УДК 004.056.53:512.6

ДЕЯКІ ВЛАСТИВОСТІ ЙМОВІРНОСТЕЙ RX-ДИФЕРЕНЦІАЛІВ ДЛЯ ОПЕРАЦІЇ, ЩО АПРОКСИМУЄ МОДУЛЬНЕ ДОДАВАННЯ

Н. С. Корж[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі досліджено алгебраїчні властивості ймовірностей RX-диференціалів операції, яка апроксимує додавання за модулем у криптосистемі NORX. Наведено аналітичні вирази для обчислення RX-ймовірностей, проаналізовано умови існування RX-диференціалів з ненульовою ймовірністю та запропоновано алгоритми пошуку таких диференціалів. Представлені аналітичні формули дозволяють ефективно оцінювати стійкість криптографічних примітивів класів ARX та LRX, які використовують апроксимації модульного додавання, до диференціально-обертального криптоаналізу.

Ключові слова: RX-аналіз, ARX, NORX, обертальний криптоаналіз.

Вступ

Криптосистеми класу ARX (*Add–Rotation–XOR*) використовують у своїй структурі лише елементарні операції: додавання за модулем 2^n, бітове додавання (XOR) та циклічні зсуви. Такий підхід дає змогу створювати високоефективні та легкі алгоритми, які застосовуються до пристроїв з обмеженими ресурсами.

Іноді модульне додавання замінюють простою логічно операцією, щоб досягти ще більшої ефективності. Такі системи неформально називають LRX-криптосистемами, де «L» означає *Logic*. До найвідоміших LRX-алгоритмів належать шифри Simon [1], NORX [2] та Ascon [3].

У роботі [4] Т. Ашур і Ю. Лю запропонували комбінований підхід — диференціально-обертальний криптоаналіз (або RX-аналіз), який об'єднує ідеї диференціального та обертального методів. Метод розглядає обертальні пари, доповнені звичайними диференціалами, утворюючи RX-диференціали, які дають змогу ефективно нейтралізувати вплив побітового додавання довільних констант. Автори вивели явну формулу для RX-ймовірностей при зсуві на один біт для модульного додавання та побудували 7-раундовий RX-розрізнювач для шифра Speck 32/64 [1].

У цій роботі досліджено властивості RX-диференціалів для операції, що апроксимує модульне додавання, запропонованої авторами шифру NORX [2]. Проведено аналіз ймовірностей RX-диференціалів для довільних значень циклічного зсуву, використовуючи відомі аналітичні формули [5, 6]. Отримані результати слугують основою для побудови автоматизованих алгоритмів пошуку характеристик і закладають підґрунтя для формального аналізу безпеки сучасних ARX- та LRX-криптосистем у межах диференціально-обертального підходу.

[a]nikitakorzh10@gmail.com

1. Нотації та визначення

В цій роботі використовується така нотація:

V_n — множина всіх бінарних векторів довжини n: $V_n = \{0,1\}^n$;

$x \in V_n$ — довільний n-бітний вектор

$$x = (x_{n-1}, x_{n-2}, \dots, x_1, x_0),\ x_i \in \{0,1\};$$

$x[i]$ — i-тий біт у векторі $x \in V_n$;

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

x^r або $x \lll r$ — циклічний зсув (обертання) x ліворуч на r бітів:

$$x^r = (x_{n-r-1}, \dots, x_0, x_{n-1}, \dots, x_{n-r});$$

x^{-r} або $x \ggg r$ — циклічний зсув x праворуч на r бітів; зауважимо, що $x^{-r} \equiv x^{n-r}$;

$x \ll r$ — нециклічний лівий зсув x на r бітів:

$$x \ll r = (x_{n-r-1}, \dots, x_0, 0, \dots, 0);$$

$x \vee y$ — побітова логічна операція OR;

$x \wedge y$ або xy — побітова логічна операція AND;

$\overline{x}$ — інверсія всіх бітів x;

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

$\mu_{n,r}$ — n-бітний вектор з нулями в позиціях $i = 0$ та $i = r$ та одиницями в усіх інших; обчислюється як $\mu_{n,r} = 2^n - 2^r - 2$.

