КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

УДК 519.7

ИССЛЕДОВАНИЕ ОДНОГО ПАРАМЕТРА БУЛЕВЫХ ФУНКЦИЙ, БЛИЗКОГО К НЕЛИНЕЙНОСТИ*

В. Б. Алексеев
Р. Р. Омаров

Московский государственный университет им. М.В. Ломоносова

e-mail: vbalekseev@rambler.ru

e-mail: rustamomarov@ya.ru

Минимальное расстояние (по Хэммингу) от булевой функции f до аффинных булевых функций называют нелинейностью функции f. Это один из параметров, характеризующих качество криптографических систем, использующих функцию f. В работе рассматривается один из классов булевых функций от $2n$ переменных, имеющих максимальную нелинейность $2^{2n-1} - 2^{n-1}$, а именно, класс Мэйорана–Мак-Фарланда. Исследуется, как меняется расстояние от функций этого класса до класса приближающих функций, если в класс приближающих функций кроме аффинных включить все функции, у которых в полиноме Жегалкина имеется одно нелинейное слагаемое. Показано, что новое расстояние может быть различным для разных функций из класса Мэйорана–Мак-Фарланда и изменяется в пределах от $2^{2n-1} - 3 \cdot 2^{n-1} + 2$ до $2^{2n-1} - 2 \cdot 2^{n-1}$, причем обе границы достижимы.

Ключевые слова: булева функция, криптографические свойства булевых функций, нелинейность, класс Мэйорана–Мак-Фарланда.

Введение. Постановка задачи

Булевы функции широко применяются в криптографии. При этом стойкость систем шифрования часто основывается на «сложности» используемых булевых функций. Поскольку аффинные функции считаются очень простыми, то в качестве одной из характеристик «сложности» булевых функций рассматривается «удаленность» данной функции от всех аффинных функций. Этому параметру, называемому нелинейностью булевой функции, посвящено множество работ. Обзор имеющихся результатов о нелинейности (с указанием имеющихся публикаций) можно найти в книге [1], где нелинейности посвящена отдельная глава. Дадим необходимые определения.

Пусть n – произвольное натуральное число. Через V_n будем обозначать векторное пространство наборов длины n с компонентами из $\{0,1\}$ с операцией $\oplus$ покоординатного сложения векторов по модулю 2.

* Работа выполнена при поддержке РФФИ, гранты 07-01-00154 и 09-01-00701.

Определение. Пусть f – булева функция от n переменных, то есть $f: V_n \to \{0,1\}$. *Весом* $wt(f)$ булевой функции f называется количество наборов, на которых функция f равна 1.

Определение. Пусть f, g – булевы функции от n переменных. *Расстоянием* от булевой функции f до булевой функции g называется величина $dist(f,g) = wt(f \oplus g)$. Таким образом, $dist(f,g)$ – это число наборов, на которых f и g принимают разные значения.

Определение. Пусть f – булева функция от n переменных и M – произвольное множество булевых функций от n переменных. *Расстоянием от* f *до множества* M называется величина $dist(f,M) = \min_{g \in M} dist(f,g)$.

Определение. Пусть $x \in V_n$, $y \in V_n$. Через $\langle x, y \rangle$ будем обозначать *скалярное произведение* x и y: $\langle x, y \rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n$ (здесь $\oplus$ – это сложение по модулю 2).

Определение. Булева функция $g(x)$ от n переменных называется *аффинной*, если существуют $a = (a_1, \ldots a_n) \in V_n$ и $c \in \{0,1\}$ такие, что $g(x) = \langle a, x \rangle \oplus c = a_1 x_1 \oplus \ldots \oplus a_n x_n \oplus c$. Множество всех аффинных булевых функций от n переменных будем обозначать A_n. Отметим, что для любой аффинной булевой функции $g(x)$ от n переменных, отличной от константы, $wt(g(x)) = 2^{n-1}$.

