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.

Дипломна робота

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

зі спеціальності: 113 Прикладна математика
на тему: **«Диференціально-обертальний криптоаналіз деяких ускладнюючих функцій ARX-криптосистем»**

Виконав:
студент 4 курсу, групи ФІ-94
Панасюк Єгор Сергійович _____

Керівник:
доц. каф. ММЗІ, к.т.н.
Яковлєв Сергій Володимирович _____

Рецензент:
ст. викл. кафедри ММАД, Ph.D. Яйлимова Г.О.
Яйлимова Ганна Олексіївна _____

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

Студент _____

Київ — 2023

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

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

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

ЗАВДАННЯ
на дипломну роботу

Студент: Панасюк Єгор Сергійович

1. Тема роботи: «*Диференціально-обертальний криптоаналіз деяких ускладнюючих функцій ARX-криптосистем*», науковий керівник дисертації: доц. каф. 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: *Ускладнюючу функції ARX-криптосистем*

4. Предмет дослідження: *Диференціально - обертальний криптоаналіз*

5. Перелік завдань: *Обертальний аналіз функції* $f(x) = (3x) mod 2^n$, *обертальний аналіз логічних функцій ускладнення,RX-аналіз лінійних функцій ускладнення,RX-аналіз нелінійних функцій ускладнення*

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: *Презентація доповіді*

7. Орієнтовний перелік публікацій: *планується доповідь на всеукраїнській конференції*

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-жовтень 2022 р.	Виконано
3	Знаходження імовірності проходження пар обертання через множення на малу константу.	Жовтень-листопад 2022 р.	Виконано
4	Знаходження імовірності проходження пар обертання через ускладнюючі функції, які апроксимують таке множення	Листопад-грудень 2022 р.	Виконано
5	Проведення диференціально-обертального криптоаналізу лінійних відображень	Січень-лютий 2023 р.	Виконано
6	Проведення диференціально-обертального криптоаналізу зазначених ускладнюючих функцій	Березень-квітень 2023 р.	Виконано
7	Оформлення отриманих результатів	Травень-червень 2023 р.	Виконано

Студент _____ Єгор Панасюк

Керівник _____ Сергій Яковлєв

РЕФЕРАТ

Кваліфікаційна робота містить: 45 стор., 6 рисунки, 20 таблиць, 9 джерел.

Метою роботи є удосконалення методів криптоаналізу ARX-криптосистем. Об'єктом дослідження є інформаційні процеси в системах криптографічного захоисту. Предметом дослідження є ARX-криптосистеми та методи їх криптоаналізу.

У ході роботи було отримано імовірності проходження пар обертання через функцію $3X mod 2^n$ та через певні логічні функції ускладнення, що використовають такі операції, як І, АБО, КСОР. Також бало узагальнено певні раніше відомі результати та показано шлях до їх отримання.Було проведено диференціально-обертальний криптоаналіз для логічних функцій ускладнення.

ARX-КРИПТОСИСТЕМИ, RX-АНАЛІЗ, ДИФЕРЕНЦІЙНИЙ АНАЛІЗ

ABSTRACT

The qualification work contains:45 p., 6 figures, 20 tables, 9 sources.

The aim of the work is to improve the methods of cryptanalysis of ARX cryptosystems. The object of research is information processes in cryptographic security systems. The subject of research is ARX cryptosystems and methods of their cryptanalysis.

In the course of the work, the probabilities of rotation pairs passing through the function $3Xmod2^n$ and through certain logic functions of complication using such operations as AND, OR, and XOR were obtained. Certain previously known results were also summarized and the way to obtain them was shown. A differential-rotational cryptanalysis was performed for the logical functions of complication.

ARX-CRYPTOSYSTEMS, RX-ANALYSIS, DIFFERENTIAL ANALYSIS

ЗМІСТ

ВСТУП

Актуальність дослідження.Останнім часом публікується все більше спрощених криптографічних примітивів. Більшість з них відносяться до ARX, які показали чудову продуктивність у програмному забезпеченні. Оскільки наразі у мережу зареєстровано понад 20 000 000 000 девайсів, то очевидно, що багато з них є дуже обмеженими у обчислювальній потужності, настільки що не можуть використовувати такі ж криптографічні алгоритми, що і PC. Прикладом таких пристроїв є RFID (Radio-Frequency IDentification) чіпи. Тому ARX-примітиви є оптимальними для реалізації, бо використовують лише прості операції.

Метою дослідження є удосконалення методів криптоаналізу ARX-криптосистем. Для досягнення мети необхідно виконати такі **завдання**:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) знайти імовірності проходження пар обертання через множення на малу константу та через ускладнюючі функції, які апроксимують таке множення;

3) провести диференціально-обертальний криптоаналіз лінійних відображень;

4) провести диференціально-обертальний криптоаналіз зазначених ускладнюючих функцій.

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

Предметом дослідження ARX-криптосистеми та методи їх криптоаналізу.

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

Наукова новизна отриманих результатів:вперше проведено обертальний та диференціально-обертальний криптоаналіз деяких

функцій ускладнення ARX-криптосистем, одержано аналітичні вирази для імовірностей, які характеризують стійкість до даних видів атак.

Практичне значення роботи. Одержані результати можуть бути використані для аналізу існуючих та побудови нових надійних ARX-криптосистем.

1 ВСТУП ДО ARX КРИПТОСИСТЕМ ТА ОБЕРТАЛЬНОГО КРИПТОАНАЛІЗУ

1.1 Що таке *ARX-криптосистеми* та *обертальний криптоаналіз*

Означення 1.1. ARX-структура це криптографічний примітив, що використовує 3 операції, XOR($\oplus$), циклічні зсуви та додавання за модулем 2^n.

Загальноприйнято вважати, що поєднання цих операцій дає хороший примітив, якщо кількість раундів достатня. Однак, немає формальної теорії, чи всі три операції необхідні та достатні для забезпечення усіх криптографічних потреб.

ARX-структури використовуються у таких функціях, як Skein та BLAKE, які були фіналістами SHA-3, потоковому шифрі Salsa20 та ChaCha, або блокових шифрах TEA, XTEA і Speck, а також у MAC алгоритмі Chaskey. Тож у них дуже широкий спектр застосування.

Означення 1.2. ***Обертальний криптоаналіз*** — це метод криптоаналізу відкрих текстів з вибраним пов'язаним ключем, запропонований Ховратовичем. По суті, при використані обертального криптоаналізу, зловмисник запитує шифрування пари відкритих текстів, де один відкритий текст отримується шляхом циклічного обертання іншого. Ховратовіч та інші показали, що пара обертання проходить з певною ймовірністю за рахунок ARX операцій.

Означення 1.3. Зафіксуємо деяке число $r(1 \leqslant r \leqslant n)$ та для $x \in V_n$ позначимо $\overrightarrow{x} = x \ggg r$. Пара $(x, \overrightarrow{x})$ називається парою обертання.

Твердження 1.1. *Пара обертання з ймовірністю 1 проходить через операції XOR($\oplus$) та циклічного зсуву($x \ggg i$)*

$$Pr\{\overrightarrow{x \oplus y} = \overrightarrow{x} \oplus \overrightarrow{y}\} = 1$$

$$Pr\{\overrightarrow{x \ggg i} = \overrightarrow{x} \ggg i\} = 1$$

і з максимальною ймовірністю $\frac{3}{8}$ *через додавання за модулем(залежить від r):*

$$Pr\{\overrightarrow{x} + \overrightarrow{y} = \overrightarrow{x+y}\} \leqslant \frac{3}{8}$$

Лема 1.1. $Pr\{(\overrightarrow{x+y} = \overrightarrow{x} + \overrightarrow{y}\} = \frac{1}{4}(1 + 2^{r-n} + 2^{-r} + 2^{-n})$*[4]*

Теорема 1.1. *Нехай q – кількість додавань у ARX схемі і* $P = Pr\{\overrightarrow{x} + \overrightarrow{y} = \overrightarrow{x+y}\}, (x, \overrightarrow{x})$ *– пара обертання пройде через схему з ймовірністю* P^q

ARX-C це ARX з введенням константи. Саме поява констант дуже сильно ускладнює криптоаналіз.

Означення 1.4. Введемо поняття обертальної похибки

$$E(X,Y) = \overrightarrow{X} \oplus Y$$

Очевидно, що $E(X,\overrightarrow{X})$=0

Додавання константи може спричинити помилку обертання (точна ймовірність залежить від r, значення константи та від того, який тип додавання використовується — модульне чи XOR). З іншого боку, модульне додавання змінних також може генерувати помилку, і з певною ймовірністю ці помилки компенсують одна одну:

$$E(X + Y + Z + C, \overrightarrow{X} + \overrightarrow{Y} + \overrightarrow{Z} + C) = 0.$$

Також достатньо очевидно, що якщо $C = \overrightarrow{C}$, то ніякого ускладнення для криптоаналізу немає.

