УДК 519.7

КРИПТОАНАЛИЗ АСИММЕТРИЧНОГО ШИФРА НА БУЛЕВЫХ ФУНКЦИЯХ

И. В. Боровкова, В. А. Кондратьев, И. А. Панкратова

Национальный исследовательский Томский государственный университет, г. Томск, Россия

Рассматривается асимметричная шифрсистема ACBF, ключом в которой служит обратимая векторная булева функция. Ключевая функция строится из порождающей (которая считается известной) с помощью операций инверсии и перестановки переменных и координат. Из этих четырёх операций некоторые являются тождественными (о чём заранее известно криптоаналитику); остальные образуют множество ключевых параметров; нахождение их значений является целью атаки. Для семи из 15 возможных наборов ключевых параметров описаны атаки с известным (для некоторых — и с выбираемым) открытым текстом, приведены оценки их сложности.

Ключевые слова: *криптосистема ACBF, векторные булевы функции, криптоанализ.*

DOI 10.17223/20710410/50/2

CRYPTANALYSIS OF AN ASYMMETRIC CIPHER ON BOOLEAN FUNCTIONS

I. V. Borovkova, V. A. Kondrat'ev, I. A. Pankratova

National Research Tomsk State University, Tomsk, Russia

E-mail: iborovkova95@gmail.com, wadim.condratjev@yandex.ru, pank@mail.tsu.ru

The asymmetric encryption system ACBF is considered. Its key is an invertible vectorial Boolean function constructing from a generating function (which is considered known) using the negation and permutation operations of variables and coordinates. Of these four operations, some are identical, the rest form a set of key parameters; finding them is the goal of the attack. For seven of 15 possible sets of key parameters, attacks with known plaintext are described, their complexity is given. For five sets of key parameters, attacks with choosen plaintext are presented too. The main stage of the attacks is the solution of the auxiliary problem of finding a columns permutation, with the means of which one Boolean matrix is obtained from another. It has been proved that, for uniquely determing the key, it is necessary to have $2\log n$ plaintexts (in average) in the attack with a known plaintext, and it is enough to choose $\log n$ plaintexts in the attack with a choosen plaintext, where n is the length of text.

Keywords: *ACBF cryptosystem, vectorial Boolean functions, cryptanalysis.*

Введение

Рассматривается шифрсистема ACBF (Asymmetric Cryptosystem on Boolean Functions) [1, 2]. Открытые тексты и шифртексты в ней — это булевы векторы длины n;

открытый ключ — функция $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$; закрытый ключ — функция f^{-1}; шифрование и расшифрование выполняются по правилам $y = f(x)$ и $x = f^{-1}(y)$ соответственно.

Функция f строится так. Выбирается обратимая функция $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — *порождающая функция криптосистемы*; функция f получается из неё с помощью перестановки и инверсии переменных x_i и координат g_i: $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, где $\sigma_1, \sigma_2 \in \mathbb{F}_2^n$; $\pi_1, \pi_2 \in \mathbb{S}_n$; $x^{\sigma_1} = x \oplus \overline{\sigma}_1$; $g^{\sigma_2}(x) = g(x) \oplus \overline{\sigma}_2$; $\pi_1(x) = x_{\pi_1(1)} \dots x_{\pi_1(n)}$; $\pi_2(g(x)) = g_{\pi_2(1)}(x) \dots g_{\pi_2(n)}(x)$.

В качестве ключевых параметров шифрсистемы ACBF выступают элементы любого непустого подмножества $J \subseteq \{\pi_1, \pi_2, \sigma_1, \sigma_2\}$ (всего 15 вариантов); операции из множества $\{\pi_1, \pi_2, \sigma_1, \sigma_2\} \backslash J$ считаются тождественными.

