarrow (\alpha \oplus \beta \oplus \gamma) \wedge \neg((\alpha \vee \beta) \ll 1) = 0$,

2) Якщо $xdp^v(\alpha, \beta \to \gamma) > 0$, то $xdp^v(\alpha, \beta \to \gamma) = 2^{-wt((\alpha \vee \beta) \ll 1)}$.

Теорема 1.4. *Для довільних n-бітних векторів α, β, γ виконуються такі твердження:*

1) $vdp^{\oplus}(\alpha, \beta \to \gamma) > 0 \Leftrightarrow (\alpha \oplus \beta \oplus \gamma) \wedge eq(\alpha,\beta,\gamma) \ll 1) = 1$,

2) Якщо $vdp^{\oplus}(\alpha, \beta \to \gamma) > 0$, то $vdp^{\oplus}(\alpha, \beta \to \gamma) = 2^{-wt((\neg eq(\alpha,\beta,\gamma) \ll 1)}$.

Твердження теореми дозволяє застосовувати до LRX-криптосистем відомі методи побудови диференціальних атак відносно операції $v(x,y)$, а також методи оцінювання стійкості до таких атак.

Теорема 1.5. *Нехай $w = (\alpha, \beta \to \gamma)$ — довільний диференціал, тоді для нього справедливі такі твердження:*

1) $\Pr_w\{xdp^v(w) \neq 0\} = \frac{1}{2} \cdot \left(\frac{7}{8}\right)^{n-1}$.

2) $\Pr_w\{xdp^v(w) = 2^{-k} \mid xdp^v(w) \neq 0\} = b_k\left(n-1, \frac{6}{7}\right)$, *де b_k — k-та ймовірність біноміального розподілу.*

Теорема 1.6. *Нехай $w = (\alpha, \beta \to \gamma)$ — довільний диференціал, тоді для нього справедливі такі твердження:*

1) $\Pr_w\{vdp^{\oplus}(w) \neq 0\} = \frac{1}{2} \cdot \left(\frac{7}{8}\right)^{n-1}$.

2) $\Pr_w\{vdp^{\oplus}(w) = 2^{-k} \mid vdp^{\oplus}(w) \neq 0\} = b_k\left(n-1, \frac{6}{7}\right)$, *де b_k — k-та ймовірність біноміального розподілу.*

З вище вказаних теорем видно, що пошук диференціалів для побудови атаки на LRX-криптосистеми, які використовують апроксимуючі операції h або v, будуть мати приблизно таку саму ймоввірність, як і для традиційних ARX-криптосистем.

Теорема 1.7. *Для довільного r ($1 \leqslant r < n$) виконується наступна рівність:*

$$rp^h(r) = rp^v(r) = \frac{9}{16}.$$

Результат теореми 1.7 показує, що ймовірність проходження пари обертання через апроксимуючі операції більша ніж через операцію модульного додавання. Відповідно, для кращого захисту від обертального криптоаналізу, LRX-системам потрібно використовувати більше апроксимуючих операцій.

Висновки до розділу 1

У цьому розділі було розглянуто диференціальний і обертальний криптоаналізи. Був описаний RX-аналіз, який який був представлений

Ашуром і Лю у своїй роботі. Було розглянуто ймовірність проходження пари обертання через операцію модульного додавання, а також розглянуті результати застосування RX-аналізу до різних шифрів.

Були введені і детально розглянуті дві операції, які апроксимують модульне додавання, одна з яких, є операцією шифру NORX. Також було розглянуто, як введені операції впливають на LRX - криптосистеми.

2 ІМОВІРНОСТІ ПРОХОДЖЕННЯ RX-ДИФЕРЕНЦІАЛІВ ЧЕРЕЗ ОПЕРАЦІЇ, ЯКІ АПРОКСИМУЮТЬ ДОДАВАННЯ

У даному розділі буде уточнено результат Ашура і Лю, який в більш зручній нотації описує ймовірність проходження RX-диференціалу через операцію модульного додавання на зсув з довільною кількістю біт.

Також будуть знайдені ймовірності проходження RX-диференціалів через операції, які апроксимують модульне додавання; зокрема, операцію $h(x,y)$, яка використовується у шифрі NORX, і аналогічну їй $v(x,y)$, яка також апроксимує модульне додавання.

2.1 Уточнений результат Ашура і Лю

Результати, які були приведені у роботі Ашура і Лю, а саме знаходження ймовірності проходження RX-диференціалу через операцію модульного додавання розповсюджується лише на один біт, тому, для подальших досліджень узагальнемо теорему, яка дає можливість обраховувати ту ж саму ймовірність, але з зсувом на довільну кількість бітів.

Теорема 2.1. *Нехай $x, y \in \mathbb{F}_{2^n}$ незалежні рівноймовірні випадкові величини. Нехай α, β, γ — константи в $\mathbb{F}_{2^n}$. Тоді*

$$\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x+y}) \oplus \gamma\} =$$

$$\begin{aligned}
&\tfrac{1}{4}\left(1 - 2^{-k} - 2^{-(n-k)} + 2^{-n}\right) \cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) \cdot xdp^{+}(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'})+\\
&\tfrac{1}{4}\left(1 - 2^{-k} + 2^{-(n-k)} - 2^{-n}\right) \cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) \cdot xdp^{+}(\alpha',\beta' \to \gamma')+\\
&\tfrac{1}{4}\left(1 + 2^{-k} + 2^{-(n-k)} + 2^{-n}\right) \cdot xdp^{+}(\alpha^*,\beta^* \to \gamma^*) \cdot xdp^{+}(\alpha',\beta' \to \gamma')+\\
&\tfrac{1}{4}\left(1 + 2^{-k} - 2^{-(n-k)} - 2^{-n}\right) \cdot xdp^{+}(\alpha^*,\beta^* \to \gamma^*) \cdot xdp^{+}(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'}).
\end{aligned}$$

де $x = x_{n-1}, x_{n-2}, \ldots, x_2, x_1, x_0$; $y = y_{n-1}, y_{n-2}, \ldots, y_2, y_1, y_0$;

$\alpha = \alpha_{n-1}, \alpha_{n-2}, \ldots, \alpha_2, \alpha_1, \alpha_0$; $\beta = \beta_{n-1}, \beta_{n-2}, \ldots, \beta_2, \beta_1, \beta_0$;

$\gamma = \gamma_{n-1}, \gamma_{n-2}, \ldots, \gamma_2, \gamma_1, \gamma_0$.

Доведення. Нехай C - вектор переносу(або carry vector) додавання $x+y$, $C_{n-k} = \left\lfloor \frac{(x^* \oplus \alpha^*)+(y^* \oplus \beta^*)}{2^{n-k}} \right\rfloor$ - біт переносу в позиції $n-k$, $C_k = \left\lfloor \frac{x'+y'}{2^k} \right\rfloor$ - біт переносу в позиції k. Почнемо доведення з того, що розглянемо кожну частину рівності окремо.

