2009 Теоретические основы прикладной дискретной математики №3(5)

DOI 10.17223/20710410/5/2

УДК 681.03

ПОЧТИ СОВЕРШЕННЫЕ НЕЛИНЕЙНЫЕ ФУНКЦИИ[1]

М. Э. Тужилин

Российский государственный гуманитарный университет, г. Москва, Россия

E-mail: mtmt@rambler.ru

Сделан обзор публикаций, посвященных почти совершенным нелинейным функциям, их свойствам и построению.

Ключевые слова: *почти совершенные нелинейные функции, почти бент-функции, криптография.*

1. PN-функции

Появление в открытой криптографии разностного метода (Differential cryptanalysis [1]) вызвало необходимость разработки подходов к построению тех классов S-боксов, которые являются оптимальными для противостояния данному методу. Одной из работ, посвященной данной проблеме и оказавшей существенное влияние на дальнейшие исследования, явилась статья K. Nyberg 1991 г. [2]. В ней было предложено два подхода к построению оптимальных S-боксов, появилось понятие совершенной нелинейной функции (Perfect Nonlinear, или, сокращенно, PN-функции).

Пусть далее натуральные m и n связаны соотношением $m \leqslant n$.

Функция $F\colon (Z/q)^n \to (Z/q)^m$ называется **совершенной нелинейной**, если для любого фиксированного ненулевого $a \in (Z/q)^n$ функция $F(x+a) - F(x)$ (ее называют производной по направлению a) принимает каждое значение из $(Z/q)^m$ ровно при q^{n-m} значениях x.

В [2, 3] приведен ряд результатов относительно PN-функций, отмечена связь их с бент-функциями, в частности приведена теорема о том, что PN-функция $F\colon (Z/q)^n \to (Z/q)$ является бент-функцией; обратное верно, если q — простое.

Однако требование к функции быть совершенной нелинейной оказалось слишком жестким, число таких функций очень невелико, а для многих важных для практики значений q и n они просто не существуют. Поэтому большее внимание уделяется введенному в [4] в 1992 г. понятию почти совершенной нелинейной функции (Almost Perfect Nonlinear или, сокращенно, APN-функции).

2. APN-функции

Всюду далее поле $\mathrm{GF}(p^n)$ отождествляется с векторным пространством $\mathrm{GF}(p)^n$.

Функция $F\colon \mathrm{GF}(p^n) \to \mathrm{GF}(p^m)$ называется **APN-функцией**, если для любых $a \neq 0$ из $\mathrm{GF}(p^n)$ и b из $\mathrm{GF}(p^m)$ уравнение $F(x+a) - F(x) = b$ имеет не более двух решений.

Строго говоря, в [4] определение APN-функции дано было для подстановок, заданных на $\mathrm{GF}(2^n)$, но в последующих работах это определение было расширено.

В [5] изложен подход к характеризации PN- и APN-функций на основе теории полуполей.

[1] Результаты работы докладывались на Международной конференции с элементами научной школы для молодёжи, г. Омск, 7–12 сентября 2009 г.

В [3] K. Nyberg ввела и более общее понятие — функции, названной ею differentially δ-uniform, для которой в приведенном выше определении APN-функции вместо двух решений уравнения рассматривается произвольное натуральное число δ. Таким образом, differentially δ-uniform функция F является PN-функцией, если $\delta = 1$, и APN-функцией, если $\delta = 2$.

Наибольший интерес исследователей прикован к случаю $p = 2$.

Как показано в [6], отношение числа APN-функций $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ степени d при $d \equiv 0, 3 \pmod 4$ к числу всех функций $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ степени d стремится к нулю с ростом n.

Многие свойства APN-функций, заданных на $\mathrm{GF}(2^n)$, описаны в обзоре [7]. Основным инструментом исследований свойств функций является их спектр, состоящий из коэффициентов Фурье. Отдельные разделы обзора посвящены квадратичным функциям (то есть функциям, чья алгебраическая степень не превышает числа 2), степенным функциям $F\colon \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$ вида $F(x) = x^d$ и APN-подстановкам — таким APN-функциям, которые являются подстановками на $\mathrm{GF}(p^n)$. Приведен список открытых проблем в области исследования APN-функций.