Рассмотрим атаки с известным и с выбираемым открытым текстом в следующих предположениях:

1) для любого $x \in \mathbb{F}_2^n$ криптоаналитик может вычислить $g(x)$ и $g^{-1}(x)$;
2) криптоаналитик знает, какие именно из операций $\pi_1, \pi_2, \sigma_1, \sigma_2$ входят в множество J, но их конкретные значения ему не известны; цель — найти эти значения;
3) при атаке с выбираемым открытым текстом криптоаналитик может вычислить $f(x)$ для любого $x \in \mathbb{F}_2^n$.

В работе [1] в тех же предположениях описаны атаки с известным открытым текстом для всех 15 вариантов подмножеств ключевых параметров, приведены оценки их сложности. В данной работе более подробно представлены алгоритмы и уточнены оценки, а также рассмотрены атаки с выбираемым открытым текстом для некоторых вариантов.

Заметим, что случаи $J = \{\sigma_1\}$ и $\{\sigma_2\}$ не представляют интереса, так как для них ключевой параметр находится тривиально по одной паре «открытый текст — шифртекст»:

$$J = \{\sigma_1\}: \quad y = f(x) = g(x \oplus \overline{\sigma}_1) \;\Rightarrow\; \overline{\sigma}_1 = x \oplus g^{-1}(y),$$
$$J = \{\sigma_2\}: \quad y = f(x) = g(x) \oplus \overline{\sigma}_2 \;\Rightarrow\; \overline{\sigma}_2 = g(x) \oplus y.$$

1. Поиск перестановки столбцов

Рассмотрим вспомогательную задачу. Пусть даны две булевых матрицы, одна из которых получена перестановкой столбцов второй матрицы. Требуется найти эту перестановку.

Пусть $\pi \in \mathbb{S}_n$ — подстановка степени n; $A = ||a_{ij}||$, $B = ||b_{ij}||$ — булевы матрицы размера $m \times n$; A_i, B_i, $i = 1, \dots, m$, — их строки; $A^{(j)}, B^{(j)}$, $j = 1, \dots, n$, — вектор-столбцы, причём $B^{(j)} = A^{(\pi(j))}$ для $j = 1, \dots, n$ (будем обозначать $B = \pi(A)$); для $x, \sigma \in \{0, 1\}$ положим $x^\sigma = \begin{cases} x, & \sigma = 1, \\ \overline{x}, & \sigma = 0. \end{cases}$ Построим матрицу $D = ||d_{jk}||$ размера $n \times n$ так:

$$d_{jk} = \bigwedge_{i=1}^{m} a_{ik}^{b_{ij}}, \quad j, k = 1, \dots, n,$$

то же самое можно записать через покомпонентную конъюнкцию строк:

$$D_j = \bigwedge_{i=1}^{m} A_i^{b_{ij}}, \quad j = 1, \dots, n. \tag{1}$$

Будем обозначать $D = T(A, B)$.

Утверждение 1. Пусть $A = ||a_{ij}||$, $B = ||b_{ij}||$ — булевы матрицы размера $m \times n$, $B = \pi_1(A)$ для некоторой $\pi_1 \in \mathbb{S}_n$. Тогда в матрице $D = T(A, B)$ элемент $d_{jk} = 1$, если и только если существует подстановка $\pi \in \mathbb{S}_n$, такая, что $B = \pi(A)$ и $\pi(j) = k$.

Доказательство. Заметим, что $d_{jk} = 1 \Leftrightarrow a_{ik} = b_{ij}$ для всех $i = 1, \ldots, m \Leftrightarrow$ $\Leftrightarrow B^{(j)} = A^{(k)}$.

Необходимость. Пусть $d_{jk} = 1$. Если $\pi_1(j) = k$, то $\pi = \pi_1$ — искомая подстановка. В противном случае пусть $\pi_1(j) = s \neq k$ и $\pi_1(i) = k$ для некоторого $i \in \{1, \ldots, n\}$. Тогда $B^{(j)} = A^{(s)}$, $B^{(i)} = A^{(k)}$, откуда ввиду $B^{(j)} = A^{(k)}$ получаем $A^{(k)} = A^{(s)}$. Умножим π_1 на транспозицию (s, k), получим подстановку π, для которой $\pi(j) = k$, $\pi(i) = s$, $\pi(A) = B$.

