Нормированной DDT-таблицей функции F будем называть таблицу, в ячейке (a, b) которой записано количество решений уравнения

$$F(x) \oplus F(x \oplus a) \oplus F(a) \oplus F(\mathbf{0}) = b.$$

Нормированной LAT-таблицей функции F будем называть LAT-таблицу функции F без линейной части.

Теорема 3. Если функции F и G EA-эквивалентны и в нормированной DDT (LAT)-таблице функции F есть совпадающие строки, то в нормированной DDT (LAT)-таблице функции G также есть совпадающие строки.

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. Iss. 1. P. 3–72.
2. *Matsui M. and Yamagishi A.* A new method for known plaintext attack of FEAL cipher // EUROCRYPT'1992. LNCS. 1992. V. 658. P. 81–91.
3. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / eds. Y. Crama and P. Hammer. Cambridge: Cambridge University Press, 2010. P. 398–470.

УДК 519.7

DOI 10.17223/2226308X/12/19

РЕКУРРЕНТНЫЕ ФОРМУЛЫ ДЛЯ ЧИСЛА k -ЭЛАСТИЧНЫХ И КОРРЕЛЯЦИОННО-ИММУННЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Получены рекуррентные формулы для распределения части вектора весов подфункций w_I^J и части вектора спектральных коэффициентов Δ_I^J линейных комбинаций координатных функций двоичного отображения из векторного пространства V_n двоичных n -мерных векторов в векторное пространство V_m . С помощью этих формул получены рекуррентные формулы для числа корреляционно-иммунных порядка k двоичных отображений и для числа k -эластичных двоичных отображений.

Ключевые слова: веса подфункций, спектральные коэффициенты, рекуррентные формулы, устойчивые вектор-функции, эластичные вектор-функции, корреляционно-иммунные функции.

Системы распределённого реестра, основанные на блокчейн-технологии, являются одной из сквозных цифровых технологий программы «Цифровая экономика Российской Федерации». В последние годы различные аспекты данной технологии стали предметом пристального изучения исследователей и разработчиков программного обеспечения. Одной из многообещающих возможностей её применения являются системы хранения важных данных, включая персональные. Однако применение норм российского и европейского законодательства, занимающегося правовым регулированием персональных данных, приводит на практике к противоречию с самой концепцией блокчейн-систем, которые предполагают неизменность данных. В информационных системах (ИС) с реестром с ограничениями на добавление информации (согласно терминологии [1]), к примеру, задача удаления персональных данных может решаться изменением всей цепочки данных («forking»), в открытых же ИС с реестром наиболее

многообещающим способом решения этой задачи может служить шифрование каждого блока персональной информации на своём ключе и удаление ключа, который хранится за пределами цепочки данных, при поступлении запроса на удаление [2]. В работе [3] этот метод разобран достаточно подробно и связан с задачей оценки числа (n, m, k) -устойчивых и корреляционно-иммунных двоичных отображений, используемых в качестве комбинирующих в поточных системах шифрования.

Обозначим через V_n множество двоичных векторов размерности n . Корреляционная иммунность и 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 [4], сводится к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций $f(\alpha)$, называемыми в [5] компонентными функциями или компонентами. Свойства компонент могут быть, в частности, выражены в терминах весов их подфункций (в обозначениях [6]):

$$w_I^J(f) = \left\| (\psi_m(J), f)_{i_1, \dots, i_{|I|}}^{1, \dots, 1} \right\|.$$

Здесь $f = (f_1, \dots, f_m)$; $\|f_1\|$ — вес булевой функции f_1 ; $|J|$ — мощность множества $J = \{j_1, \dots, j_{|J|}\} \subset \{1, \dots, m\}$; $I = \{i_1, \dots, i_{|I|}\} \subset \{1, \dots, n\}$; $\psi_m(J)$ — двоичный вектор длины m , у которого в $j_1, \dots, j_{|J|}$ координатах стоят единицы, а в остальных нули (согласно [7], $\psi_m(J)$ называется индикаторным вектором множества J); $(a, b) = a_1b_1 \oplus \dots \oplus a_nb_n$ — скалярное произведение векторов a и b из V_m ; $(\psi_m(J), f)_{i_1, \dots, i_{|I|}}^{1, \dots, 1}$ — подфункция компоненты $(\psi_m(J), f)$ отображения f , получаемая, если у аргумента компоненты $(\psi_m(J), f)$ значения координат с номерами $i_1, \dots, i_{|I|}$ положить равными единице.