1.2 Дослідження Ховратовича

Почнемо з досліджень, які було проведено Ховратовичем, який і започаткував обертальний криптоаналіз. [1]

Хоча модульне додавання часто апроксимується за допомогою XOR, для випадкових вхідних даних ці операції є зовсім різними. Додавання забезпечує дифузію та нелінійність, тоді як XOR ні. Хоча дифузія є відносно повільною, вона компенсується низькою складністю додавання як у програмному, так і в апаратному забезпеченні, тому примітиви з відносно великою кількістю додавання (десятки на байт) все ще швидкі. Обертання всередині слова усуває дисбаланс між лівими та правими бітами (введений додаванням) і прискорює дифузію.

З того, що пара обертання проходить через операцію додавання з ймовірністю $\frac{3}{8}$(див. твердження 1.1) отримуємо універсальну верхню оцінку безпеки ARX-криптосистем.

У статі було розглянуто як зменшені версії Threefish (блоковий шифр, який використовується в хеш-функції Skein) можна аналізувати за допомогою обертального криптоаналізу. Також було показано, що можна зламати 39, 42 і 43,5 раунди оригінальної версії Threefish-256, -512, 1024 з складністю $2^{252.4}, 2^{507}, 2^{1014,5}$ шифрувань відповідно.

Атаку було побудовано за алгоритмом:

1.Згенерувати довільний текст P та закодувати з ключем K;

2.Обрахувати P' та закодувати з ключем K'

3.Перевірити, чи $(E_K(P), E_{K'}(P'))$ – пара обертання.

Пара обертання дає інформацію про крайні ліві біти кожного слова ключа.

Текст P_i рахується:

$$P'_i = \overrightarrow{P_i} \oplus d_i$$

Ключ K_i рахується:

$$K_i = \overrightarrow{K_i} \oplus e_i$$

Значення d_i, e_i визначаються з таблиці на малюнку 1.1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Threefish-256																
d_i	3	10	3	15												
e_i	6	10	6	15												
Threefish-512																
d_i	0	6	3	6	3	6	3	6								
e_i	5	6	6	6	6	6	6	6								
Threefish-1024																
d_i	0	6	3	6	3	6	3	6	3	6	3	6	3	6	3	6
e_i	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

Рисунок 1.1 – Значення d_i, e_i для кожної з версій Threefish.

Також було доведено, що над Z_{2^n} використовуючи операції XOR,AND і циклічні зсуви, а також додавання константи можна реалізувати будь-яку функцію.

Було показано що AR системи(ARX системи без операції XOR) теоретично є еквівалентними до ARX систем, але не є захищеними.

1.3 Переглянуті і доповнені дослідження Ховратовича

З часом дослідження були переглянуті та викладені у статті [2]

Означення 1.5. Ланцюг Маркова - Послідовність випадкових

величин $X_n, n \geqslant 0$ називають ланцюгом Маркова, якщо для довільного натурального числа $n \geqslant 1$ має місце рівність $\mathrm{P}(X_n = i_n \mid X_{n-1} = i_{n-1}, \ldots, X_0 = i_0) = \mathrm{P}(X_n = i_n \mid X_{n-1} = i_{n-1})$, де $i_0, i_1, \ldots i_n$ - довільні елементи множини E.

Твердження 1.2. *Лай і Мессі показали, що якщо раундві ключі вибрані випадково, незалежно і рівномірно, то шифр можна змоделювати як ланцюг Маркова. Це називається припущенням ланцюга Маркова.[3]*

Твердження 1.3. *Припущення ланцюга Маркова виконується практично в усіх диференціальних та ймовірнісних атаках, навіть не зважаючи на те, що раундові ключі є незалежними але виробляються за 1 алгоритмом. В цілому на практиці у примітивах незалежність і випадковість раундових ключів замінюють*

Вони вводять достатню ентропію, тому можна вважати, що припущення ланцюга Маркова виконується, однак є винятки.

Було показано, що у обертальному криптоаналізі ARX-криптосистем припущення ланцюга Маркова не завжди виконується.

Було встановлено що ймовірність обертання примітиву ARX залежить не лише від кількості додавань за модулем, але й від їх позицій.

Загалом, чим більше додавань за модулем ланцюгом (вихід попередніх додавань є входом наступних), тим менша ймовірність. Розроблено явну формулу для ймовірності таких ланцюжкових додавань і показано, що ймовірність обертання ARX слід обчислювати як добуток ймовірностей обертання модульних ланцюжкових додавань.

Також було показано, що те, як раундові ключі включені в стан, відіграє вирішальну роль у розрахунку ймовірності проходження пари обертання. Коли раундові ключі проходять через XOR до стану, вони можуть розірвати ланцюжки модульних додавання і таким чином збільшити ймовірність. З іншого боку, якщо їх об'єднати за допомогою модульного додавання, ймовірність проходження пари обертання ARX

може бути зменшена.

На приклад малюнку 1.2 було показано, що теорема 1.1 виконується лише при непослідовних додаваннях.

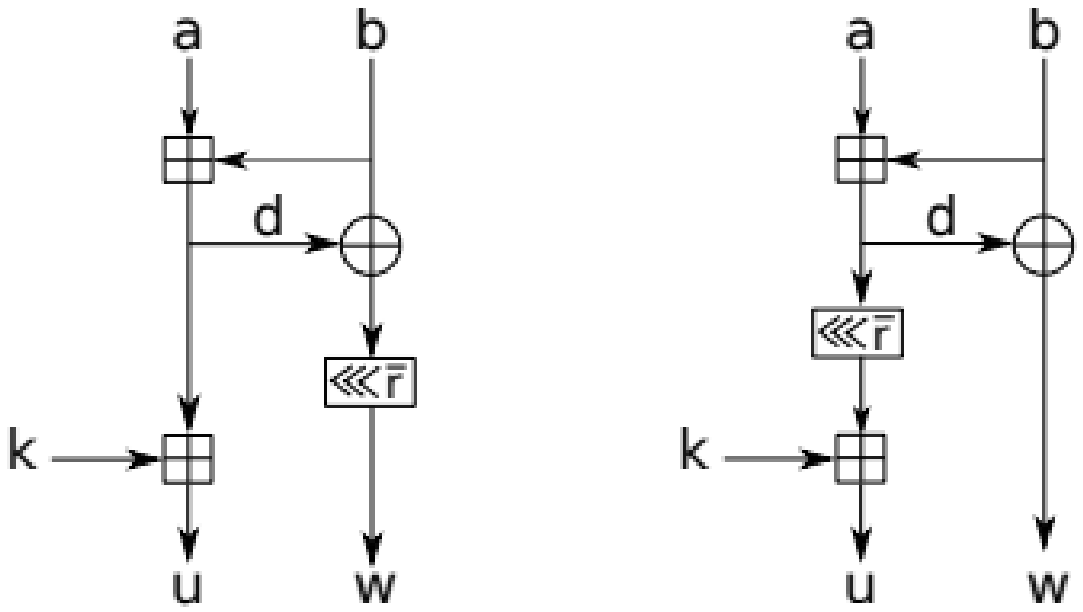

Рисунок 1.2 – Приклад двох ARX шифрів з однаковою кількістю додавань, але різною ймовірністю проходження пари обертання.

Лема 1.2 (Ланцюгові додавання за модулем)**.** *Нехай* $a_1, ... < a_k$ *n-бітові слова вибрані довільно, r- ціле, таке що* $0 \leqslant r \leqslant n$ *тоді*

$$Pr\{[(a_1 + a_2) \lll r = a_1 \lll r + a_2 \lll r] \wedge$$

$$[(a_1 + a_2 + a_3) \lll r = a_1 \lll r + a_2 \lll r + a_3 \lll r] \wedge ...$$

$$\wedge [(a_1 + ... + a_k) \lll r = a_1 \lll r + ... + a_k \lll r]\}$$

$$= \frac{1}{2^{nk}} \begin{pmatrix} k + 2^r - 1 \\ 2^r - 1 \end{pmatrix} \begin{pmatrix} k + 2^{n-r} - 1 \\ 2^{n-r} - 1 \end{pmatrix}$$

Твердження 1.4. *Ланцюгові додання за модулем не утворюють*

ланцюг Маркова і ймовірність проходження пари обертання не може бути порахована як добуток ймовірностей проходження через кожну суму, з леми 1.2.

1.4 Обертальний криптоаналіз криптосистеми MORUS

MORUS – це ARX-приптопримітив, що є фіналістом конкурсу CAESAR.

Параметри криптосистеми:

Слово 32/64 біти для MORUS-640/1280 відповідно.

Блок 128/256 біти для MORUS-640/1280 відповідно.

$Rotl\_xxx\_yy(x, b)$ розділяє xxx-бітовий блок на 4 yy-бітових блоки і зсуває кожне слово на b бітів.