1. $(\overrightarrow{x+y}) \oplus \gamma = \overrightarrow{((x^*+y^*+C_k) \oplus \gamma^*) \parallel (x'+y') \oplus \gamma'} =$
$((x'+y')) \oplus \gamma') \parallel ((x^*+y^*+C_k) \oplus \gamma^*)$, де
$x^* = x_{n-1}, x_{n-2}, \ldots, x_k$; $y^* = y_{n-1}, y_{n-2}, \ldots, y_k$;
$\gamma^* = \gamma_{n-1}, \gamma_{n-2}, \ldots, \gamma_k$; $\gamma' = \gamma_{k-1}, \gamma_{k-2}, \ldots, \gamma_0$;
$x' = x_{k-1}, x_{k-2}, \ldots, x_0$; $y' = y_{k-1}, y_{k-2}, \ldots, y_0$.
2. $(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = ((\overrightarrow{(x^* \parallel x')} \oplus \alpha) + (\overrightarrow{y^* \parallel y'}) \oplus \beta) =$
$((x' \parallel x^*) \oplus (\alpha' \parallel \alpha^*)) + ((y' \parallel y^*) \oplus (\beta' \parallel \beta^*)) =$
$((x' \oplus \alpha') + (y' \oplus \beta') + C_{n-k}) \parallel (((x^* \oplus \alpha^*) + (y^* \oplus \beta^*))$, де
$\alpha' = \alpha_{k-1}, \alpha_{k-2}, \ldots, \alpha_0$; $\beta' = \beta_{k-1}, \beta_{k-2}, \ldots, \beta_0$;
$\alpha^* = \alpha_{n-1}, \alpha_{n-2}, \ldots, \alpha_k$; $\beta^* = \beta_{n-1}, \beta_{n-2}, \ldots, \beta_k$.

Переписавши обидві частини заданої рівності, ми отримали, що $(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x+y}) \oplus \gamma$ виконується тоді і тільки тоді, коли

$$\begin{cases} (x' \oplus \alpha') + (y' \oplus \beta') + C_{n-k} = (x'+y') \oplus \gamma'. \\ (x^* \oplus \alpha^*) + (y^* \oplus \beta^*) = (x^*+y^*+C_k) \oplus \gamma^*. \end{cases}$$

Введемо наступні позначення: $x' \oplus L'(\alpha) = x''$, $y' \oplus L'(\beta) = y''$. Тоді

$$x'' + y'' + C_{n-k} = (x'' \oplus \alpha') + (y'' \oplus \beta') + \gamma'.$$

Далі переносимо γ' в ліву частину і отримуємо рівність

$$(x'' + y'' + C_{n-k}) \oplus \gamma' = ((x'' \oplus \alpha') + (y'' \oplus \beta')),$$

ймовірність якої легко порахувати за лемою(реф посилання) і означенням $xdp^+(\alpha', \beta' \to \gamma)$, і вона буде дорівнювати:

$$\begin{cases} xdp^{+}(\alpha',\beta' \to \gamma'), {}_{n-k} = 0 \\ xdp^{+}(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'}), C_{n-k} = 1 \end{cases}$$

Далі, за аналогією рахуємо ймовірність наступної рівністо

$$(x^* \oplus \alpha^* + (y^* \oplus \beta^*) = (x^* + y^* + C_k) \oplus \gamma^*,$$

яка буде дорівнювати:

$$\begin{cases} xdp^{+}(\alpha^*,\beta^* \to \gamma^*), C_k = 0 \\ xdp^{+}(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}), C_k = 1 \end{cases}$$

Звідси випливає, що ймовірність проходження пари обертання дорівнює: $\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x+y}) \oplus \gamma\} =$

$\Pr\{C_k = 1, C_{n-k} = 1\} \cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) \cdot xdp^{+}(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'}) +$

$\Pr\{C_k = 1, C_{n-k} = 0\} \cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) \cdot xdp^{+}(\alpha',\beta' \to \gamma') +$

$\Pr\{C_k = 0, C_{n-k} = 0\} \cdot xdp^{+}(\alpha^*,\beta^* \to \gamma^*) \cdot xdp^{+}(\alpha',\beta' \to \gamma') +$

$\Pr\{C_k = 0, C_{n-k} = 1\} \cdot xdp^{+}(\alpha^*,\beta^* \to \gamma^*) \cdot xdp^{+}(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'}).$

Відомо, що розподіл біту переносу обчислюється за формулами:

$$\begin{aligned} \Pr\{C_t = 1\} &= \frac{1}{2} - \frac{1}{2^{t+1}}, \\ \Pr\{C_t = 0\} &= 1 - \Pr\{C_t = 1\} = 1 - \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right) = \frac{1}{2} + \frac{1}{2^{t+1}}. \end{aligned}$$

Далі порахуємо кожну ймовірність окремо:

$$\begin{aligned} \Pr\{C_k = 1, C_{n-k} = 1\} &= \left(\frac{1}{2} - \frac{1}{2^{k+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{n-k+1}}\right) = \\ &= \frac{2^{k+1} - 2}{2 \cdot 2^{k+1}} \cdot \frac{2^{n-k+1} - 2}{2 \cdot 2^{n-k+1}} = \frac{1}{4}\left(\frac{2^n - 2^k - 2^{n-k} + 1}{2^n}\right) = \\ &= \frac{1}{4}\left(1 - 2^{-k} - 2^{-(n-k)} + 2^{-n}\right). \end{aligned}$$

$$\Pr\{C_k=0,C_{n-k}=0\}=\left(\frac{1}{2}+\frac{1}{2^{k+1}}\right)\left(\frac{1}{2}+\frac{1}{2^{n-k+1}}\right)=$$
$$=\frac{2^{k+1}+2}{2\cdot 2^{k+1}}\cdot\frac{2^{n-k+1}+2}{2\cdot 2^{n-k+1}}=\frac{1}{4}\left(\frac{2^n+2^k+2^{n-k}+1}{2^n}\right)=$$
$$=\frac{1}{4}\left(1+2^{-k}+2^{-(n-k)}+2^{-n}\right).$$

$$\Pr\{C_k=1,C_{n-k}=0\}=\left(\frac{1}{2}-\frac{1}{2^{k+1}}\right)\left(\frac{1}{2}+\frac{1}{2^{n-k+1}}\right)=$$
$$=\frac{2^{k+1}-2}{2\cdot 2^{k+1}}\cdot\frac{2^{n-k+1}+2}{2\cdot 2^{n-k+1}}=\frac{1}{4}\left(\frac{2^n+2^k-2^{n-k}-1}{2^n}\right)=$$
$$=\frac{1}{4}\left(1-2^{-k}+2^{-(n-k)}-2^{-n}\right).$$

$$\Pr\{C_k=0,C_{n-k}=1\}=\left(\frac{1}{2}+\frac{1}{2^{k+1}}\right)\left(\frac{1}{2}-\frac{1}{2^{n-k+1}}\right)=$$
$$=\frac{2^{k+1}+2}{2\cdot 2^{k+1}}\cdot\frac{2^{n-k+1}-2}{2\cdot 2^{n-k+1}}=\frac{1}{4}\left(\frac{2^n-2^k+2^{n-k}-1}{2^n}\right)=$$
$$\frac{1}{4}\left(1+2^{-k}-2^{-(n-k)}-2^{-n}\right).$$