Достаточность. Из условий $B = \pi(A)$ и $\pi(j) = k$ получаем $B^{(j)} = A^{(k)}$, откуда $d_{jk} = 1$. ■

Замечание 1. Если в матрице A все столбцы различны, то существует единственная подстановка π со свойством $B = \pi(A)$; в этом случае $D = T(A, B)$ — матрица этой подстановки (т. е. $B = AD^{\mathrm{T}}$).

Замечание 2. Пусть множество столбцов матрицы A можно разбить на классы $Q_1, \ldots, Q_k$ одинаковых столбцов, $1 \leqslant k \leqslant n$, так, что $|Q_j| = r_j$, $j = 1, \ldots, k$, $r_1 + \ldots + r_k = n$. Тогда множество строк матрицы $D = T(A, B)$ тоже разбивается на k классов одинаковых строк мощностей $r_1, \ldots, r_k$; вес строк в каждом классе равен мощности класса; все возможные подстановки π, для которых верно $\pi(A) = B$, удовлетворяют условию $\pi(i) = j \Leftrightarrow d_{ij} = 1$; количество таких подстановок равно $\prod\limits_{i=1}^{k} r_i!$.

Будем говорить, что *матрица $D = T(A, B)$ содержит все подстановки π, удовлетворяющие уравнению $\pi(A) = B$.*

Пример 1. Пусть

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Тогда

$$D = T(A, B) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}; \quad \pi(1) = 2; \quad \pi(2), \pi(4) \in \{1, 3\}; \quad \pi(3) = 4,$$

т. е. все подстановки π, такие, что $\pi(A) = B$, — это $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

Замечание 3. Рассмотрим случай, когда семейства столбцов в матрицах A и B различны, т. е. матрицу B невозможно получить из матрицы A никакой перестановкой столбцов. Пусть, например, $B^{(j_1)} = \ldots = B^{(j_r)} = A^{(k_1)} = \ldots = A^{(k_s)}$ и $r \neq s$ (в частности, может быть $s = 0$). Тогда в матрице $D = T(A, B)$ строки $D_{j_1}, \ldots, D_{j_r}$ одинаковы и имеют по s единиц — мощность класса не равна весу строк в нём. В таком случае будем говорить, что D *не является матрицей подстановок.*

Пример 2. Пусть

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Тогда $D = T(A,B) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ и D не является матрицей подстановок, так как вес строк в классе $\{D_1, D_2\}$ равен 1, а в классе $\{D_3\}$ — 2, что не совпадает с мощностью классов.

2. Криптоанализ вариантов шифрсистемы ACBF

2.1. Случай $J = \{\pi_1\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = g(\pi_1(x)); \quad \pi_1(x) = g^{-1}(y).$$

Тогда если P — матрица размера $m \times n$ со строками открытых текстов $P_1, \ldots, P_m$,

$$C_i = g(\pi_1(P_i)),\ i = 1, \ldots, m, \tag{2}$$

P' — матрица размера $m \times n$ со строками $g^{-1}(C_i)$, $i = 1, \ldots, m$, то матрица $D = T(P, P')$ содержит все возможные подстановки π_1, удовлетворяющие системе уравнений (2).

Таким образом, алгоритм криптоанализа состоит в применении формулы (1) к матрицам P и P' в качестве A и B соответственно; его сложность равна $O(nm)$. В [3, алгоритм 1] приведён другой способ нахождения подстановки π_1; главный его недостаток — необходимость сравнивать *столбцы* булевых матриц, в то время как формула (1) представляет собой покомпонентную конъюнкцию *строк* или их инверсий и может быть выполнена для всех (или, по крайней мере, группы столбцов — в зависимости от длины строки и разрядности используемого типа данных) одновременно.

