# МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.2

## КРИТЕРИИ МАРКОВОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

О. В. Денисов

*ООО «Инновационные телекоммуникационные технологии», г. Москва, Россия*

Изучаются вероятностные модели блочных шифрсистем, в которых случайные раундовые ключи независимы и одинаково распределены. Они называются марковскими шифрами, если последовательность раундовых разностей образует простую однородную цепь Маркова. Уточнены и обобщены критерий и достаточное условие марковости моделей шифрсистем. Расширен класс марковских шифров, построенный в диссертации швейцарского учёного X. Lai. Получены достаточные условия, при которых формула для матриц вероятностей переходов разностей расширенного класса содержит тензорное произведение матриц вероятностей переходов S-блоков.

**Ключевые слова:** *марковские шифры, случайные подстановки, вероятности переходов разностей.*

DOI 10.17223/20710410/41/3

## CRITERIA FOR MARKOV BLOCK CIPHERS

O. V. Denisov

*Innovative Telecommunication Technologies, LLC, Moscow, Russia*

**E-mail:** denisovOleg@yandex.ru

We study probabilistic models of block ciphers with random independent identically distributed round keys. We call they by Markov ciphers if sequence of round differentials is a simple homogeneous Markov chain. Criteria and sufficient condition for this property are adjusted and generalized. Particularly, we prove that, for an iterative $r$-round block cipher with group operation on the set $\mathcal{X}$ of blocks and round function $g$, the following four conditions are equivalent: 1) for any plaintext of two blocks $(X, X^*)$, the sequence of random round differentials $\Delta X = X^* X^{-1}, \Delta X(1) = = X^*(1)X(1)^{-1}, \ldots, \Delta X(r) = X^*(r)X(r)^{-1}$ is a homogeneous Markov chain under any distribution of $(X, X^*)$; 2) for all $a \in \mathcal{X} \setminus \{e\}$, the distribution of $g(ax)g(x)^{-1}$ doesn't depend on $x \in \mathcal{X}$; 3) $\forall a \in \mathcal{X}\setminus\{e\}, x \in \mathcal{X}$ $(g(ax)g(x)^{-1} \sim g(aX)g(X)^{-1})$ under any distribution of $X$; 4) $\forall x \in \mathcal{X}$ $(g(\Delta X\, x)g(x)^{-1} \sim g(\Delta X\, X)g(X)^{-1})$ under any distribution of $(X, \Delta X)$. The class of Markov ciphers constructed in Lai's dissertation is expanded. We give sufficient conditions under which formula for the transition probabilities matrix of the expanded class contains tensor product of S-box transition probabilities matrices.

**Keywords:** *Markov ciphers, random permutations, transition probabilities of differentials.*

## Введение

Пусть на алфавите $\mathcal{X}$ входных и выходных блоков задана групповая операция $\odot$, $e \in \mathcal{X}$ — нейтральный элемент, $X^{-1}$ — обратный к элементу $X$ группы $(\mathcal{X}, \odot)$. Как принято в дифференциальном (разностном) анализе, величины вида $X_1 \odot X_2^{-1}$ будем называть *разностями* блоков $X_1, X_2$. Через $\mathcal{X}' = \mathcal{X} \setminus \{e\}$ обозначим множество «ненулевых» разностей, $M = |\mathcal{X}| - 1$ — его мощность. Через $S(\mathcal{X})$ обозначим множество всех подстановок на множестве $\mathcal{X}$.

Рассматривается итеративный $r$-раундовый алгоритм блочного шифрования (3), в котором раундовые ключи принимают значения из некоторого множества $\Gamma$, каждый набор раундовых ключей $\gamma \in \Gamma^r$ задает шифрующую подстановку $g_\gamma \in S(\mathcal{X})$. Шифруется двублочный текст $(X, X^*)$.

