УДК 519.7

О ПОСТРОЕНИИ APN-ПЕРЕСТАНОВОК С ПОМОЩЬЮ ПОДФУНКЦИЙ[1]

В. А. Идрисова

Институт математики им. С. Л. Соболева СО РАН,
Новосибирский государственный университет, г. Новосибирск, Россия

Работа посвящена проблеме существования взаимно однозначных APN-функций от чётного числа переменных. Рассматриваются векторные 2-в-1 функции, изоморфные $(n-1)$-подфункциям APN-перестановок, которые могут быть построены с помощью специального алгоритма. Для того чтобы получить APN-перестановку, необходимо найти координатные булевы функции f, такие, что взаимно однозначная функция, полученная из данной $(n-1)$-подфункции и функции f, является APN-функцией. Вводится понятие ассоциированных перестановок и доказывается оценка на число таких координатных булевых функций для некоторой $(n-1)$-подфункции. Описан соответствующий алгоритм поиска взаимно однозначных APN-функций с помощью подфункций и координатных булевых функций.

Ключевые слова: *векторная функция, APN-функция, перестановка, подфункция.*

DOI 10.17223/20710410/41/2

ON CONSTRUCTING APN PERMUTATIONS USING SUBFUNCTIONS

V. A. Idrisova

Sobolev Institute of Mathematics, Novosibirsk State University, Novosibirsk, Russia

E-mail: vitkup@math.nsc.ru

Our subject for investigation is the problem of APN permutation existence for even number of variables. In this work, we consider 2-to-1 functions that are isomorphic to $(n-1)$-subfunctions of APN permutations. These 2-to-1 functions can be obtained with a special algorithm which searches for 2-to-1 APN functions that are potentially EA-equivalent to permutations. The algorithm is based on constructing special symbol sequences that are called admissible. It is known that $(n-1)$-subfunction of an APN permutation can be represented as a differentially 4-uniform 2-to-1 function that takes values from the half of the Boolean cube. Therefore, the following algorithm can be used to search for APN permutations. On the first step all the possible admissible sequences are constructed and we assign obtained sequences in order to find a differentially 4-uniform 2-to-1 function. Therefore, obtained function can be isomorphic to a $(n-1)$-subfunction of an APN permutation, so, this $(n-1)$-subfunction can be expanded to bijective APN function. In order to construct an APN permutation, we need to find all possible coordinate Boolean functions f such that the bijective function constructed from the given $(n-1)$-subfunction S and function f is APN.

[1]Работа поддержана грантами РФФИ № 18-31-00374 и 18-07-01394, программой фундаментальных научных исследований СО РАН № I.5.1., проект № 0314-2016-0017, Министерством образования и науки (задание № 1.12875.2018/12.1) и в рамках программы 5-100.

Unfortunately, the exhaustive search through the set of potential coordinate functions is computationally hard when $n \geqslant 7$, so, we need to estimate the number $n(S)$ of such coordinate Boolean functions. For a given bijective vectorial function F, we introduce an associated permutation $F^\star$ as follows. We split the set $\mathbb{F}_2^n$ into two disjoint subsets $\mathcal{F}_1$ and $\mathcal{F}_2$, fix integer k, indices $i_1, \ldots, i_k$, and index $j \notin \{i_1, \ldots, i_k\}$. Then the value $F^\star(x)$ is equal to $F(x)$ if $F(x) \in \mathcal{F}_1$ and $F^\star(x)$ is equal to $F(x) + e_j$ otherwise. We prove that $F^\star$ is an APN permutation if and only if F is an APN permutation. This fact allows us to obtain the necessary bound. We prove that if $n(S)$ is not equal to zero, then $n(S) \geqslant 2^n$.

Keywords: *vectorial function, APN function, permutation, subfunction.*

Введение

Стойкость современных симметричных шифров существенно зависит от характеристик, которыми обладают их компоненты, в частности S-блоки. В общем случае S-блок представляет собой векторную функцию из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$. Многие широко используемые блочные шифры, такие, например, как AES, ГОСТ Р 34.12-2015 (Кузнечик), Serpent, являются по своей структуре SP-сетями. Важным свойством, требуемым от S-блоков в SP-сетях, является их обратимость, то есть векторная функция, используемая в качестве S-блока, должна быть взаимно однозначной.

Появление метода дифференциального криптоанализа в 1990 г. потребовало от S-блоков новых характеристик. Так, было введено понятие функций с низкой дифференциальной равномерностью и APN-функций — векторных функций, обладающих оптимальной стойкостью к дифференциальному криптоанализу. Одна из самых важных задач в области APN-функций заключается в необходимости совместить свойства взаимной однозначности и минимально возможной дифференциальной равномерности в одном S-блоке. Для нечётных n существует множество конструкций таких функций, однако для чётных размерностей до сих пор известен лишь один пример взаимно однозначной APN-функции от шести переменных.