Розглянемо відображення $f : V_n \times V_n \to V_n$.

Диференціалом $\omega = (\alpha, \beta \to \gamma)$ *функції* f називають довільну трійку векторів $\alpha, \beta, \gamma \in V_n$, що задає різниці між двома вхідними (або вихідними) значеннями f відносно операції $\oplus$.

Ймовірність диференціала $\omega = (\alpha, \beta \to \gamma)$ *функції* f визначається як

$$xdp^f(\omega) = xdp^f(\alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{f(x \oplus \alpha, y \oplus \beta) = f(x, y) \oplus \gamma\}.$$

У [4] Т. Ашур і Ю. Лю узагальнили поняття диференціала до *RX-диференціала* $(r;\ \alpha, \beta \to \gamma)$ як поєднання обертання $(x, y) \mapsto (x^r, y^r)$ з диференціалом $(\alpha, \beta \to \gamma)$. Ймовірність RX-диференціала функції f визначається так:

$$xrp^f(r; \alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{f(x^r \oplus \alpha, y^r \oplus \beta) = (f(x, y))^r \oplus \gamma\}.$$

Звичайний диференціал $(\alpha, \beta \to \gamma)$ і RX-диференціал $(r; \alpha, \beta \to \gamma)$ будемо називати *відповідними диференціалами.*

Ймовірності xdp^f характеризують стійкість до диференціального криптоаналізу, а xrp^f — до диференціально-обертального криптоаналізу.

У [2] розробники шифра NORX запропонували операцію

$$h(x, y) = x \oplus y \oplus \big((x \wedge y) \ll 1\big),$$

що апроксимує додавання за модулем 2^n. Дана апроксимація ґрунтується на відомій тотожності для модульного додавання та логічних операцій [7]:

$$x + y = (x \oplus y) + \big((x \wedge y) \ll 1\big),$$

де додавання праворуч замінено на XOR.

Наступна теорема подає аналітичний вираз для RX-диференціальних ймовірностей операції $h(x, y)$.

Теорема 1 ([5]). *Для довільних векторів* $\alpha, \beta, \gamma \in V_n$ *та довільного* r, $1 \le r \le n-1$, *ймовірність RX-диференціала* $(r; \alpha, \beta \to \gamma)$ *для функції* $h(x, y)$ *визначається так:*

1) $xrp^h(r; \alpha, \beta \to \gamma) \ne 0$ *тоді й лише тоді, коли*

$$(\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta \wedge \mu_{n,r} = 0; \qquad (1)$$

2) якщо $xrp^h(r; \alpha, \beta \to \gamma) \ne 0$, *то*

$$xrp^h(r; \alpha, \beta \to \gamma) = \left(\frac{3}{4} - \frac{\delta[0]}{2}\right)\left(\frac{3}{4} - \frac{\delta[r]}{2}\right) \\ \cdot 2^{-wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r})}; \qquad (2)$$

де $\delta = \alpha \oplus \beta \oplus \gamma$.

2. Пошук RX-диференціалів з ненульовою ймовірністю функції $h(x, y)$

Як сформульовано в теоремі 1, RX-диференціал $xrp^h(r; \alpha, \beta \to \gamma)$ має ненульову ймовірність тоді й лише тоді, коли виконується умова

$$C = (\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta \wedge \mu_{n,r} = 0.$$

Введемо додаткові позначення. Нехай

$$A = (\alpha \vee \beta) \ll 1, \quad \overline{A} = \overline{(\alpha \vee \beta) \ll 1}.$$

Тоді для кожного індексу i, де $0 \le i \le n-1$, $\delta[i] = \alpha[i] \oplus \beta[i] \oplus \gamma[i]$, повинна виконуватись умова

$$\overline{A}[i] \wedge \delta[i] \wedge \mu[i] = 0.$$

Щоб мати змогу систематично описати всі вихідні різниці γ, які забезпечують ненульову ймовірність RX-диференціалу для фіксованих $\alpha, \beta \in V_n$ та зсуву r, сформулюємо процедуру їхнього повного перебору.