$K = k_0 k_1 ... k_{l_{k-1}}$-Секретний ключ розміру l_k бітів

const0: 128 бітна константа 0x000101020305080d1522375990e97962 у хексі

const1: 128 бітна константа 0xdb3d18556dc22ff12011314273b528dd у хексі

S^t - Внутрішній стан на кроці t

S^t_j - Внутрішній стан на j-му раунді кроку t

На малюнку 1.3 можна побачити параметри $bi\omega$, вони беруться з таблиці 1.4

Було досліджували доцільність обертального криптоаналізу на різних варіантах MORUS[5]. Їх дослідження показало, що всі операції, які використовуються в MORUS, зберігають пари обертання, коли відстань обертання кратна 32 або 64 для MORUS640 і MORUS-1280 відповідно. Вони також переконалися, що супротивник може будувати розрізнювач для повної версії MORUS, якщо константа є обертальним інваріантом самої себе. Однак константи, які використовуються в MORUS, не є обертально-інваріантними, що робить неможливим створення розрізнювача для більш ніж одного кроку. Завдяки неінваріантним

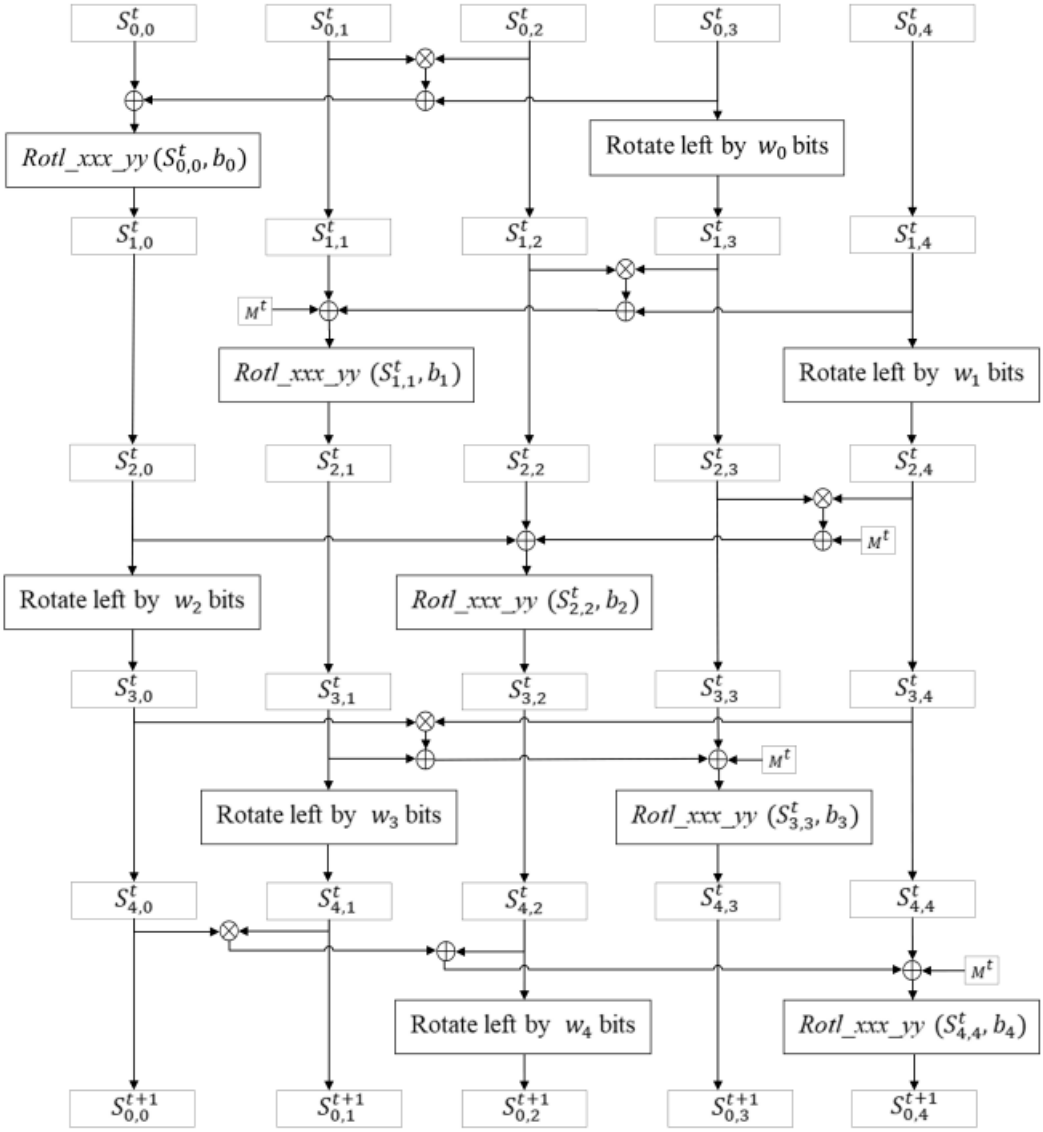

Рисунок 1.3 – Функція оновлення стану MORUS

константам, які використовуються у функції оновлення стану MORUS, виявлено, що ротаційний криптоаналіз може розрізняти вихідні дані MORUS лише для одного кроку . Для більш ніж одного кроку ймовірність збереження ротаційної пари стає 0,5 у більшості бітів. Це робить неможливим застосування розрізнювача для більш ніж одного раунду.

Проаналізувано константи MORUS-640 при застосуванні до нього r-бітного обертання. Досілджено кількість бітів у константі, які є інваріантними для r-біта обертання. MORUS-640 застосовує операцію Rotl_128_32(x, b) у своїй функції оновлення стану. Rotl_128_32(x, b)

	MORUS-640	MORUS-1280
b_0	5	13
b_1	31	46
b_2	7	38
b_3	22	7
b_4	13	4
w_0	32	64
w_1	64	128
w_2	96	192
w_3	64	128
w_4	32	64

Рисунок 1.4 – Константи MORUS

зберігає обертальні пари, якщо відстань обертання кратна 32 бітам, тобто 32, 64 або 96. Тому для аналізу констант MORUS-640 , ми встановлюємо відстань обертання r кратну 32. З наведеними вище умовами константа також має мати обертання 32, 64, 96 або 128 бітів незмінним залежно від відстані застосованих обертань. Якщо константа 32-розрядний інваріант обертання (тобто константу можна розділити на 4 маленькі підслова по 32 біти, де кожне підслово однакове), то є 2 інваріантні константи обертання з r=32. для 64-бітового інваріантну константи обертання, є 264 інваріантні константи. Досліджено обертання інваріантних бітів у константах для будь-якої відстані обертання, кратної r = 32.

1.5 Обертальний криптоаналіз Keccak

У цій статті [6] було атаковано хеш-функцію Keccak зі зменшеною кількістю раундів за допомогою обертального криптоаналізу. Автори зосередились на варіантах Keccak, запропонованих як кандидати на SHA-3 у конкурсі NIST на новий стандарт криптографічної хеш-функції. Їх головний результат — атака прообразу на 4-раундKeccak і 5-раунд розрізнювача на перестановці Keccak-f[1600] — основний будівельний блок хеш-функції Keccak.

1.6 Обертальний криптоаналіз Chaskey

Chaskey – Алгоритм MAC для 32-розрядних мікроконтролерів.

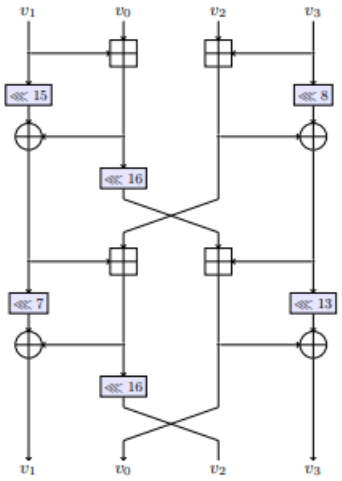

Рисунок 1.5 – Схема 1 раунду Chaskey

У цій роботі [7] показано, як, використовуючи властивість обертальних ймовірностей, ми можемо підробити дійсний тег за допомогою алгоритму MAC Chaskey. Результати не порушують безпеку алгоритму на практиці та не порушують твердження авторів щодо безпеки, однак вони показують вразливість у базовій перестановці. Найкращий результат – це розрізняльна атака на повну кількість раундів алгоритму зі складністю 2^{86}. Алгоритм Chaskey передбачає, що лише останні t бітів виводу можна використовувати як тег. Їх атака спрямована на всі 128 біт. Однак для коротшого тегу результати можна покращити, дотримуючись лише властивості обертання до 2 або 3 слів виводу. Це підлягає подальшому аналізу.

1.7 Обертальний криптоаналіз ГОСТ-у з однаковими S-блоками

ГОСТ 28147-89 радянський і російський стандарт симетричного шифрування, введений в 1990 році, також був стандартом СНД.

Це блоковий шифр Фейстеля з 32 раундами, з блоками по 64-біти і ключем 256-біт.

