ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2014. Том 21, № 5. С. 67–75

УДК 519.7

ОБ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ БЕНТ-ФУНКЦИЙ ИЗ КЛАССА ДИЛЛОНА

С. Ю. Филюзин

Аннотация. Известно, что значение алгебраической иммунности для функции от n переменных не превышает $\lceil n/2 \rceil$. В работе для алгебраической иммунности бент-функций Диллона, построенных с помощью линейных функций, доказывается верхняя оценка, равная $\lceil n/4 \rceil + 1$, что почти в два раза меньше максимальной.

Ключевые слова: булева функция, нелинейность, бент-функция, алгебраическая иммунность.

Введение

Путём детального анализа успешных способов взлома блочных и поточных шифров криптографами и математиками были сформулированы свойства булевой функции, которыми она должна обладать для использования её в криптографических приложениях. На данный момент остаётся открытым вопрос о том, как совмещаются различные криптографические свойства у одной булевой функции, в частности, высокие алгебраическая иммунность и нелинейность. В [10] получена нижняя оценка нелинейности булевых функций через алгебраическую иммунность. В [2] доказывается верхняя оценка нелинейности для предложенных в [7] булевых функций от чётного числа переменных, обладающих максимально возможной алгебраической иммунностью. В [11] получена верхняя оценка алгебраической иммунности для мономиальных функций от одной переменной с произвольным показателем степени. В [1] получены нижние оценки для ряда мономиальных функций.

В блочных и поточных шифрах бент-функции (булевые функции от чётного числа переменных с максимальной нелинейностью) и их векторные аналоги способствуют предельному повышению стойкости этих шифров к линейному и дифференциальному методам криптоанализа — основным статистическим методам криптоанализа шифров. Поэтому бент-функции используются в качестве компонент шифра и представляют интерес для изучения. С кратким обзором бент-функций можно ознакомиться в [3].

Особый интерес вызывает класс бент-функций, предложенных Диллоном [9], так как в этом классе существуют бент-функции с максимальной алгебраической иммунностью [13]. Работа [13] основана на комбинаторной гипотезе, полное доказательство которой на данный момент ещё не получено, но, например, в [6, 8] можно найти обоснования этой гипотезы в частных случаях.

Известно, что максимально возможное значение алгебраической иммунности для функции от n переменных не превышает $\lceil n/2 \rceil$. В данной работе получена верхняя оценка $\lceil n/4 \rceil + 1$ алгебраической иммунности бент-функций из класса Диллона, построенных с помощью линейных функций. Она почти в два раза меньше максимально возможного значения алгебраической иммунности функции, что даёт потенциальную возможность применить алгебраический криптоанализ к шифрам, использующим данные бент-функции. Поэтому использование линейных функций в качестве порождающих в конструкции Диллона нецелесообразно.

Известно [12], что степень любой бент-функции от $2k$ переменных не превосходит числа k. В [9] доказано, что степень бент-функций Диллона достигает своего максимума. В данной работе приведено простое доказательство аналогичного результата в частном случае, когда используются линейные функции для построения бент-функций.

1. Основные понятия

Пусть $\mathbb{Z}_2^n$ — множество двоичных векторов длины n и $x, y \in \mathbb{Z}_2^n$. Пусть символ $\oplus$ обозначает сложение по модулю два.

Расстоянием Хэмминга $d(x, y)$ между двумя векторами x и y длины n называется число координат, в которых они различаются. *Весом Хэмминга* $\mathrm{wt}(x)$ двоичного вектора x называется число его ненулевых элементов.

Булевой функцией от n переменных называется функция, действующая из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$. Любая булева функция от n переменных представляется в виде *алгебраической нормальной формы* (АНФ):

$$f(x_1, \ldots, x_n) = \left(\bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} x_{i_1} \cdot \ldots \cdot x_{i_k} \right) \oplus a_0,$$

где $a_0, a_{i_1 \ldots i_k} \in \mathbb{Z}_2$. *Алгебраической степенью* (или просто *степенью*) $\deg(f)$ булевой функции f называется число переменных в самом длинном слагаемом её АНФ. Под расстоянием Хэмминга между двумя булевыми функциями от n переменных понимается расстояние между век-

торами их значений. Булева функция называется *уравновешенной*, если она принимает значения 0 и 1 одинаково часто. *Носителем* булевой функции f от n переменных называется множество векторов длины n, на которых f принимает значение 1.

