УДК 519.7 DOI 10.17223/20710410/67/3

# О ВОЗМОЖНОСТИ МОДИФИКАЦИИ АЛГОРИТМА КБ-256 С ТОЧКИ ЗРЕНИЯ ПОИСКА НЕВОЗМОЖНЫХ ПЕРЕХОДОВ РАЗНОСТЕЙ БЛОКОВ

А. Б. Чухно

*НИУ ВШЭ, г. Москва, Россия*

**E-mail:** achuhno@hse.ru

Наличие у блочного алгоритма шифрования невозможных переходов разностей блоков может приводить к эффективным методам восстановления секретного ключа. Для алгоритма КБ-256 ранее было найдено большое количество невозможных переходов разностей блоков. В данной работе рассматривается вопрос об изменении функции обратной связи с целью уменьшения числа итераций, на которые их можно распространить. Показано, что изменение количества суммируемых подблоков в функции обратной связи не сможет уменьшить максимальное число итераций, на которое распространяется невозможный переход разностей блоков. Для выделенного типа обобщённых сетей Фейстеля предложен общий подход к поиску разностей с вероятностью 1.

**Ключевые слова:** *КБ-256, невозможные переходы разностей блоков, циркулянтная матрица, схема Фейстеля.*

# ON THE POSSIBILITY OF MODIFYING THE KB-256 ALGORITHM FROM THE SEARCHING FOR IMPOSSIBLE DIFFERENTIALS VIEW POINT

A. B. Chuhno

*Higher School of Economics, Moscow, Russia*

The presence of impossible differentials in a block cipher algorithm can lead to efficient methods for recovering the secret key. A large number of impossible differentials have been found for the KB-256 algorithm. This paper considers the modification of the feedback function to reduce the number of iterations to which they can be extended. A general approach to finding differences with probability 1 is proposed. It is shown that changing the number of summable sub-blocks in the feedback function will not reduce the maximum number of iterations to which an infeasible differential can be extended.

## Введение

Анализ криптографических алгоритмов с использованием невозможных переходов разностей блоков предложен независимо друг от друга Э. Бихамом, А. Бирюковым и А. Шамиром [1] и Л. Кнудсеном [2]. Под невозможным переходом разностей блоков при фиксированном ключе понимается невозможность заданного значения разности выходных блоков при входных блоках с фиксированной разностью.

Наличие невозможных переходов разностей блоков позволяет восстанавливать последовательность итерационных ключей. При переборе итерационных ключей проверяются разности входных блоков и соответствующие им разности выходных блоков — если появился невозможный переход разностей блоков, то ключ отбрасывается.

Алгоритм блочного шифрования КБ в нескольких вариантах предложен впервые в работе [3], в [4] проведено сравнение быстродействия 32 итераций алгоритма КБ с алгоритмом Магма. Далее под алгоритмом КБ-256 понимается вариант алгоритма с входным блоком шифрования размером 256 бит. В работе [5] для алгоритма КБ-256 найдено большое количество невозможных переходов разностей блоков.

Таким образом, алгоритм КБ-256 имеет изъян. Возникает вопрос, можно ли изменить устройство итерационной функции, чтобы уменьшить число итераций, на которые распространяется невозможный переход разностей блоков?

## 1. Основные понятия

Обозначим: $V_n = \{0,1\}^n$.

Пусть имеется алгоритм блочного шифрования $F : V_n \times V_m \to V_n$, устроенный по итеративному принципу

$$F(x,K) = G_{K_1} \circ G_{K_2} \circ \ldots \circ G_{K_t}(x) = G(G(\ldots G(x,K_1)\ldots,K_{t-1}),K_t),$$

где $x \in V_n$ — блок открытого текста; $K \in V_m$ — ключ шифрования. Последовательность $K_1, K_2, \ldots, K_t$, $K_j \in V_h$, $j = 1,\ldots,t$ — итерационные ключи, полученные из ключа $K$.