Данная работа посвящена проблеме поиска и построения взаимно однозначных APN-функций. Рассматриваются 2-в-1 векторные функции, обладающие низкой дифференциальной равномерностью, которые могут быть получены специальным алгоритмом. Показано, что с помощью данных 2-в-1 функций возможен поиск новых APN-перестановок. В п. 1 вводятся основные определения и аппарат APN-функций, а также рассматриваются некоторые известные результаты, связанные с проблемой существования APN-перестановок. В п. 2.1 описывается алгоритм поиска APN-перестановок с помощью подфункций и недостающих координатных булевых функций и формулируется основная задача работы. В п. 2.2 рассматривается дифференциально 4-равномерная 2-в-1 векторная функция и доказывается нижняя оценка числа координатных булевых функций, таких, что перестановка, полученная из исходной 2-в-1 векторной функции и данной координатной булевой функции, является APN-функцией. Данная оценка позволяет понять, как много таких координатных функций существует и, следовательно, насколько быстро найдётся APN-перестановка в процессе работы алгоритма. Для произвольной взаимно однозначной функции вводится понятие ассоциированной перестановки. Доказывается, что некоторая перестановка является APN-функцией тогда и только тогда, когда её ассоциированная перестановка также является APN-функцией.

1. Определения

1.1. Основные определения

Будем обозначать через $\mathbb{F}_2^n$ множество всех двоичных векторов длины n. Функция F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, где n и m — целые числа, называется *векторной булевой функцией*. Если $m = 1$, то функция F называется *булевой*. Произвольная векторная функция F может быть представлена как набор из m *координатных функций* $F = (f_1, \ldots, f_m)$, где f_i — булева функция от n переменных. Для произвольного ненулевого вектора $v \in \mathbb{F}_2^m$ линейная комбинация координатных функций $v \cdot F$ называется *компонентной функцией*. Любую векторную булеву функцию F можно единственным образом представить в виде *алгебраической нормальной формы* (АНФ):

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

где $a_{i_1,\ldots,i_k}, a_0 \in \mathbb{F}_2^m$. *Алгебраической степенью* функции F называется количество переменных в самом длинном слагаемом её АНФ, при котором коэффициент не равен нулю. Если алгебраическая степень F не превышает единицы, то F называется *аффинной*. Аффинная функция F называется *линейной*, если $F(\mathbf{0}) = \mathbf{0}$.

Векторная булева функция F называется *уравновешенной*, если она принимает каждое значение из $\mathbb{F}_2^m$ ровно 2^{n-m} раз, в частности, булева функция *уравновешена*, или *сбалансирована*, если она принимает каждое значение 2^{n-1} раз. В случае $n = m$ уравновешенная функция F называется *взаимно однозначной,* или *перестановкой*. *Производной* функции F по направлению a называется векторная функция $D_a F(x) = F(x+a)+F(x)$, где a — ненулевой вектор из $\mathbb{F}_2^n$. *Вектором значений* для векторной функции F называется вектор $\big(F(x^{(1)}), \ldots, F(x^{(2^n)})\big)$, где $x^{(1)}, \ldots, x^{(2^n)}$ — лексикографически упорядоченные двоичные векторы из $\mathbb{F}_2^n$. Векторная функция F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ называется *2-в-1 функцией*, если она принимает 2^{n-1} различных значений, каждое из которых встречается в векторе значений ровно два раза.

Мы можем сопоставить векторному пространству $\mathbb{F}_2^n$ конечное поле $\mathrm{GF}(2^n)$ и рассматривать векторную булеву функцию как функцию над этим полем. Тогда любая векторная функция F единственным образом представляется над $\mathrm{GF}(2^n)$ в следующей форме:

$$F(x) = \sum_{i=0}^{2^n-1} \lambda_i x^i, \ \lambda_i \in \mathrm{GF}(2^n).$$

Векторные булевы функции F и G называются *расширенно аффинно эквивалентными* (*EA-эквивалентными*), если $F = A_1 \circ G \circ A_2 + A$, где A_1, A_2 — взаимно однозначные аффинные функции над $\mathbb{F}_2^n$ и A — аффинная функция. Если функции F и G являются EA-эквивалентными и $A \equiv \mathbf{0}$, то F и G называются *аффинно эквивалентными*. Рассмотрим ещё одно отношение эквивалентности [1] на множестве векторных булевых функций. Две функции F и G называются *CCZ-эквивалентными*, если соответствующие множества $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : y = F(x)\}$ и $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : y = G(x)\}$ являются аффинно эквивалентными, т. е. если существует аффинный автоморфизм $A = (A_1, A_2)$, такой, что $y = F(x) \Leftrightarrow A_2(x, y) = G(A_1(x, y))$.

