УДК 519.7 DOI 10.17223/2226308X/15/17

О РАЗНОСТНЫХ ХАРАКТЕРИСТИКАХ КОМПОЗИЦИЙ ПОБИТОВЫХ XOR ПО МОДУЛЮ 2^n [1]

И. А. Сутормин

Рассматривается разностная характеристика $\mathrm{adp}_k^{\oplus}$ композиции побитовых XOR относительно сложения по модулю 2^n. Эта величина используется при анализе примитивов, имеющих конструкцию Addition-Rotation-XOR (ARX). Получены рекуррентные формулы, позволяющие найти значение $\mathrm{adp}_k^{\oplus}$ от аргументов размерности $n+1$ при помощи набора значений $\mathrm{adp}_k^{\oplus}$ от аргументов размерности n. Изучены симметрии и нули характеристики. В случае чётного k найден максимум $\mathrm{adp}_k^{\oplus}$ при одном фиксированном аргументе.

Ключевые слова: *разностный криптоанализ, ARX, XOR, сложение по модулю.*

Существуют различные подходы для разработки алгоритмов симметричной криптографии. Один из них — ARX. Во всех примитивах этой архитектуры используются только три операции: сложение по модулю 2^n ($\boxplus$), циклический сдвиг битов и побитовое сложение по модулю 2 ($\oplus$, XOR). ARX-шифры могут быть различных назначений, например блочные шифры FEAL [1], Threefish [2], поточные шифры Salsa20 [3] и его модификация ChaCha [4], хэш-функции BLAKE [5] и Skein [2]. Разностный криптоанализ — один из современных методов криптоанализа, предложенный в [6]. Для проведения разностного криптоанализа ARX-шифров при выборе в качестве разности сложения по модулю 2^n необходима разностная характеристика $\mathrm{adp}^{\oplus}$:

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \frac{1}{4^n}\big|\{x, y \in \mathbb{Z}_2^n : (x \boxplus \alpha) \oplus (y \boxplus \beta) = (x \oplus y) \boxplus \gamma\}\big|.$$

Здесь и далее с вектором $x \in \mathbb{Z}_2^n$ ассоциируется целое число $x_n + x_{n-1}2^1 + \ldots + x_1 2^{n-1}$.

Многие свойства $\mathrm{adp}^{\oplus}$ изучены в работах [7, 8]. Однако в некоторых ARX-шифрах присутствует применение композиции побитовых XOR. Так, например, в хэш-функции EDON-R [9] используется XOR трёх векторов. В этом случае использование характеристики $\mathrm{adp}^{\oplus}$ может привести к неверным оценкам. Более точные оценки можно получить при прямом использовании аналогичной характеристики для XOR нескольких векторов, которая определяется как

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \frac{1}{2^{kn}}\Big|\{x^1, \ldots, x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k}(x^i \boxplus \alpha^i) = \alpha^{k+1} \boxplus \bigoplus_{i=1}^{k} x^i\}\Big|.$$

Здесь и далее $k \geqslant 2$.

Многие свойства $\mathrm{adp}_k^{\oplus}$ и $\mathrm{adp}^{\oplus}$ схожи. Так, в частности, симметрии аргументов $\mathrm{adp}_k^{\oplus}$ аналогичны симметриям $\mathrm{adp}^{\oplus}$, описанным в [8, разд. 4]. Однако случай замены аргументов на обратные относительно сложения по модулю 2^n в случае нечётного k отличается от чётного k. В нечётном случае на обратный можно заменить только пару элементов одновременно.

Теорема 1. Для любого набора аргументов характеристика $\mathrm{adp}_k^{\oplus}$ обладает следующими свойствами:

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2022-281.