Побудована далі схема однозначно визначає біти γ у позиціях, де умова $C = 0$ накладає жорсткі обмеження, і залишає свободу вибору там, де таких обмежень немає. Це не лише дозволяє оцінити потужність множини допустимих γ, а й дає підґрунтя для конструювання диференціальних характеристик і подальшої кількісної оцінки атаки.

Алгоритм 1 (Пошук всіх векторів $\boldsymbol{\gamma}$, для яких ймовірність RX-диференціалу $(\boldsymbol{r; \alpha, \beta \to \gamma}) \ne \boldsymbol{0}$).

Вхід: $\alpha, \beta \in V_n$, $r \in \mathbb{Z} : 1 \le r \le n-1$.

Вихід: *множина векторів* $\gamma \in V_n$.

1. $A[i] = \alpha[i-1] \vee \beta[i-1]$.
2. *Встановлюємо біти, що визначені умовою (1):*

$$\gamma[0] \leftarrow \{0, 1\}, \qquad \gamma[r] \leftarrow \{0, 1\}.$$

3. *Для кожного індексу* $i \in \{1, \dots, n-1\} \setminus \{r\}$ *встановлюємо*
   - ***(i)*** *Якщо* $A[i] = 1$, *то* $\gamma[i] \in \{0, 1\}$ *(вибір довільний);*
   - ***(ii)*** *Якщо* $A[i] = 0$, *то* $\gamma[i] \leftarrow \alpha[i] \oplus \beta[i]$.

Наслідок 1. Потужність множини всіх векторів $\gamma \in V_n$, для яких RX-ймовірність диференціала $(r;\ \alpha, \beta \to \gamma)$ є ненульовою, дорівнює:

$$\big|\{\gamma\ :\ xrp^h(r; \alpha, \beta \to \gamma) \ne 0\}\big| = 4 \cdot 2^{wt\left(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r}\right)}.$$

Зауваження 1. З огляду на аналітичний вираз для xrp доцільно зосередити пошук RX-диференціалів максимальної ймовірності на підкласі тих векторів, для яких

$$\delta[0] = \delta[r] = 0, \qquad \delta = \alpha \oplus \beta \oplus \gamma.$$

За такої умови множник при відповідному степені двійки в (2) набуває найбільшого можливого значення 9/16, що, своєю чергою, максимізує ймовірність RX-диференціала.

Наслідок 2. Щоб описати множину векторів γ, для яких RX-диференціал $(r; \alpha, \beta \to \gamma)$ має ненульову ймовірність, а коефіцієнт в (2) дорівнює 9/16, достатньо замінити крок 2 алгоритму 1 на:

$$\gamma[0] \leftarrow \alpha[0] \oplus \beta[0], \qquad \gamma[r] \leftarrow \alpha[r] \oplus \beta[r].$$

3. Аналіз RX-диференціалів спеціального виду

3.1. RX-диференціали з однаковими аргументами $(\alpha = \beta = \gamma)$

Використаємо теорему 1 для пошуку RX-диференціалів виду $(r, \alpha, \alpha \to \alpha)$ з ненульовою ймовірністю. Маємо:

$$xrp^h(r; \alpha, \alpha \to \alpha) \ne 0 \Leftrightarrow \overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r}.$$

Відповідно, множина допустимих векторів α описується як:

$$\mathscr{A}_{n,r} = \left\{ \alpha \in V_n \;\middle|\; \overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r} = 0 \right\}.$$

Лема 1. *Для довільних параметрів n та значення обертання r $(1 \le r \le n-1)$, множина всіх векторів $A_{n,r}$ дорівнює*

$$\mathscr{A}_{n,r} = \left\{ \left(2^s - 1\right) + \left(\left(2^t - 1\right) \ll r\right) \;\middle|\; \begin{array}{l} 0 \le s \le r, \\ 1 \le t \le n - r \end{array} \right\}.$$

Доведення. Запишемо умову $\overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r} = 0$ у координатах. Для кожного i, $1 \le i \le n-1$, $i \ne r$, заборонена ситуація $\overline{\alpha_{i-1}} \wedge \alpha_i = 1$, тобто після нуля не може одразу стояти одиниця, якщо $i \ne r$. Єдині дозволені стартові позиції для блоків послідовних одиниць — це 0 та r.