1.2. Взаимно однозначные APN-функции

Рассмотрим векторную функцию F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Для векторов $a, b \in \mathbb{F}_2^n$, где $a \neq 0$, определим

$$\delta(a, b) = \big|\{x \in \mathbb{F}_2^n : F(x + a) + F(x) = b\}\big|, \quad \Delta_F = \max_{a \neq \mathbf{0}, b \in \mathbb{F}_2^n} \delta(a, b).$$

Функция F называется *дифференциально Δ_F-равномерной*. Чем меньше параметр Δ_F, тем выше стойкость шифра, содержащего F в качестве S-блока, к дифференциальному криптоанализу. Для векторных функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ наименьшее значение Δ_F равно 2. В этом случае функция F называется *почти совершенно нелинейной* (*APN-функцией*). Данные понятия введены К. Ньюберг в работе [3]. Если F является APN-функцией, то любая EA-эквивалентная/CCZ-эквивалентная функция также является APN-функцией.

Наиболее известные представители класса APN-функций — это мономиальные функции, то есть функции вида $F(x) = x^d$ (таблица) над конечным полем $\mathrm{GF}(2^n)$. Известно [12], что APN-функции изучались ещё в СССР. Так, например, в 1964 г. В. А. Башевым и Б. А. Егоровым было доказано, что инверсия элемента поля является APN-функцией. Несмотря на то, что класс APN-функций активно изучается, в данной области по-прежнему большое количество открытых вопросов. Для дальнейшего изучения темы рекомендуем, например, обзоры [12 – 16], книги [17, 18] и т.д.

Известные мономиальные APN-функции вида x^d над полем $\mathbf{GF}(2^n)$

Название	Значение d	Условия	Ссылки
Голда	2^t+1	$(t,n)=1$	[2, 3]
Касами	$2^{2t}-2^t+1$	$(t,n)=1$	[4, 5]
Уолша	2^t+3	$n=2t+1$	[6, 7]
Нихо	$2^t+2^{t/2}-1$, t чётное $2^t+2^{(3t+1)/2}-1$, t нечётное	$n=2t+1$	[8, 9]
Инверсия	$2^{2t}-1$	$n=2t+1$	[3, 10]
Доббертина	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$	[11]

Один из самых важных открытых вопросов в области APN-функций посвящён проблеме существования взаимно однозначных APN-функций, или *APN-перестановок*. В [19] выдвинута гипотеза (и доказана для случая $n=4$), что не существует APN-перестановок от чётного числа переменных. Однако в 2009 г. был найден первый пример взаимно однозначной APN-функции от шести переменных [20]. В работах [21, 22] рассматривается бесконечное семейство векторных функций, таких, что $\Delta_F \leqslant 4$, также содержащее APN-функцию Диллона, однако доказано, что это единственная APN-перестановка в данном семействе. До сих пор неизвестно, существуют ли другие APN-перестановки от шести переменных (неэквивалентные функции Диллона) и существуют ли они вообще для других чётных $n > 6$.

2. 2-в-1 функции как подфункции APN-перестановок

2.1. Алгоритм построения APN-перестановок с помощью $(n-1)$-подфункций

В работе [23] предложен новый способ построения 2-в-1 APN-функций, использующий символьные последовательности специального вида. Вектору значений 2-в-1 функции можно сопоставить символьную последовательность, такую, что одинаковым значениям соответствуют одни и те же символы, а различным значениям — разные символы. В том случае, когда F — APN-функция, такая последовательность называется *допустимой*. В [23] также описан алгоритм генерации всевозможных допустимых последовательностей.

Определение 1. Пусть F — векторная булева функция $F = (f_1, \ldots, f_n)$ из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Векторная функция F_j из $\mathbb{F}_2^n$ в $\mathbb{F}_2^{n-1}$ называется $(n-1)$-*подфункцией* функции F, если $F_j = (f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_n)$ для некоторого индекса $j \in \{1, \ldots, n\}$.

Напомним, что векторному пространству $\mathbb{F}_2^n$ можно сопоставить целочисленное множество $\{0,\dots,2^n-1\}$, где каждое целое число является десятичным представлением двоичного числа, представляющего вектор. Тогда можно рассматривать $(n-1)$-подфункцию F_j из $\mathbb{F}_2^n$ в $\mathbb{F}_2^{n-1}$ как векторную функцию из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, к которой в качестве первой координатной функции добавлена булева функция, тождественно равная нулю. Данная расширенная функция принимает значения только из множества $\{0,\dots,2^{n-1}-1\}$. Таким образом, множество $(n-1)$-подфункций изоморфно множеству таких векторных функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Далее будем рассматривать оба определения $(n-1)$-подфункции в зависимости от контекста.