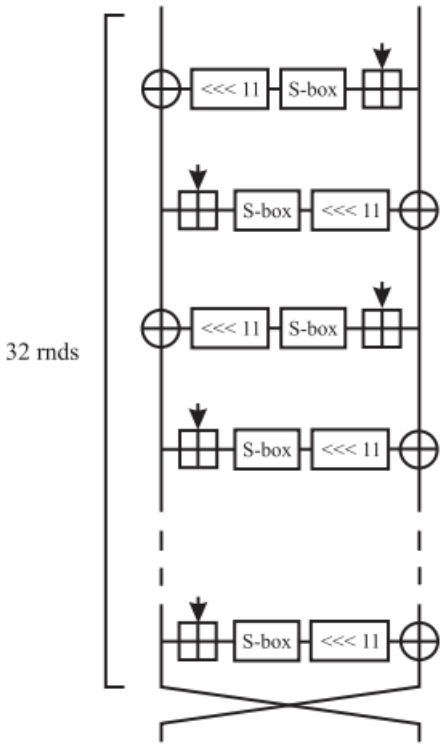

Рисунок 1.6 – Схема 1 раунду GOST

У цій статті [8] показано, що повторювані підключі також мають значний негативний вплив на обертальні властивості ГОСТу. Основні результати стосуються ГОСТу без S-блоків. Хоча нереалістично очікувати, що користувач не вибере набір сильних S-блоків. Деякі реалізації можуть дозволити супротивнику маніпулювати вибором S-блоку або обманом змусити користувача використати відображення ідентичності замість набору дійсних нелінійні S-блоків. Подібний підхід

(видалення S-блоків ГОСТу) використовувався для аналізу фіксованих точок ГОСТу .

Аналіз не охоплює розподіл похибок обертання. Попередні експериментальні результати показують, що розподіл похибок обертання також можна використовувати як розрізнювач. Це може призвести до більш сильних атак обертального типу на ГОСТ у майбутньому. Таким чином, рекомендується для кожної реалізації GOST або використовувати фіксований асиметричний набір S-блоків, або явно перевіряти параметри S-блоку на наявність обертальної симетрії, яку можна використовувати.

2 АНАЛІЗ ДЕЯКИХ ФУНКЦІЙ УСКЛАДНЕННЯ

2.1 Обертальний аналіз функції $f(X) = (3X) mod 2^n$

Дуже часто в ARX-криптосистемах використовується множення на малі константи, бо фактично фунція $f(X) = (3X) \bmod 2^n$ перетворюється у $(2X + X) \bmod 2^n$, а це в свою чергу сума X та $X \ll 1$.

Зсув ліворуч

Задачею обертального аналізу в першому випадку буде знайти ймовірність:

$$Pr_X\{f(\overleftarrow{X}) = \overleftarrow{f(X)}\} = Pr_X\{3(X \lll 1) = (3X) \lll 1\}$$

У статті [9] було опубліковано результати, а саме:

$$Pr\{3(X \lll 1) \bmod 2^{32} = (3X \bmod 2^{32}) \lll 1\} = \frac{2^{31} - 1}{3 \cdot 2^{32}}$$

Ці результати були опубліковані лише як факт і ніде більше не згадувались, тому наводжу порядок дій, які дозволяють отримати такий результат:

Таблиця 2.1 – Візуальне представлення чому будуть рівні біти у функції $(3X) \lll 1$

Біти переносу	c_{n-1}	c_{n-2}	...	c_2	$c_1 = 0$	$c_0 = 0$
X	X_{n-1}	X_{n-2}	...		X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...		X_0	0
$3X$	Y_{n-1}	Y_{n-2}	...		Y_1	Y_0
$3X \lll 1$	Y_{n-2}	Y_{n-3}	...		Y_0	Y_{n-1}

З таблиці 2.1 можна побачити, що :

$$Y_0 = X_0$$

$$Y_1 = X_0 \oplus X_1$$

$$Y_k = X_k \oplus X_{k-1} \oplus c_k$$

для $k \geqslant 2$

Таблиця 2.2 – Візуальне представлення чому будуть рівні біти у функції $3(x \lll 1)$

Біти переносу	c'_{n-1}	c'_{n-2}	...	c'_2	$c'_1 = 0$	$c'_0 = 0$
$X \lll 1$	X_{n-2}	X_{n-3}	...		X_0	X_{n-1}
$2(X \lll 1)$	X_{n-3}	X_{n-4}	...		X_{n-1}	0
$3(X \lll 1)$	W_{n-1}	W_{n-2}	...		W_1	W_0

З таблиці 2.2 можна побачити, що :

$$W_0 = X_{n-1}$$

$$W_1 = X_{n-1} \oplus X_0$$

$$W_k = X_{k-1} \oplus X_{k-2} \oplus c'_k$$

для $k \geqslant 2$

Тепер прирівняємо ці твердження так, як нам треба, а саме, щоб відповідні біти були рівними.Отримаємо систему з багатьох рівнянь:

$$Y_{n-1} = W_0 \Rightarrow X_{n-1} \oplus X_{n-2} \oplus c_{n-1} = X_{n-1}$$

$$Y_0 = W_1 \Rightarrow X_0 = X_{n-1} \oplus X_0$$

$$Y_1 = W_2 \Rightarrow X_1 \oplus X_0 = X_1 \oplus X_0 \oplus c'_2 \Rightarrow c'_2 = 0 \Rightarrow c'_k = c_{k-1}$$

З твердження, яке ми отримали на минулому кроці виходить, що усі наступні твердження для W_{k+1} і Y_k будуть тотожніми:

$$X_k \oplus X_{k-1} \oplus c_k = X_k \oplus X_{k-1} \oplus c'_{k+1}$$

Виходить, що ймовірність проходження пари обертання буде визначатись першими трьома рівностями.

Знайдемо ймовірність того, що $c'_2 = 0$:

Значення $c'_2 = \lfloor (X_0 + X_{n-1} + c'_1)/2 \rfloor$

$c'_1 = 0$, як можна побачити в нашому візуальному представленні, а $x_{n-1} = 0$ з 2 рівняння, тож $Pr\{c'_2 = 0\} = 1$.

Виходить що все буде визначатись 2-ма рівняннями, а сама ймовірність матиме вигляд:

$$Pr_X\{f(\overleftarrow{X}) = \overleftarrow{f(X)}\} = Pr_X\{3(X \lll 1) = (3X) \lll 1\} =$$

$$= Pr\{X_{n-1} = 0\} \cdot Pr\{X_{n-2} = c_{n-1}\}$$

Якщо вектор x береться рівноймовірно, то перша ймовірність $Pr\{X_{n-1} = 0\} = 1/2$

Позначимо за $p_k = Pr\{X_{k-2} = c_{k-1}\}$

Позначимо за $p_{k,0} = Pr\{X_{k-2} = c_{k-1} = 0\}$

Позначимо за $p_{k,1} = Pr\{X_{k-2} = c_{k-1} = 1\}$

Нехай n=2, тоді $c_1 = X_0$, але $c_1 = 0$ завжди, тоді буде очевидно, що:

$$p_{1,0} = Pr\{X_0 = 0\} = 1/2, p_{1,1} = 0$$

Поглянемо, що відбудеться при n=3

$c_2 = X_1$, Якщо розписати детально як виражається c_2 отримаємо:

$c_2 = \lfloor (X_0 + X_1 + c_1)/2 \rfloor = X_1$, оскільки $c_1 = 0 \Rightarrow c_2 = \lfloor (X_0 + X_1)/2 \rfloor = X_1$

Розглянемо два випадки, коли $X_1 = 1 \Rightarrow c_2 = 1$

Така подія може статись лише в тому випадку, коли одночасно $X_1 = X_0 = 1$, тому:

$$p_{2,1} = Pr\{X_1 = 1\} \cdot Pr\{X_0 = 1\} = 1/4$$

А також випадок, коли $X_1 = 0 \Rightarrow c_2 = 0$

В цьому випадку достатньо того, що $x_1 = 0$, а яке значення приймає x_0 не важливо:

$$p_{2,0} = Pr\{X_1 = c_2 = 0\} \cdot 1 = 1/2$$

Проаналізуємо, що відбуватиметься в k+1-біті:

Нехай $n = k + 1$:

$$c_k = X_{k-1} \Rightarrow \lfloor (X_{k-1} + X_{k-2} + c_{n-1})/2 \rfloor$$

Аналогічно як і для n=3 розглянемо два випадки, коли $x_{k-1} = 1$:

$X_{k-1} = 1 \Rightarrow c_k = 1$, це не виконається лише в тому випадку, коли $X_{k-2} = c_{k-1} = 0$, а це та ж сама ймовірність $p_{k-1,0}$, тоді:

$$p_{k,1} = \frac{1}{2}(1 - p_{k-1,0})$$

Розглянемо випадок, коли $X_{k-1} = 0$:

$X_{k-1} = 0 \Rightarrow c_k = 0$, це не виконається лише в тому випадку, коли $X_{k-2} = c_{k-1} = 1$, а це та ж сама ймовірність $p_{k-1,1}$, тоді:

$$p_{k,0} = \frac{1}{2}(1 - p_{k-1,1})$$

Тож отримаємо рекуренту:

$$p_k = 1 - \frac{1}{2}p_{k-1}$$

А початкові значення рекуренти у нас визначаються значеннями $p_{1,1}$,та $p_{1,0}$.