Для компоненты $(\psi_m(J), f)$ можно определить спектральный коэффициент Фурье — Уолша — Адамара

$$\Delta_I^J(f) = F_I^J(f) = \frac{1}{2} \sum_{x \in V_n} (-1)^{(\psi_m(J), f)(x) \oplus x_{i_1} \oplus \dots \oplus x_{i_{|I|}}} = 2^{n-1} - \|(\psi_m(J), f)(x) \oplus (\psi_n(I), x)\|,$$

где $(\psi_n(I), x) = x_{i_1} \oplus \dots \oplus x_{i_{|I|}}$. Согласно [8], $\Delta_I^J(f)$ называется коэффициентом статистической структуры компоненты $(\psi_m(J), f)$.

В [9] доказаны формулы однозначной связи w_I^J с коэффициентами статистической структуры

$$\Delta_I^J = \sum_{L \subset I} (-1)^{|L|} (2^{n-1} - 2^{|L|} w_L^J), \quad w_I^J - 2^{n-|I|-1} = 2^{-|I|} \sum_{L \subset I} (-1)^{|L|+1} \Delta_L^J,$$

называемые тождеством Саркара (можно назвать тождеством Денисова — Саркара). Рассмотрим для произвольной функции f из множества B_n^m вектор весов подфункций

$$\overline{W}_k(f) = (w_I^J(f) : \emptyset \neq J \subset \{1, \dots, m\}, I \subset \{1, \dots, n\}, |I| \leq k)$$

и вектор коэффициентов статистической структуры

$$\bar{\Delta}_k(f) = (\Delta_I^J(f) : \emptyset \neq J \subset \{1, \dots, m\}, I \subset \{1, \dots, n\}, |I| \leq k)$$

$$\text{длины } N = N(n, m, k) = (2^m - 1) \sum_{s=0}^k \binom{n}{s}.$$

Многие свойства двоичных отображений зависят от того, чему равен вектор, состоящий из определённых выше характеристик всех компонент или их части. Поэтому задача нахождения мощности множества функций с фиксированным начальным

вектором весов подфункций или коэффициентов статистической структуры является важной. В настоящее время имеются только асимптотические оценки, полученные в [10–14].

Рассмотрим класс функций из B_n^m

$$\begin{aligned} W_n^m(\bar{z}) &= W_n^m(z_I^J : \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n\}; |I| \leq k) = \\ &= \{f \in B_n^m : w_I^J(f) = 2^{n-|I|-1} - z_I^J, \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n\}; |I| \leq k\}, \end{aligned}$$

чьи первые (в лексикографическом порядке) веса подфункций $\bar{W}_k(f) = \bar{W} \in \mathbb{Z}^N$ равны

$$\bar{W} = (w_I^J(f) = 2^{n-|I|-1} - z_I^J(f) : I \subset \{1, \dots, n\}; \emptyset \neq J \subset \{1, \dots, m\}; |I| \leq k).$$

Теорема 1. Пусть $n, m \in \mathbb{N}$, $k \in \{1, \dots, n-1\}$, тогда

$$\begin{aligned} |W_n^m(\bar{z})| &= |W_n^m(z_I^J : I \subset \{1, \dots, n\}; \emptyset \neq J \subset \{1, \dots, m\}; |I| \leq k)| = \\ &= \sum_{\substack{z_{I \cup \{n\}}^J \in \mathbb{Z} : \emptyset \neq J \subset \{1, \dots, m\}, \\ I \subset \{1, \dots, n-1\}, |I|=k}} \left| W_{n-1}^m(z_{I \cup \{n\}}^J : \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n-1\}; |I| \leq k) \right| \times \\ &\quad \times |F_{n-1}^m(z_I^J - z_{I \cup \{n\}}^J : \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n-1\}; |I| \leq k)|. \end{aligned}$$

В теореме 1 суммирование на самом деле происходит не по всем $z_{I \cup \{n\}}^J \in \mathbb{Z}$, а только по $z_{I \cup \{n\}}^J \in \{-2^{n-k-2}, -2^{n-k-2} + 1, \dots, 2^{n-k-2}\}$.