Рассмотрим 2-в-1 функцию, которая принимает значения из $\{0,\dots,2^{n-1}-1\}$, обозначим множество таких 2-в-1 функций от n переменных через $\mathcal{T}_n$. Легко заметить, что любая $(n-1)$-подфункция взаимно однозначной векторной функции есть в точности функция из $\mathcal{T}_n$. В работе [23] доказаны следующие утверждения.

Теорема 1. Пусть F — взаимно однозначная APN-функция от n переменных. Тогда любая её $(n-1)$-подфункция является дифференциально 4-равномерной функцией из $\mathcal{T}_n$.

Вопрос характеризации APN-функции через её подфункции исследовался также в работе [24], где доказано, что любая подфункция APN-функции из $\mathbb{F}_2^{n-1}$ в $\mathbb{F}_2^{n-1}$ является APN-функцией или дифференциально 4-равномерной векторной функцией.

Напомним, что в данной работе дифференциально 4-равномерная функция — это функция, для которой значение $\max\limits_{a\neq\mathbf{0},b\in\mathbb{F}_2^n}\delta(a,b)$ равняется 4, то есть, согласно данному определению, APN-функции не являются дифференциально 4-равномерными. В некоторых работах встречается другое определение дифференциально δ-равномерных функций, которое включает функции меньших порядков дифференциальной равномерности, в частности APN-функции.

Теорема 2. Пусть F — взаимно однозначная APN-функция от n переменных. Тогда символьная последовательность, соответствующая вектору значений любой её $(n-1)$-подфункции, является допустимой последовательностью.

Из данных теорем следует, что любая APN-перестановка может быть получена из 2-в-1 дифференциально 4-равномерной функции, построенной при помощи допустимой последовательности. В [23] предложен следующий алгоритм для поиска взаимно однозначных APN-функций. На первом шаге строятся допустимые символьные последовательности и для каждой последовательности находится означивание, такое, что полученная 2-в-1 функция является дифференциально 4-равномерной. Следовательно, данная функция может быть изоморфна $(n-1)$-подфункции некоторой взаимно однозначной APN-функции и соответственно эта $(n-1)$-подфункция может быть достроена до APN-перестановки.

Без ограничения общности рассмотрим $(n-1)$-подфункцию $S=(s_1,\dots,s_{n-1})$, которая изоморфна 2-в-1 векторной функции из $\mathcal{T}_n$. Напомним, что любая такая функция является $(n-1)$-подфункцией некоторой взаимно однозначной векторной функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Для того чтобы её получить, нужно добавить к подфункции S недостающую координатную булеву функцию $f=s_n$ от n переменных, удовлетворяющую некоторым свойствам. Легко заметить, что функция f должна быть сбалансированной, так как искомая векторная функция взаимно однозначна. Поскольку $(n-1)$-подфункция $S=(s_1,\dots,s_{n-1})$ является 2-в-1 функцией, каждое из значений $0,1,\dots,2^{n-1}-1$ встретится ровно два раза. Соответственно на одну пару совпадающих значений подфункции S приходится либо упорядоченная пара значений $(0,1)$ недостающей булевой

функции, либо упорядоченная пара значений $(1, 0)$. Так как в векторе значений S имеется 2^{n-1} пар совпадающих значений, всего существует $2^{2^{n-1}}$ булевых функций $f = s_n$, таких, что $S = (s_1, \ldots, s_{n-1}, s_n)$ является взаимно однозначной функцией.

К сожалению, число $2^{2^{n-1}}$ уже при $n \geqslant 7$ очень велико для того, чтобы перебрать всевозможные варианты недостающих координатных булевых функций и проверить, является ли APN-функцией построенная взаимно однозначная функция $S = (s_1, \ldots, s_{n-1}, s_n)$. Поэтому, чтобы оценить, как быстро при переборе найдётся искомая взаимно однозначная APN-функция, необходимо найти количество тех булевых функций, которые дают именно APN-перестановку.

2.2. Оценка числа координатных булевых функций для $(n-1)$-подфункции

Для произвольного натурального n рассмотрим векторное пространство $\mathbb{F}_2^n$ и разобьём его на два равномощных непересекающихся подмножества $\mathbb{F}_2^n = V_1 \cup V_2$ следующим образом: пусть $V_1 = \{v \in \mathbb{F}_2^n : \mathrm{wt}(v) — \text{нечётное число}\}$ и $V_2 = \{v \in \mathbb{F}_2^n : \mathrm{wt}(v) — \text{чётное число}\}$, $\mathrm{wt}(v)$ — вес вектора v. Рассмотрим произвольную взаимно однозначную функцию $F = (f_1, \ldots, f_n)$. Зафиксируем k координатных функций $f_{i_1}, \ldots, f_{i_k}$ и разобьём $\mathbb{F}_2^n$ на два непересекающихся подмножества $\mathcal{F}_1$ и $\mathcal{F}_2$ следующим образом:

$$\mathcal{F}_j = \{(f_1(x), \ldots, f_n(x)) : f_{i_1}(x), \ldots, f_{i_k}(x) \in V_j,\ x \in \mathbb{F}_2^n\}, \quad j = 1, 2.$$

Пусть дано значение k, а также набор индексов $i_1, \ldots, i_k$ и индекс $j \notin \{i_1, \ldots, i_k\}$. Определим ассоциированную перестановку $F^\star$ следующим образом:

$$F^\star(x) = \begin{cases} F(x), & F(x) \in \mathcal{F}_1, \\ F(x) + \mathbf{e}_j, & F(x) \in \mathcal{F}_2. \end{cases}$$

Здесь $\mathbf{e}_j$ — вектор веса 1, содержащий 1 в j-й компоненте.

