3. *Варшамов Р. Р.* Оценка числа сигналов в кодах с коррекцией ошибок // Доклады АН СССР. 1957. С. 739–741.
4. *May A., Meurer A., and Thomae E.* Decoding random linear codes in $O(2^{0.054n})$ // Proc. Asiacrypt'2011. Seoul, South Korea, December 04–08, 2011. P. 107–124.

УДК 519.7 DOI 10.17223/2226308X/12/65

О ПОЧТИ СОВЕРШЕННЫХ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЯХ И РАЗДЕЛЯЮЩЕМ СВОЙСТВЕ МУЛЬТИМНОЖЕСТВ

М. А. Сорокин, М. А. Пудовкина

Рассматриваются некоторые классы APN-преобразований относительно возможности построения интегральных различителей с помощью разделяющего свойства. Проведён вычислительный эксперимент по определению величины $\lceil n/d \rceil$ для выбранных APN-преобразований $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, где d — алгебраическая степень. Из полученных результатов следует, что не все APN-преобразования имеют наилучшее значение $\lceil n/d \rceil = 2$. Выделены APN-преобразования с параметрами, наиболее оптимальными для противодействия интегральному анализу с помощью разделяющего свойства.

Ключевые слова: *APN-преобразование, разделяющее свойство, интегральный различитель, интегральный метод.*

Разностный метод и его обобщения являются одними из основных методов анализа симметричных шифрсистем. Один из этапов разностного метода заключается в нахождении элементов матрицы вероятностей переходов разностей компонент функции зашифрования, включая S-боксы. В работе [1] для противодействия разностному методу при синтезе алгоритмов блочного шифрования в качестве S-бокса предложено использовать APN-преобразование (если оно существует).

Определение 1 [1]. Преобразование $s : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ называется APN-преобразованием, если для каждых ненулевых элементов $\alpha, \beta \in \mathrm{GF}(2^n)$ уравнение $s(x + \alpha) - s(x) = \beta$ имеет два или нуль решений.

Актуальной задачей является исследование APN-преобразований относительно других методов криптоанализа, в частности относительно интегрального метода. В [2] приводится способ построения интегрального различителя с использованием разделяющего свойства (англ. division property).

Пусть V_n — n-мерное векторное пространство над полем $\mathrm{GF}(2)$; $\|\alpha\|$ — вес Хэмминга вектора α; α_i — i-я координата вектора $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n$, $i \in \{1, \ldots, n\}$.

Для каждого элемента $\beta \in \mathrm{GF}(2)$ положим $\beta^1 = \beta$, $\beta^0 = 1$. Тогда корректно определено отображение $\pi : V_n \times V_n \to V_n$, заданное условием

$$\pi : (\alpha, \delta) \mapsto \prod_{i=1}^{n} \alpha_i^{\delta_i}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in V_n, \ \delta = (\delta_1, \ldots, \delta_n) \in V_n.$$

Далее будем рассматривать отображение $\pi(x, \delta)$ только при фиксированном $\delta \in V_n$.

Определение 2 [2]. Пусть $n \in \mathbb{N}$, $k \in \{1, \ldots, n\}$, $S_k^{(n)} = \{\alpha \in V_n : k \leqslant \|\alpha\|\}$. Говорят, что мультимножество X с носителем V_n имеет разделяющее свойство $D_k^{(n)}$, если для каждого $\delta \in V_n \setminus S_k^{(n)}$ выполняется равенство $\bigoplus\limits_{\alpha \in X} \pi(\alpha, \delta) = 0$.

Будем говорить, что мультимножество Y с носителем V_n получено *применением* векторной булевой функции $g : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ к мультимножеству X с носителем V_n, если элементы Y есть результаты применения функции g к каждому элементу мультимножества X.

Теорема 1 [2]. Пусть $s : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ — преобразование алгебраической степени d и мультимножество X с носителем V_n имеет разделяющее свойство $D_k^{(n)}$, $k \in \{1, \ldots, n-1\}$. Тогда мультимножество, полученное применением s к X, имеет разделяющее свойство $D_{\lceil k/d \rceil}^{(n)}$.