Далі, використовуючи пораховані ймовірности, видно, що $\Pr\{(\overrightarrow{x}\oplus\alpha)+(\overrightarrow{y}\oplus\beta)=(\overrightarrow{x+y})\oplus\gamma\}=$
$\frac{1}{4}\left(1-2^{-k}-2^{-(n-k)}+2^{-n}\right)\cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*}\to\overline{\gamma^*})\cdot xdp^{+}(\overline{\alpha'},\overline{\beta'}\to\overline{\gamma'})+$
$\frac{1}{4}\left(1-2^{-k}+2^{-(n-k)}-2^{-n}\right)\cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*}\to\overline{\gamma^*})\cdot xdp^{+}(\alpha',\beta'\to\gamma')+$
$\frac{1}{4}\left(1+2^{-k}+2^{-(n-k)}+2^{-n}\right)\cdot xdp^{+}(\alpha^*,\beta^*\to\gamma^*)\cdot xdp^{+}(\alpha',\beta'\to\gamma')+$
$\frac{1}{4}\left(1+2^{-k}-2^{-(n-k)}-2^{-n}\right)\cdot xdp^{+}(\alpha^*,\beta^*\to\gamma^*)\cdot xdp^{+}(\overline{\alpha'},\overline{\beta'}\to\overline{\gamma'}).$ □

Наслідок 2.1. *У випадку циклічного зсуву на $k=1$ виникає два випадки:*

1. Якщо $\alpha'\oplus\beta'=\gamma'\oplus 1$, то

$$\Pr\{(\overrightarrow{x}\oplus\alpha)+(\overrightarrow{y}\oplus\beta)=(\overrightarrow{x+y})\oplus\gamma\}=$$
$$\left(1-\frac{1}{2^{n-1}}\right)\left(\frac{1}{8}\cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*}\to\overline{\gamma^*})+\frac{3}{8}\cdot xdp^{+}(\alpha^*,\beta^*\to\gamma^*)\right).$$

2. Якщо $\alpha' \oplus \beta' = \gamma'$, *то*

$$\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x+y}) \oplus \gamma\} =$$

$$\left(1 + \frac{1}{2^{n-1}}\right)\left(\frac{1}{8} \cdot xdp^{+}(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) + \frac{3}{8} \cdot xdp^{+}(\alpha^*,\beta^* \to \gamma^*)\right).$$

Доведення. Нехай $k = 1$, тоді довжини α', β', γ' будуть дорівнювати одиниці, тобто $\alpha' = \alpha_0$, $\beta' = \beta_0$, $\gamma' = \gamma_0$. Враховуючи це, можна порахувати наступні ймовірності $xdp^{+}(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'})$ та $xdp^{+}(\alpha',\beta' \to \gamma')$.

Для того, щоб порахувати задані ймовірності, використаємо теорему Ліпмаа та Моріаі.

1. Порахуємо значення $e = eq(\alpha' \ll 1, \beta' \ll 1, \gamma' \ll 1)$. Враховуючи, що довжини констант дорівнюють одиниці, то логічно, що, якщо їх нециклічно зсунути, то всі вони прийматимуть значення нуль. І, це в свою чергу означає, що e у будь якому випадку буде дорівнювати одиниці, тобто $e = eq(\alpha' \ll 1, \beta' \ll 1, \gamma' \ll 1 = 1$.

2. За теоремою Ліпмаа та Моріаі у випадках, коли $xdp^{+}(\alpha', \beta' \to \gamma') > 0$, $xdp^{+}(\alpha', \beta' \to \gamma') = 2^{-p}$, де

$$p = wt(\neg eq(\alpha' \ll 1, \beta' \ll 1, \gamma' \ll 1)).$$

Оскільки у всіх випадках $e = 1$, то $p = 0$ і $xdp^{+}(\alpha', \beta' \to \gamma') = 1$.

3. Нехай $\delta = (\alpha' \oplus \beta' \oplus \gamma' \oplus (\gamma' \ll 1))$.

Далі, визначивши, в яких випадках $e \wedge \delta = 0$, ми дізнаємось, коли $xdp^{+}(\alpha', \beta' \to \gamma') = 0$, а коли дорівнює 1.

1. Якщо $\alpha' = \beta' = \gamma' = 0$, то $\delta = 0 \Rightarrow e \wedge \delta = 0$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 1$.

2. Якщо $\alpha' = \beta' = 0, \gamma' = 1$, то $\delta = 1 \Rightarrow e \wedge \delta = 1$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 0$.

3. Якщо $\alpha' = 0, \beta' = 1, \gamma' = 0$, то $\delta = 1 \Rightarrow e \wedge \delta = 1$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 0$.

4. Якщо $\alpha' = 0, \beta' = 1, \gamma' = 1$, то $\delta = 0 \Rightarrow e \wedge \delta = 0$, тому

$xdp^{+}(\alpha', \beta' \to \gamma') = 1.$'

5. Якщо $\alpha' = 1, \beta' = 0, \gamma' = 0$, то $\delta = 1 \Rightarrow e \wedge \delta = 1$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 0.$

6. Якщо $\alpha' = 1, \beta' = 0, \gamma' = 1$, то $\delta = 0 \Rightarrow e \wedge \delta = 0$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 1.$

7. Якщо $\alpha' = 1, \beta' = 1, \gamma' = 0$, то $\delta = 0 \Rightarrow e \wedge \delta = 0$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 1.$

8. Якщо $\alpha' = 1, \beta' = 1, \gamma' = 1$, то $\delta = 1 \Rightarrow e \wedge \delta = 1$, тому $xdp^{+}(\alpha', \beta' \to \gamma') = 0.$

Як бачимо вище, $xdp^{+}(\alpha', \beta' \to \gamma')$ приймає лише два значення 0 та 1. Порахуємо ймовірність $\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x + y}) \oplus \gamma\}$ для обох випадків.

Зауважимо, що, якщо $xdp^{+}(\alpha', \beta' \to \gamma') = 0$, то $xdp^{+}(\overline{\alpha'}, \overline{\beta'} \to \overline{\gamma'}) = 1$ і навпаки.

а. Нехай $k = 1$, $\alpha' \oplus \beta' = \gamma' \oplus 1$, тоді $xdp^{+}(\alpha', \beta' \to \gamma') = 0$, $xdp^{+}(\overline{\alpha'}, \overline{\beta'} \to \overline{\gamma'}) = 1$, тоді $\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x + y}) \oplus \gamma\} =$

$$
\begin{aligned}
&= \frac{1}{4}\left(1 - 2^{-1} - 2^{-(n-1)} + 2^{-n}\right) \cdot xdp^{+}(\overline{\alpha^{*}}, \overline{\beta^{*}} \to \overline{\gamma^{*}}) + \\
&+ \frac{1}{4}\left(1 + 2^{-1} - 2^{-(n-1)} - 2^{-n}\right) \cdot xdp^{+}(\alpha^{*}, \beta^{*} \to \gamma^{*}) = \\
&= \frac{1}{4}\left(\frac{1}{2} - \frac{1}{2^{n-1}} + \frac{1}{2^{n}}\right) \cdot xdp^{+}(\overline{\alpha^{*}}, \overline{\beta^{*}} \to \overline{\gamma^{*}}) + \\
&+ \frac{1}{4}\left(\frac{3}{2} - \frac{1}{2^{n-1}} - \frac{1}{2^{n}}\right) \cdot xdp^{+}(\alpha^{*}, \beta^{*} \to \gamma^{*}) = \\
&= \frac{1}{8}\left(1 - \frac{1}{2^{n-1}}\right) \cdot xdp^{+}(\overline{\alpha^{*}}, \overline{\beta^{*}} \to \overline{\gamma^{*}}) + \\
&+ \frac{3}{8}\left(1 - \frac{1}{2^{n-1}}\right) \cdot xdp^{+}(\alpha^{*}, \beta^{*} \to \gamma^{*}) = \\
&= \left(1 - \frac{1}{2^{n-1}}\right)\left(\frac{1}{8} \cdot xdp^{+}(\overline{\alpha^{*}}, \overline{\beta^{*}} \to \overline{\gamma^{*}}) + \frac{3}{8} \cdot xdp^{+}(\alpha^{*}, \beta^{*} \to \gamma^{*})\right).
\end{aligned}
$$

