Теорема 1. Пусть f, g — различные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана — МакФарланда при условии, что перестановка, фигурирующая в данной конструкции, является элементом $\mathrm{GL}(n/2, \mathbb{Z}_2)$. Если бент-функции f, g самодуальные, то

$$\mathrm{dist}(f,g) \in \{2^{n-1}, 2^{n-1}(1 \pm 1/2), 2^{n-1}\left(1 \pm 1/2^2\right), \ldots, 2^{n-1}\left(1 \pm 1/2^{n/2-1}\right), 2^n\}.$$

Следствие 1. Пусть f, g — различные самодуальные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана — МакФарланда при условии, что перестановка, фигурирующая в данной конструкции, является элементом $\mathrm{GL}(n/2, \mathbb{Z}_2)$. Тогда

$$\mathrm{dist}(f,g) \geqslant 2^{n-2}.$$

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
3. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
4. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. P. 183–198.
5. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. P. 395–406.

УДК 519.7 DOI 10.17223/2226308X/9/12

УСЛОВИЯ СУЩЕСТВОВАНИЯ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ[1]

Д. П. Покрасенко

Исследуется максимальная компонентная алгебраическая иммунность и её связь с матрицами специального вида. Получены ограничения на значения n, m, при которых возможно существование векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ с максимальной компонентной алгебраической иммунностью.

Ключевые слова: *векторная булева функция, компонентная алгебраическая иммунность.*

Важным криптографическим свойством булевых функций является алгебраическая иммунность, она была введена в работе [1]. *Алгебраической иммунностью* $\mathrm{AI}(f)$ булевой функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется минимальное число d, такое, что существует булева функция g степени d, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$.

Данное понятие различными способами было обобщено на векторный случай. Одним из наиболее естественных обобщений является понятие компонентной алгебраической иммунности, введённое в [2]. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $b \cdot F$ ($b \in \mathbb{Z}_2^m$, $b \neq 0$), т. е. $\mathrm{AI}_{\mathrm{comp}}(F) = \min\{\mathrm{AI}(b \cdot F) : b \in \mathbb{Z}_2^m, b \neq 0\}$, где $b \cdot F = b_1 f_1 \oplus \ldots \oplus b_m f_m$.

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

Для булевых функций от n переменных известно [3], что алгебраическая иммунность всегда меньше или равна $\lceil n/2 \rceil$, более того, существуют функции, имеющие $\mathrm{AI}(f) = \lceil n/2 \rceil$. В случае компонентной алгебраической иммунности векторных булевых функций также получено [2], что $\mathrm{AI}_{\mathrm{comp}}(F) \leqslant \lceil n/2 \rceil$. Данная работа посвящена изучению условий существования векторных булевых функций с максимальной компонентной алгебраической иммунностью равной $\lceil n/2 \rceil$.

Для каждой векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ введём две матрицы M_F, M'_F, элементами которых являются булевы функции от n переменных. Построим эти матрицы следующим способом: в матрице M_F j-му столбцу соответствует умножение компонентной функции $b \cdot F$, $b \neq 0$, на все мономы степени меньше $\lceil n/2 \rceil$, за исключением тождественно равного нулю монома. Матрица M'_F строится аналогично, только вместо $b \cdot F$ подставляется $b \cdot F \oplus 1$. Сопоставим вектор $a = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ моному от n переменных, где $a_i = 1$ соответствует наличию в мономе переменной x_i. Нумерация столбцов идёт по вектору $b \in \mathbb{Z}_2^m$, $b \neq 0$; строки занумерованы векторами $a = (a_1, \ldots, a_n)$:

$$M_F = \begin{pmatrix} f_1 & f_2 & \ldots & f_1 \oplus f_2 \oplus \ldots \oplus f_m \\ f_1 \cdot x_1 & f_2 \cdot x_1 & \ldots & (f_1 \oplus f_2 \oplus \ldots \oplus f_m)x_1 \\ \ldots & \ldots & \ldots & \ldots \\ f_1 \cdot x_1 x_2 & \ldots & \ldots & (f_1 \oplus f_2 \oplus \ldots \oplus f_m)x_1 x_2 \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix},$$

$$M'_F = \begin{pmatrix} f_1 \oplus 1 & f_2 \oplus 1 & \ldots & f_1 \oplus \ldots \oplus f_m \oplus 1 \\ (f_1 \oplus 1)x_1 & (f_2 \oplus 1)x_1 & \ldots & (f_1 \oplus \ldots \oplus f_m \oplus 1)x_1 \\ \ldots & \ldots & \ldots & \ldots \\ (f_1 \oplus 1)x_1 x_2 & \ldots & \ldots & (f_1 \oplus \ldots \oplus f_m \oplus 1)x_1 x_2 \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

Функции $f_1, \ldots, f_n$ являются *линейно независимыми*, если выражение $a_1 f_1 \oplus a_2 f_2 \oplus \oplus \ldots \oplus a_n f_n$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}_2$, тождественно равно нулю только при условии $a_1 = = a_2 = \ldots = a_n = 0$.