3. APN-подстановки

В [8] представлено три подхода к построению APN-подстановок, действующих на $\mathrm{GF}(2^n)$. Однако все они относятся к случаю нечетного n. Вопрос о существовании APN-подстановок при четном n до сих пор остается открытой проблемой. В [3] доказано, что среди квадратичных функций таких быть не может. Позднее было доказано, что подстановка F, действующая на $\mathrm{GF}(2^n)$, не может быть APN-подстановкой, если $n = 2$ или $n = 4$.

Обратная к APN-подстановке — тоже APN-подстановка.

В [9] изучаются подстановки вида $G(x) + af(x)$, где $f(x)$ — булева функция, $a \in \mathrm{GF}(2^n)$, а $G(x)$ — подстановка или линейная функция $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$.

В силу того, что APN-подстановок при четном n до сих пор найти не удалось, актуально изучение differentially δ-uniform подстановок F с $\delta = 4$. Отметим, что именно такая подстановка используется в алгоритме AES.

4. AB-функции

Напомним, что с любой функцией $F\colon \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ можно связать n координатных булевых функций и множество их линейных комбинаций, называемых компонентами функции F.

Понятие APN-функции тесно связано с понятием почти бент-функции (Almost Bent, или AB-функции), введенном в [10].

Функция $F\colon \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ называется AB-функцией, если минимальное по Хеммингу расстояние между всеми компонентами функции F и всеми аффинными функциями максимально.

Это минимальное расстояние называется показателем нелинейности функции F, и максимально возможное значение его равно $2^{n-1} - 2^{\frac{n-1}{2}}$ [11]. AB-функции в отличие от APN-функций существуют только при нечетном n и являются наиболее стойкими по отношению к линейному криптоанализу. Кроме того, любая AB-функция является APN-функцией, и при нечетном n любая квадратичная функция является APN-функцией тогда и только тогда, когда она является AB-функцией [12]. Эта работа, появившаяся в 1998 г., стала важной вехой на пути исследований APN-функций. В ней,

в частности, отмечается связь APN-функций с линейными кодами длины $2^n - 1$, имеющими оптимальное кодовое расстояние.

5. Степенные функции

Относительно степенных функций, заданных на $\mathrm{GF}(2^n)$, в [12] доказано, что если h делит n и $d = k(2^h - 1) + 2^r$ при целых k и r, то степенная функция $F(x) = x^d$ не может быть APN-функцией. Отметим, что использование степенных функций в качестве S-боксов, с одной стороны, привлекательно для разработчиков криптосхем, так как это упрощает реализацию криптоалгоритмов, но, с другой стороны, может привести к построению криптоаналитических методов, основанных на «простом» виде функции.

6. Преобразования, сохраняющие свойства APN и AB

Для построения новых APN- или AB-функций из имеющихся представляют большой интерес те преобразования функций, при которых сохраняются свойства «быть APN-функцией» или «быть AB-функцией» соответственно.

Пусть F, A, A_1, A_2 суть функции $\mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$. Если F есть APN-функция, A_1, A_2 — аффинные подстановки и A — аффинная функция, то $F' = A_1 \circ F \circ A_2 + A$ — тоже APN-функция. В этом случае F и F' называются расширенно аффинно эквивалентными (**EA-эквивалентными**) и аффинно эквивалентными при $A = 0$.

До недавнего времени известны были только такие APN-функции, которые EA-эквивалентны степенным функциям $F(x) = x^d$. Только в 2006 г. было доказано [13], что функции вида $x^3 + ux^{36}$, заданные на полях $\mathrm{GF}(2^{10})$ и $\mathrm{GF}(2^{12})$, при определенных элементах u из этих полей являются APN-функциями, не EA-эквивалентными степенным функциям. В табл. 1 приведены все известные на данный момент серии APN-функций, EA-эквивалентных степенным функциям, заданным на поле $\mathrm{GF}(p^n)$.