б. Нехай $k = 1$, $\alpha' \oplus \beta' = \gamma'$, тоді $xdp^{+}(\alpha', \beta' \to \gamma') = 1$,

$xdp^+(\overline{\alpha'},\overline{\beta'} \to \overline{\gamma'}) = 0$, тоді $\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x+y}) \oplus \gamma\} =$

$$\begin{aligned}
&= \frac{1}{4}\left(1 - 2^{-1} + 2^{-(n-1)} - 2^{-1}\right) \cdot xdp^+(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) + \\
&+ \frac{1}{4}\left(1 + 2^{-1} + 2^{-(n-1)} + 2^{-1}\right) \cdot xdp^+(\alpha^*,\beta^* \to \gamma^*) = \\
&= \frac{1}{4}\left(\frac{1}{2} + \frac{2}{2^n} - \frac{1}{2^n}\right) \cdot xdp^+(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) + \\
&+ \frac{1}{4}\left(\frac{3}{2} + \frac{2}{2^n} + \frac{1}{2^n}\right) \cdot xdp^+(\alpha^*,\beta^* \to \gamma^*) = \\
&= \frac{1}{8}\left(1 + \frac{1}{2^{n-1}}\right) \cdot xdp^+(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) + \\
&+ \frac{3}{8}\left(1 + \frac{1}{2^{n-1}}\right) \cdot xdp^+(\alpha^*,\beta^* \to \gamma^*) = \\
&= \left(1 + \frac{1}{2^{n-1}}\right)\left(\frac{1}{8} \cdot xdp^+(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) + \frac{3}{8} \cdot xdp^+(\alpha^*,\beta^* \to \gamma^*)\right).
\end{aligned}$$

$\square$

Зауваження. Щоб отримати результат, який був виведений Ашуром і Лю [6], необхідно покласти, що $\frac{1}{2^{n-1}} \approx 0$. Звідси отримаємо, що

$$\Pr\{(\overrightarrow{x} \oplus \alpha) + (\overrightarrow{y} \oplus \beta) = (\overrightarrow{x+y}) \oplus \gamma\} =$$

$$\frac{1}{8} \cdot xdp^+(\overline{\alpha^*},\overline{\beta^*} \to \overline{\gamma^*}) + \frac{3}{8} \cdot xdp^+(\alpha^*,\beta^* \to \gamma^*)$$

За допомогою доведеного твердження можна більш гнучко будувати диференціально-обертальні атаки, використовуючи усі можливі значення зсувів, та провадити оцінки стійкості ARX-криптосистем до атак такого виду.

2.2 Ймовірність RX-диференціалу операції $h(x,y)$

Основний результат даного розділу наведений у наступній теоремі, яка дозволяє обчислити ймовірність проходження RX-диференціалу через операцію $h(x,y)$.

Теорема 2.2. *Для фіксованого значення зсуву k ймовірність*

RX-диференціалу $(\alpha, \beta \to \gamma)$ *через операцію* $h(x,y)$ *описується такими співвідношеннями:*

1) $\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} \neq 0$ *тоді та тільки тоді, коли* $(\delta \vee \overline{\varphi}) \wedge \overline{mask} = 0$*, де* $\delta = \alpha \oplus \beta \oplus \gamma$*,* $\varphi = (\alpha \vee \beta) \ll 1$*;*

2) якщо імовірність RX-диференціалу $(\alpha, \beta \to \gamma)$ *не дорівнює нулю, то вона дорівнює*

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} =$$
$$= \left(\frac{3}{4} - \frac{\delta_0}{2}\right)\left(\frac{3}{4} - \frac{\delta_{n-k}}{2}\right) \cdot 2^{-wt(\varphi \wedge \overline{mask})}.$$

Доведення.

1. Розглянемо ліву частину рівності і введемо наступні позначення:

$$u = \overrightarrow{x \oplus y \oplus ((xy) \ll 1)} \oplus \gamma,$$

$x = x_{n-1}, x_{n_2}, \ldots, x_0$ і $y = y_{n-1}, y_{n_2}, \ldots, y_0$, тоді:

$$xy = x_{n-1}y_{n-1}, x_{n-2}y_{n-2}, \ldots, x_0y_0 \Rightarrow$$
$$l = (xy) \ll 1 = x_{n-2}y_{n-2}, x_{n-3}y_{n-3}, \ldots, x_0y_0, 0.$$

Нехай

$$z = x \oplus y \oplus ((xy) \ll 1),$$

$$z_i = x_i \oplus y_i \oplus (x_{i-1}y_{i-1}),$$

тоді $u_i = \overrightarrow{z_i} \oplus \gamma_i$, де

$$\overrightarrow{z} = z_{k-1}, \ldots, z_1, \quad z_0 \quad, z_{n-1}, z_{n-2}, \ldots z_k,$$
$$\gamma = \gamma_{n-1}, \ldots, \gamma_{n-k+1}, \quad \gamma_{n-k} \quad, \gamma_{n-k-1}, \ldots, \gamma_0.$$

Звідси випливає наступна система рівнянь:

$$\begin{cases} u_i = x_{i+k} \oplus y_{i+k} \oplus (x_{i+k-1} y_{i+k-1}) \oplus \gamma_i, & 0 \leqslant i < n-k, \\ u_{n-k} = x_0 \oplus y_0 \oplus \gamma_{n-k}, & i = n-k, \\ u_i = x_{i-n+k} \oplus y_{i-n+k} \oplus (x_{i-n+k-1} y_{i-n+k-1}) \oplus \gamma_i, & i > n-k. \end{cases}$$

Далі, по аналогії розглянемо праву частину рівності. Нехай:

$$w = \overrightarrow{x} \oplus \alpha \oplus \overrightarrow{y} \oplus \beta \oplus (((\overrightarrow{x} \oplus \alpha)(\overrightarrow{y} \oplus \beta)) \ll 1),$$

де

$$\begin{aligned} \overrightarrow{x} &= x_{k-1}, \ldots, x_0, x_{n-1}, \ldots, x_k, \\ \overrightarrow{y} &= y_{k-1}, \ldots, y_0, y_{n-1}, \ldots, y_k, \\ \alpha &= \alpha_{n-1}, \ldots, \alpha_{n-k+1}, \alpha_{n-k}, \alpha_{n-k-1}, \ldots, \alpha_0, \\ \beta &= \beta_{n-1}, \ldots, \beta_{n-k+1}, \beta_{n-k}, \beta_{n-k-1}, \ldots, \beta_0. \\ f &= ((\overrightarrow{x} \oplus \alpha)(\overrightarrow{y} \oplus \beta)) \ll 1 \end{aligned}$$

