

## О СИММЕТРИЧЕСКИХ СВОЙСТВАХ APN-ФУНКЦИЙ <sup>\*</sup>)

В. А. Виткуп<sup>1,2</sup>

<sup>1</sup>Институт математики им. С. Л. Соболева,  
пр. Коптюга, 4, 630090 Новосибирск, Россия

<sup>2</sup>Новосибирский гос. университет,  
ул. Пирогова, 2, 630090 Новосибирск, Россия  
e-mail: vvitkup@yandex.ru

**Аннотация.** Исследуются симметрические свойства APN-функций, а также структура и свойства множества значений произвольной APN-функции. Доказано, что не существует перестановки переменных, относительно которой APN-функция сохраняет свои значения. Доказаны верхние оценки на количество симметрических координатных булевых функций APN-функции и её координатных функций, инвариантных относительно циклического сдвига. При  $n \leq 6$  получены верхние оценки максимального числа одинаковых значений APN-функции и нижняя оценка числа различных значений произвольной APN-функции от  $n$  переменных. Библиогр. 14.

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

### Введение

Данная работа посвящена изучению свойств специальных векторных булевых функций. Векторные функции (S-блоки) выполняют роль основного нелинейного преобразования в блочных шифрах, и стойкость шифрования существенно зависит от их криптографических свойств.

Появление в 1990 г. дифференциального криптоанализа вызвало необходимость поиска функций, наиболее стойких к данному методу: так, в 1992 г. предложено понятие APN-функции, а затем и дифференциально  $\delta$ -равномерной функции. Векторная функция из  $\mathbb{F}_2^n$  в  $\mathbb{F}_2^n$  называется APN-функцией, если для любых  $a \neq 0$  и  $b$  из  $\mathbb{F}_2^n$  уравнение  $F(x) + F(x + a) = b$  имеет не более двух решений. APN-функции вызывают большой интерес у учёных, и много работ посвящено исследованию их свойств

---

<sup>\*</sup>)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 15–31–20635).

(см., например, [5, 7, 8, 9, 12, 13]). 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 (в [5] представлена полная классификация только до  $n = 5$ ) 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 наиболее его простых представителей таких, например, как функции с низкой алгебраической степенью, симметрические функции и т. д. Данная работа посвящена изучению симметрических представителей APN-функций и некоторых симметрических свойств функций и множества их значений.

В разд. 1 приводятся некоторые базовые определения и краткий обзор известных свойств APN-функций. В разд. 2 исследуется возможность существования симметрических представителей среди APN-функций (теорема 1) и доказываются верхние оценки числа координатных симметрических функций APN-функции (теорема 2) и координатных функций, инвариантных относительно циклического сдвига (теорема 3). В разд. 3 рассматриваются свойства множества значений APN-функции, приводится нижняя оценка числа различных значений таких функций (утверждение 2) и доказываются верхние оценки мощности множества векторов, на которых APN-функция принимает одно и то же значение (теорема 4).

## 1. Определения

*Векторной булевой функцией* (*S-блоком*)  $F$  называется произвольное отображение  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ . Векторную функцию можно рассматривать как набор из  $m$  координатных булевых функций от  $n$  переменных, т. е.  $F = (f_1, \dots, f_m)$ . Далее рассматриваются только функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ .

Для векторной булевой функции так же, как и для обычной функции, существует представление в виде АНФ, таблицы истинности и функции над полем. Остановимся подробнее на двух последних представлениях.

Множество  $\mathbb{F}_2^n$  можно рассматривать как конечное поле  $GF(2^n)$ , поэтому любой векторной булевой функции из  $\mathbb{F}_2^n$  в  $\mathbb{F}_2^n$  можно сопоставить функцию  $F : GF(2^n) \rightarrow GF(2^n)$ . Она однозначно (см., например, [8])

представляется в виде многочлена  $F(x) = \sum_{k=0}^{2^n-1} \delta_k x^k$  с коэффициентами из  $GF(2^n)$ .

Таблица истинности может быть представлена как в явной форме

(каждому двоичному вектору ставится в соответствие значение функции на этом векторе), так и в следующей альтернативной записи в виде вектора значений. Поскольку каждый вектор из  $\mathbb{F}_2^n$  является двоичным представлением некоторого целого неотрицательного числа, если упорядочить вектор значений в соответствии с лексикографическим порядком аргумента  $x_i$ , получим следующее однозначное представление векторной функции:  $F = (y_1 \ y_2 \ \dots \ y_n)$ , где  $y_i$  — десятичная запись  $F(x_i)$ .

В 1990 г. израильские криптоаналитики в [4] предложили новый метод взлома блочных шифров — дифференциальный криптоанализ. В его основе лежит анализ пар открытых текстов  $(P, P')$  и соответствующих им пар шифртекстов  $(C, C')$ , между которыми существуют разности или так называемые *дифференциалы*  $\Delta P = P + P'$  и  $\Delta C = C + C'$  на различных раундах симметричного шифрования.

В [13] введено характеристическое свойство для функций, наиболее стойких к этому виду криптоанализа, — дифференциальная  $\delta$ -равномерность. Векторная функция  $F$  называется *дифференциально  $\delta$ -равномерной*, если для любых  $a \neq 0$  и  $b$  уравнение  $F(x) + F(x + a) = b$  имеет не более  $\delta$  решений. APN-функцией (Almost Perfect Nonlinear) называется дифференциально 2-равномерная векторная функция. Также имеет место [3] следующее альтернативное определение APN-функции. Для векторной булевой функции  $F$  и произвольного вектора  $a \neq 0$  определим множество

$$B_a(F) = \{F(x) + F(x + a) \mid x \in \mathbb{Z}_2^n\}.$$

Функция  $F$  — APN-функция тогда и только тогда, когда для любого ненулевого  $a$  выполнено  $|B_a(F)| = 2^{n-1}$ .

На данный момент большая часть (см., например, [2]) известных конструкций APN-функций представляет собой мономиальные функции  $F(x) = x^d$  с различными условиями на показатель  $d$ . Например, *функции Касами* с показателем  $d = 2^{2i} - 2^i + 1$ , где  $(i, n) = 1$ , *функции Голда* с  $d = 2^i + 1$ , где  $(i, n) = 1$ , *инверсивная функция* с  $d = 2^{2i} - 1$  при  $n = 2i + 1$  и т. п. Известны результаты [1] о характеристизации APN-функций через подфункции специального вида.