Алгебраической иммунностью $AI(f)$ булевой функции f называется минимальное целое число d такое, что существует ненулевая булева функция g степени d, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$. Функция g называется *аннулятором* функции f или $f \oplus 1$ соответственно.

Нелинейностью булевой функции f от n переменных называется расстояние Хэмминга от данной функции до множества всех аффинных функций. *Бент-функция* — булева функция от n переменных (n чётно), обладающая максимальной нелинейностью, равной $2^{n-1} - 2^{(n/2)-1}$.

Пусть $GF(2^n)$ — конечное поле, а $GF^*(2^n)$ — конечное поле без нулевого элемента. *След* $\mathrm{tr}(c)$ — это функция из $GF(2^n)$ в $GF(2^n)$ вида $\mathrm{tr}(c) = c + c^2 + c^{2^2} + \ldots + c^{2^{n-1}}$. Особенностью следа является то, что его значения лежат в $GF(2)$.

2. Булевы функции и конечные поля

Заметим, что любую функцию из $GF(2^n)$ в $GF(2)$ можно рассматривать как булеву функцию, действующую из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$, так как между $\mathbb{Z}_2^n$ и $GF(2^n)$ существует взаимно однозначное соответствие, а именно, элементу x из $GF(2^n)$ в некотором базисе однозначно соответствует вектор $x = (x_1, \ldots, x_n)$ из $\mathbb{Z}_2^n$, где $x_1, \ldots, x_n \in GF(2)$.

Лемма 1. *Пусть* $a, b \in GF(2^n)$. *Тогда* $(a+b)^{2^k} = a^{2^k} + b^{2^k}$, *где* n, k — *натуральные числа.*

Пусть k — натуральное число. Определим вес $\mathrm{wt}(k)$ числа k как вес его двоичного представления.

Пусть $f : GF(2^n) \to GF(2^n)$. Известно [5], что функция f представляется в виде $f(x) = \sum\limits_{i=0}^{2^n-1} \delta_i x^i$, где $\delta_i \in GF(2^n)$ и $\deg(f) = \max\limits_{i|\delta_i \neq 0} \{\mathrm{wt}(i)\}$.

Покажем, что для функций вида $f : GF(2^k) \times GF(2^k) \to GF(2^k)$ справедливо аналогичное представление.

Лемма 2. *Пусть* $f : GF(2^k) \times GF(2^k) \to GF(2^k)$. *Тогда* f *однозначно представляется в виде* $f(x,y) = \sum\limits_{i=0}^{2^k-1} \sum\limits_{j=0}^{2^k-1} \delta_{ij} x^i y^j$, *где* $\delta_{ij} \in GF(2^k)$, *при этом* $\deg(f) = \max\limits_{i,j|\delta_{ij} \neq 0} \{\mathrm{wt}(i) + \mathrm{wt}(j)\}$.

Доказательство. Разобьём доказательство на три пункта.

Представимость. Можем представить f в виде полинома

$$f(x,y)=\sum_{a\in GF(2^k)}\sum_{b\in GF(2^k)} f(a,b)(1+(x+a)^{2^k-1})(1+(y+b)^{2^k-1}).$$

Действительно, возьмём $x=a,\ y=b$, тогда

$$f(a,b)(1+(x+a)^{2^k-1})(1+(y+b)^{2^k-1})=f(a,b).$$

В остальных случаях (если $x\neq a$ и/или $y\neq b$) это слагаемое равно нулю, поскольку $x^{2^k-1}=1$ для любого $x\in GF^*(2^k)$.

