

## О МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ \*)

*Д. П. Покрасенко*<sup>1</sup>

<sup>1</sup>Новосибирский гос. университет,  
ул. Пирогова, 2, 630090 Новосибирск, Россия  
e-mail: pokrasenko.d.p@gmail.com

**Аннотация.** Исследуется компонентная алгебраическая иммунность векторных булевых функций. Доказана теорема о соответствии между максимальной компонентной алгебраической иммунностью и сбалансированностью функции. Получена связь между максимальной компонентной алгебраической иммунностью и матрицами специального вида. При малом числе переменных построены функции, имеющие максимальную компонентную алгебраическую иммунность. Табл. 1, библиогр. 8.

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

### Введение

В 2003 г. в [4] был предложен новый метод криптоанализа шифров, названный алгебраическим криптоанализом. В случае поточных шифров данный криптоанализ использует следующие слабости фильтрующей функции: наличие у неё аннигиляторов низкой степени и множителей, уменьшающих степень функции. В настоящее время данный вид криптоанализа является одним из наиболее перспективных и развивающихся. Соответственно возникает вопрос о поиске функций, способных ему противостоять.

В 2004 г. в [8] введено понятие алгебраической иммунности  $AI(f)$  для булевых функций и установлено, что высокая алгебраическая иммунность позволяет противостоять алгебраическим атакам. Данное понятие различными способами обобщено на векторный случай. Так, в [1, 2] рассмотрена алгебраическая иммунность  $S$ -блоков и введены определения

---

\*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 15–31–20635).

базовой  $AI(F)$  и графической  $AI_{gr}(F)$  алгебраической иммунности векторных булевых функций. При этом было установлено, что базовая алгебраическая иммунность больше 1 только при  $m \leq n - \log_2(n+1)$ , поэтому данный параметр анализируется у  $S$ -блоков, которые используются в поточных шифрах. Графическая алгебраическая иммунность используется для изучения сопротивляемости алгебраическим атакам блочных шифров.

Одним из наиболее естественных и универсальных обобщений с криптографической точки зрения является компонентная алгебраическая иммунность  $AI_{comp}(F)$ , которая введена в [3]. Она может быть использована для анализа функций, применяемых как в поточных, так и в блочных шифрах, а также для помощи в изучении предыдущих двух понятий. Наличие высокой компонентной алгебраической иммунности способствует наилучшему противостоянию различным методам алгебраических атак.

Для булевых функций от  $n$  переменных известно [4], что алгебраическая иммунность всегда меньше или равна  $\lceil \frac{n}{2} \rceil$ , более того существуют функции, имеющие  $AI(f) = \lceil \frac{n}{2} \rceil$ . В случае компонентной алгебраической иммунности векторных булевых функций также справедлива оценка  $AI_{comp}(F) \leq \lceil \frac{n}{2} \rceil$ , но остаётся открытым вопрос о достижимости этой оценки и существовании функций, имеющих  $AI_{comp}(F) = \lceil \frac{n}{2} \rceil$ . Данная работа посвящена изучению этого вопроса. Было найдено соответствие между компонентной алгебраической иммунностью и сбалансированностью, в частности, показано, что для любого нечётного  $n$  векторная булева функция, действующая из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2^n$  и имеющая  $AI_{comp}(F) = \lceil \frac{n}{2} \rceil$ , является взаимно однозначной. Была получена связь между компонентной алгебраической иммунностью и матрицами специального вида, определено, что значение  $AI_{comp}(F) = \lceil \frac{n}{2} \rceil$  является достижимым при малых значениях  $n$  и  $m$ , и построены функции, имеющие максимальную компонентную алгебраическую иммунность.

## 1. Базовые определения

Пусть  $\mathbb{Z}_2 = \{0, 1\}$ , а  $\mathbb{Z}_2^n$  —  $n$ -мерный булев куб. Символ  $\oplus$  обозначает сложение по модулю два. *Весом Хэмминга*  $wt(x)$  двоичного вектора  $x$  называется количество единиц, содержащихся в  $x$ . *Расстоянием Хэмминга*  $d(x, y)$  между двумя векторами  $x$  и  $y$  длины  $n$  называется число координат, в которых они различаются.

