

ЛИТЕРАТУРА

1. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2001.
3. Зубов А. Ю. Совершенные шифры. М.: Гелиос АРВ, 2003.
4. Медведева Н. В., Титов С. С. Конструкции неэндоморфных совершенных шифров // Прикладная дискретная математика. Приложение. 2020. № 13. С. 51–54.
5. Медведева Н. В., Титов С. С. К задаче описания минимальных по включению совершенных шифров // Прикладная дискретная математика. Приложение. 2021. № 14. С. 91–95.
6. Зубов А. Ю. Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
7. Зубов А. Ю. О понятии ε -совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45–52.

УДК 519.7

DOI 10.17223/2226308X/15/14

ВЫЧИСЛЕНИЕ РАЗНОСТНЫХ ХАРАКТЕРИСТИК ДЛЯ СЛОЖЕНИЯ k ЧИСЕЛ ПО МОДУЛЮ 2^n ¹

А. С. Мокроусов

Рассматривается разностная характеристика $\text{xdr}_k^+(\alpha^1, \dots, \alpha^k \rightarrow \alpha^0)$, где $\alpha^0, \alpha^1, \dots, \alpha^k \in \mathbb{Z}_2^n$, которая определяет вероятность преобразования разностей $\alpha^1, \dots, \alpha^k$ в разность α^0 (относительно побитового «исключающего или») функцией $f(x_1, \dots, x_k) = x_1 + \dots + x_k \bmod 2^n$. Данная величина используется при разностном криптоанализе криптографических примитивов, содержащих «исключающее или» и сложение по модулю 2^n , например ARX-конструкций. Предложены аналитические выражения для матриц, используемых для вычисления xdr_k^+ . Кроме того, рассмотрена разностная характеристика $\text{adr}^\oplus(\alpha, \beta \rightarrow \gamma)$, где $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, определяющая вероятность преобразования разностей α, β в разность γ (относительно сложения по модулю 2^n) функцией $x \oplus y$, и получены все тройки разностей, вероятность которых больше $1/4$.

Ключевые слова: ARX, исключающее или, сложение по модулю, разностный криптоанализ, разностные характеристики.

Одним из подходов к построению криптографических примитивов является комбинирование сложения по модулю 2^n ($\boxplus$), побитовых операций (например, «исключающего или» — $\oplus$), битовых сдвигов ($\ll$), циклических сдвигов ($\lll$). Это позволяет получить очень быстрые в программной реализации алгоритмы. Особый интерес представляют ARX-конструкции, использующие только операции $\boxplus$, $\oplus$ и $\lll$. Примерами таких шифров являются FEAL [1], TEA [2], Salsa20 [3], Speck [4].

Хорошие шифры должны быть стойкими к различным видам криптоанализа, в частности к разностному криптоанализу [5]. Это один из основных статистических методов, основанный на исследовании того, в какие разности шифртекстов могут переходить разности открытых текстов. Важным шагом при реализации метода является вычисление разностных характеристик и их максимальных значений. Для базовых операций архитектуры ARX данные характеристики определяются следующим образом [6]:

¹Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).

$$\begin{aligned} \text{xdr}^+(\alpha, \beta \rightarrow \gamma) &= \frac{1}{4^n} |\{x, y \in \mathbb{Z}_2^n : (x \oplus \alpha) \boxplus (y \oplus \beta) = \gamma \oplus (x \boxplus y)\}|, \\ \text{adr}^\oplus(\alpha, \beta \rightarrow \gamma) &= \frac{1}{4^n} |\{x, y \in \mathbb{Z}_2^n : (x \boxplus \alpha) \oplus (y \boxplus \beta) = \gamma \boxplus (x \oplus y)\}|. \end{aligned}$$

С вектором $x = (x_0, \dots, x_{n-1}) \in \mathbb{Z}_2^n$ мы ассоциируем целое число $\sum_{i=0}^{n-1} x_i 2^i$, тогда $x \boxplus \alpha$ означает сложение ассоциированных с x и α чисел по модулю 2^n .

Недостатком ARX-шифров является сложность вычисления разностных характеристик для композиций операций. Существует подход с использованием S-функций [6], позволяющий вычислить разностные характеристики как произведение специальных матриц, построенных на основе рассматриваемого преобразования. Однако его алгоритмическое применение в большинстве случаев не позволяет получить аналитические выражения для данных матриц.

1. Матричный способ вычисления $\text{xdr}_k^+(\alpha^1, \dots, \alpha^k \rightarrow \alpha^0)$

Рассмотрим функцию $f(x_1, \dots, x_k) = x_1 + \dots + x_k$. Разностная характеристика xdr_k^+ для неё определяется следующим образом:

$$\text{xdr}_k^+(\alpha^1, \dots, \alpha^k \rightarrow \alpha^0) = \frac{1}{2^{nk}} \left| \left\{ x^1, \dots, x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^k (x^i \oplus \alpha^i) = \alpha^0 \oplus \bigoplus_{i=1}^k x^i \right\} \right|.$$

Подход с использованием S-функций подразумевает построение матриц на основе преобразования, через произведения которых можно подсчитать значения разностной характеристики [5]. Для характеристики xdr_k^+ далее предлагаются явные выражения для вычисления всех ненулевых элементов матриц.

