значение PAPR, являются векторы значений бент-функций. В связи с этим возникает задача поиска кодов, состоящих из векторов значений бент-функций. Одним из способов построения таких кодов является построение линейного кода для некоторой бент-функции f, такого, что сдвиг на любую функцию из кода оставляет функцию f в классе бент-функций. Код длины 2^n называется *кодом постоянной амплитуды*, если все элементы кода являются векторами значений бент-функций. Линейный код длины 2^n называется *кодом, сохраняющим свойство бент* (*SPB-кодом*) для функции f, если сдвиг на любой элемент кода оставляет функцию f в классе бент-функций [1]. Если C — SPB-код, то его аффинный сдвиг $f \oplus C$ является кодом постоянной амплитуды. Это свойство позволяет конструировать коды постоянной амплитуды из линейных кодов.

В работе исследуются свойства бент-функций, лежащих в классе Мэйорана — МакФарланда [2]. Получена нижняя оценка максимальной размерности SPB-кода для произвольной бент-функции.

Теорема 1. Пусть f — бент-функция из класса Мэйорана — МакФарланда от $2n$ переменных. Тогда для функции f существует SPB-код размерности $2^{n+1} - 1$.

В [3] В. В. Ященко ввёл понятие *индекса линейности* для произвольной булевой функции. Любую булеву функцию можно представить в виде $f(x, y) = x_1\varphi_1(y) + \ldots + x_t\varphi_t(y) + \psi(y)$, $x \in \mathbb{F}_2^t$, $y \in \mathbb{F}_2^{n-t}$. Среди всех таких представлений есть представление с максимальным t, которое является аффинным инвариантом и называется индексом линейности булевой функции.

Теорема 2. Пусть f — бент-функция, индекс линейности которой равен k. Тогда для функции f существует SPB-код размерности $2^{k+1} - 1$.

ЛИТЕРАТУРА

1. *Павлов А. В.* Бент-функции и линейные коды в CDMA // Прикладная дискретная математика. Приложение. 2010. № 3. С. 95–97.
2. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
3. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информ. 1997. Т. 33. Вып. 1. С. 75–86.

УДК 519.212.2, 519.214 DOI 10.17223/2226308X/10/20

УТОЧНЁННЫЕ АСИМПТОТИЧЕСКИЕ ОЦЕНКИ ДЛЯ ЧИСЛА (n, m, k)-УСТОЙЧИВЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Уточнена локальная предельная теорема для распределения части вектора спектральных коэффициентов линейных комбинаций координатных функций случайного двоичного отображения. С помощью этой теоремы получена асимптотическая формула для $|R(m, n, k)|$ — числа (n, m, k)-устойчивых двоичных отображений в случае $n \to \infty$, $m \in \{1, 2, 3, 4\}$ и $k \leqslant \dfrac{n(1-\varepsilon)}{5 + 2\log_2 n}$ для произвольного $0 < \varepsilon < 1$, $k = \mathrm{O}\left(\dfrac{n}{\ln n}\right)$:

$$\log_2 |R(m,n,k)| \sim m2^n - (2^m-1)\left(\frac{n-k}{2}\binom{n}{k} + \log_2\sqrt{\frac{\pi}{2}}\sum_{s=0}^{k}\binom{n}{s}\right) +$$
$$+ \left(2\cdot 3^{m-2}-1\right)\operatorname{Ind}\{m\neq 1\}\sum_{s=0}^{k}\binom{n}{s}.$$

Найдены верхние и нижние асимптотические оценки для $|R(m,n,k)|$ в случае $n\to\infty$, $k(5+2\log_2 n)+5m\leqslant n(1-\varepsilon)$ для произвольного $0<\varepsilon<1$:

$$-\varepsilon_1(m-1)\sum_{s=0}^{k}\binom{n}{s} <$$
$$< \log_2|R(m,n,k)| - m2^n + (2^m-1)\left(\frac{n-k}{2}\binom{n}{k} + \log_2\sqrt{\frac{\pi}{2}}\sum_{s=0}^{k}\binom{n}{s}\right) <$$
$$< \varepsilon_2(m-2)(2^m-1)\sum_{s=0}^{k}\binom{n}{s} + \sum_{s=0}^{k}\binom{n}{s}$$

для произвольных $\varepsilon_1,\varepsilon_2$ $(0<\varepsilon_1,\varepsilon_2<1)$.