Определение. Расстояние $dist(f, A_n)$ от булевой функции $f(x)$ от n переменных до множества A_n аффинных булевых функций называется *нелинейностью* функции $f(x)$ и обозначается через N_f.

Лемма 1 [1]. Для любой булевой функции $f(x)$ от n переменных справедливо неравенство $N_f \le 2^{n-1} - 2^{n/2-1}$. Для четных n эта оценка достижима, то есть существуют функции $f(x)$ от $2n$ переменных, для которых $N_f = 2^{n-1} - 2^{n/2-1}$.

Определение. Булевы функции $f(x)$ от $2n$ переменных, для которых $N_f = 2^{2n-1} - 2^{n-1}$, называют *максимально-нелинейными* функциями (этот класс называют также классом *бент-функций*).

Таким образом, максимально-нелинейные функции – это булевы функции от $2n$ переменных, наиболее плохо приближаемые аффинными функциями. Мы рассмотрим вопрос о том, что происходит с максимально-нелинейными функциями, если класс аффинных функций несколько расширяется, а именно, в качестве приближающих рассматриваются все функции, у которых в полиноме Жегалкина имеется не более одного нелинейного слагаемого.

Определение. Через AE_n будем обозначать класс всех почти аффинных функций $g(x)$, а именно, функций вида $g(x) = \langle a,x \rangle \oplus c \oplus x_{i1} \cdot \ldots \cdot x_{ik}$, где $a \in V_n$, $c \in \{0,1\}$ и $\{i1, \ldots, ik\}$ – произвольное подмножество (возможно, пустое) множества $\{1, \ldots, n\}$.

В данной работе нас интересует вопрос: одинакова ли величина $dist(f, AE_{2n})$ для всех максимально-нелинейных функций f от $2n$ переменных и насколько для них $dist(f, AE_{2n})$ отличается от $dist(f, A_{2n})$? На первый вопрос мы дадим отрицательный ответ. На второй вопрос мы дадим полный ответ для одного известного дос-

таточно широкого класса максимально-нелинейных функций (множество всех максимально-нелинейных функций f от $2n$ переменных пока не описано).

Определение. Пусть $x=(x_1,\dots,x_n)$, $y=(y_1,\dots,y_n)$. Класс Мэйорана–Мак-Фарланда определяется как класс всех булевых функций $f(x,y)$ от $2n$ переменных вида $f(x,y)=\langle\pi(y),x\rangle\oplus\Phi(y)$, где π – произвольная подстановка на множестве V_n, а $\Phi(y)$ – произвольная булева функция от n переменных.

Известно, что все функции из класса Мэйорана–Мак-Фарланда являются максимально-нелинейными функциями [1]. В данной работе мы устанавливаем точные пределы, в которых изменяется значение $dist(f,AE_{2n})$ для всех функций из класса Мэйорана–Мак-Фарланда.

Оценки нового параметра для функций класса Мэйорана–Мак-Фарланда

Покажем сразу же, что для любой функции $f(x,y)=\langle\pi(y),x\rangle\oplus\Phi(y)$ из класса Мэйорана–Мак-Фарланда $dist(f,AE_{2n})<dist(f,A_{2n})$.

Лемма 2. Для любой функции $f(x,y)=\langle\pi(y),x\rangle\oplus\Phi(y)$ из класса Мэйорана–Мак-Фарланда справедливо неравенство:
$dist(f(x,y),AE_{2n})\le 2^{2n-1}-2\cdot 2^{n-1}$.

