Math-Net.Ru

Общероссийский математический портал

А. А. Городилова, Характеризация почти совершенно нелинейных функций через подфункции, *Дискрет. матем.*, 2015, том 27, выпуск 3, 3–16

DOI: <https://doi.org/10.4213/dm1331>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.92.164.108

26 апреля 2023 г., 11:50:18

Характеризация почти совершенно нелинейных функций через подфункции

© 2015 г. А. А. Городилова*

Исследуются вопросы комбинаторного описания почти совершенно нелинейных функций (APN-функций). Получена полная характеристизация APN-функций от n переменных через подфункции от $n - 1$ переменных: доказано, что векторная функция от n переменных — APN-функция тогда и только тогда, когда каждая из ее подфункций от $n - 1$ переменных является либо APN-функцией, либо имеет порядок дифференциальной равномерности 4, и при этом выполнены условия допустимости. Приведена подробная характеристизация APN-функций от 2, 3 и 4 переменных.

Исследование выполнено при поддержке гранта РФФИ 15-07-01328 и гранта НШ-1939.2014.1 Президента России для ведущих научных школ.

Ключевые слова: векторная булева функция, дифференциальная равномерность, APN-функция, характеристизация.

1. Введение

В работе исследуются криптографические свойства векторных булевых функций. В блочных шифрах роль основного нелинейного преобразования выполняет S-блок, который реализует векторную булеву функцию, в общем случае переводящую двоичный вектор размерности n в двоичный вектор размерности m . Определенные свойства S-блока повышают стойкость шифра к некоторым видам криптоанализа. Поэтому актуальной задачей на настоящий момент является построение векторных булевых функций с заданным набором свойств.

В работе [16] К. Nyberg определила специальное свойство функции — дифференциальную равномерность. Векторная булева функция $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ называется дифференциально δ -равномерной, если для любых векторов $a \neq 0$, b размерности n уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений, где δ — целое неотрицательное число. Стойкость шифра к дифференциальному криптоанализу [4] увеличивается, если использовать в нем функции с малым значением δ . Например, в стандарте американского блочного шифрования AES [11] в качестве S-блока используется дифференциально равномерная порядка 4 функция. Легко видеть, что

*Место работы: Институт математики им. С.Л. Соболева СО РАН,
e-mail: gorodilova@math.nsc.ru

минимально возможное δ равно двум, и дифференциально 2-равномерные функции называются *почти совершенно нелинейными* (APN-функциями).

Исследованию APN-функций посвящено большое число работ как российских авторов (М. М. Глухов [1], В. А. Зиновьев [9], М. Э. Тужилин [2], Д. Г. Фон-дер-Флаасс [3] и др.), так и зарубежных (L. Budaghyan [6], С. Carlet [8], Р. Charpin [10], J. Dillon [12], Н. Dobbertin [13], L. R. Knudsen [17], К. Nyberg [16] и др.). Однако в области APN-функций остается большое число открытых вопросов (см., например, [7]). Прежде всего, это построение новых APN-функций, описание класса APN-функций, поиск оценок количества APN-функций от произвольного числа переменных, исследование нелинейности APN-функций. Отдельным важным вопросом стоит существование взаимно однозначных APN-функций при четном числе переменных больше 6 (известно, что от 2 и 4 переменных таких функций нет, а единственный пример APN-подстановки от 6 переменных найден в [12]). Все известные конструкции почти совершенно нелинейных функций получены с помощью алгебраического представления, при котором функция рассматривается как функция над конечным полем. Однако таких конструкций мало. В [6] приведен подробный обзор известных APN-функций.

Здесь изучается комбинаторное строение класса APN-функций. В начале рассматриваются базовые определения и основные сведения о почти совершенно нелинейных функциях. Далее приводится краткий обзор некоторых известных подходов к описанию APN-функций. В основной части статьи получена характеристика APN-функций через подфункции. Доказывается теорема о том, что векторная функция от n переменных является APN-функцией тогда и только тогда, когда любая ее подфункция от $n - 1$ переменных является либо APN-функцией, либо имеет порядок дифференциальной равномерности 4, и при этом выполнены условия допустимости. Приводятся вычислительные результаты данной характеристики APN-функций от 2, 3, 4 переменных. В заключение описывается подход к поиску итеративной конструкции APN-функций через APN-функции от меньшего числа переменных. Приводится ряд утверждений о выборе допустимых пар векторных функций для построения APN-функций от большего числа переменных.

2. Основные определения

Пусть $\mathbb{F}_2^n$ — множество всех двоичных векторов размерности n . Пусть $\oplus$ обозначает сложение по модулю 2. Для $x, y \in \mathbb{F}_2^n$ будем использовать обозначения $x \oplus y = (x_1 \oplus y_1, \dots, x_n \oplus y_n)$ и $\langle x, y \rangle = x_1 y_1 \oplus \dots \oplus x_n y_n$. Булева функция от n переменных — это произвольное отображение $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Вес $\text{wt}(f)$ булевой функции f равен числу единиц в векторе ее значений. Векторной булевой функцией F называется произвольное отображение $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$. Векторную функцию можно рассматривать как набор из m координатных булевых функций от n переменных, т. е. $F = (f_1, \dots, f_m)$. Производной по направлению $a \in \mathbb{F}_2^n$ функции F является векторная функция $D_a F$, определенная равенством $D_a F(x) = F(x) \oplus F(x \oplus a)$ для всех $x \in \mathbb{F}_2^n$.