Welch and Niho APN-функции из табл. 1 являются AB-функциями. Для нечетного n AB-функциями являются функции Gold и Kasami.

В [12] было введено понятие Carlet-Charpin-Zinoviev эквивалентности (CCZ-эквивалентности), а именно: отображения F_1 и F_2 поля $\mathrm{GF}(p^n)$ на себя называются **CCZ-эквивалентными**, если графы отображений F_1 и F_2, то есть множества $\{(x, F_1(x)) \mid x \in \mathrm{GF}(p^n)\}$ и $\{(x, F_2(x)) \mid x \in \mathrm{GF}(p^n)\}$ являются аффинно эквивалентными.

Из определения следует, что отображения F_1 и F_2 CCZ-эквивалентны тогда и только тогда, когда существует аффинный автоморфизм $L = (L_1, L_2)$ декартова произведения $\mathrm{GF}(p^n) \times \mathrm{GF}(p^n)$, такой, что выполнено

$$y = F_1(x) \Leftrightarrow L_2(x, y) = F_2(L_1(x, y)).$$

CCZ-эквивалентность является более общей, чем EA-эквивалентность (любой класс EA-эквивалентности содержится в некотором классе CCZ-эквивалентности) и сохраняет свойства «быть APN-функцией» и «быть AB-функцией». Для бент-функций эти эквивалентности совпадают.

В [14] описана связь между EA-эквивалентностью и CCZ-эквивалентностью для функций $\mathrm{GF}(2^n) \to \mathrm{GF}(2^m)$. Показано, что для булевых функций (то есть при $m = 1$) эти понятия совпадают — две булевы функции CCZ-эквивалентны тогда и только тогда, когда они EA-эквивалентны.

В табл. 2 приведены серии APN-функций, CCZ-эквивалентных степенным функциям.

Таблица 1

APN-функции, EA-эквивалентные степенным функциям

Название функции	Экспонента d	Условия	Источник
Kloosterman	p^n-2	$p=2$ и n нечетно, или $p>2$ и $p\equiv 2(\mathrm{mod}\ 3)$	[3, 8]
Gold	2^i+1	$p=2$, НОД(i,n)=1	[15]
Kasami	$2^{2i}-2^i+1$	$p=2$, НОД(i,n)=1	[16]
Welch	2^t+3	$p=2$, $n=2t+1$	[17]
Niho	$2^t+2^{t/2}-1$, t — четное, $2^t+2^{\frac{3t+1}{2}}-1$, t — нечетное	$p=2$, $n=2t+1$	[18]
Инверсия	$2^{2t}-1$	$p=2$, $n=2t+1$	[3, 8]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$p=2$, $n=5i$	[19]
Helleseth, Sanberg	$\frac{p^n-1}{2}-1$	$p\equiv 3,7\ (\mathrm{mod}\ 20)$, $p^n>7$, $p^n\neq 27$, n нечетно	[20]
Dobbertin, Mills, Muller, Pott, Willems	$\frac{3^{(n+1)/2-1}}{2}$ $\frac{3^{(n+1)-1}}{8}$ $\frac{3^{(n+1)-1}}{8}+\frac{3^n-1}{2}$	$p=3$, $n\equiv 3\ (\mathrm{mod}\ 4)$ $p=3$, $n\equiv 1\ (\mathrm{mod}\ 4)$ $p=3$, $n\equiv 1\ (\mathrm{mod}\ 4)$	[21]
Felke	$\frac{3^{(n+1)/2-1}}{2}+\frac{3^n-1}{2}$	$p=3$, $n\equiv 1\ (\mathrm{mod}\ 4)$	[22]
Helleseth, Rong, Sandberg	$\frac{p^n+1}{4}+\frac{p^n-1}{2}$ $\frac{p^n+1}{4}$ $\frac{2p^n-1}{3}$ p^n-3	$p^n\equiv 3\ (\mathrm{mod}\ 8)$ $p^n\equiv 7\ (\mathrm{mod}\ 8)$ $p^n\equiv 2\ (\mathrm{mod}\ 8)$ $p=3$, $n>1$, n нечетно	[23]
Тривиальная	3	$p>3$	[20]