Также обозначим через $F_j(x,K)$ — применение первых $j$ итераций:

$$F_j(x,K) = G_{K_1} \circ G_{K_2} \circ \ldots \circ G_{K_j}(x), \quad F_t(x,K) = F(x,K).$$

**Определение 1.** Разностным соотношением $\widehat{\alpha,\beta}^{F_j}$ для отображения $F_j$ с фиксированным ключом $K$ называется событие

$$\widehat{\alpha,\beta}^{F_j} = \{x : F_j(x,K) \oplus F_j(x \oplus \alpha, K) = \beta\},$$

его вероятность обозначим $\Pr\left[\widehat{\alpha,\beta}^{F_j}\right] = p_{\alpha,\beta} \geqslant 0$.

Невозможным переходом разностей блоков назовём разностное соотношение с вероятностью $p_{\alpha,\beta} = 0$.

Для вектора $\mathbf{v} \in V_n$ веса $k$ введём обозначение $\mathbf{v} = [i_1, i_2 \ldots, i_k]$, где $i_1, i_2 \ldots, i_k$ — номера координат, не равных нулю.

## 2. Алгоритм КБ-256

Алгоритм шифрования КБ-256 есть отображение $F : V_{256} \times V_{256} \to V_{256}$; открытый текст $P = (X_0^0, X_1^0, X_2^0, X_3^0, X_4^0, X_5^0, X_6^0, X_7^0)$, $X_j^0 \in V_{32}$, $j = 0,\ldots,7$; ключ шифрования $K = (K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7)$, $K_j \in V_{32}$, $j = 0,\ldots,7$.

Отображение $F$ представимо в виде композиции

$$F(P,K) = G_{16}(G_{15}(\ldots G_1(P,K),K)\ldots),K) = C,$$

где $G_j(\cdot,K)$ — раундовое отображение, $j = 1,\ldots,16$.

Обозначим: $\Sigma_j = X_1 \boxplus X_3 \boxplus X_4 \boxplus X_6 \boxplus X_7$ — модульная сумма пяти подблоков входного вектора для $j$-й итерации, где $\boxplus$ — сложение по модулю $2^{32}$ (эту сумму будем называть

промежуточной суммой); $T_{\lll 19}$ — циклический сдвиг вектора в сторону старших бит; $S$ — применение к двоичному вектору блока 4-битных подстановок [6]. Тогда

$$G_j\left((X_0, X_1, \ldots, X_7), K\right) = \big(X_1, X_2 \oplus T_{\lll 19}(S(\Sigma_j \boxplus q_1^j)), X_3, X_4,$$
$$X_5 \oplus T_{\lll 19}(S(\Sigma_j \boxplus q_2^j)), X_6, X_7, X_0 \oplus T_{\lll 19}(S(\Sigma_j \boxplus q_3^j))\big),$$

где $q_1^j, q_2^j, q_3^j$ — раундовые ключи $j$-й итерации; $\oplus$ — побитовый XOR. Схематично раундовое отображение приведено на рис. 1, где через $f$ обозначена композиция отображений: $f(X) = T_{\lll 19}(S(X))$.

