Алгебраический иммунитет булевой функции*

Б. Ф. Абдурахимов*, А. Б. Саттаров, З. Х. Юлдашев
Национальный университет Узбекскистана им. Мирзо Улугбека, Ташкент, Узбекистан
*Контактный e-mail: a_bakhtiyor@mail.ru

Алгебраический метод криптоанализа, основанный на решении систем уравнений над конечным полем, является одним из современных методов криптоанализа, широко применяющихся в процессе оценки стойкости поточного алгоритма шифрования. На практике в составе большинства поточных алгоритмов шифрования в качестве основных преобразований применяются булевы функции. Алгебраический иммунитет булевой функции — один из основных параметров, определяющих стойкость алгоритма шифрования. Для определения показателя алгебраического иммунитета булевой функции использована операция вычисления ранга специально построенной матрицы. Построен алгоритм вычисления этого показателя. Метод может быть использован в процессе алгебраического криптоанализа для оценки стойкости алгоритмов поточного шифрования.

Ключевые слова: шифрование, поточный алгоритм шифрования, булева функция, аннигилятор, алгебраический иммунитет, алгебраический криптоанализ.

Библиографическая ссылка: Абдурахимов Б.Ф., Саттаров А.Б., Юлдашев З.Х. Алгебраический иммунитет булевой функции // Вычислительные технологии. 2019. Т. 24, № 5. С. 4–12. DOI: 10.25743/ICT.2019.24.5.002.

Введение

Один из основных аспектов аудита безопасности информационных систем — оценка надежности (криптостойкости) криптографических алгоритмов, использованных в них. Для определения криптостойкости алгоритмов шифрования требуется оценить их известными современными методами криптоанализа. Для поточных шифров наиболее перспективным является алгебраический метод, основанный на решении системы уравнений над конечным полем [1–4]. Начиная с 2000 г. становится актуальной задача изучения свойства алгоритмов шифрования, показывающих стойкость к данному виду атак. В результате проведенных исследований многими специалистами был предложен параметр “алгебраический иммунитет”, дающий возможность определить стойкость поточных шифров к алгебраическим атакам. Одновременно после введения понятия алгебраического иммунитета начались исследования, направленные на определение значения этого параметра и его различных свойств, а также изучение соотношения между данным параметром и остальными параметрами преобразования.

В статье предложен метод определения показателя алгебраического иммунитета булевой функции и построен алгоритм его вычисления.

*Title translation and abstract in English can be found on page 12.

1. Постановка задачи

Пусть $\mathbb{Z}_2 = \{0, 1\}$. Через $\mathbb{Z}_2^n$ обозначим множество всех упорядоченных двоичных векторов $\mathbf{x} = (x_1, x_2, x_3, \ldots, x_n)$.

Определение 1. Произвольная функция, отображающая элементы из множества $\mathbb{Z}_2^n$ в множество $\mathbb{Z}_2$, называется булевой функцией от n переменных [5].

Через $\mathcal{F}_n$ обозначим множество всех булевых функций от n переменных.

Понятие алгебраического иммунитета булевых функций введено в 2004 г. в работе [6]. Это понятие является взаимосвязанным с функцией аннигилятора (аннулирующей функцией).

Определение 2. Функция $g(x) \in \mathcal{F}_n$ называется аннигилятором функции $f(x) \in \mathcal{F}_n$, если $f(x)g(x) = 0$ [7].

Степень булевой функции $f(x) \in \mathcal{F}_n$ обозначим через $\deg f(x)$, а множество всех аннигиляторов степени $\deg \leq d$ функции $f(x)$ — через $A_d(f)$.

