УДК 004.056.55:512.6

ОБЕРТАЛЬНИЙ КРИПТОАНАЛІЗ ОДНІЄЇ З УСКЛАДНЮЮЧИХ ФУНКЦІЙ ГЕШ-ФУНКЦІЇ SHABAL

П. О. Бондар[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

В цій статті наведено застосування обертального криптоаналізу однієї з двох функцій, що використовуються у псевдовипадковій перестановці учасника конкурсу SHA-3 — геш-функції Shabal. Було одержано аналітичні вирази для обчислення ймовірності проходження пари обертання через функцію $f(x) = 3x \bmod 2^n$ для довільних n та r. Отриманий результат доповнює та узагальнює отримані раніше часткові результати для обертального криптоаналізу функції $f(x) = 3x \bmod 2^n$.

Ключові слова: обертальний криптоаналіз, ARX-криптосистеми, геш-функція Shabal

Вступ

Цікавість дослідження ARX-криптосистем викликана їх поширеністю на практиці, особливо в системах з обмеженими ресурсами, завдяки простоті реалізації таких криптосистем та ефективності виконання операцій, на яких ґрунтуються ARX-криптопримітиви: модульного додавання, циклічних зсувів та побітового виключного АБО (*англ.* Addition, Rotation, XOR).

Метод обертального криптоаналізу — це відносно новий спосіб аналізу криптосистем, що ґрунтується на дослідженні змін в парах обертання, після їх перетворення у криптопримітиві чи системі, і обчисленні імовірності їх проходження через систему. Вперше цей метод був застосований у 2006 році розробниками блокового шифру SEA [1], а формалізований він був 2010 року в роботі Ховратовича на Ніколіча [2].

За об'єкт дослідження було взято відображення $f(x) = 3x \bmod 2^n$, що є одним з двох відображень, використаних у псевдовипадковій перестановці геш-функції Shabal на конкурсі SHA-3 [3]. Для цієї функції попередньо були отримані ймовірності проходження обертальних пар для фіксованих значень $n = 32$ та $r = 1$ [4], а також для довільного значення n і фіксованих значень обертання $r = 1$ та $r = n - 1$ [5]. Метою цієї роботи є обчислення ймовірностей для довільного значення n та довільного значення обертання $r \in \{2, \dots, n-2\}$.

1. Загальні поняття та попередні результати

Введемо набір умовних позначень, які будуть використовуватися в роботі надалі:

- $V_n = \{0,1\}^n$ — множина двійкових векторів довжини n;
- $x = (x_{n-1}, x_{n-2}, \dots, x_0) \in V_n$ — двійковий вектор довжини n;
- $\oplus$ — операція побітового виключного АБО (XOR);
- $\lll r$ / $\ggg r$ — операція циклічного зсуву вліво-/вправо на r бітів;
- x^r / x^{-r} — бітовий вектор x, циклічно зсунутий вліво/вправо на r бітів ($x \lll r$ / $x \ggg r$);

При застосуванні обертального криптоаналізу стійкість системи оцінюється за ймовірністю проходження пар обертання через криптопримітив чи систему.

Довільна пара векторів виду (x, x^r) називається *парою обертання* (з обертанням r).

Ймовірність проходження пари обертання через відображення (систему) $f : V_n \to V_n$ визначається так:

$$rp^f(r) = \Pr\{f(x^r) = (f(x))^r\}.$$

Тут і надалі будемо вважати, що розподіл векторів $x \in V_n$ є рівноймовірним, тобто кожен вектор $x \in V_n$ має однакову ймовірність появи $\frac{1}{2^n}$.

Як вже зазначалося, функція $f(x) = 3x \bmod 2^n$ вже досліджувалася раніше і було отримано низку певних часткових результатів. Для повноти дослідження нам необхідно зазначити ці результати.