Доказательство. Пусть $\pi(0,\dots,0)=a=(a_1,\dots,a_n)$, $a'=a\oplus(1,0,\dots,0)$ и $\gamma=(\gamma_1,\dots,\gamma_n)=\pi^{-1}(a')$. Так как $\gamma\ne(0,\dots,0)$, то существует j такое , что $\gamma_j=1$. Рассмотрим функцию $g(x,y)=\langle a,x\rangle\oplus\langle b,y\rangle\oplus c\oplus x_1y_j$ из класса AE_{2n}, где b пока произвольно и $c=\Phi(0,\dots,0)$. Тогда $dist(f(x,y),g(x,y))=wt(h(x,y))$, где

$$h(x,y)=f(x,y)\oplus g(x,y)=\langle\pi(y),x\rangle\oplus\Phi(y)\oplus\langle a,x\rangle\oplus\langle b,y\rangle\oplus c\oplus x_1y_j=$$
$$=\langle\pi(y)\oplus a,x\rangle\oplus\Phi(y)\oplus\langle b,y\rangle\oplus\Phi(0,\dots,0)\oplus x_1y_j.$$

При $\beta=(0,\dots,0)$ получаем $h(x,\beta)\equiv 0$. При $\beta=\gamma$ получаем

$$h(x,\beta)=h(x,\gamma)=\langle\pi(\gamma)\oplus a,x\rangle\oplus\Phi(\gamma)\oplus\langle b,\gamma\rangle\oplus\Phi(0,\dots,0)\oplus x_1=\langle(1,0,\dots 0),x\rangle\oplus x_1\oplus$$
$$\oplus\Phi(\gamma)\oplus\Phi(0,\dots,0)\oplus\langle b,\gamma\rangle=\Phi(\gamma)\oplus\langle b,\gamma\rangle\oplus\Phi(0,\dots,0).$$

Положим $b_j=\Phi(\gamma)\oplus\Phi(0,\dots,0)$ и $b_i=0$ при $i\ne j$. Тогда $h(x,\gamma)\equiv 0$. При $\beta\ne(0,\dots,0)$ и $\beta\ne\gamma$ имеем $\pi(\beta)\oplus a\ne(0,\dots,0)$ и $\pi(\beta)\oplus a\ne(1,0,\dots,0)$. Поэтому в этих случаях $h(x,\beta)$ является аффинной функцией, отличной от константы, откуда $wt(h(x,\beta))=2^{n-1}$. Таким образом,

$$dist(f(x,y),g(x,y))=wt(h(x,y))=\sum_{\beta\in V_n}wt(h(x,\beta))=2^{n-1}(2^{n-1}-2)=2^{2n-1}-2\cdot 2^{n-1},$$

откуда следует утверждение леммы 2.

Лемма 3. Если нелинейное слагаемое в $g(x,y)\in AE_{2n}$ не содержит переменных $x_1,\dots,x_n$, то $dist(f(x,y),g(x,y))\ge 2^{2n-1}-2^{n-1}$ для любой функции $f(x,y)=\langle\pi(y),x\rangle\oplus\Phi(y)$ из класса Мэйорана–Мак-Фарланда.

Доказательство. Так как все функции из класса Мэйорана–Мак-Фарланда являются максимально-нелинейными, то $dist(f(x,y),g(x,y))\ge 2^{2n-1}-2^{n-1}$, если $g(x,y)$ не содержит нелинейных слагаемых. Пусть теперь $g(x,y)$ содержит нелинейное слагаемое $y_{j1}\cdot\ldots\cdot y_{jt}$. Положим

$$f_1(x,y)=f(x,y)\oplus y_{j1}\cdot\ldots\cdot y_{jt}=\langle\pi(y),x\rangle\oplus(\Phi(y)\oplus y_{j1}\cdot\ldots\cdot y_{jt})\ \text{ и}$$

$$g_1(x,y) = g(x,y) \oplus y_{j1} \cdot \ldots \cdot y_{jt}.$$

Тогда $f_1(x,y)$ лежит в классе Мэйорана–Мак-Фарланда и $g_1(x,y)$ – аффинная функция. Поэтому $dist(f(x,y),g(x,y)) = dist(f_1(x,y),g_1(x,y)) \geq 2^{2n-1} - 2^{n-1}$. Лемма доказана.