Определение 3. Алгебраическим иммунитетом $AI(f)$ булевой функции $f(x) \in \mathcal{F}_n$ называется степень булевой функции $g(x) \in \mathcal{F}_n$, где $g(x)$ — не равная тождественно нулю функция с минимальной степенью, такая что $f(x)g(x) = 0$ или $(f(x) \oplus 1)g(x) = 0$. Формально можно записать [7, 8]:

$$AI(f) = \min\{d \,|\, A_d(f) \neq 0 \;\text{ или }\; A_d(f \oplus 1) \neq 0\}. \tag{1}$$

Например, все аннигиляторы для заданной функции $f(x_1, x_2, x_3) = x_3x_2x_1 \oplus x_3x_2 \oplus x_2$ задаются в следующем виде:

1) $x_3x_2x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
2) $x_3x_2x_1 \oplus x_3x_1 \oplus x_2x_1 \oplus x_1$;
3) $x_3x_2 \oplus x_3 \oplus x_2 \oplus 1$;
4) $x_3x_2x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3$;
5) $x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
6) $x_3x_2 \oplus x_3 \oplus x_2x_1 \oplus x_1$;
7) $x_3x_2x_1 \oplus x_3x_1 \oplus x_2 \oplus 1$;
8) $x_3x_2x_1 \oplus x_3x_1$;
9) $x_3x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
10) $x_2x_1 \oplus x_1$;
11) $x_3x_2x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3 \oplus x_2 \oplus 1$;
12) $x_3x_2 \oplus x_3$;
13) $x_3x_2x_1 \oplus x_3x_1 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
14) $x_3x_2x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3 \oplus x_2x_1 \oplus x_1$;
15) $x_2 \oplus 1$;
16) $x_3x_2x_1 \oplus x_3x_2$;
17) $x_3x_1 \oplus x_3 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
18) $x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus x_1$;
19) $x_3x_2x_1 \oplus x_3 \oplus x_2 \oplus 1$;
20) $x_3x_1 \oplus x_3$;
21) $x_3x_2x_1 \oplus x_3x_2 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
22) $x_3x_2x_1 \oplus x_3 \oplus x_2x_1 \oplus x_1$;
23) $x_3x_2 \oplus x_3x_1 \oplus x_2 \oplus 1$;
24) $x_3x_2 \oplus x_3x_1$;
25) $x_3x_2x_1 \oplus x_3 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;

26) $x_3x_2x_1 \oplus x_3x_2 \oplus x_2x_1 \oplus x_1$;
27) $x_3x_1 \oplus x_3 \oplus x_2 \oplus 1$;
28) $x_3x_2x_1 \oplus x_3$;
29) $x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus x_2 \oplus x_1 \oplus 1$;
30) $x_3x_1 \oplus x_3 \oplus x_2x_1 \oplus x_1$.

Для функции $f(x) \oplus 1$ будем иметь

1) $x_3x_2x_1 \oplus x_3x_2 \oplus x_2x_1 \oplus x_2$;
2) $x_3x_2x_1 \oplus x_2x_1$;
3) $x_3x_2 \oplus x_2$;
4) $x_3x_2x_1$;
5) $x_3x_2 \oplus x_2x_1 \oplus x_2$;
6) x_2x_1.

Так как во множестве аннигиляторов существует функция со степенью $\deg = 1$, алгебраический иммунитет заданной функции будет равен $AI(f) = 1$. Значит, одним из методов определения значения параметра $AI(f)$ является нахождение всех аннигиляторов функции $f(x)$, для чего можно воспользоваться методом полного перебора. Однако эффективность этого метода сильно зависит от количества аргументов булевой функции, т. е. при большом количестве аргументов сложность решения задачи увеличивается. Это свидетельствует об актуальности разработки эффективного метода определения значения AI.

Многими специалистами проведен ряд исследований, направленных на решение задачи определения значения AI. В частности, в одной из первых работ [6] предложены два алгоритма. В работах [7, 9, 10] приведены более эффективные алгоритмы и методы определения значения AI. Ниже рассмотрен один из методов решения поставленной задачи, основанный на вычислении ранга матрицы.