Несмотря на большой интерес к классу APN-функций и многочисленные исследования существует много открытых вопросов [9] в данной области таких, как построение итеративных конструкций APN-функций, существование APN-функций с высокой нелинейностью от чётного числа переменных, проблема существования взаимно однозначной APN-функции при чётном  $n$ .

## 2. Симметрические свойства APN-функций

В силу сложности описания всего класса APN-функций естественно рассматривать свойства наиболее простых представителей этого класса таких, например, как функции с низкой алгебраической степенью, симметрические функции и т. п.

Здесь и далее результатом применения перестановки  $\pi$  к вектору  $x = (x_1, \dots, x_n)$  будем называть вектор  $\pi(x) = (x_{\pi(1)}, \dots, x_{\pi(n)})$ . Напомним определение симметрической функции в двоичном случае. Булева функция  $f$  от  $n$  переменных называется *симметрической*, если для любой перестановки  $\pi \in S_n$  для любых  $x_1, \dots, x_n$  выполнено  $f(x_1, \dots, x_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)})$ .

Можно заметить, что значение симметрической булевой функции  $f(x)$  зависит только от веса вектора  $x$ , следовательно, вектор значений и АНФ такой функции могут быть представлены в более компактном виде, что может быть полезно при аппаратной и программной реализации шифра.

Следующая теорема показывает, что не существует APN-функции, сохраняющей свои значения при произвольной перестановке переменных.

**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  $x \in \mathbb{F}_2^n$ .

**ДОКАЗАТЕЛЬСТВО.** Предположим, напротив, что существует перестановка  $\pi \in S_n$  такая, что для любого  $x$  справедливо  $F(x) = F(\pi(x))$ , т. е.  $F(x_1, \dots, x_n) = F(x_{\pi(1)}, \dots, x_{\pi(n)})$ .

Докажем, что для любой перестановки  $\pi$  существует ненулевой вектор  $a$  такой, что  $F(\pi(x) + a) = F(\pi(x + a))$ . Для этого достаточно выполнения равенства  $\pi(x) + a = \pi(x + a)$ .

Расписав подробнее последнее условие, получаем  $\pi(x) + a = (x_{\pi(1)} + a_1, \dots, x_{\pi(n)} + a_n)$ ,  $\pi(x + a) = (x_{\pi(1)} + a_{\pi(1)}, \dots, x_{\pi(n)} + a_{\pi(n)})$ , значит, равенство  $\pi(x) + a = \pi(x + a)$  эквивалентно системе уравнений

$$\begin{cases} a_1 = a_{\pi(1)}, \\ \dots \\ a_n = a_{\pi(n)}. \end{cases}$$

У этой системы из  $n$  уравнений с  $n$  неизвестными как минимум одно решение  $a = (1, 1, \dots, 1)$ .

Заметим, что существует вектор  $x^*$  такой, что  $\pi(x^*) \neq x^*$  и  $\pi(x^*) \neq x^* + a$ , где  $a = (1, 1, \dots, 1)$ . Действительно, случай, когда  $\pi(x^*) = x^* + a$ ,

возможен только при  $wt(x^*) = n/2$ . Так как перестановка  $\pi$  отлична от тождественной,  $j \neq \pi(j)$  хотя бы для одного индекса  $j$ , поэтому если у вектора  $x^*$  координата  $x_j$  не равна  $x_{\pi(j)}$ , то  $\pi(x^*) \neq x^*$ . Тем самым в качестве вектора  $x^*$  подойдёт любой вектор веса, отличного от  $n/2$ , в котором  $j$ -я и  $\pi(j)$ -я координаты различны.

Пусть  $F(x^*) + F(x^* + a) = b^*$  для  $a = (1, 1, \dots, 1)$  и  $x^* \in F_2^n$  (существование вектора  $x^*$  показано выше). Тогда  $F(\pi(x^*) + a) = F(\pi(x^* + a))$ , получаем противоречие с тем, что  $F$  — APN-функция, поскольку в этом случае

$$F(\pi(x^*)) + F(\pi(x^*) + a) = F(\pi(x^*)) + F(\pi(x^* + a)) = F(x^*) + F(x^* + a) = b^*,$$

что невозможно, так как  $|B_a(F)| = 2^{n-1}$ . Теорема 1 доказана.

В силу того, что не существует симметрической APN-функции, интересен вопрос о координатных булевых функциях APN-функции: могут ли они быть симметрическими функциями? Следующая теорема даёт ответ на этот вопрос.

**Теорема 2.** Пусть  $F$  — APN-функция из  $\mathbb{F}_2^n$  в  $\mathbb{F}_2^n$ ,  $F = (f_1, \dots, f_n)$ , где  $f_i$  — координатные булевы функции. Тогда среди  $f_1, \dots, f_n$  не более  $\lfloor n - \log_2 C_n^{\lfloor \frac{n-1}{2} \rfloor} \rfloor$  симметрических.

**ДОКАЗАТЕЛЬСТВО.** От противного. Пусть у нас  $\sigma(n)$  симметрических координатных функций  $f_1, \dots, f_{\sigma(n)}$  и  $\sigma(n) > \lfloor n - \log_2 C_n^{\lfloor \frac{n-1}{2} \rfloor} \rfloor$ , что эквивалентно  $C_n^{\lfloor \frac{n-1}{2} \rfloor} > 2^{n-\sigma(n)}$ . Для вектора из всех единиц рассмотрим следующую систему:

$$\begin{cases} f_1(x) + f_1(x+1) = b_1, \\ f_2(x) + f_2(x+1) = b_2, \\ \dots \\ f_{\sigma(n)}(x) + f_{\sigma(n)}(x+1) = b_{\sigma(n)}, \\ f_{\sigma(n)+1}(x) + f_{\sigma(n)+1}(x+1) = b_{\sigma(n)+1}, \\ \dots \\ f_n(x) + f_n(x+1) = b_n. \end{cases} \quad (1)$$