В решті решт обчисливши суму геометричної прогрессії знаходимо, що:

$$Pr_X\{f(\overleftarrow{X}) = \overleftarrow{f(X)}\} = Pr_X\{3(X \lll 1) = (3X) \lll 1\} = \frac{2^n + (-1)^{n+1}}{3 \cdot 2^n}$$

Зсув праворуч

У згаданій вище статті [9] було продемонстровано результат при

зсуві ліворуч, давайте спробуємо знайти ймовірність для зсуву праворуч, задачею обертального аналізу в другому випадку буде знайти ймовірність:

$$Pr_x\{f(\overrightarrow{x}) = \overrightarrow{f(X)}\} = Pr_X\{3(X \ggg 1) = (3X) \ggg 1\}$$

Таблиця 2.3 – Візуальне представлення чому будуть рівні біти у функції $(3x) \ggg 1$

Біти переносу	c_{n-1}	c_{n-2}	... c_2	$c_1 = 0$	$c_0 = 0$
X	X_{n-1}	X_{n-2}	...	X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...	X_0	0
$3X$	Y_{n-1}	Y_{n-2}	...	Y_1	Y_0
$3X \ggg 1$	Y_0	Y_{n-1}	...	Y_2	Y_1

З таблиці 2.3 можна побачити, що :

$$Y_0 = X_0$$

$$Y_1 = X_0 \oplus X_1$$

$$Y_k = X_k \oplus X_{k-1} \oplus c_k$$

для $k \geqslant 2$

Таблиця 2.4 – Візуальне представлення чому будуть рівні біти у функції $3(X \ggg 1)$

Біти переносу	c'_{n-1}	c'_{n-2}	... c'_2	$c'_1 = 0$	$c'_0 = 0$
$X \ggg 1$	X_0	X_{n-1}	...	X_2	X_1
$2(X \ggg 1)$	X_{n-1}	X_{n-2}	...	X_1	0
$3(X \ggg 1)$	W_{n-1}	W_{n-2}	...	W_1	W_0

З таблиці 2.4 можна побачити, що :

$$W_0 = X_1$$

$$W_1 = X_1 \oplus X_2$$

$$W_k = X_{k+1} \oplus X_k \oplus c'_k$$

для $k \geqslant 2$

Тепер прирівняємо ці твердження так як нам треба, а саме, щоб відповідні біти були рівними.Отримаємо систему з багатьох рівнянь:

$$y_1 = W_0 \Rightarrow X_1 = X_1 \oplus X_0 \Rightarrow X_0 = 0$$

$$y_2 = W_1 \Rightarrow X_1 \oplus X_2 = X_2 \oplus X_1 \oplus c_2 \Rightarrow c_2 = 0$$

$$y_3 = W_2 \Rightarrow X_3 \oplus X_2 \oplus c_3 = X_3 \oplus X_2 \oplus c'_2 \Rightarrow c'_2 = 0 \Rightarrow c'_{k-1} = c_k$$

З твердження, яке ми отримали на минулому кроці виходить, що усі наступні твердження для W_{k-1} і Y_k будуть тотожніми:

$$X_k \oplus X_{k-1} \oplus c'_{k-1} = X_k \oplus X_{k-1} \oplus c'_k$$

Спробуємо розглянути останні біти:

$$W_{n-1} = Y_0$$

Отримаємо рівняння:

$X_0 \oplus X_{n-1} \oplus c'_{n-1} = X_0 \Rightarrow X_0$ скорочується і отримаємо $X_{n-1} = c'_{n-1}$.

Формально ймовірність залежить від 3 рівнянь,тож отримаємо:

$$Pr_x\{3(X \ggg 1) = (3X) \ggg 1\} = Pr\{X_0 = 0\} \cdot Pr\{c_2 = 0\} \cdot Pr\{X_{n-1} = c'_{n-1}\}$$

Розглянемо ймовірність $Pr\{X_0 = 0\} \cdot Pr\{c_2 = 0\}$:

$$Pr\{X_0 = 0\} = 1/2$$

$Pr\{c_2 = 0\} = Pr\{\lfloor\frac{c_1+X_0+X_1}{2}\rfloor = 0\}$, $c_1 = 0$ за означенням біту переносу, а якщо і $X_0 = 0$, то ця подія буде істиною з ймовірністю рівною одиниці.

Тож отримаємо, що $Pr\{X_0 = 0\} \cdot Pr\{c_2 = 0\} = 1/2$ і наша ймовірність від 3 рівнянь зводиться до :

$$Pr_x\{3(x \ggg 1) = (3x) \ggg 1\} = \frac{1}{2} \cdot Pr\{X_{n-1} = c'_{n-1}\}$$

;

Введемо систему скорочень, які трохи полегшать розуміння та синтаксис:

Позначимо за $p_k = Pr\{X_k = c'_k\}$

Позначимо за $p_{k,0} = Pr\{X_k = c'_k = 0\}$

Позначимо за $p_{k,1} = Pr\{X_k = c'_k = 1\}$

Розпишемо ж c'_{n-1} трохи детальніше, отримаємо:

$$Pr\{X_{n-1} = c'_{n-1}\} = Pr\{X_{n-1} = \lfloor\frac{X_{n-1} + X_{n-2} + c'_{n-2}}{2}\rfloor\}$$

Розглянемо випадок, коли $X_{n-1} = 0$:

$$p_{n-1,0} = Pr\{X_{n-1} = \lfloor\frac{X_{n-1} + X_{n-2} + c'_{n-2}}{2}\rfloor = 0\}$$

Ця подія не відбудеться, тільки якщо $X_{n-2} = c'_{n-2} = 1$, не складно помітити, що це $p_{n-2,1}$

Якщо ж розглянути випадок, коли $X_{n-1} = 1$:

$$p_{n-1,1} = Pr\{X_{n-1} = \lfloor\frac{X_{n-1} + X_{n-2} + c'_{n-2}}{2}\rfloor = 1\}$$

Ця подія не відбудеться, тільки якщо $X_{n-2} = c'_{n-2} = 0$, не складно помітити, що це $p_{n-2,0}$

Можна зробити висновок що усі події нахрест виражаються через попепредні, як і в випадку, коли зсув ліворуч, врешті-решт, як результат

отримаємо:

$$Pr_X\{f(\overrightarrow{X}) = \overrightarrow{f(X)}\} = Pr_X\{3(x \ggg 1) = (3X) \ggg 1\} = \frac{2^n + (-1)^{n+1}}{3 \cdot 2^n}$$

2.2 Обертальний аналіз логічних функцій ускладнення

X∨2X

У цьому підрозділі буде знайдено $\Pr\{\overrightarrow{(X \vee 2X)} = \overrightarrow{X} \vee \overrightarrow{2X}\}$

Для цього буде записано значення бітів виходу функції $(X \vee 2X) \ggg 1(Y_k)$.

Таблиця 2.5 – $(X \vee 2X) \ggg 1$

X	X_{n-1}	X_{n-2}	...	X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...	X_0	0
$2X \vee X$	Y_{n-1}	Y_{n-2}	...	Y_1	Y_0
$(X \vee 2X) \ggg 1$	Y_0	Y_{n-1}	...	Y_2	Y_1

З таблиці 2.5 можна побачити, що:

$$Y_0 = X_0$$

$$Y_1 = X_0 \vee X_1$$

тоді аналітично:

$$Y_k = X_k \vee X_{k-1}$$

Тепер розглянемо значення бітів виходу для функції $X \ggg 1 \vee 2X \ggg 1(W_k)$

З таблиці 2.6 :

$$W_0 = X_1$$

$$W_1 = X_2 \vee X_1$$

Таблиця 2.6 – $X \ggg 1 \vee 2X \ggg 1$

$X \ggg 1$	X_0	X_{n-1}	...	X_2	X_1
$2X \ggg 1$	X_{n-1}	X_{n-2}	...	X_1	0
$(X \vee 2X) \ggg 1$	W_{n-1}	W_{n-2}	...	W_1	W_0

Тоді в загальному вигляді:

$W_k = X_{k+1} \vee X_k$ для усіх, окрім останнього біту, останній біт:

$$W_{n-1} = X_0 \vee X_{n-1}$$

Порівняємо виходи першої і другої функцій і знайдемо ймовірність їх рівності, для рівності:

$W_0 = Y_1 \Rightarrow X_1 = X_0 \vee X_1$ ймовірність цієї події $\frac{3}{4}$.

$W_1 = Y_2 \Rightarrow X_2 \vee X_1 = X_2 \vee X_1$ ймовірність цієї події 1.

$W_2 = Y_3 \Rightarrow X_2 \vee X_3 = X_2 \vee X_3$ ймовірність цієї події 1.

$W_k = Y_{k+1} \Rightarrow X_k \vee X_{k+1} = X_k \vee X_{k+1}$ ймовірність цієї події 1.

Розглянемо останні біти:

$W_{n-1} = Y_0 \Rightarrow X_0 \vee X_{n-1} = X_0$ ймовірність цієї події $\frac{3}{4}$.

Але нажаль першу та останню подію не можна розглядати незалежно,бо там перетинаються певні біти, тому розглянемо їх у сумісності, побудувавши таблицю істиності:

Подивившись такі набори бітів X_0,X_1,X_{n-1} у таблиці 2.7, у яких одночасно відбуваються ці події – отримаємо ймовірність $1/2$.