Будем работать в вероятностной модели такого случайного выбора текста и набора раундовых ключей, что

$$\text{открытый текст } (X, X^*) \text{ и набор } \gamma = (\gamma_1, \dots, \gamma_r) \text{ независимы;} \tag{1}$$

$$\text{ключи } \gamma_1, \dots, \gamma_r \text{ независимы и одинаково распределены.} \tag{2}$$

Тогда, как известно из курса теории вероятностей, случайные последовательности промежуточных блоков

$$\begin{gathered} X = X(0),\ X(1) = g_{\gamma_1}(X(0)), \dots, X(r) = g_{\gamma_r}(X(r-1)) = Y, \\ X^* = X^*(0),\ X^*(1) = g_{\gamma_1}(X(0)), \dots, X^*(r) = g_{\gamma_r}(X^*(r-1)) = Y^*, \end{gathered} \tag{3}$$

последовательность их пар

$$(X, X^*),\ (X(1), X^*(1)), \dots, (X(r), X^*(r)) = (Y, Y^*) \tag{4}$$

и последовательность промежуточных подстановок

$$g_{(\gamma_1,\dots,\gamma_t)} = g_{\gamma_1} \dots g_{\gamma_t},\ 1 \leqslant t \leqslant r,$$

являются простыми (далее рассматриваем только такие) однородными цепями Маркова. Но не всякая функция от последовательности состояний цепи Маркова (и, в частности, разность компонент пар) образует цепь Маркова. Поэтому содержательно следующее определение.

**Определение 1.** При условиях (1) и (2) будем говорить, что итеративный алгоритм шифрования (3) является *марковским шифром* (относительно операции $\odot$ при заданных распределениях входной пары $(X, X^*)$ и раундового ключа $\gamma_1$), если последовательность случайных *раундовых разностей*

$$\Delta X = X^* X^{-1},\ \Delta X(1) = X^*(1) X(1)^{-1},\ \dots,\ \Delta X(r) = X^*(r) X(r)^{-1} \tag{5}$$

образует однородную цепь Маркова.

В (5) (и далее там, где это удобно) знак операции $\odot$ опущен для краткости.

### 1. Критерии марковости последовательности раундовых разностей

Обозначим для краткости $g = g_{\gamma_1}$; распределение этой случайной подстановки совпадает с распределением остальных раундовых подстановок согласно (2).

В следующей теореме доказан критерий (7), близкий к условиям [1, 2], и новые критерии (8), (9), которые можно назвать *условиями инвариантности распределения разностей* подстановки $g$ относительно фиксации входного блока и/или входной разности. Пункт 1 доказательства основан на идее [2] использования теоремы [3] об укрупнении состояний цепей Маркова.

**Теорема 1.** Пусть выполнены условия (1) и (2), $\mathbb{P} = \|p_{a,b}\|_{a,b\in\mathcal{X}'}$ — фиксированная стохастическая матрица. Тогда эквивалентны следующие четыре условия:

$$\begin{gathered}\text{последовательность (5) образует однородную цепь Маркова}\\ \text{с матрицей вероятностей переходов } \mathbb{P} \text{ при любом распределении } (X, X^*);\end{gathered} \tag{6}$$

$$\text{для всех } a \in \mathcal{X}' \text{ распределение } g(ax)g(x)^{-1} \text{ не зависит от выбора } x \in \mathcal{X}; \tag{7}$$

$$\forall a \in \mathcal{X}', x \in \mathcal{X}\ (g(ax)g(x)^{-1} \sim g(aX)g(X)^{-1}) \text{ при любом распределении } X; \tag{8}$$

$$\forall x \in \mathcal{X}\ (g(\Delta X\, x)g(x)^{-1} \sim g(\Delta X\, X)g(X)^{-1}) \text{ при любом распределении } (X, \Delta X). \tag{9}$$

При этом матрица $\mathbb{P}$ является дважды стохастической, $p_{a,b} = \mathsf{P}\{g(ax)g(x)^{-1} = b\}$, $a, b \in \mathcal{X}'$.

***Доказательство.***

1. Докажем эквивалентность условий (6) и (7). Условие (6) означает, что цепь Маркова (4) допускает такое укрупнение состояний, при котором все пары $(x, x^*)$ с одинаковой разностью $a \in \mathcal{X}'$ объединяются в одно состояние $a' = \{(x, ax) : x \in \mathcal{X}\}$, состоящее из $|\mathcal{X}|$ пар. Заметим, что $a'$ является смежным классом группы $(\mathcal{X} \times \mathcal{X}, \odot)$ (являющейся прямым произведением двух групп) по её «диагональной» подгруппе $\mathcal{X}_1 = \{(x, x) : x \in \mathcal{X}\}$, поскольку $a' = (e, a) \odot \mathcal{X}_1$.

