Лемма 1 следует из свойств des, а её применение при нечётном $n > 1$ с определением 1 даёт $|(R_n \cap \overline{CM}(\mathbb{Z}_n))| = n \prod\limits_{p|n}(1 - 2p^{-1})$ и $|(R_n \cap SCM(\mathbb{Z}_n))| = n \prod\limits_{p|n}(1 - 3p^{-1})$.

Лемма 2. Если $\sigma \in \overline{CM}(\mathbb{Z}_n)$, то $\mathrm{des}(\sigma) + \mathrm{des}(\widetilde{\sigma}) = n - 1$.

Применение формулы вычисления статистики des к перестановкам из определения 1 даёт требуемое. Так как $\deg \widetilde{A}_{n-1}(t) = n-2$, то по лемме 2 имеем $t^{n-1}\widetilde{A}_{n-1}(t^{-1}) = \widetilde{A}_{n-1}(t)$, а также $\deg \widehat{A}_{n-1}(t) = n - 2$, $\widehat{A}_{n-1,1} = 0$ и $t^n \widehat{A}_{n-1}(t^{-1}) = \widehat{A}_{n-1}(t)$.

Определение 2. $\tau = \tau_1 \ldots \tau_{n-1} \in S_{n-1}$, $\tau = \mathbf{d}\sigma$ назовём смещением $\sigma \in S_{n-1}$, если биекция $\mathbf{d} : S_{n-1} \to S_{n-1}$ задана выражениями $\tau_i = \sigma_{i+1} - \sigma_i \pmod n$, $i = 1, \ldots, n-2$, и $\tau_{n-1} = n - \sigma_1$, а порядком $d = d(\sigma)$ назовём наименьшее $k \in \mathbb{Z}^+$, для которого $\mathbf{d}^k\sigma = \sigma$.

Лемма 3. Если $\sigma \in S_{n-1}$, то $\mathrm{des}(\mathbf{d}\sigma) = \mathrm{des}(\sigma)$ и $d|n$.

Равенство $\mathrm{des}(\mathbf{d}\sigma) = \mathrm{des}(\sigma)$ получается из свойств des, а делимость $d|n$ следует из определения 2, так как повторное применение $\mathbf{d}$ разбивает S_{n-1} на классы эквивалентности (так, $\mathbf{d}r\varepsilon = r\varepsilon$, $r\varepsilon \in R_n$, т. е. $d = 1$). При $n > 4$ в словах $\mathbf{d}^k\sigma \in S_{n-1}$, $k = 0, \ldots, d-1$, имеется $n/d - 1$ неподвижных символов σ_i, кратных d, с индексом i, кратным d.

Теоремы 1–3 доказываются с помощью лемм 1, 2 и леммы 3, справедливой также на $\overline{CM}(\mathbb{Z}_n)$ и $SCM(\mathbb{Z}_n)$, причём применяемый метод дополнительно даёт следующие сравнения: $|CM(\mathbb{Z}_n)| \equiv 1 \pmod 2$ при нечётном n и $|SCM(\mathbb{Z}_n)| \equiv 0 \pmod 2$ при $n > 1$.

ЛИТЕРАТУРА

1. *Стенли Р.* Перечислительная комбинаторика. Т. 1. М.: Мир, 1990.
2. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.
3. *Hsiang J., Hsu D. F., and Shieh Y. P.* On the hardness of counting problems of complete mappings // Discr. Math. 2004. V. 277. P. 87–100.
4. `http://oeis.org/A003111` — Sloane N. J. A. The on-line encyclopedia of integer sequences.

УДК 519.7

О НЕКОТОРЫХ ОТКРЫТЫХ ВОПРОСАХ В ОБЛАСТИ APN-ФУНКЦИЙ

В. А. Виткуп

Приведены открытые вопросы в области APN-функций, связанные с их построением. Перечислены некоторые известные результаты в данном направлении. Доказано необходимое и достаточное условие того, что сумма двух APN-функций является APN-функцией.

Ключевые слова: *векторная булева функция, APN-функция.*

Работа К. Ньюберг [1] положила начало новому направлению в исследовании векторных булевых функций — изучению совершенно и почти совершенно нелинейных векторных булевых функций, обладающих наилучшей стойкостью к дифференциальному криптоанализу.

Векторная булева функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ называется *APN-функцией* (Almost Perfect Nonlinear), 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 настоящее время APN-функции активно изучаются, но до сих пор многие важные вопросы остаются открытыми. Например, не известно точное число таких функций, нижние и верхние оценки числа APN-функций, оценка их алгебраической степени. Не так многочисленны и известные конструкции APN-функций — степенные функции вида $F(x) = x^d$ и несколько полиномиальных (см. подробнее обзоры в [2, 3]). Очень интересен вопрос о конструкции APN-функции с помощью композиции или суммы двух функций и о нахождении итеративных конструкций [4].

Важное место в исследовании векторных функций занимает проблема существования взаимно однозначных APN-функций при чётном n. В своё время была выдвинута гипотеза, что для чётного числа переменных APN-перестановок не существует, однако в 2009 г. Дж. Диллон и др. [5] опровергли это предположение, построив взаимно однозначную APN-функцию над $\mathbb{F}_{2^6}$, которая CCZ-эквивалентна APN-функции, не являющейся перестановкой. Разработанный авторами [5] метод обобщался для большего числа переменных, однако с его помощью им не удалось найти APN-перестановки от 8 и 10 переменных. Интересно, что при решении этой задачи авторы [5] в неявном виде использовали для построения композицию двух перестановок.

