Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/9/7

О СПЕЦИАЛЬНОМ ПОДКЛАССЕ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ И ПРОБЛЕМЕ СУЩЕСТВОВАНИЯ APN-ПЕРЕСТАНОВОК[1]

В. А. Виткуп

Известным открытым вопросом в области векторных булевых функций является проблема существования APN-перестановок от чётного числа переменных. Рассматривается множество векторных булевых функций специального вида, добавление к которым аффинной функции приводит к перестановке. Исследуются свойства этого множества, а также возможность и условия существования непустого пересечения с множеством APN-функций.

Ключевые слова: *векторная булева функция, APN-функция, взаимно однозначная функция, перестановка.*

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

Появление в 1990 г. дифференциального криптоанализа вызвало необходимость поиска функций, наиболее стойких к данному методу. Так, в 1992 г. было предложено понятие APN-функции, а затем и дифференциально δ-равномерной функции [1]. Векторная булева функция называется *APN-функцией* (почти совершенно нелинейной), если уравнение $F(x+a)+F(x) = b$ имеет не более двух решений для любых $a \in \mathbb{F}_2^n \setminus \{0\}$, $b \in \mathbb{F}_2^n$. Первый пример APN-функции был указан ещё в 1968 г. В. А. Башевым и в дальнейшем исследован Б. А. Егоровым [2]. Интересно, что именно эта функция была затем использована в качестве S-блока криптосистемы AES.

Центральное место в исследовании таких функций занимает проблема существования взаимно однозначных APN-функций (или *APN-перестановок*) при чётном n. В своё время была выдвинута гипотеза (и доказана для случая $n = 4$), что для чётного числа переменных APN-перестановок не существует, однако в 2009 г. Дж. Диллон и др. [3] опровергли это предположение, построив взаимно однозначную APN-функцию при $n = 6$. Более подробная информация содержится в [4, 5].

Настоящая работа посвящена изучению векторных функций со структурой множества значений определённого вида. Обозначим множество $M_y = \{x \in \mathbb{F}_2^n : F(x) = y\}$. Рассмотрим некоторую функцию F для произвольного n, такую, что для каждого y выполняется $|M_y| \in \{0, 2\}$, то есть множество всех аргументов функции разбивается на пары, на которых значение F совпадает. Будем обозначать класс таких функций $\mathcal{F}'_{n,n}$.

Две векторные функции F и G называются *аффинно эквивалентными*, если существуют аффинные перестановки A_1, A_2, такие, что выполнено $F = A_1 \circ G \circ A_2$. Заметим,

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

что взаимная однозначность, а также свойство функции быть APN сохраняются при таком преобразовании. Понятие аффинной эквивалентности расширяется следующим образом. Две векторные функции F и G называются *EA-эквивалентными* (расширенно аффинно эквивалентными), если существуют аффинные перестановки A_1, A_2 и аффинная функция A, такие, что выполнено $F = A_1 \circ G \circ A_2 + A$. Известно, что EA-эквивалентность сохраняет свойство функции быть APN, в то время как свойство взаимной однозначности может уже не сохраниться — прибавление аффинной функции может нарушить структуру перестановки.

Первая APN-перестановка от шести переменных была получена путём применения специального преобразования к некоторой APN-функции (которая изначально не являлась взаимно однозначной), такого, что эти функции CCZ-эквивалентны (другая эквивалентность более сложного вида, которая так же, как и EA-эквивалентность, сохраняет свойство функции быть APN). В этой работе мы пробуем реализовать похожую идею, однако в качестве преобразования рассмотрим частный случай EA-эквивалентности — когда преобразования A_1 и A_2 являются тождественными.

Хотелось бы выделить в множестве векторных булевых функций некоторый подкласс, состоящий из функций, отличающихся от перестановок на аффинную функцию, то есть таких, что добавление к ним аффинной функции приводит к взаимно однозначной функции. Если в таком классе при каких-то чётных n содержатся APN-функции, то мы бы получили конструктивное решение открытого вопроса о существовании взаимно однозначных перестановок от чётного числа переменных.

Лемма 1. Для любой векторной функции F из класса $\mathcal{F}'_{n,n}$ существует векторная функция S, каждая координатная булева функция которой сбалансированна или константна, такая, что $F + S$ — взаимно однозначная функция.

Напомним, что аффинные функции, отличные от константы, являются сбалансированными. Заметим, что произвольная аффинная векторная функция принадлежит множеству векторных функций S из леммы 1. Поэтому естественно предположить, что в классе $\mathcal{F}'_{n,n}$ может находиться искомый подкласс функций, отличающихся от перестановок на аффинную функцию.