Для векторной булевой функции справедливо однозначное представление в виде алгебраической нормальной формы (АНФ):

$$F(x_1, \dots, x_n) = \bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \dots x_{i_k} \oplus a_0,$$

где $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ и $a_{i_1, \dots, i_k}, a_0 \in \mathbb{F}_2^m$.

Степенью функции F (обозначается $\deg(F)$) называется количество переменных в самом длинном слагаемом ее АНФ, при котором стоит ненулевой коэффициент. Функции степени не выше 1 называются *аффинными*, и в случае $a_0 = 0$ — *линейными*.

Далее в работе рассматриваются только функции $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.

Векторная функция F от n переменных называется *дифференциально δ -равномерной* (differentially δ -uniform) [16], если для любых $a, b \in \mathbb{F}_2^n$, $a \neq 0$, уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений. Назовем *порядком* дифференциальной равномерности F минимальное такое δ , что F является дифференциально δ -равномерной. Легко видеть, что минимально возможный порядок равен двум.

Определение 1. *APN-функцией* (Almost Perfect Nonlinear) называется дифференциально 2-равномерная векторная функция.

Все известные конструкции APN-функций получены с помощью представления функции над полем. Пусть $GF(2^n)$ — конечное поле порядка 2^n . Векторную булеву функцию можно рассматривать как функцию $F : GF(2^n) \rightarrow GF(2^n)$. Для нее определено однозначное представление в виде полинома $\sum_{k=0}^{2^n-1} a_k x^k$, где $a_k \in GF(2^n)$, x пробегает элементы $GF(2^n)$ [8]. Функция вида ax^d называется *мономиальной*.

Класс *циклотомической эквивалентности* мономиальной функции с показателем d состоит из всех мономиальных функций, показатели которых равны $2^i d$, $i = 0, \dots, n-1$, и $2^i/d$, $i = 0, \dots, n-1$, если функция x^d взаимно однозначна. Таблица 1 иллюстрирует все известные показатели мономиальных APN-функций [6] с точностью до циклотомической эквивалентности. Однако найдены и APN-функции, не являющиеся CCZ-эквивалентными мономиальным (см., например, обзор [2]): функции F и F' называются *CCZ-эквивалентными*, если графики $G_F = \{(x, F(x)); x \in \mathbb{F}_2^n\}$ и $G_{F'} = \{(x, F'(x)); x \in \mathbb{F}_2^n\}$ аффинно эквивалентны. Это означает, что существует такая взаимно однозначная аффинная функция $A = (A_1, A_2)$, где $A_1, A_2 : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, что $y = F(x)$ тогда и только тогда, когда $A_2(x, y) = F'(A_1(x, y))$ для любых $x, y \in \mathbb{F}_2^n$; при этом функция $F_1(x) = A_1(x, F(x))$ должна быть взаимно однозначной. Известно [9], что CCZ-эквивалентные функции имеют одинаковый порядок дифференциальной равномерности.

Функция	Показатель d	Условия	$\deg(F)$
Gold	$d = 2^t + 1$	$\gcd(t, n) = 1$	2
Kasami	$d = 2^{2t} - 2^t + 1$	$\gcd(t, n) = 1$	$t + 1$
Welch	$2^t + 3$	$n = 2t + 1$	3
Niho	$2^t + 2^{\frac{t}{2}} - 1$, если t четно $2^t + 2^{\frac{3t+1}{2}} - 1$, если t нечетно	$n = 2t + 1$	$(t + 1)/2$ $t + 1$
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t + 3$

Таблица 1. Известные показатели мономиальных APN-функций

В [14] Н. Dobbertin сделал предположение, что показатели из таблицы 1 полностью покрывают все возможные APN-показатели. Это утверждение вычислительно проверено [13] вплоть до числа переменных $n \leq 25$.

3. Известные характеристики APN-функций

В данном разделе рассмотрим некоторые известные характеристики APN-функций в терминах смежных объектов. Для начала перечислим известные эквивалентные определения APN-функций в следующем утверждении.

Утверждение 1. Пусть $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. Следующие условия эквивалентны:

- 1) F — APN-функция, т. е. для любых векторов $a \neq 0, b$ из $\mathbb{F}_2^n$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более 2 решений,
- 2) для любых различных $x, y, z, t \in \mathbb{F}_2^n$, удовлетворяющих условию $x \oplus y \oplus z \oplus t = 0$, выполнено $F(x) \oplus F(y) \oplus F(z) \oplus F(t) \neq 0$,
- 3) для любого ненулевого $a \in \mathbb{F}_2^n$ выполнено $|B_a(F)| = 2^{n-1}$, где $B_a(F) = \{F(x) \oplus F(x \oplus a) \mid x \in \mathbb{F}_2^n\}$,
- 4) коэффициенты Уолша — Адамара $W_F(u, v)$ функции F , где $W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle v, F(x) \rangle \oplus \langle u, x \rangle}$, $u, v \in \mathbb{F}_2^n$, удовлетворяют тождеству

$$\sum_{u, v \in \mathbb{F}_2^n} (W_F(u, v))^4 = 3 \cdot 2^{4n} - 2 \cdot 2^{3n}.$$

В [9] С. Carlet, Р. Charpin и V. Zinoviev привели характеристику APN-функций через специально построенные булевы функции. Определим для $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ булеву функцию γ_F от $2n$ переменных:

$$\gamma_F(a, b) = \begin{cases} 1, & \text{если } a \neq 0 \text{ и существует решение } F(x) \oplus F(x \oplus a) = b; \\ 0, & \text{иначе.} \end{cases}$$

Утверждение 2 ([9]). Пусть $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ — векторная булева функция. Тогда F — APN-функция тогда и только тогда, когда $\text{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$.