Спробуємо знайти ймовірність проходження пари обертання при зсуві на 2 паворуч, а потім вивести аналітичну формулу.

Для цього запишемо значення бітів виходу функції $(X \vee 2X) \ggg 2(Y_k)$.

З таблиці 2.8 можна побачити, що:

$$Y_0 = X_0$$

$$Y_1 = X_0 \vee X_1$$

Таблиця 2.7 – Таблиця істиності

X_0	X_1	X_{n-1}	$X_1 = X_0 \vee X_1$	$X_0 \vee X_{n-1} = X_0$
0	0	0	True	True
0	0	1	True	False
0	1	0	True	True
0	1	1	True	False
1	0	0	False	True
1	0	1	False	True
1	1	0	True	True
1	1	1	True	True

Таблиця 2.8 – $(X \vee 2X) \ggg$

X	X_{n-1}	X_{n-2}	...	X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...	X_0	0
$2X \vee X$	Y_{n-1}	Y_{n-2}	...	Y_1	Y_0
$(X \vee 2X) \ggg 2$	Y_1	Y_0	...	Y_3	Y_2

тоді аналітично:

$$Y_k = X_k \vee X_{k-1}$$

Тепер розглянемо значення бітів виходу для функції $X \ggg 2 \vee 2X \ggg 2(W_k)$

Таблиця 2.9 – $X \ggg 2 \vee 2X \ggg 2$

$X \ggg 2$	X_1	X_0	...	X_3	X_2
$2X \ggg 2$	X_0	X_{n-1}	...	X_2	0
$(X \vee 2X) \ggg 2$	W_{n-1}	W_{n-2}	...	W_1	W_0

З таблиці 2.9 бачимо :

$$W_0 = X_2$$

$$W_1 = X_3 \vee X_2$$

Тоді в загальному вигляді: $W_k = X_{k+2} \vee X_{k+1}$ для усіх, окрім 2 останніх бітів:

$$W_{n-2} = X_0 \vee X_{n-1}$$

$$W_{n-1} = X_0 \vee X_1$$

Порівняємо виходи першої і другої функцій і знайдемо ймовірність їх рівності, для рівності:

$W_0 = Y_2 \Rightarrow X_2 = X_2 \vee X_1$ ймовірність цієї події $\frac{3}{4}$.

$W_1 = Y_3 \Rightarrow X_3 \vee X_2 = X_3 \vee X_2$ ймовірність цієї події 1.

$W_2 = Y_4 \Rightarrow X_4 \vee X_3 = X_4 \vee X_3$ ймовірність цієї події 1.

$W_k = Y_{k+2} \Rightarrow X_{k+2} \vee X_{k+1} = X_{k+2} \vee X_{k+1}$ ймовірність цієї події 1.

Розглянемо останні біти:

$W_{n-2} = Y_0 \Rightarrow X_0 \vee X_{n-1} = X_0$ ймовірність цієї події $\frac{3}{4}$. $W_{n-1} = Y_1 \Rightarrow X_0 \vee X_1 = X_0 \vee X_1$ ймовірність цієї події 1.

Тож можна сказати, що ймовірність проходження обертання функції $X \vee 2X$ при зсуві на 2 праворуч рівна $\frac{9}{16}$, невже складність буде константною в незалежності від кількості зсувів? Саме так, це буде відбуватись, через відмінність у W_0 і W_{n-k},відносно до Y_k і Y_0 відповідно де k-кількість зсувів.

X∧2X

У цьому підрозділі буде знайдено $\Pr\{\overrightarrow{(X \wedge 2X)} = \overrightarrow{X} \wedge \overrightarrow{2X}\}$

Для цього буде записано значення бітів виходу функції $(X \wedge 2X) \ggg 1 (Y_k)$.

Таблиця 2.10 – $(X \wedge 2X) \ggg 1$

X	X_{n-1}	X_{n-2}	...	X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...	X_0	0
$2X \wedge X$	Y_{n-1}	Y_{n-2}	...	Y_1	Y_0
$(X \wedge 2X) \ggg 1$	Y_0	Y_{n-1}	...	Y_2	Y_1

З таблиці 2.10 можна побачити, що:

$$Y_0 = 0$$

$$Y_1 = X_0 \wedge X_1$$

тоді аналітично:

$$Y_k = X_k \wedge X_{k-1}$$

Тепер розглянемо значення бітів виходу для функції $X >>> 1 \wedge 2X \ggg 1(W_k)$

Таблиця 2.11 – $X \ggg 1 \wedge 2X \ggg 1$

$X \ggg 1$	X_0	X_{n-1}	...	X_2	X_1
$2X \ggg 1$	X_{n-1}	X_{n-2}	...	X_1	0
$(X \wedge 2X) \ggg 1$	W_{n-1}	W_{n-2}	...	W_1	W_0

З таблиці 2.11 бачимо :

$$W_0 = 0$$

$$W_1 = X_2 \wedge X_1$$

Тоді в загальному вигляді:

$W_k = X_{k+1} \wedge X_k$ для усіх, окрім останнього біту, останній біт:

$$W_{n-1} = X_0 \wedge X_{n-1}$$

Порівняємо виходи першої і другої функцій і знайдемо ймовірність їх рівності, для рівності:

$W_0 = Y_1 \Rightarrow 0 = X_0 \wedge X_1$ ймовірність цієї події $\frac{3}{4}$.

$W_1 = Y_2 \Rightarrow X_2 \wedge X_1 = X_2 \wedge X_1$ ймовірність цієї події 1.

$W_2 = Y_3 \Rightarrow X_2 \wedge X_3 = X_2 \wedge X_3$ ймовірність цієї події 1.

$W_k = Y_{k+1} \Rightarrow X_k \wedge X_{k+1} = X_k \wedge X_{k+1}$ ймовірність цієї події 1.

Розглянемо останні біти:

$W_{n-1} = Y_0 \Rightarrow X_0 \wedge X_{n-1} = 0$ ймовірність цієї події $\frac{3}{4}$.

Але знову ж, неможна так розглядати, оскільки біти перетинаються, розглянувши в сумісності отримаємо таблицю 2.12:

Таблиця 2.12 – Таблиця істиності

X_0	X_1	X_{n-1}	$0 = X_0 \wedge X_1$	$X_0 \wedge X_{n-1} = 0$
0	0	0	True	True
0	0	1	True	True
0	1	0	True	True
0	1	1	True	True
1	0	0	True	True
1	0	1	True	False
1	1	0	False	True
1	1	1	False	False

Таким чином отримуємо ймовірність $Pr\{\overrightarrow{(X \wedge 2X)} = \overrightarrow{X} \wedge \overrightarrow{2X}\} = \frac{5}{8}$

Спробуємо знайти ймовірність проходження пари обертання при зсуві на 2 праворуч, а потім вивести аналітичну формулу.

Для цього запишемо значення бітів виходу функції $(X \wedge 2X) \ggg 2(Y_k)$.

Таблиця 2.13 – $(X \wedge 2X) \ggg 2$

X	X_{n-1}	X_{n-2}	...	X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...	X_0	0
$2X \wedge X$	Y_{n-1}	Y_{n-2}	...	Y_1	Y_0
$(X \wedge 2X) \ggg 2$	Y_1	Y_0	...	Y_3	Y_2

З таблиці 2.13 можна побачити, що:

$$Y_0 = 0$$

$$Y_1 = X_0 \wedge X_1$$

тоді аналітично:

$$Y_k = X_k \wedge X_{k-1}$$

Тепер розглянемо значення бітів виходу для функції $X \ggg 2 \wedge 2X \ggg 2(W_k)$

Таблиця 2.14 – $X \ggg 2 \wedge 2X \ggg 2$

$X \ggg 2$	X_1	X_0	...	X_3	X_2
$2X \ggg 2$	X_0	X_{n-1}	...	X_2	0
$(X \wedge 2X) >>> 2$	W_{n-1}	W_{n-2}	...	W_1	W_0

З таблиці 2.14 :

$$W_0 = 0$$

$$W_1 = X_3 \wedge X_2$$

Тоді в загальному вигляді:

$W_k = X_{k+2} \wedge X_{k+1}$ для усіх, окрім 2 останніх бітів:

$$W_{n-2} = X_0 \wedge X_{n-1}$$

$$W_{n-1} = X_0 \wedge X_1$$

Порівняємо виходи першої і другої функцій і знайдемо ймовірність їх рівності, для рівності:

$W_0 = Y_2 \Rightarrow 0 = X_2 \wedge X_1$ ймовірність цієї події $\frac{3}{4}$.

$W_1 = Y_3 \Rightarrow X_3 \wedge X_2 = X_3 \wedge X_2$ ймовірність цієї події 1.

$W_2 = Y_4 \Rightarrow X_4 \wedge X_3 = X_4 \wedge X_3$ ймовірність цієї події 1.

$W_k = Y_{k+2} \Rightarrow X_{k+2} \wedge X_{k+1} = X_{k+2} \wedge X_{k+1}$ ймовірність цієї події 1.