Розіб'ємо $\mathscr{A}_{n,r}$ за значеннями $\alpha[0]$ та $\alpha[r]$. Для $\varepsilon, \delta \in \{0,1\}$ покладемо

$$\mathscr{A}_{n,r}^{(\varepsilon,\delta)} = \{\alpha \in \mathscr{A}_{n,r} \mid \alpha[r] = \varepsilon,\ \alpha[0] = \delta\}.$$

Маємо $\mathscr{A}_{n,r} = \mathscr{A}_{n,r}^{(0,0)} \cup \mathscr{A}_{n,r}^{(0,1)} \cup \mathscr{A}_{n,r}^{(1,0)} \cup \mathscr{A}_{n,r}^{(1,1)}$, і ці підмножини попарно не перетинаються.

Опишемо кожну підмножину:

1. $\alpha[0] = 0,\ \alpha[r] = 0$. Жоден блок одиниць не з'являється у векторі, тому $A_{n,r}^{(0,0)}$ містить тільки нульовий вектор.
2. $\alpha[0] = 1,\ \alpha[r] = 0$. Єдиний блок $1 \dots 1$ починається у позиції 0 і закінчується в одній із позицій $1, \dots, r-1$. Отже, α може мати лише форму

$$\alpha \;=\; 2^k - 1, \qquad 0 < k \le r.$$

3. $\alpha[0] = 0,\ \alpha[r] = 1$. В цьому випадку блок одиниць починається з позиції r і закінчується в одній із позицій $r + 1 \le t \le n - t$.

$$\alpha \;=\; \left(2^t - 1\right) \ll r, \qquad 0 < t \le n - r.$$

4. $\alpha[0] = 1,\ \alpha[r] = 1$. Цей випадок особливий, бо тут виходить два блока з одиниць, перший з яких, починається в позиції 0, а інший в позиції r, тому:

$$\alpha \;=\; \left(2^k - 1\right) + \left(\left(2^t - 1\right) \ll r\right),$$

де $0 < k < r$, а $0 < t \le n - r$.

Бачимо, що можна об'єднати всі випадки в єдиний спосіб:

$$\mathscr{A}_{n,r} = \left\{ \left(2^s - 1\right) + \left(\left(2^t - 1\right) \ll r\right) \;\middle|\; \begin{array}{l} 0 \le s \le r, \\ 1 \le t \le n - r \end{array} \right\},$$

що і треба було довести.

Наслідок 3. Для будь-якого фіксованого значення r, кількість векторів $\alpha \in V_n$, які задовільняють умові $\overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r} = 0$, дорівнює

$$|\mathscr{A}_{n,r}| = (r+1)(n-r+1).$$

Доведення. В нотації доведення леми 1 маємо

$$\begin{aligned} |\mathscr{A}_{n,r}| &= |\mathscr{A}_{n,r}^{(0,0)}| + |\mathscr{A}_{n,r}^{(0,1)}| + |\mathscr{A}_{n,r}^{(1,0)}| + |\mathscr{A}_{n,r}^{(1,1)}| = \\ &= 1 + (n-r) + r + (n-r)r = \\ &= n + 1 + nr - r^2 = n(r+1) - (r^2 - 1) = \\ &= (r+1)(n-r+1). \end{aligned}$$

3.2. RX-диференціали з тотожними вхідними різницями

Розглянемо RX-диференціали виду $(r; \alpha, \alpha \to \gamma)$. Сконцентруємо увагу на диференціалах із найбільшими коефіцієнтами в формулі (2) (див. зауваження 1). Відповідно, будемо розглядати диференціали, для яких виконуються умови

$$\delta[0] = 0, \quad \delta[r] = 0, \quad \delta = \gamma.$$

Множина допустимих векторів для даного RX-диференціалу із $\gamma[0] = \gamma[r] = 0$ визначається за формулою:

$$\mathscr{B}_{n,r}(\alpha) = \left\{ \gamma \in V_n \;\middle|\; \overline{(\alpha \ll 1)} \wedge \gamma \wedge \mu_{n,r} = 0 \right\}.$$