Кроме того, при вычислении по формуле (1) можно выполнять конъюнкцию не всех m строк (или их инверсий) матрицы P, а остановиться тогда, когда вес строки D_j станет равным 1. Так, в примере 1 для вычисления строки D_1 достаточно двух шагов ($\neg(1010) \wedge (1110) = (0100)$), как и для вычисления D_3 ($\neg(1010) \wedge \neg(1110) = (0001)$).

Компьютерные эксперименты с программами на языке ЛЯПАС [4] (в котором, в частности, есть операция взвешивания булева вектора) показывают преимущество вычислений по формуле (1) перед алгоритмом 1 из [3]; так, при $n = m = 31$ первый способ быстрее второго примерно в 10 раз, если учитывать время транспонирования матрицы в алгоритме 1, и в 1,3 раза без учёта этого времени.

Согласно замечаниям 1 и 2, ключ (подстановка π_1) определяется однозначно, если и только если все столбцы в матрице P различны.

Утверждение 2. Если открытые тексты распределены случайно равновероятно, то при атаке с известным открытым текстом для однозначного определения ключа в среднем понадобится $2 \log n$ открытых текстов.

Доказательство. В булевой матрице с m строками столбцы могут принимать 2^m различных значений; при случайных равновероятных строках они также случайны и равновероятны. Согласно парадоксу дней рождения [5, Ch. 2.1.5], в среднем число попарно различных столбцов равно $n = \sqrt{\pi 2^m / 2}$. Отсюда получаем $m \approx 2 \log n$. ■

Справедливость утверждения 2 подтверждена в компьютерном эксперименте.

Пусть x — булев вектор длины k; через $(x)^t$ обозначим булев вектор длины kt — конкатенацию t одинаковых векторов x.

Утверждение 3. Если производится атака с выбираемым открытым текстом, то для нахождения ключа достаточно рассмотреть $m = \lceil \log n \rceil$ пар (P_i, C_i).

Доказательство. Согласно замечанию 1, достаточно выбрать открытые тексты P_i, $i = 1, \ldots, m$, так, чтобы в матрице P со строками P_i все столбцы были различны.

Пусть $m = \lceil \log n \rceil$, $t = 2^m \geqslant n$. Построим матрицу P'' размера $m \times t$ со строками

$$\begin{aligned} P''_1 &= (0)^{t/2}(1)^{t/2}, \\ P''_2 &= (0)^{t/4}(1)^{t/4}(0)^{t/4}(1)^{t/4}, \\ &\ldots \\ P''_m &= (01)^{t/2} \end{aligned} \tag{3}$$

(очевидно, все её столбцы различны); удалим из неё любые $(t - n)$ столбцов; строки получившейся матрицы примем за открытые тексты P_i, $i = 1, \ldots, m$. ■

2.2. Случай $J = \{\pi_2\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = \pi_2(g(x)).$$

Тогда если $P_1, \ldots, P_m$ — открытые тексты, C — матрица размера $m \times n$ со строками шифртекстов

$$C_i = \pi_2(g(P_i)),\ i = 1, \ldots, m, \tag{4}$$

C' — матрица размера $m \times n$ со строками $g(P_i)$, $i = 1, \ldots, m$, то матрица $D = T(C', C)$ содержит все возможные подстановки π_2, удовлетворяющие системе уравнений (4).

Если открытые тексты P_i, $i = 1, \ldots, m$, выбираются в $\mathbb{F}_2^n$ случайно равновероятно, то, в силу обратимости (взаимной однозначности) функции g, значения $g(P_i)$ также имеют равномерное распределение. Поэтому по аналогии с утверждением 2 получаем, что при атаке с известным открытым текстом для однозначного определения ключа в среднем понадобится $2 \log n$ открытых текстов.