Следующая теорема дает явную формулу для вычисления $dist(f(x,y),AE_{2n})$ для любой функции $f(x,y)$ из класса Мэйорана–Мак-Фарланда и служит основой для получения дальнейших оценок.

Теорема 1. Для любой функции $f(x,y) = \langle \pi(y), x \rangle \oplus \Phi(y)$ из класса Мэйорана–Мак-Фарланда от $2n$ переменных выполняется равенство:

$$dist(f(x,y),AE_{2n}) = 2^{2n-1} - 2^{n-1} -$$

$$- \max_{I,J,\beta',b} \left(2^{n-k} \cdot \sum_{\beta \in P \cap Q} sg\left(\langle \beta \oplus \beta', b \rangle \oplus \Phi(\beta) \oplus \Phi(\beta') \oplus \langle \pi(\beta) \oplus \pi(\beta'), (1,1,\ldots,1) \rangle \right) \right),$$

где $I = \{i1,\ldots,ik\} \subseteq \{1,\ldots,n\}$, $k = |I| \geq 1$, $J = \{j1,\ldots,jt\} \subseteq \{1,\ldots,n\}$, $\beta' \in V_n$, $b \in V_n$, $P = \{\beta \in V_n \mid (\pi(\beta))_s = (\pi(\beta'))_s$ при всех $s \notin I\}$, $Q = \{\beta \in V_n \mid \beta_{j1} = \ldots = \beta_{jt} = 1\}$, $sg(0) = -1$, $sg(1) = +1$ (если $P \cap Q = \varnothing$, то соответствующая сумма считается равной 0).

Доказательство. Заметим вначале, что, если $f(x_1,\ldots,x_n) \equiv c$, где c – константа $(c \in \{0,1\})$, то $wt(f(x_1,\ldots,x_n)) = 2^{n-1} + 2^{n-1} sg(c)$, где $sg(0) = -1$, $sg(1) = +1$. Это представление будет часто использоваться в дальнейшем.

Пусть $f(x,y) = \langle \pi(y), x \rangle \oplus \Phi(y)$ и пусть $g(x,y) = \langle a, x \rangle \oplus \langle b, y \rangle \oplus$ $\oplus c \oplus x_{i1} \cdot \ldots \cdot x_{ik} \cdot y_{j1} \cdot \ldots \cdot y_{jt}$ – произвольная функция из класса AE_{2n}, где $a \in V_n$, $b \in V_n$, $c \in \{0,1\}$, $I = \{i1,\ldots,ik\} \subseteq \{1,\ldots,n\}$, $J = \{j1,\ldots,jt\} \subseteq \{1,\ldots,n\}$. С учетом лемм 2 и 3, будем считать, что $k = |I| \geq 1$. Выражение $x_{i1} \cdot \ldots \cdot x_{ik} \cdot y_{j1} \cdot \ldots \cdot y_{jt}$ будем сокращенно записывать как $x_I y_J$, при этом положим $x_I y_\varnothing = x_I$. Положим

$$h(x,y) = f(x,y) \oplus g(x,y) = \langle \pi(y), x \rangle \oplus \Phi(y) \oplus \langle a, x \rangle \oplus \langle b, y \rangle \oplus c \oplus x_I y_J =$$
$$= \langle \pi(y) \oplus a, x \rangle \oplus \Phi(y) \oplus \langle b, y \rangle \oplus c \oplus x_I y_J.$$

Тогда $dist(f(x,y),g(x,y)) = wt(h(x,y))$ и наша задача – исследовать $wt(h(x,y))$.