Таблица 2

APN-функции, CCZ-эквивалентные степенным функциям

Функция $F(x)$	Условия	Источник
$x^{2^i+1}+(x^{2^i}+x+1)\mathrm{tr}(x^{2^i+1})$	$n\geqslant 4$, n четно, НОД(i,n)=1	[24]
$[x+\mathrm{tr}_{n/3}(x^{2(2^i+1)}+x^{4(2^i+1)}+\mathrm{tr}(x)\mathrm{tr}_{n/3}(x^{2^i+1}+x^{2^{2i}(2^i+1)})]^{2^i+1}$	n четно, $n=3k$, НОД(i,n)=1	[24]

В табл. 3 приведены построенные в 2006–2007 гг. с помощью подхода C. Carlet серии APN-функций, не CCZ-эквивалентных степенным функциям.

Другой подход к построению таких функций предложен в [13]. В [25] показано, как изменить одну координатную функцию APN-функции, чтобы получить новую APN-функцию. Такой подход к построению новых APN-функций оказался весьма эффективным.

Таблица 3

APN-функции, не CCZ-эквивалентные степенным функциям

Функция $F(x)$	Условия	Источник
$x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$	$n=3k$, НОД(k,3)=НОД(s,3k)=1, $k\geqslant 4$, $i=sk \pmod 3$, $m=3i$, ord$w$=$2^{2k}+2^k+1$	[26, 27]
$x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$	$n=4k$, НОД(k,2)=НОД(s,2k)=1, $k\geqslant 3$, $i=sk \pmod 4$, $m=4i$, ord$w$=$2^{3k}+2^{2k}+2^k+1$	[28]
$x^3+\mathrm{tr}(x^9)$	$n\geqslant 7$, $n>2p$ для наименьшего $p>1$, такого, что $p\neq 3$ и НОД$(p,n)=1$	[29]
$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	$n=2m$, $m\geqslant 3$, $q=2^m$, $c^{q+1}=1$, $c\notin\lambda^{(2^i+1)(q-1)}, \lambda\in \mathrm{GF}(2)$, НОД$(i,m)=1$, $cb^q+b\neq 0$	[30]
$x(x^{2^i}+x^q+cx^{2^iq})+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$n=2m$, $m\geqslant 3$, $q=2^m$, $s\notin \mathrm{GF}(q)$, $x^{2^i+1}+cx^{2^i}+c^qx+1$ неприводим над $\mathrm{GF}(2^n)$	[30]

7. Примеры других семейств APN-функций

В [31] введено в рассмотрение семейство функций вида

$$F(x)=ux^{\frac{p^n-1}{2}}+x^{p^n-2}$$

над $\mathrm{GF}(p^n)$ ($n\geqslant 3$ и нечетно), элемент $u\in\mathrm{GF}(p^n)$ удовлетворяет условию

$$\chi(u+1)=\chi(u-1)=\chi(u),$$

где χ — мультипликативный характер поля $\mathrm{GF}(p^n)$. Доказано, что такие функции являются APN-функциями. В [32] доказано, что это семейство не CCZ-эквивалентно ни одному из известных семейств APN-функций.

В [33] построено новое семейство APN-функций

$$F(x)=bx^{2^s+1}+b^{2^k}x^{2^{k+s}+2^k}+cx2^{k+s}+2^s+\sum_{i=0}^{k-1}r_ix^{2^{i+k}+2^i},$$

где k,s — нечетные взаимно простые числа; $b,c\in\mathrm{GF}(2^{2k})$; $r_i\in\mathrm{GF}(2^k)$.