Пусть векторная булева функция F имеет следующий вид:

$$F(x) = (f_1(x), \ldots, f_n(x)), \quad \text{где } f_i(x) = a^F_{i,0} \oplus a^F_{i,1}x_1 \oplus \ldots \oplus a^F_{i,1\ldots n}x_1x_2\ldots x_n.$$

Утверждение 1. Пусть F_1 и F_2 — APN-функции из $\mathbb{F}_2^2$ в $\mathbb{F}_2^2$. Тогда $F = F_1 \oplus F_2$ — APN-функция тогда и только тогда, когда $(a^{F_1}_{1,12} \oplus a^{F_2}_{1,12}) \vee (a^{F_1}_{2,12} \oplus a^{F_2}_{2,12}) = 1$.

Всего в $\mathbb{F}_2^2$ существует 192 APN-функции, значит, всевозможных пар $\mathrm{C}^2_{192} = 18336$. Из них 12288 пар F_1 и F_2, сумма которых является APN-функцией, что составляет около 67 %.

Перечислим некоторые интересные открытые вопросы в области APN-функций, связанные с проблемой их построения.

- Как построить APN-функцию путём композиции или суммы двух векторных функций? Какими свойствами должна обладать такая пара функций?
- Можно ли представить произвольную APN-функцию в виде композиции двух векторных функций? В том числе функций, обладающих более «простыми» характеристиками (например, меньшей алгебраической степенью или более коротким полиномиальным представлением)? Так, в работе [5] приведён пример взаимно однозначной APN-функции над $\mathbb{F}_{2^6}$ алгебраической степени 4, которую можно представить через композицию двух векторных булевых функций меньших степеней — 2 и 3.
- Пусть F — APN-функция, действующая из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Какими свойствами обладают её подфункции? Существует ли характеризация APN-функции через её компонентные булевы функции? Одна из возможных характеризаций APN-функций через подфункции предложена в [4].
- Описать группу автоморфизмов класса APN-функций, APN-перестановок. Какие преобразования не выводят функцию (перестановку) за рамки класса?
- Исследовать метрические свойства класса APN-функций. Некоторые продвижения по этому вопросу недавно получены в [6].
- Осуществить классификацию квадратичных APN-функций от n переменных. Напомним, что квадратичная APN-функция также является AB-функцией, т. е. её компонентные функции находятся на максимальном расстоянии от класса аффинных функций, что означает оптимальную стойкость к линейному криптоанализу.

Ответы на эти вопросы помогут получить новые конструкции APN-функций, включая итеративные и композиционные, а также упростить их программную и аппаратную реализацию в симметричных шифрах.

ЛИТЕРАТУРА

1. *Nyberg K.* Perfect nonlinear S-boxes // LNCS. 1991. V. 547. P. 378–386.
2. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Habilitation Thesis. University of Paris, 8 Sept. 2013.
3. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
4. *Городилова А. А.* Характеризация APN-функций через подфункции // Прикладная дискретная математика. Приложение. 2014. № 7. С. 15–16.
5. *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.
6. *Шушуев Г. И.* Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.

УДК 512.62

ЗАДАЧА, ЭКВИВАЛЕНТНАЯ ПРОВЕРКЕ ПРОСТОТЫ ЧИСЕЛ ФЕРМА

Кр. Л. Геут, С. С. Титов

Работа посвящена постановке задачи, эквивалентной проверке простоты чисел Ферма. Сформулирована задача последовательного построения неприводимых многочленов над конечными полями характеристики два и три, эквивалентная проверке простоты чисел. Показана эквивалентность построения всех неприводимых симметричных многочленов степени 2^{k+1} над полем GF(2) и определения простоты числа Ферма 2^{2^k}. Рассмотрена взаимосвязь между проверкой простоты чисел Ферма и построением неприводимых многочленов над GF(3).

Ключевые слова: *неприводимый многочлен, простые числа, числа Ферма.*

Неприводимые многочлены — аналог простых чисел — имеют большую ценность в теории информации, помехоустойчивом кодировании, работе конечных автоматов, стандартах защиты информации. Поэтому актуален поиск взаимосвязи между ними [1 – 4].

Интерес представляют многочлены степени 2^n над полем GF(2), коэффициенты которых при преобразовании в битовые строки широко используются для работы ЭВМ. В кодировании применяются симметричные (самовозвратные) многочлены [5] порядка $p = 2^{2^k} + 1$ степени $N = 2^{k+1}$. Легко показать, что если неприводимый над GF(2) многочлен имеет степень $2m$ и порядок $2^m + 1$, то он симметричен.

Утверждение 1. Простота числа Ферма $p = 2^{2^k} + 1$ эквивалентна равенству p порядков всех неприводимых симметричных многочленов степени $n = 2^{k+1}$ над GF(2).

Так, например, при $k = 0$, $p = 3$ имеется один симметричный многочлен $x^2 + x + 1$ степени 2, порядка 3; при $k = 1$, $p = 5$ — один симметричный многочлен $x^4+x^3+x^2+x+1$ степени 4, порядка 5; при $k = 2$, $p = 17$ — два многочлена степени 8, порядка 17: $x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$ и $x^8 + x^5 + x^4 + x^3 + 1$; при $k = 4$, $p = 65537$ имеется 2048 многочленов степени 32 порядка p [6].

При $k = 5$ число $p = 4294967297 = 64 \cdot 6700417$ непростое, это означает, что неприводимые симметричные многочлены степени 64 имеют порядок 4294967297, или 641, или 6700417. Последовательным подбором коэффициентов были найдены 10 неприводимых симметричных многочленов степени 64 порядка 641 [4].