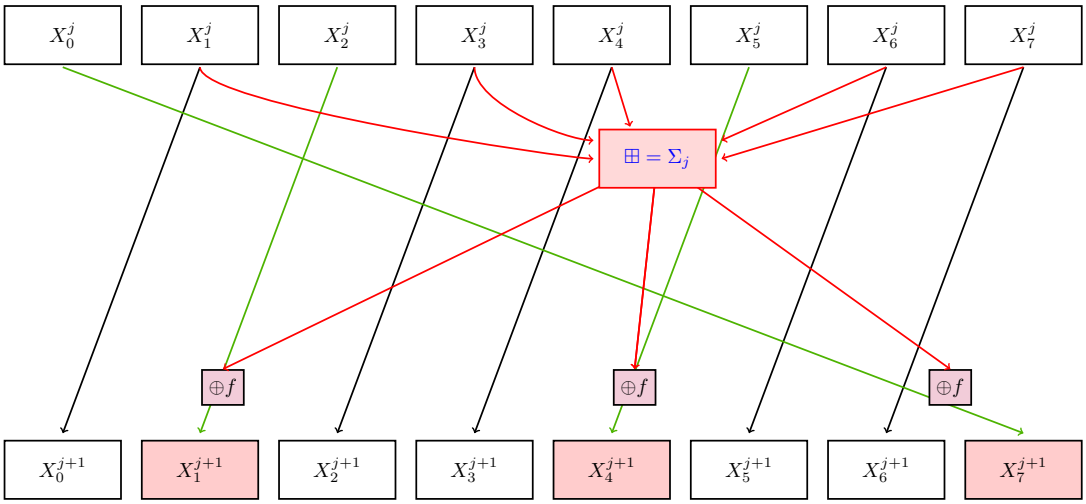


Рис. 1. Одна итерация алгоритма КБ-256

## 3. Циркулянтные матрицы с элементами из $\mathbb{F}_2$

Приведём вспомогательные факты о циркулянтных двоичных матрицах, которые будут использоваться в дальнейшем. Рассмотрим матрицу, образованную циклическим сдвигом строки $a_0, a_1, \ldots, a_{n-1}$ на одну позицию. Подобная матрица называется циркулянтной или просто циркулянтом и имеет вид

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & \ldots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & a_4 & \ldots & a_{n-1} & a_0 \\ & & & \ldots & \ldots & & \\ a_{n-1} & a_0 & a_1 & a_2 & \ldots & a_{n-3} & a_{n-2} \end{pmatrix}. \tag{1}$$

В данной работе нас интересует случай, когда $a_i \in \mathbb{F}_2$, $i = 0, \ldots, n-1$.

**Утверждение 1.** Пусть дан двоичный вектор $(a_0, a_1, a_2, a_3, \ldots, a_{n-2}, a_{n-1})$ и вектор $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$, тогда

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & \ldots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & a_4 & \ldots & a_{n-1} & a_0 \\ & & & \ldots & \ldots & & \\ a_{n-1} & a_0 & a_1 & a_2 & \ldots & a_{n-3} & a_{n-2} \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \ldots \\ b_{n-1} \end{pmatrix} =$$
$$= \begin{pmatrix} b_0 & b_1 & b_2 & \ldots & b_{n-1} \\ b_{n-1} & b_0 & b_1 & \ldots & b_{n-2} \\ & & \ldots & & \\ b_1 & b_2 & b_3 & \ldots & b_0 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \ldots \\ a_{n-1} \end{pmatrix}.$$

***Доказательство.***

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & \dots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & a_4 & \dots & a_{n-1} & a_0 \\ & & & \dots & \dots & & \\ a_{n-1} & a_0 & a_1 & a_2 & \dots & a_{n-3} & a_{n-2} \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \dots \\ b_{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} b_0a_0 \oplus b_1a_1 \oplus b_2a_2 \oplus b_3a_3 \oplus \dots \oplus b_{n-1}a_{n-1} \\ b_0a_1 \oplus b_1a_2 \oplus b_2a_3 \oplus b_3a_4 \oplus \dots \oplus b_{n-1}a_0 \\ \dots \\ b_0a_{n-1} \oplus b_1a_0 \oplus b_2a_1 \oplus b_3a_2 \oplus \dots \oplus b_{n-1}a_{n-2} \end{pmatrix} =$$

$$= a_0 \begin{pmatrix} b_0 \\ b_{n-1} \\ \dots \\ b_1 \end{pmatrix} \oplus a_1 \begin{pmatrix} b_1 \\ b_0 \\ \dots \\ b_2 \end{pmatrix} \oplus a_2 \begin{pmatrix} b_2 \\ b_1 \\ \dots \\ b_3 \end{pmatrix} \oplus \dots \oplus a_{n-1} \begin{pmatrix} b_{n-1} \\ b_{n-2} \\ \dots \\ b_0 \end{pmatrix} =$$

$$= \begin{pmatrix} b_0 & b_1 & b_2 & \dots & b_{n-1} \\ b_{n-1} & b_0 & b_1 & \dots & b_{n-2} \\ & & \dots & & \\ b_1 & b_2 & b_3 & \dots & b_0 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_{n-1} \end{pmatrix}.$$

