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.

совершенно нелинейных (APN) функций, так как его решение может потенциально привести к новым конструкциям APN-функций. В работе начато изучение данного вопроса с исследования аффинных функций, прибавление которых к квадратичным APN-функциям не выводит за рамки их классов дифференциальной эквивалентности. Полностью описаны такие аффинные функции для известного класса APN-функций Голда. Получены вычислительные результаты для известных квадратичных APN-функций от малого числа переменных 2, ..., 8.

Ключевые слова: *векторная булева функция, почти совершенно нелинейная функция, дифференциальная эквивалентность.*

Отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *почти совершенно нелинейной* функцией (APN-функцией), если для любых векторов $a, b \in \mathbb{F}_2^n$, $a \neq (0, \ldots, 0)$, уравнение $F(x) + F(x + a) = b$ имеет не более двух решений. 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 [1], А. Потта [2]. Некоторые открытые вопросы в области APN-функций представлены в работе К. Карле [3]. Например, открытому вопросу о существовании APN-подстановок посвящены работы М. М. Глухова [4], В. Н. Сачкова [5].

Для векторной функции F от n переменных 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. Легко видеть, что F — APN-функция тогда и только тогда, когда $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$, где wt — вес Хэмминга булевой функции. Введём следующее определение.

Определение 1. Функции F и G называются *дифференциально эквивалентными*, если $\gamma_F = \gamma_G$. Обозначим класс дифференциальной эквивалентности F через $\mathcal{DE}_F$.

Говорят, что две векторные функции F и G *EA-эквивалентны*, если существуют аффинные взаимно однозначные функции A', A'' и аффинная функция A, такие, что $G = A' \circ F \circ A'' + A$. Дифференциальная и EA-эквивалентности сохраняют свойство функции быть почти совершенно нелинейной. Однако в настоящий момент не известно, вкладываются ли классы дифференциальной эквивалентности APN-функций в соответствующие классы EA-эквивалентности APN-функций. Ответ на этот вопрос может потенциально привести к новым конструкциям APN-функций.

Утверждение 1. Пусть F и G — EA-эквивалентные функции. Тогда $|\mathcal{DE}_F| = |\mathcal{DE}_G|$. Более того, если $G = A' \circ F \circ A'' + A$ и $\mathcal{DE}_F = \{F_1, \ldots, F_k\}$, то $\mathcal{DE}_G = \{A' \circ F_1 \circ A'' + A, \ldots, A' \circ F_k \circ A'' + A\}$.

Легко видеть, что класс дифференциальной эквивалентности любой APN-функции F содержит 2^{2n} тривиальных различных функций $F_{c,d}(x) = F(x + c) + d$, $c, d \in \mathbb{F}_2^n$. В [6] найден пример APN-функции от четырёх переменных, чей класс дифференциальной эквивалентности шире, чем тривиальный (состоящий из 2^{2n} функций $F_{c,d}$). В данной работе случай $n = 4$ рассмотрен полностью. В табл. 1 приведены значения мощностей классов дифференциальной эквивалентности APN-функций от малого числа переменных $n = 2, 3, 4$.

Поскольку задача описания класса дифференциальной эквивалентности в общем случае представляется сложной, в данной работе начато её рассмотрение применительно к квадратичным APN-функциям, а именно исследуется вопрос, когда функции F и $F + A$ дифференциально эквивалентны, где F — квадратичная APN-функция, а A — произвольная аффинная функция. Заметим, что для любой квадратичной

Таблица 1

n	Кол-во EA-классов	EA-представитель $F(x)$	$\deg(F)$	$\lvert\mathcal{DE}_F\rvert$
2	1	x^3	2	2^4
3	1	x^3	2	2^6
4	2	x^3	2	2^{10}
		$x^3 + (x^2 + x + 1)\,\mathrm{tr}(x^3)$	3	2^{10}

APN-функции 2^{2n} таких аффинных функций всегда существует, поскольку $F_{c,d}(x) = F(x + c) + d = F(x) + (F(x) + F(x + c) + d) = F(x) + A^F_{c,d}(x)$, где $A^F_{c,d}$ — аффинная функция в силу квадратичности F.

По аналогии с утверждением 1 справедливо следующее

Утверждение 2. Для квадратичной APN-функции F число различных аффинных функций A, таких, что F и $F + A$ дифференциально эквивалентны, инвариантно относительно EA-преобразования.

Для известного класса APN-функций Голда получена следующая теорема, полностью описывающая все аффинные функции, прибавление которых к исходной функции не выводит за рамки её класса дифференциальной эквивалентности. Напомним, что векторную функцию $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ можно рассматривать как функцию над конечным полем $\mathbb{F}_{2^n}$ и однозначно представлять в виде полинома степени не выше $2^n - 1$: $F(x) = \sum\limits_{i=0}^{2^n-1} a_i x^i$, где $a_i \in \mathbb{F}_{2^n}$. При этом степень функции равна $\max\{\mathrm{wt}(i) : \ a_i \neq 0\}$, где $\mathrm{wt}(i)$ — двоичный вес числа.

