УДК 519.7 DOI 10.17223/2226308X/14/7

О СВОЙСТВАХ РАЗНОСТНЫХ ХАРАКТЕРИСТИК XOR ПО МОДУЛЮ 2^n [1]

Н. Муха, Н. А. Коломеец, Д. А. Ахтямов, И. А. Сутормин, М. А. Панферов, К. М. Титова, Т. А. Бонич, Е. А. Ищукова, Н. Н. Токарева, Б. Ф. Жантуликов

Рассматривается вероятность $\mathrm{adp}^{\oplus}(\alpha,\beta,\gamma)$ преобразования разностей в функции XOR по модулю 2^n, где $\alpha,\beta,\gamma \in \mathbb{Z}_2^n$. Эта величина используется при анализе примитивов с симметричным ключом, сочетающих XOR и сложение по модулю, например ARX-конструкций. Основное внимание уделяется характеристикам с максимальной вероятностью при одном фиксированном аргументе. Установлено, что $\max\limits_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha,\beta,\gamma) = \mathrm{adp}^{\oplus}(0,\gamma,\gamma)$, и доказано, что существуют либо две, либо восемь различных пар (α,β), для которых достигается вероятность $\mathrm{adp}^{\oplus}(0,\gamma,\gamma)$. Получены упрощенное представление величины $\mathrm{adp}^{\oplus}(0,\gamma,\gamma)$ и формула для $\min\limits_{\gamma} \mathrm{adp}^{\oplus}(0,\gamma,\gamma)$.

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

ARX — одна из современных архитектур в симметричной криптографии. В компонентах таких шифров используются только три операции: сложение по модулю 2^n, циклический сдвиг и покомпонентное сложение по модулю 2 (XOR). Архитектуру ARX имеют блочные шифры FEAL [1], Threefish [2], один из победителей eSTREAM поточный шифр Salsa20 [3] и его модификация ChaCha [4], входящая в TLS, а также финалисты SHA-3 хэш-функции BLAKE [5] и Skein [2]. Разностный криптоанализ [6] основан на изучении преобразования разностей открытых текстов в разности шифртекстов, сложность такого изучения является недостатком ARX-шифров. Выбирая в качестве разности разность по модулю 2^n, вероятности разностных характеристик операции XOR определяются функцией $\mathrm{adp}^{\oplus}$:

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

С вектором $x \in \mathbb{Z}_2^n$ мы ассоциируем целое число $x_0 + x_1 2^1 + \ldots + x_{n-1}2^{n-1}$, $x+\alpha$ означает сложение по модулю 2^n ассоциированных с x и α чисел, $-x$ является обратным к ассоциированному с x числу относительно сложения по модулю 2^n. Известно [7], что $\mathrm{adp}^{\oplus}(\alpha,\beta\to\gamma)$ при $\alpha,\beta,\gamma\in\mathbb{Z}_2^n$ представимо в виде произведения матриц размера 8×8, что позволяет эффективно вычислять $\mathrm{adp}^{\oplus}$ за линейное по n время.

Отметим, что данная работа началась в рамках Первого воркшопа Математического центра в Академгородке (см. `http://mca.nsu.ru/workshop/`).

Приведём преобразования аргументов, не меняющие значение $\mathrm{adp}^{\oplus}$.

Утверждение 1. Пусть $\alpha,\beta,\gamma\in\mathbb{Z}_2^n$. Тогда справедливо следующее:

1) $\mathrm{adp}^{\oplus}$ является симметрической, т. е. не меняет значение при перестановке α,β,γ;
2) значение $\mathrm{adp}^{\oplus}$ не изменится, если к любым двум аргументам прибавить 2^{n-1} по модулю 2^n: $\mathrm{adp}^{\oplus}(\alpha,\beta\to\gamma) = \mathrm{adp}^{\oplus}(\alpha+2^{n-1},\beta+2^{n-1}\to\gamma)$;

[1] Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2019-1613, и лаборатории криптографии JetBrains Research.

3) $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \beta \to -\gamma)$; в силу п. 1 можно поставить «$-$» перед любым аргументом.

В [7, теорема 3] сформулирована теорема о максимальном значении $\mathrm{adp}^{\oplus}(\alpha, \beta{\to}\gamma)$ при фиксированном γ. Однако доказательство не было приведено («The proof is omitted from the conference version») и впоследствии нигде не было опубликовано. Мы доказали, что это утверждение действительно является верным.

Теорема 1. Для любого $\gamma \in \mathbb{Z}_2^n$ выполняется

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

Метод доказательства позволяет также найти количество пар (α, β), на которых достигается значение $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$.