Утверждение 1 доказано. ■

Определим многочлен $\varphi_{\mathbf{a}}(x) = a_0 \oplus a_1 x \oplus a_2 x^2 \oplus \dots \oplus a_{n-1}x^{n-1} \in \mathbb{F}_2[x]$. Известно [7, 8], что для обратимости циркулянтной матрицы, образованной строкой $a_0, a_1, \dots, a_{n-1}$, необходимо и достаточно, чтобы многочлен $\varphi_{\mathbf{a}}(x)$ был взаимно прост с многочленом $x^n \oplus 1$: $\text{НОД}(\varphi_{\mathbf{a}}(x), x^n \oplus 1) = 1$.

Если вес вектора $a_0, a_1, \dots, a_{n-1}$ чётный, то $(x \oplus 1) \,|\, \text{НОД}(\varphi_{\mathbf{a}}(x), x^n \oplus 1)$, поэтому матрица (1) необратима.

**Утверждение 2.** Пусть $n = 2^t$ и $A$ — циркулянтная матрица размера $n \times n$, образованная строкой $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ нечётного веса. Тогда матрица $A$ обратима.

***Доказательство.*** Для обратимости матрицы $A$ необходимо и достаточно подтвердить взаимную простоту многочленов $x^{2^t} \oplus 1$ и $\varphi_{\mathbf{a}}(x)$. Поскольку $x^{2^t} \oplus 1 = (x \oplus 1)^{2^t}$, то $(x \oplus 1)$ — его единственный неприводимый делитель, и он не делит $\varphi_{\mathbf{a}}(x)$, поскольку у последнего нечётное число мономов, а значит, 1 не является его корнем. ■

## 4. Невозможные переходы разностей блоков для алгоритма КБ-256 и возможность изменения функции обратной связи

### 4.1. Максимальное число итераций для разности с вероятностью 1

Построение невозможных переходов разностей блоков базируется на наличии разностных соотношений, проходящих с вероятностью 1. Сформулируем очевидное утверждение, с помощью которого строятся невозможные переходы разностей блоков.

**Утверждение 3.** Пусть для алгоритма $F(x, K) = F_t(x, K)$ имеется пара разностных соотношений $\widehat{\alpha, \beta}^{F_i}$ и $\widehat{\gamma, \lambda}^{F_j}$ с вероятностью 1, $i + j < t$. Если разностное соотношение $\widehat{\beta, \gamma}^{F_{t-i-j}}$ является невозможным, то соотношение $\widehat{\alpha, \lambda}^{F_t}$ тоже невозможно.

В работе [5] для построения невозможных переходов разностей блоков найдено разностное соотношение с вероятностью 1 на шесть итераций алгоритма КБ-256 и ещё одно на семь итераций. Для построения этих соотношений использовано следующее

свойство: модульное сложение векторов со значащими старшими битами ведет себя как $\oplus$. Поэтому брались векторы, различающиеся лишь в старшем бите.

Разности с вероятностью 1 для алгоритма КБ-256 имеют следующий вид: на шесть итераций — $(0,[31],0,0,0,0,[31],0) \to ([31],0,0,[31],0,0,0,0)$; на семь итераций — $([31],[31],0,0,0,0,0,[31]) \to ([31],[31],[31],0,0,0,0,0)$. Поскольку для каждого блока разность появляется лишь в старшем бите, то сопоставим разностям 8-битные векторы: $(0,1,0,0,0,0,1,0) \to (1,0,0,1,0,0,0,0)$ и $(1,1,0,0,0,0,0,1) \to (1,1,1,0,0,0,0,0)$; таким образом, каждому биту соответствует разность в старшем бите подблока текста.

Укажем явно это соответствие. Пусть $\mathbf{a} = (a_0,\dots,a_7) \in V_8$ — 8-битный вектор, $\mathbf{a} = [i_1,\dots,i_l]$, $l \leqslant 8$. Этому вектору соответствует вектор разностей в старших битах подблоков $(0,\dots,0,\underbrace{[31]}_{i_1},0,\dots,0,\underbrace{[31]}_{i_2},\underbrace{\dots}_{\dots},\underbrace{[31]}_{i_l},0,\dots,0)$.