В той же работе найдена характеристика APN-функций в терминах теории кодирования. Данный подход позволил найти некоторые ограничения на вид полиномиального представления APN-функций как функций над конечным полем.

Утверждение 3 ([9]). Пусть $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, причем $F(0) = 0$. Определим линейный $[2^n - 1, k, d]$ -код C_F с помощью проверочной матрицы

$$H_F = \begin{pmatrix} 1 & 2 & \dots & x & \dots & 2^n - 1 \\ F(1) & F(2) & \dots & F(x) & \dots & F(2^n - 1) \end{pmatrix},$$

где вхождения x и $F(x)$ в матрицу рассматриваются как двоичные вектор-столбцы размерности n . Тогда F — APN-функция тогда и только тогда, когда кодовое расстояние d кода C_F равно 5.

В следующем утверждении приводится характеристизация квадратичных однородных APN-функций через специальные матрицы, полученная Y. Yu, M. Wang, Y. Li в [19] и позволившая найти APN-функции от 7 и 8 переменных, которые не покрывались известными ранее конструкциями.

Утверждение 4 ([19]). Пусть $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$, $\alpha_i \in GF(2^n)$, — произвольный базис $GF(2^n)$ над $GF(2)$ и M — $(n \times n)$ -матрица с коэффициентами $M[i, j] = \alpha_j^{2^{i-1}}$, где $i, j = 1, \dots, n$. Пусть $F : GF(2^n) \rightarrow GF(2^n)$ задана полиномом $F(x) = \sum_{1 \leq i < j \leq n} c_{i,j} x^{2^{i-1} + 2^{j-1}}$ и $H = M^T C_F M$, где C_F — $(n \times n)$ -матрица с коэффициентами $C_F[i, j] = C_F[j, i] = c_{i,j}$ при $1 \leq i < j \leq n$ и $C_F[i, i] = 0$ при $1 \leq i \leq n$. Тогда F — APN-функция тогда и только тогда, когда любая ненулевая линейная комбинация n строк H имеет ранг $n - 1$.

Известны также характеристизации APN-функций (в частности, квадратичных) через объекты проективной геометрии. Подробно они описаны, например, в [15], [18]. С помощью таких характеристизаций можно проверять эквивалентность между APN-функциями через изоморфизм соответствующих им объектов проективной геометрии.

4. Характеризация APN-функций через подфункции

В данном разделе будет получена полная характеристизация APN-функций через набор ее подфункций от меньшего числа переменных. Данная характеристизация отражает комбинаторную структуру APN-функции, а также дает возможность для итеративного построения APN-функций.

4.1. Конструктивное описание APN-функций. Пусть S — векторная функция от n переменных, $S = (s_1, \dots, s_n)$.

Определение 2. Назовем четыре 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:

$$F(x) = (s_1(\bar{x}_{i,0}), \dots, s_{j-1}(\bar{x}_{i,0}), s_{j+1}(\bar{x}_{i,0}), \dots, s_n(\bar{x}_{i,0})), \quad f(x) = s_j(\bar{x}_{i,0}),$$

$$G(x) = (s_1(\bar{x}_{i,1}), \dots, s_{j-1}(\bar{x}_{i,1}), s_{j+1}(\bar{x}_{i,1}), \dots, s_n(\bar{x}_{i,1})), \quad g(x) = s_j(\bar{x}_{i,1}),$$

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 $x \in \mathbb{F}_2^{n-1}, x_n \in \mathbb{F}_2$):

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

Определение 3. Назовем набор функций F, G, f, g *допустимым*, где F и G — векторные, а f и g — булевы функции от n переменных, если выполнены условия:

(*) для всех $x, y, a \in \mathbb{F}_2^n, a \neq 0$, 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 $x, y, a \in \mathbb{F}_2^n, a \neq 0, x \neq y, y \oplus a$, 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 $h = g$.

Замечание 1. Если в наборе функций F, G, f, g какая-либо из функций F или G является APN-функцией, то для нее и соответствующей булевой функции f или g условие (**) из определения допустимого набора всегда выполнено.

Справедлива следующая теорема о характеристизации APN-функций через набор подфункций.

Теорема 1. Пусть $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. Тогда:

(i) если S — APN-функция, то все ее наборы подфункций F, G, f, g допустимые, причем каждая из F и G либо APN, либо порядка дифференциальной равномерности 4;

(ii) если некоторый набор подфункций F, G, f, g функции S допустимый и каждая из F и G либо APN, либо порядка дифференциальной равномерности 4, то S — APN-функция.

