Теорема 1. Булева бент-функция f от чётного числа переменных n является самодуальной (анти-самодуальной) тогда и только тогда, когда при каждом фиксированном $y \in \mathbb{F}_2^n$ для булевой функции $F_y(x) = f(x) \oplus f(y) \oplus x \cdot y$ справедливо $\mathrm{wt}(F_y) = 2^{n-1} - 2^{n/2-1}$ (соответственно $2^{n-1} + 2^{n/2-1}$).

ЛИТЕРАТУРА

1. *Carlet C., Danielson L. E., Parker M. G., Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
2. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. Iss. 2. P. 183–198.

УДК 519.7 DOI 10.17223/2226308X/8/14

ОБ ОБРАТИМОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

И. А. Панкратова

Рассматривается класс $\mathcal{F}_{n,m,k}$ обратимых векторных булевых функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, координатные функции которых существенно зависят от заданного числа k переменных. Доказано: 1) таких функций не существует при любом $n = m$ и $k = 2$; 2) функции класса $\mathcal{F}_{n,n,n-1}$ могут (не могут) быть построены из аффинных координатных функций при чётном (нечётном) n; 3) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то и $\mathcal{F}_{n+1,m+1,k} \neq \varnothing$.

Ключевые слова: *векторная булева функция, обратимые функции.*

Задача построения обратимых векторных булевых функций возникает при создании многих криптосистем; в частности, такие функции используются в многораундовых симметричных блочных шифрах класса SIBCipher [1]. Для того чтобы значения функции можно было эффективно вычислять, часто вводится ограничение на количество существенных переменных у каждой координатной функции векторной функции.

Для $n, m, k \in \mathbb{Z}$ обозначим через $\mathcal{F}_{n,m,k}$ класс функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, где $F = (f_1 \dots f_m)$, таких, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, m$, существенно зависят ровно от k переменных и функция F — инъекция (т. е. обратима).

В случае $n = m$ (практически важном для построения многораундовых шифров) будем обозначать $\mathcal{F}_{n,k} = \mathcal{F}_{n,n,k}$.

Непосредственно проверяются следующие свойства:

1) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $m \geqslant n$;
2) если $F \in \mathcal{F}_{n,k}$, то F есть подстановка на $\mathbb{F}_2^n$ и все её координатные функции уравновешены;
3) если $F = (f_1 \dots f_m) \in \mathcal{F}_{n,m,k}$, то и $F' = (f_1 \dots \bar{f}_i \dots f_m) \in \mathcal{F}_{n,m,k}$, $i \in \{1, \dots, m\}$;
4) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $\mathcal{F}_{n,t,k} \neq \varnothing$ для любого $t > m$;
5) если $\mathcal{F}_{k,k} \neq \varnothing$, то $\mathcal{F}_{ks,k} \neq \varnothing$ для любого $s > 1$.

Последнее свойство используется при построении шифров SIBCiphers семейства Люцифер [1]: ks переменных разбиваются на блоки по k переменных в каждом и «большая» раундовая функция набирается из s «маленьких» функций — подстановок на $\mathbb{F}_2^k$.

Пример 1. Функция $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ с вектором значений (0 6 7 2 4 3 1 5) принадлежит множеству $\mathcal{F}_{3,3}$; её координатные функции $f_1 = x_1 \oplus x_2 \oplus x_3$, $f_2 = x_1x_2 \oplus x_2x_3 \oplus x_2 \oplus x_3$, $f_3 = x_1x_3 \oplus x_2x_3 \oplus x_2$.

Утверждение 1. $\mathcal{F}_{n,2} = \varnothing$ для любого $n \geqslant 2$.

Доказательство. Предположим, $F \in \mathcal{F}_{n,2}$. Тогда по свойству 2 все её координатные функции уравновешены, т. е. имеют вид $x_i \oplus x_j \oplus c$ для некоторых $1 \leqslant i < j \leqslant n$, $c \in \mathbb{F}_2$. Но в этом случае $F(x) = F(\bar{x})$ для любого $x \in \mathbb{F}_2^n$, что невозможно для инъективной функции. ■

Заметим, что при $m > n$ уравновешенность координатных функций уже не обязательна и класс $\mathcal{F}_{n,m,2}$ может быть не пуст.