Возьмём произвольный вектор  $x$  веса  $\lfloor \frac{n-1}{2} \rfloor$ . Таких векторов ровно  $C_n^{\lfloor \frac{n-1}{2} \rfloor}$ . Заметим, что это максимальное количество векторов одного слоя таких, что  $wt(x) \neq wt(x+a)$ , и для любых таких двух векторов  $x', x''$  выполняется

$$f_i(x') + f_i(x' + a) = f_i(x'') + f_i(x'' + a) = b_i, \quad i = 1, \dots, \sigma(n).$$

Возможных вариантов значения вектора  $(b_{\sigma(n)+1}, \dots, b_n) - 2^{n-\sigma(n)}$ , однако количество векторов веса  $\lfloor \frac{n-1}{2} \rfloor$  больше чем  $2^{n-\sigma(n)}$ , поэтому согласно принципу Дирихле существуют хотя бы два вектора  $x_1$  и  $x_2$  веса  $\lfloor \frac{n-1}{2} \rfloor$  такие, что

$$\begin{aligned} F_a^*(x_1) &= (f_{\sigma(n)+1}(x_1) + f_{\sigma(n)+1}(x_1 + a), \dots, f_n(x_1) + f_n(x_1 + a)) \\ &= (b_{\sigma(n)+1}, \dots, b_n) = F_a^*(x_2). \end{aligned}$$

Так как для этих двух векторов значения первых  $\sigma(n)$  координатных функций совпадают ввиду их симметричности,  $F(x_1) + F(x_1 + a) = b$  и  $F(x_2) + F(x_2 + a) = b$  для некоторых  $x_1 \neq x_2$  таких, что  $x_1 + a \neq x_2$ ; противоречие тому, что  $F$  — APN-функция. Теорема 2 доказана.

Помимо симметрических булевых функций интерес в криптографии представляют также функции, которые сохраняют значения на всех циклических сдвигах координат вектора  $x$ , т. е.  $f(x_1, x_2, \dots, x_n) = f(x_2, \dots, x_n, x_1) = \dots = f(x_n, x_1, \dots, x_{n-1})$  для любого вектора  $x$  из  $F_2^n$  — так называемые *Rotation Symmetric Boolean functions* (RotS) [14]. Следующее утверждение даёт верхнюю оценку числа координатных RotS-функций у APN-функции.

**Теорема 3.** Пусть  $F$  — APN-функция от  $n$  переменных,  $F = (f_1, \dots, f_n)$ , где  $f_i$  — координатные булевы функции. Тогда среди  $f_1, \dots, f_n$  не более  $\lfloor n - \log_2 n \rfloor$  RotS-функций.

**ДОКАЗАТЕЛЬСТВО.** От противного. Пусть  $\rho(n)$  координатных функций  $f_1, \dots, f_{\rho(n)}$  являются RotS-функциями и выполнено  $\rho(n) > \rho(n) = \lfloor n - \log_2 n \rfloor$ , что эквивалентно  $n > 2^{n-\rho(n)}$ . По аналогии с предыдущим доказательством рассматриваем систему (1) и все векторы веса 1 — каждый из  $n$  таких векторов может быть получен с помощью циклического сдвига из любого другого. Возможных вариантов значения вектора  $(b_{t+1}, \dots, b_{\rho(n)})$  существует  $2^{n-\rho(n)}$ , однако количество векторов веса 1 больше чем  $2^{n-\rho(n)}$ , поэтому в силу принципа Дирихле существуют хотя бы два вектора  $x_1$  и  $x_2$ , отличающихся на некоторый сдвиг, таких, что

$$\begin{aligned} F_a^*(x_1) &= (f_{\rho(n)+1}(x_1) + f_{\rho(n)+1}(x_1 + a), \dots, f_n(x_1) + f_n(x_1 + a)) \\ &= (b_{\rho(n)+1}, \dots, b_n) = F_a^*(x_2). \end{aligned}$$

Следовательно,  $F(x_1) + F(x_1 + a) = b$  и  $F(x_2) + F(x_2 + a) = b$  для некоторых  $x_1 \neq x_2$  таких, что  $x_1 + a \neq x_2$ , и  $F$  не может быть APN-функцией. Теорема 3 доказана.

### 3. Множество значений APN-функции

Ввиду несуществования симметрической APN-функции и строгих ограничений на число её симметрических координатных функций возникают естественные вопросы: насколько далёк класс APN-функций от симметрических и насколько разнообразно множество значений такой функции? В данном разделе эти вопросы исследуются.

**3.1. Свойства множества значений APN-функции.** Известно, что при нечётных  $n$  существуют взаимно однозначные APN-функции, следовательно, максимально возможное число различных значений равно  $2^n$ , но при чётных  $n$  оно неизвестно. Следующее утверждение даёт нижнюю оценку числа различных значений произвольной APN-функции.

**Утверждение 1.** Любая APN-функция от  $n$  переменных принимает не менее  $\mu(n)$  различных значений, где

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

**ДОКАЗАТЕЛЬСТВО.** Согласно альтернативной формулировке определения APN-функции мощность множества  $B_a(F)$  равна  $2^{n-1}$ , где  $B_a(F) = \{F(x) + F(x + a) \mid x \in \mathbb{Z}_2^n\}$ . Пусть  $\mu(n)$  — мощность множества значений функции  $F$ . Заметим, что для того чтобы выполнялось условие на мощность  $|B_a(F)|$ , необходимо, чтобы  $C_{\mu(n)}^2 + 1 \geq 2^{n-1}$ . Отсюда

$$\frac{\mu(n)!}{2!(\mu(n) - 2)!} + 1 \geq 2^{n-1}, \quad \mu(n)(\mu(n) - 1) \geq 2^n - 2.$$

Решая квадратное неравенство, получаем  $\mu(n) \geq \frac{1 + \sqrt{2^{n+2} - 7}}{2}$ . Утверждение 1 доказано.

Пусть функция  $F$  принимает  $t$  различных значений  $y_1, \dots, y_t$ . Определим множество  $M_i = \{x \in F_2^n \mid F(x) = y_i\}$ .

