Алгоритм 1. Тест на принадлежность функции f классу NR_n

Вход: Функция $f \in P_2(n)$; матрица A со строками $\{a_1, \ldots, a_r\}$.

$x := a_1$.
Для $i = 2, \ldots, r$
    $y := x \oplus a_i$.
    Если $x \& \bar{y} = \mathbf{0}$, **то**
        выход, ответ: $f \notin NR_n$.
    $x := y$.
Ответ: $f \in NR_n$.

$= (b_0 b_1 \ldots b_{2^n-1})$, $b_i = f(i)$ (здесь мы не различаем число в диапазоне от 0 до $2^n - 1$ и его представление в виде булева вектора длины n).

В самом общем виде (если $M_0 = M_1 = \varnothing$) решение задачи состоит в следующем: для каждого x, такого, что $\mathrm{w}(x) > k$, в соответствии с формулой (1) составляем уравнение $\bigoplus\limits_{i \leqslant x} b_i = 0$. Обозначим матрицу полученной системы линейных однородных уравнений (СЛОУ) $B_{n,k}$. Все решения получившейся СЛОУ

$$B_{n,k}\mathbf{b} = \mathbf{0} \tag{2}$$

являются векторами значений функций из $D_{n,\leqslant k}$.

Для поиска доопределений частично заданной функции (если $M_0 \neq \varnothing$ или $M_1 \neq \varnothing$) решаем ту же систему относительно переменных множества $\{b_i : i \notin M_0 \cup M_1\}$, объявив константами 0 и 1 переменные b_i с номерами из множеств M_0 и M_1 соответственно. Таким образом, СЛОУ (2) преобразуется к системе уже не обязательно однородных уравнений.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. №38. С. 57–65.
2. *Агибалов Г. П.* SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. №7. С. 43–48.
3. *Sloan N. J. A.* The On-line Encyclopedia of Integer Sequences. `https://oeis.org/`
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

УДК 519.7 DOI 10.17223/2226308X/12/18

О СВЯЗИ НЕЛИНЕЙНЫХ И ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

А. В. Милосердов

Исследуются связи таблиц линейного приближения (LAT) и распределения разностей (DDT) векторных булевых функции. Доказано, что наличие совпадающих строк в DDT и LAT является инвариантом относительно аффинной эквивалентности, а также относительно EA-эквивалентности для нормированных DDT- и

[1]Работа поддержана грантами РФФИ, проекты №18-07-01394 и 18-31-00374.

LAT-таблиц. Выдвинута гипотеза о том, что если в LAT (DDT)-таблице векторной булевой функции F все строки попарно различны, то в её DDT (LAT)-таблице все строки также попарно различны. Данная гипотеза проверена для функций от малого числа переменных и для известных APN-функций от не более чем 10 переменных.

Ключевые слова: *APN-функция, AB-функция, дифференциальная равномерность, нелинейность.*

При создании и использовании какого-либо шифра необходимо, чтобы он был устойчив к различным видам криптоанализа. Один из таких методов криптоанализа — дифференциальный [1]. Шифр устойчив к данному методу криптоанализа, если для функции F, лежащей в его основе, уравнение $F(x) \oplus F(x \oplus a) = b$ для любых $a \neq \mathbf{0}, b$ имеет как можно меньше решений. Число решений данного уравнения при различных парах (a, b) формулируют *таблицу распределения разностей* (DDT) размера $2^n \times 2^n$. Если в данной таблице при $a \neq \mathbf{0}$ для функции F все элементы равны 0 или 2, то такая функция называется *почти совершенно нелинейной функцией* (*APN-функцией*).

Для функции можно рассмотреть также *таблицу линейного приближения* (LAT) размера $2^n \times 2^n$, в ячейке (v, u) которой хранится квадрат коэффициента Уолша — Адамара $W_F(u, v) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{\langle v, F(x) \rangle \oplus \langle u, x \rangle}$. Данная таблица рассматривается при исследовании шифра на устойчивость к линейному криптоанализу [2]. LAT-таблица отражает нелинейность функции F. Если каждый коэффициент Уолша — Адамара функции F при $v \neq 0$ лежит в множестве $\{0, \pm 2^{(n+1)/2}\}$, то такая функция называется *почти бент-функцией* (*AB-функцией*).

Известно, что AB-функции и APN-функции тесно связаны.

Теорема 1 [3]. Каждая AB-функция является APN-функцией.

Интересно рассмотреть связи данных таблиц. Выдвинута следующая

Гипотеза 1. Если в LAT (DDT)-таблице векторной булевой функции F все строки попарно различны, то в её DDT (LAT)-таблице все строки попарно различны.

Гипотеза 1 подтверждена для всех векторных булевых функций от 3 переменных и для известных APN-функций от не более чем 10 переменных.

Гипотеза 1 верна для квадратичных APN-функций от чётного числа переменных.

Утверждение 1. Для любой квадратичной APN-функции от чётного числа переменных в LAT- и DDT-таблицах есть совпадающие строки.

Интересно понять, при каких преобразованиях наличие совпадающих строк LAT- и DDT-таблиц является инвариантом.

Векторные булевы функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ и $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называются *расширенно аффинно эквивалентными* (*EA-эквивалентными*), если $F = A_1 \circ G \circ A_2 \oplus A$, где A_1, $A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — взаимно-однозначные аффинные функции и $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — аффинная функция. Если $A \equiv \mathbf{0}$, то функции называются *аффинно эквивалентными.*

Теорема 2. Если функции F и G аффинно эквивалентны и в DDT (LAT)-таблице функции F есть совпадающие строки, то в DDT (LAT)-таблице функции G также есть совпадающие строки.

Аналогичную теорему можно сформулировать и для EA-эквивалентности, но для этого нужно рассматривать немного модифицированные DDT- и LAT-таблицы.

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