Из теоремы 1 следует, что чем больше значение $\lceil n/d \rceil$, тем для большего числа раундов существует интегральный различитель, получаемый посредством применения предложенного в работе [2] алгоритма.

В настоящей работе проведён вычислительный эксперимент по определению величины $\lceil n/d \rceil$ для некоторых APN-преобразований $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, приведённых в [3]. Из полученных результатов следует, что не все APN-преобразования имеют наилучшее значение $\lceil n/d \rceil = 2$. Результаты отражены в табл. 1–3 (указаны лучшие параметры, если они найдены).

Таблица 1

APN-преобразования и их параметры, при которых $\lceil n/d \rceil = 2$

Формула и условия	Параметры
x^j, $j = 2^n - 2$, $n = 2k + 1$	$n \in \{3, 5, \ldots, 11\}$
x^j, $j = 2^t + 2^{0,5t} - 1$, если $t = 2k, k \in \mathbb{N}$; $j = 2^t + 2^{1,5t+0,5} - 1$, если $t = 2k+1, k \in \mathbb{N}$; $n = 2t + 1$	Для $n = 7, t = 3$ и $n = 11, t = 5$ имеем $d = 4$ и $d = 6$ соответственно
x^j, $j = 2^{2t} - 1$, $n = 2t + 1$, $t \in \mathbb{N}$	$t \in \{1, \ldots, 6\}$
x^j, $j = 2^{2i} - 2^i + 1$, $(i, n) = 1$	$(n, i) \in \{(9, 4), (9, 5)\}$, $d = 5$
x^j, $j = 2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$, $n = 5i$, $i \in \mathbb{N}$	$i \in \{1, 2\}$
$\left(x + \mathrm{tr}_{n/3}\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right) + \right.$ $\left. + \mathrm{tr}(x)\mathrm{tr}_{n/3}\left(x^{2^i+1} + x^{2^{2i}(2^i+1)}\right)\right)^{2^i+1}$, $n = 3k$, $k = 2l$, $l \in \mathbb{N}$, $(i, n) = 1$	$n = 6$

Таблица 2

APN-преобразования и их параметры, при которых $\lceil n/d \rceil = 6$

Формула и условия	Параметры
$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$, $n = 3k$, $k \in \mathbb{N}$, $(k, 3) = (s, 3k) = 1$, $k \geqslant 4$, $i \equiv sk \pmod 3$, $m = 3i$, $\mathrm{ord}(w) = 2^{2k} + 2^k + 1$	$n = 12$
$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$, $n = 4k$, $k \in \mathbb{N}$, $(k, 2) = (s, 2k) = 1$, $k \geqslant 3$, $i \equiv sk \pmod 4$, $m = 4i$, $\mathrm{ord}(w) = 2^{3k} + 2^{2k} + 2^k + 1$	$n = 12$

Таблица 3

APN-преобразования, для которых $\lceil n/d \rceil$ растёт с ростом n

Формула и условия	Параметры
x^j, $j = 2^i + 1$, $(i, n) = 1$	$n \in \{2, \ldots, 12\}$, $d = 2$
$x^{2^i+1} + \left(x^{2^i} + x + 1\right) \operatorname{tr}\left(x^{2^i+1}\right)$, $n \geqslant 4$, $n = 2k + 1$, $k \in \mathbb{N}$, $(i, n) = 1$	$n \in \{4, 6, \ldots, 12\}$, $d = 3$
$x^3 + \operatorname{tr}(x^9)$, $n > 2p \geqslant 7$ для такого наименьшего p, что $p > 1$, $p \neq 3$ и $(p, n) = 1$	$n \in \{7, 9, 11, 12, 13\}$, $d = 2$

ЛИТЕРАТУРА

1. *Nyberg K. and Knudsen L.R.* Provable security against differential cryptanalysis // CRYPTO 1992. LNCS. 1993. V. 740. P. 566–574.
2. *Todo Y.* Structural evaluation by generalized integral property // EUROCRYPT 2015. P. I. LNCS. 2015. V. 9056. P. 287–314.
3. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. Т. 5. № 3. С. 14–20.