

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

### ЛИНЕЙНЫЙ СПЕКТР КВАДРАТИЧНЫХ APN-ФУНКЦИЙ<sup>1</sup>

А. А. Городилова

*Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия*

Работа посвящена изучению почти совершенно нелинейных (APN) функций. Введено понятие линейного спектра квадратичной APN-функции; доказана теорема о нулевых значениях линейного спектра при чётном числе переменных; приведены вычислительные данные при малых значениях переменных  $n = 3, 4, 5, 6$ . Для известного класса APN-функций Голда  $F(x) = x^{2^k+1}$ , где  $(k, n) = 1$ , доказана теорема о крайнем значении линейного спектра.

**Ключевые слова:** APN-функция, ассоциированная булева функция, линейный спектр, функция Голда.

DOI 10.17223/20710410/34/1

### THE LINEAR SPECTRUM OF QUADRATIC APN FUNCTIONS

A. A. Gorodilova

*Sobolev Institute of Mathematics, Novosibirsk, Russia*

**E-mail:** gorodilova@math.nsc.ru

Almost perfect nonlinear (APN) functions are studied. We introduce the linear spectrum  $\Lambda^F = (\lambda_0^F, \dots, \lambda_{2^n-1}^F)$  of a quadratic APN function  $F$ , where  $\lambda_k^F$  equals the number of linear functions  $L$  such that  $|\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : B_a(F) = B_a(F+L)\}| = k$  and  $B_a(F) = \{F(x)+F(x+a) : x \in \mathbb{F}_2^n\}$ . We prove that  $\lambda_k^F = 0$  for all even  $k \leq 2^n - 2$  and for all  $k < (2^n - 1)/3$ , where  $F$  is a quadratic APN function in even number of variables  $n$ . Linear spectra for APN functions in small number of variables  $n = 3, 4, 5, 6$  are computed and presented. We consider APN Gold functions  $F(x) = x^{2^k+1}$  for  $(k, n) = 1$  and prove that  $\lambda_{2^n-1}^F = 2^{n+n/2}$  if  $n = 4t$  for some  $t$  and  $k = n/2 \pm 1$ , and  $\lambda_{2^n-1}^F = 2^n$  otherwise.

**Keywords:** APN function, associated Boolean function, linear spectrum, Gold function.

### Введение

Отображение  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  называется *почти совершенно нелинейной* функцией (APN-функцией), если для любых векторов  $a, b \in \mathbb{F}_2^n$ ,  $a \neq \mathbf{0}$ , уравнение  $F(x)+F(x+a) = b$  имеет не более двух решений. APN-функции ввели Л. Р. Кнудсен и К. Ньюберг

<sup>1</sup>Работа поддержана грантом РФФИ № 15-31-20635 и проектом РАН № 0314-2015-0011.

в работе [1], однако известно [2], что первый пример таких функций был указан В. А. Башевым и исследован Б. А. Егоровым в 1968 г. APN-функции интересны для использования в криптографических приложениях в силу их оптимальной стойкости к дифференциальному методу криптоанализа. Обзорам APN-функций посвящены работы М. Э. Тужилина [3] и А. Потта [4]. Некоторые открытые вопросы в области APN-функций представлены в работе К. Карле [5]. Например, открытому вопросу о существовании APN-подстановок посвящены работы М. М. Глухова [6] и В. Н. Сачкова [7].

Введём понятие линейного спектра квадратичной APN-функции. *Линейным спектром* квадратичной APN-функции  $F$  назовём вектор  $\Lambda^F = (\lambda_0^F, \dots, \lambda_{2^n-1}^F)$ , где  $\lambda_k^F$  — число линейных функций  $L$ , таких, что  $|\{a \in \mathbb{F}_2^n \setminus \{0\} : B_a(F) = B_a(F + L)\}| = k$ , где  $B_a(F) = \{F(x) + F(x + a) : x \in \mathbb{F}_2^n\}$ . Исследование линейного спектра представляется интересным в связи с подходом, описанным в [8], для поиска итеративной конструкции квадратичных APN-функций. Кроме того, отдельным вопросом стоит определение крайнего значения  $\lambda_{2^n-1}^F$  линейного спектра, что является подзадачей открытого вопроса, упомянутого в [5], о связи APN-функций  $F$  и  $G$ , для которых  $B_a(F) = B_a(G)$  для всех  $a$ . Настоящая работа посвящена изучению некоторых значений линейного спектра квадратичных APN-функций. Получены результаты о нулевых значениях линейного спектра, а также найдено крайнее значение линейного спектра для известного класса APN-функций Голда.

Основные определения и обозначения приведены в п. 1, где, в частности, для векторной булевой функции  $F$  определяется ассоциированная булева функция  $\gamma_F$ . В п. 2 доказана теорема о виде функции  $\gamma_F$  квадратичных APN-функций от чётного числа переменных. В п. 3 определено понятие линейного спектра  $\Lambda^F = (\lambda_0^F, \dots, \lambda_{2^n-1}^F)$  квадратичной APN-функции  $F$ . Доказано, что  $\lambda_k^F = 0$  для всех чётных  $0 \leq k \leq 2^n - 2$  и для всех  $0 \leq k < (2^n - 1)/3$  для любой квадратичной APN-функции от чётного числа переменных. Получены значения линейных спектров квадратичных APN-функций от малого числа переменных  $n = 3, 4, 5, 6$ . В п. 4 доказана теорема о крайнем значении линейного спектра  $\lambda_{2^n-1}^F$  для известного класса APN-функций Голда  $F(x) = x^{2^k+1}$ , где  $(k, n) = 1$ , а именно:  $\lambda_{2^n-1}^F = 2^{n+n/2}$ , если  $n = 4t$  для некоторого  $t$  и  $k = n/2 \pm 1$ , и  $\lambda_{2^n-1}^F = 2^n$  иначе. Вычислительно показано, что среди всех известных квадратичных APN-функций вплоть до 8 переменных функции  $F$ , для которых  $\lambda_{2^n-1}^F > 2^n$ , исключительны.

## 1. Определения

Пусть  $\mathbb{F}_2^n$  — множество всех двоичных векторов длины  $n$ ,  $\mathbf{0}$  — нулевой вектор,  $\mathbb{F}_{2^n}$  — конечное поле порядка  $2^n$ . Через  $+$  будем обозначать как покомпонентное сложение векторов из  $\mathbb{F}_2^n$  по модулю 2, так и операцию сложения в поле  $\mathbb{F}_{2^n}$  (из контекста будет видно, какая операция имеется в виду). Для  $x, y \in \mathbb{F}_2^n$  будем использовать обозначение  $\langle x, y \rangle = x_1y_1 + \dots + x_ny_n$ . *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 её значений. Через  $f|_M$  будем обозначать ограничение функции  $f$  на множество  $M \subseteq \mathbb{F}_2^n$ . *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.  $F = (f_1, \dots, f_m)$ . Для  $F$  справедливо однозначное представление в виде *алгебраической нормальной формы* (АНФ):  $F(x_1, \dots, x_n) = \sum_{k=1}^n \sum_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \dots x_{i_k} + a_0$ , 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 её АНФ, при котором стоит ненулевой коэффициент. Функции степени не выше 1 называются *аффинными* (в случае  $a_0 = \mathbf{0}$  — *линейными*), степени 2 — *квадратичными*.