По аналогії з першим випадком отримали наступну систему рівнянь:

$$\begin{cases} w_0 = x_k \oplus \alpha_0 \oplus y_k \oplus \beta_0, & i = 0 \\ w_i = x_{i+k} \oplus \alpha_i \oplus y_{i+k} \oplus \beta_i \oplus & \\ \qquad \oplus (x_{i+k-1} \oplus \alpha_{i-1})(y_{i+k-1} \oplus \beta_{i-1}), & 0 < i < n-k, \\ w_{n-k} = x_0 \oplus \alpha_{n-k} \oplus y_0 \oplus \beta_{n-k} \oplus & \\ \qquad \oplus (x_{n-1} \oplus \alpha_{n-k-1})(y_{n-1} \oplus \beta_{n-k-1}), & i = n-k, \\ w_i = x_{i-n+k} \oplus \alpha_i \oplus y_{i-n+k} \oplus \beta_i \oplus & \\ \qquad \oplus (x_{i-n+k-1} \oplus \alpha_{i-1})(y_{i-n+k-1} \oplus \beta_{i-1}), & i > n-k. \end{cases}$$

Імовірність проходження RX-диференціалу дорівнює ймовірності того, що $u = w$. Обчислимо цю ймовірність, розглядаючи дану рівність побітово.

1. Якщо $i = 0$, то

$$x_k \oplus y_k \oplus (x_{k-1}y_{k-1}) \oplus \gamma_0 = x_k \oplus \alpha_0 \oplus y_k \oplus \beta_0,$$
$$x_{k-1}y_{k-1} = \alpha_0 \oplus \beta_0 \oplus \gamma_0.$$

2. Якщо $i = n - k$, то

$$x_0 \oplus y_0 \oplus \gamma_{n-k} = x_0 \oplus \alpha_{n-k} \oplus y_0 \oplus \beta_{n-k} \oplus (x_{n-1} \oplus \alpha_{n-k-1})(y_{n-1} \oplus \beta_{n-k-1}),$$
$$(x_{n-1} \oplus \alpha_{n-k-1})(y_{n-1} \oplus \beta_{n-k-1}) = \alpha_{n-k} \oplus \beta_{n-k} \oplus \gamma_{n-k}.$$

3. Якщо $i < n - k$, то

$$x_{i+k} \oplus y_{i+k} \oplus (x_{i+k-1}y_{i+k-1}) \oplus \gamma_i =$$
$$= x_{i+k} \oplus \alpha_i \oplus y_{i+k}\beta_i \oplus (x_{i+k-1} \oplus \alpha_{i-1})(y_{i+k-1} \oplus \beta_{i-1});$$
$$\alpha_i \oplus \beta_i \oplus \gamma_i = x_{i+k-1}\beta_{i-1} \oplus \alpha_{i-1}y_{i+k-1} \oplus \alpha_{i-1}\beta_{i-1}$$

4. Якщо $i > n - k$, то

$$x_{i-n+k} \oplus y_{i-n+k} \oplus (x_{i-n+k-1}y_{i-n+k-1}) \oplus \gamma_i =$$
$$= x_{i-n+k} \oplus \alpha_i \oplus y_{i-n+k}\beta_i \oplus (x_{i-n+k-1} \oplus \alpha_{i-1})(y_{i-n+k-1} \oplus \beta_{i-1});$$
$$\alpha_i \oplus \beta_i \oplus \gamma_i = x_{i-n+k-1}\beta_{i-1} \oplus \alpha_{i-1}y_{i-n+k-1} \oplus \alpha_{i-1}\beta_{i-1}.$$

Введемо наступні позначення:

$$\delta = \alpha \oplus \beta \oplus \gamma;$$
$$mask = (0, \ldots, 0, 1, 0, \ldots, 0, 1),$$

де одиниці лише в позиціях $i = n - k$ та $i = 0$.

$$\varphi = (\alpha \vee \beta) \ll 1.$$

Нехай p_i — імовірність виконання рівності диференціального переходу в i-тому біті, тоді

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = \prod_{i=0}^{n-1} p_i.$$

Обчислимо імовірності p_i для кожного значення i.

1. Нехай $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = \delta_0$ і $i = 0$, то

$$x_{k-1}y_{k-1} = \alpha_0 \oplus \beta_0 \oplus \gamma_0 = \delta_0.$$

Якщо $\delta_0 = 0$, то

$$p_0 = \Pr\{x_{k-1}y_{k-1} = 0\} = \frac{3}{4}.$$

Якщо $\delta_0 = 1$, то

$$p_0 = \Pr\{x_{k-1}y_{k-1} = 0\} = \frac{1}{4}.$$

Тому,

$$p_0 = \left(\frac{3}{4} - \frac{\delta_0}{2}\right).$$

2. Нехай $(x_{n-1} \oplus \alpha_{n-k-1})(y_{n-1} \oplus \beta_{n-k-1}) = \alpha_{n-k} \oplus \beta_{n-k} \oplus \gamma_{n-k} = \delta_{n-k}$ і $i = n - k$, тоді по аналогії з першим випадком, ймовірність проходження диференціалу буде дорівнювати:

$$p_{n-k} = \left(\frac{3}{4} - \frac{\delta_{n-k}}{2}\right).$$

3. Далі розглядаємо випадок для всіх інших значень i, коли $i \neq 0$ та $i \neq n - k$. Усі ці випадки описуються загальним рівнянням такого виду:

$$\delta_i = \alpha_i \oplus \beta_i \oplus \gamma_i = x_*\beta_{i-1} \oplus y_*\alpha_{i-1} \oplus \alpha_{i-1}\beta_{i-1},$$

де x_* та y_* є випадковими незалежними бітами.

У таблиці 2.1 наведено значення ймовірності p_i для усіх можливих значень параметрів даного рівняння.

Таблиця 2.1 – Таблиця ймовірностей проходження диференціалу через $h(x,y)$.

α_{i-1}	β_{i-1}	δ_i	result	p_i
0	0	0	0=0	1
0	0	1	1=0	0
0	1	0	$0 = y_*$	$\frac{1}{2}$
0	1	1	$1 = y_*$	$\frac{1}{2}$
1	0	0	$0 = x_*$	$\frac{1}{2}$
1	0	1	$1 = x_*$	$\frac{1}{2}$
1	1	0	$0 = x_* \oplus y_* \oplus 1$	$\frac{1}{2}$
1	1	1	$1 = x_* \oplus y_* \oplus 1$	$\frac{1}{2}$

Із наведених у таблиці 2.1 даних випливає, що існує єдине значення параметрів α_{i-1}, β_{i-1} і δ_i, за яких ймовірність $p_i = 0$. Відповідно,

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = 0$$

тоді та тільки тоді, коли існує таке i ($i \neq 0$ та $i \neq n-k$), при якому $\alpha_{i-1} = \beta_{i-1} = 0$ та $\delta_i = 1$, тобто

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} \neq 0 \Leftrightarrow (\delta \vee \overline{\varphi}) \wedge \overline{mask} = 0.$$

Якщо ймовірність RX-диференціалу не дорівнює нулю, то у випадку $\alpha_{i-1} = \beta_{i-1} = 0$ імовірність p_i дорівнює одиниці, а в усіх інших випадках (коли хоча б один з двох бітів α_{i-1}, β_{i-1} дорівнює одиниці) імовірність p_i дорівнюватиме $\frac{1}{2}$. Таким чином, з усіх наведених співвідношень випливає, що

