2. *Millan W., Clark A., and Dawson E.* An effective genetic algorithm for finding highly nonlinear Boolean functions // LNCS. 1997. V. 1334. P. 149–158.
3. *Clark J., Jacob J., Stepney S., et al.* Evolving Boolean functions satisfying multiple criteria // LNCS. 2002. V. 2551. P. 246–259.
4. *Picek S., Jakobovic D., Miller J., et al.* Cryptographic Boolean functions: one output, many design criteria // Appl. Soft Computing. 2016. No. 40. P. 635–653.
5. *Behera P. and Gangopadhyay S.* An improved hybrid genetic algorithm to construct balanced Boolean function with optimal cryptographic properties // Evolutionary Intelligence. 2021. No. 1. P. 1–15.
6. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386–397.
7. *Лобанов М. С.* Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций. 2008. Т. 15. №6. С. 34–47.

УДК 519.7 DOI 10.17223/2226308X/14/5

S-БЛОКИ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ ОТ МАЛОГО ЧИСЛА ПЕРЕМЕННЫХ[1]

Д. А. Зюбина, Н. Н. Токарева

Пусть π — перестановка n элементов, f — булева функция от n переменных. Рассмотрим векторную булеву функцию $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ вида $F_\pi(x) = (f(x), f(\pi(x)), \cdots, f(\pi^{n-1}(x)))$. Изучается компонентная алгебраическая иммунность функции F_π в зависимости от булевой функции f и перестановки π при $n = 3, 4, 5$. Получены полные множества булевых и частичные векторных булевых функций с максимальной алгебраической иммунностью от малого числа переменных.

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

S-блоки играют решающую роль в обеспечении стойкости блочных шифров к различным типам атак. Основная причина этого в том, что в классических и современных блочных шифрах нелинейный слой представлен именно данными блоками. S-блок является отображением множества двоичных векторов длины n в множество двоичных векторов длины m. В 2003 г. в [1] был представлен новый вид криптоанализа — алгебраический, основанный на понижении степени системы уравнений, описывающей шифр. Для противостояния такому роду атак необходимо, чтобы S-блок имел максимально возможное значение компонентной алгебраической иммунности.

Будем рассматривать S-блоки определённого вида, а именно $F_\pi(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$, где $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$; f — булева функция от n переменных; π — циклический сдвиг влево на один. Эта конструкция предложена А. Удовенко в решении олимпиадной задачи на NSUCRYPTO-2016 [2]. Он показал, что при таком построении векторной функции можно получить функцию с максимальной алгебраической иммунностью от 3, 4, ..., 10 переменных. В настоящее время остаётся открытым вопрос о существовании векторной булевой функции с максимальной компонентной иммунностью $\lceil n/2 \rceil$ от произвольного числа переменных n.

Алгебраической иммунностью $\mathrm{AI}(f)$ булевой функции f называется минимальное число d, такое, что существует булева функция g степени d, не тождественно равная ну-

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект №FWNF-2022-0018) при поддержке лаборатории криптографии JetBrains Research.

лю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$ [3]. Известно, что для произвольной булевой функции f от n переменных выполнено $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции F называется минимальная алгебраическая иммунность её компонентных функций, т. е. функций $f_b(x) = \langle b, F(x) \rangle$, где $b \in \mathbb{F}_2^n$, $b \neq 0$ и $\langle a, b \rangle = a_1 b_1 \oplus \ldots \oplus a_n b_n$ — скалярное произведение векторов по модулю 2.

В данной работе для построения S-блока с максимальной компонентной алгебраической иммунностью реализован метод нахождения линейного подпространства размерности n в множестве, содержащем векторы значений нулевой функции и всех булевых функций от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. В первую очередь путём полного перебора формируется множество булевых функций с максимальной алгебраической иммунностью. К этому множеству добавляется нулевой вектор. Далее из этого множества выбирается функция и на её основе строятся оставшиеся $n - 1$ функций (применением перестановки π к аргументам); все такие функции также лежат в этом множестве. Затем проверяется, порождают ли все n функций линейное подпространство размерности n. Если да, то данное подпространство позволяет построить S-блок с максимальной компонентной иммунностью, выбрав в качестве координатных функций S-блока базис подпространства. Для однозначности пусть функция строится в виде $F_\pi(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$.