Лемма 4. Пусть $\beta' = \pi^{-1}(a)$, $k = |I| \geq 1$, $P = \{\beta \in V_n \mid (\pi(\beta))_s = (\pi(\beta'))_s$ при всех $s \notin I\}$, $Q = \{\beta \in V_n \mid \beta_{j1} = \ldots = \beta_{jt} = 1\}$ (если $J = \{j1,\ldots,jt\}$ пусто, то $Q = V_n$). Тогда

$$wt(h(x,y)) = 2^{2n-1} + 2^{n-1} sg\left(\langle \beta', b \rangle \oplus \Phi(\beta') \oplus c \right) -$$
$$- 2^{n-k} \cdot \sum_{\beta \in P \cap Q} sg\left(\langle \beta, b \rangle \oplus \Phi(\beta) \oplus c \oplus \langle \pi(\beta) \oplus a, (1,1,\ldots,1) \rangle \right).$$

Доказательство. Пусть

$$h_1(x,y) = \langle \pi(y) \oplus a, x \rangle \oplus \Phi(y) \oplus \langle b, y \rangle \oplus c, \quad h_2(x,y) = x_I y_J.$$

Тогда $h(x,y) = h_1(x,y) \oplus h_2(x,y)$. При $\beta \neq \beta'$ имеем $\pi(\beta) \neq a$ и функция $h_1(x,\beta)$ является аффинной функцией, отличной от константы, откуда $wt(h_1(x,\beta)) = 2^{n-1}$. Если $\beta = \beta'$, то $\pi(\beta') \oplus a = 0$, $h_1(x,\beta') = \Phi(\beta') \oplus \langle b, \beta' \rangle \oplus c$ (константа) и $wt(h_1(x,\beta')) = = 2^{n-1} + 2^{n-1} sg(\Phi(\beta') \oplus \langle b,\beta' \rangle \oplus c)$. Отсюда

$$wt(h_1(x,y)) = \sum_{\beta \in V_n} wt(h_1(x,\beta)) = 2^{n-1}\cdot 2^n + 2^{n-1} sg(\Phi(\beta') \oplus \langle b,\beta'\rangle \oplus c) = 2^{2n-1} + 2^{n-1} sg(\Phi(\beta') \oplus \langle b,\beta'\rangle \oplus c).$$

Легко видеть, что $wt(h_2(x,y)) = 2^{n-k}\cdot 2^{n-t} = 2^{2n-k-t}$.

Исследуем теперь вес функции $h_1(x,y)\cdot h_2(x,y) = h_1(x,y)\cdot x_I y_J$. Имеем

$$wt(h_1(x,y)\cdot h_2(x,y)) = \sum_{\beta\in Q} wt(h_1(x,\beta)\cdot x_I) = \sum_{\beta\in Q} wt\left((\langle \pi(\beta)\oplus a, x\rangle \oplus \Phi(\beta) \oplus \langle b,\beta\rangle \oplus c)\cdot x_I\right).$$

Пусть x' – набор всех переменных x, кроме $x_{i1},\ldots,x_{ik}$, и пусть $h_3(x',\beta)$ – функция от $n-k$ переменных, получающаяся из $h_1(x,\beta)$ при подстановке $x_{i1} = \ldots = x_{ik} = 1$. Тогда $wt(h_1(x,\beta)\cdot x_I) = wt(h_3(x,\beta))$. При этом, если хотя бы для одной координаты $s \notin I$ выполняется $(\pi(\beta))_s \neq a_s$, то функция $h_3(x',\beta)$ – аффинная функция, отличная от константы, и поэтому ее вес равен 2^{n-k-1}. Если же $(\pi(\beta))_s = a_s$ при всех $s \notin I$, то $h_3(x',\beta)$ – константа, равная $\langle \pi(\beta)\oplus a,(1,1,\ldots,1)\rangle \oplus \Phi(\beta)\oplus\langle b,\beta\rangle\oplus c$, и ее вес равен $2^{n-k-1} + 2^{n-k-1} sg\left(\langle \pi(\beta)\oplus a,(1,1,\ldots,1)\rangle \oplus \Phi(\beta)\oplus\langle b,\beta\rangle\oplus c\right)$.