Ван Ассхе у короткій статті 2010 року [4] навів (без доведення) значення ймовірності проходження обертальної пари через функцію $f(x)$ для значень $n = 32$ і $r = 1$:

$$rp^f(1) = \frac{2^{32} - 1}{3 \cdot 2^{32}} \approx \frac{1}{3}.$$

В одній з попередніх робіт [5] було наведено імовірності для довільного значення n, але для фіксованих значень обертання $r = 1$ та $r = n - 1$.

[a] bondar.petro@lll.kpi.ua

Отримані результати мали такий вигляд:

$$rp^f(1) = \frac{2^n + (-1)^{n+1}}{3 \cdot 2^n},$$
$$rp^f(n-1) = \frac{2^n + (-1)^{n+1}}{3 \cdot 2^n}.$$

2. Обертальний криптоаналіз функції множення на 3 в загальному випадку

Для повноти розуміння властивостей, необхідно обчислити ймовірності проходження обертальних пар для довільних значень $r \in \{2, \dots, n-2\}$. В ході дослідження було отримано такий результат.

Теорема 1. *Для довільного значення n, ймовірність проходження пари обертання через функцію $f(x) = 3x \mod 2^n$ при довільному значенні обертання $r \in \{2, \dots, n-2\}$ можна обчислити за такою формулою:*

$$rp^f(r) = \frac{1}{9}\left(1 + \frac{2^{1-(n-r) \bmod 2}}{2^{n-r}}\right)\left(1 + \frac{2^{1-r \bmod 2}}{2^r}\right).$$

Виокремимо два часткові випадки, що випливають з отриманого результату.

Наслідок 1. Ймовірність проходження пари обертання через функцію $f(x) = 3x \mod 2^n$ при обертанні $r = 2$ дорівнює

$$rp^f(2) = \frac{1}{6} + \frac{2^{1+(n \bmod 2)}}{3 \cdot 2^n} \approx \frac{1}{6}.$$

Наслідок 2. Ймовірність проходження пари обертання через функцію $f(x) = 3x \mod 2^n$ при обертанні $r = 3$ дорівнює

$$rp^f(3) = \frac{1}{8} + \frac{2^{1-(n \bmod 2)}}{2^n} \approx \frac{1}{8}.$$

За виглядом формули ймовірності з теореми 1 можна побачити, що для певного фіксованого значення обертання r зі збільшенням значення n ймовірність буде прямувати до деякої константи. Так, наприклад, для випадків $r = 2$ (наслідок 1) та $r = 3$ (наслідок 2) це будуть значення $\frac{1}{6}$ та $\frac{1}{8}$ відповідно. Отриманий результат не є узагальненням випадків $r = 1$ та $r = n-1$, бо в цих випадках утворюється тільки один ланцюг залежних бітів переносу, на відміну від інших значень r, і через це аналіз дещо відрізняється.

2.1. Допоміжні твердження

Розглянемо побітове представлення значення $y = 3x \mod 2^n$ для загального вигляду $x \in V_n$, яке наведено у таблиці 1.

У цій таблиці c_i – біти переносу операції $x + 2x$, що обчислюються як

$$\forall i \in \{2, \dots, n-1\} : \; c_i = \left\lfloor \frac{x_{i-1} + x_{i-2} + c_{i-1}}{2} \right\rfloor. \quad (1)$$

Розглянемо подію $x_{k-1} = c_k = 1$ і позначимо ймовірність $p_k = \Pr\{x_{k-1} = c_k = 1\}$.

Лема 1. Для довільного $k \in \{2, \dots, n-1\}$ ймовірність p_k можна обчислити таким чином:

$$p_k = \frac{12\hat{p}_2 + (-2)^k - 4}{3 \cdot (-2)^k}, \quad (2)$$
$$\text{де } \hat{p}_2 = \begin{cases} \frac{1}{4}, & \text{якщо } k \text{ — парне,} \\ \frac{1}{2}, & \text{інакше.} \end{cases}$$

Доведення. Введемо додаткові позначення:

$$p_{i,0} = \Pr\{x_{i-1} = c_i = 0\},$$
$$p_{i,1} = \Pr\{x_{i-1} = c_i = 1\}.$$

Можна побачити, що $p_k = p_{k,1}$.

