5. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2021.
6. *Siegenthaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. V. 30. No. 5. P. 776–780.

УДК 519.7 DOI 10.17223/2226308X/15/10

О РАЗЛОЖЕНИИ БЕНТ-ФУНКЦИЙ ОТ ВОСЬМИ ПЕРЕМЕННЫХ В СУММУ ДВУХ БЕНТ-ФУНКЦИЙ[1]

А. С. Шапоренко

Максимально нелинейная булева функция от чётного числа переменных называется бент-функцией. Исследуется гипотеза о представлении произвольных булевых функций от n переменных степени не больше $n/2$ как суммы двух бент-функций. Доказано, что произвольная бент-функция от восьми переменных степени не больше 3 представляется как сумма двух бент-функций. Показано, что каждая квадратичная булева функция от чётного числа переменных $n \geqslant 4$ раскладывается в сумму двух бент-функций специального вида.

Ключевые слова: *бент-функции, булевы функции, разложение в сумму бент-функций.*

Булева функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ от чётного числа переменных n называется *бент-функцией*, если она находится на максимальном расстоянии Хэмминга от множества всех аффинных функций [1]. Обозначим через $\mathcal{B}_n$ множество бент-функций. Дальше полагаем, что n является чётным целым числом.

Преобразованием Уолша — Адамара булевой функции f от n переменных называется целочисленная функция, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x,y \rangle} \text{ для любого } y \in \mathbb{Z}_2^n.$$

Для любой бент-функции f от n переменных $W_f(y) = \pm 2^{n/2}$ [2]. Определим *дуальную бент-функцию* $\tilde{f}$ к $f \in \mathcal{B}_n$ равенством $W_f(y) = 2^{n/2}(-1)^{\tilde{f}(y)}$ для любого $y \in \mathbb{Z}_2^n$.

Шифры, в которых используются бент-функции, более устойчивы к линейному криптоанализу [3], потому что бент-функции крайне плохо аппроксимируются аффинными функциями. Бент-функции используются в структуре блочного шифра CAST как координатные функции S-блоков [4], а также для построения регистра сдвига с нелинейной обратной связью в поточном шифре Grain [5]. Бент-функции связаны также с некоторыми объектами теории кодирования, например с кодами Рида — Маллера [2].

В работе исследуется известная открытая проблема о разложении произвольной булевой функции в сумму двух бент-функций [6].

Гипотеза 1 (Н. Н. Токарева, [7]). Любая булева функция от n переменных степени не больше $n/2$ может быть представлена как сумма двух бент-функций от n переменных.

В [7] показано, что гипотеза 1 верна для $n \leqslant 6$. Известно, что если гипотеза 1 верна, то справедлива следующая нижняя оценка числа бент-функций [7]:

$$|\mathcal{B}_n| \geqslant 2^{2^{n-2} + \binom{n}{n/2}/4}.$$

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).

Утверждение 1 [7, 8]. Пусть f_0, f_1 и f_2 — бент-функции от n переменных. Тогда функция g, определенная следующим образом:

$$g(x,0,0) = f_0(x), \qquad g(x,0,1) = f_1(x),$$
$$g(x,1,0) = f_2(x), \qquad g(x,1,1) = f_3(x),$$

является бент-функцией от $n+2$ переменных тогда и только тогда, когда f_3 — бент-функция от n переменных и $\tilde{f}_0 \oplus \tilde{f}_1 \oplus \tilde{f}_2 \oplus \tilde{f}_3 = 1$.

Бент-функции, которые получаются с помощью утверждения 1, называются *бент итеративными функциями.*

Следствие 1. Пусть g и ℓ являются бент-функцией и линейной функцией от n переменных соответственно. Тогда $f(x, x_{n+1}, x_{n+2}) = x_{n+2}(x_{n+1} \oplus \ell(x)) \oplus g(x)$ является бент-функцией от $n+2$ переменных.

Известно, что бент-функции от восьми переменных степени не больше 3 разбиваются на 10 классов аффинной эквивалентности [9]. В таблице представлены разложения каждого представителя класса аффинной эквивалентности в сумму двух бент итеративных функций от восьми переменных, которые имеют форму из следствия 1. Заметим, что в утверждении 1 и следствии 1 переменные x_{n+1}, x_{n+2} используются для разложения бент итеративных функций на подфункции. В таблице такие переменные для бент итеративных функций выделены жирным шрифтом. Для простоты мы используем обозначение 12 вместо x_1x_2.