Пример 2. Функция $F : \mathbb{F}_2^2 \to \mathbb{F}_2^3$ с вектором значений (0 5 4 2) принадлежит классу $\mathcal{F}_{2,3,2}$; её координатные функции $f_1 = x_1 \oplus x_2$, $f_2 = x_1 x_2$, $f_3 = x_1 x_2 \oplus x_2$.

Утверждение 2.

1) Если n чётное, то некоторая $F \in \mathcal{F}_{n,n-1}$ может быть построена из аффинных координатных функций.
2) Если n нечётное, то никакая $F \in \mathcal{F}_{n,n-1}$ не может быть построена из аффинных координатных функций.

Доказательство. Пусть $F(x_1, \ldots, x_n) = (f_1 \ldots f_n)$, $f_i = \bigoplus\limits_{j \neq i} x_j \oplus c_i$, $c_i \in \mathbb{F}_2$, $i = 1, \ldots, n$; $a = (a_1 \ldots a_n) \in \mathbb{F}_2^n$ — произвольное значение. Ввиду свойства 3 без ограничения общности можно полагать, что все c_i равны нулю. Составим уравнение $F(x) = a$, или в матричном виде $Ax = a$, где x и a — вектор-столбцы, A — $(n \times n)$-матрица:

$$A = \begin{pmatrix} 0 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & 1 & \ldots & 1 & 1 \\ 1 & 1 & 0 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & 0 & 1 \\ 1 & 1 & 1 & \ldots & 1 & 0 \end{pmatrix}.$$

Легко убедиться, что $\det A = (n-1) \bmod 2$ над полем $\mathbb{F}_2$, поэтому уравнение $F(x) = a$ имеет решения для всех a (что равносильно условию $F \in \mathcal{F}_{n,n-1}$), если и только если n чётно.

Для завершения доказательства п. 2 утверждения осталось заметить, что перестановка координатных функций не влияет на принадлежность функции F классу $\mathcal{F}_{n,n-1}$; других способов выбора n различных аффинных функций, существенно зависящих от $(n-1)$ переменных каждая и от всех n переменных в совокупности (что, очевидно, необходимо для принадлежности функции F классу $\mathcal{F}_{n,n-1}$), нет. ■

Следствие 1. $\mathcal{F}_{n,n-1} \neq \varnothing$ для любого чётного n.

Утверждение 3. Если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $\mathcal{F}_{n+1,m+1,k} \neq \varnothing$.

Доказательство. Пусть $F(x_1, \ldots, x_n) = (f_1 \ldots f_m) \in \mathcal{F}_{n,m,k}$. Построим функцию $G : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{m+1}$ так: $G(x_1, \ldots, x_n, x_{n+1}) = (f_1 \ldots f_m\, g)$, где $g(x_1, \ldots, x_n, x_{n+1}) = x_{n+1} \oplus \oplus\, h(x_1, \ldots, x_n)$, h — любая функция, существенно зависящая от $(k-1)$ переменных. Тогда $G(a_1, \ldots, a_n, 0) \neq G(a_1, \ldots, a_n, 1)$ для любого $a_1 \ldots a_n \in \mathbb{F}_2^n$ ввиду линейности функции g по переменной x_{n+1}; $G(a_1, \ldots, a_n, c) \neq G(b_1, \ldots, b_n, c)$ для любых $a_1 \ldots a_n \neq \neq b_1 \ldots b_n$, $c \in \mathbb{F}_2$ ввиду обратимости функции F. ■

Из утверждения 3, свойства 4 и примеров 1 и 2 следует, что $\mathcal{F}_{n,m,3} \neq \varnothing$ для всех $m \geqslant n \geqslant 3$ и $\mathcal{F}_{n,m,2} \neq \varnothing$ для всех $m > n \geqslant 2$.

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.