1) $\mathrm{adp}_k^{\oplus}$ — симметрическая функция, то есть её значение не изменится при перестановке аргументов. Например, для любых $\alpha^1, \ldots, \alpha^4 \in \mathbb{Z}_2^n$ справедливо

$$\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \to \alpha^4) = \mathrm{adp}_3^{\oplus}(\alpha^2, \alpha^1, \alpha^3 \to \alpha^4).$$

2) Значение $\mathrm{adp}_k^{\oplus}$ не изменится, если к любым двум аргументам прибавить 2^{n-1} по модулю 2^n. Например, для любых $\alpha^1, \ldots, \alpha^4 \in \mathbb{Z}_2^n$ справедливо

$$\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \to \alpha^4) = \mathrm{adp}_3^{\oplus}(\alpha^1 \boxplus 2^{n-1}, \alpha^2 \boxplus 2^{n-1}, \alpha^3 \to \alpha^4).$$

3) Значение $\mathrm{adp}_k^{\oplus}$ не изменится, если два аргумента одновременно заменить на обратные относительно сложения по модулю 2^n. Например, для любых $\alpha^1, \ldots, \alpha^4 \in \mathbb{Z}_2^n$ справедливо

$$\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3, \to \alpha^4) = \mathrm{adp}_3^{\oplus}(-\alpha^1, -\alpha^2, \alpha^3, \to \alpha^4).$$

4) При чётном k значение $\mathrm{adp}_k^{\oplus}$ не изменится, если любой из аргументов заменить на обратный относительно сложения по модулю 2^n. Например, для любых $\alpha^1, \ldots, \alpha^5 \in \mathbb{Z}_2^n$ справедливо

$$\mathrm{adp}_4^{\oplus}(\alpha^1, \alpha^2, \alpha^3, \alpha^4 \to \alpha^5) = \mathrm{adp}_4^{\oplus}(-\alpha^1, \alpha^2, \alpha^3, \alpha^4 \to \alpha^5).$$

Для вектора $\alpha \in \mathbb{Z}_2^n$ обозначим через $\alpha||1$ и $\alpha||0$ векторы $(\alpha_1, \ldots \alpha_n, 1)$ и $(\alpha_1, \ldots \alpha_n, 0)$ из $\mathbb{Z}_2^{n+1}$ соответственно; вес Хэмминга $\mathrm{wt}(\alpha) = \sum\limits_{i=1}^{n} \alpha_i$. Запись $b \preceq a$ обозначает, что для векторов $a, b \in \mathbb{Z}_2^{k+1}$ выполнено $b_i \leqslant a_i$, $i = 1, \ldots, k+1$. Тогда для $\mathrm{adp}_k^{\oplus}$ можно доказать рекуррентные формулы, аналогичные [8, теорема 3] и позволяющие получить значение $\mathrm{adp}_k^{\oplus}$ от аргументов размерности $n+1$ при помощи набора значений $\mathrm{adp}_k^{\oplus}$ от аргументов размерности n.

Теорема 2. Для любого набора векторов $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ и вектора $a \in \mathbb{Z}_2^{k+1}$, составленного из младших бит аргументов, выполняются следующие равенства:

1) если $\mathrm{wt}(a)$ нечётный, то $\mathrm{adp}_k^{\oplus}(\alpha^1||a_1, \ldots \alpha^k||a_k \to \alpha^{k+1}||a_{k+1}) = 0$;
2) если k нечётное и $a = (1, \ldots, 1)$, то

$$\mathrm{adp}_k^{\oplus}(\alpha^1||1, \ldots \alpha^k||1 \to \alpha^{k+1}||1) =$$
$$= \frac{1}{2^k} \sum_{\substack{b \preceq a, \\ \mathrm{wt}(b) - \text{четн.}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus b_1, \ldots, \alpha^k \boxplus b_k \to \alpha^{k+1} \boxplus b_{k+1});$$

3) во всех остальных случаях

$$\mathrm{adp}_k^{\oplus}(\alpha^1||a_1, \ldots \alpha^k||a_k \to \alpha^{k+1}||a_{k+1}) =$$
$$= \frac{1}{2^{\mathrm{wt}(a)}} \sum_{b \preceq a} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus b_1, \ldots, \alpha^k \boxplus b_k \to \alpha^{k+1} \boxplus b_{k+1}).$$