Обозначим через $\text{wt}(x)$ вес Хэмминга вектора x . Определим $N(a, b) = a + 2kb$, где $0 \leq a, b < 2k$. Мы будем использовать матрицы размера $4k^2 \times 4k^2$. Заметим, что $0 \leq N(a, b) < 4k^2$. Таким образом, через $N(a, b)$ будем представлять номер строки или столбца матрицы с помощью пары чисел (a, b) .

Зададим матрицы A_m размера $4k^2 \times 4k^2$ для всех $m \in \mathbb{Z}_2^{k+1}$ следующим образом. Рассмотрим любую четвёрку целых чисел x, y, x', y' , таких, что $0 \leq x, y, x', y' < 2k$. Пусть $c = \text{wt}(m_1, \dots, m_k)$,

$$\begin{aligned} \Delta x &= x' - \left\lfloor \frac{x}{2} \right\rfloor, & a &= \left\lfloor \frac{\Delta x + \Delta y - c}{2} \right\rfloor, \\ \Delta y &= y' - \left\lfloor \frac{y}{2} \right\rfloor, & b &= \left\lfloor \frac{\Delta x - \Delta y + c}{2} \right\rfloor. \end{aligned}$$

Тогда элемент матрицы A_m в $N(x', y')$ -й строке и $N(x, y)$ -м столбце определяется следующим образом:

- 1) 0, если выполнено одно из следующих условий:
 - хотя бы одно из чисел $\Delta x, \Delta y, a$ или b меньше нуля,
 - $x_1 + y_1 + c + m_0$ — нечётное,
 - $\Delta x + \Delta y + c$ — нечётное;
- 2) $\binom{k-c}{a} \binom{c}{b}$ в противном случае.

С использованием матриц A_m , а также матриц $L = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$ размера $1 \times 4k^2$ и $C = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}^T$ размера $4k^2 \times 1$ можно вычислить значения характеристики xdr_k^+ .

Теорема 1. Пусть $\alpha^0, \alpha^1, \dots, \alpha^k \in \mathbb{Z}_2^n$. Тогда

$$\text{xdr}_k^+(\alpha^1, \dots, \alpha^k \rightarrow \alpha^0) = \frac{1}{2^{nk}} L A_{w_{n-1}} \dots A_{w_1} A_{w_0} C, \text{ где } w_j = (\alpha_j^0, \dots, \alpha_j^k) \in \mathbb{Z}_2^{k+1}.$$

Заметим, что элементы матрицы A_m зависят только от $\text{wt}(m_1, \dots, m_k)$ и m_0 .

Следствие 1. В последовательности матриц A_m , где $m \in \mathbb{Z}_2^{k+1}$, существует лишь $2(k+1)$ различных матриц.

Переобозначим эти матрицы как $A_{\text{wt}(m_1, \dots, m_k), m_0}$. Алгоритм 1 позволяет вычислять все матрицы $A_{0,0}, \dots, A_{k,0}$ и $A_{0,1}, \dots, A_{k,1}$ одновременно за $O(k^6)$ операций.

Алгоритм 1. Алгоритм одновременного вычисления всех матриц $A_{i,j}$

- 1: Для всех целых m, i, j , таких, что $0 \leq m \leq k, 0 \leq i \leq k, 0 \leq j \leq 1$:
 - 2: $B_{i,j}^m$ — матрица размера $4k^2 \times 4k^2$, изначально заполненная нулями.
 - 3: Для всех целых x, y , таких, что $0 \leq x, y < 2k$:
 - 4: $c := x_1 \oplus y_1$;
 - 5: $B_{0,c}^0[N(\lfloor x/2 \rfloor, \lfloor y/2 \rfloor)][N(x, y)] := 1$.
 - 6: Для всех m от 1 до k :
 - 7: Для всех x, y, x', y' , таких, что $0 \leq x, y, x', y' < 2k$:
 - 8: Для всех i от 0 до $m-1$, j от 0 до 1:
 - 9: $P := B_{i,j}^{m-1}[N(x', y')][N(x, y)]$;
 - 10: $B_{i,j}^m[N(x', y')][N(x, y)] += P$.
 - 11: Если $x' + 1 < 2k$ и $y' + 1 < 2k$, то
 - 12: $B_{i,j}^m[N(x' + 1, y' + 1)][N(x, y)] += P$.
 - 13: Для всех j от 0 до 1:
 - 14: $P := B_{m-1,j}^{m-1}[N(x', y')][N(x, y)]$;
 - 15: $j' := j \oplus 1$.
 - 16: Если $y' + 1 < 2k$, то
 - 17: $B_{m,j'}^m[N(x', y' + 1)][N(x, y)] += P$.
 - 18: Если $x' + 1 < 2k$, то
 - 19: $B_{m,j'}^m[N(x' + 1, y')][N(x, y)] += P$.
 - 20: Для всех i, j , таких, что $0 \leq i \leq k, 0 \leq j \leq 1$:
 - 21: $A_{i,j} := B_{i,j}^k$.
 - 22: Вернуть $A_{i,j}$ для всех i, j , таких, что $0 \leq i \leq k, 0 \leq j \leq 1$.
-

Отметим, что для разностной характеристики xdr^+ , которая является частным случаем xdr_k^+ при $k = 2$, известен более простой способ вычисления без использования матриц [7]. Однако на случай xdr_k^+ он, по всей видимости, не обобщается.