Лема 2. *Для будь-якого фіксованого значення r і довільного вектора $\alpha \in V_n$ кількість векторів γ, які задовільняють умові $\overline{(\alpha \ll 1)} \wedge \gamma \wedge \mu_{n,r} = 0$, $\gamma[0] = \gamma[r] = 0$ дорівнює:*

$$|\mathscr{B}_{n,r}(\alpha)| = 2^{wt(\alpha \ll 1) - \alpha[r-1]}.$$

Доведення. У координатах 0 та r маємо умову $\overline{\gamma[0] = \gamma[r]} = 0$. У всіх інших позиціях діє рівняння $\overline{(\alpha \ll 1)} \wedge \gamma = 0$, тобто

$$\gamma[i] = \begin{cases} 0, & \text{якщо } (\alpha \ll 1)[i] = 0, \\ 0 \text{ або } 1, & \text{якщо } (\alpha \ll 1)[i] = 1. \end{cases}$$

Отже γ має вільні біти саме там, де $i \notin \{0, r\}$ і $(\alpha \ll 1)[i] = 1$. Таких позицій

$$\mathrm{wt}(\alpha \ll 1) - \alpha[r-1],$$

бо можливу одиницю у координаті r нівелює маска. Кожен вільний біт задається незалежно, тому

$$|\mathscr{B}_{n,r}(\alpha)| = 2^{\,\mathrm{wt}(\alpha \ll 1) - \alpha[r-1]},$$

що й треба було довести. □

Алгоритм 2 (Пошук векторів $\boldsymbol{\gamma}$, які максимізують ймовірність для диференціалу $\boldsymbol{(r; \alpha, \alpha \to \gamma)}$.

Вхід: *$\alpha \in V_n$, фіксоване значення обертання r $(1 \le r \le n-1)$.*

Вихід: *множина $\mathscr{B}_{n,r}(\alpha)$.*

1. *Фіксуємо біти, що визначені умовою зауваження 1:*

$$\gamma[0] \leftarrow 0, \qquad \gamma[r] \leftarrow 0.$$

2. *Для кожного індексу $i \in \{1, \dots, n-1\} \setminus \{r\}$ виконуємо*

(i) $\alpha[i-1]=1$, *то* $\gamma[i]\in\{0,1\}$ *(вибір довільний);*
(ii) $\alpha[i-1]=0$, *то* $\gamma[i]\leftarrow 0$.

Одержано замкнену оцінку потужності множини допустимих векторів $\mathscr{B}_{n,r}(\alpha)$, яка описує всі можливі вихідні різниці RX-диференціалів виду $(r;\alpha,\alpha\to\gamma)$ за умови $\gamma[0]=\gamma[r]=0$. Запропонований алгоритм *перебирає всю множину* $\mathscr{B}_{n,r}(\alpha)$ і будує кожен її вектор за *сумарний* час $O\big(n\,2^k\big)$,

$$k=\mathrm{wt}(\alpha\ll 1)-\alpha[r-1].$$

Такий підхід гарантує мінімальний можливий повний перебір та забезпечує точне оцінювання RX-ймовірностей, що істотно звужує простір пошуку під час аналізу ARX- та LRX-конструкцій.

3.3. RX-диференціали типу $(r;\alpha,\beta\to\alpha\oplus\beta)$

Знайдемо ймовірності RX-диференціалів операції $h(x,y)$ для диференціалу виду $(r;\alpha,\beta\to\alpha\oplus\beta)$. З теореми 1 маємо:

$$xrp^h(r;\alpha,\beta\to\gamma)\neq 0\Leftrightarrow(\overline{(\alpha\vee\beta)\ll 1})\wedge 0\wedge\mu_{n,r}=0.$$

Отже, ймовірність всіх таких RX-диференціалів не нульова. Із зауваження (1) відомо, що нас цікавлять RX-диференціали для якомога більшої ймовірності.

