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.

Стойкость криптосистемы существенно зависит от правильного выбора её нелинейных компонент (S-блоков). Математически S-блок представляет собой векторную булеву функцию. *Векторной булевой функцией* F называется произвольное отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Далее рассматриваются только функции вида $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Среди требований, выдвигаемых к криптографическим булевым функциям, важное место занимает устойчивость к дифференциальному криптоанализу. Векторные функции, обладающие оптимальной такой стойкостью, называются APN-функциями, или почти совершенно нелинейными. Понятие APN-функции введено К. Ньюберг в 1992 г. [1], однако известно [2], что APN-функции изучались в СССР В. А. Башевым и Б. А. Егоровым начиная с 1968 г. Векторная булева функция называется *APN-функцией*, если уравнение $F(x \oplus a) \oplus F(x) = b$ имеет не более двух решений для любых $a \in \mathbb{F}_2^n \setminus \{0\}$, $b \in \mathbb{F}_2^n$.

В SP-сети для обратимости процесса шифрования используются взаимно однозначные векторные функции, или перестановки. Поэтому центральное место в изучении почти совершенно нелинейных функций занимает проблема существования взаимно однозначных APN-функций для чётного числа переменных, известная в англоязычной литературе как «the Big APN Problem». Лишь в 2009 г. была представлена первая APN-перестановка для $n = 6$ [3], причём до этого долгое время считалось, что при чётных n таких функций нет. Интересно, что данная функция сразу же нашла применение в легковесном блочном шифре FIDES. Для чётных размерностей, превосходящих 6, вопрос до сих пор открыт и значительных продвижений не получено. Подробную информацию об исследованиях в данной области можно найти в обзорах [4, 5].

В данной работе рассматривается множество 2-в-1 векторных функций. Векторная функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *2-в-1 функцией,* если её множество значений состоит из 2^{n-1} элементов и каждое значение она принимает ровно на двух аргументах.

Лемма 1 [6]. Для любой 2-в-1 векторной функции F от n переменных существует векторная функция G, каждая координатная булева функция которой сбалансирована или константна, такая, что $F \oplus G$ — взаимно однозначная функция.

Данный факт влечёт за собой интересное свойство: если F — APN-функция, а G — аффинная, то $F \oplus G$ является APN-перестановкой, поскольку полученная функция EA-эквивалентна исходной. Две векторных функции F и H называются *расширенно аффинно эквивалентными, или EA-эквивалентными*, если $F = A_1 \circ H \circ A_2 \oplus A$, где A_1, A_2 — аффинные перестановки; A — аффинная функция. Важным фактом является то, что свойство APN инвариантно относительно расширенного аффинного преобразования. Возможность получения перестановки путём сложения APN-функции с аффинной функцией уже рассматривалась в [7]. Авторы исследовали мономиальные APN-функции, то есть APN-функции вида $F(x) = x^d$ над конечным полем $\mathrm{GF}(2^n)$. Были получены некоторые ограничения на выбор d, при которых не существует такой линейной векторной функции L, что $F + L$ — взаимно однозначная APN-функция.

В данной работе предложен алгоритм поиска взаимно однозначных APN-функций через 2-в-1 APN-функции. Алгоритм можно разбить на три этапа. На первом этапе строятся всевозможные символьные последовательности, потенциально представляющие собой вектор значений некоторой 2-в-1 APN-функции. На следующем этапе символам в построенных последовательностях присваиваются двоичные векторы, удовлетворяющие специальным ограничениям, в результате чего получаются 2-в-1 APN-функции. На заключительном этапе для каждой построенной функции F мы ищем

аффинную функцию, если таковая существует, которая в сумме с F даёт APN-перестановку.

В работе для $n = 5$ и 6 найдены примеры 2-в-1 APN-функций и соответствующих линейных функций, дающих в сумме взаимно однозначные функции. Ниже представлены 2-в-1 функция F от пяти переменных, которая эквивалентна APN-перестановке, и сответствующая линейная функция A:
$F = (0\ 9\ 29\ 19\ 16\ 29\ 4\ 20\ 23\ 16\ 2\ 30\ 18\ 20\ 1\ 2\ 1\ 28\ 0\ 4\ 25\ 19\ 18\ 30\ 14\ 23\ 28\ 14\ 25\ 6\ 9\ 6)$;
$A = (x_2 \oplus x_3 \oplus x_4, x_4 \oplus x_5, x_1 \oplus x_4, x_1 \oplus x_2 \oplus x_3 \oplus x_4, x_3 \oplus x_4)$.

Интересно, что при $n = 5$ для всех пяти существующих (с точностью до аффинной эквивалентности) APN-перестановок найдены 2-в-1 APN-функции, которые в сумме с линейными функциями дают эти перестановки.

Ниже представлены 2-в-1 APN-функция F от шести переменных и соответствующая линейная функция A, такие, что $F \oplus A$ — единственная известная (с точностью до эквивалентности) на данный момент APN-перестановка от чётного числа переменных, полученная в работе [3]:

$F = (54\ 63\ 48\ 50\ 4\ 38\ 40\ 1\ 63\ 38\ 45\ 11\ 8\ 32\ 42\ 29\ 54\ 11\ 7\ 36\ 14\ 46\ 23\ 8\ 36\ 51\ 4\ 25\ 9\ 25\ 59\ 32\ 16\ 60\ 59\ 8\ 42\ 1\ 41\ 14\ 50\ 31\ 9\ 23\ 60\ 12\ 21\ 29\ 27\ 24\ 21\ 46\ 27\ 41\ 53\ 53\ 40\ 16\ 51\ 7\ 12\ 31\ 45\ 24)$;

$A = (x_1 \oplus x_2 \oplus x_6, x_1 \oplus x_2 \oplus x_6, x_1 \oplus x_2 \oplus x_4 \oplus x_6, x_1 \oplus x_2 \oplus x_6, x_1 \oplus x_2 \oplus x_4 \oplus x_6, x_4 \oplus x_6)$.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentily uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. *Глухов М. М.* О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7. № 4. С. 29–50.
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An apn permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
4. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3(5). С. 14–20.
5. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.
6. *Виткуп В. А.* О специальном подклассе векторных булевых функций и проблеме существования APN-перестановок // Прикладная дискретная математика. Приложение. 2016. № 9. С. 19–21.
7. *Pasalic E. and Charpin P.* Some results concerning cryptographically significant mappings over GF(2^n) // Designs, Codes and Cryptography. 2010. V. 57. P. 257–269.

УДК 519.7 DOI 10.17223/2226308X/10/15

СВОЙСТВА КООРДИНАТНЫХ ФУНКЦИЙ ОДНОГО КЛАССА ПОДСТАНОВОК НА $\mathbb{F}_2^n$

Л. А. Карпова, И. А. Панкратова

В классе $\mathcal{F}_n$ подстановок на $\mathbb{F}_2^n$, координатные функции которых существенно зависят от всех переменных, рассматривается подкласс $\mathcal{K}_n$, подстановки в котором получены из тождественной подстановки с помощью n независимых транспозиций. Приводятся некоторые свойства координатных функций подстановок из $\mathcal{K}_n$. Экспериментально подсчитана мощность $|\mathcal{K}_n|$ для $n = 3, \ldots, 6$.

Ключевые слова: *векторная булева функция, обратимые функции, нелиней-*