При атаке с выбираемым открытым текстом надо выбрать тексты P_i так, чтобы в матрице со строками $g(P_i)$, $i = 1, \ldots, m$, все столбцы были различны. Это можно сделать, например, так: построить матрицу P'', как в (3), удалить из неё любые $t - n$ столбцов (обозначим строки получившейся матрицы B_i) и положить $P_i = g^{-1}(B_i)$, $i = 1, \ldots, m$.

2.3. Случай $J = \{\pi_1, \sigma_1\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = g(\pi_1(x^{\sigma_1})) = g(\pi_1(x \oplus b)),$$

где $b = \overline{\sigma}_1$. Поскольку $\pi_1(x \oplus b) = \pi_1(x) \oplus \pi_1(b)$, имеем

$$g^{-1}(y) = \pi_1(x) \oplus \pi_1(b).$$

Составим систему

$$\begin{cases} g^{-1}(C_1) = \pi_1(P_1) \oplus \pi_1(b), \\ \ldots \\ g^{-1}(C_m) = \pi_1(P_m) \oplus \pi_1(b), \\ g^{-1}(C_{m+1}) = \pi_1(P_{m+1}) \oplus \pi_1(b), \end{cases}$$

прибавим по модулю 2 последнее уравнение к каждому из предыдущих и снова применим свойство линейности подстановки π_1; в результате получим систему

$$\begin{cases} g^{-1}(C_1) \oplus g^{-1}(C_{m+1}) = \pi_1(P_1 \oplus P_{m+1}), \\ \dots \\ g^{-1}(C_m) \oplus g^{-1}(C_{m+1}) = \pi_1(P_m \oplus P_{m+1}), \\ g^{-1}(C_{m+1}) = \pi_1(P_{m+1}) \oplus \pi_1(b). \end{cases} \tag{5}$$

Построим матрицы $P_\oplus$ со строками $P_i \oplus P_{m+1}$ и $P'_\oplus$ со строками $g^{-1}(C_i) \oplus g^{-1}(C_{m+1})$, $i = 1, \dots, m$. Тогда матрица $D = T(P_\oplus, P'_\oplus)$ содержит все возможные подстановки π_1, удовлетворяющие первым m уравнениям системы (5).

Зная π_1, значение σ_1 найдём из последнего уравнения: $\sigma_1 = \overline{b}$, $b = \pi_1^{-1}(g^{-1}(C_{m+1})) \oplus$ $\oplus P_{m+1}$. Сложность атаки та же, что в предыдущих случаях: $O(nm)$; для однозначного определения ключа в атаке с известным открытым текстом в среднем понадобится $2 \log n$ открытых текстов; при атаке с выбором открытого текста ключ определится однозначно, если открытые тексты P_i, $i = 1, \dots, m+1$, $m = \lceil \log n \rceil$, выбрать следующим образом: построить матрицу P'', как в (3); удалить из неё любые $t - n$ столбцов; P_{m+1} выбрать случайно в $\mathbb{F}_2^n$; открытый текст P_i для $i = 1, \dots, m$ получить как сумму i-й строки матрицы и P_{m+1}.

2.4. Случай $J = \{\pi_2, \sigma_2\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = \pi_2(g^{\sigma_2}(x)) = \pi_2(g(x) \oplus d),$$

где $d = \overline{\sigma}_2$. Пусть $P_1, \dots, P_m, P_{m+1}$ — открытые тексты; $C_1, \dots, C_m, C_{m+1}$ — соответствующие шифртексты. Составим систему

$$\begin{cases} \pi_2^{-1}(C_1) = g(P_1) \oplus d, \\ \dots \\ \pi_2^{-1}(C_m) = g(P_m) \oplus d, \\ \pi_2^{-1}(C_{m+1}) = g(P_{m+1}) \oplus d, \end{cases}$$

прибавим по модулю 2 последнее уравнение к каждому из предыдущих, применим к обеим частям уравнений подстановку π_2 и учтём её линейность; в результате получим систему

$$\begin{cases} C_i \oplus C_{m+1} = \pi_2(g(P_i) \oplus g(P_{m+1})), \quad i = 1, \dots, m, \\ \pi_2^{-1}(C_{m+1}) = g(P_{m+1}) \oplus d. \end{cases} \tag{6}$$

Построим матрицы $C_\oplus$ со строками $C_i \oplus C_{m+1}$ и $C'_\oplus$ со строками $g(P_i) \oplus g(P_{m+1})$, $i =$ $= 1, \dots, m$. Тогда матрица $D = T(C'_\oplus, C_\oplus)$ содержит все возможные подстановки π_2, удовлетворяющие первым m уравнениям системы (6).