Ключевые слова: *случайное двоичное отображение, локальная предельная теорема, спектральные коэффициенты, устойчивые вектор-функции, эластичные вектор-функции.*

Как известно, многие свойства двоичных отображений и определяемые ими классы вектор-функций исторически выделялись под влиянием задач разработки и анализа криптографических систем. К таким классам относятся и широко известные в математике и её приложениях (n,m,k)-устойчивые или, как их можно назвать в соответствии с [1], k-эластичные отображения. Такие вектор-функции используются, например, в поточных шифрсистемах в качестве комбинирующих функций, обладающих способностью противостоять корреляционному методу криптоанализа, так как их выход статистически не зависит от некоторых комбинаций входов.

Обозначим через V_n множество двоичных векторов размерности n. В [2] доказано, что многие важные свойства двоичного отображения $f(\alpha)=(f_1(\alpha),f_2(\alpha),\ldots,f_m(\alpha)): V_n\to V_m$, к которым относится и (n,m,k)-устойчивость, сводятся к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций $f(\alpha)$, называемыми в [3] компонентными функциями или компонентами. Свойства компонент могут быть, в частности, выражены в терминах их спектральных коэффициентов Фурье — Уолша — Адамара [4], или, иначе говоря, коэффициентов статистической структуры в соответствии с [5, с. 71]:

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

где $f=(f_1,\ldots,f_m)$; $\|f_1\|$ — вес булевой функции f_1; $J=\{j_1,\ldots,j_{|J|}\}\subset\{1,\ldots,m\}$; $\psi_m(J)$ — двоичный вектор длины m, у которого на $j_1,\ldots,j_{|J|}$ координатах стоят единицы, а на остальных нули. В терминологии [6] $\psi_m(J)$ называется индикаторным вектором множества J.

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

Пусть функция f выбирается случайно и равновероятно из множества B_n^m. Рассмотрим для этой функции вектор коэффициентов статистической структуры

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

длины $N = N(n,m,k) = (2^m-1)\sum\limits_{s=0}^{k}\binom{n}{s}$. Для упрощения записи введём обозначения $\exp_2 x = 2^x$,

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

Теорема 1. Пусть при всех достаточно больших n для произвольного $0 < \varepsilon < 1$ выполняется $k(5+2\log_2 n) + 5m \leqslant n(1-\varepsilon)$. Тогда для векторов $a = (a_I^J : \varnothing \neq J \subset \subset \{1,\dots,m\}, I \subset \{1,\dots,n\}, |I| \leqslant k)$ размерности N, координаты которых удовлетворяют сравнениям (см. [7])

$$\sum_{L\subset I}(-1)^{|L|}a_L^J \equiv 0\left(\mathrm{mod}2^{|I|}\right), \sum_{\varnothing\neq S\subset J, L\subset I}(-1)^{|L|+|S|}a_L^S \equiv 0\left(\mathrm{mod}2^{|I|+|J|-1}\right),$$

для любых $\varnothing \neq J \in \{1,\dots,m\}$ и $I \in \{1,\dots,n\}$ справедливо:

$$\mathsf{P}\left(\overline{\Delta}_k = a\right) = \theta_5(a)\exp\left(-2^{n\varepsilon-1-\log_2 5}\right) +$$
$$+\exp_2(-T(n,m,k))\Bigg(\exp\Bigg(-2^{1-n}\sum_{\varnothing\neq J\in\{1,\dots,m\}}\sum_{I\subset\{1,\dots,n\},|I|\leqslant k}\left(a_I^J\right)^2\Bigg)\times$$
$$\times\left(1+\theta_1(a)2^{(\log_2 3-9)m-n/2}+\theta_2(a)2^{-8m-n}+\theta_3(a)2^{(\log_2 3-17)m-3n/2}\right)+$$
$$+\theta_4(a)n^k 2^{2m+k-n/2}\exp\left(-2^{n-2m-2k-3}n^{-2k}\right)\Bigg)\times$$
$$\times\sum_{\overrightarrow{r}\in\Re^{**}(m,N)}\exp\left(-i\pi\sum_{\varnothing\neq J\subset\{1,\dots,m\}}\sum_{I\subset\{1,\dots,n\},|I|\leqslant k}2^{n/2-|I|}r_I^J\sum_{L\subset I}(-1)^{|L|+1}a_L^J\right),$$