*Булевой функцией* от  $n$  переменных называется функция, действующая из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2$ . Каждую булеву функцию можно единственным образом

представить в виде полинома

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

где индексы  $i_1, \dots, i_k$  различны,  $i_1 < i_2 < \dots < i_k$  и  $a_0, a_{i_1, \dots, i_k} \in \mathbb{Z}_2$ . Такое представление называется *алгебраической нормальной формой* (АНФ) функции  $f$ , или *полиномом Жегалкина*.

*Степенью*  $\deg(f)$  булевой функции  $f$  называется число переменных в самом длинном слагаемом её АНФ (степень тождественно нулевой функции равна минус бесконечности). Булева функция называется *сбалансированной* (*уравновешенной*), если она принимает значения 0 и 1 одинаково часто (её вес равен  $2^{n-1}$ ).

Функции  $f_1, \dots, f_n$  являются *линейно независимыми*, если выражение  $a_1 f_1 \oplus a_2 f_2 \oplus \dots \oplus a_n f_n$ , где  $a_1, a_2, \dots, a_n \in \mathbb{Z}_2$ , тождественно равно нулю только при условии  $a_1 = a_2 = \dots = a_n = 0$ . Соответственно функции  $f_1, \dots, f_n$  являются *линейно зависимыми*, если существуют такие коэффициенты  $a_1, a_2, \dots, a_n \in \mathbb{Z}_2$ , что  $a_1 f_1 \oplus a_2 f_2 \oplus \dots \oplus a_n f_n = 0$  и при этом  $a_1, a_2, \dots, a_n$  одновременно не обращаются в нуль.

*Векторной булевой функцией*  $F$  называется произвольное отображение  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ . Известно, что её всегда можно представить в виде  $F(x) = (f_1(x), \dots, f_m(x))$ , где  $f_i$  — булевы функции от  $n$  переменных, называемые *координатными функциями*. *Компонентной функцией* называется любая линейная комбинация координатных функций, т. е. булева функция  $bF = b_1 f_1 \oplus \dots \oplus b_m f_m$ , где  $b \in \mathbb{Z}_2^m$ . *Степенью*  $\deg(F)$  векторной булевой функции  $F$  называется максимальная из степеней её координатных функций. Функция  $F$  называется *сбалансированной*, если для любого  $b \in \mathbb{Z}_2^m$  верно  $|F^{-1}(b)| = 2^{n-m}$ , где  $F^{-1}(b)$  — прообраз векторной булевой функции  $F(x)$ , т. е. все  $a \in \mathbb{Z}_2^n$  такие, что  $F(a) = b$ .

## 2. Алгебраическая иммунность векторных булевых функций

*Алгебраической иммунностью*  $AI(f)$  булевой функции  $f$  называется минимальное число  $d$  такое, что существует булева функция  $g \not\equiv 0$  степени  $d$ , для которой  $fg = 0$  или  $(f \oplus 1)g = 0$ .

*Аннигилятором множества*  $E \subseteq \mathbb{Z}_2^n$  является любая булева функция от  $n$  переменных, которая равна нулю на этом множестве. *Алгебраическая иммунность*  $AI(E)$  множества  $E \subseteq \mathbb{Z}_2^n$  — минимальная степень ненулевых аннигиляторов множества  $E$ .

Пусть  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  — векторная булева функция. В [1–3] введены следующие понятия.

Базовая алгебраическая иммунность  $AI(F)$  векторной булевой функции — минимальная алгебраическая иммунность прообразов  $F^{-1}(z)$  для любого  $z \in \mathbb{Z}_2^m$ . Доказано, что  $AI(F)$  может быть больше 1 только при  $m \leq n - \log_2(n+1)$ . Поэтому данный параметр анализируется у  $S$ -блоков, которые используются в поточных шифрах.

Графическая алгебраическая иммунность  $AI_{\text{gr}}(F)$  векторной булевой функции — алгебраическая иммунность графика  $\{(x, F(x)) \mid x \in \mathbb{Z}_2^n\}$ .

