УДК 519.7 DOI 10.17223/2226308X/9/16

ФУНКЦИИ НА РАССТОЯНИИ ОДИН ОТ APN-ФУНКЦИЙ ОТ МАЛОГО ЧИСЛА ПЕРЕМЕННЫХ[1]

Г. И. Шушуев

Исследуется вопрос существования APN-функций на расстоянии один друг от друга. Доказано, что гипотеза о том, что таких APN-функций нет, выполнена для большинства известных APN-функций от не более чем восьми переменных.

Ключевые слова: *векторная булева функция, дифференциально δ-равномерная функция, APN-функция.*

В работе рассматриваются векторные булевы функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Каждая такая векторная булева функция единственным образом представляется в виде АНФ:

$$F(x) = \sum_{I \in \mathcal{P}(N)} (\prod_{i \in I} x_i) = \sum_{I \in \mathcal{P}(N)} a_I x^I,$$

где $\mathcal{P}(N)$ — множество всех подмножеств множества $N = \{1, \ldots, n\}$; a_I из $\mathbb{F}_2^n$. *Алгебраической степенью* функции F называется величина равная $\max\{|I| : a_I \neq (0, \ldots, 0), I \in \in \mathcal{P}(N)\}$. Функции с алгебраической степенью, не превосходящей 1, называются *аффинными*. Функция называется *дифференциально δ-равномерной* [1], если для любого ненулевого вектора $a \in \mathbb{F}_2^n$ и любого вектора $b \in \mathbb{F}_2^n$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет δ решений, где δ — целое положительное число. *Порядком* дифференциальной равномерности функции F называется минимальное возможное δ, такое, что F — дифференциально δ-равномерная функция. *Расстоянием* между векторными булевыми функциями F и G называется мощность множества $\{x \in \mathbb{Z}_2^n : F(x) \neq G(x)\}$.

Векторные булевы функции также известны как S-блоки — примитивные элементы шифров. Чем меньше порядок дифференциальной равномерности S-блока, тем выше стойкость шифра, в котором он используется, к дифференциальному криптоанализу [2]. Минимальный возможный порядок равен двум. Функция с порядком дифференциальной равномерности 2 называется APN-функцией (*Almost Perfect Nonlinear*).

В работе [3] поднимается вопрос существования APN-функции на расстоянии один от произвольной APN-функции и доказано, что для тех APN-функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, для которых выполнено

$$\forall x' \in \mathbb{F}_2^n \left(\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (B_a(F) \oplus F(x' \oplus a)) = \mathbb{F}_2^n \right), \tag{1}$$

все функции на расстоянии один являются дифференциально равномерными порядка 4; таким образом, на расстоянии один от них нет APN-функций. В работе [3] выдвигается также гипотеза о том, что все APN-функции удовлетворяют этому условию.

Данный вопрос тесно связан с вопросом существования APN-функций максимальной алгебраической степени, а именно, если найдутся две APN-функции на расстоянии один, то одна из них обладает максимальной алгебраической степенью. В [4] доказано, что для большинства известных APN-функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ функция $x^{2^n-1} + F(x)$ алгебраической степени n не является APN-функцией.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.

В данной работе исследуется вопрос: удовлетворяют ли APN-функции от малого числа переменных условию (1). Функции F и G из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ называются *EA-эквивалентными*, если G представима в виде $G = A_1 \circ F \circ A_2 \oplus A$, где A, A_1 и A_2 — аффинные отображения из F_2^n в F_2^n; A_1 и A_2 являются перестановками.

Утверждение 1. Если векторные булевы функции F и G EA-эквивалентны и условие (1) выполнено для F, то оно выполнено и для G.

Прямым следствием данного утверждения является то, что если какая-то функция из класса EA-эквивалентности удовлетворяет условию (1), то все функции из этого класса также удовлетворяют этому условию. Таким образом, достаточно проверять только одного представителя класса EA-эквивалентности.

В [5] приведены представители классов EA-эквивалентности векторных булевых функций, которые покрывают все APN-функции от не более чем пяти переменных (10 классов) и все квадратичные APN-функции от шести переменных (13 классов). В [6] приведён список всех известных представителей классов EA-эквивалентности APN-функций от семи (490 классов) и восьми переменных (8180 классов). В данной работе с помощью компьютерных вычислений были проверены представители этих классов и установлено, что они удовлетворяют условию (1).

Утверждение 2. Условию (1) удовлетворяют все APN-функции от не более чем пяти переменных, все квадратичные APN-функции от шести переменных и все известные APN-функции от семи и восьми переменных.

Таким образом, на расстоянии один от любой такой APN-функции все функции являются дифференциально равномерными порядка 4, т. е. на расстоянии один от таких APN-функций нет других APN-функций.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
2. *Biham E. and Shamir A.* Differential cryptoanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
3. *Шушуев Г. И.* Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.
4. *Budagyan L., Carlet C., Helleseth T., and Li N.* On the (non-)existence of APN (n,n)-functions of algebraic degree n. `ia.cr/2016/143`.
5. *Brinkmann M. and Leander G.* On the classification of APN functions up to dimension five // Des. Codes Cryptogr. 2008. V. 49. P. 273–288.
6. *Yu Y., Wang M., and Li Y.* A matrix approach for constructing quadratic APN functions // Des. Codes Cryptogr. 2014. V. 73. P. 587–600.