где

$$\Re^{**}(m,N) = \Big\{\overrightarrow{r} = \left(r_I^J, \varnothing \neq J \subset \{1,\dots,m\}, I \subset \{1,\dots,n\}, |I| \leqslant k\right) \in \left(\mathbb{Z}_{2^{m-1}}\right)^N :$$
$$\forall I\,\forall s \in \{1,\dots,m\}\,\forall \delta \in V_m\left(\sum_{\substack{J\subset\{1,\dots,m\},\\ s\in J}}(-1)^{(\delta,\psi_m(J))}r_I^J = 0\right)\Big\};$$

$|\theta_1(a)| \leqslant 32$; $|\theta_2(a)| \leqslant 8$; $|\theta_3(a)| \leqslant 267$; $|\theta_4(a)| \leqslant 3{,}2$; $|\theta_5(a)| \leqslant 1$; $\mathbb{Z}_{2^{m-1}}$ — кольцо вычетов по модулю 2^{m-1}.

Пусть $R(m,n,k)$ — множество всех (n,m,k)-устойчивых двоичных отображений.

Следствие 1. В условиях теоремы 1 при $n \to \infty$

$$|R(m,n,k)| \sim |\Re^{**}(m,N)| \cdot \exp_2\left(m2^n - T(n,m,k)\right).$$

Следствие 2. Пусть при всех достаточно больших n для произвольного $0 < \varepsilon < 1$ выполняется $k \leqslant \dfrac{n(1-\varepsilon)}{5+2\log_2 n}$, $k = \mathrm{O}\left(\dfrac{n}{\ln n}\right)$ и $m \in \{1,2,3,4\}$. Тогда при $n \to \infty$

$$|R(m,n,k)| \sim \exp_2\left(m2^n - T(n,m,k) + N(n,1,k)\left(2\cdot 3^{m-2}-1\right)\mathrm{Ind}\{m \neq 1\}\right),$$

где $\mathrm{Ind}\{A\}$ — индикатор события A.

Следствие 3. В условиях теоремы 1 существует n_0, такое, что для любых $\varepsilon_1, \varepsilon_2 > 0$, $n > n_0$ верны неравенства

$$(1-\varepsilon_1)\exp_2\left(m2^n - T(n,m,k) + (m-1)N(n,1,k)\right) < |R(m,n,k)| <$$
$$< (1+\varepsilon_2)\exp_2\left(m2^n - T(n,m,k) + (m-2)N(n,m,k) + N(n,1,k)\right).$$

Данные оценки уточняют или улучшают результаты работ [1, 4] в связи с [8].

ЛИТЕРАТУРА

1. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
2. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
3. *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.
4. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
5. Словарь криптографических терминов. М.: МЦНМО, 2006.
6. *Сачков В. Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013.
7. *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.
8. *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.

УДК 519.7 DOI 10.17223/2226308X/10/21

КОМПОНЕНТНАЯ АЛГЕБРАИЧЕСКАЯ ИММУННОСТЬ S-БЛОКОВ, ИСПОЛЬЗУЮЩИХСЯ В НЕКОТОРЫХ БЛОЧНЫХ ШИФРАХ

Д. П. Покрасенко

Установлено точное значение компонентной алгебраической иммунности S-блоков, которые используются в работе известных блочных шифров. Получено, что такие шифры, как DES, CAST-256, KASAMI, PRESENT не обладают максимальной иммунностью и потенциально являются менее стойкими к алгебраическому криптоанализу.

Ключевые слова: *векторная булева функция, компонентная алгебраическая иммунность, S-блоки, DES, AES, PRESENT, KUZNYECHIK.*

Известно, что любой шифр можно представить в виде системы булевых уравнений, которые описывают его работу. Данная система строится на основе известного алгоритма шифрования и позволяет связать между собой биты открытого текста, ключа и шифротекста. Решение систем булевых уравнений в общем случае является NP-трудной задачей. Существуют различные алгоритмы решения таких систем, но большинство из них решают только линейные системы либо нелинейные при достаточно низком значении степени уравнений, трудоёмкость нахождения решения в таком случае слишком велика. Подробнее с методами решения систем булевых уравнений можно ознакомиться в [1].