*Спектр Уолша — Адамара* булевой функции  $f$  от  $n$  переменных состоит из коэффициентов  $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle u, x \rangle}$ , где  $u \in \mathbb{F}_2^n$ .

Говорят, что две векторные функции  $F, G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  *EA-эквивалентны*, если существуют аффинные взаимно однозначные функции  $A', A'' : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  и аффинная функция  $A : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ , такие, что  $G = A' \circ F \circ A'' + A$ .

Векторную булеву функцию  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  можно рассматривать как функцию над конечным полем  $\mathbb{F}_{2^n}$  и однозначно представлять в виде полинома степени не выше  $2^n - 1$ :  $F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i$ , где  $\delta_i \in \mathbb{F}_{2^n}$ . При этом степень функции равна  $\max\{\text{wt}(i) : \delta_i \neq 0\}$ , где  $\text{wt}(i)$  — двоичный вес числа.

*Циклотомическим классом* числа  $t$  по модулю  $2^n - 1$  называется множество  $C(t) = \{2^j t \bmod (2^n - 1) : 0 \leq j < n\}$ . Функция *след*, действующая из  $\mathbb{F}_{2^n}$  в  $\mathbb{F}_2$ , определяется следующим образом:  $\text{tr}(x) = x + x^2 + x^{2^2} + \dots + x^{2^{n-1}}$ .

**Определение 1** [1]. Отображение  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  называется *почти совершенно нелинейной функцией* (APN-функцией), если для любых векторов  $a, b \in \mathbb{F}_2^n$ ,  $a \neq \mathbf{0}$ , уравнение  $F(x) + F(x + a) = b$  имеет не более двух решений.

**Определение 2** [9]. Для векторной функции  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  *ассоциированной булевой функцией*  $\gamma_F$  от  $2n$  переменных называется функция, определённая по правилу:  $\gamma_F(a, b) = 1$ ,  $a, b \in \mathbb{F}_2^n$ , если  $a \neq \mathbf{0}$  и уравнение  $F(x) + F(x + a) = b$  имеет решение, и  $\gamma_F(a, b) = 0$  иначе.

Легко видеть, что  $F$  — APN-функция от  $n$  переменных тогда и только тогда, когда  $\text{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$ .

## 2. Свойства ассоциированной булевой функции

Пусть  $F$  — квадратичная APN-функция от  $n$  переменных. Тогда множество  $B_a(F) = \{F(x) + F(x + a) : x \in \mathbb{F}_2^n\}$  — аффинное подпространство размерности  $n - 1$  для любого  $a \neq \mathbf{0}$ . Следовательно,  $B_a(F) = L_a(F) + y_a(F)$ , где  $L_a(F)$  — линейное подпространство;  $y_a(F)$  — вектор (определяется не однозначно). Множества  $B_a(F)$  можно представить с помощью функций  $\Phi_F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ ,  $\varphi_F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  в виде

$$B_a(F) = \{y \in \mathbb{F}_2^n : \langle \Phi_F(a), y \rangle = \varphi_F(a)\},$$

где  $\Phi_F(\mathbf{0}) = \mathbf{0}$ ,  $\varphi_F(\mathbf{0}) = 1$ . Отметим, что  $\varphi_F(a) = 0$  тогда и только тогда, когда  $B_a(F) = L_a(F)$  — линейное (эквивалентно, когда  $y_a(F) \in L_a(F)$ ).

В обозначениях выше функция  $\gamma_F$  имеет вид  $\gamma_F(a, b) = \langle \Phi_F(a), b \rangle + \varphi_F(a) + 1$ .

**Утверждение 1.** Пусть  $F$  — квадратичная APN-функция от  $n$  переменных и  $\Phi_F(a) = \Phi_F(b)$  для некоторых векторов  $a, b \in \mathbb{F}_2^n$ . Тогда  $\Phi_F(a) = \Phi_F(a + b)$ .

*Доказательство.* Поскольку  $\Phi_F(a) = \Phi_F(b)$ , то  $L_a(F) = L_b(F)$ , где  $L_a(F)$  — линейная часть  $B_a(F)$ :  $L_a(F) = B_a(F) + F(\mathbf{0}) + F(a)$ . Рассмотрим  $L_{a+b}(F)$ :

$$\begin{aligned} L_{a+b}(F) &= \{F(x + a) + F(x + b) + F(a) + F(b) : x \in \mathbb{F}_2^n\} = \\ &= \{F(x) + F(x + a) + F(\mathbf{0}) + F(a) + F(x) + F(x + b) + F(\mathbf{0}) + F(b) : x \in \mathbb{F}_2^n\}. \end{aligned}$$

Обозначим  $c_a(x) = F(x) + F(x + a) + F(\mathbf{0}) + F(a)$  и  $c_b(x) = F(x) + F(x + b) + F(\mathbf{0}) + F(b)$ . Тогда  $c_a(x) \in L_a(F)$  и  $c_b(x) \in L_b(F)$  для любого  $x \in \mathbb{F}_2^n$  и  $L_{a+b}(F) = \{c_a(x) + c_b(x) : x \in \mathbb{F}_2^n\} = L_a(F)$ , поскольку  $L_a(F) = L_b(F)$  и  $|L_{a+b}(F)| = 2^{n-1}$ . ■

Введём следующее обозначение:  $A_v^F = \{a \in \mathbb{F}_2^n : \Phi_F(a) = v\}$ ,  $v \in \mathbb{F}_2^n$ .

**Утверждение 2.** Пусть  $F$  — квадратичная APN-функция от  $n$  переменных. Тогда  $A_v^F \cup \{0\}$  — линейное подпространство для любого  $v \in \mathbb{F}_2^n$ ,  $v \neq 0$ , и  $A_0^F = \{0\}$ .

*Доказательство.* Прямое следствие утверждения 1 и того, что  $\Phi_F(0) = 0$ . ■

**Утверждение 3.** Пусть  $F$  — квадратичная APN-функция от  $n$  переменных. Тогда для любого  $v \in \mathbb{F}_2^n$  верно:  $\varphi_F(x)|_{A_v^F} = \langle c_v, x \rangle|_{A_v^F}$  для некоторого вектора  $c_v \in \mathbb{F}_2^n$ .