Из теоремы 1 непосредственно получаем

**Следствие 1.** Если  $F$  — APN-функция от  $n$  переменных, принимающая  $t$  различных значений  $y_1, \dots, y_t$ , то множества  $M_i$ ,  $i = 1, \dots, t$ , не могут все одновременно являться слоями булева куба  $E^n$ .

Стоит заметить, что отдельно рассматриваемое множество  $M_i$ ,  $i \in \{1, \dots, t\}$ , может быть слоем в  $E^n$ . Например, у APN-функции от трёх переменных, заданной вектором значений  $(0, 4, 4, 7, 4, 5, 6, 0)$ , множество  $M_2 = \{x \in F_2^3 \mid F(x) = 4\}$  состоит из векторов 001, 010 и 100, образующих первый слой булева куба.

Из утверждения 1 естественно вытекает верхняя оценка мощности множества  $M_i$ .

**Следствие 2.** Пусть  $F$  — APN-функция от  $n$  переменных. Тогда

$$|M_{\max}| \leq 2^n - \mu(n) + 1,$$

где  $M_{\max}$  — максимальное по мощности множество  $M_i$ .

**ДОКАЗАТЕЛЬСТВО.** Заметим, что поскольку у функции должно быть не менее  $\mu(n)$  различных значений, в списке значений остаётся  $2^n - \mu(n)$  произвольных векторов, которые могут совпадать, поэтому возможный максимум количества совпадающих значений реализуется тогда, когда все эти  $2^n - \mu(n)$  векторов совпадают с одним из  $\mu(n)$  различных значений. Следствие 2 доказано.

К сожалению, эта оценка для достаточно больших  $n$  становится тривиальной, поэтому необходимо более тщательное исследование таких множеств и их максимально возможной мощности.

**3.2. Оценки числа одинаковых значений APN-функции.** Для произвольной APN-функции и любого её множества  $M_i$  справедливо следующее свойство.

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

**ДОКАЗАТЕЛЬСТВО.** От противного. Пусть для некоторого  $i$  найдутся четыре вектора  $v_r, v_j, v_l, v_s$  из  $M_i$  такие, что  $v_r + v_j + v_l + v_s = 0$ . Следовательно,  $v_r + v_j = v_l + v_s = a$ . Для вектора  $a$  рассмотрим множество  $B_a(F)$ . Для APN-функции выполняется  $|B_a(F)| = 2^{n-1}$ , но  $F(v_r) + F(v_r + a) = F(v_r) + F(v_j) = 0$  и  $F(v_l) + F(v_l + a) = F(v_l) + F(v_s) = 0$ , а значит, мощность  $B_a(F)$  меньше чем  $2^{n-1}$ . Утверждение 2 доказано.

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

**Теорема 4.** Пусть  $F$  — APN-функция от  $n$  переменных,  $n \leq 6$ . Тогда мощность  $|M_{\max}|$  не превышает числа  $\xi(n)$ , где  $\xi(n)$  принимает значения из следующей таблицы.

$n$	2	3	4	5	6
$\xi(n)$	3	4	6	7	11



ДОКАЗАТЕЛЬСТВО. Идея доказательства заключается в том, чтобы для каждого  $n$  найти максимально возможную мощность подмножества  $M$  векторов в  $\mathbb{F}_2^n$  такого, что  $v_r + v_j + v_l + v_s \neq 0$  для любых четырёх векторов  $v_r, v_j, v_l, v_s$ . Мощность этого подмножества и будет верхней оценкой на мощность  $|M_{\max}|$ .

Для каждой размерности  $n$  всегда можно выбрать  $n$  линейно независимых векторов. Пусть без ограничения общности это векторы  $e_1, \dots, e_n$  с единицей в соответствующей координате.

Для  $n = 2$  доказательство тривиально — само  $\mathbb{F}_2^2$  есть линейное пространство размерности 2, следовательно, все его четыре вектора входят в множество  $M_{\max}$  не могут, но для любых трёх векторов условие из утверждения 2 выполнено, следовательно,  $\xi(n) = 3$ .

Пусть  $n = 3$ . Рассмотрим все векторы в  $\mathbb{F}_2^3$ , разбив их в группы по весу:

$$\begin{aligned} wt(v) = 0 &: \{0\}, \\ wt(v) = 1 &: \{e_1, e_2, e_3\}, \\ wt(v) = 2 &: \{e_1 + e_2, e_2 + e_3, e_1 + e_3\}, \\ wt(v) = 3 &: \{e_1 + e_2 + e_3\}. \end{aligned}$$

Опишем общий алгоритм для любого  $n$ . В множество  $M_{\max}$  набираем все векторы веса 1 (как условились, без ограничения общности это произвольно выбранные векторы базиса). Далее, в каждой группе векторов удаляем векторы, которые с векторами внутри группы и базисными векторами образуют линейную комбинацию из четырёх векторов, равную нулю. Затем смотрим на выполнение условия для векторов между групп и удаляем те, которые ему не удовлетворяют. Оставшиеся векторы и будут образовывать максимальное по мощности множество, свободное от векторов таких, что  $v_r + v_j + v_l + v_s = 0$ .

Рассмотрим группу  $wt(v) = 2$ . Вектор  $e_1 + e_2$  не противоречит набору базисных векторов, поэтому можем его добавить в  $M_{\max}$ . Заметим, что выбор здесь проводился без ограничения общности, можно добавить первым любой другой вектор веса 2. Рассмотрим векторы  $e_2 + e_3$  и  $e_1 + e_3$  — в  $M_{\max}$  уже есть вектор  $e_1 + e_2$  и три базисных, и  $(e_2 + e_3) + (e_1 + e_2) + e_1 + e_3 = 0$ , равно как и  $(e_1 + e_3) + (e_1 + e_2) + e_2 + e_3 = 0$ , поэтому из векторов веса 2 только один может попасть в  $M_{\max}$ . Вектор нулевого веса не вступает в противоречие с базисными векторами. В группе  $wt(v) = 3$  единственный вектор  $e_1 + e_2 + e_3$  в сумме с тремя базисными векторами даёт 0, поэтому он тоже удаляется. Итого  $M_{\max} = \{0, e_1, e_2, e_3, e_1 + e_2\}$ , однако  $e_1 + e_2 + (e_1 + e_2) + 0 = 0$ , поэтому нулевой вектор удаляется из  $M_{\max}$ , следовательно,  $|M_{\max}| \leq 4$ .