Неэквивалентные бент-функции степени $\leqslant 3$	Разложение
12 + 34 + 56 + 78	13 + 25 + **48** + 67 + 12 + 56
	13 + 25 + 48 + 67 + 34 + **78**
123 + 14 + 25 + 36 + 78	**1**(**6** + 23) + 24 + 58 + 37 + 14 + 78
	16 + 24 + 58 + **3**(**7** + 6) + 25
123 + 245 + 34 + 26 + 17 + 58	**2**(**7** + 45 + 13 + 6) + 14 + 38 + 56 + 34
	7(**2** + 1) + 14 + 38 + 56 + 58
123 + 245 + 13 + 15 + 26 + 34 + 78	**2**(**7** + 45 + 13 + 6) + 14 + 38 + + 56 + 34 + 15
	7(**2** + 8) + 14 + 38 + 56 + 13
123 + 245 + 346 + 35 + 26 + 25 + 17 + 48	**2**(**7** + 45 + 6 + 5) + 14 + 38 + 56 + 48
	3(**8** + 46 + 12 + 5) + 27 + 14 + 56 + 17
123 + 245 + 346 + 35 + 13 + 14 + 27 + 68	**2**(**6** + 13 + 45 + 7) + 14 + 78 + 35 + 45
	3(**1** + 46) + 26 + 78 + 45 + 68
123 + 245 + 346 + 35 + 26 + 25 + 12 + 13 + 14 + 78	**2**(**7** + 13 + 45 + 5 + 1 + 6) + 14 + 56 + + 38 + 45 + 68
	3(**1** + 46 + 8 + 5) + 27 + 45 + 68 + + 56 + 78
123 + 245 + 346 + 35 + 16 + 27 + 48	**1**(**4** + 23 + 6) + 27 + 58 + 36 + 26 + 78
	4(**1** + 25 + 36 + 8) + 35 + 26 + 78 + + 36 + 58
127 + 347 + 567 + 14 + 36 + 25 + 45 + 78	**7**(**1** + 34 + 56 + 8 + 6) + 36 + + 45 + 28 + 35 + 56
	1(**4** + 27 + 7) + 28 + 35 + 67 + 25 + 56
123 + 245 + 346 + 147 + 35 + 27 + 15 + 16 + 48	**4**(**1** + 36 + 25) + 35 + 26 + 78 + 36
	1(**5** + 23 + 47 + 4 + 6) + 27 + + 48 + 36 + 78 + 26

Известно, что функции, аффинно эквивалентные бент-функции, также являются бент-функциями [2]. Следовательно, если функция f раскладывается в сумму двух

бент-функций, то функция, аффинно эквивалентная f, также представляется как сумма двух бент-функций.

Теорема 1. Произвольная бент-функция от восьми переменных степени не больше 3 раскладывается в сумму двух бент-функций от восьми переменных.

Известно, что каждая квадратичная функция от $n \geqslant 4$ переменных представляется как сумма двух бент-функций от n переменных [10]. Справедливо следующее утверждение:

Утверждение 2. Любая квадратичная булева функция от $n \geqslant 4$ переменных представляется как сумма двух бент итеративных функций.

Исследование разложения булевых функций в сумму двух бент итеративных функций может привести к интересным результатам, касающимся рассматриваемой гипотезы. В настоящее время ведётся работа по разложению кубических булевых функций от восьми переменных в сумму двух бент итеративных функций. Получены частичные результаты, но необходимо продолжение исследования.

ЛИТЕРАТУРА

1. *Rothaus O. S.* On "bent" functions // J. Combinat. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
3. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386–397.
4. *Adams C.* Constructing symmetric ciphers using the CAST design procedure // Design, Codes, Cryptogr. 1997. V. 12. No. 3. P. 283–316.
5. *Hell M., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128 // IEEE Intern. Symp. Inform. Theory. 2006. P. 1614–1618.
6. *Carlet C.* Open questions on nonlinearity and on APN Functions // LNCS. 2015. V. 9061. P. 83–107.
7. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Commun. 2011. V. 5. No. 4. P. 609–621.
8. *Canteaut A. and Charpin P.* Decomposing bent functions // IEEE Trans. Inform. Theory. 2003. V. 49. No. 8. P. 2004–2019.
9. *Hou X. D.* Cubic bent functions // Discr. Math. 1998. V. 189. Iss. 1–3. P. 149–161.
10. *Qu L. and Li C.* New results on the Boolean functions that can be expressed as the sum of two bent functions // IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 2016. V. 99-A. No. 8. P. 1584–1590.