*Доказательство.* Пусть  $A_v^F$  непусто. По определению  $\Phi_F(a) = v$  для любого  $a \in A_v^F$ . Следовательно,  $L_a(F) = L_v$  для всех  $a \in A_v^F$ , где  $L_v = \{x \in \mathbb{F}_2^n : \langle x, v \rangle = 0\}$ . Тогда  $B_a(F) = L_v + y_a(F)$  для всех  $a \in A_v^F$ . Пусть  $a, b \in A_v^F$ , тогда по утверждению 1  $a + b \in A_v^F$ . Покажем, что  $\varphi_F(a + b) = \varphi_F(a) + \varphi_F(b)$ . Действительно,  $\varphi_F(a + b) = 0$  тогда и только тогда, когда  $y_{a+b}(F) \in L_v$ , что, в свою очередь, эквивалентно тому, что  $y_a(F) + y_b(F) \in L_v$ . ■

Известно [9], что при нечётном числе переменных  $\Phi_F$  — взаимно однозначная функция, поэтому все  $A_v^F$ ,  $v \in \mathbb{F}_2^n$ , — различные одноэлементные множества. Для чётного числа переменных получена следующая теорема.

**Теорема 1.** Пусть  $F$  — квадратичная APN-функция от  $n$  переменных,  $n$  чётно. Тогда для любого  $v \in \mathbb{F}_2^n$  размерность  $A_v^F \cup \{0\}$  чётна.

*Доказательство.*

**Шаг 1.** Известно [9], что коэффициенты Уолша — Адамара функций  $F$  и  $\gamma_F$  связаны соотношением (здесь  $F_v = \langle v, F \rangle$  — компонентная функция функции  $F$ )

$$W_{\gamma_F}(u, v) = 2^{2n} \delta(u, v) - (W_{F_v}(u))^2 + 2^n, \quad (1)$$

где  $\delta(u, v) = 1$  при  $(u, v) = (0, 0)$  и  $\delta(u, v) = 0$  иначе.

Поскольку нетрудно убедиться, что у APN-функций не может быть аффинных компонентных функций, то у квадратичной APN-функции  $F$  все компонентные функции квадратичны. Тогда [10]  $W_{F_v} \in \{0, \pm 2^{k_v}\}$  для любого  $v \neq 0$ , где  $k_v$  — целое число,  $n/2 \leq k_v \leq n - 1$ . Рассмотрим, какие значения принимает  $W_{\gamma_F}(u, v)$ , используя равенство (1).

Если  $v = 0$ :

— при  $u = 0$  выполнено  $W_{\gamma_F}(u, v) = 2^{2n} - 2^{2n} + 2^n = 2^n$ ;

— при  $u \neq 0$  выполнено  $W_{\gamma_F}(u, v) = 0 - 0 + 2^n = 2^n$ .

Если  $v \neq 0$ :

— при  $W_{F_v}(u) = 0$  выполнено  $W_{\gamma_F}(u, v) = 0 - 0 + 2^n = 2^n$ ;

— при  $W_{F_v}(u) = \pm 2^{k_v}$  выполнено  $W_{\gamma_F}(u, v) = 0 - 2^{2k_v} + 2^n = 2^n - 2^{2k_v}$ .

**Шаг 2.** С другой стороны,  $W_{\gamma_F}(u, v) = -2^n \sum_{a \in A_v^F} (-1)^{\varphi_F(a) + \langle u, a \rangle}$ .

Действительно, распишем  $W_{\gamma_F}$ , используя  $\gamma_F(a, b) = \langle b, \Phi_F(a) \rangle + \varphi_F(a) + 1$ :

$$\begin{aligned} W_{\gamma_F}(u, v) &= \sum_{a, b \in \mathbb{F}_2^n} (-1)^{\langle b, \Phi_F(a) \rangle + \varphi_F(a) + 1 + \langle u, a \rangle + \langle v, b \rangle} = - \sum_{a \in \mathbb{F}_2^n} (-1)^{\varphi_F(a) + \langle u, a \rangle} \sum_{b \in \mathbb{F}_2^n} (-1)^{\langle b, \Phi_F(a) \rangle + \langle v, b \rangle} = \\ &= \sum_{b \in \mathbb{F}_2^n} (-1)^{\langle v, b \rangle} - \sum_{a \in \mathbb{F}_2^n, a \neq 0} (-1)^{\varphi_F(a) + \langle u, a \rangle} \sum_{b \in \mathbb{F}_2^n} (-1)^{\langle b, \Phi_F(a) \rangle + \langle v, b \rangle}. \end{aligned}$$

Если  $v = 0$ , то  $W_{\gamma_F}(u, v) = 2^n - 0 = 2^n$ , так как  $\Phi_F(a) \neq 0$  при  $a \neq 0$ .

Если  $v \neq 0$ , то  $W_{\gamma_F}(u, v) = 0 - 2^n \sum_{a \in \mathbb{F}_2^n, \Phi_F(a) = v} (-1)^{\varphi_F(a) + \langle u, a \rangle}$ .

**Шаг 3.** Далее рассмотрим  $W_{\gamma_F}(u, v) = -2^n \sum_{a \in A_v^F} (-1)^{\varphi_F(a) + \langle u, a \rangle}$ . По утверждению 3  $\varphi_F|_{A_v^F}$  линейна. Следовательно, существует  $u'$ , такой, что  $\varphi_F(a)|_{A_v^F} \equiv \langle u', a \rangle|_{A_v^F}$ . Тогда  $W_{\gamma_F}(u', v) = -2^n |A_v^F|$ . По шагу 1 получаем единственно возможный случай:  $-2^n |A_v^F| = 2^n - 2^{2k_v}$ , что влечёт  $|A_v^F| + 1 = 2^{2k_v - n}$ , или  $\dim(A_v^F \cup \{0\}) = 2k_v - n$ . Так как  $n$  по условию чётно, получаем требуемое. ■

Таким образом, согласно теореме 1, при чётном числе переменных прообраз  $\Phi_F^{-1}(v)$  каждого ненулевого элемента  $v \in \mathbb{F}_2^n$  либо пустое множество, либо образует линейное подпространство чётной размерности без нулевого вектора.

### 3. Линейный спектр

Пусть  $F$  — квадратичная APN-функция от  $n$  переменных и  $L : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  — линейная функция. Тогда  $B_a(F + L) = B_a(F)$  или  $B_a(F + L) = \mathbb{F}_2^n \setminus B_a(F)$  для любого  $a \in \mathbb{F}_2^n$ .

