Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/8/8

О ЧИСЛЕ СИММЕТРИЧЕСКИХ КООРДИНАТНЫХ ФУНКЦИЙ APN-ФУНКЦИИ[1]

В. А. Виткуп

Исследуются симметрические свойства APN-функций. Доказана теорема о несуществовании перестановки на координатах, относительно которой APN-функция сохраняет свои значения. Получены верхние оценки количества симметрических булевых функций среди координатных функций APN-функции, а также количества функций, сохраняющих своё значение на циклических сдвигах координат. Получена нижняя оценка числа различных значений APN-функции. Доказаны утверждения о максимально возможном количестве одинаковых значений у APN-функции при малом числе переменных.

Ключевые слова: *векторная булева функция, APN-функция, симметрическая функция.*

Важной частью в конструкции блочных шифров являются векторные булевы функции (S-блоки), которые должны обладать определёнными криптографическими свойствами. Доказанной стойкостью к дифференциальному криптоанализу обладает класс APN-функций — почти совершенно нелинейных функций [1]. В основе данной криптоатаки лежит анализ пар открытых текстов (P, P') и соответствующих им пар шифртекстов (C, C'), между которыми существуют разности $\Delta P = P \oplus P'$ и $\Delta C = C \oplus C'$.

Функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *APN-функцией*, если для любого $a \in (\mathbb{F}_2^n)^*$ и любого $b \in \mathbb{F}_2^n$ уравнение $F(x) + F(x + a) = b$ имеет не более двух решений. В разное время [2] были получены некоторые алгебраические конструкции APN-функций: R. Gold (1968), T. Kasami (1971), H. Dobbertin (1999, 2000), T. Beth и C. Ding (1993), L. Budaghyan, C. Carlet, G. Leander (2008, 2009, 2013) [3], C. Bracken, E. Byrne, N. Markin, G. McGuire (2008, 2011). Исследованию свойств APN-функций посвящено много работ (М. М. Глухов, В. А. Зиновьев, K. Nyberg, C. Carlet, P. Charpin, H. Dobbertin, L. Budaghyan и др.). Тем не менее класс APN-функций до сих пор не описан и мало изучен, поэтому в данной области существует много интересных открытых вопросов, таких, как классификация и оценки количества функций этого класса, поиск конструкций и построение новых APN-функций, в частности взаимно однозначных. В силу сложности описания этого класса естественно рассматривать свойства его наиболее простых представителей, таких, например, как функций с низкой алгебраической степенью, симметрических функции и т. д.

Булева функция f от n переменных — *симметрическая*, если для любой перестановки $\pi \in S_n$ для любых $x_1, \ldots, x_n$ выполнено $f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$. Можно заметить, что значение симметрической булевой функции $f(x)$ зависит только от веса вектора x, следовательно, вектор значений и АНФ такой функции могут быть

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

представлены в более компактном виде, что может быть полезно при аппаратной и программной реализации шифра.

Теорема 1. Пусть F — APN-функция от n переменных. Тогда не существует перестановки $\pi \in S_n$, отличной от тождественной, такой, что $F(x) = F(\pi(x))$ для любого $x \in \mathbb{F}_2^n$.

Пусть функция F принимает t различных значений $y_1, \ldots, y_t$. Определим множество $M_i = \{x : F(x) = y_i\}$. Заметим, что если F — APN-функция от n переменных и принимает t различных значений $y_1, \ldots, y_t$, то множества M_i, $i = 1, \ldots, t$, не могут все одновременно являться слоями булева куба E^n.

Теорема 2. Пусть F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, f_i — координатные булевы функции. Тогда среди $f_1, \ldots, f_n$ не более $\sigma(n)$ симметрических, где

$$\sigma(n) = \left\lfloor n - \log_2 C_n^{\lfloor (n-1)/2 \rfloor} \right\rfloor.$$

Помимо симметрических булевых функций, интерес в криптографии представляют также функции, которые сохраняют значения на всех циклических сдвигах координат вектора x, т. е. $f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1) = \ldots = f(x_n, x_1, \ldots, x_{n-1})$ для любого вектора x из $\mathbb{F}_2^n$ — так называемые *rotation symmetric Boolean functions* (RotS). Следующее утверждение даёт верхнюю оценку количества координатных RotS-функций у APN-функции.

