УДК 04.056.53

ДИФЕРЕНЦІАЛЬНО-ОБЕРТАЛЬНИЙ КРИПТОАНАЛІЗ ОПЕРАЦІЙ, ЯКІ АПРОКСИМУЮТЬ ДОДАВАННЯ ЗА МОДУЛЕМ

Н. С. Корж[1,а], С. В. Яковлєв[1,б]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі розглядається новітній метод криптоаналізу ARX-криптосистем — диференціально-обертальний криптоаналіз, або RX-аналіз, та його застосування до деяких класів LRX-криптосистем. Знайдено аналітичні вирази для імовірностей проходження RX-диференціалів через перетворення, які побудовані з логічних операцій та апроксимують додавання за модулем; одне з таких перетворень використовується у шифрі NORX. Одержані результати дозволяють використовувати наявні формалізовані методи та інструменти для оцінювання стійкості LRX-криптосистем, побудованих із використанням зазначених перетворень, до RX-аналізу.

Ключові слова: диференціальний криптоаналіз, обертальний криптоаналіз, ARX-криптосистеми, NORX

Вступ

Обертальний криптоаналіз (англ. *rotational cryptanalysis*) є специфічним видом криптоаналізу, оскільки він може бути застосованим лише до ARX-криптосистем. Він був запропонований Д. Ховратовичем та І. Ніколічем [1].

Основна ідея обертального криптоаналізу полягає в аналізі закономірностей шифрування текстів із відомими різницями, як і, наприклад, у диференціальному криптоаналізі; однак у даному випадку використовується «різниця» за унарною операцією циклічного зсуву, що є властивістю даного методу атаки та обмежує сферу її використання саме ARX-криптосистемами. Виявилось, що використання додавання констант (за довільними операціями) ефективно протидіє обертальному криптоаналізу.

У роботі [2] 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. 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.

NORX — схема автентифікованого шифрування з асоційованими даними (AEAD) [3], 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.

У роботі [4] було запропоновано нову операцію, яка також апроксимує модульне додавання та має потенційно ще більш привабливі криптографічні властивості, ніж операція у NORX.

У даній роботі буде розглянуто стійкість зазначених операцій до RX-аналізу; зокрема, буде знайдено аналітичні вирази для імовірностей проходження узагальнених диференціалів через вузли, побудовані на основі операцій, які апроксимують додавання за модулем.

1. Імовірності проходження RX-диференціалів через операції, які апроксимують додавання

У подальшому у даній роботі будемо використовувати таку нотацію:

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;

$x \ll 1$ — нециклічний зсув вектору x на 1 біт ліворуч;

$x \vee y$ — операція логічного АБО;

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

[а] nik.korzh.ita@gmail.com
[б] yasv@rl.kiev.ua

$mask = (0, \dots, 0, 1, 0, \dots, 1)$ — 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).

У роботі [3] розробники шифру NORX ввели операцію

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

яка апроксимує модульне додавання. У роботі [4] була запропонована інша операція

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

яка також апроксимує модульне додавання в інший спосіб. Окремі алгебраїчні властивості цих операцій були досліджені авторами відповідних робіт.

Основним інструментом диференціально-обертального криптоаналізу є так званий узагальнений диференціал, або RX-диференціал, який ми визначимо таким чином.

Нехай $f\colon V_n \times V_n \to V_n$ — деяке відображення. *RX-диференціалом* функції f називається довільна трійка векторів $(\alpha, \beta, \gamma) \in V_n^3$, для яких виконується співвідношення

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

при заздалегідь зафіксованому значенні циклічного зсуву $k \in \mathbb{N}$. Імовірністю RX-диференціала називається ймовірність виконання рівняння (1) при $x, y \in_R V_n$.

Т. Ашур і Ю. Лю у роботі [2] знайшли аналітичні вирази для імовірності проходження RX-диференціалу через функцію $f(x, y) = (x+y) \bmod 2^n$. Нам вдалось одержати аналогічні результати для операцій, які апроксимують модульне додавання. Ці результати наведені у двох наступних теоремах.

Теорема 1. Для фіксованого значення зсуву k імовірність 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. Необхідно порахувати імовірність виконання співвідношення

$$\overrightarrow{x \oplus y \oplus ((xy) \ll 1)} \oplus \gamma = \\ = \overrightarrow{x} \oplus \alpha \oplus \overrightarrow{y} \oplus \beta \oplus (((\overrightarrow{x} \oplus \alpha)(\overrightarrow{y} \oplus \beta)) \ll 1).$$

Почнемо з того, що розглянемо кожну частину рівняння окремо. Введемо позначення

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

Розглядаючи ці величини побітово, отримаємо таку систему співвідношень для u:

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

і аналогічну систему співвідношень для v:

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

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

1. Якщо $i = 0$, то

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

2. Якщо $i = n - k$, то

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

3. Якщо $i < n - k$, то

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

4. Якщо $i > n - k$, то

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

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. У випадку $i = 0$, якщо $\delta_0 = 0$, то

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

а якщо $\delta_0 = 1$, то

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

Отже, можемо записати, що

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

2. Випадок $i = n - k$ розглядається аналогічно попередньому випадку; імовірність 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 1 наведено значення ймовірності p_i для усіх можливих значень параметрів даного рівняння.

Табл. 1. Таблиця ймовірностей проходження диференціалу через $h(x, y)$.

α_{i-1}	β_{i-1}	δ_i	рівняння	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 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

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

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.

Теорема 2. 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 теореми 2 з точністю до позначень повторює доведення теореми 1.

З формулювань тверджень теорем 1 та 2 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 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 знайдено аналітичні вирази для імовірностей RX-диференціалів таких операцій та сформульовано умови їх неможливості. Показано, що для обох операцій RX-диференціали мають однакову умову можливості, 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 використаних джерел

1. *Khovratovich D.*, *Nikolić I.* Rotational Cryptanalysis of ARX // Fast Software Encryption. — Springer Berlin Heidelberg, 2010. — С. 333—346. — DOI: https://doi.org/10.1007/978-3-642-13858-4_19.
2. *Ashur T.*, *Liu Y.* Rotational Cryptanalysis in the Presence of Constants. — 2016. — URL: https://eprint.iacr.org/2016/826.pdf.
3. *Aumasson J.-F.*, *Jovanovic P.*, *Neves S.* Analysis of NORX: Investigating Differential and Rotational Properties. — 2014. — URL: https://eprint.iacr.org/2014/317.pdf.
4. *Яковлєв С.* Криптографічні властивості операцій, які апроксимують додавання за модулем // Інформаційні технології та комп'ютерне моделювання (15-16 грудня 2022 року, м. Івано-Франківськ). — Івано-Франківськ: п. Голіней О.М., 2022. — С. 112—115.