Компонентной алгебраической иммунностью  $AI_{\text{comp}}(F)$  векторной булевой функции  $F$  называется минимальная алгебраическая иммунность компонентных функций  $bF$  ( $b \in \mathbb{Z}_2^m$ ,  $b \neq 0$ ), т. е.

$$AI_{\text{comp}}(F) = \min \{AI(bF) \mid b \in \mathbb{Z}_2^m, b \neq 0, bF = b_1 f_1 \oplus \dots \oplus b_m f_m\}.$$

В [1] получены оценки на графическую и базовую алгебраические иммунности:

$$AI(F) \leq AI_{\text{gr}}(F) \leq AI(F) + m, \quad AI(F) \leq d_{n,m}, \quad AI_{\text{gr}}(F) \leq D_{n,m},$$

где  $d_{n,m}$  и  $D_{n,m}$  — минимальные целые числа такие, что  $\sum_{i=0}^{d_{n,m}} \binom{n}{i} > 2^{n-m}$ ,

$$\sum_{i=0}^{D_{n,m}} \binom{n+m}{i} > 2^n.$$

В [6] доказано, что оценка  $AI(F) \leq d_{n,m}$  достижима. В [1] предложен метод построения векторных булевых функций с  $AI_{\text{gr}}(F) > d$ , также численно доказано, что оценка  $AI_{\text{gr}}(F) \leq D_{n,m}$  достижима при  $n \leq 14$ .

В [3] получены следующие оценки:

$$AI(F) \leq AI_{\text{comp}}(F), \quad AI_{\text{gr}}(F) \leq AI_{\text{comp}}(F) + 1, \\ AI_{\text{comp}}(F) \leq \min \{ \lceil n/2 \rceil, d_{\min}^0 F \},$$

где  $d_{\min}^0 F$  — минимальная степень компонентных функций  $bF$ .

При этом остаётся неизученным вопрос о существовании функций, имеющих  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$  для любого  $n$ .

### 3. Компонентная алгебраическая иммунность

Для начала приведём утверждения, которые понадобятся в дальнейшем.

**Утверждение 1** [4]. Для любой булевой функции  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  всегда верно, что  $AI(f) \leq \lceil n/2 \rceil$ .

При этом данная оценка достижима и существуют различные конструкции булевых функций, имеющих  $AI(f) = \lceil \frac{n}{2} \rceil$ .

**Утверждение 2** [5]. Пусть  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  — булева функция, у которой  $AI(f) > d$ . Тогда  $\sum_{i=0}^d \binom{n}{i} \leq wt(f) \leq \sum_{i=0}^{n-(d+1)} \binom{n}{i}$ .

Утверждение 2 устанавливает зависимость веса булевой функции от алгебраической иммунности. В дальнейшем будет использовано следствие из него.

**Утверждение 3** [5]. Если  $AI(f) = \lceil \frac{n}{2} \rceil$  и  $n$  нечётно, то  $f$  является сбалансированной.

Сбалансированность — важное криптографическое свойство булевых функций. Следующее утверждение упрощает проверку сбалансированности векторных булевых функций.

**Утверждение 4** [7]. Векторная булева функция  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  сбалансирована тогда и только тогда, когда все её компонентные функции  $bF$ ,  $b \in \mathbb{Z}_2^m$ ,  $b \neq 0$ , сбалансированы.

На первом этапе работы представлялось интересным определить свойства векторной булевой функции с максимальной компонентной алгебраической иммунностью.

**Теорема 1.** Векторная булева функция  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ , имеющая  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$ , для любого нечётного  $n$  сбалансирована. При  $n = m$  функция  $F$  взаимно однозначна.

**ДОКАЗАТЕЛЬСТВО.** С учётом утверждения 1  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$  тогда и только тогда, когда  $AI(bF) = \lceil \frac{n}{2} \rceil$  для любого  $b \in \mathbb{Z}_2^m$ ,  $b \neq 0$ .

По определению функция сбалансирована, если  $|\mathbb{F}^{-1}(b)| = 2^{n-m}$  для любого  $b \in \mathbb{Z}_2^m$ . Все компонентные функции  $bF$  имеют максимальную алгебраическую иммунность,  $n$  нечётно, тем самым из утверждения 3 следует, что они сбалансированы. Тогда из утверждения 4 следует, что векторная булева функций  $F$  также сбалансирована.

В случае  $n = m$  известно, что любая векторная булева функция, действующая из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2^n$ , взаимно однозначна тогда и только тогда, когда она сбалансирована. Теорема 1 доказана.