Поскольку сложение старших битов вектора ведёт себя как побитовое, для описания распространения разностей рассмотрим битовый вектор $\mathbf{a} = (a_0,\dots,a_7) \in V_8$ — разность в старших битах для входных блоков — и набор индексов для вычисления промежуточной суммы $\mathbf{m} = (0,1,0,1,1,0,1,1) \in V_8$. Следующая система задаёт вычисление разностей в каждом из блоков последовательно от итерации к итерации:

$$\begin{cases} a_0\cdot 0 \oplus a_1\cdot 1 \oplus a_2\cdot 0 \oplus a_3\cdot 1 \oplus a_4\cdot 1 \oplus a_5\cdot 0 \oplus a_6\cdot 1 \oplus a_7\cdot 1 = 0,\\ a_1\cdot 0 + a_2\cdot 1 + a_3\cdot 0 + a_4\cdot 1 + a_5\cdot 1 + a_6\cdot 1 + a_7\cdot 0 + a_0\cdot 1 = 0,\\ a_2\cdot 0 + a_3\cdot 1 + a_4\cdot 0 + a_5\cdot 1 + a_6\cdot 1 + a_7\cdot 0 + a_0\cdot 1 + a_1\cdot 1 = 0,\\ a_3\cdot 0 + a_4\cdot 1 + a_5\cdot 0 + a_6\cdot 1 + a_7\cdot 1 + a_0\cdot 0 + a_1\cdot 1 + a_2\cdot 1 = 0,\\ a_4\cdot 0 + a_5\cdot 1 + a_6\cdot 0 + a_7\cdot 1 + a_0\cdot 1 + a_1\cdot 0 + a_2\cdot 1 + a_3\cdot 1 = 0,\\ a_5\cdot 0 + a_6\cdot 1 + a_7\cdot 0 + a_0\cdot 1 + a_1\cdot 1 + a_2\cdot 0 + a_3\cdot 1 + a_4\cdot 1 = 0,\\ a_6\cdot 0 + a_7\cdot 1 + a_0\cdot 0 + a_1\cdot 1 + a_2\cdot 1 + a_3\cdot 0 + a_4\cdot 1 + a_5\cdot 1 = 0,\\ a_7\cdot 0 + a_0\cdot 1 + a_1\cdot 0 + a_2\cdot 1 + a_3\cdot 1 + a_4\cdot 0 + a_5\cdot 1 + a_6\cdot 1 = 1. \end{cases}$$

Перепишем систему в матричном виде:

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7\\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0\\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1\\ a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2\\ a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3\\ a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4\\ a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5\\ a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \begin{pmatrix} 0\\1\\0\\1\\1\\0\\1\\1 \end{pmatrix} = A\cdot\mathbf{m} = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\1 \end{pmatrix}. \tag{2}$$

Если системе (2) удовлетворяют вектор входных разностей и вектор для точек съёма промежуточной суммы, то данное заполнение даёт разностное соотношение с вероятностью 1 на семь итераций, поскольку сохранение сдвига нарушается впервые после седьмой итерации. Аналогично рассмотрим однородную систему

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 \\ a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 \\ a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = A \cdot \mathbf{m} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{3}$$

Матрица, удовлетворяющая системе (3), позволит построить разностное соотношение с вероятностью 1 на любое число итераций.

В работе [5] начальных заполнений (циркулянтных матриц), удовлетворяющих данной системе, не было найдено.

На основе утверждения 1 системы (2) и (3) могут быть переписаны в виде

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = M \cdot \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = M \cdot \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Матрица $M$ — циркулянт размера $8 \times 8$, образованный строкой нечётного веса.

Возможны следующие случаи для нечётного веса: 1, 3, 5, 7. По утверждению 2 все такие матрицы являются обратимыми. Значит, найдётся набор входных разностей $\mathbf{a}$, порождающий разностное соотношение на семь итераций, и не найдётся никакого, отличного от нулевого, вектора разностей $\mathbf{a}$, который можно протянуть на восемь итераций и, как следствие, на любое число итераций.