Зная π_2, значение σ_2 найдём из условия $\sigma_2 = \overline{d}$, $d = \pi_2^{-1}(C_{m+1}) \oplus g(P_{m+1})$. Сложность атаки $O(nm)$; для однозначного определения ключа в атаке с известным открытым текстом в среднем понадобится $2 \log n$ открытых текстов; при атаке с выбором открытого текста ключ определится однозначно, если открытые тексты P_i, $i = 1, \dots, m+1$, $m = \lceil \log n \rceil$, выбрать следующим образом: построить матрицу P'', как в (3); удалить из неё любые $t - n$ столбцов (обозначим строки получившейся матрицы B_i); P_{m+1} выбрать случайно в $\mathbb{F}_2^n$ и положить $P_i = g^{-1}(B_i \oplus g(P_{m+1}))$, $i = 1, \dots, m$.

2.5. Случай $J = \{\pi_1, \sigma_2\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = g^{\sigma_2}(\pi_1(x)) = g(\pi_1(x)) \oplus d, \quad \pi_1(x) = g^{-1}(y \oplus d), \quad \text{где } d = \overline{\sigma}_2.$$

Утверждение 4. Если производится атака с выбираемым открытым текстом, то для нахождения ключевых параметров достаточно $\lceil \log n \rceil + 1$ пар (P_i, C_i).

Доказательство. Положим $m = \lceil \log n \rceil$ и выберем открытые тексты $P_1, \ldots, P_m$, как в утверждении 3, а $P_{m+1} \in \{(0)^n, (1)^n\}$. Пусть

$$C_i = g(\pi_1(P_i)) \oplus d, \quad i = 1, \ldots, m+1. \tag{7}$$

Тогда $\pi_1(P_{m+1}) = P_{m+1}$, следовательно, d находится однозначно: $d = g(P_{m+1}) \oplus C_{m+1}$. Построим матрицы P и P' размера $m \times n$ со строками P_i и $g^{-1}(C_i \oplus d)$ соответственно. Матрица $D = T(P, P')$ содержит все подстановки π_1, удовлетворяющие системе (7). ■

Атака с известным открытым текстом описана в [1] и использует тот факт, что перестановка компонент вектора x не меняет его вес $\mathrm{w}(x)$, поэтому

$$\mathrm{w}(P_i) = \mathrm{w}(g^{-1}(C_i \oplus d)), \quad i = 1, \ldots, m. \tag{8}$$

Систему (8) будем решать последовательно. Для нахождения всех d, удовлетворяющих первому уравнению, построим множества

$$X = \{x \in \mathbb{F}_2^n : \mathrm{w}(x) = \mathrm{w}(P_1)\}, \quad D_1 = \{g(x) \oplus C_1 : x \in X\}.$$

Тогда $\mathrm{w}(P_1) = \mathrm{w}(g^{-1}(C_1 \oplus d))$ для любого $d \in D_1$. Затем построим множества

$$D_i = \{d \in D_{i-1} : \mathrm{w}(P_i) = \mathrm{w}(g^{-1}(C_i \oplus d))\}, \quad i = 2, \ldots, m;$$

имеем: D_m — множество значений d, удовлетворяющих системе (8).

Поскольку $|X| = |D_1| = \mathrm{C}_n^{\mathrm{w}(P_1)}$, для сокращения перебора имеет смысл в качестве P_1 выбирать из имеющегося множества открытых текстов такой, вес которого максимально далёк от $n/2$.