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = \\ = \left(\frac{3}{4} - \frac{\delta_0}{2}\right)\left(\frac{3}{4} - \frac{\delta_{n-k}}{2}\right) \cdot 2^{-wt(\varphi \wedge \overline{mask})},$$

де $\delta = \alpha \oplus \beta \oplus \gamma$, $\varphi = (\alpha \vee \beta) \ll 1$. Звідси випливає твердження теореми. □

Розглядаючи дану теорему, можна помітити деяку схожість з іншими результатами; так, якщо $\delta_0 = \delta_{n-k} = 0$, то порахувавши результат двох перших множників отримаємо $\frac{9}{16}$, що вказує на ймовірність проходження диференціалів через циклічні зсуви [Теорема 1.7]. В свою чергу третій множник результату нагадує нам ймовірність проходження звичайних диференціалів відносно операції $h(x,y)$ [Лема 1.4]. Даний результат показує, що диференціально-обертальний криптоаналіз комбінує обидві техніки; бачимо, що в перших двох множниках є сліди аналітичних результатів стійкості до обертального криптоаналізу, а в третьому множнику — результати стійкості до диференціального криптоаналізу.

2.3 Ймовірність RX-диференціалу операції $v(x,y)$

Основний результат даного розділу наведений у наступній теоремі, яка дозволяє обчислити ймовірність проходження RX-диференціалу через операцію $v(x,y)$.

Теорема 2.3. *Для фіксованого значення зсуву k імовірність RX-диференціалу $(\alpha, \beta \to \gamma)$ через операцію $v(x, y)$ описується такими співвідношеннями:*

1) $\Pr\{\overrightarrow{v(x,y)} \oplus \gamma = v(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} \neq 0$ *тоді та тільки тоді, коли* $(\delta \vee \overline{\varphi}) \wedge \overline{mask} = 0$*, де* $\delta = \alpha \oplus \beta \oplus \gamma$*;* $\varphi = (\alpha \vee \beta) \ll 1$.

2) якщо імовірність RX-диференціалу $(\alpha, \beta \to \gamma)$ не дорівнює нулю, *то вона дорівнює*

$$\Pr\{\overrightarrow{v(x,y)} \oplus \gamma = v(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} =$$
$$= \left(\frac{1}{4} + \frac{\delta_0}{2}\right)\left(\frac{1}{4} + \frac{\delta_{n-k}}{2}\right) \cdot 2^{-wt(\varphi \wedge \overline{mask})}.$$

Доведення.

1. Розглянемо ліву частину рівності і введемо наступні позначення:

$$u = \overrightarrow{x \oplus y \oplus ((x \vee y) \ll 1) \oplus 1} \oplus \gamma,$$

$x = x_{n-1}, x_{n_2}, \ldots, x_0$ і $y = y_{n-1}, y_{n_2}, \ldots, y_0$, тоді:

$$x \vee y = x_{n-1} \vee y_{n-1}, x_{n-2} \vee y_{n-2}, \ldots, x_0 \vee y_0 \Rightarrow$$

$$l = (x \vee y) \ll 1 = x_{n-2} \vee y_{n-2}, x_{n-3} \vee y_{n-3}, \ldots, x_0 \vee y_0, 0.$$

Нехай

$$z = x \oplus y \oplus ((x \vee y) \ll 1) \oplus 1$$

$$z_0 = x_0 \oplus y_0 \oplus 1,$$

тоді $u_i = \overrightarrow{z_i} \oplus \gamma_i$, де

$$\begin{aligned} \overrightarrow{z} &= z_{k-1}, \ldots, z_1, z_0, z_{n-1}, z_{n-2}, \ldots z_k, \\ \gamma &= \gamma_{n-1}, \ldots, \gamma_{n-k+1}, \gamma_{n-k}, \gamma_{n-k-1}, \ldots, \gamma_0. \end{aligned}$$

Звідси випливає наступна система рівнянь:

$$\begin{cases} u_i = x_{i+k} \oplus y_{i+k} \oplus (x_{i+k-1} \vee y_{i+k-1}) \oplus \gamma_i, & 0 \leqslant i < n-k, \\ u_{n-k} = x_0 \oplus y_0 \oplus 1 \oplus \gamma_{n-k}, & i = n-k, \\ u_i = x_{i-n+k} \oplus y_{i-n+k} \oplus (x_{i-n+k-1} \vee y_{i-n+k-1}) \oplus \gamma_i, & i > n-k. \end{cases}$$

Далі, по аналогії розглянемо праву частину рівності. Нехай:

$$f = \overrightarrow{x} \oplus \alpha \oplus \overrightarrow{y} \oplus \beta \oplus (((\overrightarrow{x} \oplus \alpha) \vee (\overrightarrow{y} \oplus \beta)) \ll 1) \oplus 1,$$

де

$$\overrightarrow{x} = x_{k-1}, \ldots, x_0, x_{n-1}, \ldots, x_k,$$

$$\overrightarrow{y} = y_{k-1}, \ldots, y_0, y_{n-1}, \ldots, y_k,$$

$$\alpha = \alpha_{n-1}, \ldots, \alpha_{n-k+1}, \alpha_{n-k}, \alpha_{n-k-1}, \ldots, \alpha_0,$$

$$\beta = \beta_{n-1}, \ldots, \beta_{n-k+1}, \beta_{n-k}, \beta_{n-k-1}, \ldots, \beta_0.$$

Звідси випливає наступна система рівнянь:

$$\begin{cases} f_0 = x_k \oplus \alpha_0 \oplus y_k \oplus \beta_0, & i = 0 \\ f_i = x_{i+k} \oplus \alpha_i \oplus y_{i+k} \oplus \beta_i \oplus & \\ \qquad \oplus ((x_{i+k-1} \oplus \alpha_{i-1}) \vee (y_{i+k-1} \oplus \beta_{i-1})), & 0 < i < n-k, \\ f_{n-k} = x_0 \oplus \alpha_{n-k} \oplus y_0 \oplus \beta_{n-k} \oplus & \\ \qquad \oplus ((x_{n-1} \oplus \alpha_{n-k-1}) \vee (y_{n-1} \oplus \beta_{n-k-1})) \oplus 1, & i = n-k, \\ f_i = x_{i-n+k} \oplus \alpha_i \oplus y_{i-n+k} \oplus \beta_i \oplus & \\ \qquad \oplus ((x_{i-n+k-1} \oplus \alpha_{i-1}) \vee (y_{i-n+k-1} \oplus \beta_{i-1})), & i > n-k. \end{cases}$$

Імовірність проходження RX-диференціалу дорівнює ймовірності того, що $u = f$. Обчислимо цю ймовірність, розглядаючи дану рівність побітово.