2. Метод решения

В работе [4] доказано, что для любой функции $f(x) \in \mathcal{F}_n$ справедлива оценка

$$AI(f) \leq \lceil n/2 \rceil.$$

Пусть справедливо равенство $AI(f) = 1$ для некой функции $f(x) \in \mathcal{F}_n$. Тогда существует $g(x) \in \mathcal{F}_n$ — функция со степенью $\deg(g) = 1$ такая, что будет справедливо $f(x)g(x) = 0$ или $(f(x) \oplus 1)g(x) = 0$. Наоборот, на основе данного утверждения можно сформулировать следующую задачу: если определить существование функций $g(x) \in \mathcal{F}_n$ со степенью $\deg(g) = 1$, удовлетворяющих условию $f(x)g(x) = 0$ или $(f(x) \oplus 1)g(x) = 0$, то $AI(f) = 1$.

Например, пусть заданы булева функция и ее таблица истинности $f(x_1, x_2, x_3) = x_3x_2x_1 \oplus x_3x_1 \oplus x_2 \oplus 1$, $f(x_1, x_2, x_3) = \{11001000\}$. В этом случае алгебраическая нормальная форма (АНФ) линейной функции аннигилятора $g(x) \in \mathcal{F}_3$ имеет общий вид

$$g(x) = a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0, \quad a_i \in \mathbb{Z}_2. \tag{2}$$

Значит, если существуют ненулевые коэффициенты a_0, a_1, a_2 и a_3, удовлетворяющие равенствам $g(000) = 0$, $g(001) = 0$ и $g(100) = 0$, то $AI(f) = 1$, потому что значение функции $f(x)$ будет равно единице только тогда, когда входные значения функции будут равны 000, 001, 100. На основе вышесказанного можно определить значения данных коэффициентов:

— из равенства $g(000) = 0$ вытекает выражение $a_3 \cdot \mathbf{0} \oplus a_2 \cdot \mathbf{0} \oplus a_1 \cdot \mathbf{0} \oplus a_0 = 0$;
— из равенства $g(001) = 0$ вытекает выражение $a_3 \cdot \mathbf{0} \oplus a_2 \cdot \mathbf{0} \oplus a_1 \cdot \mathbf{1} \oplus a_0 = 0$;
— из равенства $g(100) = 0$ вытекает выражение $a_3 \cdot \mathbf{1} \oplus a_2 \cdot \mathbf{0} \oplus a_1 \cdot \mathbf{0} \oplus a_0 = 0$.

В результате решения этих выражений (системы) получим $a_0 = 0$, $a_1 = 0$, $a_3 = 0$. Следовательно, равенство $f(x)g(x) = 0$ будет верно при любых значениях коэффициента a_2, если $a_0 = a_1 = a_3 = 0$. Исходя из этого функция аннигилятора будет $g(x) = x_2$ и справедливо $AI(f) = 1$.

На основе данной идеи можно не только определить значения параметра $AI(f)$, но и построить все функции аннигиляторов. Например, пусть заданы булева функция и ее таблица истинности

$$f(x_1, x_2, x_3) = x_3x_1 \oplus x_3 \oplus x_2x_1 \oplus x_2, \quad f(x_1, x_2, x_3) = \{00101000\}.$$

В соответствии с вышеуказанной идеей для построения и определения существования аннигилятора со степенью $\deg(g) = 1$ сформируем следующую матрицу исходя из системы уравнений связанных коэффициентов a_i:

$$T_{2,5} = \begin{pmatrix} 01010 \\ 10010 \end{pmatrix}.$$

Из этой матрицы (т. е. в результате решения систем) определяем, что $a_3 = a_2 = a_0$. Следовательно, функции, построенные в виде (2) при условии $a_3 = a_2 = a_0$, будут аннигиляторами для заданной функции $f(x)$, а также определено, что $AI(f) = 1$. Приведем эти аннигиляторы:

1) $a_3 = a_2 = a_0, \quad a_1 = 1 \;\Rightarrow\; g_1(x) = x_1$;
2) $a_3 = a_2 = a_0 = a_1 = 1 \;\Rightarrow\; g_2 = x_3 \oplus x_2 \oplus x_1 \oplus 1$;
3) $a_3 = a_2 = a_0 = 1, \quad a_1 = 0 \;\Rightarrow\; g_3 = x_3 \oplus x_2 \oplus 1$.