Теорема 3. Перестановка F является APN-функцией тогда и только тогда, когда перестановка $F^\star$ является APN-функцией.

Доказательство. Поскольку F — APN-функция, для любого ненулевого вектора $a \in \mathbb{F}_2^n$ её производная $D_aF(x) = F(x) + F(x + a)$ является 2-в-1 функцией. Зафиксируем произвольный вектор a' и рассмотрим вектор значений функции $D_{a'}F$. Он состоит из 2^{n-1} различных значений $B_{a'}F = \{b_1, \ldots, b_{2^{n-1}}\}$, каждое из которых встречается ровно два раза.

Рассмотрим перестановку $F^\star(x)$ и производную $D_{a'}F^\star$ для того же вектора a'. Без ограничения общности, для фиксированного аргумента x' возможны три случая:

1) $F(x') \in \mathcal{F}_1$ и $F(x' + a') \in \mathcal{F}_1$;
2) $F(x') \in \mathcal{F}_1$ и $F(x' + a') \in \mathcal{F}_2$;
3) $F(x') \in \mathcal{F}_2$ и $F(x' + a') \in \mathcal{F}_2$.

Рассмотрим первый случай. Поскольку $F(x')$ и $F(x' + a')$ лежат в $\mathcal{F}_1$, значение $D_{a'}F^\star(x') = D_{a'}F^\star(x' + a') = D_{a'}F(x') = D_{a'}F(x' + a')$ принадлежит $B_{a'}F$ и встречается два раза.

В третьем случае оба значения $F(x')$ и $F(x' + a')$ лежат в $\mathcal{F}_2$. Тогда значение производной $D_{a'}F^\star(x')$ равно значению производной $D_{a'}F(x')$, поскольку $D_{a'}F^\star(x') = F^\star(x') + F^\star(x' + a') = F(x') + \mathbf{e}_j + (x' + a') + \mathbf{e}_j = F(x') + (x' + a')$. Заметим, что $D_{a'}F^\star(x')$ совпадает со значением $D_{a'}F^\star(x' + a')$, следовательно, оно принадлежит $B_{a'}F$ и встречается два раза.

Чтобы доказать, что перестановка $F^\star$ является APN-функцией, необходимо показать, что значение производной, получаемое во втором случае, отлично от значений производной, получаемых в первом и третьем случаях, а также показать, что оно встретится в векторе значений функции $D_{a'}F^\star$ ровно два раза.

Докажем вторую часть необходимого условия. Поскольку $F(x')$ принадлежит $\mathcal{F}_1$, а $F(x'+a')$ принадлежит $\mathcal{F}_2$, значение производной $D_{a'}F^\star(x')$ равно значению $D_{a'}F(x')+$ $+\,\mathbf{e}_j$. Поскольку F — APN-функция, значение $D_{a'}F^\star(x')$ встречается ровно два раза, а значит, и $D_{a'}F^\star(x')$ встретится среди значений $D_{a'}F^\star(x')$ ровно два раза.

Заметим, что для любой пары $v_1, w_1 \in V_1$ и любой пары $v_2, w_2 \in V_2$ выполнено $v_i + w_i \in V_2$, $i = 1, 2$, а для любой пары $v_1 \in V_1$, $v_2 \in V_2$ выполнено $v_1 + v_2 \in V_1$. Следовательно, по построению множества $\mathcal{F}_1$ и $\mathcal{F}_2$ обладают аналогичными свойствами, а именно: для любой пары $v_1, w_1 \in \mathcal{F}_1$ и любой пары $v_2, w_2 \in \mathcal{F}_2$ выполнено $v_i + w_i \in \mathcal{F}_2$, $i = 1, 2$, а для любой пары $v_1 \in \mathcal{F}_1$, $v_2 \in \mathcal{F}_2$ выполнено $v_1 + v_2 \in \mathcal{F}_1$. Из этого следует, что значения производных в первом и третьем случаях принадлежат $\mathcal{F}_2$, а во втором случае — $\mathcal{F}_1$. Следовательно, поскольку $\mathcal{F}_1$ и $\mathcal{F}_2$ не пересекаются, производная $D_{a'}F^\star$ является 2-в-1 функцией. В силу произвольности выбора a' получаем, что производные функции $F^\star$ по всем направлениям являются 2-в-1 функциями, следовательно, $F^\star$ — APN-перестановка. ■

Пусть S является 2-в-1 дифференциально 4-равномерной функцией из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, принимающей значения из множества $\{0, \ldots, 2^{n-1} - 1\}$, которая может быть представлена в виде $(n-1)$-подфункции $S = (s_1, \ldots, s_{n-1})$. Обозначим через $n(S)$ число таких булевых функций f от n переменных, что $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой.

