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

$n = 2$, $F =$(0 0 0 1);

$n = 3$, $F =$(0 2 2 2 2 3 6 5);

$n = 5$, $F =$(0 0 0 1 0 2 4 8 0 3 6 12 7 16 25 23 0 7 3 22 28 19 9 0 19 8 15 28 21 9 29 2).

Для следующих функций достижима оценка $\xi(n) - 1$:

$n = 4, F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13);

$n = 6$, $F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13 0 8 16 25 5 15 17 26 32 44 54 59 45 35 63 48 0 16 26 36 34 48 60 0 45 57 49 11 7 17 31 39 43 28 14 23 12 57 45 54 38 21 5 24 9 56 46 49).

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // Eurocrypt'1993. LNCS. 1994. V. 765. P. 55–64.
2. *Туэжилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Habilitation Thesis, University of Paris, Sept. 2013.

УДК 519.7 DOI 10.17223/2226308X/8/9

О ПЕРЕСЕЧЕНИИ МНОЖЕСТВ ЗНАЧЕНИЙ ПРОИЗВОДНЫХ APN-ФУНКЦИЙ[1]

А. А. Городилова

Исследуются пересечения множеств значений производных двух APN-функций. Формулируются два вопроса: какова минимальная мощность таких пересечений и как связаны любые две APN-функции, множества значений производных которых попарно совпадают по каждому направлению. Получены частичные результаты по каждому из вопросов.

Ключевые слова: *векторная булева функция, производная по направлению, APN-функция.*

В работе рассматривается специальный класс векторных булевых функций — почти совершенные нелинейные функции (APN-функции). Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *APN-функцией*, если для любых векторов $a, b \in \mathbb{F}_2^n$, где a — ненулевой вектор, уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более двух решений. Данные функции представляют интерес для использования в качестве узлов замены в блочных шифрах в силу их оптимальной стойкости к разностному криптоанализу. Однако класс APN-функций достаточно слабо изучен (см., например, обзор [2]), остаётся большое число открытых вопросов [3].

Настоящая работа посвящена исследованию пересечений множеств значений производных APN-функций. Производной функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ по направлению $a \in \mathbb{F}_2^n$ называется функция $D_aF(x) = F(x) \oplus F(x \oplus a)$. По определению F — APN-функция, если её производные по каждому направлению принимают в точности 2^{n-1} различных значений, т. е. $|B_a(F)| = |\{D_aF(x) : x \in \mathbb{F}_2^n\}| = 2^{n-1}$. Для автора представляется интересным найти ответы на следующие вопросы.

Открытый вопрос 1. Каково минимальное пересечение множеств значений производных двух APN-функций?

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

Открытый вопрос 2. Как связаны APN-функции F и G от n переменных, если их производные по каждому направлению имеют одинаковые множества значений соответственно, т. е. для любого $a \neq 0$ верно $B_a(F) = B_a(G)$?

Первый вопрос связан, в частности, с поиском итеративной конструкции. Из теоремы 1 [1] следует, что если взять две APN-функции F, G от n переменных и две булевы функции f, g от n переменных, для которых выполнено условие допустимости (для всех $x, y, a \in \mathbb{F}_2^n$, $a \neq 0$, хотя бы одно из равенств $D_aF(x) = D_aG(y)$ и $D_af(x) = D_ag(y)$ нарушается), то по ним можно определить APN-функцию от $n+1$ переменной. Фактически, вся сложность описанного подхода к итеративному построению APN-функций заключается в поиске исходных *допустимых* векторных функций F и G (т. е. тех, для которых существуют булевы функции f, g, такие, что для F, G, f, g выполнено условие допустимости). Получен следующий эквивалентный критерий проверки допустимости пары APN-функций F и G, который не включает в рассмотрение соответствующие булевы функци f и g.

Утверждение 1. Пара APN-функций F и G от n переменных допустима тогда и только тогда, когда для любого нечётного k, $k \geqslant 3$, не существует набора векторов x^i, y^i, a^i, $i = 1, \ldots, k$, где $a^i \neq 0$, таких, что $F(x^i) \oplus F(x^i \oplus a^i) = G(y^i) \oplus G(y^i \oplus a^i)$, $i = 1 \ldots, k$, и каждый из векторов x и y среди x^i, $x^i \oplus a^i$ и y^i, $y^i \oplus a^i$ соответственно $(i = 1, \ldots, k)$ встречается чётное число раз.

Как можно видеть из утверждения 1, необходимо отслеживать, какие пересечения имеют множества значений производных функций F и G по всем направлениям. Логично предположить, что чем меньше мощности пересечений значений производных функций F и G, тем больше вероятность, что будут выполнены условия утверждения 1.