По теореме 6.3.2 [3, с. 160] такое укрупнение возможно при любом начальном распределении исходной цепи и даёт цепь Маркова с матрицей переходных вероятностей $\mathbb{P}$ тогда и только тогда, когда при любых фиксированных $a, b \in \mathcal{X}'$ вероятности

$$p_{(x,x^*),b'} = \sum_{(y,y^*)\in b'} \mathsf{P}\{X(1) = y, X^*(1) = y^* \,|\, X = x, X^* = x^*\}$$

одинаковы для всех пар $(x, x^*) \in a'$ и равны $p_{a,b}$. Но для таких пар $x^* = ax^{-1}$ и можно преобразовать

$$p_{(x,x^*),b'} = \sum_{y\in\mathcal{X}} \mathsf{P}\{g(X) = y, g(\Delta X)g(X)^{-1} = b \,|\, X = x, \Delta X = a\} = \mathsf{P}\{g(ax)g(x)^{-1} = b\},$$

где в последнем переходе использовано условие независимости (1).

Итак, цепь Маркова (4) допускает укрупнение состояний при любом распределении $(X, X^*)$ тогда и только тогда, когда правые части последнего равенства одинаковы и равны $p_{a,b}$ для всех $x \in \mathcal{X}$, т. е. выполнено условие (7).

2. Справедливо следующее утверждение: если случайная величина $\xi$ является функцией от случайного вектора $\eta$ и, возможно, некоторых других случайных величин, то условие инвариантности условных распределений $(\xi \,|\, \eta = c)$ относительно всех возможных фиксаций вектора $\eta$ эквивалентно тому, что распределение $\xi$ одинаково при любом распределении $\eta$. Действительно, необходимость условия инвариантности относительно фиксаций очевидна, а достаточность легко вытекает из формулы полной вероятности

$$\mathsf{P}\{\xi = b\} = \sum_c \mathsf{P}\{\eta = c\}\, \mathsf{P}\{\xi = b|\, \eta = c\} = \mathsf{P}\{\xi = b|\, \eta = c_0\}$$

для любого фиксированного $c_0$ из множества значений $\eta$.

Применяя это утверждение к случайной величине $\xi = g(aX)g(X)^{-1}$ при $\eta = X$, получаем равносильность (7) и (8). Применяя это утверждение к случайной величине $\xi = g(\Delta X\, X)g(X)^{-1}$ при $\eta = \Delta X$, получаем равносильность (7) и (9).

3. Полагая $x = e$ в (7), получаем формулу

$$p_{a,b} = \mathsf{P}\left\{g(a)g(e)^{-1} = b\right\}. \tag{10}$$

Из неё легко вытекает дважды стохастичность матрицы $\mathbb{P}$:

$$\sum_{a\in\mathcal{X}'} p_{a,b} = \sum_{a\in\mathcal{X}'} \mathsf{P}\{b\,g(e) = g(a)\} = \mathsf{P}\left\{b\,g(e) \in \mathcal{X}\setminus\{g(e)\}\right\},$$

что равно 1, поскольку $b\,g(e) \neq g(e)$. Теорема 1 доказана. ■

Рассмотрим класс шифров, у которых раундовый ключ может быть разделён на две независимые части $\gamma = (\delta, \varepsilon)$, первая из которых равномерно распределена на $\mathcal{X}$ и накладывается на шифруемый блок в соответствии с групповой операцией, а вторая определяет применяемую случайную подстановку $f$:

$$\gamma = (\delta,\varepsilon),\ g_\gamma(x) = f_\varepsilon(x\odot\delta), \quad \delta \sim U(\mathcal{X}) \text{ и } \varepsilon \text{ независимы}. \tag{11}$$

Схема шифрования пар блоков такими раундовыми подстановками иллюстрируется рис. 1.

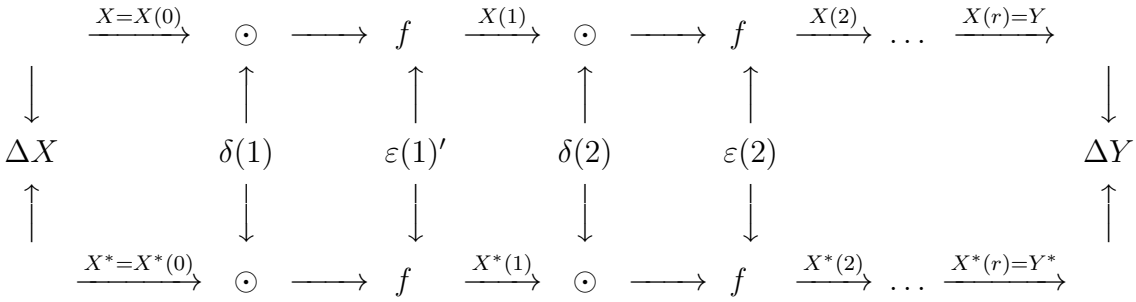


Рис. 1. Схема шифрования [4], обеспечивающая марковость алгоритма

Заметим, что схемы шифрования, использующие раундовые подстановки вида (11), близки к так называемым «key-alternating» шифрам, активно изучаемым в настоящее время.