Обозначим  $k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{0\} : B_a(F) = B_a(F + L)\}|$ . Если представить  $\gamma_F$  как  $\gamma_F(a, b) = \langle \Phi_F(a), b \rangle + \varphi_F(a) + 1$ , то  $\gamma_{F+L}(a, b) = \gamma_F(a, b + L(a)) = \langle \Phi_F(a), b \rangle + \langle \Phi_F(a), L(a) \rangle + \varphi_F(a) + 1$ . Тогда

$$k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{0\} : \langle \Phi_F(a), L(a) \rangle = 0\}|. \quad (2)$$

**Определение 3.** *Линейным спектром* квадратичной APN-функции  $F$  назовём вектор  $\Lambda^F = (\lambda_0^F, \dots, \lambda_{2^n-1}^F)$ , где  $\lambda_k^F$  — число линейных функций  $L$ , таких, что  $k_L^F = k$ .

Легко видеть, что из определения  $\sum_{k=0}^{2^n-1} \lambda_k^F = 2^{n^2}$ .

Понятие линейного спектра естественно возникает при изучении квадратичных APN-функций  $F$ , их конструкций и соответствующих им ассоциированных функций  $\gamma_F$ . Отметим два конкретных направления исследований APN-функций, для которых представляет интерес линейный спектр. В [8] описан подход для поиска итеративной конструкции APN-функций. В частности, для построения квадратичной APN-функции  $S$  от  $n + 1$  переменных с помощью данного метода в качестве двух исходных *допустимых* [8, определение 4] векторных APN-функций  $F$  и  $G$  от  $n$  переменных необходимо брать квадратичные функции, которые в сумме дают аффинную функцию, а именно:  $S(x, x_{n+1}) = ((x_{n+1} + 1)F(x) + x_{n+1}G(x), (x_{n+1} + 1)f(x) + x_{n+1}g(x))$ , где  $f, g$  — некоторые булевы функции от  $n$  переменных. Тогда по построению первые  $n$  координатных функций  $x_{n+1}(F(x) + G(x)) + F(x)$  определяют квадратичную функцию тогда и только тогда, когда  $F$  — квадратичная и  $F + G$  — аффинная, следовательно,  $G$  также является квадратичной функцией. Там же доказано утверждение [8, утверждение 7], которое в терминах данной работы формулируется так: пара функций  $F$  и  $F + L$  не допустима, где  $F$  — квадратичная APN-функция и  $L$  — линейная функция, если  $k_L^F > 2^{n-1}$ . Следовательно, перед тем как проверять условия допустимости, возникает вопрос, а какие значения могут принимать  $k_L^F$ ?

Другое направление связано с понятием дифференциально эквивалентных APN-функций. Функции  $F$  и  $G$  называются *дифференциально эквивалентными* [11], если  $\gamma_F = \gamma_G$ . Описание классов дифференциальной эквивалентности является актуальной открытой задачей, которая возникает у многих специалистов [5], поскольку её решение может потенциально привести к новым конструкциям APN-функций. Тогда крайнее значение линейного спектра  $\lambda_{2^n-1}^F$  квадратичной APN-функции  $F$  отвечает за то, сколько существует дифференциально эквивалентных  $F$  функций, отличающихся от  $F$  на линейную функцию.

Кроме того, по следующему утверждению 4 линейный спектр является ЕА-инвариантом, следовательно, может быть использован для проверки неэквивалентности относительно ЕА-преобразования.

**Утверждение 4.** Линейный спектр квадратичной АРН-функции инвариантен относительно ЕА-преобразования.

*Доказательство.* Пусть  $G = A' \circ F \circ A'' + A$ , где  $F, G$  — квадратичные АРН-функции от  $n$  переменных,  $A', A''$  — взаимно однозначные аффинные функции,  $A$  — аффинная функция. Тогда  $B_a(G) = A'(B_{A''(a)+A''(0)}(F)) + A'(\mathbf{0}) + A(a) + A(\mathbf{0})$ . Следовательно, для любой линейной функции  $L$  верно, что  $k_L^F = k_L^G$ , поскольку  $B_a(F) = B_a(F + L)$  тогда и только тогда, когда  $B_a(G) = B_a(G + L')$ , где  $L'(x) = A'(L(x)) + A'(\mathbf{0})$ . Так как  $A'$  — взаимно однозначная функция,  $L'$  пробегает все возможные линейные функции при переборе всех возможных линейных функций  $L$ . Таким образом, по определению линейного спектра  $\Lambda^F = \Lambda^G$ . ■

Справедливо следующее утверждение о крайнем значении линейного спектра.

**Утверждение 5.** Пусть  $F$  — квадратичная АРН-функция от  $n$  переменных,  $n > 1$ . Тогда  $\lambda_{2^n-1}^F \geq 2^n$ .

*Доказательство.* Рассмотрим  $L_c(x) = F(x) + F(x+c) + F(\mathbf{0}) + F(c)$  для произвольного  $c \in \mathbb{F}_2^n$ . Функции  $L_c$  линейны в силу квадратичности  $F$  и при этом  $\gamma_F \equiv \gamma_{F+L_c}$  для любого  $c \in \mathbb{F}_2^n$ . Кроме того, так как  $F$  — АРН-функция и  $n > 1$ , то все  $2^n$  функций  $L_c$ ,  $c \in \mathbb{F}_2^n$ , попарно различны. Следовательно,  $\lambda_{2^n-1}^F \geq 2^n$ . ■

Получена следующая теорема о нулевых значениях линейного спектра.

**Теорема 2.** Пусть  $F$  — квадратичная АРН-функция от  $n$  переменных,  $n$  чётно,  $n > 1$ . Тогда выполнены следующие утверждения:

- 1)  $\lambda_k^F = 0$  для всех чётных  $k$ ,  $0 \leq k \leq 2^n - 2$ ;
- 2)  $\lambda_k^F = 0$  для всех  $k$ ,  $0 \leq k < (2^n - 1)/3$ .

*Доказательство.* Пусть  $\gamma_F(a, b) = \langle \Phi_F(a), b \rangle + \varphi_F(a) + 1$ . Напомним, что  $A_v^F = \{a \in \mathbb{F}_2^n : \Phi_F(a) = v\}$  для любого  $v \in \mathbb{F}_2^n$ . По теореме 1 для любого  $v \in \mathbb{F}_2^n$  размерность  $A_v^F \cup \{\mathbf{0}\}$  чётна. Следовательно, минимально возможная ненулевая  $|A_v^F|$  равна 3. Кроме того, если  $|A_v^F| > 3$ , то  $A_v^F$  можно представить как объединение  $|A_v^F|/3$  линейных подпространств  $A_{v,i}^F$  размерности 2 без нулевого вектора,  $i = 1, \dots, |A_v^F|/3$ .