Для заданной функции общий вид АНФ аннигилятора со степенью $\deg(g) \leq 2$ имеет вид

$$g(x) = a_6x_3 \oplus a_5x_2 \oplus a_4x_1 \oplus a_3x_3x_2 \oplus a_2x_3x_1 \oplus a_1x_2x_1 \oplus a_0, \quad a_i \in \mathbb{Z}_2. \tag{3}$$

Значит, матрица, определяющая аннигилятор степенью $\deg(g) \leq 2$, формируется в следующем виде:

$$T_{2,8} = \begin{pmatrix} 01000010 \\ 10000010 \end{pmatrix}.$$

Из этой матрицы определяем, что $a_6 = a_5 = a_0$. При таком условии функции, построенные в виде (3), состоят из следующих:

1) $a_6 = a_5 = a_3 = a_2 = a_1 = a_0 = 0, \quad a_4 = 1 \;\Rightarrow\; g_1(x) = x_1$;
2) $a_6 = a_5 = a_4 = a_2 = a_1 = a_0 = 0, \quad a_3 = 1 \;\Rightarrow\; g_2(x) = x_3x_2$;
3) $a_6 = a_5 = a_4 = a_3 = a_1 = a_0 = 0, \quad a_2 = 1 \;\Rightarrow\; g_3(x) = x_3x_1$;
4) $a_6 = a_5 = a_4 = a_3 = a_2 = a_0 = 0, \quad a_1 = 1 \;\Rightarrow\; g_4(x) = x_2x_1$;
5) $a_6 = a_5 = a_2 = a_1 = a_0 = 0, \quad a_4 = a_3 = 1 \;\Rightarrow\; g_5(x) = x_1 \oplus x_3x_2$;
6) $a_6 = a_5 = a_3 = a_1 = a_0 = 0, \quad a_4 = a_2 = 1 \;\Rightarrow\; g_6(x) = x_1 \oplus x_3x_1$;
7) $a_6 = a_5 = a_3 = a_2 = a_0 = 0, \quad a_4 = a_1 = 1 \;\Rightarrow\; g_7(x) = x_1 \oplus x_2x_1$;
8) $a_6 = a_5 = a_4 = a_1 = a_0 = 0, \quad a_3 = a_2 = 1 \;\Rightarrow\; g_8(x) = x_3x_2 \oplus x_3x_1$;
9) $a_6 = a_5 = a_4 = a_2 = a_0 = 0, \quad a_3 = a_1 = 1 \;\Rightarrow\; g_9(x) = x_3x_2 \oplus x_2x_1$;
10) $a_6 = a_5 = a_4 = a_3 = a_0 = 0, \quad a_2 = a_1 = 1 \;\Rightarrow\; g_{10}(x) = x_3x_1 \oplus x_2x_1$;
11) $a_6 = a_5 = a_1 = a_0 = 0, \quad a_4 = a_3 = a_2 = 1 \;\Rightarrow\; g_{11}(x) = x_1 \oplus x_3x_2 \oplus x_3x_1$;