Таким образом,

$$wt(h_1(x,y)\cdot h_2(x,y)) = \sum_{\beta\in Q} wt(h_3(x',\beta)) = 2^{n-t}\cdot 2^{n-k-1} +$$

$$+ \sum_{\beta\in P\cap Q} 2^{n-k-1} sg\left(\langle \pi(\beta)\oplus a,(1,1,\ldots,1)\rangle \oplus \Phi(\beta)\oplus\langle b,\beta\rangle\oplus c\right).$$

Подставляя полученные формулы для $wt(h_1(x,y))$, $wt(h_2(x,y))$ и $wt(h_1(x,y)\cdot h_2(x,y))$ в равенство

$$wt(h(x,y)) = wt(h_1(x,y)\oplus h_2(x,y)) = wt(h_1(x,y)) + wt(h_2(x,y)) - 2\cdot wt(h_1(x,y)\cdot h_2(x,y)),$$

получим утверждение леммы 4.

Лемма 5. Пусть $\beta' = \pi^{-1}(a),$, $\langle \beta', b\rangle \oplus \Phi(\beta') \oplus c = 1$. Тогда $wt(h(x,y)) \geq 2^{2n-1} - 2^{n-1}$.

Доказательство. При $I = \varnothing$ утверждение следует из леммы 3. При $I \neq \varnothing$ воспользуемся леммой 4. Так как в лемме 4 имеем $|P| = 2^k$, то слагаемых под знаком суммирования в лемме 4 не больше 2^k. Тогда при условиях леммы 5:

$$wt(h(x,y)) \geq 2^{2n-1} + 2^{n-1} - 2^{n-k}2^k = 2^{2n-1} - 2^{n-1}.$$

Лемма доказана.

Из лемм 2, 3 и 5 вытекает, что для вычисления $dist(f(x,y), AE_{2n})$ для любой функции $f(x,y) = \langle \pi(y), x\rangle \oplus \Phi(y)$ из класса Мэйорана–Мак-Фарланда достаточно рассматривать $dist(f(x,y), g(x,y))$ только для таких функций $g(x,y) = \langle a, x\rangle \oplus \langle b, y\rangle \oplus c \oplus x_I y_J$, в которых $I \neq \varnothing$ и $c = \langle \beta', b\rangle \oplus \Phi(\beta')$, где $\beta' = \pi^{-1}(a)$.

По лемме 4 в таких случаях получим:

$$wt(h(x,y)) = 2^{2n-1} - 2^{n-1} - 2^{n-k}\cdot \sum_{\beta\in P\cap Q} sg\left(\langle \beta\oplus\beta', b\rangle \oplus \Phi(\beta)\oplus\Phi(\beta')\oplus\langle \pi(\beta)\oplus\pi(\beta'),(1,1,\ldots,1)\rangle\right).$$

Рассматривая минимум $wt(h(x,y))$ по всем таким функциям $h(x,y)$, получаем утверждение теоремы 1. Теорема 1 доказана.

Теорема 2. Для всех функций $f(x,y) = \langle \pi(y), x\rangle \oplus \Phi(y)$ из класса Мэйорана–Мак-Фарланда от $2n$ переменных при всех $n \geq 2$ выполняются неравенства:

$$2^{2n-1} - 3\cdot 2^{n-1} + 2 \leq dist(f, AE_{2n}) \leq 2^{2n-1} - 2\cdot 2^{n-1},$$

причем обе границы достижимы. (При $n=1$ $dist(f, AE_{2n})=0$ для всех f).