Для $n = 3$ путём полного перебора получено, что существует 56 булевых функций с максимальной алгебраической иммунностью 2. Из них на основе 12 функций (им отвечают четыре подпространства) можно построить векторную булеву функцию с максимальным значением иммунности. Все эти функции можно представить в виде АНФ общего вида.

Утверждение 1. Булевы функции f от трёх переменных с максимальной алгебраической иммунностью 2, такие, что векторные функции вида $F_\pi(x) = (f(x), f(\pi(x)), f(\pi^2(x)))$, где π — циклический сдвиг, также имеют максимальную компонентную алгебраическую иммунность 2, можно описать следующей конструкцией:

$$f(x_1, x_2, x_3) = x_i + x_j + x_i x_k + a, \quad \text{где} \quad \{i, j, k\} = \{1, 2, 3\}, \ a \in \mathbb{F}_2.$$

Для $n = 4$ путём полного перебора получено, что существует 54 952 булевых функций с максимальной алгебраической иммунностью 2. При рассмотрении всевозможных перестановок π (а не только циклического сдвига влево, как это происходило ранее) оказалось, что только при шести перестановках существуют векторные булевы функции, которые сохраняют максимальную иммунность. Эти перестановки можно представить в векторном виде: (2, 3, 4, 1), (2, 4, 1, 3), (3, 1, 4, 2), (3, 4, 2, 1), (4, 1, 2, 3), (4, 3, 1, 2) или циклическом (1234), (1243), (1342), (1324), (1432), (1423). Для каждой перестановки существует 6144 булевых функций (или 1536 линейных подпространств), построенные на основе которых векторные булевы функции также имеют максимально возможную компонентную алгебраическую иммунность.

Утверждение 2. Пусть f — булева функция от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. Если векторная булева функция $F_\pi(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$ имеет максимальную компонентную алгебраическую иммунность, то π является полноцикловой перестановкой.

Для $n = 5$ путём полного перебора получено, что всего существует 197 765 122 булевых функций с максимальной алгебраической иммунностью 3. Существует как

минимум четыре булевых функции (им отвечает одно подпространство), на основе которых строится векторная булева функция с максимальным значением иммунности.

С учётом экспериментальных результатов сформулированы следующие гипотезы:

Гипотеза 1. Для любого $n \geqslant 2$ в множестве, состоящем из булевых функций от n переменных с максимальной алгебраической иммунностью и нулевой функции, существует линейное подпространство размерности n.

Данная гипотеза доказана для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко. Для $n = 7, 9$ пока не найдено таких подпространств.

Гипотеза 2. Пусть f — булева функция от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. Тогда в её АНФ присутствует по меньшей мере по одному моному каждой степени i, где $i = 1, 2, \ldots, \lceil n/2 \rceil$.

Данная гипотеза проверена для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко.

Таким образом, возможно построение S-блока от малого числа переменных, который устойчив к алгебраическим атакам. В дальнейшем планируется анализ булевых и векторных булевых функций от большего числа переменных.

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attack 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 presented at the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474–491.

УДК 519.7 DOI 10.17223/2226308X/14/6

О НЕКОТОРЫХ СВОЙСТВАХ САМОДУАЛЬНЫХ ОБОБЩЁННЫХ БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Бент-функции вида $\mathbb{F}_2^n \to \mathbb{Z}_q$, где $q \geqslant 2$ — натуральное число, называются обобщёнными бент-функциями. Обобщённые бент-функции, для которых можно определить дуальную бент-функцию, называются регулярными. Регулярная обобщённая бент-функция называется самодуальной, если она совпадает со своей дуальной. Получены необходимые и достаточные условия самодуальности обобщённых бент-функций из класса Елисеева — Мэйорана — МакФарланда. Представлен полный спектр расстояний Ли между данными функциями. Доказано несуществование аффинных самодуальных обобщённых бент-функций. Приведён класс изометричных отображений, сохраняющих самодуальность обобщённой бент-функции. С помощью данных отображений получена уточнённая классификация самодуальных бент-функций вида $\mathbb{F}_2^4 \to \mathbb{Z}_4$.

Ключевые слова: *самодуальная бент-функция, обобщённая бент-функция, класс Елисеева — Мэйорана — МакФарланда, расстояние Ли.*

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке РФФИ (проект № 20-31-70043) и лаборатории криптографии JetBrains Research.