Пусть  $n = 4$ . Имеем группы векторов

$$wt(v) = 0: \{0\},$$

$$wt(v) = 1: \{e_1, e_2, e_3, e_4\},$$

$$wt(v) = 2: \{e_1 + e_2, e_1 + e_3, e_1 + e_4, e_2 + e_3, e_2 + e_4, e_3 + e_4\},$$

$$wt(v) = 3: \{e_1 + e_2 + e_3, e_1 + e_2 + e_4, e_1 + e_3 + e_4, e_2 + e_3 + e_4\},$$

$$wt(v) = 4: \{e_1 + e_2 + e_3 + e_4\}.$$

Снова в  $M_{\max}$  помещаем базисные векторы и нулевой вектор и рассматриваем оставшиеся группы по весу. В группе  $wt(v) = 2$  без ограничения общности рассматриваем вектор  $e_1 + e_2$ , он не противоречит набору базисных векторов, поэтому помещаем его в  $M_{\max}$ . Тогда векторы  $e_1 + e_3$  и  $e_1 + e_4$  должны быть удалены, поскольку

$$(e_1 + e_2) + (e_1 + e_3) + e_2 + e_3 = 0, \quad (e_1 + e_2) + (e_1 + e_4) + e_2 + e_4 = 0.$$

Следующие два вектора  $(e_2 + e_3)$  и  $(e_2 + e_4)$  удаляются, поскольку для них выполнено  $(e_1 + e_2) + (e_2 + e_3) + e_1 + e_3 = 0$  и  $(e_1 + e_2) + (e_2 + e_4) + e_1 + e_4 = 0$ . Вектор  $e_3 + e_4$  не противоречит базисным векторам и вектору  $e_1 + e_2$ , поэтому добавляем его в  $M_{\max}$ . Таким образом, на данном этапе  $M_{\max} = \{0, e_1, e_2, e_3, e_4, e_1 + e_2, e_3 + e_4\}$ .

Рассмотрим группу  $wt(v) = 3$ . Заметим, что для любого вектора веса три всегда найдутся три базисных вектора, которые в сумме с ним дадут нуль, поэтому ни один вектор из этой группы не может попасть в  $M_{\max}$ . В последней группе всего один вектор  $e_1 + e_2 + e_3 + e_4$ , и он не противоречит базисным векторам, поэтому добавляем его в  $M_{\max}$ .

Теперь  $M_{\max}$  состоит из векторов  $0, e_1, e_2, e_3, e_4, e_1 + e_2, e_3 + e_4, e_1 + e_2 + e_3 + e_4$ . Однако заметим, что

$$(e_1 + e_2 + e_3 + e_4) + (e_1 + e_2) + e_3 + e_4 = 0,$$

$$(e_1 + e_2 + e_3 + e_4) + (e_3 + e_4) + e_1 + e_2 = 0,$$

поэтому вектор  $e_1 + e_2 + e_3 + e_4$  не может принадлежать  $M_{\max}$  (удаляем его, поскольку иначе придётся удалить оба вектора  $e_1 + e_2$  и  $e_3 + e_4$ , что противоречит максимальнойности множества). Тем не менее нулевой вектор мы вынуждены удалить, поскольку  $0 + e_1 + e_2 + (e_1 + e_2) = 0$  и  $0 + e_3 + e_4 + (e_3 + e_4) = 0$ , следовательно,  $|M_{\max}| \leq 6$ .

Для  $n = 5$  имеем группы векторов

$$wt(v) = 0: \{0\},$$

$$wt(v) = 1: \{e_1, e_2, e_3, e_4, e_5\},$$

$$wt(v) = 2: \{e_1 + e_2, e_1 + e_3, e_1 + e_4, e_1 + e_5, e_2 + e_3, e_2 + e_4, e_2 + e_5, e_3 + e_4, e_3 + e_5, e_4 + e_5\},$$

$$wt(v) = 3: \{e_1 + e_2 + e_3, e_1 + e_2 + e_4, e_1 + e_2 + e_5, e_1 + e_3 + e_4, e_1 + e_3 + e_5, e_1 + e_4 + e_5, e_2 + e_3 + e_4, e_2 + e_3 + e_5, e_2 + e_4 + e_5, e_3 + e_4 + e_5\},$$

$$wt(v) = 4: \{e_1 + e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_5, e_1 + e_2 + e_4 + e_5, e_1 + e_3 + e_4 + e_5, e_2 + e_3 + e_4 + e_5\},$$

$$wt(v) = 5: \{e_1 + e_2 + e_3 + e_4 + e_5\}.$$

Аналогично рассуждениям выше получаем, что нулевой вектор и вектор максимального веса в силу единственности в своей группе и непротиворечивости базисным векторам попадают в  $M_{\max}$  и ни один вектор веса 3 не может находиться в  $M_{\max}$ .

Рассмотрим группу  $wt(v) = 2$ . Как видели раньше, из этой группы в  $M_{\max}$  могут попадать только те представители, которые не пересекаются по составляющим базисным векторам, поскольку  $(e_i + e_j) + (e_i + e_k) + e_k + e_j = 0$ , поэтому из второй группы без ограничения общности берём векторы  $e_1 + e_2$  и  $e_3 + e_4$ . В группе  $wt(v) = 4$  можем без противоречий с базисными векторами взять любой вектор, например,  $e_1 + e_2 + e_3 + e_4$ , однако любой другой вектор пересекается с ним по трём составляющим базисным векторам, поэтому в силу свойства  $(e_{j_1} + e_{j_2} + e_{j_3} + e_{j_4}) + (e_{j_1} + e_{j_2} + e_{j_3} + e_{j_5}) + e_{j_4} + e_{j_5} = 0$  данный вектор единственный из группы веса 4, который может попасть в  $M_{\max}$ .