Доказательство. Верхняя оценка доказана в лемме 2. Покажем, что эта оценка достижима. Рассмотрим функцию $f(x,y)=\langle y,x\rangle$. Она входит в класс Мэйорана–Мак-Фарланда (при $\pi(y)\equiv y$ и $\Phi(y)\equiv 0$), поэтому мы можем использовать для нее теорему 1. Выражение под суммой в теореме 1 для данной функции примет вид:

$$sg\big(\langle\beta\oplus\beta',b\rangle\oplus\langle\beta\oplus\beta',(1,1,\ldots,1)\rangle\big)=sg\big(\langle\beta\oplus\beta',b\oplus(1,1,\ldots,1)\rangle\big).$$

При этом $I\neq\varnothing$ и $P=\{\beta\in V_n\mid(\beta)_s=(\beta')_s$ при всех $s\notin I\}$. Пусть $I=\{i1,\ldots,ik\}$, $k=|I|\geq 1$. Пусть b и β' фиксированы. Тогда при β, пробегающем множество P, выражение $\langle\beta\oplus\beta',b\oplus(1,1,\ldots,1)\rangle$ можно рассматривать как аффинную функцию от переменных $\beta_{i1},\ldots,\beta_{ik}$ без свободного члена. Такая функция принимает значение 1 не более 2^{k-1} раз. Поэтому для функции $f(x,y)=\langle y,x\rangle$ при любых фиксированных I,J,β',b сумма в теореме 1 не превосходит 2^{k-1} и, следовательно, максимум не превосходит 2^{n-1}. Тогда $dist(\langle x,y\rangle, AE_{2n})\geq 2^{2n-1}-2^{n-1}-2^{n-1}=2^{2n-1}-2\cdot 2^{n-1}$. С учетом леммы 2, получаем $dist(\langle x,y\rangle, AE_{2n})=2^{2n-1}-2\cdot 2^{n-1}$.

Докажем теперь нижнюю оценку. Посмотрим, какие значения может принимать сумма по множеству $P\cap Q$ в теореме 1. Так как $|P|=2^k$, то число слагаемых в сумме не превосходит 2^k и, следовательно, сама сумма не превосходит 2^k, а выражение под максимумом не превосходит 2^n. Отсюда максимум не превосходит 2^n и теорема 1 дает неравенство $dist(f, AE_{2n})\geq 2^{2n-1}-3\cdot 2^{n-1}$. Однако эта оценка недостижима. Заметим, что $\beta'\in P$ и при $\beta=\beta'$ слагаемое в сумме в теореме 1 равно $sg(0)=-1$. Поэтому, если $\beta'\in Q$, то $\beta'\in P\cap Q$ и сумма по множеству $P\cap Q$ в теореме 1 не превосходит 2^k-2, а соответствующее выражение под максимумом не превосходит $2^{n-k}\cdot(2^k-2)=2^n-2\cdot 2^{n-k}\leq 2^n-2$. Пусть теперь $\beta'\notin Q$. Тогда рассматриваемая сумма содержит не более 2^k-1 слагаемых и, следовательно, не превосходит 2^k-1. Тогда соответствующее выражение под максимумом не превосходит $2^{n-k}\cdot(2^k-1)=2^n-2^{n-k}\leq 2^n-2$ при $k<n$. Остается рассмотреть случай $k=n$ и $\beta'\notin Q$. Тогда $Q\neq V_n$ и $t\geq 1$. Поэтому $|P\cap Q|\leq|Q|\leq 2^{n-1}$. Тогда рассматриваемая сумма и соответствующее выражение под максимумом не превосходят $2^{n-1}\leq 2^n-2$ при $n\geq 2$. Таким образом, выражение под максимумом всегда не превосходит 2^n-2. Следовательно, и максимум не превосходит 2^n-2. Отсюда следует нижняя оценка в теореме 2. Докажем теперь, что она достижима.

Лемма 6. Для любой подстановки π на V_n существует функция $\Phi(y)$ от n переменных такая, что для функции $f(x,y)=\langle\pi(y),x\rangle\oplus\Phi(y)$ из класса Мэйорана–Мак-Фарланда от $2n$ переменных выполняется равенство $dist(f, AE_{2n})=2^{2n-1}-3\cdot 2^{n-1}+2$.