Степень. Пусть $\{\alpha_1,\ldots,\alpha_k\}$ — базис $GF(2^k)$ как векторного пространства над $GF(2)$. Тогда любое $x\in GF(2^k)$ представимо в виде $x=\sum\limits_{l=1}^{k} x_l\alpha_l$, где $x_l\in\{0,1\}$. Так как любое число $j\in\{0,\ldots,2^k-1\}$ можно представить в двоичной системе счисления: $j=\sum\limits_{s=0}^{k-1} j_s 2^s$, где $j_s\in\{0,1\}$, функция f будет выглядеть следующим образом:

$$f(x,y)=\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\delta_{ij}\left(\sum_{l=1}^{k}x_l\alpha_l\right)^{\sum\limits_{v=0}^{k-1}i_v2^v}\left(\sum_{l=1}^{k}y_l\alpha_l\right)^{\sum\limits_{s=0}^{k-1}j_s2^s}$$
$$=\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\delta_{ij}\prod_{v=0|i_v\neq0}^{k-1}\sum_{l=1}^{k}x_l\alpha_l^{2^v}\prod_{s=0|i_s\neq0}^{k-1}\sum_{l=1}^{k}y_l\alpha_l^{2^s}.$$

Последнее равенство получается из леммы 1.

Отсюда $\deg(f)\leqslant\max\limits_{i,j|\delta_{ij}\neq0}\{\mathrm{wt}(i)+\mathrm{wt}(j)\}$. В действительности, степень всегда равна этой приведённой верхней границе, так как число $2^{k\sum\limits_{i=0}^{d}\binom{n}{i}}$ всех функций степени, не превышающей d, совпадает с числом полиномов $\sum\limits_{i=0}^{2^k-1}\sum\limits_{j=0}^{2^k-1}\delta_{ij}x^iy^j$ таких, что $\max\limits_{i,j=0,\ldots,2^k-1|\delta_{ij}\neq0}\{\mathrm{wt}(i)+\mathrm{wt}(j)\}\leqslant d$ для любых d.

Однозначность. Поскольку для каждой функции существует полином и согласно предыдущему пункту число полиномов совпадает с числом функций, представление однозначно. Лемма 2 доказана.

Замечание. Так как $GF(2^n)$ включает в себя $GF(2)$, далее будем рассматривать данное представление для функций $f:GF(2^n)\to GF(2)$.

Лемма 3 [4]. *Линейная функция $f : GF(2^n) \to GF(2)$ может быть представлена в виде $f(c) = \mathrm{tr}(ac)$ для подходящего элемента $a \in GF(2^n)$.*

Лемма 4. *Пусть f, ψ — булевы функции от n переменных. Тогда функция $h = f\psi$, где $\deg(h) \geqslant 1$, является аннулятором функции $f \oplus 1$.*

Доказательство. Действительно, домножим обе части равенства $h = f\psi$ на f. Так как $ff = f$, получаем $fh = f\psi = h$. Тогда $fh = h$ и $(f \oplus 1)h = 0$. Лемма 4 доказана.

3. Двоичное представление целых чисел

Пусть $d \in \mathbb{Z}$. Обозначим через $d_{n-1} \dots d_1 d_0$ двоичное представление числа d, где $d = \sum\limits_{s=0}^{n-1} d_s \cdot 2^s$.

Замечание. Для подсчёта степени алгебраического полинома функции $f : GF(2^k) \times GF(2^k) \to GF(2^k)$ из леммы 2 требуется, чтобы показатели степеней переменной принадлежали множеству $\{0, \dots, 2^k - 1\}$. Определим правило приведения произвольной целой степени $i > 0$ к нужному виду:

$$\eta(i) = b, \quad \text{где } b \in \{1, \dots, 2^k - 1\} \text{ и } b \equiv i \bmod (2^k - 1).$$

Действительно, функция $\eta(i)$ определена корректно и $x^{\eta(i)} = x^i$ для всех $x \in GF(2^k)$ при всех целых положительных i.