Так, например, для любых $\alpha^1, \ldots, \alpha^4 \in \mathbb{Z}_2^n$, согласно п. 1, справедливо

$$\mathrm{adp}_3^{\oplus}(\alpha^1||0, \alpha^2||0, \alpha^3||1 \to \alpha^4||0) = 0.$$

Согласно п. 3, справедливо

$$\mathrm{adp}_3^{\oplus}(\alpha^1||0, \alpha^2||0, \alpha^3||1 \to \alpha^4||1) = \frac{1}{4}\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \to \alpha^4) + \frac{1}{4}\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \boxplus 1 \to \alpha^4 \boxplus 1) +$$
$$+ \frac{1}{4}\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \boxplus 1 \to \alpha^4) + \frac{1}{4}\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \to \alpha^4 \boxplus 1).$$

Заметим, что ранее известные формулы для $\mathrm{adp}^{\oplus}$ описываются пп. 1 и 3.

Для вектора $\alpha \in \mathbb{Z}_2^n$ обозначим через $\overline{\alpha}$ вектор $(\alpha_1 \oplus 1, \ldots, \alpha_n \oplus 1)$. Тогда симметрии из теоремы 1 позволяют в некоторых случаях записать рекуррентные формулы при помощи операции инверсии, анализировать которую проще, чем сложение по модулю. Например,

$$\mathrm{adp}_3^{\oplus}(\alpha||1, \alpha||1, \alpha||1 \to \alpha||1) = \frac{3}{4}\mathrm{adp}_3^{\oplus}(\overline{\alpha}, \overline{\alpha}, \alpha \to \alpha) + \frac{1}{8}\mathrm{adp}_3^{\oplus}(\overline{\alpha}, \overline{\alpha}, \overline{\alpha} \to \overline{\alpha}) + \\ + \frac{1}{8}\mathrm{adp}_3^{\oplus}(\alpha, \alpha, \alpha \to \alpha).$$

Рекуррентные формулы позволяют также найти максимум $\mathrm{adp}_k^{\oplus}$ при чётном k, аналогичный максимуму при $k = 2$, доказанному в [8, теорема 2].

Теорема 3. Для любого $\gamma \in \mathbb{Z}_2^n$ и любого чётного k выполняется

$$\max_{\alpha^1, \ldots, \alpha^k \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \gamma) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma).$$

Однако при нечётном k данное утверждение неверно и аналогичный максимум $\mathrm{adp}_k^{\oplus}$ выглядит иначе. Мы предполагаем, что он выглядит так:

Гипотеза 1. Для любого $\gamma \in \mathbb{Z}_2^n$ и любого нечётного k выполняется

$$\max_{\alpha^1, \ldots, \alpha^k \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \gamma) = \mathrm{adp}_k^{\oplus}(\gamma, \ldots, \gamma \to \gamma).$$

Гипотеза подтверждается вычислительными экспериментами и разбором некоторых частных случаев. В случае $k = 3$ для этого полезны следующие неравенства:

Теорема 4. Для любого $\gamma \in \mathbb{Z}_2^n$ выполняется

$$\mathrm{adp}_3^{\oplus}(\gamma, \gamma, \overline{\gamma} \to \overline{\gamma}) \leqslant \mathrm{adp}_3^{\oplus}(\gamma, \gamma, \gamma \to \gamma) \leqslant 3\,\mathrm{adp}_3^{\oplus}(\gamma, \gamma, \overline{\gamma} \to \overline{\gamma}).$$

Отметим, что для разностного криптоанализа важно различать наборы аргументов, на которых $\mathrm{adp}_k^{\oplus}$ равно нулю.