Доказательство. Известно, что порядки дифференциальной равномерности функций S и $A' \circ S \circ A''$ совпадают [9], где A', A'' — произвольные взаимно однозначные аффинные функции. Поэтому без ограничения общности можно рассматривать набор подфункций функции $S = (s_1, \dots, s_n)$, полученный при фиксации координаты x_n и функции s_n . Таким образом, если выполнено утверждение (i) теоремы для данного набора, то оно выполнено и для всех остальных. Далее покажем, что свойство функции S быть APN эквивалентно тому, что данный набор подфункций удовлетворяет условиям теоремы.

Будем использовать для векторов из $\mathbb{F}_2^n$ обозначение $\bar{x} = (x, x_n)$, где $x \in \mathbb{F}_2^{n-1}$. По определению функция S — APN-функция тогда и только тогда, когда $|B_{\bar{a}}(S)| = 2^{n-1}$ для всех ненулевых $\bar{a} \in \mathbb{F}_2^n$. Рассмотрим множества $B_{\bar{a}}(S)$ для всех $\bar{a} \neq 0$.

Случай 1. Пусть $\bar{a} = (a, 0)$, где $a \in \mathbb{F}_2^{n-1}, a \neq 0$. Имеем

$$B_{\bar{a}}(S) = \{S(\bar{x}) \oplus S(\bar{x} \oplus \bar{a}) \mid \bar{x} \in \mathbb{F}_2^n\} = M_F \cup M_G,$$

где

$$M_F = \{(F(x) \oplus F(x \oplus a), f(x) \oplus f(x \oplus a)) \mid x \in \mathbb{F}_2^{n-1}\},$$

$$M_G = \{(G(x) \oplus G(x \oplus a), g(x) \oplus g(x \oplus a)) \mid x \in \mathbb{F}_2^{n-1}\}.$$

Заметим, что по построению $|M_F|, |M_G| \leq 2^{n-2}$. Функция S — APN-функция тогда и только тогда, когда $|B_{\bar{a}}(S)| = 2^{n-1}$, а, следовательно, множества M_F и M_G

должны не пересекаться, и каждое иметь максимальную мощность 2^{n-2} . Множества не пересекаются тогда и только тогда, когда выполнено условие (*) из определения допустимого набора F, G, f, g . Кроме того, M_F и M_G имеют максимальные мощности, если и только если каждая из F и G либо APN-функция, либо имеет порядок дифференциальной равномерности 4, и при этом выполнено условие (**) для F, G, f, g .

Случай 2. Пусть $\bar{a} = (a, 1)$, где $a \in \mathbb{F}_2^{n-1}$. Имеем

$$B_{\bar{a}}(S) = \{S(\bar{x}) \oplus S(\bar{x} \oplus \bar{a}) \mid \bar{x} \in \mathbb{F}_2^n\} = M'_F \cup M'_G,$$

где

$$M'_F = \{(F(x) \oplus G(x \oplus a), f(x) \oplus g(x \oplus a)) \mid x \in \mathbb{F}_2^{n-1}\},$$

$$M'_G = \{(G(x) \oplus F(x \oplus a), g(x) \oplus f(x \oplus a)) \mid x \in \mathbb{F}_2^{n-1}\}.$$

После замены $y = x \oplus a$ получаем, что

$$M'_G = \{(F(y) \oplus G(y \oplus a), f(y) \oplus g(y \oplus a)) \mid y \in \mathbb{F}_2^{n-1}\},$$

а следовательно, $M'_F = M'_G$. Таким образом, $B_{\bar{a}}(S) = M'_F$. Получаем, что $|B_{\bar{a}}(S)| = 2^{n-1}$ тогда и только тогда, когда в M'_F все элементы различны. Покажем, что условие (*) эквивалентно тому, что в M'_F все элементы различны.

Предположим, что нашлись такие $x, y \in \mathbb{F}_2^{n-1}$, $x \neq y$, что

$$F(x) \oplus G(x \oplus a) = F(y) \oplus G(y \oplus a), \quad (1)$$

$$f(x) \oplus g(x \oplus a) = f(y) \oplus g(y \oplus a). \quad (2)$$

Обозначим $a' = x \oplus y$, $a' \neq 0$, и $y' = y \oplus a$. Тогда равенства (1) и (2) примут вид:

$$F(x) \oplus F(x \oplus a') = G(y') \oplus G(y' \oplus a'),$$

$$f(x) \oplus f(x \oplus a') = g(y') \oplus g(y' \oplus a'),$$

что противоречит условию (*). Обратно аналогично.

Таким образом, рассмотрев случаи 1 и 2, доказали требуемое.

Пример 1. Интересно отметить, что единственная известная с точностью до ССЗ-эквивалентности взаимно однозначная APN-функция S от 6 переменных, найденная в [12],

$$S = \begin{pmatrix} 0 & 54 & 48 & 13 & 15 & 18 & 53 & 35 & 25 & 63 & 45 & 52 & 3 & 20 & 41 & 33 \\ 59 & 36 & 2 & 34 & 10 & 8 & 57 & 37 & 60 & 19 & 42 & 14 & 50 & 26 & 58 & 24 \\ 39 & 27 & 21 & 17 & 16 & 29 & 1 & 62 & 47 & 40 & 51 & 56 & 7 & 43 & 44 & 38 \\ 31 & 11 & 4 & 28 & 61 & 46 & 5 & 49 & 9 & 6 & 23 & 32 & 30 & 12 & 55 & 22 \end{pmatrix}$$

имеет следующую характеризацию, согласно теореме 1:

• при фиксации переменной x_4 и координатной функции s_6 по определению 2 получаем функции F и G , которые имеют порядок дифференциальной равномерности равный 4, и являются взаимно однозначными, где

$$F = \begin{pmatrix} 0 & 27 & 24 & 6 & 12 & 31 & 22 & 26 & 29 & 18 & 1 & 17 & 30 & 9 & 21 & 7 \\ 19 & 13 & 10 & 8 & 23 & 20 & 25 & 28 & 15 & 5 & 2 & 14 & 4 & 3 & 11 & 16 \end{pmatrix},$$

$$G = \begin{pmatrix} 7 & 9 & 26 & 17 & 1 & 10 & 20 & 16 & 5 & 4 & 28 & 18 & 25 & 13 & 29 & 12 \\ 8 & 14 & 0 & 31 & 3 & 21 & 22 & 19 & 30 & 23 & 2 & 24 & 15 & 6 & 27 & 11 \end{pmatrix};$$

• при всех остальных фиксациях получаем F и G , которые являются функциями порядка дифференциальной равномерности 4, но не взаимно однозначными.

Известно, что любая линейная комбинация координатных функций APN-функции от n переменных, $n \geq 3$, не может быть аффинной [8]. Из этого факта и теоремы 1 следует следующее утверждение.

Следствие 1. Для любых двух APN-функций F и G от n переменных, $n \geq 2$, существует такой ненулевой вектор $a \in \mathbb{F}_2^n$, что множества значений производных $D_a F$ и $D_a G$ пересекаются.

Доказательство. Предположим, что существуют такие APN-функции F и G от n переменных, $n \geq 2$, что если $B_a(F) = \{F(x) \oplus F(x \oplus a) \mid x \in \mathbb{F}_2^n\}$ и $B_a(G) = \{G(x) \oplus G(x \oplus a) \mid x \in \mathbb{F}_2^n\}$, то $B_a(F) = \mathbb{F}_2^n \setminus B_a(G)$ для любого ненулевого вектора $a \in \mathbb{F}_2^n$. Тогда набор функций F, G, f, g будет допустимым при любой паре булевых функций f, g от n переменных. Действительно, так как для любых $a, x, y \in \mathbb{F}_2^n$, $a \neq 0$, верно $D_a F(x) \neq D_a G(y)$, то условие (*) выполняется для произвольных f и g , в частности, для $f \equiv g \equiv 0$. Тогда по теореме 1 функция $S(x, x_n) = ((x_n \oplus 1)F(x) \oplus x_n G(x), 0)$ от $n + 1$ переменных является почти совершенно нелинейной, что противоречит тому, что у APN-функции нет аффинных компонентных функций.

4.2. Вычислительные результаты характеристики В таблице 2 приведены результаты характеристики почти совершенно нелинейных функций от малого числа переменных n , где K_n равно числу всех APN-функций от n переменных.

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

Таблица 2. Характеризация APN-функций от малого числа переменных

Вычисления для случая четырех переменных проводились на кластере НКС-30Т ССКЦ СО РАН.

Забегая вперед (см. раздел 5.1), интересно отметить, что наблюдается равномерность в образовании допустимых наборов функций из представителей классов эквивалентности относительно группы сдвигов (по утверждению 5 достаточно рассматривать только их). Два класса эквивалентности относительно группы сдвигов векторных функций назовем *подходящими*, если их представители образуют допустимые пары. Используем сокращение “экв.” для эквивалентности относительно группы сдвигов. Вычислительно получены следующие результаты, где F и G — функции от n переменных:

- $n = 2$: 12 классов экв. APN-функций мощности 16;
 16 классов экв. функций порядка диф. равн. 4 мощности 4;
 F и G — APN-функции:
 Каждому классу подходят 3 других при 64 различных парах f, g ;
 F и G — порядка дифференциальной равномерности 4:
 Каждому классу подходят 6 других при 64 различных парах f, g ;
- $n = 3$: 10 752 классов экв. APN-функций мощности 64;
 169 344 классов экв. функций порядка диф. равн. 4 мощности 64;
 F и G — APN-функции:
 Каждому классу подходят 287 других:
 — 7 классов при 4096 различных парах f, g ;
 — 280 классов при 256 различных парах f, g ;
 F и G — порядка дифференциальной равномерности 4:
 Каждому классу подходят либо 56, либо 145 других, а именно:
 • 150528 классам подходит 56 других при 256 различных парах f, g ;
 • 18816 классам подходит 145 других:
 — 1 класс при 4096 различных парах f, g ;
 — 144 класса при 256 различных парах f, g ;
 Одна функция — APN, другая — порядка диф. равн. 4:
 Каждому классу APN-функций подходит 112 классов функций
 порядка диф. равн. 4 при 256 различных парах f, g .

5. Итеративный подход к построению APN-функций

Теорема 1 показывает, как можно строить APN-функции от n переменных из двух векторных и двух булевых функций от $n - 1$ переменных. А именно, необходимо выбрать две векторные функции от $n - 1$ переменных, каждая из которых — либо APN-функция, либо порядка дифференциальной равномерности 4, и проверить, существуют ли для них булевы функции f и g , при которых выполнены условия допустимости (*) и (**). Отметим, что основная сложность такого подхода заключается именно в выборе исходных векторных функций.

