

УДК 519.651

ПОСТРОЕНИЕ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ С ЗАДААННЫМИ КРИПТОГРАФИЧЕСКИМИ СВОЙСТВАМИ НА ОСНОВЕ КООРДИНАТНЫХ ФУНКЦИЙ СТЕПЕННЫХ ПРЕОБРАЗОВАНИЙ КОНЕЧНЫХ ПОЛЕЙ¹

А. В. Иванов, В. Н. Романов

Пусть $\mathbb{F}_2$ — поле из двух элементов с единицей e ; $\mathbb{F}_{2^n}$ — его расширение натуральной степени n ; $\text{tr}_t^n(\alpha) = \sum_{k=0}^{t-1} \alpha^{2^{t \cdot k}}$ — функция след из поля $\mathbb{F}_{2^n}$ в его подполе $\mathbb{F}_{2^t}$ для натурального t , такого, что $t|n$; $\|t\|_2$ — двоичный вес числа $t \in \mathbb{N}$; $\mathcal{F}_n$ — множество отображений поля $\mathbb{F}_{2^n}$ в поле $\mathbb{F}_2$; $\mathcal{B}_n$ — множество булевых функций от n переменных.

Фиксация базиса векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$ устанавливает взаимнооднозначное соответствие между множествами $\mathcal{B}_n$ и $\mathcal{F}_n$. Это позволяет при изучении свойств булевых функций рассматривать их представления отображениями из множества $\mathcal{F}_n$.

При получении результатов в работе использовано приведенное представление булевых функций от n переменных многочленами над полем $\mathbb{F}_{2^n}$, принимающими значения в поле $\mathbb{F}_2$. В связи с этим предполагается знакомство читателя с работами [1, 2].

Для элемента $\alpha \in \mathbb{F}_{2^n}$ и преобразования Φ поля $\mathbb{F}_{2^n}$ через $S_\alpha^{(\Phi)}$ обозначим отображение, задаваемое равенством $S_\alpha^{(\Phi)}(x) = \text{tr}_1^n(\alpha \Phi(x))$. Заметим, что $S_\alpha^{(\Phi)}(x)$ есть линейная комбинация координатных функций преобразования Φ .

В работе для отображений из множества $\mathcal{F}_n$ рассматриваются классы приближений вида $S_\alpha^{(\Phi)}(x) + \text{tr}_1^n(\beta x)$, где $\alpha, \beta \in \mathbb{F}_{2^n}$; $\Phi(x)$ — некоторое преобразование поля $\mathbb{F}_{2^n}$. Получены условия на вид преобразования Φ , при выполнении которых построенные классы приближают отображения из множества $\mathcal{F}_n$ точнее класса отображений, соответствующих аффинным функциям. Описаны множества показателей степени d монома, задающего преобразование $\Phi(x) = x^d$, при которых Φ удовлетворяет этим условиям.

В качестве показателя близости отображений $F, G \in \mathcal{F}_n$ будем использовать величину $\Delta(F, G) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)+G(x)}$. Если отображение G соответствует линейной булевой функции, то $\Delta(F, G)$ есть коэффициент Уолша — Адамара функции F [3]. Известно [4], что для любого отображения $F \in \mathcal{F}_n$ существует отображение $L \in \mathcal{F}_n$, соответствующее линейной булевой функции, такое, что $|\Delta(F, G)| \geq 2^{\frac{n}{2}}$.

Теорема 1. Пусть n — натуральное число, большее двух, $\Phi(x) \in \mathbb{F}_{2^n}[x]$. Если выполнено одно из условий:

- $\Phi(x)$ — редуцированный многочлен, такой, что $\text{ind } \Phi(x) > n/2$;
- $\Phi(x)$ — подстановочный многочлен [5] над полем $\mathbb{F}_{2^n}$, $\Psi(x)$ — многочлен над $\mathbb{F}_{2^n}$, такой, что для любого $x \in \mathbb{F}_{2^n}$ выполнено $\Phi(\Psi(x)) = x$ и индекс нелинейности редуцированного многочлена приведенного представления функции $S_e^{(\Psi)}$ больше $n/2$;
- существуют элементы $t_1, t_2 \in \mathbb{F}_{2^n} \setminus \{0\}$, такие, что мощность множества $\tilde{X} = \{x \in \mathbb{F}_{2^n} : \Phi(x) + \Phi(x + t_1) \in \{0, t_2\}\}$ не кратна четырем,

то для любой функции $F \in \mathcal{F}_n$ выполняется неравенство

$$\max \{ |\Delta(F, S_\alpha^{(\Phi)} + \text{tr}_1^n(\beta x))| : \alpha, \beta \in \mathbb{F}_{2^n} \} > 2^{\frac{n}{2}}.$$

¹Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.