В случае чётного  $n$  утверждение 3 является, вообще говоря, неверным. Поэтому для чётного  $n$  из максимальной компонентной алгебраической иммунности векторной булевой функции не следует сбалансированность. В этом случае судить прямо о взаимной однозначности векторной

булевой функции затруднительно. Возникает задача поиска векторных булевых функций, обладающих максимальной компонентной иммунностью и взаимной однозначностью.

Для  $F : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^4$  найдены функции, обладающие максимальной компонентной алгебраической иммунностью и являющиеся взаимно однозначными, однако для общего случая вопрос существования таких функций остаётся открытым.

Для каждой векторной булевой функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  введём две матрицы  $M_F, M'_F$ , элементами которых являются булевы функции от  $n$  переменных. Занумеруем через  $a = (a_1, \dots, a_n) \in \mathbb{Z}_2^n$  мономы от  $n$  переменных, где  $a_i$  соответствует появлению в мономе переменной  $x_i$ , а  $a = (0, \dots, 0)$  — появлению 1. Например, вектор  $a = (1, 0, 1, 0, \dots, 0)$  соответствует моному  $x_1 x_3$ . Построим матрицы следующим способом. В матрице  $M_F$   $j$ -му столбцу соответствует умножение компонентной функции  $bF$ ,  $b \neq 0$ , на мономы степени меньше  $\lceil \frac{n}{2} \rceil$ . Нумерация столбцов идёт по вектору  $b \in \mathbb{Z}_2^m$ ,  $b \neq 0$ . Соответственно число столбцов равно  $2^m - 1$ . Строки занумерованы с помощью вектора  $a = (a_1, \dots, a_n)$ . Матрица  $M'_F$  строится аналогично, только вместо  $bF$  подставляется  $bF \oplus 1$ :

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

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

Следующая теорема связывает максимальную компонентную алгебраическую иммунность векторной булевой функции со структурой матриц  $M_F, M'_F$ .

**Теорема 2.** Векторная булева функция  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  имеет максимальную компонентную алгебраическую иммунность  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$  тогда и только тогда, когда в матрицах  $M_F$  и  $M'_F$  элементы любого столбца образуют линейно независимое множество.

**Доказательство.** НЕОБХОДИМОСТЬ. Пусть  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$ , значит, для любой компонентной функции выполняется  $AI(bF) = \lceil \frac{n}{2} \rceil$ , т. е.

при умножении  $bF$  и  $bF \oplus 1$  на любую функцию  $g$  такую, что  $\deg(g) < \lceil \frac{n}{2} \rceil$ , выполняется  $(bF)g \neq 0$  и  $(bF \oplus 1)g \neq 0$ .

Предположим, что элементы некоторого столбца образуют линейно зависимое множество. По определению это значит, что существуют коэффициенты  $a_0, a_1, a_2, \dots, a_{i_1, \dots, i_k} \in \mathbb{Z}_2$  такие, что  $a_0 bF \oplus a_1 bF x_1 \oplus a_2 bF x_2 \oplus \dots \oplus a_{i_1, \dots, i_k} bF x_{i_1, \dots, i_k} = 0$ , при этом все  $a_0, a_1, a_2, \dots, a_{i_1, \dots, i_k}$  не обращаются одновременно в нуль. Вынесем за скобку  $bF$  и получим, что выполняется соотношение  $bF(a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_{i_1, \dots, i_k} x_{i_1, \dots, i_k}) = 0$ . Обозначим выражение в скобке через  $g$ . Так как все мономы в  $g$  имеют степень меньше  $\lceil \frac{n}{2} \rceil$ ,  $\deg(g) < \lceil \frac{n}{2} \rceil$ . Значит, получили некоторую не тождественно равную нулю функцию  $g$  степени меньше  $\lceil \frac{n}{2} \rceil$ , при умножении на которую компонентной функции  $bF$  получаем 0. Это противоречит условию  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$ , следовательно, элементы любого столбца образуют линейно независимое множество. Аналогично для матрицы  $M'_F$ .