Следовательно, найденная в работе [5] разность с вероятностью 1 на семь итераций — максимальная по числу итераций.

### 4.2. Изменение выбора подблоков для вычисления промежуточной суммы

Рассмотрим битовый вектор $\mathbf{a} = (a_0, \ldots, a_7) \in V_8$ (разность в старших битах для входных блоков) и набор индексов для вычисления промежуточной суммы $\mathbf{m} = (m_0, m_1, \ldots, m_7) \in V_8$. Для каждого вектора $\mathbf{m}$ и каждого начального заполнения $\mathbf{a}$ проведена экспериментальная проверка максимальной длины разностного соотношения с вероятностью 1.

В результате экспериментов выяснилось, что для максимального числа итераций для разностного соотношения с вероятностью 1 возможны две ситуации: оно равно семи итерациям или не ограничено.

Объяснение данных результатов связано с разрешимостью систем

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 \\ a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 \\ a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \end{pmatrix} = A \cdot \mathbf{m} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{4}$$

или

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 \\ a_3 & a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 \\ a_4 & a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 \\ a_6 & a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_7 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{pmatrix} \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \end{pmatrix} = A \cdot \mathbf{m} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{5}$$

Если начальное заполнение и вектор точек съёма удовлетворяют системе (4), то это даёт разность с вероятностью 1 на семь итераций. Если начальное заполнение и вектор точек съёма удовлетворяют системе (5), то получим разностное соотношение с вероятностью 1 на любое число итераций.

По утверждению 1 системы (4) и (5) можно переписать в виде

$$\begin{pmatrix} m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 \\ m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 \\ m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 \\ m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = M \cdot \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}; \tag{6}$$

$$\begin{pmatrix} m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 \\ m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 \\ m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 \\ m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = M \cdot \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{7}$$

В зависимости от количества точек съёма (веса вектора $\mathbf{m}$) циркулянт $M$ или вырожденный (четное число единиц), или обратимый (нечетное число единиц). Если матрица $M$ обратима, то система (7) имеет только нулевое решение, а для системы (6) всегда найдётся решение.

Если матрица $M$ вырождена, иначе — имеет чётное число единиц в строках, то система (7) имеет не только нулевое решение. А система (6) может вообще не иметь решений, да и их поиск теряет смысл, ведь найдётся разность на любое число итераций.

Значит, любой вариант выбора точек съёма не уменьшит число итераций, на которое можно распространить разностное соотношение с вероятностью 1. Это демонстрирует неулучшаемость данной схемы с точки зрения построения невозможных переходов разностей блоков.

## 5. Обобщённая схема Фейстеля и поиск невозможных переходов разностей блоков

Рассмотрим обобщённую схему Фейстеля со следующим устройством итерационного отображения $G(X, K)$.

Входной блок $X \in V_{tn}$ делится на $t$ блоков по $n$ бит: $X = (X_0, X_2, \ldots, X_{t-1})$. Для вычисления функции обратной связи берётся сумма $\sigma$ некоторых блоков, это может быть как модульное сложение, так и покоординатная сумма по модулю 2. Введём $(m_0, m_1, \ldots, m_{t-1})$ — вектор из нулей и единиц, задающий, какие блоки $X_i$ берутся для суммы: $\sigma = \sum\limits_{i=0}^{t-1} m_i X_i$. Результат одной итерации зашифрования вычисляется по следующему правилу:

$$G\big((X_0, X_1, \ldots, X_{t-1}), K\big) = \big(X_1 \oplus \overline{m_1} f(\sigma, K_1), \ldots, X_{t-1} \oplus \overline{m_{t-1}} f(\sigma, K_{t-1}), X_0 \oplus \overline{m_0} f(\sigma, K_0)\big).$$

Здесь $f(\cdot\,, K)$ — отображение, которое при фиксированном значении $K$ является биективным по первому аргументу; последовательность $K_0, K_1, \ldots, K_{t-1}$ — итерационные ключи.

