Утверждение 1. Пусть x, y, z — переменные со значениями в $\mathbb{Z}_2^n$, $\mathbb{Z}_2^m$ и $\mathbb{Z}_2^k$ соответственно и для всех $1 \leq s \leq l$ и $1 \leq i_1 < i_2 < \dots < i_s \leq l$ функции $f_{i_1}(x, y) \oplus \dots \oplus \oplus f_{i_s}(x, y)$ статистически не зависят от переменных в x . Тогда для любой функции g от $l + k$ переменных суперпозиция $g(f_1(x, y), \dots, f_l(x, y), z)$ статистически не зависит от переменных в x .

Замечание 1. В ряде случаев (для конкретных функций g и ограничений на функции $f_1, \dots, f_l$) можно сократить количество достаточных условий утверждения; этот вопрос составляет предмет дальнейших исследований.

ЛИТЕРАТУРА

1. Колчева О. Л., Панкратова И. А. О статистической независимости суперпозиции булевых функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 11–12.
2. Колчева О. Л., Панкратова И. А. О статистической независимости суперпозиции булевых функций. II // Прикладная дискретная математика. Приложение. 2012. № 5. С. 14–15.

УДК 519.7

ВЕРХНЯЯ ОЦЕНКА АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ НЕКОТОРЫХ БЕНТ-ФУНКЦИЙ ДИЛЛОНА

С. Ю. Филюзин

Получена верхняя оценка алгебраической иммунности некоторых бент-функций Диллона. Приводится степень бент-функций максимальной алгебраической иммунности, предложенных З. Ту и Й. Денгом.

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

Путём детального анализа успешных способов взлома блочных и поточных шифров были определены 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. Данная работа посвящена изучению алгебраической иммунности при максимальной нелинейности булевой функции.

Булева функция от n переменных представима единственным образом в виде алгебраической нормальной формы (АНФ): $f(x_1, \dots, x_n) = \left(\bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_k} \right) \oplus a_0$, где $a_0, a_i \in \mathbb{Z}_2$. Степенью $\deg(f)$ булевой функции f называется число переменных в самом длинном слагаемом её АНФ. Алгебраической иммунностью $AI(f)$ булевой функции f называется минимальное целое число $d \geq 1$, такое, что существует булева функция g степени d , для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$. Нелинейностью $nl(f)$ булевой функции f от n переменных называется расстояние Хэмминга от данной функции до множества аффинных функций от n переменных. Бент-функция — булева функция от n переменных (n чётно), обладающая максимальной нелинейностью равной $2^{n-1} - 2^{(n/2)-1}$.

На сегодняшний день полная классификация бент-функций не произведена, но предложены способы построения таких функций. Функцию вида $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$ будем рассматривать как булеву, зафиксировав некоторый базис в поле $\text{GF}(2^k)$. В работе [1] Диллон приводит следующий способ построения бент-функций. Пусть

$g : \text{GF}(2^k) \rightarrow \text{GF}(2)$ — уравновешенная функция от k переменных и $g(0) = 0$. Тогда функция $f(x, y) = g(x \cdot y^{2^k-2})$ является бент-функцией от $2k$ переменных.

В данной работе исследуется алгебраическая иммунность некоторых бент-функций Диллона. В качестве уравновешенных рассматриваются линейные функции, как самые простые. Доказана

Теорема 1. Пусть функция $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$ линейна, $g \neq \text{const}$ и f построена с помощью конструкции Диллона по функции g , а именно $f(x, y) = g(x \cdot y^{2^k-2})$. Тогда $\text{AI}(f) \leq \lceil k/2 \rceil + 1$. При $k = 2, \dots, 8$ оценка достигается.

Из теоремы заключаем, что алгебраическая иммунность бент-функций Диллона, построенных с помощью линейных булевых функций, отличается от максимально возможной почти в 2 раза.

В конструкции Диллона свойства бент-функции f зависят от выбора g . Возникает ряд вопросов — существуют ли такие g , чтобы $\text{AI}(f)$ была максимальной, а если существуют, то какими свойствами обладают.

В работе [2] предлагается способ построения таких g . Пусть $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$, $\text{supp}(g) = \{\alpha^s, \dots, \alpha^{s+2^{k-1}-1}\}$, где α — примитивный элемент поля $\text{GF}(2^k)$ и $s \in \mathbb{N}$. Тогда бент-функция f , построенная с помощью конструкции Диллона, обладает максимальной алгебраической иммунностью. Доказано

Утверждение 1. Пусть $g : \text{GF}(2^k) \rightarrow \text{GF}(2)$, $\text{supp}(g) = \{\alpha^s, \dots, \alpha^{s+2^{k-1}-1}\}$, где α — примитивный элемент $\text{GF}(2^k)$ и $s \in \mathbb{N}$. Тогда для $k = 2, 3, \dots, 8$ верно $\text{deg}(g) = k - 1$.

ЛИТЕРАТУРА

1. *Dillon J. F.* Elementary Hadamard difference sets. Ph. D. Thesis. Univ. of Maryland, 1974.
2. *Tu Z. and Deng Y.* A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity // *Designs, Codes and Cryptography*. 2011. V. 60. Iss. 1. P. 1–14.

УДК 519.6

ЭКВИВАЛЕНТНОСТЬ ПРИМИТИВНЫХ МНОЖЕСТВ

В. М. Фомичев

Исследована эквивалентность примитивных множеств натуральных чисел в связи с диофантовой проблемой Фробениуса. Эквивалентность используется для упрощения определения числа Фробениуса $g(a_1, \dots, a_k)$, а также всех чисел, не содержащихся в аддитивной полугруппе, порождённой множеством $\{a_1, \dots, a_k\}$.

Ключевые слова: функция Фробениуса, примитивное множество, аддитивная полугруппа чисел.

Основные обозначения:

$\mathbb{N}$ — множество натуральных чисел, $k, n \in \mathbb{N}$, $A = \{a_1, \dots, a_k\} \subset \mathbb{N}$;

$(a_1, \dots, a_k)$ — наибольший общий делитель чисел $a_1, \dots, a_k$;

$\langle a_1, \dots, a_k \rangle$ — аддитивная полугруппа, порождённая множеством $\{a_1, \dots, a_k\}$;

$n\{a_1, \dots, a_k\} = \{na_1, \dots, na_k\}$;

$A^{(i)} = \{a_1, \dots, a_i\}$, $C(A^{(i)}) = d_i \mathbb{N}_0 \setminus \langle A^{(i)} \rangle$, $d_i = (a_1, \dots, a_i)$, $i = 2, \dots, k$.

Множество $A = \{a_1, \dots, a_k\}$ натуральных чисел, $k > 1$, называется примитивным, если $(a_1, \dots, a_k) = 1$.