Теорема 4. Если значение $n(S)$ не равно нулю, то $n(S) \geqslant 2^n$.

Доказательство. Из теоремы 3 следует, что если $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой для некоторой булевой функции f, то ассоциированная перестановка $H^\star$ для некоторого набора индексов $i_1, \ldots, i_k$ также является APN-функцией. Чтобы оценить число булевых функций f, таких, что $H = S \cup f$ является APN-перестановкой, необходимо найти количество ассоциированных перестановок $H^\star$, имеющих общую $(n-1)$-подфункцию $S = (s_1, \ldots, s_{n-1})$.

Чтобы определить ассоциированную перестановку $H^\star$, в общем случае необходимо задать значение k, набор индексов $i_1, \ldots, i_k$ и индекс $j \notin \{i_1, \ldots, i_k\}$. Заметим, что перестановки H и $H^\star$ имеют общую $(n-1)$-подфункцию $S = (s_1, \ldots, s_{n-1})$ тогда и только тогда, когда $j = n$. Докажем, что каждой ассоциированной перестановке соответствует своё число k и набор индексов $i_1, \ldots, i_k$; соответственно для построения перестановки необходимо и достаточно задать лишь эти параметры. Для этого требуется доказать, что ни для какого $k^* < k$ не найдётся непересекающихся множеств V_1^*, V_2^*, таких, что $\mathbb{F}_2^{k^*} = V_1^* \cup V_2^*$ и выполнено следующее свойство: для вектора длины k зафиксируем произвольные $t = k - k^*$ координат, тогда любой вектор $v^* \in V_i^*$ может быть получен выкалыванием этих t координат из некоторого вектора $v \in V_i$, $i = 1, 2$.

По построению все векторы из $\mathbb{F}_2^k$ нечётного веса лежат в V_1, а значит, все векторы стандартного базиса $\mathbf{e}_j$, $j = 1, \ldots, k$, также лежат в V_1. Заметим, что нулевой вектор лежит в V_2. Рассмотрим вектор $\mathbf{e}_j$, такой, что координата j встречается среди t фиксированных координат $i_1, \ldots, i_t$. После выкалывания координат $i_1, \ldots, i_t$ из $\mathbf{e}_j$ получается нулевой вектор, который принадлежит V_1^*, однако нулевой вектор также лежит и в V_2^*, поскольку он уже лежал в V_2 до операции выкалывания. Поскольку для

любого $k^* < k$ и любого $t = k - k^*$ такой вектор $\mathbf{e}_j$ найдётся, множества V_1^* и V_2^* всегда будут пересекаться для любых t и $k*$.

Следовательно, для каждого k множества $\mathcal{F}_1$ и $\mathcal{F}_2$, полученные из таких V_1 и V_2, не совпадут ни с какими множествами $\mathcal{F}_1'$ и $\mathcal{F}_2'$, определёнными для некоторого $k^* < k$. Это значит, что для каждой ассоциированной перестановки существует единственное число k и единственный набор индексов $i_1, \ldots, i_k$, и для того, чтобы найти число возможных ассоциированных перестановок для APN-перестановки H, нужно посчитать число возможных наборов координат $i_1, \ldots, i_k$ для каждого значения $k = 1, \ldots, n-1$. Их в точности $\sum\limits_{j=1}^{n-1} \binom{2^{n-1}}{j} = 2^{n-1} - 1$.

Напомним, что прибавление аффинной функции не меняет свойства функции быть APN, следовательно, если $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой, то и $G = (s_1, \ldots, s_{n-1}, f + \mathbf{1})$ также ею является. Заметим, что прибавление единицы к последней координате эквивалентно тому, что мы меняем местами множества V_1 и V_2 при построении $\mathcal{F}_1$ и $\mathcal{F}_2$. Вместе с исходной функцией H имеем 2^{n-1} APN-перестановок, а поскольку к последней координате каждой перестановки ещё можем прибавить единицу, то всего получаем 2^n различных APN-перестановок, имеющих общую $(n-1)$-подфункцию $S = (s_1, \ldots, s_{n-1})$. Таким образом, если существует хотя бы одна булева функция f, такая, что $H = (s_1, \ldots, s_{n-1}, f)$ является APN-перестановкой и, следовательно, $n(S) \neq 0$, то $n(S) \geqslant 2^n$. ■

С помощью компьютерных вычислений установлено, что данная оценка является точной для $n = 3, 5$ и для всех рассмотренных спорадических примеров дифференциально 4-равномерных функций из $\mathcal{T}_n$ от шести переменных.

