

УДК 519.7

ХАРАКТЕРИЗАЦИЯ APN-ФУНКЦИЙ ЧЕРЕЗ ПОДФУНКЦИИ¹

А. А. Городилова

Получена полная характеристика APN-функций от n переменных через векторные подфункции от $n - 1$ переменной, а именно: доказано, что векторная функция от n переменных — APN-функция, если и только если каждая из её подфункций от $n - 1$ переменной либо APN-функция, либо имеет порядок дифференциальной равномерности 4, и при этом выполнены условия допустимости.

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

Векторной булевой функцией F называется любое отображение $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$. Векторную функцию можно рассматривать как набор из n координатных булевых функций от n переменных, т. е. $F = (f_1, \dots, f_n)$. Производной по направлению $a \in \mathbb{Z}_2^n$ функции F называется векторная функция $D_a F$, определённая как $D_a F(x) = F(x) \oplus F(x \oplus a)$ для всех $x \in \mathbb{Z}_2^n$. Векторная функция F называется дифференциально δ -равномерной [1], если для любых $a \neq 0$, b уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений. Назовём порядком дифференциальной равномерности F минимальное δ , такое, что F является дифференциально δ -равномерной. Легко видеть, что минимально возможный порядок равен двум. APN-функцией (Almost Perfect Nonlinear) называется дифференциально 2-равномерная векторная функция.

Исследованию APN-функций посвящено большое число работ как в России (М. М. Глухов, В. А. Зиновьев, М. Э. Тужилин, Д. Г. Фон-дер-Флаасс и др.), так и за рубежом (К. Nyberg, L. R. Knudsen, C. Carlet, L. Budaghyan, J. Dillon и др.). APN-функции представляют интерес для криптографических приложений, в частности для использования в качестве S-блоков в блочных шифрах, поскольку обеспечивают оптимальную стойкость к дифференциальному криптоанализу. Обзор известных APN-функций приводится в работе [2].

Пусть S — векторная функция от n переменных, $S = (s_1, \dots, s_n)$.

Определение 1. Назовём функции F, G, f, g набором подфункций S , если они получены из S при фиксации координаты x_i и функции s_j , где $i, j = 1, \dots, n$, следующим образом:

$$\begin{aligned} F(x) &= (s_1(\bar{x}_{i,0}), \dots, s_{j-1}(\bar{x}_{i,0}), s_{j+1}(\bar{x}_{i,0}), \dots, s_n(\bar{x}_{i,0})), & f(x) &= s_j(\bar{x}_{i,0}), \\ G(x) &= (s_1(\bar{x}_{i,1}), \dots, s_{j-1}(\bar{x}_{i,1}), s_{j+1}(\bar{x}_{i,1}), \dots, s_n(\bar{x}_{i,1})), & g(x) &= s_j(\bar{x}_{i,1}), \end{aligned}$$

где $\bar{x}_{i,0} = (x_1, \dots, x_{i-1}, 0, x_i, \dots, x_{n-1})$ и $\bar{x}_{i,1} = (x_1, \dots, x_{i-1}, 1, x_i, \dots, x_{n-1})$.

В случае $i = n, j = n$ функция S представляется через набор подфункций следующим образом (здесь $x \in \mathbb{Z}_2^{n-1}$, $x_n \in \mathbb{Z}_2$):

$$S(x, x_n) = ((x_n \oplus 1)F(x) \oplus x_n G(x), (x_n \oplus 1)f(x) \oplus x_n g(x)).$$

Определение 2. Назовём набор функций F, G, f, g допустимым, где F, G — векторные, а f, g — булевы функции от n переменных, если выполнены следующие условия:

¹Работа поддержана грантом НШ-1939.2014.1 Президента России для ведущих научных школ.

- (*) для всех $x, y, a \in \mathbb{Z}_2^n$, $a \neq 0$, хотя бы одно из равенств $D_a F(x) = D_a G(y)$ и $D_a f(x) = D_a g(y)$ нарушается;
- (**) для всех $x, y, a \in \mathbb{Z}_2^n$, $a \neq 0$, $x \neq y$, $y \oplus a$, хотя бы одно из равенств $D_a H(x) = D_a H(y)$ и $D_a h(x) = D_a h(y)$ нарушается, где $H = F$ и $h = f$, либо $H = G$ и $h = g$.

Получена следующая теорема о характеристизации APN-функций через набор подфункций, обобщающая результат теоремы 3 из [3].

Теорема 1. Векторная функция S от n переменных — APN-функция тогда и только тогда, когда набор её подфункций F, G, f, g является допустимым и каждая из векторных функций F и G либо APN-функция, либо имеет порядок дифференциальной равномерности равный 4.

При малом числе переменных получена следующая характеристизация APN-функций от n переменных через векторные подфункции F и G от $n - 1$ переменных:

	$n = 2$	$n = 3$	$n = 4$
Количество всех APN-функций от n пер.	192	668 128	18 940 805 775 360
F, G — APN-функции	192	$589\,824 = 6/7$ от всех	$4\,419\,521\,347\,584 = 7/30$ от всех
F, G — порядка диф. рав. 4	—	$98\,304 = 1/7$ от всех	$11\,995\,843\,657\,728 = 19/30$ от всех
Одна функция — APN, другая — порядка диф. рав. 4	—	—	$2\,525\,440\,770\,048 = 4/30$ от всех

Вычисления для случая $n = 4$ проводились на кластере НКС-30Т ССКЦ СО РАН.

ЛИТЕРАТУРА

1. Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. Тузиллин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. Фролова А. А. Итеративная конструкция APN-функций // Прикладная дискретная математика. Приложение. 2013. № 6. С. 24–25.

УДК 519.716.32+519.854

КЛАССИФИКАЦИЯ ФУНКЦИЙ НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ В СВЯЗИ С МЕТОДОМ ПОКООРИНАТНОЙ ЛИНЕАРИЗАЦИИ

М. В. Заец

Известно, что для решения систем полиномиальных уравнений над примарным кольцом вычетов можно применять метод покоординатной линеаризации. Рассматривается классификация функций над примарным кольцом вычетов, порождающих системы уравнений, для которых также применим указанный метод. Класс полиномиальных функций расширяется классом вариационно-координатно-полиномиальных функций (ВКП-функций), который, в свою очередь, расширяется классом квази-ВКП-функций и классом координатно-линейно разрешимых функций. Описываются свойства введенных классов функций.