**ДОСТАТОЧНОСТЬ.** Пусть элементы любого столбца образуют линейно независимое множество. Тогда для любых  $a_0, a_1, a_2, \dots, a_{i_1, \dots, i_k} \in \mathbb{Z}_2$  из того, что  $a_0 bF \oplus a_1 bF x_1 \oplus a_2 bF x_2 \oplus \dots \oplus a_{i_1, \dots, i_k} bF x_{i_1, \dots, i_k} = 0$ , т. е.  $bF(a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_{i_1, \dots, i_k} x_{i_1, \dots, i_k}) = 0$ , следует, что все  $a_i = 0$ . Выражение, которое стоит в скобке, порождает все булевы функции от  $n$  переменных степени меньше чем  $\lceil \frac{n}{2} \rceil$ , тем самым при умножении компонентных функций на любую булеву функцию степени меньше чем  $\lceil \frac{n}{2} \rceil$  следует, что данная функция тождественно равна 0, аналогично из матрицы  $M'_F$  получается условие для  $(bF \oplus 1)$ . Стало быть, все компонентные булевы функции имеют иммунитет  $\lceil \frac{n}{2} \rceil$ , а значит,  $AI_{\text{comp}}(F) = \lceil \frac{n}{2} \rceil$ . Теорема 2 доказана.

Приведём пример, использующий теорему 2. Рассмотрим векторную булеву функцию  $F : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^2$ , имеющую вид  $F = (x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus 1, x_1 x_2 \oplus x_1 \oplus x_3 \oplus 1)$ . Тогда матрица  $M_F$  имеет вид

$$\begin{pmatrix} x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus 1 & x_1 x_2 \oplus x_1 \oplus x_3 \oplus 1 & x_1 x_3 \oplus x_2 x_3 \oplus x_1 \oplus x_3 \\ x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_1 & x_1 x_2 \oplus x_1 x_3 & x_1 x_2 x_3 \oplus x_1 \\ x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_2 & x_2 x_3 \oplus x_2 & x_1 x_2 x_3 \oplus x_1 x_2 \\ x_1 x_2 x_3 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_3 & x_1 x_2 x_3 \oplus x_1 x_3 & x_2 x_3 \oplus x_3 \end{pmatrix}.$$

Рассмотрим первый столбец и определим, является ли линейно независимым множество, составленное из его элементов.

$x$	$f_1$	$f_1 x_1$	$f_1 x_2$	$f_1 x_3$
000	1	0	0	0

011	0	0	0	0
001	1	0	0	1
010	1	0	1	0
100	1	1	0	0
101	0	0	0	0
110	0	0	0	0
111	0	0	0	0

Выписав только ненулевые строки, получим

1	0	0	0
1	0	0	1
1	0	1	0
1	1	0	0

Очевидно, что столбцы данной матрицы независимы. Аналогично для 2-го и 3-го столбцов матрицы  $M_F$  имеем

1	0	0	0
1	0	1	0
1	1	0	1
1	1	0	0

и

1	0	0	1
1	1	0	0
1	1	0	1
1	1	1	0

Очевидно, что столбцы матриц линейно независимы. Для матрицы  $M'_F$ , аналогично удалив нулевые строки, получим

1	0	1	1
1	1	0	1
1	1	0	0
1	1	1	1

,

1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

,

1	0	0	0
1	0	1	0
1	0	1	1
1	1	1	1

У всех трёх матриц столбцы линейно независимы. Тем самым для матриц  $M_F$  и  $M'_F$  выполняется условие теоремы 2. Таким образом, представленная функция имеет  $AI_{\text{comp}} = \lceil \frac{n}{2} \rceil$ .

#### 4. Примеры для малых размерностей

Для малого числа переменных программно установлено, что существуют векторные булевы функции, которые имеют  $AI_{\text{comp}} = \lceil \frac{n}{2} \rceil$ . Далее приведены примеры таких функций при различных значениях  $n, m$ .