Теорема 5. При любом k и любом наборе аргументов $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ значение $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 0$ тогда и только тогда, когда существует позиция i, такая, что вектор $(\alpha_i^1, \ldots, \alpha_i^{k+1}) \neq (0, \ldots, 0)$, а для любой позиции j, $n \geqslant j > i$ верно $(\alpha_j^1, \ldots, \alpha_j^{k+1}) = (0, \ldots, 0)$, и выполняется одно из следующих условий:

1) вектор $(\alpha_i^1, \ldots, \alpha_i^{k+1})$ имеет нечётный вес;
2) k нечётное, $i > 1$, вектор $(\alpha_i^1, \ldots, \alpha_i^{k+1})$ равен $(1, \ldots, 1)$ и вектор битов на разряд выше $(\alpha_{i-1}^1, \ldots, \alpha_{i-1}^{k+1})$ имеет нечётный вес.

Заметим, что нули функции в случае чётного k выглядят аналогично нулям для $\mathrm{adp}^{\oplus}$. Случай 2 появляется только при нечётном k и порождает дополнительное множество нулей характеристики.

ЛИТЕРАТУРА

1. *Shimizu A. and Miyaguchi S.* Fast data encipherment algorithm FEAL // LNCS. 1988. V. 304. P. 267–278.
2. *Ferguson N., Lucks S., Schneier B., et al.* The Skein Hash Function Family. `http://www.skein-hash.info`. 2009.
3. *Bernstein D. J.* Salsa20 Specification. `https://cr.yp.to/snuffle/spec.pdf`. 2005.

4. *Bernstein D. J.* ChaCha, a Variant of Salsa20. `https://cr.yp.to/chacha/chacha-20080128.pdf`. 2008.
5. *Aumasson J.-P., Meier W., Phan R. C.-W., and Henzen L.* The Hash Function BLAKE. `https://www.researchgate.net/publication/316806226_The_Hash_Function_BLAKE`. 2014.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
7. *Lipmaa H., Wallen J., and Dumas P.* On the additive differential probability of exclusive-or // LNCS. 2004. V. 3017. P. 317–331.
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.
9. *Gligoroski D., Odegard R. S., Mihova M., et al.* Cryptographic hash function Edon-R // Proc. IWSCN. 2009. P. 1–9.

UDC 519.17 DOI 10.17223/2226308X/15/18

KEY SCHEDULE BASED ON A MODIFIED ADDITIVE GENERATOR[1]

V. M. Fomichev, D. A. Bobrovskiy, R. R. Sotov

A method of round key generation for iterated block ciphers based on a modified additive generator (MAG), and, in addition, on MAG and a linear congruent generator in a series circuit is proposed. The bijectivity of the generating transformation is demonstrated. Using the matrix-graph approach the number of iterations necessary for achieving enhanced cryptographic properties is experimentally evaluated. This number depends on the generator characteristics.

Keywords: *key scheduling algorithm, iterative block ciphers, matrix-graph approach, modified additive generator, mixing properties, nonlinearity.*

1. Introduction

The key schedule is an important component of any iterated block cipher. The first versions of key schedules (DES, GOST 28147-89) involved bit sampling from the cipher key which gives the cryptanalyst grounds for attacks such as differential analysis. In AES, the generation of round keys is more complex and requires a non-stationary recurrence relation over a set of binary vectors. The Kuznechik algorithm provides a complex key dependency using the Feistel network. The goal of key schedule algorithms is to combine a complex functional relationship between the bits of the cipher key and the round keys with a relatively low computational complexity of key generation.

This paper proposes a round key generator (RKG) based on a modified additive generator and, in addition, on MAG and a linear congruent generator (LCG) in a series circuit.

2. Additive generator

The additive generator (AG) is a shift register of length n with feedback $f(z_0, \ldots, z_{n-1})$ over the space of binary r-dimensional vectors, i.e., a register transformation φ of the set $V_{nr} = \{(z_0, \ldots, z_{n-1}) : z_0, \ldots, z_{n-1} \in V_r\}$:

$$\varphi(z_0, \ldots, z_{n-1}) = (z_1, \ldots, z_{n-1}, f(z_0, \ldots, z_{n-1})), \tag{1}$$

where the function $f\colon V_{nr} \to V_r$ is the shift register feedback function.