Утверждение 2. Для любых двух APN-функций F и G от n переменных, $n \geqslant 3$, существует ненулевой вектор $a \in \mathbb{F}_2^n$, такой, что множества значений производных D_aF и D_aG пересекаются.

Далее рассмотрим отдельно случай двух квадратичных APN-функций, которые в сумме дают линейную функцию. Пусть F — квадратичная APN-функция, а L — линейная от n переменных (для любых $x, y \in \mathbb{F}_2^n$ выполнено $L(x \oplus y) = L(x) \oplus L(y)$). Тогда производные F по всем направлениям аффинны и, следовательно, множества $B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{F}_2^n\}$ являются аффинными подпространствами $\mathbb{F}_2^n$ размерности $n-1$. Далее, поскольку $B_a(F \oplus L) = B_a(F) \oplus L(a)$, то $B_a(F)$ и $B_a(F \oplus L)$ либо совпадают, либо не пересекаются. Из этого следует также, что $F \oplus L$ является APN-функцией.

Утверждение 3. Пусть F — квадратичная APN-функция, а L — произвольная линейная функция от n переменных. Пусть существуют в точности k различных ненулевых $a^i \in \mathbb{F}_2^n$, при которых $B_{a^i}(F) = B_{a^i}(F \oplus L)$. Тогда если $k > 2^{n-1}$, то пара F, $F \oplus L$ не является допустимой.

Гипотеза 1. Для любой квадратичной APN-функции F от n переменных существует линейная функция L от n переменных, такая, что пара F и $F \oplus L$ является допустимой.

Гипотеза 1 выполняется для $n = 3$; найдены также примеры, подтверждающие её при $n = 4, 5$ (эти размерности вычислительно не позволяют провести полный перебор).

Второй вопрос связан с описанием классов APN-функций, у которых множества значений производных попарно совпадают по каждому направлению. Ранее авто-

ром неверно предполагалось, что для каждой APN-функции F такой класс состоит только из функций $F(x \oplus c) \oplus d$, где c, d пробегают $\mathbb{F}_2^n$. Однако найдены примеры квадратичных функций F от 4 переменных, для которых существуют линейные функции L, прибавление которых к исходной функции F сохраняет множества значений производных по всем направлениям, но при этом $F \oplus L$ не лежит в классе $\{F(x \oplus c) \oplus d : c, d \in \mathbb{F}_2^n\}$. Например, в качестве F можно выбрать APN-функцию $F(x_1, x_2, x_3, x_4) = (x_1x_2,\ x_1x_3 \oplus x_2x_4,\ x_2x_3 \oplus x_1x_4 \oplus x_2x_4,\ x_3x_4)$, а в качестве линейной следующую: $L(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_2,\ x_3 \oplus x_4)$. Тогда для любого ненулевого $a \in \mathbb{F}_2^4$ верно $B_a(F) = B_a(F \oplus L)$.

ЛИТЕРАТУРА

1. *Городилова А. А.* Характеризация APN-функций через подфункции // Прикладная дискретная математика. Приложение. 2014. № 7. С. 15–16.
2. *Туэкилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.

УДК 512.552.18 DOI 10.17223/2226308X/8/10

ИССЛЕДОВАНИЕ ГРУППЫ БИЕКТИВНЫХ ДИФФЕРЕНЦИРУЕМЫХ ПО МОДУЛЮ p^n ФУНКЦИЙ

А. С. Ивачев

Описана с точностью до изоморфизма группа биективных дифференцируемых по модулю p^n функций, предложен способ поиска сопрягающего элемента в этой группе с помощью решения системы линейных уравнений над $\mathbb{Z}_p$, а также предложен способ генерации транзитивных функций с помощью биективных дифференцируемых по модулю p^n функций путём сопряжения функции $f(x) = x + 1$ биективными функциями.

Ключевые слова: *дифференцируемая по модулю p^n функция, биективная функция, транзитивная функция, сопряжение.*

Генерация последовательностей больших периодов, состоящих из элементов конечного кольца, является важной задачей в криптографии. Для генерации последовательности может использоваться следующая рекуррентная формула:

$$x_{i+1} = f(x_i), i = 1, 2, \ldots,$$

где f — некоторая функция над кольцом $\mathbb{Z}_{p^n}$.

Возникает проблема выбора f, такой, чтобы она легко вычислялась и генерировала последовательность $x_1x_2\ldots$ максимального периода p^n.

Как вариант выбора таких f в [1] предложены и исследованы дифференцируемые по модулю p^n функции, в том числе те из них, которые являются биективными и транзитивными. В частности, построены критерии биективности и транзитивности и получена формула для вычисления обратных биективных дифференцируемых по модулю p^n функций.

В данной работе проведено более глубокое изучение биективных дифференцируемых функций, а также основных задач, в которых данные функции могут быть применимы.