Теорема 3. Пусть F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, f_i — координатные булевы функции. Тогда среди $f_1, \ldots, f_n$ не более $\rho(n)$ RotS-функций, где

$$\rho(n) = \lfloor n - \log_2 n \rfloor.$$

Утверждение 1. Пусть F — APN-функция от n переменных. Тогда:
а) F принимает не менее $\mu(n)$ различных значений, где

$$\mu(n) = \frac{1 + \sqrt{2^{n+2} - 7}}{2};$$

б) мощность $|M_{\max}| \leqslant 2^n - \mu(n) + 1$, где $M_{\max}$ — максимальное по мощности множество M_i.

Верхняя оценка из утверждения 1, к сожалению, не даёт приближенного значения величины $|M_{\max}|$ для наиболее распространённых размерностей, однако следующие свойства множеств M_i дают близкие к точным (в некоторых случаях — точные) оценки для малых n.

Утверждение 2. Пусть F — APN-функция. Тогда для любого i, для любых попарно различных векторов v_r, v_j, v_l, v_s из M_i верно $v_r + v_j + v_l + v_s \neq 0$. В частности, никакое аффинное подпространство $\mathcal{L}$, $\dim(\mathcal{L}) \geqslant 2$, не может быть подмножеством M_i.

Из утверждения 2 и свойств линейных пространств следуют оценки размера множества $M_{\max}$.

Утверждение 3. Пусть F — APN-функция от n переменных, $n \leqslant 9$. Тогда мощность $|M_{\max}|$ не превышает числа $\xi(n)$, где $\xi(n)$ имеет следующие значения:

n	2	3	4	5	6	7	8	9
$\xi(n)$	3	4	6	7	9	11	14	15

На следующих функциях оценка $\xi(n)$ достигается:

$n = 2$, $F =$(0 0 0 1);

$n = 3$, $F =$(0 2 2 2 2 3 6 5);

$n = 5$, $F =$(0 0 0 1 0 2 4 8 0 3 6 12 7 16 25 23 0 7 3 22 28 19 9 0 19 8 15 28 21 9 29 2).

Для следующих функций достижима оценка $\xi(n) - 1$:

$n = 4, F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13);

$n = 6$, $F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13 0 8 16 25 5 15 17 26 32 44 54 59 45 35 63 48 0 16 26 36 34 48 60 0 45 57 49 11 7 17 31 39 43 28 14 23 12 57 45 54 38 21 5 24 9 56 46 49).

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // Eurocrypt'1993. LNCS. 1994. V. 765. P. 55–64.
2. *Туэжилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Habilitation Thesis, University of Paris, Sept. 2013.

УДК 519.7 DOI 10.17223/2226308X/8/9

О ПЕРЕСЕЧЕНИИ МНОЖЕСТВ ЗНАЧЕНИЙ ПРОИЗВОДНЫХ APN-ФУНКЦИЙ[1]

А. А. Городилова

Исследуются пересечения множеств значений производных двух APN-функций. Формулируются два вопроса: какова минимальная мощность таких пересечений и как связаны любые две APN-функции, множества значений производных которых попарно совпадают по каждому направлению. Получены частичные результаты по каждому из вопросов.

Ключевые слова: *векторная булева функция, производная по направлению, APN-функция.*

В работе рассматривается специальный класс векторных булевых функций — почти совершенные нелинейные функции (APN-функции). Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *APN-функцией*, если для любых векторов $a, b \in \mathbb{F}_2^n$, где a — ненулевой вектор, уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более двух решений. Данные функции представляют интерес для использования в качестве узлов замены в блочных шифрах в силу их оптимальной стойкости к разностному криптоанализу. Однако класс APN-функций достаточно слабо изучен (см., например, обзор [2]), остаётся большое число открытых вопросов [3].

Настоящая работа посвящена исследованию пересечений множеств значений производных APN-функций. Производной функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ по направлению $a \in \mathbb{F}_2^n$ называется функция $D_aF(x) = F(x) \oplus F(x \oplus a)$. По определению F — APN-функция, если её производные по каждому направлению принимают в точности 2^{n-1} различных значений, т. е. $|B_a(F)| = |\{D_aF(x) : x \in \mathbb{F}_2^n\}| = 2^{n-1}$. Для автора представляется интересным найти ответы на следующие вопросы.

Открытый вопрос 1. Каково минимальное пересечение множеств значений производных двух APN-функций?

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.