Для  $F = (f_1, f_2) : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$

$$f_1 = x_1 \oplus x_2,$$

$$f_2 = x_1x_2.$$

Для  $F = (f_1, f_2) : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^2$

$$f_1 = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1,$$

$$f_2 = x_1x_2 \oplus x_1 \oplus x_3 \oplus 1.$$

Для  $F = (f_1, f_2, f_3) : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^3$

$$f_1 = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1,$$

$$f_2 = x_3x_2 \oplus x_1 \oplus x_3 \oplus 1,$$

$$f_3 = x_3x_2 \oplus x_1x_3 \oplus x_3 \oplus x_2.$$

Для  $F = (f_1, f_2) : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^2$

$$f_1 = x_1x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus 1,$$

$$f_2 = x_1x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus x_4 \oplus 1.$$

Для  $F = (f_1, f_2, f_3) : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^3$

$$f_1 = x_1x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus 1,$$

$$f_2 = x_1x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus x_4 \oplus 1,$$

$$f_3 = x_1x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1 \oplus x_2.$$

Для  $F = (f_1, f_2, f_3, f_4) : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^4$

$$f_1 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4 \oplus 1,$$

$$f_2 = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_4 \oplus 1,$$

$$f_3 = x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1 \oplus x_3 \oplus x_4 \oplus 1,$$

$$f_4 = x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_4 \oplus x_1 \oplus x_2.$$

Также было подсчитано число таких функций. В табл. 1 приведено количество векторных булевых функций с максимальной компонентной алгебраической иммунностью, общее количество векторных булевых функций, действующих из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2^m$ , и доля функций с  $AI_{\text{comp}} = \lceil \frac{n}{2} \rceil$  от общего числа векторных булевых функций.

Т а б л и ц а 1

Количество функций, имеющих  $AI_{\text{comp}} = \lceil \frac{n}{2} \rceil$

$(n, m)$	Функции с $AI_{\text{comp}} = \lceil \frac{n}{2} \rceil$	Все функции из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2^m$	Доля функций с $AI_{\text{comp}} = \lceil \frac{n}{2} \rceil$
(2,2)	168	256	0.65625
(3,2)	1344	65536	0.02051
(3,3)	10752	16777216	0.00064
(4,2)	$\approx 10^8$	4294967296	$\approx 0.02$

Выражаю благодарность научному руководителю Н. Н. Токаревой и Е. В. Горкунову за полезные советы.

## ЛИТЕРАТУРА

1. **Armknecht F., Krause M.** Constructing single- and multi-output Boolean functions with maximal algebraic immunity // Automata, Languages and Programming (Proc. 33rd Int. Colloq. ALP, Venice, Italy, July 10–14, 2006). Pt. II. Berlin; Heidelberg: Springer-Verl., 2006. P. 180–191. (Lect. Notes Comput. Sci.; Vol. 4052).
2. **Ars G., Faugère J.-C.** Algebraic immunities of functions over finite fields // Boolean Functions: Cryptography and Applications (Proc. 1st Workshop BFCA, Mont-Saint-Aignan, France, March 7–8, 2005). Mont-Saint-Aignan: Publ. Univ. Rouen Havre, 2005. P. 21–38.
3. **Carlet C.** On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing cryptographic primitives with techniques from error correcting codes. (Proc. NATO Adv. Res. Workshop ACPTECC, Veliko Tarnovo, Bulgaria, Oct. 6–9, 2008). Amsterdam: IOS Press, 2009. P. 104–116.
4. **Courtois N. T., Meier W.** Algebraic attacks on stream ciphers with linear feedback // Advances in Cryptology — EUROCRYPT 2003 (Proc. Int. Conf. Theory Appl. Cryptogr. Tech., Warsaw, Poland, May 4–8, 2003). Heidelberg: Springer-Verl, 2003. P. 345–359. (Lect. Notes Comput. Sci.; Vol. 2656).
5. **Dalai D. K., Gupta K. C., Maitra S.** Results on algebraic immunity for cryptographically significant Boolean functions // Progress in Cryptology — INDOCRYPT 2004 (Proc. 5th Int. Conf. Cryptol. India, Chennai, India, Dec. 20–22, 2004). Heidelberg: Springer-Verl, 2005. P. 92–106. (Lect. Notes Comput. Sci.; Vol. 3348).
6. **Feng K., Liao Q., Yang J.** Maximal values of generalized algebraic immunity // Des. Codes Cryptogr. 2009. Vol. 50, No. 2. P. 243–252.
7. **Lidl R., Niederreiter H.** Finite fields. Reading, MA: Addison-Wesley, 1983. 755 p.
8. **Meier W., Pasalic E., Carlet C.** Algebraic attacks and decomposition of Boolean functions // Advances in Cryptology — EUROCRYPT 2004 (Proc. Int. Conf. Theory Appl. Cryptogr. Tech., Interlaken, Switzerland, May 2–6, 2004). Berlin: Springer-Verl., 2005. P. 474–491. (Lect. Notes Comput. Sci.; Vol. 3027).