Розглянемо останні біти:

$W_{n-2} = Y_0 \Rightarrow X_0 \wedge X_{n-1} = 0$ ймовірність цієї події $\frac{3}{4}$. $W_{n-1} = Y_1 \Rightarrow X_0 \wedge X_1 = X_0 \wedge X_1$ ймовірність цієї події 1.

Тож можна сказати, що ймовірність проходження обертання функції $X \wedge 2X$ при зсуві на 2 праворуч рівна $\frac{9}{16}$, невже складність буде константною

в незалежності від кількості зсувів? Саме так, це буде відбуватись, через відмінність у W_0 і W_{n-k},відносно до Y_k і Y_0 відповідно де k-кількість зсувів.

Обертальний аналіз функції $\oplus$

У цьому підрозділі буде знайдено $\Pr\{\overrightarrow{(X \oplus 2X)} = \overrightarrow{X} \oplus \overrightarrow{2X}\}$

Для цього буде записано значення бітів виходу функції $(X \oplus 2X) \ggg 1(Y_k)$.

Таблиця 2.15 – $(X \oplus 2X) \ggg 1$

X	X_{n-1}	X_{n-2}	...	X_1	X_0
$2X$	X_{n-2}	X_{n-3}	...	X_0	0
$2X \oplus X$	Y_{n-1}	Y_{n-2}	...	Y_1	Y_0
$(X \oplus 2X) \ggg 1$	Y_0	Y_{n-1}	...	Y_2	Y_1

З таблиці 2.15 можна побачити, що:

$$Y_0 = X_0$$

$$Y_1 = X_1 \oplus X_0$$

тоді аналітично:

$$Y_k = X_k \oplus X_{k-1}$$

Тепер розглянемо значення бітів виходу для функції $X \ggg 1 \oplus 2X \ggg 1(W_k)$

Таблиця 2.16 – $X \ggg 1 \oplus 2X \ggg 1$

$X \ggg 1$	X_0	X_{n-1}	...	X_2	X_1
$2X \ggg 1$	X_{n-1}	X_{n-2}	...	X_1	0
$(X \oplus 2X) \ggg 1$	W_{n-1}	W_{n-2}	...	W_1	W_0

З таблиці 2.16 бачимо :

$$W_0 = X_1$$

$$W_1 = X_2 \oplus X_1$$

Тоді в загальному вигляді:

$W_k = X_{k+1} \oplus X_k$ для усіх, окрім останнього біту, останній біт:

$$W_{n-1} = X_0 \oplus X_{n-1}$$

Порівняємо виходи першої і другої функцій і знайдемо ймовірність їх рівності, для рівності:

$W_0 = Y_1 \Rightarrow X_1 = X_0 \oplus X_1$ ймовірність цієї події $\frac{1}{2}$.

$W_1 = Y_2 \Rightarrow X_2 \oplus X_1 = X_2 \oplus X_1$ ймовірність цієї події 1.

$W_2 = Y_3 \Rightarrow X_2 \oplus X_3 = X_2 \oplus X_3$ ймовірність цієї події 1.

$W_k = Y_{k+1} \Rightarrow X_k \oplus X_{k+1} = X_k \oplus X_{k+1}$ ймовірність цієї події 1.

Розглянемо останні біти:

$W_{n-1} = Y_0 \Rightarrow X_0 \oplus X_{n-1} = X_0$ ймовірність цієї події $\frac{1}{2}$.

Але знову ж, неможна так розглядати, оскільки біти перетинаються, розглянувши в сумісності отримаємо таблицю 2.17:

Таблиця 2.17 – Таблиця істиності

X_0	X_1	X_{n-1}	$X_1 = X_0 \oplus X_1$	$X_0 \oplus X_{n-1} = X_0$
0	0	0	True	True
0	0	1	True	False
0	1	0	False	True
0	1	1	False	False
1	0	0	True	True
1	0	1	True	False
1	1	0	False	True
1	1	1	False	False

Таким чином отримуємо ймовірність $Pr\{\overrightarrow{(X \oplus 2X)} = \overrightarrow{X} \oplus \overrightarrow{2X}\} = \frac{2}{8}$

Для більшої кількості зсувів ситуація буде аналогічною, як і для $X \vee 2X$, тож для довільного зсуву ймовірність проходження пари

обертання буде 1/4.

2.3 Диференціально-обертальний криптоаналіз деяких ускладнюючих функцій ARX-криптосистем

Надалі буде показано результат RX-аналізу функції $f(X) = X \oplus (X \ll 1)$

Аналіз лінійних функцій відносно $\oplus$

Твердження 2.1. *Якщо $f(X)$ – лінійна відносно $\oplus$то:*

$$rp^f(\alpha,\beta) = Pr\{f(\overrightarrow{X}) \oplus \overrightarrow{f(X)} = f(\alpha) \oplus \beta\}$$

Доведення. Оскільки f–лінійна, то:

$$f(X \oplus Y) = f(X) \oplus f(Y)$$

В нашому ж випадку:

$$f(\overrightarrow{X} \oplus \alpha) = \overrightarrow{f(X)} \oplus \beta \Rightarrow f(\overrightarrow{X}) \oplus f(\alpha) = \overrightarrow{f(X)} \oplus \beta$$

З нього не складно отримати наступне твердження:

$$f(\overrightarrow{X}) \oplus \overrightarrow{f(X)} = f(\alpha) \oplus \beta$$

□

Наслідок 2.1.

$$rp^f(\alpha,\beta) = \begin{cases} Pr\{f(\overrightarrow{X}) \oplus \overrightarrow{f(X)} = \delta_i\}, \text{ якщо } \beta = f(X) \oplus \delta_i \\ 0, \text{ у інших випадках.} \end{cases} \quad (2.1)$$

Як висновок диференційно-обертальний криптоаналіз лінійних відображень зводиться до звичайного обертального криптоаналізу.

Розглянемо більш детально **RX-аналіз** $f(X) = X \oplus (X \ll 1)$

Повернемось до суті роботи, а саме RX-аналізу $f(X) = X \oplus (X \ll 1)$

Нехай $u = f(\overrightarrow{x} \oplus \alpha)$, а $v = \overrightarrow{f(X)} \oplus \beta$

$$u_0 = X_1 \oplus \alpha_0, v_0 = X_1 \oplus x_0 \oplus \beta_0$$

$$u_1 = X_2 \oplus \alpha_1 \oplus X_1 \oplus \alpha_0, v_1 = X_2 \oplus X_1 \oplus \beta_1$$

$$u_2 = X_3 \oplus \alpha_2 \oplus X_2 \oplus \alpha_1, v_2 = X_3 \oplus X_2 \oplus \beta_2$$

$$...$$

$$u_{n-2} = X_{n-1} \oplus \alpha_{n-2} \oplus X_{n-2} \oplus \alpha_{n-3}, v_{n-2} = X_{n-1} \oplus X_{n-2} \oplus \beta_{n-2}$$

$$u_{n-1} = X_0 \oplus \alpha_{n-1} \oplus X_{n-1} \oplus \alpha_{n-2}, v_{n-1} = X_0 \oplus \beta_{n-1}$$

Якщо пильно придивитись до отриманих значень u_i, та v_i можна помітити, що з 1 до n-2 біту включно вони визначаються однаково схожим чином.. Для $i = 0, X_0 = \alpha_0 \oplus \beta_0$

Ймовірність цієї події $1/2$.

Для $i = n - 1, X_{n-1} = \beta_{n-1} \oplus \alpha_{n-1} \oplus \alpha_{n-2}$

Ймовірність цієї події $1/2$.

Тепер настав час розглянути біти з 1 до n-2.

$$\forall k : 2 \leqslant k \leqslant n - 2, \alpha_k \oplus \alpha_{k-1} = \beta_k$$

А це те ж саме, що і $f(\alpha) = \beta$, окрім крайніх бітів, ймовірність для яких ми вже знайшли.

Для цього звернемось до наслідку 2.1.

при $\beta = f(\alpha) \oplus \delta$.

Якщо $\delta = 00...00$, або $\delta = 10...00$, або $\delta = 00...01$, або $\delta = 10...01$ то $Pr\beta = f(\alpha) = 1$, інакше 0.

Звідси отримуємо фінальний результат: $Pr = \frac{1}{4} \cdot [\beta = f(\alpha)]$

Диференційно-обертальний криптоаналіз фунції $X \wedge (X \ll 1)$

$$f(\overrightarrow{X} \oplus \alpha) = \overrightarrow{f(X)} \oplus \beta$$

Нехай $u = f(\overrightarrow{X} \oplus \alpha)$, а $v = \overrightarrow{f(X)} \oplus \beta$

$$u_0 = 0, v_0 = X_1X_0 \oplus \beta_0$$

$$u_k = (X_{k+1} \oplus \alpha_k)(X_k \oplus \alpha k - 1), v_k = X_{k+1}X_k \oplus \beta_k$$

$$u_{n-1} = (X_0 \oplus \alpha_{n-1})(X_{n-1} \oplus \alpha n - 2), v_{n-1} = \beta_{n-1}$$

Позначимо $\gamma = \beta \oplus f(X)$.