Доказательство. Для данной подстановки π определим функцию $\Phi(y)$ от n переменных следующим образом. Пусть $\Phi(0,\ldots,0)$ произвольно и $\Phi(y)=\Phi(0,\ldots,0)\oplus\langle\pi(y)\oplus\pi(0,\ldots,0),(1,1,\ldots,1)\rangle\oplus 1$ при $y\neq(0,\ldots,0)$. Возьмем $I=\{1,\ldots,n\}$, $J=\varnothing$, $\beta'=(0,\ldots,0)$, $b=(0,\ldots,0)$. Тогда $k=n$, $P=Q=V_n$. При этом в сумме в теореме 1 будет 2^n слагаемых вида $sg(\Phi(\beta)\oplus\Phi(0,\ldots,0)\oplus\oplus\langle\pi(\beta)\oplus\pi(0,\ldots,0),(1,1,\ldots,1)\rangle)$. При $\beta=(0,\ldots,0)$ это слагаемое равно $sg(0)=-1$. При

остальных β, подставляя в это слагаемое $\Phi(\beta) = \Phi(0,\ldots,0) \oplus$ $\oplus \langle \pi(\beta) \oplus \pi(0,\ldots,0), (1,1,\ldots 1)\rangle \oplus 1$, получаем, что это слагаемое равно $\mathrm{sg}(1) = 1$. Поэтому рассматриваемая сумма будет равна $2^n - 2$ и максимум будет не меньше $2^n - 2$. Поэтому для рассматриваемой функции $f(x,y) = \langle \pi(y), x\rangle \oplus \Phi(y)$ выполняется неравенство $dist(f, AE_{2n}) \le 2^{2n-1} - 3\cdot 2^{n-1} + 2$. С учетом доказанной нижней оценки в теореме 2 получаем, что для этой функции $dist(f, AE_{2n}) = 2^{2n-1} - 3\cdot 2^{n-1} + 2$. Лемма 6, а вместе с ней и теорема 2 доказаны.

Заключение

Таким образом, максимально-нелинейные функции из класса Мэйорана–Мак-Фарланда имеют разную стойкость при приближении их почти аффинными функциями класса AE_{2n}. В работе установлены точные пределы, в которых изменяется значение $dist(f, AE_{2n})$ для всех функций из класса Мэйорана–Мак-Фарланда. Вопрос о точных границах изменения величины $dist(f, AE_{2n})$ для произвольных максимально-нелинейных функций f от $2n$ переменных требует дальнейшего изучения.

Литература

1. Логачёв, О.А. Булевы функции в теории кодирования и криптологии [Текст] / О.А. Логачёв, А.А. Сальников, В.В. Ященко. – М.: Изд-во МЦНМО, 2004.-470 с.

INVESTIGATION OF A PARAMETER OF BOOLEAN FUNCTIONS CLOSED TO NONLINEARITY

V. B. Alekseev
R. R. Omarov

Lomonosov Moscow State University, Moscow

e-mail: vbalekseev@rambler.ru

e-mail: rustamomarov@ya.ru

Minimal distance (by Hamming) between Boolean function f and all affine Boolean functions is said to be *nonlinearity* of function f. This is one of the parameters characterizing quality of cryptographic systems using this function. We consider one set of Boolean functions having maximal nonlinearity, namely the Maiorana–McFarland set. We investigate how the distance between these functions and the set of approximating functions changes when we include in the set of approximating functions not only affine functions but also all functions having one nonlinear term in their Zhegalkin polynomial form. We show that new distance can be different for different functions from the Maiorana–McFarland set and it can vary between $2^{2n-1} - 3\cdot 2^{n-1} + 2$ and $2^{2n-1} - 2\cdot 2^{n-1}$ and both bounds can be achieved.

Key words: Boolean function, cryptographic properties of Boolean functions, nonlinearity, Maiorana–McFarland set.