Для каждого $d \in D_m$ находим все возможные подстановки π_1, как в доказательстве утверждения 4. Если для некоторого d получим, что матрица $T(P, P')$ не является матрицей подстановок (см. замечание 3), то такое d не может быть частью ключа. Количество значений $d \in D_m$ в худшем случае равно $\mathrm{C}_n^{n/2}$.

2.6. Случай $J = \{\pi_2, \sigma_1\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = \pi_2(g(x^{\sigma_1})) = \pi_2(g(x \oplus b)), \quad \text{где } b = \overline{\sigma}_1.$$

Атака с известным открытым текстом аналогична предыдущему случаю: находим все векторы b, удовлетворяющие условию

$$\mathrm{w}(C_i) = \mathrm{w}(g(P_i \oplus b)), \quad i = 1, \ldots, m,$$

выбирая в качестве C_1 шифртекст с максимально далёким от $n/2$ весом; для каждого из них все возможные подстановки π_2 содержатся в матрице $T(C', C)$, где C', C — матрицы со строками $g(P_i \oplus b)$ и C_i соответственно.

2.7. Случай $J = \{\pi_1, \pi_2\}$

По определению получаем

$$y = f(x) = \pi_2(g(\pi_1(x))).$$

В [3] сформулировано (без доказательства) следующее утверждение.

Утверждение 5. Пусть имеется m пар открытых текстов и шифртекстов вида (P_i, C_i), $i = 1, \ldots, m$. Составим матрицы P и C размера $m \times n$ со строками P_i и C_i соответственно. Необходимым условием единственности решения системы уравнений

$$C_i = \pi_2(g(\pi_1(P_i))), \quad i = 1, \ldots, m, \tag{9}$$

относительно подстановок π_1, π_2 является отсутствие одинаковых столбцов в каждой из матриц P и C.

Доказательство. Предположим, что подстановки π_1, π_2 удовлетворяют системе (9) и в матрице P есть одинаковые столбцы, например $P^{(j)} = P^{(k)}$, $j \neq k$. Построим подстановку π_1', умножив π_1 на транспозицию $(\pi_1(k), \pi_1(j))$. Тогда $\pi_1'(P) = \pi_1(P)$, т. е. $\pi_1'(P_i) = \pi_1(P_i)$ для всех $i = 1, \ldots, m$, и пара π_1', π_2 также удовлетворяет системе (9).

Аналогично доказывается необходимость отсутствия одинаковых столбцов в матрице C. ■

Атака с известным открытым текстом может быть проведена следующим образом:

1) строим матрицу C со строками C_i, $i = 1, \ldots, m$;
2) перебираем $n!$ подстановок π_1' («кандидатов» в π_1);
3) для каждой π_1' строим матрицу C' со строками $g(\pi_1'(P_i))$, $i = 1, \ldots, m$;
4) находим $D = T(C', C)$;
5) если D не является матрицей подстановок, то π_1' не может быть частью ключа; иначе все пары (π_1, π_2), где $\pi_1 = \pi_1'$ и π_2 содержится в D, удовлетворяют системе (9).

Сложность атаки та же, что и у предложенных в [1, 3], — $O(n!)$. Можно попытаться сократить перебор подстановок π_1', воспользовавшись, как и в прошлых двух случаях, инвариантностью веса булева вектора относительно перестановки его координат, а именно: в качестве «кандидатов» в π_1 рассматривать только такие подстановки π_1', которые удовлетворяют условиям

$$\mathrm{w}(g(\pi_1'(P_i))) = \mathrm{w}(C_i), \quad i = 1, \ldots, m. \tag{10}$$

Для этого на шаге 3 атаки надо дополнительно проверять условие $\mathrm{w}(g(\pi_1'(P_i))) = \mathrm{w}(C_i)$ и прекращать построение матрицы C', переходя к следующей подстановке π_1', сразу же, как только оно нарушится для некоторого $i \in \{1, \ldots, m\}$. Для сокращения перебора имеет смысл переупорядочить пары (P_i, C_i) так, чтобы сначала шли шифртексты с максимально далёким от $n/2$ весом.