12) $a_6 = a_5 = a_2 = a_0 = 0, \quad a_4 = a_3 = a_1 = 1 \Rightarrow g_{12}(x) = x_1 \oplus x_3x_2 \oplus x_2x_1$;
13) $a_6 = a_5 = a_3 = a_0 = 0, \quad a_4 = a_2 = a_1 = 1 \Rightarrow g_{13}(x) = x_1 \oplus x_3x_1 \oplus x_2x_1$;
14) $a_6 = a_5 = a_4 = a_0 = 0, \quad a_3 = a_2 = a_1 = 1 \Rightarrow g_{14}(x) = x_3x_2 \oplus x_3x_1 \oplus x_2x_1$;
15) $a_6 = a_5 = a_0 = 0, \quad a_4 = a_3 = a_2 = a_1 = 1 \Rightarrow g_{15}(x) = x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1$;
16) $a_4 = a_3 = a_2 = a_1 = 0, \quad a_6 = a_5 = a_0 = 1 \Rightarrow g_{16}(x) = x_3 \oplus x_2 \oplus x_1 \oplus 1$;
17) $a_3 = a_2 = a_1 = 0, \quad a_6 = a_5 = a_0 = a_4 = 1 \Rightarrow g_{17}(x) = x_3 \oplus x_2 \oplus x_1 \oplus 1$;
18) $a_4 = a_2 = a_1 = 0, \quad a_6 = a_5 = a_0 = a_3 = 1 \Rightarrow g_{18}(x) = x_3 \oplus x_2 \oplus x_3x_2 \oplus 1$;
19) $a_4 = a_3 = a_1 = 0, \quad a_6 = a_5 = a_0 = a_2 = 1 \Rightarrow g_{19}(x) = x_3 \oplus x_2 \oplus x_3x_1 \oplus 1$;
20) $a_4 = a_3 = a_2 = 0, \quad a_6 = a_5 = a_0 = a_1 = 1 \Rightarrow g_{20}(x) = x_3 \oplus x_2 \oplus x_2x_1 \oplus 1$;
21) $a_2 = a_1 = 0, \quad a_6 = a_5 = a_0 = a_4 = a_3 = 1 \Rightarrow g_{21}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_3x_2 \oplus 1$;
22) $a_3 = a_1 = 0, \quad a_6 = a_5 = a_0 = a_4 = a_2 = 1 \Rightarrow g_{22}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_3x_1 \oplus 1$;
23) $a_3 = a_2 = 0, \quad a_6 = a_5 = a_0 = a_4 = a_1 = 1 \Rightarrow g_{23}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_2x_1 \oplus 1$;
24) $a_4 = a_1 = 0, \quad a_6 = a_5 = a_0 = a_3 = a_2 = 1 \Rightarrow g_{24}(x) = x_3 \oplus x_2 \oplus x_3x_2 \oplus x_3x_1 \oplus 1$;
25) $a_4 = a_2 = 0, \quad a_6 = a_5 = a_0 = a_3 = a_1 = 1 \Rightarrow g_{25}(x) = x_3 \oplus x_2 \oplus x_3x_2 \oplus x_2x_1 \oplus 1$;
26) $a_1 = 0, \quad a_6 = a_5 = a_0 = a_4 = a_3 = a_2 = 1 \Rightarrow g_{26}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus 1$;
27) $a_2 = 0, \quad a_6 = a_5 = a_0 = a_4 = a_3 = a_1 = 1 \Rightarrow g_{27}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_3x_2 \oplus x_2x_1 \oplus 1$;
28) $a_3 = 0, \quad a_6 = a_5 = a_0 = a_4 = a_2 = a_1 = 1 \Rightarrow g_{28}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_3x_1 \oplus x_2x_1 \oplus 1$;
29) $a_4 = 0, \quad a_6 = a_5 = a_0 = a_3 = a_2 = a_1 = 1 \Rightarrow g_{29}(x) = x_3 \oplus x_2 \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus 1$;
30) $a_6 = a_5 = a_0 = a_4 = a_3 = a_2 = a_1 = 1 \Rightarrow g_{30}(x) = x_3 \oplus x_2 \oplus x_1 \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus 1$.

Таким образом, можно построить все аннигиляторы со степенью $\deg(g) \le 3$.

3. Обсуждение результатов

В общем случае на основе вышеуказанного метода при нахождении аннигилятора со степенью $\deg(g) \le d$ для функции $f(x) \in \mathcal{F}_n$, где $f(x \,|\, x \in \mathcal{B}) = 1$, $f(x \,|\, x \in \mathcal{O}) = 0$, требуется построить матрицу $T_d(f)$, состоящую из $|\mathcal{B}|$ строк и $1 + \sum\limits_{i=0}^{d} C_n^i$ $\left(C_n^i = \dfrac{n!}{i!(n-i)!} \right)$ столбцов. Если для ранга $\operatorname{rang}(T_d(f))$ данной матрицы выполняется условие

$$\operatorname{rang}(T_d(f)) < \sum_{i=0}^{d} C_n^i, \tag{4}$$

то существуют аннигиляторы со степенью $\deg(g) \le d$. Аналогично можно определить и для функций $f(x) \oplus 1$.