Лемма 5. *Если $d_{k-1} \dots d_0$ — двоичное представление $d \in \mathbb{Z}$, то двоичное представление числа $d \cdot 2^j \mod (2^k - 1)$ есть циклический сдвиг $d_{k-1} \dots d_0$ на j элементов влево.*

Доказательство. Рассмотрим случай $j = 1$. Имеем

$$\begin{aligned} 2 \cdot d \bmod (2^k - 1) &= d_{k-2} \dots d_0 0 + d_{k-1} \cdot 2^k \bmod (2^k - 1) \\ &= d_{k-2} \dots d_0 0 + d_{k-1} \cdot (2^k - 1 + 1) \bmod (2^k - 1) \\ &= d_{k-2} \dots d_0 0 + d_{k-1} \cdot (2^k - 1) + d_{k-1} \bmod (2^k - 1) \\ &= d_{k-2} \dots d_0 d_{k-1} \bmod (2^k - 1). \end{aligned}$$

Из доказанного выше следует, что при $j > 1$ условие леммы также верно. Лемма 5 доказана.

Лемма 6. *Пусть $k \geqslant 3$, $\beta = \sum\limits_{s=0}^{\lceil \frac{k}{2} \rceil - 1} 2^{2s}$. Тогда при $0 \leqslant i, j \leqslant k-1$ верно*

$$\mathrm{wt}(\eta(\beta 2^j - 2^i + 2^k - 1)) \leqslant \lceil k/2 \rceil.$$

Доказательство. Очевидно, что

$$\mathrm{wt}(\eta(\beta 2^j - 2^i + 2^k - 1)) = \mathrm{wt}(\eta(\beta^{(j)} - 2^i + 2^k - 1)),$$

где $\beta^{(j)} = \eta(\beta 2^j)$.

По лемме 5 получаем

$$\beta^{(j)} = \sum_{s=0}^{\lceil \frac{k}{2} \rceil - 1} 2^{(2s+j) \bmod k}. \tag{1}$$

Заметим следующий факт. Пусть $0 \leqslant r \leqslant k-1$. Тогда либо слагаемое 2^r, либо слагаемое $2^{r+1 \bmod k}$ присутствует в сумме из (1).

Поскольку $k \geqslant 3$, имеем $\beta^{(j)} \neq 2^i$.

Случай 1: $\beta^{(j)} > 2^i$. Тогда

$$\mathrm{wt}(\eta(\beta^{(j)} - 2^i + 2^k - 1)) = \mathrm{wt}(\beta^{(j)} - 2^i)) \leqslant \mathrm{wt}(\beta^{(j)}) = \lceil k/2 \rceil,$$

так как либо 2^i, либо 2^{i+1} присутствует в сумме (1).

Случай 2: $\beta^{(j)} < 2^i$. Это возможно только тогда, когда $i = k-1$ и в сумме из (1) отсутствует слагаемое 2^{k-1}. Следовательно, должно присутствовать слагаемое $2^{k \bmod k} = 1$. Тем самым имеем

$$\begin{aligned}\mathrm{wt}(\eta(\beta^{(j)} - 2^i + 2^k - 1)) &= \mathrm{wt}(\beta^{(j)} - 2^{k-1} + 2^k - 1) \\ &= \mathrm{wt}(\beta^{(j)} + 2^{k-1} - 1) = \mathrm{wt}(\beta^{(j)}) = \lceil k/2 \rceil.\end{aligned}$$

Лемма 6 доказана.

4. Оценка алгебраической иммунности функций Диллона

Функцию $g : GF(2^k) \to GF(2)$ будем рассматривать как булеву, зафиксировав некоторый базис в поле $GF(2^k)$. В [9] Диллон приводит следующий способ построения бент-функций.

Конструкция Диллона. Пусть $g : GF(2^k) \to GF(2)$ — уравновешенная функция от k переменных и $g(0) = 0$. Тогда функция $f(x, y) = g(xy^{2^k-2})$ является бент-функцией от $2k$ переменных.

Рассмотрим бент-функции Диллона, построенные с помощью линейных функций.