Остаются открытыми несколько интересных вопросов. Пусть S является дифференциально 4-равномерной функцией из $\mathcal{T}_n$. Может ли величина $n(S)$ в таком случае быть равной нулю? Другими словами, из любой ли 2-в-1 дифференциально 4-равномерной функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, принимающей значения из множества $\{0, \ldots, 2^{n-1} - 1\}$, можно получить APN-перестановку? Для всех рассмотренных примеров $n(S)$ не равнялась нулю. Более того, с помощью компьютерных вычислений получено, что при $n = 4$ в $\mathcal{T}_n$ не существует дифференциально 4-равномерных функций. Напомним, что APN-перестановок при $n = 4$ также не существует.

Понятия EA-эквивалентности и CCZ-эквивалентности очень важны, когда мы говорим о поиске новых функций, поскольку найти новую APN-перестановку от шести переменных — это найти APN-перестановку, неэквивалентную APN-функции Диллона. Можно заметить, что утверждение теоремы 3 задаёт отношение эквивалентности на множестве APN-перестановок. Как эта эквивалентность соотносится с уже известными отношениями эквивалентности? Так, мы проверили несколько пар ассоциированных APN-перестановок от пяти и шести переменных, и все рассмотренные примеры являлись попарно CCZ-эквивалентными.

Заключение

В работе представлен новый способ поиска взаимно однозначных APN-функций. Описан алгоритм получения APN-перестановок из 2-в-1 дифференциально 4-равномерных векторных функций и координатных булевых функций. Доказана оценка числа таких координатных булевых функций для данной векторной функции. Данный результат позволяет оценить, насколько эффективен предложенный алгоритм поиска APN-перестановок. Введено понятие ассоциированной перестановки для взаимно од-

нозначной функции и доказано, что некоторая перестановка является APN-функцией тогда и только тогда, когда её ассоциированная перестановка также является APN-функцией. Сформулированы некоторые открытые вопросы, например про свойства отношения эквивалентности на множестве взаимно однозначных APN-функций, которое задаётся аппаратом ассоциированных перестановок.

Автор выражает благодарность Наталье Токаревой, Николаю Коломейцу и Анастасии Городиловой за обсуждения, ценные замечания и дополнения.

ЛИТЕРАТУРА

1. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Des. Codes Cryptogr. 2000. V. 15. P. 125–156.
2. *Gold R.* Maximal recursive sequences with 3-valued recursive crosscorrelation functions // IEEE Trans. Inform. Theory. 1968. V. 14. P. 154–156.
3. *Nyberg K.* Differentially uniform mappings for cryptography // EUROCRYPT'93. LNCS. 1994. V. 765. P. 55–64.
4. *Kasami T.* The weight enumerators for several classes of subcodes of the second order binary Reed — Muller codes // Inform. Control. 1971. V. 18. P. 369–394.
5. *Janwa H. and Wilson R.* Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes // Proc. AAECC-10. LNCS. 1993. V. 673. P. 180–194.
6. *Canteaut A., Charpin P., and Dobbertin H.* Binary m-sequences with three-valued crosscorrelation: a proof of Welch conjecture // IEEE Trans. Inform. Theory. 2000. V. 46. P. 4–8.
7. *Dobbertin H.* Almost perfect nonlinear functions over GF(2^n): the Welch case // IEEE Trans. Inform. Theory. 1999. V. 45. P. 1271–1275.
8. *Dobbertin H.* Almost perfect nonlinear functions over GF(2^n): the Niho case // Inform. Comput. 1999. V. 151. P. 57–72.
9. *Hollmann H., and Xiang Q.* A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences // Finite Fields Appl. 2001. V. 7. P. 253–286.
10. *Beth T. and Ding C.* On almost perfect nonlinear permutations // EUROCRYPT'93. LNCS. 1993. V. 765. P. 65–76.
11. *Dobbertin H.* Almost perfect nonlinear power functions over GF(2^n): a new case for n divisible by 5 / eds. D. Jungnickel and H. Niederreiter. Finite Fields and Applications. Berlin; Heidelberg: Springer, 2001. P. 113–121.
12. *Глухов М. М.* О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7. № 4. С. 29–50.
13. *Blondeau C. and Nyberg K.* Perfect nonlinear functions and cryptography // Finite Fields Appl. 2015. V. 32. P. 120–147.
14. *Carlet C.* Open questions on nonlinearity and on APN Functions // LNCS. 2015. V. 9061. P. 83–107.
15. *Pott A.* Almost perfect and planar functions // Des. Codes Cryptography. 2016. V. 78(1). P. 141–195.
16. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
17. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer International Publishing, 2014. 168 p.
18. *Carlet C.* Vectorial Boolean functions for cryptography // Ch. 9 of the monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering". Cambridge Univ. Press, 2010. P. 398–472.

