

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-

вых двоичных отображений, которые могут быть использованы в системах поточного шифрования в качестве комбинирующих отображений.

Понятия корреляционной иммунности и (n, m, k) -устойчивости будем понимать в соответствии с [6], где подробно рассмотрены их свойства. Задаче оценки числа отображений и булевых функций, обладающих соответствующими свойствами, посвящён целый ряд работ, среди которых можно отметить [7–10]. Ряд результатов был доложен автором на конференциях SIBECRYPT [11–13].

Обозначим через V_n множество двоичных векторов размерности n . Корреляционная иммунность и k -эластичность (или (n, m, k) -устойчивость) двоичного отображения $f(\alpha) = (f_1(\alpha), f_2(\alpha), \dots, f_m(\alpha)) : V_n \rightarrow V_m$, согласно [6], сводится к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций (компонентами [14]). В [15, 16] получены асимптотические оценки числа корреляционно-иммунных и (n, m, k) -устойчивых двоичных отображений с точностью до оценок мощности множества специального вида $\mathfrak{R}^{**}(m, N)$:

$$\mathfrak{R}^{**}(m, N) = \left\{ \vec{r} = (r_I^J, \emptyset \neq J \subset \{1, \dots, m\}, I \subset \{1, \dots, n\}, |I| \leq k) \in (\mathbb{Z}_{2^{m-1}})^N : \right. \\ \left. \forall I \forall s \in \{1, \dots, m\} \forall \delta \in V_m \left(\sum_{\substack{J \subset \{1, \dots, m\}, \\ s \in J}} (-1)^{(\delta, \psi_m(J))} r_I^J = 0 \right) \right\},$$

где $\mathbb{Z}_{2^{m-1}}$ — кольцо вычетов по модулю 2^{m-1} ; $\psi_m(J)$ — индикаторный вектор множества $J \subset \{1, \dots, m\}$ [17].

Если использовать обозначение [8]

$$M(n, k) = \sum_{s=0}^k \binom{n}{s},$$

то легко показать, что

$$\mathfrak{R}^{**}(m, N) = (\mathfrak{R}(m))^{M(n, k)},$$

где

$$\mathfrak{R}(m) = \left\{ \vec{r} = (r_J, \emptyset \neq J \subset \{1, \dots, m\}) \in (\mathbb{Z}_{2^{m-1}})^{2^m-1} : \right. \\ \left. \forall s \in \{1, \dots, m\} \forall \delta \in V_m \sum_{\substack{J \subset \{1, \dots, m\}, \\ s \in J}} (-1)^{(\delta, \psi_m(J))} r_J = 0 \right\}.$$

В [15] найдены точные значения мощности множества $\mathfrak{R}(m)$ при $m \in \{1, 2, 3, 4\}$ и верхние и нижние оценки при $m \geq 5$:

$$m - 1 \leq \log_2 |\mathfrak{R}(m)| \leq (m - 2) 2^m - m + 3.$$

Последний результат удалось улучшить:

Теорема 1. Во введённых обозначениях при $m \geq 5$ выполняется

$$\frac{m^2 - m - 12}{2} + 17 \leq \log_2 |\mathfrak{R}(m)| \leq \left(m - 2 \frac{15}{16} \right) 2^m - m + 3.$$

Обозначим через $R(n, m, k)$ множество всех (n, m, k) -устойчивых (k -эластичных) двоичных отображений из B_n^m всех m -мерных двоичных функций от n переменных,

а через $K(n, m, k)$ — множество всех корреляционно-иммунных порядка k двоичных отображений из B_n^m .

Для упрощения записи удобно ввести следующее обозначение:

$$T(n, m, k) = (2^m - 1) \left(\frac{n - k}{2} \binom{n}{k} + M(n, k) \log_2 \sqrt{\frac{\pi}{2}} \right).$$

Используя теорему 1, легко доказать

Следствие 1. Пусть при всех достаточно больших n для произвольного $0 < \gamma < 1/3$ выполняется неравенство $k(5 + 2\log_2 n) + 6m \leq n(1/3 - \gamma)$. Тогда существует n_0 , такое, что для любых $\varepsilon_1, \varepsilon_2 > 0$, $n > n_0$ верны неравенства

$$\begin{aligned} \left(\frac{m^2 - m - 12}{2} + 17 \right) M(n, k) - \varepsilon_1 &\leq \log_2 |R[n, m, k]| - m2^n + T(n, m, k) \leq \\ &\leq ((16m - 47)2^{m-4} - m + 3) M(n, k) + \varepsilon_2. \end{aligned}$$

Следствие 2. Пусть при всех достаточно больших n для произвольного $0 < \gamma < 5/18$ выполняется неравенство $k(5 + 2\log_2 n) + 6m \leq n(5/18 - \gamma)$. Тогда существует n_0 , такое, что для любых $\varepsilon_1, \varepsilon_2 > 0$, $n > n_0$ верны неравенства

$$\begin{aligned} \left(\frac{m^2 - m - 12}{2} + 17 \right) M(n, k) - \varepsilon_1 &\leq \\ \leq \log_2 |K(n, m, k)| - m2^n - \left(\frac{n + 1 + \log_2 \pi}{2} - k \right) (2^m - 1) + m2^{m-1} + T(n, m, k) &\leq \\ \leq ((16m - 47)2^{m-4} - m + 3) M(n, k) + \varepsilon_2 \end{aligned}$$

Полученные в следствиях 1 и 2 результаты улучшают оценки, полученные ранее в работах [11, 12, 16, 18].