В [34] показано, что функция $\mathrm{GF}(p^{3k})\to\mathrm{GF}(p^{3k})$ вида

$$x^{p^s+1}-ux^{p^k+p^{2k+s}}$$

при выполнении условий $n=3k$, НОД$(3,k)=1$, НОД$(s,n)=t$, u — примитивный элемент поля $\mathrm{GF}(p^{3k})$, является PN-функцией, если p и n/t — нечетные, и APN-функцией, если $p=2$.

8. Классификация APN-функций при малых n

В [35] приведены результаты классификации всех APN-функций $\mathrm{GF}(2^n)\to\mathrm{GF}(2^n)$ для $n=4,5$. Вычисления производились с помощью ЭВМ, в основе их лежала

лемма о том, что функция $F\colon \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ является APN-функцией, если и только если для всех попарно различных t, u, v, w, принадлежащих любому аффинному подпространству размерности 2 пространства $\mathrm{GF}(2^n)$, выполнено неравенство $F(t) + F(u) + F(v) + F(w) \neq 0$.

Показано, что при $n = 4$ существует один класс CCZ-эквивалентности, содержащий два класса EA-эквивалентности, причем только один из них содержит степенную функцию. Для $n = 5$ существует 3 класса CCZ-эквивалентности и 7 классов EA-эквивалентности, из них два класса не содержат степенные функции, оставшиеся пять классов содержат APN-подстановки. Подстановки из каждого класса EA-эквивалентности аффинно эквивалентны степенной функции $F(x) = x^d$, каждому классу соответствует одно значение $d \in \{3, 5, 7, 11, 15\}$.

В заключение отметим, что в Интернете доступна предварительная версия обзора по APN-функциям, написанная C. Carlet в 2008 г. [36]. В обзоре, в частности, отмечается, что все известные APN-функции обладают не самыми лучшими характеристиками по отношению к другим, отличным от разностного, криптографическим методам. Следовательно, рекомендовать их для использования в качестве S-боксов пока рано. Требуются дальнейшие исследования.

ЛИТЕРАТУРА

1. *Biham E., Shamir A.* Provable Security Against Differential Cryptography // Crypto 1990, Lecture Notes in Computer Science. 1991. V. 537. P. 2–21.
2. *Nyberg K.* Perfect nonlinear S-boxes // Eurocrypt 1991, Lecture Notes in Computer Science. 1991. V. 547. P. 378–386.
3. *Nyberg K.* Differently uniform mappings for cryptography // Eurocrypt 1993, Lecture Notes in Computer Science. 1994. V. 765. P. 55–64.
4. *Nyberg K., Knudsen L. R.* Provable Security Against Differential Cryptography // Crypto 1992, Lecture Notes in Computer Science. V. 740. P. 566–574.
5. *Bierbrauer J.* New semifields, PN and APN functions // http://www.math.mtu.edu-/jbierbra/HOMEZEUGS/PNpub06Dez08.pdf, 2008.
6. *Voloch J. F.* Symmetric Cryptography and Algebraic Curves // Proceedings of Algebraic Geometry and its Applications. 2007. P. 135–141.
7. *Berger T., Canteaut A., Charpin P., Laigle-Chapuy Y.* On Almost Perfect Nonlinear Functions Over F_{2^n} // IEEE Transactions on Information Theory. 2006. V. 52. No. 9. P. 4160–4170.
8. *Beth T., Ding C.* On almost perfect nonlinear permutations // Eurocrypt 1993, Lecture Notes in Computer Science. 1994. V. 765. P. 65–76.
9. *Charpin P., Kyureghyan G.* On a class of permutation polynomials over F_{2^n} // SETA 2008, Lecture Notes in Computer Science. 2008. V. 5203. P. 368–376.
10. *Chabaud F., Vaudenay S.* Links between differential and linear cryptanalysis // Eurocrypt 1994, Lecture Notes in Computer Science. 1994. V. 950. P. 356–365.
11. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.
12. *Carlet C., Charpin P., Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. V. 15(2). P. 125–156.
13. *Edel Y., Kyureghyan G., Pott A.* A new APN function which is not equivalent to a power mapping // IEEE Transactions on Information Theory. 2006. V. 52. No. 2. P. 744–747.
14. *Budaghyan L., Carlet C.* On CCZ-equivalence and its use in secondary constructions of bent functions // Cryptology ePrint Archive 2009/042.