Лема 3. *Для фіксованого значення* $r,1\le r\le n-1$, *існує всього 16 різних варіантів побудувати пару векторів* $(\alpha,\beta)\in V_n$, *які дають максимальну ймовірність* (9/16) *RX-диференціала виду* $(r;\alpha,\beta\to\alpha\oplus\beta)$.

Доведення. Щоб отримати максимальну RX-диференціальну ймовірність, необхідно, щоб $wt(((\alpha\vee\beta)\ll 1)\wedge\mu_{n,r})=0$, де $\mu_{n,r}$ - це вектор з одиниць в позиціях 0 та r.

В свою чергу це означає, що у векторах α та β на позиціях $n-1$ та $r-1$ можуть стояти або одиниця, або нуль; звідси слідує, що є $2^4=16$ різних способів побудувати таку пару векторів (α,β), для яких ймовірність RX-диференціала буде максимальна.

Усі диференціали цього класу задаються шаблоном $\alpha,\beta\in\{\star,0,\dots,0,\star,0,\dots,0\}$, де $\star\in\{0,1\}$ та знаходиться в позиціях $n-1$ і $r-1$.

Наведені результати встановлюють строгі верхні межі обчислювальної складності диференціально-обертальної атаки та надають вичерпний опис екстремальних пар (α,β), що досягають максимальної RX-ймовірності. Це створює необхідну основу для формального RX-диференціального аналізу ARX- і LRX-криптосистем та оптимізації відповідних автоматизованих пошукових методів.

Висновки

У даній роботі було сформульовано деякі алгебраїчні властивості ймовірностей RX-диференціалів функції $h(x,y)$, яка апроксимує модульне додавання та використовується в криптосистемах класу ARX, зокрема, в шифрі NORX. Було розглянуто необхідні й достатні умови існування RX-диференціалів з ненульовою ймовірністю та проведено детальний аналіз граничних випадків. Запропоновано ефективні алгоритми для пошуку RX-диференціалів максимальних ймовірностей. Встановлено, що кількість векторів, які утворюють RX-диференціали, безпосередньо залежить від структури бітових векторів, що використовуються як вхідні значення.

Отримані результати можуть бути застосовані для оцінки стійкості ARX- та LRX-криптосистем, які використовують апроксимацію модульного додавання, щодо RX-диференціального криптоаналізу. Це дозволяє більш ефективно проєктувати криптографічні алгоритми та аналізувати їх безпеку проти сучасних криптоаналітичних атак.

Перелік використаних джерел

1. The SIMON and SPECK Families of Lightweight Block Ciphers / R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers. — 2013. — URL: https://eprint.iacr.org/2013/404. Cryptology ePrint Archive, Paper 2013/404.
2. *Aumasson J.-P.*, *Jovanovic P.*, *Neves S.* NORX V3.0: Submission to the CAESAR Competition. — 2015. — URL: https://competitions.cr.yp.to/round3/norxv30.pdf.
3. Ascon v1.2: Lightweight Authenticated Encryption and Hashing / C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer // Journal of Cryptology. — 2021. — Т. 34. — DOI: 10.1007/s00145-021-09398-9.
4. *Ashur T.*, *Liu Y.* Rotational Cryptanalysis in the Presence of Constants // IACR Transactions on Symmetric Cryptology. — 2016. — Груд. — Т. 2016, № 1. — С. 57—70. — DOI: 10.13154/tosc.v2016.i1.57-70.
5. *Yakovliev S.*, *Korzh N.* Differential-Rotational Probabilities of Modular Addition and Its Approximations // Vol. 6 No. 2 (2024): Theoretical and Applied Cyber Security. — 2025. — DOI: https://doi.org/10.20535/tacs.2664-29132024.2.
6. *Biryukov A.*, *Lambin B.*, *Udovenko A.* Exact Formula for RX-Differential Probability through Modular Addition for All Rotations. — 2025. — DOI: 10.46586/tosc.v2025.i1.542-591. — Cryptology ePrint Archive, Paper 2025/550.
7. *Warren H.* Hacker's Delight. — Addison-Wesley, 2013. — С. 494. — (Always learning). — ISBN 9780321842688.