Покрасенко Денис Павлович

Статья поступила

29 мая 2015 г.

Исправленный вариант —

8 декабря 2015 г.

UDC 519.7

DOI: 10.17377/daio.2016.23.495

ON THE MAXIMAL COMPONENT ALGEBRAIC IMMUNITY  
OF VECTORIAL BOOLEAN FUNCTIONSD. P. Pokrasenko<sup>1</sup><sup>1</sup>Novosibirsk State University,

2 Pirogov St., 630090 Novosibirsk, Russia

e-mail: pokrasenko.d.p@gmail.com

**Abstract.** The component algebraic immunity of vectorial Boolean functions is studied. We prove a theorem on the correspondence between the maximum component algebraic immunity of a function and its balancedness. Some relationship between the maximal component algebraic immunity and matrices of a special form is obtained. We construct several functions with maximal component algebraic immunity in case of few variables. Tab. 1, bibliogr. 8.

**Keywords:** component algebraic immunity, vectorial Boolean function, balancedness.

## REFERENCES

1. **F. Armknecht** and **M. Krause**, Constructing single- and multi-output Boolean functions with maximal algebraic immunity, in *Automata, Languages and Programming* (Proc. 33rd Int. Colloq. ALP, Venice, Italy, July 10–14, 2006), Pt. II, pp. 180–191, Springer, Heidelberg, 2006 (Lect. Notes Comput. Sci., Vol. 4052).
2. **G. Ars** and **J.-C. Faugère**, Algebraic immunities of functions over finite fields, in *Boolean Functions: Cryptography and Applications* (Proc. 1st Workshop BFCA, Mont Saint-Aignan, France, Mar. 7–8, 2005), pp. 21–38, Publ. Univ. Rouen Havre, Mont Saint-Aignan, 2005.
3. **C. Carlet**, On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions, in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes* (Proc. NATO Adv. Res. Workshop ACPTECC, Veliko Tarnovo, Bulgaria, Oct. 6–9, 2008), pp. 104–116, IOS Press, Amsterdam, 2009.
4. **N. T. Courtois** and **W. Meier**, Algebraic attacks on stream ciphers with linear feedback, in E. Biham, ed., *Advances in Cryptology — EUROCRYPT 2003* (Proc. Int. Conf. Theory Appl. Cryptogr. Tech., Warsaw, Poland, May 4–8, 2003), pp. 345–359, Springer, Heidelberg, 2003 (Lect. Notes Comput. Sci., Vol. 2656).

5. **D. K. Dalai, K. C. Gupta, and S. Maitra**, Results on algebraic immunity for cryptographically significant Boolean functions, in A. Canteaut and K. Viswanathan, eds., *Progress in Cryptology — INDOCRYPT 2004* (Proc. 5th Int. Conf. Cryptol. India, Chennai, India, Dec. 20–22, 2004), pp. 92–106, Springer, Heidelberg, 2005 (Lect. Notes Comput. Sci., Vol. 3348).
6. **K. Feng, Q. Liao and J. Yang**, Maximal values of generalized algebraic immunity, *Des. Codes Cryptogr.*, **50**, No. 2, 243–252, 2009.
7. **R. Lidl and H. Niederreiter**, *Finite Fields*, Addison-Wesley, Reading, MA, USA, 1983.
8. **W. Meier, E. Pasalic, and C. Carlet**, Algebraic attacks and decomposition of Boolean functions, in C. Cachin and J. L. Camenisch, eds., *Advances in Cryptology — EUROCRYPT 2004* (Proc. Int. Conf. Theory Appl. Cryptogr. Tech., Interlaken, Switzerland, May 2–6, 2004), pp. 474–491, Springer, Berlin, 2005 (Lect. Notes Comput. Sci., Vol. 3027).

Denis P. Pokrasenko

Received

29 May 2015

Revised

8 December 2015