15. *Gold R.* Maximal recursive sequence with 3-valued recursive cross-correlation functions // IEEE Transactions on Information Theory. 1968. V. 14. No. 1. P. 154–156.

16. *Kasami T.* The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes // Information and Control. 1971. V. 18. P. 369–394.

17. *Dobbertin H.* Almost perfect nonlinear power functions over GF(2^n): The Welch case // IEEE Transactions on Information Theory. 1999. V. 45. No. 4. P. 1271–1275.

18. *Dobbertin H.* Almost perfect nonlinear power functions over GF(2^n): The Niho case // International J. of Computer and Information Sciences. 1999. V. 151. P. 57–72.

19. *Dobbertin H.* Almost perfect nonlinear power functions over GF(2^n): A new case for n divisible 5 // Proc. of Finite Fields and Applications Fq5. Springer Verlag, 2001. P. 113–121.

20. *Helleseth T., Sandberg D.* Some power mappings with low differential uniformity // Applicable Algebra in Engineering, Communication and Computing. 1997. V. 8. P. 363–370.

21. *Dobbertin H., Mills D., Muller E., Pott A., Willems W.* APN functions in odd characteristic // Discrete Mathematics. 2003. V. 267. P. 95–112.

22. *Felke P.* Computing the uniformity of power mappings: a systematic approach with the multivariate method over finite fields of odd characteristic // Ph. D. dissertation, University of Bochum, Germany. 2005.

23. *Helleseth T., Rong C., Sandberg D.* New families of almost perfect nonlinear power mappings // IEEE Transactions on Information Theory. 1999. V. 45. No. 2. P. 475–485.

24. *Budaghyan L., Carlet C., Pott A.* New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials // Proceedings of the Workshop on Coding and Cryptography. 2005. P. 306–315.

25. *Edel Y., Pott A.* A new almost perfect nonlinear function which is not quadratic // Cryptology ePrint Archive 2008/313.

26. *Budaghyan L., Carlet C., Leander G.* A class of quadratic APN binomials inequivalent to power functions // Cryptology ePrint Archive 2006/445.

27. *Budaghyan L., Carlet C., Felke P., Leander G.* An infinite class of quadratic APN functions which are not equivalent to power mappings // Proceedings of the IEEE International Symposium on Information Theory. 2006.

28. *Budaghyan L., Carlet C., , Leander G.* Another class of quadratic APN binomials over F_2^n: the case n divisible by 4. // Cryptology ePrint Archive 2006/428.

29. *Budaghyan L., Carlet C., Leander G.* Constructing new APN functions from known ones // Cryptology ePrint Archive 2007/063.

30. *Budaghyan L., Carlet C.* Classes of Quadratic APN Trinomials and Hexanomials and Related Structures // Cryptology ePrint Archive 2007/098.

31. *Ness G., Helleseth T.* A new family of ternary almost perfect nonlinear mappings // IEEE Transactions on Information Theory. 2007. V. 53. No. 7. P. 2581–2586.

32. *Zeng X., Hu L., Yang Y., Jiang W.* On the inequivalence of Ness-Helleseth APN functions // Cryptology ePrint Archive 2007/379.

33. *Bracken C., Byrne E., Markin N., McGuire G.* Quadratic Almost Perfect Nonlinear Functions with Many Terms // Cryptology ePrint Archive 2007/115.

34. *Zha Z., Kyureghyan G., Wang X.* A New Family of Perfect Nonlinear Binomials // Cryptology ePrint Archive 2008/196.

35. *Brinkmann M., Leander G.* On the Classification of APN Functions up to Dimension Five // Proceedings of the Workshop on Coding and Cryptography. 2007. P. 39–48.

36. *Carlet C.* Vectorial Boolean Functions for Cryptography // www-roc.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf. 2008.