Для довільного c_i, де $2 < i < k$, розглянемо такі випадки.

Якщо $x_{i-1} = 1$, то, за формулою (1), $c_i = x_{i-1} = 1$ тоді й тільки тоді, коли $x_{i-2} + c_{i-1} \neq 0$, а отже:

$$p_{i,1} = \Pr\{x_{i-1} = 1\} \cdot \Pr\{x_{i-2} + c_{i-1} \neq 0\} = \\ = \frac{1}{2}(1 - p_{i-1,0}).$$

Якщо $x_{i-1} = 0$, то, за формулою (1), $c_i = x_{i-1} = 0$ тоді й тільки тоді, коли $x_{i-2} + c_{i-1} \neq 1$, а отже:

$$p_{i,0} = \Pr\{x_{i-1} = 0\} \cdot \Pr\{x_{i-2} + c_{i-1} \neq 1\} = \\ = \frac{1}{2}(1 - p_{i-1,1}).$$

Виникла рекурента зі змінними початковими значеннями: $p_{2,1}$ та $p_{2,0}$. Іншими словами, якщо для досягнення початкового значення необхідна парна кількість кроків (обчислення рекуренти) — тоді початковим значенням буде $p_{2,1}$, а якщо непарна кількість кроків — тоді $p_{2,0}$. Парність кількості кроків можна обчислити із парності значення k, бо кількість кроків рекуренти становить $k - 2$. Оскільки вигляд рекуренти однаковий і змінюється тільки початкове значення, тоді зведемо ці дві рекуренти до однієї:

$$\hat{p}_i = \frac{1}{2}(1 - \hat{p}_{i-1}).$$

Позначимо для певного фіксованого значення k: $\hat{p}_2 = p_{2,1}$, якщо k — парне і $\hat{p}_2 = p_{2,0}$, якщо k — непарне.

З таблиці 1 можна побачити, що значення другого біту переносу обчислюється як

$$c_2 = \lfloor (x_1 + x_0 + 0)/2 \rfloor = x_1 \,\&\, x_0,$$

а отже отримаємо початкові значення, обчисливши відповідні ймовірності.

1. $c_2 = x_1 = 1$ тоді й тільки тоді, коли $x_1 = 1$ і $x_0 = 1$. Ймовірність цієї події дорівнює 1/4.
2. $c_2 = x_1 = 0$ тоді й тільки тоді, коли $x_1 = 0$ (значенням x_0 можна знехтувати). Ймовірність цієї події дорівнює 1/2.

З цього можна зробити висновок, що $\hat{p}_2 = \frac{1}{4}$, якщо k — парне і $\hat{p}_2 = \frac{1}{2}$, якщо k — непарне.

Розписавши отриману рекуренту для певного значення k і згорнувши отриману суму за формулою суми геометричної прогресії з часткою 1/2, ми отримаємо таку формулу:

$$p_k = \hat{p}_k = \frac{12\hat{p}_2 + (-2)^k - 4}{3 \cdot (-2)^k}.$$

□

2.2. Доведення теореми 1

Перейдемо до доведення основної теореми.

Позначимо $y = 3x \bmod 2^n$ і $l = 3(x \lll r) \bmod 2^n$. Розглянемо таблиці 1 та 2, які є побітовим представленням застосування функції $f(x) = 3x \bmod 2^n$ до вектора x зі зсувом і після цього застосуванням $f(x)$ до зсунутого вектора $x \lll r$. Щоб порахувати ймовірність події $y \lll r = l$, необхідно зіставити ці два вектори побітово.