Обозначим через $S_n^m(\bar{\Delta})$ класс функций из B_n^m , обладающих следующим начальным вектором коэффициентов статистической структуры:

$$\bar{\Delta} = (\Delta_I^J(f) : \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n\}; |I| \leq k).$$

Используя тождества Денисова — Саркара, можно доказать

Теорема 2. Пусть $n, m \in \mathbb{N}$, $k \in \{1, \dots, n-1\}$, тогда

$$\begin{aligned} |S_n^m(\bar{\Delta})| &= |S_n^m(\Delta_I^J : I \subset \{1, \dots, n\}; \emptyset \neq J \subset \{1, \dots, m\}; |I| \leq k)| = \\ &= \sum_{\substack{\Delta_{I \cup \{n\}}^J \in \mathbb{Z} : \\ \emptyset \neq J \subset \{1, \dots, m\}, \\ I \subset \{1, \dots, n-1\}, |I|=k}} \left| S_{n-1}^m\left(\frac{\Delta_I^J - \Delta_{I \cup \{n\}}^J}{2} : \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n-1\}; |I| \leq k\right) \right| \times \\ &\quad \times \left| S_{n-1}^m\left(\frac{\Delta_I^J + \Delta_{I \cup \{n\}}^J}{2} : \emptyset \neq J \subset \{1, \dots, m\}; I \subset \{1, \dots, n-1\}; |I| \leq k\right) \right|. \end{aligned}$$

В теореме 2 суммирование также происходит только по тем $\Delta_{I \cup \{n\}}^J$, что лежат в множестве $\{-2^{n-1}, -2^{n-1} + 1, \dots, 2^{n-1}\}$.

Определение 1. Отображение f из множества B_n^m всех m -мерных двоичных функций от n переменных называется k -эластичным ((n, m, k) -устойчивым), если для любых I, J , $\emptyset \neq J \subset \{1, \dots, m\}$, $I \subset \{1, \dots, n\}$, $|I| \leq k$, выполняется $\Delta_I^J(f) = 0$.

Обозначим $R(n, m, k)$ множество всех k -эластичных двоичных отображений из B_n^m .

Следствие 1. В условиях теорем 1 и 2 верно

$$|R(n, m, k)| = \sum_{\substack{\Delta(I, J) \in \{-2^{n-k-2}, \dots, 2^{n-k-2}\}: \\ \emptyset \neq J \subset \{1, \dots, m\}, \\ I \subset \{1, \dots, n-1\}, |I|=k}} |\{f \in B_{n-1}^m : \Delta_I^J(f) = 0 : I \subset \{1, \dots, n-1\}, |I| < k; \\ \Delta_I^J(f) = 2^k \Delta(I, J) : I \subset \{1, \dots, n-1\}, |I| = k; \emptyset \neq J \subset \{1, \dots, m\}\}| \times \\ \times |\{h \in B_{n-1}^m : \Delta_I^J(h) = 0 : I \subset \{1, \dots, n-1\}, |I| < k; \\ \Delta_I^J(h) = -2^k \Delta(I, J) : I \subset \{1, \dots, n-1\}, |I| = k; \emptyset \neq J \subset \{1, \dots, m\}\}|.$$

В работе [3] следствие 1 доказано как отдельный результат, причём в формулировке допущена опечатка.

Определение 2. Отображение f из множества B_n^m всех m -мерных двоичных функций от n переменных называется корреляционно-иммунным порядка k , если для любого J , $\emptyset \neq J \subset \{1, \dots, m\}$, существует такая величина $r_J \in \{-2^{n-k-1}, \dots, 2^{n-k-1}\}$, что для любого I , $I \subset \{1, \dots, n\}$, $|I| \leq k$, выполняется $w_I^J(f) = 2^{n-|I|-1} + r_J 2^{k-|I|}$.

Определение 2 эквивалентно тому, что для любых I, J , $\emptyset \neq J \subset \{1, \dots, m\}$, $I \subset \{1, \dots, n\}$, $1 \leq |I| \leq k$, выполняется $\Delta_I^J(f) = 0$.