1. Якщо $i = 0$, то

$$x_k \oplus y_k \oplus (x_{k-1} \vee y_{k-1}) \oplus \gamma_0 = x_k \oplus \alpha_0 \oplus y_k \oplus \beta_0,$$
$$x_{k-1} \vee y_{k-1} = \alpha_0 \oplus \beta_0 \oplus \gamma_0.$$

2. Якщо $i = n - k$, то

$$x_0 \oplus y_0 \oplus 1 \oplus \gamma_{n-k} =$$
$$= x_0 \oplus \alpha_{n-k} \oplus y_0 \oplus \beta_{n-k} \oplus ((x_{n-1} \oplus \alpha_{n-k-1}) \vee (y_{n-1} \oplus \beta_{n-k-1})) \oplus 1 \Rightarrow$$
$$\alpha_{n-k} \oplus \beta_{n-k} \oplus \gamma_{n-k} = (x_{n-1} \oplus \alpha_{n-k-1}) \vee (y_{n-1} \oplus \beta_{n-k-1}).$$

3. Якщо $i < n-k$, то

$$x_{i+k} \oplus y_{i+k} \oplus (x_{i+k-1} \vee y_{i+k-1}) \oplus \gamma_i =$$
$$= x_{i+k} \oplus \alpha_i \oplus y_{i+k} \oplus \beta_i \oplus ((x_{i+k-1} \oplus \alpha_{i-1}) \vee (y_{i+k-1} \oplus \beta_{i-1})) \Rightarrow$$
$$\alpha_i \oplus \beta_i \oplus \gamma_i = ((x_{i+k-1} \oplus \alpha_{i-1}) \vee (y_{i+k-1} \oplus \beta_{i-1})) \oplus (x_{i+k-1} \vee y_{i+k-1}).$$

4. Якщо $i > n-k$, то

$$x_{i-n+k} \oplus y_{i-n+k} \oplus (x_{i-n+k-1} \vee y_{i-n+k-1}) \oplus \gamma_i =$$
$$= x_{i-n+k} \oplus \alpha_i \oplus y_{i-n+k} \oplus \beta_i \oplus ((x_{i-n+k-1} \oplus \alpha_{i-1}) \vee (y_{i-n+k-1} \oplus \beta_{i-1})) \Rightarrow$$
$$\alpha_i \oplus \beta_i \oplus \gamma_i = ((x_{i-n+k-1} \oplus \alpha_{i-1}) \vee (y_{i-n+k-1} \oplus \beta_{i-1})) \oplus (x_{i-n+k-1} \vee y_{i-n+k-1}).$$

Введемо наступні позначення:

$$\delta = \alpha \oplus \beta \oplus \gamma;$$
$$mask = (0,\ldots,0,1,0,\ldots,0,1),$$

де одиниці лише в позиціях $i = n-k$ та $i = 0$.

$$\varphi = (\alpha \vee \beta) \ll 1.$$

Нехай p_i — імовірність виконання рівності диференціального переходу в i-тому біті, тоді

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = \prod_{i=0}^{n-1} p_i.$$

Обчислимо імовірності p_i для кожного значення i.

1. Нехай $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = \delta_0$ і $i = 0$, то

$$x_{k-1} \vee y_{k-1} = \alpha_0 \oplus \beta_0 \oplus \gamma_0 = \delta_0.$$

Якщо $\delta_0 = 0$, то

$$p_0 = \Pr\{x_{k-1} \vee y_{k-1} = 0\} = \frac{1}{4}.$$

Якщо $\delta_0 = 1$, то

$$p_0 = \Pr\{x_{k-1} \vee y_{k-1} = 0\} = \frac{3}{4}.$$

Тому,

$$p_0 = \left(\frac{1}{4} + \frac{\delta_0}{2}\right).$$

2. Нехай $(x_{n-1} \oplus \alpha_{n-k-1}) \vee (y_{n-1} \oplus \beta_{n-k-1}) = \alpha_{n-k} \oplus \beta_{n-k} \oplus \gamma_{n-k} = \delta_{n-k}$ і $i = n-k$, тоді по аналогії з першим випадком, ймовірність проходження диференціалу буде дорівнювати:

$$p_{n-k} = \left(\frac{1}{4} + \frac{\delta_{n-k}}{2}\right).$$

3. Далі розглядаємо випадок для всіх інших i, коли $i \neq 0$ та $i \neq n-k$. Усі ці випадки описуються загальним рівнянням такого виду:

$$\begin{aligned}
\delta_i &= \alpha_i \oplus \beta_i \oplus \gamma_i = (x_* \vee y_*) \oplus ((x_* \oplus \alpha_{i-1}) \vee (y_* \oplus \beta_{i-1})) = \\
&= x_* \oplus y_* \oplus x_* y_* \oplus x_* \oplus \alpha_{i-1} \oplus y_* \oplus \beta_{i-1} \oplus x_* y_* \oplus \\
&\oplus x_* \beta_{i-1} \oplus y_* \alpha_{i-1} \oplus \alpha_{i-1} \beta_{i-1} = \\
&= x_* \beta_{i-1} \oplus y_* \alpha_{i-1} \oplus \alpha_{i-1} \oplus \beta_{i-1} \oplus \alpha_{i-1} \beta_{i-1},
\end{aligned}$$

де x_* та y_* є випадковими незалежними бітами.

У таблиці 2.2 наведено значення ймовірності p_i для усіх можливих значень параметрів даного рівняння.

Із наведених у таблиці 2.2 даних випливає, що існує єдине значення параметрів α_{i-1}, β_{i-1} і δ_i, за яких ймовірність $p_i = 0$. Відповідно,

$$\Pr\{\overrightarrow{v(x,y)} \oplus \gamma = v(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = 0$$

тоді та тільки тоді, коли існує таке i ($i \neq 0$ та $i \neq n-k$), при якому

Таблиця 2.2 – Таблиця ймовірностей проходження диференціалу через v(x,y).

α_{i-1}	β_{i-1}	δ_i	result	p_i
0	0	0	0=0	1
0	0	1	1=0	0
0	1	0	$0 = y_*$	$\frac{1}{2}$
0	1	1	$1 = y_*$	$\frac{1}{2}$
1	0	0	$0 = x_*$	$\frac{1}{2}$
1	0	1	$1 = x_*$	$\frac{1}{2}$
1	1	0	$0 = x_* \oplus y_* \oplus 1$	$\frac{1}{2}$
1	1	1	$1 = x_* \oplus y_* \oplus 1$	$\frac{1}{2}$

$\alpha_{i-1} = \beta_{i-1} = 0$ та $\delta_i = 1$, тобто

$$\Pr\{\overrightarrow{h(x,y)} \oplus \gamma = h(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} \neq 0 \Leftrightarrow (\delta \vee \overline{\varphi}) \wedge \overline{mask} = 0.$$

З даної таблиці випливає 2 випадки, коли ймовірність дорівнює нуль, і коли не дорівнює.

Тобто,

$$\Pr\{\overrightarrow{v(x,y)} \oplus \gamma = v(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = 0$$

тоді, і тільки тоді, коли існує таке i, яке $\neq 0$ та $\neq n-k$, при якому $\alpha_{i-1} = \beta_{i-1} = 0$ та $\delta_i = 1$.