В работе [4] установлено, что векторная булева функция имеет максимальную компонентную алгебраическую иммунность $\mathrm{AI}_{\mathrm{comp}}(F) = \lceil n/2 \rceil$ тогда и только тогда, когда в матрицах M_F и M'_F элементы любого столбца образуют линейно независимое множество. В продолжение данной работы получено утверждение, поясняющее структуру матриц.

Введём новую матрицу M, которая строится из матрицы M_F приписыванием справа от неё матрицы M'_F. Таким образом получаем матрицу, у которой элементы — булевы функции, количество строк такое же, как у матриц M_F и M'_F, а количество столбцов увеличивается в 2 раза.

Утверждение 1. Если векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ имеет максимальную компонентную алгебраическую иммунность $\mathrm{AI}_{\mathrm{comp}}(F) = \lceil n/2 \rceil$, то в любой строке матрицы M все элементы попарно различны.

При изучении максимальной компонентной иммунности возникает вопрос о существовании ограничений на значения n, m, а также на их связь друг с другом. Получено следующее соотношение.

Утверждение 2. Векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ может иметь максимальную компонентную алгебраическую иммунность $\mathrm{AI}_{\mathrm{comp}}(F) = \lceil n/2 \rceil$ только для

таких n, m, для которых выполняется следующее условие:

$$m \leqslant 2^{\lceil (n+1)/2 \rceil} - 1.$$

ЛИТЕРАТУРА

1. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt 2004. LNCS. 2004. V. 3027. P. 474–491.
2. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, 2009. P. 104–116.
3. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt 2003. LNCS. 2003. V. 2656. P. 345–359.
4. *Pokrasenko D.* On the maximal component algebraic immunity of vectorial Boolean functions // J. Appl. Industr. Math. 2016. V. 10. P. 257–263.

УДК 512.13 DOI 10.17223/2226308X/9/13

ПРЕДСТАВЛЕНИЕ ПОЛУБАЙТОВЫХ ПОДСТАНОВОК АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ МАГМА И 2-ГОСТ АЛГЕБРАИЧЕСКИМИ ПОРОГОВЫМИ ФУНКЦИЯМИ

Д. А. Сошин

Работа посвящена реализации полубайтовых подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ алгебраическими пороговыми функциями (АПФ). Для каждой из подстановок алгоритмов Магма рассмотрен вопрос принадлежности линейных комбинаций координатных функций к классу АПФ. Для подстановок 2-ГОСТ предложено их задание через линейные комбинации АПФ.

Ключевые слова: *алгебраические пороговые функции, подстановки.*

В работе [1] вводится новый класс функций, который назван классом алгебраических пороговых функций.

Определение 1. Функция k-значной логики $f_n^k : \Omega_k^n \to \Omega_k$ называется *алгебраической пороговой*, если существуют целочисленные наборы $(c_0, c_1, \ldots, c_n)$, $(b_0, b_1, \ldots, b_k)$ и модуль m, такие, что для любого $\alpha \in \{0, \ldots, k-1\}$ выполняется

$$f_n^k(x_1,\ x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant r_m(c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n) < b_{\alpha+1},$$

где $r_m(y)$ — *функция взятия остатка* при делении целого числа y на модуль m ($r_m(y) \in \{0, 1, \ldots, m-1\}$); $\Omega_k = \{0, 1, \ldots, k-1\}$; $\Omega_k^n = \underbrace{\Omega_k \times \Omega_k \times \cdots \times \Omega_k}_{n}$.

Тройку $((c_0, c_1, \ldots, c_n); (b_0, b_1, \ldots, b_k); m\ )$ назовём *структурой алгебраической пороговой функции* f_n^k.

В [1] проведено исследование вопроса реализации булевых функций трёх переменных функциями из класса АПФ. Для этого доказана замкнутость данного класса относительно операций перестановки переменных, инвертирования переменных в смысле Лукашевича и инвертирования функции (геометрическая замкнутость). Геометрическим типом функции f назовём класс эквивалентности относительно указанных преобразований. Для булевых функций от трёх переменных доказано, что только геометрический тип с представителем $f(x_1, x_2, x_3) = x_1x_3 \vee x_2\overline{x_3}$ не задаётся через АПФ.