На основе предложенного метода разработан алгоритм определения значения параметра $AI(f)$, состоящий из такой последовательности.

Вход: $f(x) \in \mathcal{F}_n$ (где $f(x \,|\, x \in \mathcal{B}) = 1$, $f(x \,|\, x \in \mathcal{O}) = 0$).

Выход: $AI(f)$.

1. $AI(f) = \lceil n/2 \rceil$, $i = 1$.
2. $r_1 = \operatorname{rang}(T_i(f))$.
3. $r_2 = \operatorname{rang}(T_i(f \oplus 1))$.
4. Если $r_1 < \sum\limits_{j=0}^{i} C_n^j$ или $r_2 < \sum\limits_{j=0}^{i} C_n^j$, то $AI(f) = i$ и закончить алгоритм.
5. $i = i + 1$.
6. Если $i = AI(f)$, то закончить алгоритм, иначе вернуться к шагу 2.

Сложность приведенного алгоритма зависит от сложности вычисления ранга матрицы $T_i(f)$. Для определения ранга матрицы при использовании метода Гаусса данный

Т а б л и ц а 1. Сравнительные свойства алгоритмов

Метод решения проблем	Сложность
Многомерная полиномиальная интерполяция (multivariate polynomial interpolation) [9]	$O\left(\left(\approx \binom{n}{d}\right)^2\right)$
Ленивое исключение Гаусса (lazy Gaussian elimination) [10]	$O(n^d)$
Решение системы линейных уравнений [6]	$O\left(\frac{1}{8}\binom{n}{d}^3\right)$
Решение однородной системы линейных уравнений [7]	$O\left(M_f\binom{n}{d}^3\right)$, где M_f — длина многочлена Жегалкина для функции f
Определение ранга матрицы (настоящая работа)	$\leq O\left(2\binom{n}{d}^3\right)$

алгоритм требует максимального количества W арифметических действий для функции $f(x) \in \mathcal{F}_n$:

$$W \approx 2\Big(\big(C_n^0\big)^3 + \big(C_n^1\big)^3 + \big(C_n^2\big)^3 + \ldots + \big(C_n^{\lceil n/2\rceil-1}\big)^3\Big). \tag{5}$$

В табл. 1 представлены сравнительные свойства ранее известных алгоритмов, приведенных в работах [6, 7, 9, 10] и в настоящей работе.

С помощью разработанного программного обеспечения, используя предложенный алгоритм, проводились соответствующие эксперименты по следующим критериям:

— наблюдать распределение показателя $AI(f)$ для всех булевых функций в поле $\mathcal{F}_n$;

— наблюдать распределение показателя $AI(f)$ для всех сбалансированных булевых функций в поле $\mathcal{F}_n$.

В соответствии с полученными результатами на основе первого критерия в табл. 2, 3 приведено количественное распределение показателей AI булевых функций в зависимости от полей $\mathcal{F}_n$, в которых они определены.

Из полученных результатов можно сделать вывод о том, что для всевозможных значений параметра AI существуют аннигиляторы в поле $\mathcal{F}_n$ $(1 < n < 6)$. Отметим, что в распределении параметра AI (количество аннигиляторов) отсутствует какая-либо закономерность.