ЛИТЕРАТУРА

1. МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров» М.: Технический комитет по стандартизации «Криптографическая защита информации», 2018. 10 с.
2. Блокчейн-революция в банках и финансовых институтах. Отчет. М.: MINDSMITH, 2020. <https://mindsmith.io/blockchain-finance/>
3. Колонка MINDSMITH: Блокчейн в зените лета. 6 августа 2020 года. <https://ict.moscow/news/blockchain-trends-mindsmith/>
4. Елистратов А., Маршалко Г. Б., Светушкин В. Подводные камни сертификации блокчейн-решений // Открытые системы. СУБД. 2019. № 1. С. 19.
5. Pankov K. Enumeration of Boolean mapping with given cryptographic properties for personal data protection in Blockchain Data Storage // Proc. 24th Conf. Open Innovations Assoc. FRUCT, Moscow, Russia, 2019. P. 300–306.
6. Логачев О. А., Сальников А. А., Смышляев С. В., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
7. Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций // Дискретная математика. 1991. № 2. С. 25–46.
8. Денисов О. В. Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
9. Canfield E. R., Gao Z., Greenhill C., et al. Asymptotic enumeration of correlation-immune Boolean functions // Cryptogr. Commun. 2010. No. 1. P. 111–126.

10. Potapov V. N. A lower bound on the number of boolean functions with median correlation immunity // 16th Int. Symp. "Problems of redundancy in information and control systems", Moscow, Russia, 2019. P. 45–46.
11. Панков К. Н. Уточнённые асимптотические оценки для числа (n, m, k) -устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
12. Панков К. Н. Уточнённые асимптотические оценки для числа корреляционно-иммунных двоичных функций и отображений // Прикладная дискретная математика. Приложение. 2018. № 11. С. 49–52.
13. Панков К. Н. Рекуррентные формулы для числа k -эластичных и корреляционно-иммунных двоичных отображений // Прикладная дискретная математика. Приложение. 2019. № 12. С. 62–66.
14. Carlet C. Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398–472.
15. Панков К. Н. Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
16. Pankov K. N. Improved asymptotic estimates for the numbers of correlation-immune and k -resilient vectorial Boolean functions // Discr. Math. Appl. 2019. No. 3. P. 195–213.
17. Сачков В. Н. Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013. 336 с.
18. Панков К. Н. Улучшенные асимптотические оценки для числа корреляционно-иммунных и k -эластичных двоичных вектор-функций // Дискретная математика. 2018. № 2. С. 73–98.

УДК 519.719.2

DOI 10.17223/2226308X/14/9

О СПОСОБЕ ПОСТРОЕНИЯ ДИФФЕРЕНЦИАЛЬНО 2 δ -РАВНОМЕРНЫХ ПОДСТАНОВОК НА $\mathbb{F}_{2^{2m}}$

Д. Б. Фомин

Рассмотрены способы построения дифференциально 2 δ -равномерных подстановок на $\mathbb{F}_{2^{2m}}$ для случая $m \geq 3$. Предложенный подход излагается с использованием так называемого TU -представления функций и обобщает известный способ построения дифференциально 4-равномерных подстановок поля $\mathbb{F}_{2^{2m}}$ с применением подстановки обращения ненулевых элементов поля.

Ключевые слова: S -Box, подстановка, дифференциальная равномерность, TU -представление.

Исследование способов построения нелинейных биективных преобразований с заданными криптографическими характеристиками является актуальной и сложной задачей. Одним из известных подходов, позволяющих строить нелинейные преобразования с достаточно высокими криптографическими характеристиками и допускающие эффективную программную и аппаратную реализацию, является использование подстановок, имеющих декомпозицию.

Пусть $\mathbb{F}_2 = \{0, 1\}$ — поле из двух элементов с операциями сложения «+» и умножения « $\cdot$ »; $(\mathbb{F}_2^n, +) = \{(a_0, a_1, \dots, a_{n-1}) : a_i \in \mathbb{F}_2, i = 0, \dots, n-1\}$ — арифметическое векторное пространство размерности n . Задав специальным образом операцию умножения на множестве $\mathbb{F}_2^n$, можно определить поле $\mathbb{F}_{2^n}$, состоящее из 2^n элементов. Везде