Якщо ймовірність RX-диференціалу не дорівнює нулю, то у випадку $\alpha_{i-1} = \beta_{i-1} = 0$ імовірність p_i дорівнює одиниці, а в усіх інших випадках (коли хоча б один з двох бітів α_{i-1}, β_{i-1} дорівнює одиниці) імовірність p_i дорівнюватиме $\frac{1}{2}$. Таким чином, з усіх наведених співвідношень випливає, що

$$\Pr\{\overrightarrow{v(x,y)} \oplus \gamma = v(\overrightarrow{x} \oplus \alpha, \overrightarrow{y} \oplus \beta)\} = \\ = \left(\frac{1}{4} + \frac{\delta_0}{2}\right)\left(\frac{1}{4} + \frac{\delta_{n-k}}{2}\right) \cdot 2^{-wt(\varphi \wedge \overline{mask})},$$

де $\delta = \alpha \oplus \beta \oplus \gamma$, $\varphi = (\alpha \vee \beta) \ll 1$. Звідси випливає твердження теореми. □

Результат даної теореми майже аналогічний теоремі 2.2; зокрема, даний результат також показує, що диференціально-обертальний криптоаналіз кобмінує техніки обертального та диференціального криптоаналізів на рівні аналітичних результатів.

Також, порівнюючи отримані результати між собою, можна побачити, що:

1) у випадку, коли $\delta_0 = \delta_{n-k} = 0$, то перші два множники першої теореми дають результат $\frac{9}{16}$, а перші два множники другої теореми дорівнюють $\frac{1}{16}$, тобто при вказаних значеннях дельти бачимо, що результати відрізняються у 9 разів.

2) у випадку, коли $\delta_0 = \delta_{n-k} = 1$, отримаємо, що результат перших двох множників першої теореми дорівнює $\frac{1}{16}$, а другої $\frac{9}{16}$, тобто при вказаних значеннях дельти результати також відрізняються у 9 разів.

3) у випадку, коли одне із значень дельти дорівнює нулю, а інше дорівнює одиниці отримаємо однакові результати для обох теорем ($\frac{3}{16}$).

Таким чином, бачимо, що ймовірності довільного RX-диференціалу для обох операцій або співпадають, або відрізняються у 9 разів.

Приведені результати дозволяють стверджувати, що обидві операції мають приблизно однаковий рівень стійкості до RX-аналізу та можуть використовуватися як альтернативи.

Висновки до розділу 2

У даному розділі було уточнено результат Ашура і Лю, за допомогою якого можна більш гнучко будувати диференціально-обертальні атаки, використовуючи усі можливі значення зсувів, та провадити оцінки стійкості ARX-криптосистем до атак такого виду.

Було знайдено аналітичні вирази для ймовірностей проходження RX-диференціалів через операції $h(x,y)$ та $v(x,y)$. З одержаних результатів видно, що поведінка імовірностей RX-диференціалів функцій $h(x, y)$ та $v(x, y)$ описується практично ідентичними виразами, а чисельні значення або співпадають, або відрізняються в 9 разів (за рахунок відмінностей у бітах на позиціях 0 та $n - k$). Це дозволяє стверджувати, що обидві операції мають приблизно однаковий рівень стійкості до RX-аналізу та можуть використовуватись як альтернативи.

ВИСНОВКИ

У даній роботі було розглянуто диференціальний і обертальний криптоаналізи, а також техніку диференціально-обертального криптоаналізу, яку запропонували Ашур та Лю.

Також, було розглянуто застосування диференціально-обертального криптоаналізу до класів LRX-криптосистем, що використовують операції, які апроксимують модульне додавання. У роботі розглядалось дві таких операції, одну з яких було запропоновано у шифрі NORX.

Було уточнено аналітичні вирази для ймовірностей проходження RX-диференціалів через операцію модульного додавання, які застосовні для будь-якої величини циклічного зсуву векторів на відміну від зсуву на один біт у Ашура і Лю. Ці результати розширюють можливості для проведення аналізу класичних ARX-криптосистем.

Було знайдено аналітичні вирази для імовірностей RX-диференціалів таких операцій та сформульовано умови їх неможливості. Показано, що для обох операцій RX-диференціали мають однакову умову неможливості, а значення імовірностей можливих диференціалів або співпадають, або відрізняються у константну кількість разів. Це дозволяє стверджувати, що обидві операції, які розглядались, забезпечують однаковий рівень стійкості до RX-аналізу.

Одержані результати дозволять оцінювати стійкість LRX-криптосистем до диференціально-обертального криптоаналізу і використовувати існуючі інструменти для побудови перспективних LRX-криптосистем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Biham, Eli and Adi Shamir. Differential Cryptanalysis of the Data Encryption Standard. [електронний ресурс] // 1993. – Режим доступу: https://doi.org/10.1007/0-387-23483-7_108

2. Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems. [електронний ресурс] //J. Cryptology 4, 3–72 1991. – Режим доступу: https://doi.org/10.1007/BF00630563

3. Biham, E., Shamir, A. Differential Cryptanalysis of the Full 16-round DES. [електронний ресурс] // In: Brickell, E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. 1993. – https://doi.org/10.1007/3-540-48071-4_34

4. Khovratovich, D., Nikolić, I. (2010). Rotational Cryptanalysis of ARX. [електронний ресурс] // In: Hong, S., Iwata, T. (eds) Fast Software Encryption. FSE 2010. Lecture Notes in Computer Science, vol 6147. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13858-4_19

5. Daum, M. Cryptanalysis of Hash Functions of the MD4-Family. [електронний ресурс] // PhD thesis, Ruhr-Universität Bochum 2005. – https://d-nb.info/97642777x/34

6. Ashur, T. and Liu, Y. Rotational Cryptanalysis in the Presence of Constants [електронний ресурс]// Cryptology ePrint Archive, Report 2016/826 2016. – Режим доступу: https://eprint.iacr.org/2016/826.pdf

7. Jinyu Lu, Yunwen Liu, Tomer Ashur, Bing Sun, Chao Li. Rotational-XOR Cryptanalysis of Simon-like Block Ciphers. [електронний ресурс]// Cryptology ePrint Archive, Report 2020/486 2020. – Режим доступу: https://eprint.iacr.org/2020/486.pdf

8. Jinyu Lu, Yunwen Liu1, Tomer Ashur, Bing Sun, Chao Li. Improved Rotational-XOR Cryptanalysis of Simon-like Block Ciphers. [електронний ресурс]// Cryptology ePrint Archive, Report 2022/402 2022. – Режим доступу: https://eprint.iacr.org/2022/402.pdf

9. Adri´an Ranea, Yunwen Liu, Tomer Ashur. An Easy-To-Use Tool for Rotational-XOR Cryptanalysis of ARX Block Ciphers. [електронний ресурс]// Cryptology ePrint Archive, Report 2020/727 2020. – Режим доступу: https://eprint.iacr.org/2020/727.pdf

10. Yunwen Liu, Glenn De Witte, Adrián Ranea and Tomer Ashur. Rotational-XOR Cryptanalysis of Reduced-round SPECK. [електронний ресурс]// Cryptology ePrint Archive, Report 2017/1036 2017. – Режим доступу: https://eprint.iacr.org/2017/1036.pdf

11. Jean-Philippe Aumasson, Philipp Jovanovic and Samuel Neves. Analysis of NORX: Investigating Differential and Rotational Properties. [електронний ресурс]// Cryptology ePrint Archive, Report 2014/317 2014. – Режим доступу: https://eprint.iacr.org/2014/317.pdf

12. Яковлєв, С.В. Криптографічні властивості операцій, які апроксимують додавання за модулем. Матеріали Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерне моделювання» (15-16 грудня 2022 року, м. Івано-Франківськ)".