Обозначим через $K(n, m, k)$ множество всех корреляционно-иммунных порядка k двоичных отображений из B_n^m . Из утверждения в [15] следует, что если $f \in K(n, m, k)$, то $\|f\| \equiv 0 \equiv \Delta_\emptyset^J \pmod{2^k}$

Следствие 2. В условиях теорем 1 и 2 верно

$$|K(m, n, k)| = \sum_{s=-2^{n-k-1}}^{2^{n-k-1}} \sum_{\substack{\Delta(I, J) \in \{-2^{n-k-1}, \dots, 2^{n-k-1}\}: \emptyset \neq J \subset \{1, \dots, m\}, \\ I \subset \{1, \dots, n-1\}, |I|=k}} |\{f \in B_{n-1}^m : \Delta_\emptyset^J(f) = 2^{k-1}s; \\ \Delta_I^J(f) = 0 : I \subset \{1, \dots, n-1\}, |I| < k; \\ \Delta_I^J(f) = 2^{k-1} \Delta(I, J) : I \subset \{1, \dots, n-1\}, |I| = k; \emptyset \neq J \subset \{1, \dots, m\}\}| \times \\ \times |\{h \in B_{n-1}^m : \Delta_\emptyset^J(h) = 2^{k-1}s; \Delta_I^J(h) = 0 : I \subset \{1, \dots, n-1\}, |I| < k; \\ \Delta_I^J(h) = -2^{k-1} \Delta(I, J) : I \subset \{1, \dots, n-1\}, |I| = k; \emptyset \neq J \subset \{1, \dots, m\}\}|.$$

Полученные рекуррентные формулы позволяют вычислять точные значения мощностей множеств $R(t, m, k)$ и $K(t, m, k)$ для $t > n$ при фиксированных значениях переменных m и k , предварительно экспериментально находя распределение мощности множеств $S_n^m(\bar{\Delta})$ соответствующего вида.

ЛИТЕРАТУРА

1. МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров». <https://tc26.ru/standarts/metodicheskie-rekomendatsii/>
2. Michels D. Here's how GDPR and the blockchain can coexist. <https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/>
3. Pankov K. Enumeration of Boolean mapping with given cryptographic properties for personal data protection in blockchain data storage // Proc. 24th Conf. of Open Innovations Association FRUCT, Moscow, Russia, 2019. P. 300–306.
4. Логачев О. А., Сальников А. А., Смышляев С. В., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.

5. 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.
6. Панков К. Н. Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4. С. 14–30.
7. Сачков В. Н. Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.
8. Словарь криптографических терминов. М.: МЦНМО, 2016. 94 с.
9. Денисов О. В. Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
10. Панков К. Н. Уточнённые асимптотические оценки для числа (n, m, k) -устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
11. Панков К. Н. Уточнённые асимптотические оценки для числа корреляционно-иммунных двоичных функций и отображений // Прикладная дискретная математика. Приложение. 2018. № 11. С. 49–52.
12. Canfield E. R., Gao Z., Greenhill C., et al. Asymptotic enumeration of correlation-immune Boolean functions // Cryptography and Communications. 2010. No. 1. P. 111–126.
13. Панков К. Н. Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
14. Панков К. Н. Улучшенные асимптотические оценки для числа корреляционно-иммунных и k -эластичных двоичных вектор-функций // Дискретная математика. 2018. № 2. С. 73–98.
15. Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций // Дискретная математика. 1991. № 2. С. 25–46.

УДК 519.7

DOI 10.17223/2226308X/12/20

О КОМПОНЕНТАХ НЕКОТОРЫХ КЛАССОВ ОБРАТИМЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ¹

И. А. Панкратова

В классе обратимых векторных булевых функций от n переменных, координатные функции которых существенно зависят от всех переменных, рассматриваются подклассы $\mathcal{K}_n$ и $\mathcal{K}'_n$, функции в которых получены с помощью n независимых транспозиций из тождественной подстановки и из подстановки, каждая координатная функция которой существенно зависит от одной переменной, соответственно. Приводятся некоторые свойства компонент функций из этих классов.

Ключевые слова: векторная булева функция, обратимые функции, нелинейность векторной булевой функции, компонентная алгебраическая иммунность.

Для $n \in \mathbb{N}$ рассмотрим обратимые векторные булевы функции $F = (f_1 \dots f_n)$ на $\mathbb{F}_2^n$, такие, что координатные функции $f_i : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят от всех n переменных. В [1] предложен алгоритм построения некоторой такой функции, который состоит в следующем: стартуя с тождественной подстановки $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, на i -м шаге, $i = 1, \dots, n$, выбираем два соседних по i -й координате и не выбранных на предыдущих шагах вектора $a, b \in \mathbb{F}_2^n$ и меняем местами значения $G(a)$ и $G(b)$.

¹Работа поддержана грантом РФФИ, проект № 17-01-00354.