Теорема 1. *Пусть функция $g : GF(2^k) \to GF(2)$ линейна, $g \neq \mathrm{const}$ и f построена с помощью конструкции Диллона по функции g, а именно $f(x, y) = g(xy^{2^k-2})$. Тогда $AI(f) \leqslant \lceil k/2 \rceil + 1$.*

Доказательство. Пусть $k \geqslant 3$, поскольку при $k = 1, 2$ оценка следует из неравенства $\deg(f) \leqslant k$. Так как $f(x, y) = g(xy^{2^k-2})$ и g линейна, по лемме 3 представим f в виде $f(x, y) = \mathrm{tr}(axy^{2^k-2})$ для подходящего $a \in GF(2^k)$. Будем искать аннулятор функции $f \oplus 1$, используя лемму 4, где $\psi(x, y) = \mathrm{tr}(by^\beta)$ при некотором $\beta \in \mathbb{Z}$. Заметим, что $AI(f) \leqslant \deg(h)$, где $h = f\psi$. Распишем функцию h:

$$h(x,y) = f(x,y)\psi(x,y) = \mathrm{tr}(axy^{2^k-2}) \cdot \mathrm{tr}(by^\beta)$$
$$= \sum_{i=0}^{k-1}(axy^{2^k-2})^{2^i} \sum_{j=0}^{k-1}(by^\beta)^{2^j} = \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} a^{2^i}b^{2^j}x^{2^i}y^{(2^k-1)2^i-2^i+\beta 2^j}$$
$$= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} a^{2^i}b^{2^j}x^{2^i}y^{\beta 2^j-2^i+2^k-1}.$$

Тогда $AI(f) \leqslant \deg(h) \leqslant \max\limits_{i,j}(\mathrm{wt}(2^i) + \mathrm{wt}(\eta(\beta 2^j - 2^i + 2^k - 1)))$.

Рассмотрим первое слагаемое. Очевидно, что $\mathrm{wt}(2^i) = 1$.

Рассмотрим второе слагаемое $\mathrm{wt}(\eta(\beta 2^j - 2^i + 2^k - 1))$. Пусть $\beta = \sum\limits_{s=0}^{\lceil k/2\rceil-1} 2^{2s}$. Тогда по лемме 6 получим

$$\mathrm{wt}(\eta(\beta 2^j - 2^i + 2^k - 1)) \leqslant \lceil k/2\rceil.$$

Следовательно, $\deg(h) \leqslant \lceil k/2\rceil + 1$. Также если $\deg(h) = 0$, то ψ аннулирует функцию f, при этом при некотором b имеем $\deg(\psi) = \mathrm{wt}(\beta) = \lceil k/2\rceil$.

В результате получаем $AI(f) \leqslant \lceil k/2\rceil + 1$. Теорема 1 доказана.

Данная оценка почти в два раза меньше максимально возможного значения алгебраической иммунности функции, что даёт потенциальную возможность применить алгебраический криптоанализ к шифрам, использующим данные бент-функции.

5. О степенях булевых функций в конструкции Диллона

Известно [12], что степень любой бент-функции от $2k$ переменных не превосходит числа k.

В [9] доказано, что бент-функции Диллона достигают своей максимальной степени. Приведём простое доказательство данного утверждения в случае, когда g линейна.

Утверждение 1. *Пусть функция $g : GF(2^k) \to GF(2)$ линейна, $g \neq \mathrm{const}$ и f построена с помощью конструкции Диллона по функции g: $f(x, y) = g(xy^{2^k-2})$. Тогда $\deg(f) = k$.*

Доказательство. Согласно лемме 2 функция f может быть представлена в виде полинома от двух переменных:

$$f(x,y)=\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\delta_{ij}x^iy^j,\quad \delta_{ij}\in GF(2^k).$$