З таблиці 1 можна отримати такі співвідношення:

$$\begin{aligned}
&y_0 = x_0, && c_0 = c_1 = 0;\\
&1 < i < n: && y_i = x_i \oplus x_{i-1} \oplus c_i;\\
&1 < i < n-1: && c_{i+1} = \left\lfloor \frac{x_i + x_{i-1} + c_i}{2} \right\rfloor.
\end{aligned}$$

З таблиці 2 можна отримати такі співвідношення:

$$\begin{aligned}
&l_0 = x_{n-r}, && c'_0 = c'_1 = 0;\\
&l_1 = x_{n-r+1} \oplus x_{n-r}, && c'_2 = x_{n-r+1} \,\&\, x_{n-r};\\
&l_r = x_0 \oplus x_{n-1} \oplus c'_r, && c'_{r+1} = \left\lfloor \frac{x_0 + x_{n-1} + c'_r}{2} \right\rfloor;\\
&1 < i < r: && l_i = x_{n-r+i} \oplus x_{n-r+i-1} \oplus c'_i,\\
& && c'_{i+1} = \left\lfloor \frac{x_{n-r+i} + x_{n-r+i-1} + c'_i}{2} \right\rfloor;\\
&r < i < n: && l_i = x_{i-r} \oplus x_{i-r-1} \oplus c'_i,\\
& && c'_{i+1} = \left\lfloor \frac{x_{i-r} + x_{i-r-1} + c'_i}{2} \right\rfloor;
\end{aligned}$$

Зіставивши відповідні біти векторів $y \lll r$ та l, отримаємо такі умови:

$$\begin{aligned}
l_0 = y_{n-r}, \quad l_1 &= y_{n-r+1};\\
l_r = y_0, \quad l_{r+1} &= y_1;\\
1 < i < r: \quad l_i &= y_{n-r+i};\\
r+1 < i < n: \quad l_i &= y_{i-r}.
\end{aligned}$$

Розписавши їх значення відповідно до зазначеного вище, отримаємо умови, необхідні для виконання рівності:

$$\begin{aligned}
x_{n-r-1} &= c_{n-r}; && (3)\\
c_{n-r+1} &= 0; && (4)\\
x_{n-1} &= c'_r; && (5)\\
c'_{r+1} &= 0; && (6)\\
\forall 1 < i < r: \quad c'_i &= c_{n-r+i}; && (7)\\
\forall r+1 < i < n: \quad c'_i &= c_{i-r}. && (8)
\end{aligned}$$

Зменшимо кількість цих умов, встановивши між ними зв'язок.

1. З умови (4) випливає умова (7).
   Розглянемо для $i = 2$:
   $$\begin{aligned}
   c_{n-r+2} &= \lfloor (x_{n-r+1} + x_{n-r} + c_{n-r+1})/2 \rfloor =\\
   &= \left| \text{за ум. (4)} \right| = \lfloor (x_{n-r+1} + x_{n-r})/2 \rfloor =\\
   &= x_{n-r+1} \,\&\, x_{n-r} = c'_2.
   \end{aligned}$$
   Для всіх інших значень з проміжку $\overline{3 \dots r-1}$ умова виконуватиметься автоматично, оскільки починаючи з $i = 2$ значення c'_i та c_{n-r+i} почнуть збігатися завдяки показаному вище.
2. Аналогічним чином можна показати, що з умови (6) випливає умова (8).
3. Поєднаємо умови (3) та (4):
   $$\begin{aligned}
   &x_{n-r-1} = c_{n-r} \,\&\, c_{n-r+1} = 0 \Leftrightarrow\\
   &\Leftrightarrow \left| c_{n-r+1} = \lfloor (x_{n-r} + x_{n-r-1} + c_{n-r})/2 \rfloor \right| \Leftrightarrow\\
   &\Leftrightarrow x_{n-r-1} = c_{n-r} = 0. \qquad (9)
   \end{aligned}$$
4. Поєднаємо умови (5) та (6):
   $$\begin{aligned}
   &x_{n-1} = c'_r \,\&\, c'_{r+1} = 0 \Leftrightarrow\\
   &\Leftrightarrow \left| c'_{r+1} = \lfloor (x_0 + x_{n-1} + c'_r)/2 \rfloor \right| \Leftrightarrow\\
   &\Leftrightarrow x_{n-1} = c_r = 0. \qquad (10)
   \end{aligned}$$

Поєднавши умови (9) та (10) з виглядом таблиць 1 та 2 виведемо чотири незалежні за побудовою події та оцінимо їх імовірності.