На данном этапе  $M_{\max}$  состоит из векторов  $0, e_1, e_2, e_3, e_4, e_5, e_1 + e_2, e_3 + e_4, e_1 + e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_4 + e_5$ , однако

$$(e_1 + e_2 + e_3 + e_4 + e_5) + (e_1 + e_2) + (e_3 + e_4) + e_5 = 0,$$

$$(e_1 + e_2 + e_3 + e_4 + e_5) + (e_1 + e_2 + e_3 + e_4) + e_4 + 0 = 0,$$

поэтому вектор веса 5 удаляется из  $M_{\max}$ . Аналогично  $(e_1 + e_2) + e_1 + e_2 + 0 = 0$  и  $(e_3 + e_4) + e_3 + e_4 + 0 = 0$ , поэтому удаляется нулевой вектор. Для вектора  $e_1 + e_2 + e_3 + e_4$  выполнено  $(e_1 + e_2 + e_3 + e_4) + (e_1 + e_2) + e_3 + e_4 = 0$ , поэтому в  $M_{\max}$  остаются только базисные векторы и два вектора веса 2, следовательно,  $|M_{\max}| \leq 7$  для  $n = 5$ .

Для  $n = 6$  имеем группы векторов

$$wt(v) = 0: \{0\},$$

$$wt(v) = 1: \{e_1, e_2, e_3, e_4, e_5, e_6\},$$

$$wt(v) = 2: \{e_1 + e_2, e_1 + e_3, e_1 + e_4, e_1 + e_5, e_1 + e_6, e_2 + e_3, e_2 + e_4, e_2 + e_5, e_2 + e_6, e_3 + e_4, e_3 + e_5, e_3 + e_6, e_4 + e_5, e_4 + e_6, e_5 + e_6\},$$

$$wt(v) = 3: \{e_1 + e_2 + e_3, e_1 + e_2 + e_4, e_1 + e_2 + e_5, e_1 + e_2 + e_6, e_1 + e_3 + e_4, e_1 + e_3 + e_5, e_1 + e_3 + e_6, e_1 + e_4 + e_5, e_1 + e_4 + e_6, e_1 + e_5 + e_6, e_2 + e_3 + e_4, e_2 + e_3 + e_5, e_2 + e_3 + e_6, e_2 + e_4 + e_5, e_2 + e_4 + e_6, e_2 + e_5 + e_6, e_3 + e_4 + e_5, e_3 + e_4 + e_6, e_3 + e_5 + e_6, e_4 + e_5 + e_6\},$$

$$\begin{aligned}
wt(v) = 4: & \{e_1 + e_2 + e_3 + e_4, e_1 + e_2 + e_3 + e_5, e_1 + e_2 + e_3 + e_6, e_1 + \\
& e_2 + e_4 + e_5, e_1 + e_2 + e_4 + e_6, e_1 + e_2 + e_5 + e_6, e_1 + e_3 + \\
& e_4 + e_5, e_1 + e_3 + e_4 + e_6, e_1 + e_3 + e_5 + e_6, e_1 + e_4 + e_5 + \\
& e_6, e_2 + e_3 + e_4 + e_5, e_2 + e_3 + e_4 + e_6, e_2 + e_3 + e_5 + e_6, \\
& e_2 + e_4 + e_5 + e_6, e_3 + e_4 + e_5 + e_6\}, \\
wt(v) = 5: & \{e_1 + e_2 + e_3 + e_4 + e_5, e_1 + e_2 + e_3 + e_4 + e_6, e_1 + e_2 + e_3 + e_5 + e_6, \\
& e_1 + e_2 + e_4 + e_5 + e_6, e_1 + e_3 + e_4 + e_5 + e_6, e_2 + e_3 + e_4 + e_5 + e_6\}, \\
wt(v) = 6: & \{e_1 + e_2 + e_3 + e_4 + e_5 + e_6\}.
\end{aligned}$$

Как и для предыдущих размерностей, базисные векторы и нулевой автоматически помещаются в  $M_{\max}$ , а векторы веса три полностью удаляются. Векторы веса два, имеющие пересечения, не могут быть одновременно помещены в  $M_{\max}$ , поэтому без ограничения общности в  $M_{\max}$  помещаются векторы  $e_1 + e_2$ ,  $e_3 + e_4$  и  $e_5 + e_6$ .

Рассмотрим группу  $wt(v) = 4$ . Без ограничения общности добавляем вектор  $e_1 + e_2 + e_3 + e_4$ . Векторы, которые пересекаются с ним по трём базисным векторам, не могут попасть в  $M_{\max}$ , поскольку  $(e_{j_1} + e_{j_2} + e_{j_3} + e_{j_4}) + (e_{j_1} + e_{j_2} + e_{j_3} + e_{j_5}) + e_{j_4} + e_{j_5} = 0$ , значит, удаляются векторы  $e_1 + e_2 + e_3 + e_5$ ,  $e_1 + e_2 + e_3 + e_6$ ,  $e_1 + e_2 + e_4 + e_5$ ,  $e_1 + e_2 + e_4 + e_6$ ,  $e_1 + e_3 + e_4 + e_5$ ,  $e_1 + e_3 + e_4 + e_6$ ,  $e_2 + e_3 + e_4 + e_5$  и  $e_2 + e_3 + e_4 + e_6$ . Заметим, что количество удалённых векторов не зависит от выбора первого вектора из группы, поэтому такое удаление корректно.

В группе  $wt(v) = 5$  можно взять только один вектор, поскольку все векторы в этой группе пересекаются друг с другом по четырём базисным векторам, а стало быть, для любой пары из  $wt(v) = 5$  найдутся два базисных вектора, сумма с которыми даст 0. Поэтому без ограничения общности берём вектор  $e_1 + e_2 + e_3 + e_4 + e_5$ . Единственный вектор веса 6 также оставляем.