19. *Hou X.-D.* Affinity of permutations of F_2^n // Discr. Appl. Math. Special Issue: Coding and Cryptography Archive. 2006. V. 154. P. 313–325.
20. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six // 9-th Intern. Conf. Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, 2010. V. 518. P. 33–42.
21. *Canteaut A., Duval S., and Perrin L.* A generalisation of Dillon's APN permutation with the best known differential and linear properties for all fields of size 2^{4k+2} // IEEE Trans. Inform. Theory. 2016. V. 63. P. 7575–7591.
22. *Perrin L., Udovenko A., and Biryukov A.* Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem // CRYPTO 2016. Part II. LNCS. 2016. V. 9815. P. 93–122.
23. *Idrisova V.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem" // Cryptography and Communications. 2018. P. 1–19.
24. *Городилова А. А.* Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. № 27(3). С. 3–16.

REFERENCES

1. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr., 2000, vol. 15, pp. 125–156.
2. *Gold R.* Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory, 1968, vol. 14, pp. 154–156.
3. *Nyberg K.* Differentially uniform mappings for cryptography. EUROCRYPT'93, LNCS, 1994, vol. 765, pp. 55–64.
4. *Kasami T.* The weight enumerators for several classes of subcodes of the second order binary Reed — Muller codes. Inform. Control., 1971, vol. 18, pp. 369–394.
5. *Janwa H. and Wilson R.* Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. Proc. AAECC-10, LNCS, 1993, vol. 673, pp. 180–194.
6. *Canteaut A., Charpin P., and Dobbertin H.* Binary m-sequences with three-valued crosscorrelation: a proof of Welch conjecture. IEEE Trans. Inform. Theory, 2000, vol. 46, pp. 4–8.
7. *Dobbertin H.* Almost perfect nonlinear functions over GF(2^n): the Welch case. IEEE Trans. Inform. Theory, 1999, vol. 45, pp. 1271–1275.
8. *Dobbertin H.* Almost perfect nonlinear functions over GF(2^n): the Niho case. Inform. Comput., 1999, vol. 151, pp. 57–72.
9. *Hollmann H. and Xiang Q.* A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields Appl., 2001, vol. 7, pp. 253–286.
10. *Beth T. and Ding C.* On almost perfect nonlinear permutations. EUROCRYPT'93, LNCS, 1993, vol. 765, pp. 65–76.
11. *Dobbertin H.* Almost perfect nonlinear power functions over GF(2^n): a new case for n divisible by 5. Eds. D. Jungnickel and H. Niederreiter. Finite Fields and Applications, Berlin, Heidelberg, Springer, 2001, pp. 113–121.
12. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Mat. Vopr. Kriptogr., 2016, vol. 7, iss. 4, pp. 29–50. (in Russian)
13. *Blondeau C. and Nyberg K.* Perfect nonlinear functions and cryptography. Finite Fields Appl., 2015, vol. 32, pp. 120–147.
14. *Carlet C.* Open questions on nonlinearity and on APN Functions. LNCS, 2015, vol. 9061, pp. 83–107.

15. *Pott A.* Almost perfect and planar functions. Des. Codes Cryptography, 2016, vol. 78(1), pp. 141–195.
16. *Tuzhilin M. E.* Pochti sovershennye nelineynye funktsii [APN-functions]. Prikladnaya Diskretnaya Matematika, 2009, no. 3, pp. 14–20. (in Russian)
17. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer International Publ., 2014. 168 p.
18. *Carlet C.* Vectorial Boolean functions for cryptography. Ch. 9 of the monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Cambridge Univ. Press, 2010, pp. 398–472.
19. *Hou X.-D.* Affinity of permutations of F_2^n. Discr. Appl. Math. Special Issue: Coding and Cryptography Archive, 2006, vol. 154, pp. 313–325.
20. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six. 9-th Intern. Conf. Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, 2010, vol. 518, pp. 33–42.
21. *Canteaut A., Duval S., and Perrin L.* A generalisation of Dillon's APN permutation with the best known differential and linear properties for all fields of size 2^{4k+2}. IEEE Trans. Inform. Theory, 2016, vol. 63, pp. 7575–7591.
22. *Perrin L., Udovenko A., and Biryukov A.* Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. CRYPTO 2016, Part II, LNCS, 2016, vol. 9815, pp. 93–122.
23. *Idrisova V.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptography and Communications, 2018, pp. 1–19.
24. *Gorodilova A. A.* Characterization of almost perfect nonlinear functions in terms of subfunctions. Discr. Math. Appl., 2016, vol. 26(4), pp. 193–202.