5.1. Допустимые векторные функции. В данном разделе приводятся некоторые утверждения, касающиеся выбора допустимых пар функций.

Определение 4. Пару векторных функций F и G от n переменных назовем *допустимой*, если существуют такие булевы функции f и g от n переменных, что набор F, G, f, g является допустимым.

Определение 5. Векторные функции F и G , действующие из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, назовем *эквивалентными относительно группы сдвигов*, если существуют такие векторы $c, d \in \mathbb{F}_2^n$, что $G(x) = F(x \oplus c) \oplus d$.

Следующее утверждение позволяет сократить перебор при выборе допустимых пар векторных функций для построения APN-функции с помощью теоремы 1, а именно, показывает, что в качестве допустимой пары достаточно рассматривать представители различных классов эквивалентности относительно группы сдвигов.

Утверждение 5. Пусть F и G — векторные функции от n переменных, $n \geq 2$. Тогда справедливы следующие утверждения:

(i) если F и G эквивалентны относительно группы сдвигов, то пара F и G не допустима;

(ii) если пара F и G допустима, то пара F' и G' , где $F'(x) = F(x \oplus c^1) \oplus d^1$ и $G'(x) = G(x \oplus c^2) \oplus d^2$, где $c^1, d^1, c^2, d^2 \in \mathbb{F}_2^n$, также является допустимой, и при этом все соответствующие булевы функции f', g' явно выражаются через f, g для F, G следующим образом: $f'(x) = f(x \oplus c^1)$ и $g'(x) = g(x \oplus c^2)$.

Доказательство. (i) Доказательство от противного. Предположим, что пара F и G допустима. В частности, существуют такие f и g , что выполнено условие (*) из определения.

По определению эквивалентности относительно группы сдвигов существуют такие $c, d \in \mathbb{F}_2^n$, что $G(x) = F(x \oplus c) \oplus d$ для всех $x \in \mathbb{F}_2^n$. С учетом этого выпишем условие (*): для всех $x, y, a \in \mathbb{F}_2^n$, $a \neq 0$, нарушается хотя бы одно из равенств: $F(x) \oplus F(x \oplus a) = F(y \oplus c) \oplus d \oplus F(y \oplus c \oplus a) \oplus d$, $f(x) \oplus f(x \oplus a) = g(y) \oplus g(y \oplus a)$. Заметим, что первое равенство всегда выполнено для любых $x, y = x \oplus c, a \neq 0$. Выберем три пары значений x, a и выпишем для функций f и g условия:

$$\begin{aligned} x = 0, \quad a = a^1, \quad a^1 \neq 0, \quad & f(0) \oplus f(a^1) = g(c) \oplus g(c \oplus a^1) \oplus 1; \\ x = 0, \quad a = a^2, \quad a^2 \neq 0, \quad a^1, & f(0) \oplus f(a^2) = g(c) \oplus g(c \oplus a^2) \oplus 1; \\ x = a^1, \quad a = a^1 \oplus a^2, & f(a^1) \oplus f(a^2) = g(c \oplus a^1) \oplus g(c \oplus a^2) \oplus 1. \end{aligned}$$

Если сложить по модулю 2 уравнения из первых двух условий и сравнить результат с третьим, то получим противоречие. Следовательно, таких f и g не существует для F и G , т.е. пара F и G не допустима.

(ii) Пусть для допустимой пары F и G существует в точности k пар булевых функций $f_i, g_i, i = 1, \dots, k$, при которых выполнены условия допустимости. Рассмотрим произвольную пару функций F' и G' , где $F'(x) = F(x \oplus c^1) \oplus d^1$ и $G'(x) = G(x \oplus c^2) \oplus d^2$ при $c^1, d^1, c^2, d^2 \in \mathbb{F}_2^n$. Тогда непосредственной подстановкой в условия (*) и (**) устанавливаем, что для F' и G' существуют соответствующие булевы функции f'_i и g'_i , где $f'_i(x) = f_i(x \oplus c^1)$ и $g'_i(x) = g_i(x \oplus c^2)$ и при этом только они. Действительно, если существует некоторая пара f', g' , не совпадающая для некоторого i с f'_i, g'_i , то пара $f(x) = f'(x \oplus c_1), g(x) = g'(x \oplus c_2)$ не будет совпадать с некоторой парой среди $f_i, g_i, i = 1, \dots, k$, что противоречит максимальной выборке k .

Следующее утверждение содержит эквивалентный критерий проверки допустимости пары двух APN-функций, не включающий в рассмотрение поиск соответствующих булевых функций.

Утверждение 6. Пара APN-функций F и G от n переменных допустима тогда и только тогда, когда для любого нечетного $k, k \geq 3$, не существует такого набора векторов x^i, y^i, a^i , где $a^i \neq 0, i = 1, \dots, k$, что

$$F(x^i) \oplus F(x^i \oplus a^i) = G(y^i) \oplus G(y^i \oplus a^i), \quad i = 1, \dots, k,$$

и в обоих наборах $x^i, x^i \oplus a^i, i = 1, \dots, k$, и $y^i, y^i \oplus a^i, i = 1, \dots, k$, каждый вектор встречается четное число раз.