На следующем этапе из  $M_{\max}$  удаляем вектор  $e_1 + e_2 + e_3 + e_4 + e_5 + e_6$ , поскольку в сумме с любым из векторов веса 4 и двумя базисными он даст 0. Вектор  $e_1 + e_2 + e_3 + e_4 + e_5$  также будет удалён, поскольку  $(e_1 + e_2 + e_3 + e_4 + e_5) + (e_1 + e_2) + (e_3 + e_4) + e_5 = 0$ . Нулевой вектор следует удалить для максимальности искомого множества, поскольку  $(e_1 + e_2 + e_3 + e_4) + (e_1 + e_2) + (e_3 + e_4) + 0 = (e_3 + e_4 + e_5 + e_6) + (e_3 + e_4) + (e_5 + e_6) + 0 = 0$ . После удалений в  $wt(v) = 4$  остались следующие векторы:  $e_1 + e_2 + e_3 + e_4$ ,  $e_1 + e_2 + e_5 + e_6$ ,  $e_1 + e_3 + e_5 + e_6$ ,  $e_1 + e_4 + e_5 + e_6$ ,  $e_2 + e_3 + e_5 + e_6$ ,  $e_2 + e_4 + e_5 + e_6$ ,  $e_3 + e_4 + e_5 + e_6$ , однако, вместе с векторами веса 2 они не могут попасть в  $M_{\max}$ , поскольку все они содержат либо сумму  $e_1 + e_2$ , либо  $e_5 + e_6$ , а значит, двумя базисными векторами мы всегда получим сумму четырёх векторов, равную нулю. Нужно понять, какие векторы удалять оптимальнее — векторы веса 2 или векторы веса 4. Заметим, что

из семи векторов веса 4 есть три комбинации, дающие нам 0: это суммы

$$(e_1 + e_3 + e_5 + e_6) + (e_1 + e_4 + e_5 + e_6) + (e_2 + e_3 + e_5 + e_6) + (e_2 + e_4 + e_5 + e_6) = 0,$$

$$(e_1 + e_2 + e_5 + e_6) + (e_1 + e_4 + e_5 + e_6) + (e_2 + e_3 + e_5 + e_6) + (e_3 + e_4 + e_5 + e_6) = 0,$$

$$(e_1 + e_2 + e_5 + e_6) + (e_1 + e_3 + e_5 + e_6) + (e_2 + e_4 + e_5 + e_6) + (e_3 + e_4 + e_5 + e_6) = 0.$$

Каждые две комбинации пересекаются по двум различным векторам, поэтому недостаточно будет удалить только один вектор, чтобы избежать пересечения, придётся удалить два, например, без ограничения общности, шестой и седьмой векторы. Запишем оставшееся множество векторов в виде матрицы, где строки суть имеющиеся векторы:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Как можно заметить, сумма никаких четырёх строк не равна нулю, поэтому убрать три вектора веса 2 оптимальнее, чем пять векторов веса 4. Следовательно, в  $M_{\max}$  остались только базисные векторы и пять векторов веса 4, описанных выше, и  $|M_{\max}| \leq 11$ . Теорема 4 доказана.

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

$$F = (0001) \text{ при } n = 2,$$

$$F = (0222365) \text{ при } n = 3,$$

$$F = (00010248036127162523073222819901981528219292) \text{ при } n = 5.$$

Для функции  $F = (0001024704638141013)$  достижима оценка  $\xi(n) - 1$  при  $n = 4$ .

Напомним, что вектор значений APN-функции приводится в лексикографическом порядке аргумента функции.

Стоит отметить интересное свойство множеств  $M_i$  для APN-функций Касами и Голда при чётных значениях  $n$  (определение функций приведено в разд. 1). Для любого  $i$  кроме нуля мощность  $M_i$  равна 3, а число различных значений функции равно  $\frac{2^n-1}{3}$ . Объяснение данного факта следует непосредственно из самой конструкции. Если рассмотреть следующие элементы поля  $GF(2^n)$ :  $x = \alpha^k$ ,  $x = \alpha^{k+\frac{2^n-1}{3}}$  и  $x = \alpha^{k+2\frac{2^n-1}{3}}$ ,

то можно заметить, что значение функции  $F$  на всех трёх переменных совпадает. Действительно, если  $F$  — функция Голда, то

$$\begin{aligned} F(\alpha^{k+\frac{2^n-1}{3}}) &= (\alpha^{k+\frac{2^n-1}{3}})^{2^i+1} = \alpha^{k(2^i+1)+(2^n-1)\frac{2^i+1}{3}} \\ &= \alpha^{k(2^i+1)} = F(\alpha^k) = F(\alpha^{k+2\frac{2^n-1}{3}}), \end{aligned}$$

поскольку  $(i, n) = 1$ , следовательно,  $i$  нечётно и  $2^i + 1$  делится на 3, а по свойствам  $GF(2^n)$  для любого  $x$  выполнено  $x^{2^n-1} = 1$ . Аналогично и для функций Касами, поскольку  $2^{2i} - 2^i + 1$  также делится на 3 для любых нечётных  $i$ .

Выражаю благодарность научному руководителю Н. Н. Токаревой, а также коллегам А. А. Городиловой, Н. А. Коломейцу и Г. И. Шушуеву за ценные замечания и полезные обсуждения.

## ЛИТЕРАТУРА

1. **Городилова А. А.** Характеризация почти совершенно нелинейных функций через подфункции // Дискрет. математика. 2015. Т. 27, № 3. С. 3–16.
2. **Тужилин М. Э.** Почти совершенные нелинейные функции // Прикл. дискрет. математика. 2009. № 3. С. 14–20.
3. **Beth T., Ding C.** On almost perfect nonlinear permutations // Advances in cryptology. Proc. Workshop Theory Appl. Cryptogr. Tech. (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer-Verl., 1994. P. 65–76. (Lect. Notes Comput. Sci.; Vol. 765).
4. **Biham E., Shamir A.** Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. Vol. 4, No. 1. P. 3–72.
5. **Brinkman M., Leander G.** On the classification of APN functions up to dimension five // Des. Codes Cryptogr. 2008. Vol. 49, No. 1–3. P. 273–288.
6. **Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J.** An APN permutation in dimension six // Proc. 9th Int. Conf. Finite Fields Appl. (Dublin, Ireland, July 13–17, 2009). AMS, 2010. P. 33–42. (Contemp. Math.; Vol. 518).
7. **Budaghyan L.** Construction and analysis of cryptographic functions. Cham, Switzerland: Springer-Verl., 2014. 168 p.
8. **Carlet C.** Vectorial Boolean functions for cryptography // Boolean models and methods in mathematics, computer science, and engineering. New York: Cambridge Univ. Press, 2010. P. 398–472. (Encycl. Math. Its Appl.; Vol. 134).
9. **Carlet C.** Open questions on nonlinearity and on APN functions // Arithmetic of finite fields. Proc. 5th Int. Workshop on the Arithmetic of Finite Fields (WAIFI 2014). (Gebze, Turkey, Sept. 27–28, 2014). Cham, Switzerland: Springer-Verl., 2015. P. 83–107. (Lect. Notes Comput. Sci.; Vol. 9061).