Следствие 1. Количество пар $(\alpha, \beta) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$, таких, что $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, где $\gamma \in \mathbb{Z}_2^n$, равно:

1) 2, если $\gamma = 0$ или $\gamma = 2^{n-1}$, а именно это пары

$$(0,0),(2^{n-1},2^{n-1}) \text{ при } \gamma = 0 \quad \text{и} \quad (0,2^{n-1}),(2^{n-1},0) \text{ при } \gamma = 2^{n-1};$$

2) 8 для всех других γ, а именно это пары

$$(0,\gamma),\ (\gamma,0),\ (2^{n-1},-\gamma+2^{n-1}),\ (-\gamma+2^{n-1},2^{n-1}),$$
$$(0,-\gamma),\ (-\gamma,0),\ (2^{n-1},\ \gamma+2^{n-1}),\ (\gamma+2^{n-1},2^{n-1}).$$

Заметим, что все приведённые пары являются симметриями, описанными в утверждении 1. Кроме того, если γ равна 0 или 2^{n-1}, то $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = 1$.

Используя S-функции [8], величину $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ можно представить в виде произведения матриц размера 3×3. Однако если исключить старший бит, достаточно матриц размера 2×2.

Теорема 2. Для любого $\gamma \in \mathbb{Z}_2^n$ выполнено

$$\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = (1,1)B_{\gamma_{n-2}}B_{\gamma_{n-3}}\dots B_{\gamma_0}(1,0)^{\mathrm{T}},$$

где $B_0 = \frac{1}{4}\begin{pmatrix}4 & 1\\ 0 & 1\end{pmatrix}$; $B_1 = \frac{1}{4}\begin{pmatrix}1 & 0\\ 1 & 4\end{pmatrix}$.

Более прозрачную формулу для $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ получить не удалось. Косвенным подтверждением сложности этой задачи является непростое выражение для минимального из значений $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ при фиксированном n.

Теорема 3. Пусть $m_n = \min\limits_{\gamma\in\mathbb{Z}_2^n} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. Тогда для любого n выполнено

$$m_{n+2} = \frac{1}{4}m_{n+1} + \frac{1}{4}m_n.$$

Следствие 2. Числа m_n, $n = 1, 2, \dots$, образуют последовательность Хорадама [9] и для них верно

$$m_n = \frac{1}{34 \cdot 8^n}\left((17+\sqrt{17})(1+\sqrt{17})^n + (17-7\sqrt{17})(1-\sqrt{17})^n\right).$$

Тем не менее сумму всех элементов $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ вычислить несложно.

Утверждение 2. Для любого n выполнено

$$\sum_{\gamma\in\mathbb{Z}_2^n} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = 2\,(3/2)^{n-1}.$$

Подробно с результатами работы можно ознакомиться в [10].

ЛИТЕРАТУРА

1. *Shimizu A. and Miyaguchi S.* Fast data encipherment algorithm (FEAL) // 1988. 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. V. 4. No. 1. 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., Velichkov V., De Canniere C., and Preneel B.* The differential analysis of S-functions // LNCS. 2011. V. 6544. P. 36–56.
9. *Horadam A. F.* Basic properties of a certain generalised sequence of numbers // The Fibonacci Quarterly. 1965. V. 3. No. 3. P. 161–176.
10. *Mouha N., Kolomeec N., Akhtiamov D., et al.* Maximums of the additive differential probability of Exclusive-Or // IACR Trans. Symmetric Cryptology. 2021. V. 2021. No. 2. P. 292–313.

УДК 519.7 DOI 10.17223/2226308X/14/8

УЛУЧШЕННЫЕ ОЦЕНКИ ДЛЯ ЧИСЛА k-ЭЛАСТИЧНЫХ И КОРРЕЛЯЦИОННО-ИММУННЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Получены улучшенные нижние и верхние оценки для числа корреляционно-иммунных порядка k и k-эластичных ((n, m, k)-устойчивых) двоичных отображений.

Ключевые слова: *распределённый реестр, блокчейн, информационная безопасность, устойчивые вектор-функции, эластичные вектор-функции, корреляционно-иммунные функции.*

В настоящее время использование систем распределённого реестра, основанных на технологии цепной записи данных (блокчейн) [1], становится всё более распространённым в самых различных отраслях современной цифровой экономики [2]. Пандемия COVID-19, продолжавшаяся весь 2020 год и не оконченная до сих пор, дала, согласно мнению ряда экспертов [3], дополнительный импульс развитию дистанционных доверенных сервисов, основой функционирования которых являются системы распределённых реестров, признанные в Российской Федерации, согласно [4], средством криптографической защиты информации. Как уже отмечалось в [5], в связи с расширением применения технологии блокчейн жизненно важным становится исследование информационной безопасности систем распределённого реестра, на этой технологии основанных. Одним из способов обеспечения безопасности данных в подобных системах является использование шифрования, например поточного, в связи с чем возникает задача оценки числа корреляционно-иммунных и (n, m, k)-устойчи-