Т а б л и ц а 2. Результаты проверки для функции $f(x) \in \mathcal{F}_n$ (первый критерий)

$\mathcal{F}_n$	Количество всех булевых функций	Распределение $AI(f)$	
		$AI = 1$	$AI = 2$
$\mathcal{F}_2$	14	14 (100 %)	—
$\mathcal{F}_3$	254	184 (72.44 %)	70 (27.56 %)
$\mathcal{F}_4$	65 534	10 552 (16.10 %)	54 982 (83.90 %)

Т а б л и ц а 3. Результаты проверки для функции $f(x) \in \mathcal{F}_5$ (первый критерий)

Количество произвольно выбранных булевых функций	Распределение $AI(f)$		
	$AI = 1$	$AI = 2$	$AI = 3$
2700	86 (3.19 %)	2604 (96.44 %)	10 (0.37 %)

Т а б л и ц а 4. Результаты проверки для функции $f(x) \in \mathcal{F}_n$ (второй критерий)

$\mathcal{F}_n$	Количество всех сбалансированных булевых функций	Распределение $AI(f)$	
		$AI = 1$	$AI = 2$
$\mathcal{F}_2$	6	6 (100 %)	—
$\mathcal{F}_3$	70	0	70 (100 %)
$\mathcal{F}_4$	12 870	0	12 870 (100 %)

Т а б л и ц а 5. Результаты проверки для функции $f(x) \in \mathcal{F}_5$ (второй критерий)

Количество произвольно выбранных булевых функций	Распределения $AI(f)$		
	$AI = 1$	$AI = 2$	$AI = 3$
20 000	0	20 000 (100 %)	0

В соответствии с полученными результатами на основе второго критерия в табл. 4, 5 приведено распределение показателя $AI(f)$ для всех сбалансированных функций, принадлежащих разным полям $\mathcal{F}_n$.

Из полученных результатов по второму критерию можно сделать вывод о том, что в составе сбалансированных булевых функций в поле $\mathcal{F}_n$ $(1 < n < 6)$ не существует аннигиляторов с минимальным значением.

Заключение

Каждый метод криптоанализа, разработанный в качестве атаки на алгоритм шифрования, основывается на той или иной уязвимости шифра, т. е. если алгоритм шифрования уязвим, то степень эффективности атаки, проводимой с помощью метода криптоанализа, будет высокой. Для оценки стойкости алгоритма шифрования к методам криптоанализа в первую очередь целесообразно определить наличие уязвимости в алгоритме. Если найдется такая уязвимость, то можно сделать вывод о том, что алгоритм нестойкий к рассматриваемому методу криптоанализа.

Степень эффективности алгебраического метода криптоанализа к поточным шифрам прямо зависит от значения параметра AI булевой функции $f(x)$, использованной в шифре. Вместе с тем в процессе криптоанализа используются аннигиляторы с самой низкой степенью булевой функции $f(x)$. Если не существует аннигиляторов с низкой степенью (т. е. значение AI большое) или не решен вопрос их определения, то оценка стойкости шифра с помощью алгебраического метода криптоанализа может быть невозможна. В этих случаях нельзя сделать вывод о стойкости и надежности анализируемого шифра.

Предложенный алгоритм служит для повышения эффективности оценки стойкости поточных шифров методами алгебраического криптоанализа.

Список литературы / References

[1] **Abdurakhimov, B.F., Sattarov, A.B.** An algorithm for constructing S-boxes for block symmetric encryption // Universal J. of Math. and Appl. 2018. Vol. 1, No. 1. P. 29–32.

[2] **Abdurakhimov, B.F., Sattarov, A.B.** The method of constructing S-boxes with maximum algebraic immunity // Transactions of the Intern. Sci. Conf. "Modern Problems of Applied Mathematics and Information Technologies-Al-Khorezmiy 2016", Tashkent, 2016. P. 130–132.

[3] **Courtois, N.** Fast algebraic attacks on stream ciphers with linear feedback / D. Boneh (ed.). CRYPTO 2003 // Lecture Notes in Computer Sciences. 2003. Vol. 2729. P. 176–194.

[4] **Courtois, N., Meier, W.** Algebraic attacks on stream ciphers with linear feedback / E. Biham (ed.). EUROCRYPT // Lecture Notes in Computer Sciences. 2003. Vol. 2656. P. 345–359.