Пусть  $M \cup \{\mathbf{0}\}$  — линейное подпространство размерности 2, совпадающее либо с некоторым  $A_v^F$ , либо с  $A_{v,i}^F$  при  $|A_v^F| > 3$ . Заметим, что таких подпространств  $M$  в точности  $(2^n - 1)/3$ . Тогда  $\langle \Phi_F(a), L(a) \rangle|_M = \langle c, L(a) \rangle|_M$  — линейная функция, где  $c$  — некоторый вектор. Следовательно,  $\langle \Phi_F(a), L(a) \rangle|_M = 0$  либо для всех трёх векторов  $a \in M$ , либо только для одного. Так как число  $(2^n - 1)/3$  нечётно, то, согласно (2), с учётом рассуждений выше получаем, что  $k_L^F$  нечётно. Кроме того, поскольку для каждого  $M$  хотя бы для одного  $a \in M$  выполнено  $\langle \Phi_F(a), L(a) \rangle|_M = 0$ , то  $\lambda_k^F = 0$  для всех  $0 \leq k < (2^n - 1)/3$ . ■

**Замечание 1.** Строго говоря, оценку п. 2 теоремы 2 можно улучшить. Но для этого необходимо знать, каковы мощности  $A_v^F$  для квадратичной функции  $F$ . Пусть сначала  $d = (2^n - 1)/3$ , тогда по п. 2 теоремы 2  $\lambda_k^F = 0$  для всех  $0 \leq k < d$ . Просматривая  $v \in \mathbb{F}_2^n$ , заменяем текущее число  $d$  на  $d - |A_v^F|/3 + 2^{\dim(A_v^F \cup \{\mathbf{0}\}) - 1} - 1$ , как только  $|A_v^F| > 3$  для некоторого  $v \in \mathbb{F}_2^n$ , поскольку в доказательстве теоремы вместо подпространств  $A_{v,i}^F$ ,  $i = 1, \dots, |A_v^F|/3$ , можно по аналогии рассмотреть всё множество  $A_v^F$ . Рассмотрев все возможные  $v$ , получим итоговую оценку:  $\lambda_k^F = 0$  для всех  $0 \leq k < d$ .

**Замечание 2.** Вычислительно найдены линейные спектры всех представителей классов EA-эквивалентности квадратичных APN-функций от  $n$  переменных для  $n = 3, 4, 5, 6$  (табл. 1–4). Для этих размерностей классификация всех квадратичных APN-функций известна полностью [12–14]. Представителей классов EA-эквивалентности можно найти в работе [12] (функция № 13 в [12, табл. 5] не является квадратичной). Вычисления для  $n = 6$  проводились на кластере НКС-30Т ССКЦ СО РАН. Отметим, что для  $n = 5$  спектры различных представителей попарно различны, а при  $n = 6$  существует два класса (№ 3 и 10), спектры которых совпадают. Кроме того, оценка из п. 2 теоремы 2 с учётом замечания 1 является точной для рассмотренных  $n$ . Замечание 1 реализуется лишь для одного класса при  $n = 6$ : для функции № 11 существует одно множество  $A_v^F$  мощности 15.

Таблица 1

**Линейный спектр квадратичных APN-функций от 3 переменных**

№	$\Lambda^F$							
1	0	56	0	280	0	168	0	8

Таблица 2

**Линейный спектр квадратичных APN-функций от 4 переменных**

№	$\Lambda^F$															
1	0	0	0	0	0	15552	0	25920	0	17280	0	5760	0	960	0	64

Таблица 3

**Линейные спектры квадратичных APN-функций от 5 переменных**

№	№ [12]	$\Lambda^F$															
1	1	0	0	0	0	0	5952	0	84320	0	605120	0	2737920	0	6249600	0	9663072
		0	8035200	0	4563200	0	1331264	0	252960	0	25792	0	0	0	0	0	32
2	2	0	0	0	0	0	6944	0	74400	0	649760	0	2618880	0	6457920	0	9413088
		0	8243520	0	4444160	0	1375904	0	243040	0	26784	0	0	0	0	0	32

**4. Крайнее значение линейного спектра APN-функций Голда**

Функцией Голда  $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$  называется мономиальная функция  $F(x) = x^{2^k+1}$ . Легко видеть, что функции Голда квадратичные. Известно [15], что при  $(k, n) = 1$  функция Голда является APN-функцией. Получим значение  $\lambda_{2^n-1}^F$  для произвольной APN-функции Голда. Приведём две вспомогательные леммы.

**Лемма 1.** Пусть  $n$  — натуральное число и  $P_k^i = 2^i - 2^k - 1$ , где  $i = 0, \dots, n - 1$  и  $k = 1, \dots, n - 1$ , за исключением  $k = n/2$  при чётном  $n$ . Тогда выполнены следующие утверждения:

- 1)  $P_k^0$  и  $P_k^k$  принадлежат одному циклотомическому классу по модулю  $2^n - 1$  (скажем,  $C$ ) при всех  $k$ ;
- 2)  $P_k^i$  и  $P_k^j$  принадлежат различным циклотомическим классам по модулю  $2^n - 1$ , отличным от  $C$ , при всех  $i \neq j$  и  $i, j \neq 0, k$ ;
- 3) если  $n$  нечётно, то  $|C(P_k^i)| = n$  для всех  $i$  и  $k$ ;
- 4) если  $n$  чётно, то  $|C(P_k^i)| = n$  для всех  $i$  и  $k$ , кроме  $|C(P_{n/2-1}^{n-1})| = |C(P_{n/2+1}^{k-1})| = n/2$ .