1. $x_{n-1} = 0$: за припущенням про рівноймовірний розподіл векторів x, імовірність цієї події становить $\Pr\{x_{n-1} = 0\} = \frac{1}{2}$.
2. $x_{n-r-1} = 0$: аналогічним чином імовірність цієї події становить $\Pr\{x_{n-r-1} = 0\} = \frac{1}{2}$.
3. $c_{n-r} = 0$: при виконанні $x_{n-r-1} = 0$, ця умова рівносильна $x_{n-r-2} \,\&\, c_{n-r-1} = 0$, що за визначенням операції ТА є еквівалентним $\neg(x_{n-r-2} = c_{n-r-1} = 1)$. Ймовірність цієї події можна обчислити за допомогою леми 1:
   $$\begin{aligned}
   &\Pr\{x_{n-r-2} \,\&\, c_{n-r-1} = 0\} =\\
   &\quad = 1 - \Pr\{x_{n-r-2} = c_{n-r-1} = 1\} = 1 - p_{n-r-1} =\\
   &\quad = 1 - \frac{12\hat{p}_2 + (-2)^{n-r-1} - 4}{3 \cdot (-2^{n-r-1})},
   \end{aligned}$$
   де $\hat{p}_2 = \frac{1}{4}$, якщо $(n-r-1)$ — парне, і $\hat{p}_2 = \frac{1}{2}$, якщо це значення непарне.

   Після низки арифметичних перетворень отримаємо такий результат:
   $$\Pr\{x_{n-r-2} \,\&\, c_{n-r-1} = 0\} = \frac{2}{3}\left(1 + \frac{2^{1-(n-r) \bmod 2}}{2^{n-r}}\right).$$
4. $c'_r = 0$: за умови $x_{n-1} = 0$, ця умова рівносильна $x_{n-2} \,\&\, c'_{r-1} = 0$. А це рівносильно $\neg(x_{n-2} = c'_{r-1} = 1)$.

Таблиця 1. Двійкове представлення $y = 3x \bmod 2^n$ та $y \lll r$.

c	c_{n-1}	c_{n-2}	c_{n-3}	$\dots$	c_{r+1}	c_r	c_{r-1}	$\dots$	c_2	$c_1 = 0$	$c_0 = 0$
x	x_{n-1}	x_{n-2}	x_{n-3}	$\dots$	x_{r+1}	x_r	x_{r-1}	$\dots$	x_2	x_1	x_0
$2x$	x_{n-2}	x_{n-3}	x_{n-4}	$\dots$	x_r	x_{r-1}	x_{r-2}	$\dots$	x_1	x_0	0
$3x$	y_{n-1}	y_{n-2}	y_{n-3}	$\dots$	y_{r+1}	y_r	y_{r-1}	$\dots$	y_2	y_1	y_0
$3x \lll r$	y_{n-1-r}	y_{n-2-r}	y_{n-3-r}	$\dots$	y_1	y_0	y_{n-1}	$\dots$	y_{n-r+2}	y_{n-r+1}	y_{n-r}

Таблиця 2. Двійкове представлення $l = 3(x \lll r) \bmod 2^n$.

c'	c'_{n-1}	c'_{n-2}	c'_{n-3}	$\dots$	c'_{r+1}	c'_r	c'_{r-1}	$\dots$	c'_2	$c'_1 = 0$	$c'_0 = 0$
$x \lll r$	x_{n-1-r}	x_{n-2-r}	x_{n-3-r}	$\dots$	x_1	x_0	x_{n-1}	$\dots$	x_{n-r+2}	x_{n-r+1}	x_{n-r}
$2(x \lll r)$	x_{n-2-r}	x_{n-3-r}	x_{n-4-r}	$\dots$	x_1	x_0	x_{n-1}	$\dots$	x_{n-r+1}	x_{n-r}	0
$3(x \lll r)$	l_{n-1}	l_{n-2}	l_{n-3}	$\dots$	l_{r+1}	l_r	l_{r-1}	$\dots$	l_2	l_1	l_0