**Следствие 1.** Пусть выполнены условия (1) и (2). Тогда условие (11) является достаточным для каждого из условий (6)–(9).

***Доказательство.*** Согласно теореме 1, достаточно доказать, что условие (11) обеспечивает условие (7) инвариантности распределения разностей $g_\gamma$ относительно фиксации входных блока и разности. Действительно, так как при любом $x \in \mathcal{X}$ случайная величина $y = x\delta$ также имеет равномерное распределение на $\mathcal{X}$ и не зависит от случайной подстановки $f_\varepsilon$, то распределение

$$g_\gamma(ax)g_\gamma(x)^{-1} = f_\varepsilon(ax\delta)f_\varepsilon(x\delta)^{-1} = f_\varepsilon(ay)f_\varepsilon(y)^{-1}$$

определяется распределением $f_\varepsilon$ и значением $a$. ■

Заметим, что кроме случайных подстановок вида (11) условию (8) удовлетворяет равномерно распределённая подстановка $\sigma \sim U(S(\mathcal{X}))$, поскольку для неё распределение разности также не зависит от $x \in \mathcal{X}$ и даже от $a \in \mathcal{X}'$:

$$\mathsf{P}\{\sigma(ax)\sigma(x)^{-1}=b\}=\sum_{y\in\mathcal{X}}\mathsf{P}\{\sigma(ax)\sigma(x)^{-1}=b,\,\sigma(x)=y\}=$$
$$=\sum_{y\in\mathcal{X}}\mathsf{P}\{\sigma(x)=y,\sigma(ax)=by\}=(M+1)\frac{1}{(M+1)M}=\frac{1}{M}.$$

Обсудим возможную практическую пользу от формулы (10).

Начнем с *автономной вероятностной модели*: пусть $\mathscr{K}$ — множество всех ключей шифрования произвольной блочной шифрсистемы с некоторым заданным на нём вероятностным распределением. Это распределение при заданном алгоритме развёртывания ключа (АРК) индуцирует некоторое распределение на множестве $\Gamma^r$ всех раундовых ключей, что с учётом распределения входной пары блоков позволяет найти матрицу $\mathbb{P}^{(r)}$ вероятностей переходов разностей (5) за $r$ раундов. Для реализации разностной атаки различения с фиксированной входной разностью $a$ требуется знание строки $\mathbb{P}_a^{(r)}$. Временная сложность метода вычисления $\mathbb{P}_a^{(r)}$ путём перебора ключей шифрования и вычисления переходов за $r$ раундов всех пар блоков с фиксированной разностью $a$ близка к сложности

$$|\mathscr{K}|(M+1)\odot 2r \tag{12}$$

операций вычисления значений раундовых подстановок.

Эта величина превосходит сложность тотального опробования, и в ряде работ по разностному анализу (в основном начиная с [5, 6]) рассматриваются *неавтономные вероятностные модели* шифрсистем, где АРК отсутствует, и раундовые ключи считаются независимыми одинаково распределёнными случайными величинами, т. е. выполняется условие (2). Марковские шифры удобны тем, что для них $\mathbb{P}^{(r)}=\mathbb{P}^r$ и сложность вычисления $\mathbb{P}^{(r)}$ близка к сложности вычисления $\mathbb{P}$, которая, согласно (13), меньше (12) примерно в $2r|\mathscr{K}|/|\Gamma|$ раз.

