УДК 512.13:004.021+003.26

ВИЗНАЧЕННЯ ДИФЕРЕНЦІАЛЬНИХ ВЛАСТИВОСТЕЙ ОПЕРАЦІЇ ПОБЛОКОВОГО ДОДАВАННЯ

І. О. Ломаченко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

У роботі розглянуто диференціальні властивості поблокового додавання, наведено умови існування ненульових імовірностей та представлення у вигляді S-функції. Також показано, як звести процес обчислення відповідних імовірностей до загального фреймворку аналізу розширених S-функцій. Отримані результати можуть бути застосовані для криптоаналізу блокових та потокових шифрів, зокрема, ARX-криптосистем.

Ключові слова: диференціальний криптоаналіз, ARX-криптосистеми, S-функції

Вступ

В наш час диференціальний криптоаналіз є надзвичайно потужним засобом аналізу криптопримітивів, що все ще продовжує свій розвиток. Розроблюються нові підходи до рішення задач, вдосконалюються старі, з'являються нові напрями подальшого розвитку.

На даний момент у зв'язку з розвитком і розповсюдженням ARX-криптосистем та покращенням методів криптоаналізу актуальним є дослідження диференціальних властивостей одних операцій над векторами довільної довжини відносно інших. Надалі мова буде іти про властивості поки що малодослідженої, але перспективної операції поблокового додавання.

1. Формалізація задачі

Введемо наступні позначення:

Вектори x, $y \in V_{2n}$ належать простору $2n$-бітних векторів

$>> n$ – зсув бітів на n позицій в сторону менших розрядів

$\oplus$ – операція XOR над векторами;

$+$ – операція додавання векторів, як чисел за модулем 2^n;

$c(x, y) \in V_{2n}$ – вектор переносів для суми x+y, що задається рекурсивно

$c_0 = 0$, $c_{i+1} = (x_i \cap y_i) \oplus (x_i \cap c_i) \oplus (y_i \cap c_i)$

$[+]$ – операція поблокового додавання векторів, що задається таким чином:

$$x = (x_1, x_2), y = (y_1, y_2); x_1, x_2, y_1, y_2 \in V_n$$

$$x[+]y = (x_1 + y_1, x_2 + y_2)$$

Диференціальною імовірністю XOR відносно додавання будемо називати імовірність

$$xdp^+(\alpha, \beta \to \gamma) = P[(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma]$$

Диференціальною імовірністю додавання відносно XOR будемо називати імовірність

$$adp^\oplus(\alpha, \beta \to \gamma) = P[(x + \alpha) \oplus (y + \beta) = (x \oplus y) + \gamma]$$

Диференціальною імовірністю поблокового додавання відносно модульного додавання будемо називати імовірність

$$bdp^+(\alpha, \beta \to \gamma) = P(x[+]\alpha) + (y[+]\beta) = (x + y)[+]\gamma$$

Імовірності xdp^+ та $adp^\oplus$ вже досліджені Лімпаа[1], Валленом[2], Величковим[3] та ін.

2. Аналіз умов існування ненульових bdp^+

В ході досліджень імовірності bdp^+ були отримана наступна умова існування ненульових імовірностей, що накладається на параметри α, β, γ:

$$\alpha + \beta - \gamma = \underbrace{(c(x, \alpha)_n + c(y, \beta)_n - c(x + y, \gamma)_n)}_{\varphi} * 2^n$$

Бачимо, що $\alpha + \beta - \gamma$ приймає всього 4 значення. Але в залежності від конкретних векторів не всі значення φ досяжні. Сформулюємо необхідні умови досягання різних значень φ:

1) $\varphi = 2$;

$$\exists i, j \in \overline{0, n-1} : \alpha_i = \beta_j = 1$$

$$\gamma \text{ – будь-яке}$$

2) $\varphi = -1$;

$$\exists i \in \overline{0, n-1} : \gamma_i = 1$$

$$\alpha, \gamma \text{ – будь-які}$$

3) $\varphi = 1$;

$$\exists i, j, k \in \overline{0, n-1} : \alpha_i = \beta_j = \gamma_k = 1$$

4) $\varphi = 0$;

$$\exists i \in \overline{0, n-1} : \alpha_i \cup \beta_j = 1$$

$$\gamma \text{ – будь-яке}$$

Наведені умови є необхідними, але не достатніми. Кожен окремий випадок виникає із деякою імовірністю, яка залежить від x, y. При збільшенні кількості блоків адекватним засобом опису поведінки імовірності bdp^+ є її представлення у вигляді S-функції[3].

3. Представлення bdp^+ у вигляді S-функції

Згідно методики, описаної у [3], обчислення bdp^+ може бути виконане за лінійний відносно кількості блоків час, якщо представити процес обчислення як S-функцію.

Ми представимо обчислення bdp^+ у вигляді розширеної S-функції, що оперує не окремими бітами, а бітовими блоками.

Нагадаємо, що S-функцією ми називаємо перетворення виду $\gamma = f(x, y, \alpha, \beta)$, обчислення якого зводиться до обчислень виду

$$(\gamma[i], S[i+1]) = f(x[i], y[i], \alpha[i], \beta[i], S[i]),$$

де S – деякі допоміжні стани.

Наведемо представлення функції f такої, що

$$bdp^+(\alpha, \beta \to \gamma) = P(f(x, y, \alpha, \beta) = \gamma) :$$

$$x[+]\alpha \to x_1$$

$$y[+]\beta \to y_1$$

$$x + y \to z_1$$

$$x_1 + y_1 \to z_2$$

$$z_2[-]z1 \to \gamma$$

$$x[i] + \alpha[i] \to x_1[i]$$

$$y[i] + \beta[i] \to y_1[i]$$

$$x[i] + y[i] + c_1[i] \to z_1[i]$$

$$x_2[i] + y_2[i] + c_2[i] \to z_2[i]$$

$$(x[i] + y[i] + c_1[i]) >> n \to c_1[i+1]$$

$$(x_1[i] + y_1[i] + c_2[i]) >> n \to c_2[i+1]$$

$$z_2[i] - z_1[i] \to \gamma[i]$$

Станом є пара бітів переносу $(c_1[i], c_2[i]) \to S[i]$

Таким чином, обчислення bdp^+ може бути виконано за допомогою ефективного алгоритму, що грунтується на аналізі S-функції. Однак ресурсні вимоги цього алгоритму є відкритим питанням, якому планується присвятити подальші дослідження.

Висновки

В даній роботі було досліджено диференціальні властивості операції поблокового додавання. Сформульовано умови розв'язуваності та показано, як звести процес обчислення відповідних імовірностей до загального фреймворку аналізу розширених S-функцій. Отримані результати можуть бути застосовані для криптоаналізу блокових та потокових шифрів, зокрема, ARX-криптосистем.

Перелік використаних джерел

1. Lipmaa H., Moriai S. Efficient Algorithms for Computing Differential Properties of Addition. In M. Matsui, editor, FSE, volume 2355 of Lecture Notes in Computer Science. — 2001. — 336–350 p.
2. Walle'n J. On the Differential and Linear Properties of Addition. Helsinki University of Technology Laboratory for Theoretical Computer Science Research Reports 84. — 2003. — 12-19 p.
3. Mouha N., Velichkov V., De Cannie're C., Preneel B. The Differential Analysis of S-functions. Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven. — 4-12 p.