Доказательство. По определению пара F и G допустима, если существуют булевы функции f и g , при которых выполнены условия допустимости (*). Рассмотрим

систему линейных булевых уравнений от 2^{n+1} неизвестных $f_x \stackrel{\text{def}}{=} f(x)$, $g_x \stackrel{\text{def}}{=} g(x)$, где $x \in \mathbb{F}_2^n$, состоящую из уравнений $f_x \oplus f_{x \oplus a} \oplus g_y \oplus g_{y \oplus a} = 1$ для всех тех x, y, a , при которых $F(x) \oplus F(x \oplus a) = G(y) \oplus G(y \oplus a)$. По построению, пара допустима тогда и только тогда, когда совместна построенная система уравнений относительно значений функций f и g . По известной теореме Кронекера — Капелли система линейных уравнений совместна тогда и только тогда, когда ранг матрицы системы равен рангу расширенной матрицы. В данном случае совместность рассматриваемой системы эквивалентна тому, что не найдется k различных уравнений системы, таких, что их сумма по модулю два приводит к уравнению вида $0 = 1$, что, в свою очередь, равносильно тому, что k нечетно и каждая переменная, входящая в данные уравнения встречается четное число раз.

Замечание 2. Если пара APN-функций F и G допустима, то значения соответствующих булевых функций f и g определяются как решение системы линейных уравнений, рассмотренной в доказательстве утверждения 6.

5.2. Квадратичные APN-функции. Для построения квадратичной APN-функции S от $n + 1$ переменных с помощью описанного выше метода в качестве двух исходных допустимых векторных функций F и G от n переменных необходимо брать квадратичные функции, которые в сумме дают аффинную функцию. Действительно, без ограничения общности можно рассматривать $S(x, x_{n+1}) = ((x_{n+1} \oplus 1)F(x) \oplus x_{n+1}G(x), (x_{n+1} \oplus 1)f(x) \oplus x_{n+1}g(x))$. Тогда по построению первые n координатных функций $x_{n+1}(F(x) \oplus G(x)) \oplus F(x)$ определяют квадратичную функцию тогда и только тогда, когда F — квадратичная и $F \oplus G$ — аффинная, следовательно, G также является квадратичной функцией. Отметим, что данное условие не является достаточным, так как $(n + 1)$ -я координатная функция S может не быть квадратичной функцией. Поскольку порядок дифференциальной равномерности инвариантен относительно прибавления аффинной функции, то в качестве F и G в этом случае следует рассматривать только функции одного порядка дифференциальной равномерности.

Утверждение 7. Пусть F — квадратичная APN-функция, а L — произвольная линейная функция от n переменных. Пусть существует в точности k различных ненулевых $a^i \in \mathbb{F}_2^n$, при которых $B_{a^i}(F) = B_{a^i}(F \oplus L)$. Тогда, если $k > 2^{n-1}$, то пара $F, F \oplus L$ не является допустимой.

Доказательство. Так как F — квадратичная APN-функция, то все ее производные аффинны, и, следовательно, множества $B_a(F) = \{F(x) \oplus F(x \oplus a) \mid x \in \mathbb{F}_2^n\}$ являются аффинными подпространствами размерности $n - 1$. Поскольку L — линейная функция, то $B_a(F \oplus L) = B_a(F) \oplus L(a)$, где под сложением вектора и множества понимается сложение всех элементов множества с данным вектором. Тогда для каждого ненулевого вектора a множества $B_a(F)$ и $B_a(F \oplus L)$ либо совпадают, либо не пересекаются. Поскольку по условию для $a^1, \dots, a^k$ множества совпадают, для любого x найдутся такие векторы $y^1, \dots, y^k$, что

$$F(x) \oplus F(x \oplus a^1) = F(y^1) \oplus F(y^1 \oplus a^1) \oplus L(a^1),$$

...

$$F(x) \oplus F(x \oplus a^k) = F(y^k) \oplus F(y^k \oplus a^k) \oplus L(a^k).$$

Если $k > 2^{n-1}$, то среди $2k$ векторов $y^i, y^i \oplus a^i, i = 1, \dots, k$, найдутся два одинаковых, например, $y^j = y^\ell = y$ (заметим, что $y^i \neq y^i \oplus a^i$ для любого i , так как $a^i \neq 0$). Тогда

$$F(x) \oplus F(x \oplus a^j) = F(y) \oplus F(y \oplus a^j) \oplus L(a^j),$$

$$F(x) \oplus F(x \oplus a^\ell) = F(y) \oplus F(y \oplus a^\ell) \oplus L(a^\ell),$$

$$F(x \oplus a^j) \oplus F(x \oplus a^\ell) = F(y \oplus a^j) \oplus F(y \oplus a^\ell) \oplus L(a^j \oplus a^\ell),$$

где третье равенство получается путем сложения по модулю 2 первых двух. Таким образом, по утверждению 6 получаем, что пара F и $F \oplus L$ не является допустимой.

Гипотеза 1. Для любой квадратичной APN-функции F существует такая линейная функция L , что пара F и $F \oplus L$ является допустимой.

В качестве подтверждения гипотезы 1 при малом числе переменных с помощью ЭВМ получено следующее утверждение.

Утверждение 8. Пусть $F_1, \dots, F_k$ — представители всех классов эквивалентности относительно группы сдвигов APN-функций от 3 переменных. Тогда для любой F_i существует в точности 35 функций $F_{i_1}, \dots, F_{i_{35}}$ таких, что пара F_i и F_{i_j} допустима и $F_i \oplus F_{i_j}$ — линейная функция для любого $j = 1, \dots, 35$. Аналогично для каждого представителя классов функций порядка дифференциальной равномерности 4 число допустимых представителей других классов, отличающихся на линейную функцию, равно либо 0, либо 1, либо 2.

