УДК 519.7 DOI 10.17223/2226308X/11/14

КОНСТРУКЦИИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ[1]

А. В. Милосердов

Исследуется компонентная алгебраическая иммунность векторных булевых функций. Рассмотрен метод построения векторных булевых функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ с максимальной компонентной алгебраической иммунностью из булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ с максимальной алгебраической иммунностью в следующем виде: $F(x) = (f(x), f(Ax), \ldots, f(A^{m-1}x))$, где A — невырожденная булева матрица порядка n. Найдены функции с максимальной компонентной алгебраической иммунностью от 3 и 4 переменных. Доказано, что не существует функций $F : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ с максимальной компонентной алгебраической иммунностью, построенных по данному методу.

Ключевые слова: *векторные булевы функции, алгебраическая иммунность, компонентная алгебраическая иммунность.*

Многие шифры могут быть заданы в виде системы булевых уравнений. В 2003 г. предложен метод криптоанализа шифров, названный алгебраическим криптоанализом [1]. Основная его идея заключается в понижении степени системы уравнений и, следовательно, упрощении всей задачи. Данный вид криптоанализа является одним из наиболее перспективных и развивающихся в настоящее время. Соответственно возникает вопрос о возможности построения функций, способных ему противостоять.

Алгебраической иммунностью $\mathrm{AI}(f)$ функции f называется минимальное число d, такое, что существует булева функция g степени d, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ функции F называется минимальная алгебраическая иммунность компонентных функций $F \cdot b = b_1 f_1 \oplus \ldots \oplus b_m f_m$, где $b \in \mathbb{F}_2^m$, $b \neq 0$.

На олимпиаде NSUCRYPTO 2016 предлагалась открытая задача по построению векторных булевых функций с максимальной компонентной алгебраической иммунностью. Участником олимпиады Алексеем Удовенко предложено искать векторную булеву функцию $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ с максимальной компонентной алгебраической иммунностью в виде $F(x) = (f(x), f(Ax), \ldots, f(A^{m-1}x))$, где $f : \mathbb{F}_2^n \to \mathbb{F}_2$ — некоторая булева функция с максимальной алгебраической иммунностью; A — невырожденная булева матрица $n \times n$. Алексеем Удовенко найдены функции с максимальной компонентной алгебраической иммунностью, где в качестве линейного преобразования A выбрана функция циклического сдвига координат на одну позицию влево. Его идеи описаны в [2], где приводятся решения всех задач олимпиады.

В качестве функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ выберем наиболее простую и известную функцию с максимальной алгебраической иммунностью — функцию Dalai [3]. Это функция вида

$$f(x) = \begin{cases} 0, & \mathrm{wt}(x) < n/2, \\ 1, & \mathrm{wt}(x) > n/2, \\ *, & \mathrm{wt}(x) = n/2, \end{cases}$$

где $\mathrm{wt}(x)$ — вес вектора x.

[1]Работа поддержана грантами РФФИ, проекты № 17-41-543364 и 18-31-00374.

Теорема 1. Существуют матрицы A, такие, что функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ вида

$$F(x) = (f(x), f(Ax), \ldots, f(A^{n-1}x)),$$

где f — функция Dalai от $n = 3, 4$ переменных, имеет максимальную компонентную алгебраическую иммунность $\lceil n/2 \rceil$.

Теорема 2. Не существует функций $F : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ вида

$$F(x) = (f(x), f(Ax), f(A^2x), f(A^3x), f(A^4x)),$$

где f — функция Dalai от 5 переменных, с максимальной компонентной алгебраической иммунностью 3.

Теорема 3. Пусть f — булева функция с максимальной алгебраической иммунностью от нечётного числа переменных n, A — невырожденная матрица $n \times n$. Тогда функция $g(x) = f(x) + f(Ax)$ обладает максимальной алгебраической иммунностью только в том случае, если под действием линейного преобразования A ровно половина элементов множества $\mathrm{supp}(f)$ остаётся в этом множестве, где $\mathrm{supp}(f)$ — носитель функции f.

Теорема 4. Пусть функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ имеет вид

$$F(x) = (f(x), f(Ax), \ldots, f(A^{n-1}x)),$$

где f — булева функция от n переменных с максимальной алгебраической иммунностью; n — нечётное число. Если функция F имеет максимальную компонентную алгебраическую иммунность, то матрицы $A, \ldots, A^{n-1}$ должны удовлетворять условию теоремы 3.

Продолжаются исследования существования векторных булевых функций с максимальной компонентной алгебраической иммунностью при $n \geqslant 6$.

ЛИТЕРАТУРА

1. *Courtois N. T. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Dalai D. K., Maitra S., and Sarkar S.* Basic theory in construction of Boolean functions with maximum possible annihilator immunity // Designs, Codes and Cryptography. 2006. V. 40. P. 41–58.