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 $\mathbb{F}_2^n$[1]

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 $n = 3, \ldots, 6$.

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Ключевые слова: *векторная булева функция, обратимые функции, нелинейность булевой функции, корреляционная иммунность, алгебраическая иммунность.*

Для $n \in \mathbb{Z}$ обозначим через $\mathcal{F}_n$ класс функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, где $F = (f_1 \dots f_n)$, таких, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят от всех n переменных и функция F — подстановка (т. е. обратима). В [1] предложен алгоритм построения некоторой функции из $\mathcal{F}_n$, который состоит в следующем: стартуя с тождественной подстановки F, на i-м шаге, $i = 1, \dots, n$, выбираем пару наборов a, b, отличающихся только в i-й компоненте и не выбранных на предыдущих шагах, и меняем местами значения $F(a)$ и $F(b)$. Обозначим класс подстановок, которые можно получить алгоритмом (при всевозможных способах выбора пар a, b), через $\mathcal{K}_n$. В [1] доказано, что $\mathcal{K}_n \neq \varnothing$ для всех $n > 2$ и $\mathcal{K}_2 = \mathcal{F}_2 = \varnothing$. В данной работе приведены результаты исследования функций из $\mathcal{K}_n$.

Для булевой функции f от n переменных обозначим $\mathrm{w}(f)$ вес функции f, $\deg f$ — её степень, N_f — нелинейность (расстояние до класса аффинных функций $\mathcal{A}(n)$), $\mathrm{cor}(f)$ — максимальный порядок корреляционной иммунности, $\mathrm{AI}(f)$ — алгебраическую иммунность; пусть $\mathrm{d}(f, g)$ — расстояние между функциями f и g.

Утверждение 1. Пусть $F = (f_1 \dots f_n) \in \mathcal{K}_n$, $n > 2$. Тогда для всех $i \in \{1, \dots, n\}$ имеет место:

1) $\deg f_i = n - 1$;
2) $N_{f_i} = 2$;
3) $\mathrm{cor}(f_i) = 0$;
4) $\mathrm{AI}(f_i) = 2$.

Доказательство.

1) По построению $\mathrm{d}(f_i, x_i) = 2$, т. е. $\mathrm{w}(f_i \oplus x_i) = 2$. По утверждению о связи веса и степени функции [2, лемма 3] $\mathrm{w}(f_i \oplus x_i) \geqslant 2^{n - \deg(f_i \oplus x_i)}$. Отсюда получаем $\deg(f_i \oplus x_i) = n - 1$ и, ввиду равенства $\deg(f_i \oplus x_i) = \deg f_i$, свойство 1 доказано.

2) $N_{f_i} \leqslant 2$, так как $\mathrm{d}(f_i, x_i) = 2$ и $x_i \in \mathcal{A}(n)$; $N_{f_i} \neq 0$, так как $\deg f_i = n - 1 > 1$; $N_{f_i} \neq 1$, так как f_i и все аффинные функции, кроме констант, уравновешены, а векторы значений уравновешенных функций не могут отличаться ровно на одном наборе.

3) Свойство следует из неравенства Зигенталера [2, лемма 4] для уравновешенных функций: $\mathrm{cor}(f_i) \leqslant n - \deg f_i - 1 = 0$.

4) В [3, теорема 1] получена следующая оценка: $N_f \geqslant 2 \sum\limits_{i=0}^{\mathrm{AI}(f)-2} \binom{n-1}{i}$. С учётом $N_{f_i} = 2$ отсюда получаем $\mathrm{AI}(f_i) \leqslant 2$. С другой стороны, никакая аффинная функция $g \neq \mathrm{const}$ не может быть аннигилятором f_i, так как иначе, ввиду уравновешенности f_i и g, получим $g = \bar{f}_i$, что не так ($f_i \notin \mathcal{A}(n)$). То же верно и для аннигилятора функции $f_i \oplus 1$. Следовательно, $\mathrm{AI}(f_i) = 2$.

Утверждение доказано. ■

Замечание 1. Утверждение 1 остаётся верным и для модификации алгоритма построения подстановок из класса $\mathcal{K}_n$, предложенной в [1] и состоящей в том, что отправной точкой алгоритма является не обязательно тождественная подстановка, а такая, что каждая координатная функция существенно зависит ровно от одной переменной (т. е. $f_i = x_j$ или $f_i = \overline{x_j}$).

Приведём некоторые экспериментальные данные. В таблице указаны мощности классов $\mathcal{K}_n$ для $n = 3, \dots, 6$; для построения всех функций из $\mathcal{K}_6$ понадобилось больше 1,5 ч. Мощность $|\mathcal{K}_n|$ быстро растёт с ростом n, тем не менее $|\mathcal{K}_n| \ll |\mathcal{F}_n|$; например, в результате перебора $8! = 40\,320$ подстановок на $\mathbb{F}_2^3$ установлено, что $|\mathcal{F}_3| = 24\,576$.

n	$\lvert\mathcal{K}_n\rvert$
3	8
4	608
5	250 624
6	390 317 056

Обозначим $\mathcal{K}'_n$ класс подстановок, которые можно получить с помощью модификации алгоритма (см. замечание 1). Очевидно, что $|\mathcal{K}'_n| \leqslant 2^n n! |\mathcal{K}_n|$ (2^n способов инвертировать переменные и $n!$ способов переставить их); в частности, для $n = 3$ эта граница равна 384, для $n = 4$ — уже 233 472 и т. д. Вопрос о достижимости границы и близости к ней мощности $|\mathcal{K}'_n|$ составляет предмет дальнейших исследований.

Экспериментально подсчитаны характеристики координатных функций f_i подстановок из $\mathcal{F}_n$. Для $n = 3$ оказалось, что всегда $N_{f_i} \in \{0, 2\}$, $\deg f_i \in \{1, 2\}$. Все подстановки на $\mathbb{F}_2^4$ перебрать не удалось; из 10 000 000 опробованных оказалось, что классу $\mathcal{F}_4$ принадлежат 7 842 917 и для них $N_{f_i} \in \{2, 4\}$ и $\deg f_i \in \{2, 3\}$.

Поскольку отмеченные в утверждении 1 свойства 2–4 координатных функций подстановок из $\mathcal{K}_n$ (а в силу замечания 1 — и из $\mathcal{K}'_n$) свидетельствуют об их криптографической слабости, актуальна задача разработки алгоритма построения *любой* подстановки класса $\mathcal{F}_n$. Кроме того, для синтеза криптосхем с функциональными ключами [4, 5] интересны обратимые векторные булевы функции, координатные функции которых зависят *от заданного числа* (не от всех) аргументов. В [1, 6] полностью решена задача существования таких функций; остаётся открытым вопрос их построения и исследования криптографических свойств.

ЛИТЕРАТУРА

1. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
2. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Матем. вопросы кибернетики. 2002. Вып. 11. С. 91–148.
3. *Лобанов М. С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Т. 18. Вып. 3. С. 152–159.
4. *Агибалов Г. П.* SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43–48.
5. *Агибалов Г. П.* Криптоавтоматы с функциональными ключами // Прикладная дискретная математика. 2017. № 36. С. 59–72.
6. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.