Кроме того, для числа переменных $n = 4$ и $n = 5$ с помощью утверждения 6 найдены допустимые квадратичные APN-функции F и G , которые отличаются на линейную функцию, и соответствующие квадратичные f и g , которые также в сумме дают линейную. Ниже приведены такие примеры.

Пример 2. Случай $n = 4$:

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

$$G = (0 \ 8 \ 2 \ 11 \ 1 \ 11 \ 7 \ 12 \ 0 \ 12 \ 4 \ 9 \ 9 \ 7 \ 9 \ 6 \),$$

$$f = (1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \),$$

$$g = (1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \).$$

Случай $n = 5$:

$$\begin{aligned}
 F &= (\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 2 & 4 & 7 & 0 & 4 & 8 & 13 & 16 & 22 & 28 & 27 \\ 0 & 8 & 16 & 25 & 5 & 15 & 17 & 26 & 22 & 26 & 14 & 3 & 3 & 13 & 31 & 16 \end{array}), \\
 G &= (\begin{array}{cccccccccccccccc} 0 & 20 & 26 & 15 & 2 & 20 & 28 & 11 & 1 & 17 & 19 & 2 & 19 & 1 & 5 & 22 \\ 0 & 28 & 10 & 23 & 7 & 25 & 9 & 22 & 23 & 15 & 21 & 12 & 0 & 26 & 6 & 29 \end{array}), \\
 f &= (\begin{array}{cccccccccccccccc} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}), \\
 g &= (\begin{array}{cccccccccccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}).
 \end{aligned}$$

Автор выражает свою благодарность И. А. Круглову за внимательное прочтение и полезные замечания.

Список литературы

1. Глухов М. М., “О матрицах переходов разностей при использовании некоторых модулярных групп”, *Математические вопросы криптографии*, **4:4** (2013), 27–47.
2. Тужилин М. Э., “Почти совершенные нелинейные функции”, *Прикладная дискретная математика*, 2009, № 3, 14–20.
3. Bending T. D., Fon-der-Flaass D., “Crooked functions, bent functions, and distance regular graphs”, *Electron. J. Comb.*, **5** (1998).
4. Biham E., Shamir A., “Differential cryptanalysis of DES-like cryptosystems”, *J. Cryptology*, **4:1** (1991), 3–72.
5. Brinkman M., Leander G., “On the classification of APN functions up to dimension five”, *Proc. Int. Workshop on Coding and Cryptography 2007* (Versailles, France, 2007), 39–48.
6. Budaghyan L., *Construction and analysis of cryptographic functions*, Habilitation Thesis, Univ. of Paris 8, Sept. 2013.
7. Carlet C., “Open Questions on Nonlinearity and on APN Functions”, *Arithmetic of Finite Fields, Lecture Notes in Computer Science*, **9061** (2015), 83–107.
8. Carlet C., *Vectorial Boolean functions for cryptography*, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge Univ. Press, 2010, 398–472. <http://www.math.univ-paris13.fr/~carlet/pubs.html>
9. Carlet C., Charpin P., Zinoviev V., “Codes, bent functions and permutations suitable for DES-like cryptosystems”, *Designs, Codes and Cryptography*, **15:2** (1998), 125–156.
10. Charpin P., “On almost perfect nonlinear functions over F_2^n ”, *IEEE Trans. Inf. Theory*, **52:9** (2006), 4160–4170.
11. Daemen J., Rijmen V., *The Design of Rijndael: AES — Advanced Encryption Standard*, Springer, 2002, 256 pp.
12. Dillon J. F., “APN polynomials: an update”, *Proc. 9th Int. Conf. Finite Fields and Appl.* (Dublin, Ireland, July 2009), <http://mathsci.ucd.ie/~gm/Fq9Talks/Dillon.pdf>.
13. Dobbertin H., “Almost perfect nonlinear power functions on $GF(2^n)$: a new class for n divisible by 5”, *Proc. of Finite Fields and Appl. Fq5* (Berlin, Germany: Springer-Verlag, 2000), 113–121.
14. Dobbertin H., “Almost perfect nonlinear power functions over $GF(2n)$: the Niho case”, *Inf. and Comput.*, **151:1-2** (1999), 57–72.
15. Edel Y., “On quadratic APN functions and dimensional dual hyperovals”, *Designs, Codes and Cryptography*, **57:1** (2010), 35–44.
16. Nyberg K., “Differentially uniform mappings for cryptography”, *Eurocrypt 1993, Lect. Notes Comput. Sci.*, **765** (1994), 55–64.

17. Nyberg K., Knudsen L. R., “Provable security against a differential attack”, *J. Cryptology*, **8**:1 (1995), 27–37.
18. Yoshiara Y., “Notes on APN functions, semibiplanes and dimensional dual hyperovals”, *Designs, Codes and Cryptography*, **56**:2–3 (2010), 197–218.
19. Yu Y., Wang M., Li Y., “A matrix approach for constructing quadratic APN functions”, *Designs, Codes and Cryptography*, **73**:2 (2014), 587–600.

Статья поступила 28.08.2014.