Так как функция g линейна, по лемме 3 она представима с помощью следа: $g(x)=\mathrm{tr}(ax)$ при некотором $a\in GF(2^k)$. Тогда

$$\begin{aligned}f(x,y)=g(xy^{2^k-2})&=\mathrm{tr}(axy^{2^k-2})\\&=axy^{2^k-2}+(axy^{2^k-2})^2+\ldots+(axy^{2^k-2})^{2^{k-1}}\\&=axy^{2^k-2}+a^2x^2y^{2^{k+1}-2^2}+\ldots+a^{2^{k-1}}x^{2^{k-1}}y^{2^k-1-2^{k-1}}.\end{aligned}$$

Заметим, что если $c\in GF^*(2^n)$, то $c^{2^n-1}=1$. Поэтому при $i\geqslant 0$ выводим

$$(c^{(2^k-2)})^{2^i}=c^{2^{k+i}-2^{i+1}}=c^{(2^k-1)(2^i-1)+(2^k-1-2^i)}=c^{2^k-1-2^i}.$$

Из леммы 2 следует, что $\deg(f)=(\mathrm{wt}(2^{k-1})+\mathrm{wt}(2^k-1-2^{k-1}))$. Так как 2^n в двоичном представлении имеет вид $1\underbrace{0\ldots0}_{n}$, получаем $\mathrm{wt}(2^k-1-2^{k-1})=k-1$ и $\mathrm{wt}(2^{k-1})=1$. Стало быть, $\deg(f)=k$.

Таким образом, бент-функции Диллона f от $2k$ переменных, построенные с помощью линейных функций, имеют максимально возможную степень k. Утверждение 1 доказано.

ЛИТЕРАТУРА

1. **Баев В. В.** Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими след-формами // Пробл. передачи информ. — 2008. — Т. 44, вып. 3. — С. 81–104.
2. **Коломеец Н. А.** О верхней оценке нелинейности некоторого класса булевых функций с максимальной алгебраической иммунностью // Прикл. дискрет. математика. — 2013. — Вып. 1. — С. 14–16.
3. **Токарева Н. Н.** Бент-функции: результаты и приложения. Обзор работ // Прикл. дискр. мат. — 2009. — № 1. — С. 15—37.
4. **Токарева Н. Н.** Симметричная криптография. Краткий курс: учебное пособие. — Новосибирск: Новосиб. гос. ун-т, 2012. — 234 с.
5. **Carlet C.** Vectorial Boolean functions for cryptography // Boolean models and methods in mathematics, computer science, and engineering. — Cambridge: Cambridge Univ. Press, 2010. — P. 398–472.
URL: www.math.univ-paris13.fr/ carlet

6. **Cusick T. W., Yuan L., Stănică P.** On a combinatoric conjecture // Integers. — 2011. — Vol. 1. — P. 185–203.
7. **Dalai D. K., Maitra S., Sarkar S.** Basic theory in construction of Boolean functions with maximum possible annihilator immunity // Des. Codes Cryptogr. — 2006. — Vol. 40, N 1. — P. 41–58.
8. **Deng G.** A note on a combinatorial conjecture // Open J. Discrete Math. — 2013. — Vol. 3. — P. 49–52.
9. **Dillon J. F.** Elementary Hadamard difference sets: Thes.... doct. philosophy. — Univ. of Maryland, 1974.
10. **Lobanov M.** Exact relation between nonlinearity and algebraic immunity // Discrete Math. Appl. — 2006. — Vol. 16, N 5. — P. 453–460.
11. **Nawaz Y., Gong G., Gupta K. C.** Upper bounds on algebraic immunity of Boolean power functions // FSE. — 2006. — P. 243–265. (Lect. Notes Comput. Sci.; Vol. 4047).
12. **Rothaus O.** On bent functions // J. Comb. Theory. Ser. A. — 1976. — Vol. 20, N 3. — P. 300–305.
13. **Tu Z., Deng Y.** A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity // Des. Codes Cryptogr. — 2011. — Vol. 60, N 1. — P. 1–14.

Филюзин Станислав Юрьевич,
e-mail: forgogu@inbox.ru

Статья поступила
20 августа 2013 г.

Переработанный вариант —
28 марта 2014 г.