Знову маємо схожі залежності для усіх бітів окрім останнього і першого.

$$p_0 = Pr\{0 = X_1x_0 \oplus \beta\}$$

$$p_k = Pr\{\alpha_{k-1}X_{k+1} \oplus \alpha_kX_k = \beta_k \oplus \alpha_k\alpha_{k-1}\}$$

$$p_{n-1} = Pr\{\alpha_{n-1}X_0 \oplus \alpha_{n-2}X_{n-1} = \beta_{n-1}\}$$

Отримаємо підзадачу:

$$Pr\{X_0X_1 = \beta_0, \alpha_{n-1}X_0 \oplus \alpha_{n-2}X_{n-1} = \beta_{n-1}\}$$

Якщо $\alpha = 1 \Rightarrow X \oplus \alpha = \overline{X}$

Тож можна отримати ліворуч у другій рівності чотири варіанти:

$$X_0X_{n-1} = \beta_{n-1}$$

$$\overline{X_0}X_{n-1} = \beta_{n-1}$$

$$\overline{X_0X_{n-1}} = \beta_{n-1}$$

$$X_0\overline{X_{n-1}} = \beta_{n-1}$$

Давайте чесно побудуємо таблицю істиності для всіх можливих варіантів.

Таблиця 2.18 – Можливі значення X_0,X_{n-1}, в залежності від $\alpha_{n-1}, \alpha_{n-2}$

X_0	X_1	X_{n-1}	X_0X_1	X_0X_{n-1}	$\overline{X_0}X_{n-1}$	$\overline{X_0X_{n-1}}$	$X_0\overline{X_{n-1}}$
0	0	0	0	0	0	0	1
0	0	1	0	0	0	1	0
0	1	0	0	0	0	0	1
0	1	1	0	0	0	1	0
1	0	0	0	0	1	0	0
1	0	1	0	1	0	0	0
1	1	0	1	0	1	0	0
1	1	1	1	1	0	0	0

Таблиця 2.19 – Таблиця співпадінь, відносно β_0,β_{n-1}

$\beta_0\beta_{n-1}$	Співп	Співп	Співп	Співп
00	5	5	4	4
01	1	1	2	2
10	1	1	2	2
11	1	1	0	0

З таблиці 2.19, якщо $\alpha_{n-1} = \beta_0 = \beta_{n-1} = 1 \Rightarrow Pr = 0$.

Якщо ж почати розглядати центральні випадки, то їх необхідно розглядати по у зв'язці:

$$\alpha_{k-1}X_{k-1} \oplus \alpha_k X_k = \gamma_k$$

$$\alpha_k X_{k+2} \oplus \alpha_{k+1}X_{k+1} = \gamma_{k+1}$$

Розглянемо 3 випадки:

1)$\alpha_{k-1} = \alpha_k = 0 \Rightarrow 0 = \gamma_k = \beta_k$

$$p_k = [\beta = 0] = \begin{cases} 1, \text{ якщо } \beta_k = 0 \\ 0, \text{ у інших випадках.} \end{cases} \tag{2.2}$$

2)$\alpha_k = 1 \Rightarrow X_k = \gamma_k \oplus \alpha_{k-1}X_{k-1}$

Але $\gamma_k \oplus \alpha_{k-1}X_{k-1}$ є константою відносно x_k, тому ймовірність $\frac{1}{2}$

3)$\alpha_k = 0$,$\alpha_{k-1} = 1$:

В цьому випадку у нас лишається система з 2 рівнянь:

$$\begin{cases} X_{k+1} = \gamma_k = \beta_k \\ \alpha_{k-1}X_{k+1} = \gamma_{k+1} = \beta_{k+1} \end{cases} \tag{2.3}$$

Можна побачити, що тут фігурує α_{k+1} про яке ми нічого не знаємо, тому розглянемо 2 випадки:

Якщо $\alpha_{k+1} = 0$, то друге рівняння з системи скоротиться, і $p_k = \frac{1}{2}$.

Якщо ж $\alpha_{k+1} = 1$, то :

$$\begin{cases} X_{k+1} = \beta_k \\ X_{k+1} = \beta_{k+1} \end{cases} \tag{2.4}$$

Підсумувавши усе вищесказане про центральні випадки у таблицю 2.20 отримаємо:

Таблиця 2.20 – Узагальнення всіх випадків

α_{k-1}	α_k	α_{k+1}	β_k	p_k
0	0	*	0	1
0	0	*	1	0
*	1	*	*	$\frac{1}{2}$
1	0	0	*	$\frac{1}{2}$
1	0	1	$\beta_k = \beta_{k+1}$	1
1	0	1	$\beta_k \neq \beta_{k+1}$	0

Скомбінувавши дані, наведені в таблицях 2.18,2.19,2.20 можна обчислити ймовірність проходження загальної пари обертання через функцію $f(X) = X \oplus (X \ll 1)$, шляхом побітового розглядання. Одержати аналітичний вираз, який описував би імовірність загалом не

вдалось, бо при k=n-2 наше центральне рівняння буде у зв'язці із крайовим, а перше крайове рівняння(при k=0) може впливати на 1 центральне рівняння.

Для n=2 все фактично побудовано, бо описується першим і останнім рівнянням, а вони були розглянуті нами в сумісності. Для n=3 буде лише одне центральне рівняння, так що воно вирішується теж не складно, а вже починаючи від n=4 можна для кожної конкретної пари α,β порахувати ймовірність проходження пари обертання, але аналітичний вираз знайти не вдалось.

ВИСНОВКИ

У роботі були розглянуті функції ускладнення ARX-криптосистем які мають відносно легку реалізацію:множення на константу 3 та його аналоги, побудовані виключно з логічних операцій.Для таких функцій було проведено обертальний криптоаналіз та знайдено імовірності проходження пар обертання:

Для логічних операцій отримали константи,при зсуві більше ніж на 1 позицію а саме:$9/16$ для $x \wedge (x \ll 1)$ та $x \vee (x \ll 1)$ і $1/4$ для $x \oplus (x \ll 1)$

Було узагальнено відомі результати обертального криптоаналіщу для функції 3x, та показано, що воно асимптотично прямує до $1/3$.

Було проведено диференціально-обертальний криптоаналіз для логічних функцій ускладнення. Показано, що для лінійних відображень диференціально-обертальний криптоаналіз зводиться до звичайного обертального. Для функції ускладнення $x \wedge (x \ll 1)$ було знайдено аналітичні вирази для проходження пар обертання із різницями на рівні окремих бітів, що в цілому дозволяє знаходити імовірності проходження пар обертання через дану функцію шляхом безпосередніх обчислень.

В якості напрямків подальших досліджень можна зазначити знаходження точних аналітичних виразів для імовірностей проходження пар обертання через інші класи функцій ускладнення та ARX-криптосистеми в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Khovratovich D., Nikolic I. Rotational Cryptavrnalysis of ARX [електронний ресурс] //Fast Software Encryption (FSE‘2010) — Режим доступу: https://www.iacr.org/archive/fse2010/61470339/61470339.pdf.

2. Khovratovich D., Nikolic I., Pieprzyk J., Sokolowski P., Steinfeld R. Rotational Cryptanalysis of ARX Revisited [електронний ресурс] // Cryptology ePrint Archive, Report 2015/095. — Режим доступу: https://eprint.iacr.org/2015/095.pdf.

3. X. Lai and J. L. Massey. Markov ciphers and differentail cryptanalysis.// Advances in Cryptology — EUROCRYPT ’91, Workshop on the Theory and Application of of Cryptographic Techniques (Brighton, UK, April 8-11, 1991). — Lecture Notes in Computer Science. — Volume 547. — Springer, 1991. — pages 17–38.

4. Daum M. Cryptanalysis of Hash Functions of the MD4-Family : PhD thesis [електронній ресурс] — Bochum: RuhrUniversitat, 2005. — Режим доступу: https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/docId/616

5. Salam, I. Rotational Cryptanalysis of MORUS. Symmetry 2021, 13, 2426.https://doi.org/10.3390/sym13122426

6. Morawiecki P., Pieprzyk J., Srebrny M. Rotational cryptanalysis of round-reduced Keccak [електронний ресурс] — Режим доступу: https://typeset.io/pdf/rotational-cryptanalysis-of-round-reduced-keccak-4bmcuh8c42.pdf

7. Kraleva L., Ashur T., Rijmen V. Rotational Cryptanalysis on MAC Algorithm Chaskey [електронний ресурс] — Режим доступу: https://typeset.io/pdf/rotational-cryptanalysis-on-mac-algorithm-chaskey-2dewbwjmyf.pdf

8. Zajac P., Ondro M. Rotational cryptanalysys of GOST with identical s-boxes [електронний ресурс] — Режим доступу: https://typeset.io/pdf/rotational-cryptanalysis-of-gost-with-identical-s-boxes-531rlr0qk0.pdf

9. Van Assche G. A rotational distinguisher on Shabal's keyed permutation and its impact on the security proofs [електронний ресурс] — Режим доступу: http://gva.noekeon.org/papers/ShabalRotation.pdf