Нетрудно видеть, что рассуждения из п. 4 применимы и для данной схемы, а именно: поиск разностных соотношений с вероятностью 1 связан с разрешимостью систем

$$\begin{pmatrix} m_0 & m_1 & m_2 & m_3 & \ldots & m_{t-1} \\ m_{t-1} & m_0 & m_1 & m_2 & \ldots & m_{t-2} \\ \vdots & & & & & \\ m_1 & m_2 & m_3 & m_4 & \ldots & m_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = M \cdot \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} m_0 & m_1 & m_2 & m_3 & \ldots & m_{t-1} \\ m_{t-1} & m_0 & m_1 & m_2 & \ldots & m_{t-2} \\ \vdots & & & & & \\ m_1 & m_2 & m_3 & m_4 & \ldots & m_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = M \cdot \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

В работе [3] предложены несколько конструкций блочного алгоритма шифрования на основе обобщённой схемы Фейстеля, одна из них — с входным блоком на 512 бит. Одна итерация этого алгоритма изображена на рис. 2.

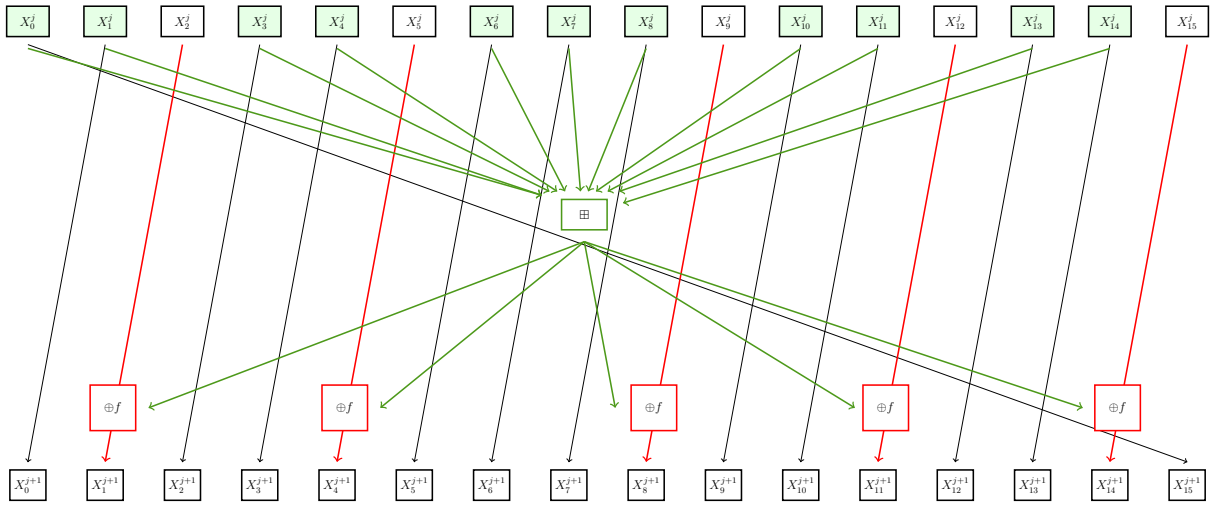

Рис. 2. Пример обобщённой схемы Фейстеля

В качестве функции $f$ изначально предполагалось использовать раундовую функцию алгоритма Магма [6]. У данного варианта алгоритма есть разностное соотношение с вероятностью 1 на 15 итераций, его вид приведён в таблице. Здесь $1$ — вектор из $V_{32}$, у которого 1 в старшем бите, а остальные равны нулю; $0$ — нулевой вектор из $V_{32}$.

| | |
|---|---|
| 0 | $(0,0,0,0,0,1,1,1,0,0,0,0,0,0,0,0)$ |
| 1 | $(0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0)$ |
| 2 | $(0,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0)$ |
| 3 | $(0,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0)$ |
| 4 | $(0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0)$ |
| 5 | $(1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0)$ |
| 6 | $(1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,1)$ |
| 7 | $(1,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1)$ |
| 8 | $(0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1)$ |
| 9 | $(0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0)$ |
| 10 | $(0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0)$ |
| 11 | $(0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0)$ |
| 12 | $(0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,0)$ |
| 13 | $(0,0,0,0,0,0,0,0,1,1,1,0,0,0,0,0)$ |
| 14 | $(0,0,0,0,0,0,0,1,1,1,0,0,0,0,0,0)$ |
| 15 | $(0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0)$ |