Полезность такой модификации на практике составляет предмет дальнейших исследований; в частности, предстоит выяснить:

1) что более трудозатратно — вычисление m раз (в худшем случае) веса вектора $g(\pi_1'(P_i))$ или проверка того, является ли матрица D матрицей подстановок;
2) сколько в среднем строк матрицы C' приходится строить, прежде чем обнаруживается нарушение условия (10).

Заключение

Для шифрсистемы ACBF рассмотрены следующие подмножества ключевых параметров: $J = \{\pi_1\}$, $\{\pi_2\}$, $\{\pi_1, \sigma_1\}$, $\{\pi_2, \sigma_2\}$, $\{\pi_1, \sigma_2\}$, $\{\pi_2, \sigma_1\}$, $\{\pi_1, \pi_2\}$. Описаны атаки с известным открытым текстом; для первых пяти вариантов — и с выбираемым открытым текстом.

В таблице приведён порядок $h(n)$ вычислительной сложности $O(h(n))$ для предложенных атак; для сравнения в третьей строке указан порядок сложности атаки, построенной по общей схеме [2], $p(n)$ — некоторый полином от n. Видно, что для $J = \{\pi_1, \sigma_1\}$ получена атака меньшей сложности; для остальных случаев уточнены оценки и/или алгоритмы атак.

J	$\{\pi_1\}$	$\{\pi_2\}$	$\{\pi_1, \sigma_1\}$	$\{\pi_2, \sigma_2\}$	$\{\pi_1, \sigma_2\}$	$\{\pi_2, \sigma_1\}$	$\{\pi_1, \pi_2\}$
$h(n)$ (настоящая работа)	$n \log n$	$n \log n$	$n \log n$	$n \log n$	$\mathrm{C}_n^{n/2}$	$\mathrm{C}_n^{n/2}$	$n!$
$h(n)$ [2]	$p(n)$	$p(n)$	$\mathrm{C}_n^{n/2}$	$p(n)$	$\mathrm{C}_n^{n/2}$	$\mathrm{C}_n^{n/2}$	$n!$

ЛИТЕРАТУРА

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
2. *Агибалов Г. П., Панкратова И. А.* Криптосистемы с открытым ключом на булевых функциях // Прикладная дискретная математика. Приложение. 2018. № 11. С. 54–57.
3. *Боровкова И. В., Панкратова И. А.* Криптоанализ шифрсистемы ACBF // Прикладная дискретная математика. Приложение. 2019. № 12. С. 90–93.
4. *Агибалов Г. П., Липский В. Б., Панкратова И. А.* О криптографическом расширении и его реализации для русского языка программирования // Прикладная дискретная математика. 2013. № 3(21). С. 93–104.
5. *Menezes A. J., Van Oorshot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. N.Y.: CRC Press, 1997.

REFERENCES

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 23–33.
2. *Agibalov G. P. and Pankratova I. A.* Kriptosistemy s otkrytym klyuchom na bulevykh funktsiyakh [Public key cryptosystems on Boolean functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2018, no. 11, pp. 54–57. (in Russian)
3. *Borovkova I. V. and Pankratova I. A.* Kriptoanaliz shifrsistemy ACBF [Cryptanalysis of the ACBF encryption system]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2019, no. 12, pp. 90–93. (in Russian)
4. *Agibalov G. P., Lipskiy V. B., and Pankratova I. A.* O kriptograficheskom rasshirenii i ego realizatsii dlya russkogo yazyka programmirovaniya [Cryptographic extension and its implementation for Russian programming language]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 93–104. (in Russian)
5. *Menezes A. J., Van Oorshot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. N.Y., CRC Press, 1997.