Следствие. Пусть n, d — натуральные числа, такие, что $n > 2$, $d < 2^n - 1$, $\|d\|_2 > n/2$. Тогда для любой функции $F \in \mathcal{F}_n$ выполняется неравенство

$$\max \{ |\Delta(F, \text{tr}_1^n(\alpha x^d) + \text{tr}_1^n(\beta x))| : \alpha, \beta \in \mathbb{F}_{2^n} \} > 2^{\frac{n}{2}}.$$

З а м е ч а н и е. Зафиксируем натуральное n . В качестве примера показателя d , удовлетворяющего условию следствия, можно привести число $2^t - 1$, где $t > n/2$. Если требуется, чтобы моном x^d задавал подстановку на $\mathbb{F}_{2^n}$, то t необходимо выбрать взаимно простым с n . Таким условиям при $n > 2$ удовлетворяет t , равное $n - 1$.

Теоретический и практический интерес представляют задачи количественной оценки для натурального n , $d \in \overline{1, 2^n - 1}$ и функции $F \in \mathcal{F}_n$ величины

$$\max \{ |\Delta(F, \text{tr}_1^n(\alpha x^d) + \text{tr}_1^n(\beta x))| : \alpha, \beta \in \mathbb{F}_{2^n} \}$$

как для всех функций из $\mathcal{F}_n$, так и для отдельных классов таких функций, например бент-функций [4]. Рассмотрим способ построения бент-функций с помощью координатных функций степенных преобразований поля $\mathbb{F}_{2^n}$ и продемонстрируем эффективность аппроксимации построенных функций приближениями из рассмотренных классов.

Теорема 2. Пусть натуральные числа n и s четны, $n/2$ нечетно и $(n, s) = 2$. Положим $d = 1 + 2^s$ и выберем натуральное число σ таким, что $\sigma d \equiv 1 \pmod{2^n - 1}$. Пусть значения функции $F_{a,b} \in \mathcal{F}_n$ для любого элемента $x \in \mathbb{F}_{2^n}$ определены равенством $F_{a,b}(x) = \text{tr}_1^n(b^\sigma x) \text{tr}_1^n(ax) + \text{tr}_1^n(bx^d)$, а элементы $a, b \in \mathbb{F}_{2^n} \setminus \{0\}$ таковы, что $\text{tr}_1^n(ab^{-\sigma}) = e$. Тогда:

а) $F_{a,b}$ является бент-функцией;

б) $\max \{ |\Delta(F_{a,b}(x), \text{tr}_1^n(c_1 x^{d'}) + \text{tr}_1^n(c_2 x))| : c_1, c_2 \in \mathbb{F}_{2^n}, d' \in \overline{1, 2^n - 2} \} \geq 2^{n-1}$.

ЛИТЕРАТУРА

1. Иванов А. В. Использование приведенного представления булевых функций при построении их нелинейных аппроксимаций // Вестник Томского государственного университета. Приложение. 2007. № 23. С. 31–35.
2. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18. № 1. С. 9–29.
3. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МНЦМО, 2004. 470 с.
4. Rothaus O. S. On “bent” functions // J. Comb. Theory. 1976. Ser. A. V. 20. P. 300–305.
5. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. 818 с.

УДК 519.7

СВЯЗЬ ПОДПРОСТРАНСТВ, НА КОТОРЫХ АФФИННЫ БЕНТ-ФУНКЦИЯ И ДУАЛЬНАЯ К НЕЙ¹

Н. А. Коломеец

Настоящая работа является продолжением исследований, начатых в [1]. Ранее было установлено, что минимальное расстояние Хэмминга между бент-функциями от n переменных равно $2^{n/2}$ и бент-функции находятся на этом расстоянии тогда и только тогда, когда их значения отличаются на аффинном подпространстве и обе функции

¹Работа выполнена при финансовой поддержке гранта Президента РФ для молодых российских ученых (грант МК № 1250.2009.1).