ЛИТЕРАТУРА

1. *Агибалов Г. П.* SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43–48.

УДК 519.7 DOI 10.17223/2226308X/8/15

ОБ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

Д. П. Покрасенко

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.

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

В 2003 г. N. Courtois и W. Meier предложили алгебраический метод криптоанализа шифров [1]. В случае поточных шифров этот метод 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. W. Meier, E. Pasalic и C. Carlet в работе [2] ввели понятие алгебраической иммунности для булевых функций. *Алгебраической иммунностью* $\mathrm{AI}(f)$ булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется такое минимальное число d, что существует булева функций g степени d, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$. Для любой булевой функции выполняется $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$ и существуют функции, имеющие $\mathrm{AI}(f) = \lceil n/2 \rceil$. Высокая алгебраическая иммунность позволяет противостоять алгебраическим атакам.

Понятие алгебраической иммунности различными способами было обобщено на векторный случай. Так, в работе [3] F. Armknecht и M. Krause, а также G. Ars и J.-C. Faugère в [4] рассмотрели алгебраическую иммунность S-блоков и ввели понятия базовой $\mathrm{AI}(F)$ и графической $\mathrm{AI}_{\mathrm{gr}}(F)$ алгебраической иммунности векторных булевых функций. При этом базовая алгебраическая иммунность больше 1 только при малых значениях m, поэтому данный параметр анализируется у S-блоков, которые используются в поточных шифрах. Графическая алгебраическая иммунность используется для изучения сопротивляемости алгебраическим атакам блочных шифров.

Следующее обобщение является одним из наиболее естественных с криптографической точки зрения. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $b \cdot F$ ($b \in \mathbb{F}_2^m, b \neq 0$), т. е. $\mathrm{AI}_{\mathrm{comp}}(F) = \min\{\mathrm{AI}(b \cdot F) : b \in \mathbb{F}_2^m, b \neq 0\}$, где $b \cdot F = b_1 f_1 \oplus \ldots \oplus b_m f_m$. Данное определение является наиболее универсальным, наличие высокой компонентной алгебраической иммунности S-блоков

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

способствует противостоянию алгебраическому криптоанализу поточных и блочных шифров.

В [5] получена оценка $\mathrm{AI}_{\mathrm{comp}} \leqslant \min\{\lceil n/2 \rceil, d^o_{\min} F\}$, где $d^o_{\min} F$ — минимальная степень компонентных функций $b \cdot F$. При этом остаётся не изученным вопрос о существовании функций, имеющих $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$.

В работе получены следующие результаты.

Теорема 1. Для любого нечётного n векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, имеющая $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$, является сбалансированной. В случае $n = m$ функция F взаимно однозначна.

Занумеруем через $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ мономы от n переменных, где a_i соответствует появлению в мономе переменной x_i, а $a = (0, \ldots, 0)$ соответствует 1. Например, вектор $a = (1, 0, 1, 0, \ldots, 0)$ соответствует моному $x_1 x_3$. Для каждой векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ 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 мономы степени меньше $\lceil n/2 \rceil$. Нумерация столбцов идёт по вектору $b \in \mathbb{F}_2^m$, $b \neq 0$. Соответственно число столбцов $2^m - 1$. Строки занумерованы с помощью вектора $a = (a_1, \ldots, a_n)$. Матрица M'_F строится аналогично, только вместо $b \cdot F$ подставляется $b \cdot F \oplus 1$:

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

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

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

Теорема 2. Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ 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.

Для малого числа переменных найдены векторные булевы функции, которые имеют $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$, подсчитано число таких функций. В таблице приведено количество векторных булевых функций с максимальной компонентной алгебраической иммунностью, общее количество векторных булевых функций, действующих из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, и доля функций с $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$ от общего числа векторных булевых функций.

(n,m)	Функции с $\mathrm{AI}_{\mathrm{comp}}(F)=\lceil n/2\rceil$	Все функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$	Доля функций
(2,2)	168	256	0,65625
(3,2)	1344	65536	0,02051
(3,3)	10752	16777216	0,00064
(4,2)	$\approx 10^8$	4294967296	$\approx 0{,}02$

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt'2003. LNCS. 2003. V. 2656. P. 345–359.
2. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt'2004. LNCS. 2004. V. 3027. P. 474–491.
3. *Armknecht F. and Krause M.* Constructing single- and multi-output Boolean functions with maximal immunity // ICALP'2006. LNCS. 2006. V. 4052. P. 180–191.
4. *Ars G. and Faugère J.-C.* Algebraic immunities of functions over finite fields // Proc. Conf. BFCA. 2005. P. 21–38.
5. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009. P. 104–116.

УДК 519.7 DOI 10.17223/2226308X/8/16

СВОЙСТВА p-ИЧНЫХ БЕНТ-ФУНКЦИЙ, НАХОДЯЩИХСЯ НА МИНИМАЛЬНОМ РАССТОЯНИИ ДРУГ ОТ ДРУГА[1]

В. Н. Потапов

Доказано, что минимальное расстояние Хэмминга между двумя p-ичными бент-функциями от $2n$ переменных равно p^n в случае, когда число p простое. Число p-ичных бент-функций на минимальном расстоянии от квадратичной бент-функции равно $p^n(p^{n-1}+1)\cdots(p+1)(p-1)$ при $p>2$.

Ключевые слова: *бент-функция, расстояние Хэмминга, квадратичная форма.*

Введение

Рассмотрим конечную абелеву группу G и векторное пространство $V(G)$, состоящее из функций $f: G \to \mathbb{C}$, со скалярным произведением

$$(f,g)=\sum_{x\in G} f(x)\overline{g(x)}.$$

Характерами называются гомоморфизмы группы G в мультипликативную группу поля $\mathbb{C}$, т. е. такие $\phi \in V(G)$, что $\phi(x+y)=\phi(x)\phi(y)$, для любых $x,y\in G$. Характеры абелевой группы G образуют ортогональный базис в $V(G)$. Если $G=\mathbb{Z}_q^n$, то для любого $z\in\mathbb{Z}_q^n$ характер группы G определяется равенством $\phi_z(x)=\xi^{\langle x,z\rangle}$, где $\xi=e^{2\pi i/q}$ и $\langle x,y\rangle = x_1y_1+\ldots+x_ny_n \bmod q$. Характерами прямой суммы двух групп являются всевозможные попарные произведения характеров первой и второй группы. Поскольку любая конечная абелева группа представляется в виде прямой суммы циклических групп, характеры произвольной конечной абелевой группы являются произведениями функций определённого выше вида.

Преобразованием Фурье функции из $V(G)$ называется вектор коэффициентов в разложении по базису характеров. Нам будет удобнее определить преобразование Фурье

[1]Работа поддержана грантом РФФИ № 13-01-00463.