

Здесь через G_f обозначена группа инерции функции f в группе G ; $[G]\mathbf{S}_r$ — операция экспоненцирования группы G с помощью симметрической группы $\mathbf{S}_r$ степени r . Аналогичное описание справедливо для полной линейной группы $\mathbf{GL}(n, p)$.

ЛИТЕРАТУРА

1. Черемушкин А. В. Однозначность разложения двоичной функции в неповторное произведение нелинейных неприводимых сомножителей // Вестник Московского государственного университета леса «Лесной вестник». 2004. № 4(35). С. 86–90.

УДК 519.7

DOI 10.17223/2226308X/14/11

О ПРОИЗВОДНЫХ БУЛЕВЫХ БЕНТ-ФУНКЦИЙ¹

А. С. Шапоренко

Бент-функция может быть определена как булева функция $f(x)$ от n переменных (n чётно), такая, что для любого ненулевого вектора y её производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ сбалансирована — принимает значения 0 и 1 одинаково часто. Справедливо ли, что любая сбалансированная функция — производная некоторой бент-функции? Эта задача рассмотрена для частного случая — аффинных функций. Доказано, что любая неконстантная аффинная функция от $n \geq 4$ (n чётно) переменных является производной для $(2^{n-1} - 1)|\mathcal{B}_{n-2}|^2$ бент-функций, где $\mathcal{B}_{n-2}$ — класс бент-функций от $n - 2$ переменных. Получены итерационные нижние границы для числа бент-функций.

Ключевые слова: бент-функции, булевы функции, производные бент-функций, нижние границы для числа бент-функций.

Пусть $\langle x, y \rangle$ — скалярное произведение двоичных векторов по модулю 2. Функция $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Булева функция от чётного числа переменных называется бент-функцией, если она максимально нелинейна [1]. Обозначим через $\mathcal{B}_n$ множество бент-функций от n переменных.

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

Другое определение бент-функции — булева функция $f(x)$ от n переменных (n чётно), такая, что для любого ненулевого вектора y её производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ сбалансирована — принимает значения 0 и 1 одинаково часто [5]. Справедливо ли, что любая сбалансированная функция — производная некоторой бент-функции? В [6] показано, что любая сбалансированная функция g от $n \leq 6$ переменных степени не выше $n/2 - 1$, такая, что $g(x) = g(x \oplus y)$ для всех x при некотором y , является производной некоторой бент-функции от n переменных. В данной работе эта задача рассмотрена для частного случая сбалансированных функций — аффинных: $\ell_{a,b}(x) = \langle a, x \rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ — ненулевой вектор и $b \in \mathbb{Z}_2$.

Теорема 1. Любая неконстантная аффинная функция $\ell_{a,b}(x)$ от $n \geq 4$ (n чётно) переменных является производной для $(2^{n-1} - 1)|\mathcal{B}_{n-2}|^2$ бент-функций.

¹Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research.

Лемма 1. Для любой бент-функции g и любых $y \neq y'$ справедливо: $D_y g(x) \neq D_{y'} g(x)$.

Лемма 2. Пусть $D_y g(x) = l_{a,b}(x)$ для бент-функции $g(x)$. Тогда при любом y' $D_{y'} g(x) \neq l_{a,b}(x) \oplus 1$.

Теорема 1 вместе с леммами 1 и 2 даёт итерационные нижние границы для количества бент-функций от $n + 2$ переменных (теорема 2).

Теорема 2. Для любого чётного $n \geq 4$ верно

$$|\mathcal{B}_{n+2}| \geq (2^{n+2} - 2)|\mathcal{B}_n|^2.$$

Данная граница хуже представленной в [7], но она, вероятно, может быть улучшена, если рассматривать больше одной аффинной функции или учитывать функции, которые не имеют аффинных производных. Однако задача выделения бент-функций, которые имеют производную $\ell_{a,b}$ и не имеют $\ell_{c,d}$, является непростой. Бент-функции, которые не имеют аффинных производных, рассмотрены, например, в [8].

ЛИТЕРАТУРА

1. Rothaus O. S. On bent functions // J. Combinat. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. Matsui M. Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386–397.
3. Adams C. Constructing symmetric ciphers using the CAST design procedure // Design, Codes, Cryptogr. 1997. V. 12. No. 3. P. 283–316.
4. Hell M., Johansson T., Maximov A., and Meier W. A stream cipher proposal: Grain-128 // IEEE Intern. Symp. Inform. Theory. 2006. P. 1614–1618.
5. Tokareva N. Bent Functions: Results and Applications to Cryptography. Acad. Press., 2015.
6. Токарева Н. Н. О множестве производных булевой бент-функции // Прикладная дискретная математика. Приложение. 2016. №9. С. 35.
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.