Напомним, что под *расстоянием* между двумя булевыми функциями подразумевается расстояние Хэмминга между их векторами значений.

Лемма 2. Для любой булевой функции f чётного веса от n переменных, которая находится на расстоянии не более чем $2n + 2$ от константной функции, существует аффинная булева функция a, такая, что $a + f$ — сбалансированная функция.

Заметим, что все координатные булевы функции произвольной векторной функции F из класса $\mathcal{F}'_{n,n}$ имеют чётный вес. Значит, для векторных булевых функций, чьи координатные функции удовлетворяют условиям леммы 2, найдутся аффинные векторные функции, сумма с которыми даёт покоординатно сбалансированные векторные функции, частным случаем которых и являются перестановки.

Пусть K — множество всех таких функций F из $\mathcal{F}'_{n,n}$, что для каждой функции существует аффинная функция A, дающая в сумме с F взаимно однозначную функцию. Заметим, что множество K непусто. Действительно, для любого n в этом классе лежат функции $F_1 = (0, x_2, \ldots, x_n)$, $F_2 = (x_1, 0, x_2, \ldots, x_n)$, $\ldots$, $F_n = (x_1, x_2, \ldots, x_{n-1}, 0)$. Заметим, что если взять соответственно аффинные функции $A_1 = (x_1, 0, \ldots, 0)$, $A_2 = (0, x_2, 0, \ldots, 0)$, $\ldots$, $A_n = (0, \ldots, 0, x_n)$, то их суммы равны $A_i + F_i = (x_1, \ldots, x_n)$, то есть являются тождественной функцией, которая взаимно однозначна.

Сформулируем необходимое условие того, что функция из $\mathcal{F}'_{n,n}$ является APN-функцией.

Лемма 3. Пусть APN-функция F от n переменных принадлежит $\mathcal{F}'_{n,n}$, другими словами, множество наборов её аргументов разбивается на пары $x_{i,1}, x_{i,2}$, $i = 1, \ldots, 2^{n-1}$, такие, что для каждого i выполнено $F(x_{i,1}) = F(x_{i,2})$. Тогда для любых $j, k \in \{1, \ldots, 2^{n-1}\}$, $j \neq k$, справедливо $x_{j,1} + x_{j,2} + x_{k,1} + x_{k,2} \neq 0$.

Заметим, что из леммы 3 следует, в частности, что в классе $\mathcal{F}'_{2,2}$ не может быть APN-функций.

Гипотеза 1. Для любого $n > 2$ в классе $\mathcal{F}'_{n,n}$ есть APN-функции.

В результате компьютерных экспериментов при $n = 3$ обнаружено, что для каждой APN-функции из класса $\mathcal{F}'_{3,3}$, веса координатных функций которой равны 2 или 6, существует ровно 128 аффинных векторных функций, дающих в сумме с ней APN-перестановку. Для APN-функций с другими весами координатных функций также всегда существуют соответствующие аффинные функции. Естественно предположить далее, что для некоторых других n пересечение множества APN-функций с классом K также непусто. Заметим, что для $n = 4$ в классе K нет APN-функций, поскольку иначе существовала бы APN-перестановка от четырёх переменных, что, как известно, не так.

Гипотеза 2. Для некоторых значений $n \geqslant 5$ в классе K есть APN-функции.

Истинность гипотезы 2 для конкретных чётных значений n влечёт существование взаимно однозначных APN-функций для соответствующего числа переменных.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentily uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. *Глухов М. М.* О совершенно нелинейных и почти совершенно нелинейных функциях // Матем. вопр. криптограф. 2016. (в печати)
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An APN permutation in dimension six // Amer. Math. Soc. 2010. V. 518. P. 33–42.
4. *Туэжилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
5. *Carlet C.* Open questions on nonlinearity and on APN Functions // LNCS. 2015. V. 9061. P. 83–107.

УДК 519.7 DOI 10.17223/2226308X/9/8

О ДИФФЕРЕНЦИАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ КВАДРАТИЧНЫХ APN-ФУНКЦИЙ[1]

А. А. Городилова

Для векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ определяется ассоциированная булева функция γ_F от $2n$ переменных по правилу: $\gamma_F(a, b) = 1$, где $a, b \in \mathbb{F}_2^n$, если $a \neq (0, \ldots, 0)$ и уравнение $F(x) + F(x + a) = b$ имеет решение, и $\gamma_F(a, b) = 0$ иначе. Вводится понятие дифференциально эквивалентных векторных булевых функций как функций, имеющих одинаковые ассоциированные булевы функции. Интересен вопрос описания классов дифференциальной эквивалентности почти

[1]Работа поддержана грантом РФФИ, проект 15-07-01328.