Теорема 1. Пусть F — APN-функция Голда от n переменных, $F(x) = x^{2^k+1}$ и $(k, n) = 1$. Тогда выполнены следующие утверждения:

1) если $n = 4t$ для некоторого t и $k = n/2 \pm 1$, то существуют в точности $2^{2n+n/2}$ различных аффинных функций A, таких, что F и $F + A$ дифференциально эквивалентны, при этом $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k} + \delta x^{2^j}$, где $\alpha, \lambda, \delta \in \mathbb{F}_{2^n}$; $\delta = \delta^{2^{n/2}}$; $j = k - 1$ при $k = n/2 + 1$ и $j = n - 1$ при $k = n/2 - 1$;
2) иначе существуют в точности 2^{2n} различных аффинных функций A, таких, что F и $F + A$ дифференциально эквивалентны, при этом $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k}$, где $\alpha, \lambda \in \mathbb{F}_{2^n}$.

Теорема 1 показывает, что среди APN-функций Голда существуют такие, чей класс дифференциальной эквивалентности шире, чем тривиальный. А именно это функции $F(x) = x^{2^{n/2\pm1}+1}$ при n, кратном 4 (заметим, что эти функции EA-эквивалентны). В табл. 2 приведены вычислительные результаты, полученные для всех известных EA-классов квадратичных APN-функций от 2 до 8 переменных. Отметим, что EA-классификация квадратичных APN-функций вплоть до 6 переменных известна полностью, а для 7 и 8 переменных найдена частичная классификация (см. [2]).

Как видно из табл. 2, для почти всех рассмотренных EA-классов существует только 2^{2n} тривиальных аффинных функций $A_{c,d}$. Исключения составляют следующие:

$n = 4$: 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 2

n	Кол-во EA-классов	Кол-во аффинных функций A: $F + A \in \mathcal{DE}_F$
2	1	2^4
3	1	2^6
4	1	2^{10}
5	2	Для обоих классов: 2^{10}
6	13	Для одного класса: 2^{13}; для остальных 12 классов: 2^{12}
7	$\geqslant 487$	Для всех известных 487 классов: 2^{14}
8	$\geqslant 8179$	Для одного класса из известных 8179: 2^{20}; для остальных 8178 классов: 2^{16}

ЛИТЕРАТУРА

1. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
2. *Pott A.* Almost perfect and planar functions // Des. Codes Cryptogr. 2016. V. 78. P. 141–195.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // Arithmetic of Finite Fields. LNCS. 2015. V. 9061. P. 83–107.
4. *Глухов М. М.* О матрицах переходов разностей при использовании некоторых модулярных групп // Матем. вопр. криптограф. 2013. Т. 4. № 4. С. 27–47.
5. *Сачков В. Н.* Комбинаторные свойства дифференциально 2-равномерных подстановок // Матем. вопр. криптограф. 2015. Т. 6. № 1. С. 159–179.
6. *Городилова А. А.* О пересечении множеств значений производных APN-функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 25–27.

УДК 512.542.3 DOI 10.17223/2226308X/9/9

ФУНКЦИИ С ВАРИАЦИОННО-КООРДИНАТНОЙ ПОЛИНОМИАЛЬНОСТЬЮ НАД ГРУППОЙ

А. И. Зуева, А. В. Карпов

Определён класс функций с вариационно-координатной полиномиальностью над группой, являющийся обобщением класса ВКП-функций над примарным кольцом вычетов. Представлен алгоритм нахождения координат для элемента группы. Доказано, что класс ВКП-функций над $UT_n(\mathbb{Z}_p)$ не совпадает с классом полиномиальных функций. Указан способ обращения биективной ВКП-функции над $UT_n(\mathbb{Z}_p)$.

Ключевые слова: *функции над группой, функции с вариационно-координатной полиномиальностью, координатные функции.*

В [1] определён класс функций с вариационно-координатной полиномиальностью (ВКП-функций) над примарным кольцом вычетов, порождающий системы ВКП-уравнений, для решения которых применим метод покоординатной линеаризации.

В данной работе делается обобщение класса ВКП-функций на случай, когда полиномы рассматриваются над группой с нормальным рядом. Получающийся при этом класс ВКП-функций над группой даёт конструктивный пример дифференцируемых функций над группой, рассмотренных в [2].

Пусть задана группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$. Как и в случае примарного кольца вычетов, для определения класса ВКП-функций над группой необходимо определить понятие координатной функции полинома над группой.