10. Carlet C., Charpin P., Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems // Des. Codes Cryptogr. 1998. Vol. 15, No. 2. P. 125–156.
11. Daemen J., Rijmen V. The Design of Rijdael: AES — the Advanced Encryption Standard. Heidelberg: Springer-Verl., 2002. 256 p.
12. Dobbertin H. Another proof of Kasami's theorem // Des. Codes Cryptogr. 1999. Vol. 17, No. 1–3. P. 177–180.
13. Nyberg K. Differentially uniform mappings for cryptography // Advances in cryptology. Proc. Workshop Theory Appl. Cryptogr. Tech. (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer-Verl., 1994. P. 55–64. (Lect. Notes Comput. Sci.; Vol. 765).
14. Pieprzyk J., Qu C. X. Fast hashing and rotation-symmetric functions // J. UCS. 1999. Vol. 5, No. 1. P. 20–31.

Виткуп Валерия Александровна

Статья поступила  
11 июня 2015 г.

Исправленный вариант —  
27 августа 2015 г.

DISKRETNYYI ANALIZ I ISSLEDOVANIE OPERATSII  
January–March 2016. Volume 23, No. 1. P. 65–81

UDC 519.7

DOI: 10.17377/daio.2016.23.498

## ON SYMMETRIC PROPERTIES OF APN FUNCTIONS

V. A. Vitkup<sup>1,2</sup>

<sup>1</sup>Sobolev Institute of Mathematics,  
4 Koptug Ave., 630090 Novosibirsk, Russia

<sup>2</sup>Novosibirsk State University,  
2 Pirogov St., 630090 Novosibirsk, Russia  
e-mail: vvitkup@yandex.ru

**Abstract.** We study symmetric properties of APN functions and the structure of their images. It is proven that there is no permutation of variables which keeps an APN function values. Upper bounds for the number of symmetric coordinate Boolean functions in APN function are obtained. Also, there are proven upper bounds for the number of coordinate Boolean functions of an APN function which are invariant under circular translation of indices. Upper bounds for the maximal number of coincidental values are obtained for  $n \leq 6$ . A lower bound for the number of different values of an arbitrary APN function is proven. Bibliogr. 14.

**Keywords:** vectorial Boolean function, APN function, symmetric function.

## REFERENCES

1. **A. A. Gorodilova**, A characterization of almost perfect nonlinear functions in terms of subfunctions, *Diskretn. Mat.*, **27**, No. 3, 3–16, 2015.
2. **M. E. Tuzhilin**, Almost perfect nonlinear functions, *Prikl. Diskretn. Mat.*, No. 3, 14–20, 2009.
3. **T. Beth** and **C. Ding**, On almost perfect nonlinear permutations, in T. Hellese, ed., *Advances in Cryptology — EUROCRYPT'93* (Proc. Workshop Theory Appl. Cryptogr. Tech., Lofthus, Norway, May 23–27, 1993), pp. 65–76, Springer-Verl., Heidelberg, 1994 (Lect. Notes in Comput. Sci., Vol. 765).
4. **E. Biham** and **A. Shamir**, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.*, **4**, No. 1, 3–72, 1991.
5. **M. Brinkman** and **G. Leander**, On the classification of APN functions up to dimension five, *Des. Codes Cryptogr.*, **49**, No. 1–3, 273–288, 2008.
6. **K. A. Browning**, **J. F. Dillon**, **M. T. McQuistan**, and **A. J. Wolfe**, An APN permutation in dimension six, in *Finite Fields: Theory and Applications*



- (Proc. 9th Int. Conf. Finite Fields Appl., Dublin, Ireland, July 13–17, 2009), pp. 33–42, AMS, 2010 (Contemp. Math., Vol. 518).
7. **L. Budaghyan**, *Construction and Analysis of Cryptographic Functions*, Springer-Verl., Cham, Switzerland, 2014.
  8. **C. Carlet**, Vectorial Boolean functions for cryptography, in Y. Crama and P. Hammer, eds., *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pp. 398–472, Cambridge Univ. Press, New York, 2010 (Encycl. Math. Its Appl., Vol. 134).
  9. **C. Carlet**, Open questions on nonlinearity and on APN functions, in *Arithmetic of Finite Fields* (Revised Sel. Pap. 5th Int. Workshop Arith. Finite Fields, Gebze, Turkey, Sept. 27–28, 2014), pp. 83–107, Springer-Verl., Cham, Switzerland, 2015. (Lect. Notes Comput. Sci., Vol. 9061).
  10. **C. Carlet**, **P. Charpin**, and **V. A. Zinoviev**, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.*, **15**, No. 2, 125–156, 1998.
  11. **J. Daemen** and **V. Rijmen**, *The Design of Rijndael: AES — The Advanced Encryption Standard*, Springer-Verl., Heidelberg, 2002.
  12. **H. Dobbertin**, Another proof of Kasami’s Theorem, *Des. Codes Cryptogr.*, **17**, No. 1–3, 177–180, 1999.
  13. **K. Nyberg**, Differentially uniform mappings for cryptography, in T. Helleseth, ed., *Advances in Cryptology — EUROCRYPT’93* (Proc. Workshop Theory Appl. Cryptogr. Tech., Lofthus, Norway, May 23–27, 1993), pp. 55–64, Springer-Verl., Heidelberg, 1994 (Lect. Notes Comput. Sci., Vol. 765).
  14. **J. Pieprzyk** and **Ch. X. Qu**, Fast hashing and rotation-symmetric functions, *J. UCS*, **5**, No. 1, 20–31, 1999.

Valeriya A. Vitkup

Received

11 April 2015

Revised

16 August 2015