## Линейные спектры квадратичных APN-функций от 6 переменных

№	№ [12]	$\Lambda^F$							
1	1	00	00	00	00	00	00	00	00
		00	00	0 2565573	0 17869363	0 59537331	0 125825973	0 188763661	0 213866654
		0 190026141	0 135740661	0 79238211	0 38171835	0 15254095	0 5076811	0 1405263	0 325493
		0 62735	0 10311	0 1500	0 190	0 18	0 4	0 0	0 1
2	2	00	00	00	00	00	00	00	00
		00	00	0 2553543	0 17877699	0 59589621	0 125781705	0 188741889	0 213800958
		0 190121337	0 135798669	0 79173675	0 38162187	0 15236991	0 5094747	0 1409499	0 327285
		0 59859	0 11151	0 882	0 126	0 0	0 0	0 0	0 1
3	3	00	00	00	00	00	00	00	00
		00	00	0 2542806	0 17905671	0 59586660	0 125776980	0 188633340	0 213945417
		0 190123668	0 135775332	0 79089192	0 38209626	0 15282540	0 5048316	0 1425060	0 329238
		0 54684	0 11340	0 1890	0 63	0 0	0 0	0 0	0 1
4	4	00	00	00	00	00	00	00	00
		00	00	0 2554340	0 17874904	0 59587206	0 125810414	0 188677693	0 213867958
		0 190098845	0 135772125	0 79211561	0 38138853	0 15249741	0 5086925	0 1411959	0 326341
		0 62023	0 9639	0 1151	0 135	0 9	0 1	0 0	0 1
5	5	00	00	00	00	00	00	00	00
		00	00	0 2557241	0 17872451	0 59577007	0 125814360	0 188696571	0 213867180
		0 190078715	0 135775295	0 79212625	0 38139345	0 15258109	0 5082923	0 1411065	0 325759
		0 61833	0 9853	0 1346	0 128	0 16	0 1	0 0	0 1
6	6	00	00	00	00	00	00	00	00
		00	00	0 2560448	0 17872948	0 59553053	0 125832589	0 188720207	0 213854452
		0 190068147	0 135758015	0 79225563	0 38153459	0 15254401	0 5079821	0 1408589	0 325919
		0 62817	0 9957	0 1289	0 133	0 14	0 2	0 0	0 1
7	7	00	00	00	00	00	00	00	00
		00	00	0 2554224	0 17872307	0 59600606	0 125785578	0 188702449	0 213850382
		0 190100817	0 135791481	0 79195077	0 38133595	0 15258913	0 5085601	0 1412147	0 325797
		0 61795	0 9659	0 1255	0 126	0 13	0 1	0 0	0 1
8	8	00	00	00	00	00	00	00	00
		00	00	0 2567716	0 17858235	0 59557665	0 125814883	0 188753869	0 213881510
		0 190016913	0 135750653	0 79230265	0 38172707	0 15255327	0 5075247	0 1408231	0 323437
		0 63067	0 10415	0 1455	0 206	0 20	0 2	0 0	0 1
9	9	00	00	00	00	00	00	00	00
		00	00	0 2555995	0 17877082	0 59574886	0 125801851	0 188718247	0 213851252
		0 190094459	0 135757863	0 79214449	0 38150271	0 15253395	0 5080817	0 1412525	0 325359
		0 62017	0 9901	0 1312	0 131	0 11	0 0	0 0	0 1
10	10	00	00	00	00	00	00	00	00
		00	00	0 2542806	0 17905671	0 59586660	0 125776980	0 188633340	0 213945417
		0 190123668	0 135775332	0 79089192	0 38209626	0 15282540	0 5048316	0 1425060	0 329238
		0 54684	0 11340	0 1890	0 63	0 0	0 0	0 0	0 1
11	11	00	00	00	00	00	00	00	00
		00	00	00	0 10089045	0 53809170	0 134516080	0 209269815	0 227340608
		0 184963439	0 119789795	0 66717075	0 34914745	0 17946799	0 8758623	0 3769445	0 1351275
		0 395005	0 92041	0 16273	0 2310	0 275	0 5	0 0	0 1
12	12	00	00	00	00	00	00	00	00
		00	00	0 2579442	0 17845114	0 59521616	0 125838552	0 188808200	0 213899042
		0 189939792	0 135702744	0 79305436	0 38173660	0 15256304	0 5072200	0 1396584	0 327292
		0 62320	0 12040	0 1218	0 266	0 0	0 0	0 0	0 2
13	14	00	00	00	00	00	00	00	00
		00	00	0 2554106	0 17873083	0 59600915	0 125783545	0 188687890	0 213892662
		0 190078149	0 135762125	0 79218325	0 38152995	0 15239255	0 5085771	0 1413065	0 327485
		0 61575	0 9519	0 1237	0 110	0 10	0 0	0 1	0 1

Примечание. Все значения в таблице необходимо домножить на 64.

**Доказательство.**

1) Всюду далее под  $P_k^i$  будем подразумевать представителя смежного класса числа  $P_k^i$  по модулю  $2^n - 1$ , принадлежащего интервалу от 0 до  $2^n - 2$ . По определению двоичные веса чисел  $P_k^0 = -2^k$  и  $P_k^k = -1$  равны  $n - 1$ . Легко видеть, что все целые числа от 0 до  $2^n - 2$  двоичного веса  $n - 1$  принадлежат одному циклотомическому классу по модулю  $2^n - 1$  (скажем,  $C$ ) мощности  $n$ .

2) Рассмотрим все числа  $P_k^i$  и их двоичные представления (табл. 5). Числа  $P_k^1, \dots, P_k^{k-1}$  имеют двоичные веса  $n - k, \dots, n - 2$  соответственно. Следовательно, они принадлежат попарно различным циклотомическим классам по модулю  $2^n - 1$ , отличным от  $C$ . Аналогично, числа  $P_k^{k+1}, \dots, P_k^{n-1}$  принадлежат попарно различным циклотомическим классам по модулю  $2^n - 1$ , отличным от  $C$ , так как их двоичные веса пробегают значения от  $k$  до  $n - 2$  соответственно.

Таблица 5

Двоичные представления чисел  $P_k^i$

$i$	$P_k^i = 2^i - 2^k - 1 \pmod{(2^n - 1)} = (b_{n-1}, \dots, b_k, \dots, b_0) \in \mathbb{F}_2^n$	$\text{wt}(P_k^i)$
0	1 1 ... 1 1 <b>0</b> 1 1 ... 1 1 1 1 1	$n - 1$
1	1 1 ... 1 1 <b>1</b> 0 0 ... 0 0 0 0 0	$n - k$
2	1 1 ... 1 1 <b>1</b> 0 0 ... 0 0 0 1 0	$n - k + 1$
3	1 1 ... 1 1 <b>1</b> 0 0 ... 0 0 1 1 0	$n - k + 2$
...	...	...
$k - 1$	1 1 ... 1 1 <b>1</b> 0 1 ... 1 1 1 1 0	$n - 2$
$k$	1 1 ... 1 1 <b>1</b> 1 1 ... 1 1 1 1 0	$n - 1$
$k + 1$	0 0 ... 0 0 <b>0</b> 1 1 ... 1 1 1 1 1	$k$
$k + 2$	0 0 ... 0 1 <b>0</b> 1 1 ... 1 1 1 1 1	$k + 1$
...	...	...
$n - 1$	0 1 ... 1 1 <b>0</b> 1 1 ... 1 1 1 1 1	$n - 2$

Векторы двоичного представления чисел  $P_k^i$  содержат по две группы подряд идущих единиц длин  $n - k$  и  $i - 1$  при  $i = 1, \dots, k - 1$  и длин  $k$  и  $i - k - 1$  при  $i = k + 1, \dots, n - 1$ . Необходимым условием принадлежности двух таких чисел одному циклотомическому классу является равенство длин групп подряд идущих единиц. Следовательно, любые два числа в каждой из рассмотренных выше групп ( $P_k^1, \dots, P_k^{k-1}$  и  $P_k^{k+1}, \dots, P_k^{n-1}$ ) принадлежат различным циклотомическим классам. Действительно,  $n - k \neq k$  по условию леммы и  $n - k \neq i - k - 1$  для всех  $i = k + 1, \dots, n - 1$ .