На основе этого соотношения можно утверждать, что существует невозможный переход разностей не менее чем на 32 итерации. Непосредственной проверкой можно убедиться, что разностное соотношение

$$(0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0) \;\to\; (0,0,0,0,0,1,1,1,0,0,0,0,0,0,0,0)$$

является невозможным для двух итераций алгоритма (см. рис. 2); по утверждению 3 оно невозможно для 32 итераций.

## Заключение

Наличие разностных соотношений с вероятностью 1 позволяет строить невозможные переходы разностей блоков. Поэтому чем большее число итераций может пройти

разность с вероятностью 1, тем на большее число итераций может быть распространён невозможный переход разностей блоков (утверждение 3).

По результатам исследования выяснилось, что для алгоритма КБ-256 при любом сочетании суммирующихся блоков на итерации всегда найдётся разностное соотношение с вероятностью 1 не менее чем на семь итераций. Таким образом показана конструктивная неулучшаемость в плане уменьшения максимального числа итераций, для которой найдётся разность с вероятностью 1.

Автор выражает благодарность А. А. Дмуху за помощь в постановке задачи и ценные рекомендации в процессе её решения.

## ЛИТЕРАТУРА

1. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // LNCS. 1999. V. 1592. P. 12–23.
2. *Knudsen L.* Deal — a 128-bit block cipher // Complexity. 1998. V. 258. No. 2.
3. *Fomichev V. M., Koreneva A. M., Miftakhutdinova A. R., et al.* Evaluation of the maximum performance of block encryption algorithms. // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 181–191.
4. *Fomichev V. M. and Koreneva A. M.* Encryption performance and security of certain wide block ciphers // J. Comput. Virol. Hack. Tech. 2020. V. 16. P. 197–216.
5. *Astrakhantsev R., Chuhno A., Dmukh A., et al.* Differences with high probability and impossible differentials for the KB-256 cipher // J. Comput. Virol. Hack. Tech. 2024. V. 20. P. 525–531.
6. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2018.
7. *Guan Ph. and He Y.* Exact results for deterministic cellular automata with additive rules // J. Stat. Phys. 1986. V. 43. P. 463–478.
8. *Bini D., Del Corso G. M., Manzini G., and Margara L.* Inversion of circulant matrices over $\mathbb{Z}_m$ // LNCS. 1998. V. 1443. P. 719–730.

## REFERENCES

1. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. LNCS, 1999, vol. 1592, pp. 12–23.
2. *Knudsen L.* Deal — a 128-bit block cipher. Complexity, 1998, vol. 258, no. 2.
3. *Fomichev V. M., Koreneva A. M., Miftakhutdinova A. R., et al.* Evaluation of the maximum performance of block encryption algorithms. Matematicheskie Voprosy Kriptografii, 2019, vol. 10, no. 2, pp. 181–191.
4. *Fomichev V. M. and Koreneva A. M.* Encryption performance and security of certain wide block ciphers. J. Comput. Virol. Hack. Tech., 2020, vol. 16, pp. 197–216.
5. *Astrakhantsev R., Chuhno A., Dmukh A., et al.* Differences with high probability and impossible differentials for the KB-256 cipher. J. Comput. Virol. Hack. Tech., 2024, vol. 20, pp. 525–531.
6. GOST 34.12-2018. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry [GOST 34.12-2018. Information Technology. Cryptographic Protection of Information. Block Ciphers]. Moscow, Standartinform, 2018.
7. *Guan Ph. and He Y.* Exact results for deterministic cellular automata with additive rules. J. Stat. Phys., 1986, vol. 43, pp. 463–478.
8. *Bini D., Del Corso G. M., Manzini G., and Margara L.* Inversion of circulant matrices over $\mathbb{Z}_m$. LNCS, 1998, vol. 1443, pp. 719–730.