УДК 519.7 DOI 10.17223/2226308X/10/13

КЛАССИФИКАЦИЯ ДИФФЕРЕНЦИАЛЬНО НЕЭКВИВАЛЕНТНЫХ КВАДРАТИЧНЫХ APN-ФУНКЦИЙ ОТ 5 И 6 ПЕРЕМЕННЫХ[1]

А. А. Городилова

Получена классификация дифференциально неэквивалентных квадратичных APN-функций от 5 и 6 переменных. Доказано, что для любой квадратичной APN-функции F от n переменных, $n \leqslant 6$, все дифференциально эквивалентные ей квадратичные функции представляются как $F \oplus A$, где A — аффинная функция.

Ключевые слова: *APN-функции, дифференциальная эквивалентность, линейный спектр.*

Почти совершенно нелинейные (APN) функции определяются как векторные булевы функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, наиболее сильно отличающиеся от самых простых — аффинных функций, если в качестве меры отличия рассматривать максимальное число решений уравнения $F(x) \oplus F(x \oplus a) = b$ по всем $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$. Для APN-функций это число решений минимально и равно 2. Класс APN-функций мало изучен, несмотря на большое число работ в данной области, не описаны даже все самые простые — квадратичные — APN-функции. Обзору результатов об APN-функциях и смежных с ними посвящена работа М. М. Глухова [1].

Будем обозначать $B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{F}_2^n\}$.

Функции F и G *дифференциально эквивалентны* [2], если $B_a(F) = B_a(G)$ для любого $a \in \mathbb{F}_2^n$. *Линейным спектром* [3] квадратичной APN-функции F называется вектор $\Lambda^F = (\lambda_0^F, \ldots, \lambda_{2^n-1}^F)$, где λ_k^F — число линейных функций L, таких, что $k_L^F = k$, где $k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \ B_a(F) = B_a(F \oplus L)\}|$.

Из определений естественно следует *свойство*: линейные спектры дифференциально эквивалентных квадратичных APN-функций равны. Обратное в общем случае неверно, т. е. из того, что линейные спектры двух функций совпадают, не следует, что эти функции дифференциально эквивалентны.

Функции F и G *EA-эквивалентны*, если существуют аффинные взаимно однозначные функции A', A'' и аффинная функция A, такие, что $G = A' \circ F \circ A'' \oplus A$. EA-эквивалентность сохраняет свойство функции быть APN. В [3] показано, что линейный спектр — EA-инвариант, и найдены линейные спектры всех квадратичных APN-функций от $n = 3, 4, 5, 6$ переменных. При $n = 3, 4$ существует только по одному классу EA-эквивалентности квадратичных APN-функций; при $n = 5$ — два класса, и их линейные спектры различны; при $n = 6$ — 13 классов, линейные спектры которых попарно различны, кроме одной пары (функции 3 и 10 в [3, табл. 4]). Из данных результатов по свойству выше следует, что не существует дифференциально эквивалентных квадратичных APN-функций, принадлежащих разным классам EA-эквивалентности, при $n = 3, 4, 5, 6$, кроме, быть может, одного случая при $n = 6$. Однако удалось вычислительно доказать, что данный случай не реализуется. Доказательство существенно опирается на отличительное свойство квадратичных APN-функций от чётного числа переменных [3]:

— пусть F — квадратичная APN-функция от n переменных, n чётно. Тогда для любого $v \in \mathbb{F}_2^n$ размерность $A_v^F \cup \{\mathbf{0}\}$ чётна. Здесь A_v^F — множество векторов $a \in \mathbb{F}_2^n$, таких, что линейная часть подпространства $B_a(F)$ совпадает с линейным подпространством $\{y \in \mathbb{F}_2^n : \langle y, v \rangle = 0\}$, где $v \in \mathbb{F}_2^n$.

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.

В этих же обозначениях можно сформулировать следующий известный факт:

— пусть F — квадратичная APN-функция от n переменных, n нечётно. Тогда для любого $v \in \mathbb{F}_2^n$, $v \neq \mathbf{0}$, множество A_v^F состоит из одного элемента.

Следующий шаг — проверить, какие функции дифференциально эквивалентны в каждом классе EA-эквивалентности. При $n = 3, 4$ данные результаты известны [2]. Для $n = 5, 6$ проведены вычислительные эксперименты, основанные на свойствах выше и том факте, что для любой квадратичной APN-функции F множество $B_a(F)$ — аффинное подпространство размерности $n-1$, поэтому его линейная часть может быть однозначно задана одним вектором, ортогональным данному линейному подпространству. Обобщая полученные результаты, сформулируем теорему.

Теорема 1. Пусть F — квадратичная APN-функция от n переменных, $n \in \{3, 4, 5, 6\}$. Тогда все дифференциально эквивалентные ей квадратичные APN-функции G представляются в виде $G = F \oplus A$, где A — аффинная функция. При этом число K таких аффинных функций A равно 2^{2n} для всех функций, за исключением функций из трёх классов EA-эквивалентности со следующими представителями:

1) $n = 4$: APN-функция Голда $F(x) = x^3$, $K = 2^{10}$;
2) $n = 6$: APN-функция $F(x) = \alpha^7 x^3 + x^5 + \alpha^3 x^9 + \alpha^4 x^{10} + x^{17} + \alpha^6 x^{18}$, $K = 2^{13}$;
3) $n = 8$: APN-функция Голда $F(x) = x^9$, $K = 2^{20}$.

Здесь функции заданы над конечным полем $\mathbb{F}_{2^n}$, α — примитивный элемент поля.

Один из дальнейших интересных вопросов следующий: можно ли предложить способ описания всех представителей классов дифференциальной эквивалентности квадратичных APN-функций, отличный от полного их перечисления?

ЛИТЕРАТУРА

1. *Глухов М. М.* О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7. Вып. 4. С. 29–50.
2. *Городилова А. А.* О дифференциальной эквивалентности квадратичных APN-функций // Прикладная дискретная математика. Приложение. 2016. № 9. С. 21–24.
3. *Городилова А. А.* Линейный спектр квадратичных APN-функций // Прикладная дискретная математика. 2016. № 4(34). С. 5–16.

УДК 519.7 DOI 10.17223/2226308X/10/14

О ПОСТРОЕНИИ APN-ФУНКЦИЙ СПЕЦИАЛЬНОГО ВИДА И ИХ СВЯЗИ С ВЗАИМНО ОДНОЗНАЧНЫМИ APN-ФУНКЦИЯМИ[1]

В. А. Идрисова

Важным открытым вопросом в области криптографических булевых функций является проблема существования APN-перестановок от чётного числа переменных. Рассматривается алгоритм построения 2-в-1 APN-функций и поиска соответствующих аффинных функций, таких, что сумма 2-в-1 функции и аффинной — взаимно однозначная APN-функция. Найдены 2-в-1 функции от 5 и 6 переменных, которые эквивалентны APN-перестановкам.

Ключевые слова: *векторная булева функция, APN-функция, взаимно однозначная функция, 2-в-1 функция, перестановка.*

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.