3, 4) Согласно рассуждениям выше о двоичных представлениях чисел  $P_k^i$ , единственный возможный случай, когда  $|C(P_k^i)| \neq n$ , следующий: если длины групп подряд идущих единиц обе равны  $n/2 - 1$ . Если  $n$  нечётно, то этот случай реализоваться не может. Если  $n$  чётно, возможны следующие случаи:  $i = n - 1$  при  $k = n/2 - 1$  и  $i = k - 1$  при  $k = n/2 + 1$ . В обоих случаях  $P_k^i = 2^{n/2} P_k^i$  по модулю  $2^n - 1$ , что завершает доказательство. ■

**Лемма 2.** Пусть  $\ell$  — целое число,  $\ell > 1$ . Если  $\ell$  чётно, то  $(2\ell, \ell \pm 1) = 1$ ; если  $\ell$  нечётно, то  $(2\ell, \ell \pm 1) = 2$ .

**Доказательство.** Пусть  $(2\ell, \ell \pm 1) = d$ . Тогда  $2\ell = xd$  и  $\ell \pm 1 = yd$ , где  $(x, y) = 1$ . Выразая  $\ell$  из второго равенства и подставляя его в первое, получаем  $2 = (\mp x \pm 2y)d$ . Следовательно, единственно возможные случаи следующие:  $d = 1$  или  $d = 2$ . Тогда если  $\ell$  чётное, то  $\ell \pm 1$  нечётное и  $d = 1$ ; иначе  $d = 2$ . ■

Следующая теорема содержит основной результат о APN-функциях Голда.

**Теорема 3.** Пусть  $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$  — APN-функция Голда  $F(x) = x^{2^k+1}$ , где  $(k, n) = 1$ . Тогда выполнены следующие утверждения:

- 1)  $\lambda_{2^n-1}^F = 2^{n+n/2}$ , если  $n = 4t$  для некоторого  $t$  и  $k = n/2 \pm 1$ ;
- 2)  $\lambda_{2^n-1}^F = 2^n$  иначе.

**Доказательство.** Известно [9], что для APN-функции Голда  $F = x^{2^k+1}$  функция  $\gamma_F$  имеет следующий вид:  $\gamma_F(a, b) = \text{tr}((a^{2^k+1})^{-1}b) + \text{tr}(1) + 1$  при  $a \neq 0$  и  $\gamma_F(0, b) = 0$  для всех  $b \in \mathbb{F}_{2^n}$ . Следовательно,  $\Phi_F(a) = (a^{2^k+1})^{-1}$ .

Тогда для того, чтобы определить число  $\lambda_{2^n-1}^F$ , необходимо найти число  $N$  линейных функций  $L$ , таких, что  $k_L^F = 2^n - 1$ , или, согласно (2), таких, что

$$\text{tr}((a^{2^k+1})^{-1}L(a)) = 0 \quad (3)$$

для всех  $a \in \mathbb{F}_{2^n}$ .

Пусть  $L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}$  — линейная функция, где  $\delta_i \in \mathbb{F}_{2^n}$ ,  $i = 0, \dots, n-1$ . Тогда, подставляя выражение для  $L$  в (3), получаем цепочку равенств, выполненных для всех  $a \in \mathbb{F}_{2^n}$ :

$$\text{tr}((a^{2^k+1})^{-1}L(a)) = \text{tr}\left(\sum_{i=0}^{n-1} \delta_i a^{2^i} (a^{2^k+1})^{-1}\right) = \sum_{i=0}^{n-1} \text{tr}(\delta_i a^{2^i-2^k-1}) = 0.$$

Последнее равенство представляет собой полиномиальное уравнение от переменной  $a$  степени не выше  $2^n - 1$ , которое имеет  $2^n$  решений. Следовательно, коэффициенты при всех мономах равны 0. Определим вид коэффициентов при каждом из мономов  $x^d$ ,  $d = 0, \dots, 2^n - 1$ . Для этого рассмотрим циклотомические классы всех экспонент  $P_k^i = 2^i - 2^k - 1$ ,  $i = 0, \dots, n-1$ , для данного  $k$ . По лемме 1 (свойства 1, 2) существуют только две экспоненты  $P_k^0$  и  $P_k^k$ , принадлежащие одному циклотомическому классу по модулю  $2^n - 1$ . Следовательно,  $\delta_0$  и  $\delta_k$  связаны соотношением  $\delta_0 = (\delta_k)^{2^k}$  при всех  $n$ , так как  $P_k^0 = 2^k P_k^k \pmod{(2^n - 1)}$ . Далее рассмотрим несколько случаев.

**С л у ч а й 1.** Если  $n$  нечётно, то по лемме 1 (свойства 2 и 3) получаем  $\delta_i = 0$  при  $i \neq 0, k$ . Таким образом,  $N = 2^n$ , поскольку  $\delta_k$  может быть произвольным элементом  $\mathbb{F}_{2^n}$ .

Пусть  $n$  чётно,  $n = 2\ell$ . Рассмотрим два случая в зависимости от чётности  $\ell$ .

**С л у ч а й 2.** Если  $\ell$  нечётно, то  $(n, n/2 \pm 1) = 2$  по лемме 2. Следовательно, случай  $k = n/2 \pm 1$  не рассматривается по условию теоремы. Тогда  $\delta_i = 0$  при  $i \neq 0, k$  по лемме 1 (свойство 4). Аналогично случаю 1,  $N = 2^n$ .

**С л у ч а й 3.** Если  $\ell$  чётно, то по лемме 2  $(n, n/2 \pm 1) = 1$  и

- если  $k \neq n/2 \pm 1$ , то по лемме 1 (свойство 4) имеем  $\delta_i = 0$  при  $i \neq 0, k$ . Тогда  $N = 2^n$ ;
- если  $k = n/2 + 1$ , то по лемме 1 (свойство 4) имеем  $\delta_i = 0$  при  $i \neq 0, k-1, k$  и  $\delta_{k-1} = (\delta_k)^{2^{n/2}}$ . Так как число элементов  $x \in \mathbb{F}_{2^n}$ , удовлетворяющих уравнению  $x = x^{2^{n/2}}$ , равно  $2^{n/2}$ , получаем  $N = 2^{n+n/2}$ ;
- если  $k = n/2 - 1$ , то по лемме 1 (свойство 4) имеем  $\delta_i = 0$  при  $i \neq 0, k, n-1$  и  $\delta_{n-1} = (\delta_k)^{2^{n/2}}$ . Аналогично подслучаю выше,  $N = 2^{n+n/2}$ .