[5] **Токарева Н.Н.** Нелинейные булевы функции: бент-функции и их обобщения. Саарбрюккен, Германия: Изд. дом "LAP", 2011. 180 с.
Tokaryeva, N.N. Nonlinear Boolean functions: Bent functions and their generalizations. Saarbrucken, Germany: Lambert Acad. Publ., 2011. 180 p. (In Russ.)

[6] **Meier, W., Pasalic, E., Carlet, C.** Algebraic attacks and decomposition of boolean functions: Advances in Cryptology — EUROCRYPT 2004 // Lecture Notes in Computer Sciences. 2004. Vol. 3027. P. 474–491.

[7] **Баев В.В.** Эффективные алгоритмы получения оценок алгебраической иммунности булевых функций: Дис. ... канд. физ.-мат. наук. М.: МГУ им. М.В. Ломоносова, 2007. 101 с.
Bayev, V.V. Effective algorithms for obtaining estimates of algebraic immunity of Boolean functions: Dis. ... kand. fiz.-math. nauk. Moscow: MGU im. M.V. Lomonosov, 2007. 101 p. (In Russ.)

[8] **Лобанов М.С.** О соотношениях между алгебраической иммунностью и нелинейностью булевых функций: Дис. ... канд. физ.-мат. наук. М.: МГУ им. М.В. Ломоносова, 2009. 64 с.
Lobanov, M.S. On the relationship between algebraic immunity and nonlinearity of Boolean functions: Dis. ... kand. fiz.-math. nauk. Moscow: MGU im. M.V. Lomonosov, 2009. 64 p. (In Russ.)

[9] **Armknecht, F., Carlet, C., Gaborit, P. et al.** Advances in Cryptology — EUROCRYPT 2006 // Lecture Notes in Computer Science. 2006. No. 4004. P. 147–164.

[10] **Didier, F., Tillich, J.-P.** Computing the algebraic immunity efficiently / M. Robshaw (ed.) FSE 2006 // Lecture Notes in Computer Sciences. 2006. Vol. 4047. P. 359–374.

Поступила в редакцию 3 июня 2019 г.,
с доработки — 29 июля 2019 г.

Algebraic immunity of Boolean function

Abdurakhimov, Bakhtiyor F.*, Sattarov, Alizhon B., Yuldashev, Ziyaviddin Kh.

National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, 100174, Uzbekistan

*Corresponding author: Abdurakhimov, Bakhtiyor F., e-mail: a_bakhtiyor@mail.ru

The algebraic method of cryptanalysis, based on solving systems of equations over a finite field, is one of the modern methods that is widely used in the process of assessing the strength of a stream encryption algorithm. In practice, as part of the

majority of stream encryption algorithms, Boolean functions are used as the main transformations. The algebraic immunity of this Boolean function is one of the main parameters determining the strength of the encryption algorithm. In the article, a method for determining the index of algebraic immunity of a Boolean function is proposed, and an algorithm for calculating this function is constructed. To determine the index of algebraic immunity of a Boolean function, the operation of calculating the rank of a specially constructed matrix is used.

A number of examples are given for calculation of the algebraic immunity of a Boolean function and construction of annihilator functions. Also, the results of the experiments are shown, by the definition of the algebraic immunity of all balanced and unbalanced Boolean functions over a finite field $\mathcal{F}_n$ $(1 < n < 6)$. The method may be used in the process of algebraic cryptanalysis in order to assess the strength of stream encryption algorithms.

Keywords: encryption, stream encryption algorithm, Boolean function, annihilator, algebraic immunity, algebraic cryptanalysis.

Cite: Abdurakhimov, B.F., Sattarov, A.B., Yuldashev, Z.KH. Algebraic immunity of Boolean function // Computational Technologies. 2019. Vol. 24, No. 5. P. 4–12. (In Russ.) DOI: 10.25743/ICT.2019.24.5.002.

Received June 3, 2019
Received in revised form July 29, 2019