2. Максимумы $\text{adr}^\oplus(\alpha, \beta \rightarrow \gamma)$

Рассмотрим характеристику $\text{adr}^\oplus(\alpha, \beta, \gamma)$. В [8] изучены максимумы при фиксированном значении γ . В данной работе мы рассматриваем максимумы без фиксации γ , по всем возможным тройкам $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$. В результате обнаружено, что n максимальных значений данной характеристики имеют достаточно простые выражения.

Теорема 2. Пусть $p_1, \dots, p_n$ — n различных максимальных значений $\text{adr}^\oplus(\alpha, \beta, \gamma)$, где $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, $p_1 > p_2 > \dots > p_n$. Тогда

- 1) $p_1 = 1$ и $p_i = p_{i-1} - \frac{1}{2 \cdot 4^{i-2}}$ при $2 \leq i \leq n$;
- 2) $\text{adp}^\oplus(\alpha, \beta, \gamma) = p_i \iff$ тройка (α, β, γ) получается из тройки $(0, 2^{n-i}, 2^{n-i})$ композицией следующих преобразований, сохраняющих значение $\text{adp}^\oplus$ [8]:
 - а) перестановка элементов тройки;
 - б) $(\alpha, \beta, \gamma) \mapsto (\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}, \gamma)$;
 - в) $(\alpha, \beta, \gamma) \mapsto (\pm\alpha, \pm\beta, \pm\gamma)$, где $\pm\alpha$ обозначает α или $-\alpha \bmod 2^n$.

Замечание 1. Если $\text{adp}^\oplus(\alpha, \beta, \gamma) \neq p_i$ для $1 \leq i \leq n$ из теоремы 2, то

$$\text{adp}^\oplus(\alpha, \beta, \gamma) \leq 1/4.$$

Из теоремы 2 нетрудно получить количество разностей, на которых достигаются данные максимальные значения. Обозначим количество разностей (α, β, γ) , $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, на которых достигается $\text{adp}^\oplus(\alpha, \beta, \gamma) = p_i$, как C_i .

Следствие 2. Для C_i верны следующие утверждения:

- $C_1 = 4$, $C_2 = 24$;
- $C_3 = C_4 = \dots = C_n = 48$.

ЛИТЕРАТУРА

1. Shimizu A. and Miyaguchi S. Fast data encipherment algorithm FEAL // LNCS. 1988. V. 304. P. 267–278.
2. Wheeler D. J. and Needham R. M. TEA, a tiny encryption algorithm // LNCS. 1995. V. 1008. P. 363–366.
3. Bernstein D. J. Salsa20 specification. eSTREAM Project algorithm description. <http://www.ecrypt.eu.org/stream/salsa20pf.html>. 2005.
4. Beaulieu R., Shors D., Smith J., et al. The SIMON and SPECK Families of Lightweight Block Ciphers. <https://eprint.iacr.org/2013/404>.
5. Biham E. and Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
6. Mouha N., Velichkov V., De Cannière C., and Preneel B. The differential analysis of S-functions // LNCS. 2011. V. 6544. P. 36–56.
7. Lipmaa H. and Moriai S. Efficient algorithms for computing differential properties of addition // LNCS. 2002. V. 2355. P. 336–350.
8. Mouha N., Kolomeec N., Akhtiamov D., et al. Maximums of the additive differential probability of Exclusive-Or // IACR Trans. Symmetric Cryptology. 2021. No. 2. P. 292–313.

УДК 519.7

DOI 10.17223/2226308X/15/15

НЕКОТОРЫЕ УСЛОВИЯ ПРИМЕНИМОСТИ ИНТЕГРАЛЬНОГО МЕТОДА К ЧЕТЫРЁМ РАУНДАМ AES-ПОДОБНЫХ АЛГОРИТМОВ

К. Н. Панков

Получен ряд необходимых и одно достаточное условие того, что к блочным алгоритмам, построенным аналогично алгоритму AES (например, SQUARE, Rijndael, Crypton) с уменьшенным до четырёх числом раундов может быть применён интегральный метод криптоанализа. Приведены данные экспериментов о применении интегрального метода к алгоритму Rijndael.

Ключевые слова: блочные алгоритмы, AES, SQUARE, Rijndael, Crypton, спектральные коэффициенты, интегральный метод.