Теорема доказана. ■

**Замечание 3.** Согласно теореме 3, в классе APN-функций Голда существуют функции, для которых  $\lambda_{2^n-1}^F > 2^n$ . Проведённые вычислительные эксперименты (табл. 6) показывают, что среди всех известных квадратичных APN-функций вплоть до 8 переменных [12–14, 16] такие функции исключительны. Ими являются:

- $n = 4$ : APN-функция Голда  $x^3$ ;  
 $n = 6$ : APN-функция  $u^7x^3 + x^5 + u^3x^9 + u^4x^{10} + x^{17} + u^6x^{18}$ ;  
 $n = 8$ : APN-функция Голда  $x^9$ .

Таблица 6

Крайнее значение  $\lambda_{2^n-1}^F$  линейного спектра квадратичных APN-функций

$n$	Кол-во EA-классов	Значение $\lambda_{2^n-1}^F$
2	1	$2^2$
3	1	$2^3$
4	1	$2^6$
5	2	Для обоих классов: $2^5$
6	13	Для одного класса: $2^7$ ; для остальных 12 классов: $2^6$
7	$\geq 487$	Для всех известных 487 классов: $2^7$
8	$\geq 8179$	Для одного класса из известных 8179: $2^{12}$ Для остальных 8178 классов: $2^8$

### ЛИТЕРАТУРА

1. Nyberg K. and Knudsen L. R. Provable security against differential cryptanalysis // CRYPTO'92. LNCS. 1993. V. 740. P. 566–574.
2. Глухов М. М. О совершенно и почти совершенно нелинейных функциях // Математические вопросы криптографии. 2016. (в печати)
3. Тужилин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
4. Pott A. Almost perfect and planar functions // Des. Codes Cryptogr. 2016. V. 78. P. 141–195.
5. Carlet C. Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.
6. Глухов М. М. О матрицах переходов разностей при использовании некоторых модулярных групп // Математические вопросы криптографии. 2013. Т. 4. № 4. С. 27–47.
7. Сачков В. Н. Комбинаторные свойства дифференциально 2-равномерных подстановок // Математические вопросы криптографии. 2015. Т. 6. № 1. С. 159–179.
8. Городилова А. А. Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27. Вып. 3. С. 3–16.
9. Carlet C., Charpin P., and Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems // Des. Codes Cryptogr. 1998. V. 15. P. 125–156.
10. Carlet C. and Prouff E. On plateaued functions and their constructions // LNCS. 2003. V. 2887. P. 54–73.
11. Городилова А. А. О дифференциальной эквивалентности квадратичных APN-функций // Прикладная дискретная математика. Приложение. 2016. № 9. С. 21–24.
12. Brinkman M. and Leander G. On the classification of APN functions up to dimension five // Des. Codes Cryptogr. 2008. V. 49. Iss. 1. P. 273–288.
13. Browning K. A., Dillon J. F., Kibler R. E., and McQuistan M. T. APN polynomials and related codes // J. Combinatorics, Information and System Science. 2009. V. 34. No. 1–4. P. 135–159.
14. Edel Y. Quadratic APN functions as subspaces of alternating bilinear forms // Contact Forum Coding Theory and Cryptography III. Belgium, 2009. P. 11–24.
15. Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt'93. LNCS. 1994. V. 765. P. 55–64.

16. Yu Y., Wang M., and Li Y. A Matrix Approach for Constructing Quadratic APN Functions. Cryptology ePrint Archive, Report 2013/007. 2013.

## REFERENCES

1. Nyberg K. and Knudsen L. R. Provable security against differential cryptanalysis. CRYPTO'92, LNCS, 1993, vol. 740, pp. 566–574.
2. Glukhov M. M. O sovershenno i pochti sovershenno nelineynykh funktsiyakh [About perfectly and almost perfectly non-linear functions]. Matematicheskie Voprosy Kriptografii, 2016. (to be published) (in Russian)
3. Tuzhilin M. E. Pochti sovershennye nelineynye funktsii [APN-functions]. Prikladnaya Diskretnaya Matematika, 2009, no. 3, pp. 14–20. (in Russian)
4. Pott A. Almost perfect and planar functions. Des. Codes Cryptogr., 2016, vol. 78, pp. 141–195.
5. Carlet C. Open questions on nonlinearity and on APN functions. LNCS, 2015, vol. 9061, pp. 83–107.
6. Glukhov M. M. O matritsakh perekhodov raznostey pri ispol'zovanii nekotorykh modulyarnykh grupp [On the matrices of transitions of differences for some modular groups]. Mat. Vopr. Kriptogr., 2013, vol. 4, iss. 4, pp. 27–47. (in Russian)
7. Sachkov V. N. Kombinatornye svoystva differentsial'no 2-ravnomernykh podstanovok [Combinatorial properties of differentially 2-uniform substitutions]. Mat. Vopr. Kriptogr., 2015, vol. 6, iss. 1, pp. 159–179. (in Russian)
8. Gorodilova A. A. Kharakterizatsiya pochti sovershenno nelineynykh funktsiy cherez podfunktsii [Characteristics of almost perfectly non-linear functions by subfunctions]. Diskr. Mat., 2015, vol. 27, no. 3, pp. 3–16. (in Russian)
9. Carlet C., Charpin P., and Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr., 1998, vol. 15, pp. 125–156.
10. Carlet C., Prouff E. On plateaued functions and their constructions. LNCS, 2003, vol. 2887, pp. 54–73.
11. Gorodilova A. A. O differentsial'noy ekvivalentnosti kvadraticnykh APN-funktsiy [On differential equivalence of quadratic APN functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2016, no. 9, pp. 21–24. (in Russian)
12. Brinkman M. and Leander G. On the classification of APN functions up to dimension five. Des. Codes Cryptogr., 2008, vol. 49, iss. 1, pp. 273–288.
13. Browning K. A., Dillon J. F., Kibler R. E., and McQuistan M. T. APN polynomials and related codes. J. Combinatorics, Information and System Science, 2009, vol. 34, no. 1–4, pp. 135–159.
14. Edel Y. Quadratic APN functions as subspaces of alternating bilinear forms. Contact Forum Coding Theory and Cryptography III, Belgium, 2009, pp. 11–24.
15. Nyberg K. Differentially uniform mappings for cryptography. Eurocrypt'93, LNCS, 1994, vol. 765, pp. 55–64.
16. Yu Y., Wang M., and Li Y. A Matrix Approach for Constructing Quadratic APN Functions. Cryptology ePrint Archive, Report 2013/007, 2013.