Тут також застосовна лема 1 до зсунутого вектора:

$$\Pr\{x_{n-2} \,\&\, c'_{r-1} = 0\} = \\ = 1 - \Pr\{x_{n-2} = c'_{r-1} = 1\} = 1 - p_{r-1} = \\ = 1 - \frac{12\hat{p}_2 + (-2)^{r-1} - 4}{3 \cdot (-2^{r-1})},$$

де $\hat{p}_2 = \frac{1}{4}$, якщо $(r-1)$ — парне, і $\hat{p}_2 = \frac{1}{2}$, якщо це значення непарне.

Провівши аналогічні перетворення, як і в попередньому пункті, отримаємо:

$$\Pr\{x_{n-2} \,\&\, c'_{r-1} = 0\} = \frac{2}{3}\left(1 + \frac{2^{1-r \bmod 2}}{2^r}\right).$$

Враховуючи, що наведені вище події є незалежними й тільки за їх виконання є істинним твердження $y \lll r = l$, то можна стверджувати, що:

$$rp^f(r) = \Pr\{y \lll r = l\} = \\ = \Pr\{x_{n-1} = 0,\ x_{n-r-1} = 0, \\ x_{n-r-2} \,\&\, c_{n-r-1} = 0,\ x_{n-2} \,\&\, c'_{r-1} = 0\} = \\ = \Pr\{x_{n-1} = 0\} \cdot \Pr\{x_{n-r-1} = 0\} \times \\ \times \Pr\{x_{n-r-2} \,\&\, c_{n-r-1} = 0\} \cdot \Pr\{x_{n-2} \,\&\, c'_{r-1} = 0\} = \\ = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{3}\left(1 + \frac{2^{1-(n-r) \bmod 2}}{2^{n-r}}\right) \times \\ \times \frac{2}{3}\left(1 + \frac{2^{1-r \bmod 2}}{2^r}\right) = \\ = \frac{1}{9}\left(1 + \frac{2^{1-(n-r) \bmod 2}}{2^{n-r}}\right)\left(1 + \frac{2^{1-r \bmod 2}}{2^r}\right).$$

Теорему доведено.

Висновки

В ході виконаного дослідження було проаналізовано функцію $f(x) = 3x \bmod 2^n$ за допомогою обертального криптоаналізу. Було одержано значення імовірностей проходження пари обертання через цю функцію для довільних значень n та r, що є основним параметром, що визначає стійкість до обертального криптоаналізу.

Отриманий результат відкриває нові можливості статистичного аналізу цієї функції завдяки аналітичному вигляду формули ймовірності проходження обертальної пари через примітив. Це допоможе краще оцінювати стійкість криптопримітивів, що використовують функцію $f(x)$.

Перелік використаних джерел

1. SEA: A Scalable Encryption Algorithm for Small Embedded Applications / F.-X. Standaert, G. Piret, N. Gershenfeld, J.-J. Quisquater // Smart Card Research and Advanced Applications / за ред. J. Domingo-Ferrer, J. Posegga, D. Schreckling. — Springer Berlin Heidelberg, 2006. — С. 222—236. — ISBN 978-3-540-33312-8.
2. *Khovratovich D., Nikolić I.* Rotational Cryptanalysis of ARX // Fast Software Encryption / за ред. S. Hong, T. Iwata. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2010. — С. 333—346. — ISBN 978-3-642-13858-4.
3. Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition / E. Bresson [та ін.]. — 2008. — Submission to NIST.
4. *Assche G. van.* A Rotational Distinguisher on Shabal's Keyed Permutation and Its Impact on the Security Proofs. — 2010. — URL: http://gva.noekeon.org/papers/ShabalRotation.pdf.
5. *Панасюк Є. С.* Диференціально-обертальний криптоаналіз деяких ускладнюючих функцій ARX-криптосистем : дипломна робота ... бакалавра : 113 Прикладна математика. — 2023. — URL: https://ela.kpi.ua/handle/123456789/63228.