В следующей за [6] пионерской работе [1] перед теоремой 3 приведена («The $(i,j)$ entry in $\Pi$ is $\mathsf{P}\{\Delta Y(1)=\alpha_j\mid\Delta X=\alpha_i\}$») фактически формула (в наших обозначениях) $p_{a,b}=\mathsf{P}\{g(aX)g(X)^{-1}=b\}$ для элементов $\mathbb{P}$. Вычисление по ней фиксированной строки $\mathbb{P}_a$ может быть осуществлено перебором всех $x\in\mathcal{X}$, $\gamma\in\Gamma$ и добавлением произведений $\mathsf{P}\{X=x\}\,\mathsf{P}\{\gamma_1=\gamma\}$ к счётчику, соответствующему элементу $p_{a,b}$, $b=g_\gamma(x)^{-1}g_\gamma(xa)$. Для этого надо

$$(M+1)|\Gamma| \tag{13}$$

раз произвести две операции вычисления значения раундовой подстановки, две групповые операции и одну операцию вычисления обратного элемента в группе $(\mathcal{X},\odot)$. Осталось заметить, что для вычисления $\mathbb{P}_a$ по формуле (10) аналогичным способом достаточно $|\Gamma|$ операций вычисления значения раундовой подстановки и операций $\odot$, что примерно в $2M$ раз меньше сложности вычисления по формуле [1].

## 2. Шифрование параллельным набором S-боксов и подстановкой

Рассмотрим практически важный подкласс класса (11) марковских шифров, шифрование в перемешивающем слое которого осуществляется параллельным набором S-боксов, а затем действует подстановка $\pi$:

$$\begin{gathered}g_\gamma(x)=\pi\left(f_{1,\varepsilon_1}(x_1\odot_1\delta_1),\ldots,f_{m,\varepsilon_m}(x_m\odot_m\delta_m)\right),\\ \gamma=(\delta,\varepsilon),\ \delta=(\delta_1,\ldots,\delta_m),\ \varepsilon=(\varepsilon_1,\ldots,\varepsilon_m),\\ x=(x_1,\ldots,x_m)\in\mathcal{X}=\mathcal{X}_1\times\ldots\times\mathcal{X}_m,\end{gathered} \tag{14}$$

где $i$-й S-бокс действует на множестве $\mathcal{X}_i$, $1 \leqslant i \leqslant m$, и выбирается случайно (в общем случае) из некоторого фиксированного набора функций $(f_{i,j} : \mathcal{X}_i \to \mathcal{X}_i, j \in J_i)$, $J_i$ — некоторое множество индексов. В этом случае $(\mathcal{X}, \odot)$ — прямое произведение групп $(\mathcal{X}_1, \odot_1), \ldots, (\mathcal{X}_m, \odot_m)$.

Здесь в следующей формуле для матрицы вероятностей переходов разностей возникает тензорное произведение матриц вероятностей переходов разностей меньшей размерности.

**Теорема 2.** Пусть при условиях (1), (2) в каждом раунде (14) компоненты $\delta_1, \ldots, \delta_m$, $\varepsilon_1, \ldots, \varepsilon_m$ раундового ключа $\gamma$ независимы, $\delta_i \sim U(\mathcal{X}_i)$, $1 \leqslant i \leqslant m$, подстановка $\pi$ является гомоморфизмом группы $(\mathcal{X}, \odot)$. Тогда при любом распределении $(X, X^*)$ последовательность (5) образует однородную цепь Маркова с множеством состояний $\mathcal{X}$ и дважды стохастической матрицей

$$\mathbb{P} = (\mathbb{P}_1 \otimes \ldots \otimes \mathbb{P}_m)\Pi, \quad \mathbb{P}_i = \|p_{a,b}^{(i)}\|_{a,b \in \mathcal{X}_i},\ 1 \leqslant i \leqslant m,$$

где $\Pi$ — матрица подстановки $\pi$; вероятности $p_{a,b}^{(i)} = \mathsf{P}\{f_{i,\varepsilon_i}(a \odot_i x) f_{i,\varepsilon_i}(x)^{-1} \odot_i = b\}$ вычислены в предположении независимости $x \sim U(\mathcal{X}_i)$ от $\varepsilon_i$.

***Доказательство.*** Положим $f_\gamma(x) = \pi\left(f_{1,\varepsilon_1}(x_1), \ldots, f_{m,\varepsilon_m}(x_m)\right)$. Тогда $g_\gamma(x) = f_\gamma(x \odot \delta)$ и выполнено условие (11), поскольку, согласно условию теоремы, случайные векторы $\delta \sim U(\mathcal{X})$ и $\varepsilon$ независимы.

Поэтому из следствия 1 и теоремы 1 получаем, что последовательность разностей образует однородную цепь Маркова с дважды стохастической матрицей переходных вероятностей и множеством состояний $\mathcal{X} \setminus \{e\}$, $e = (e_1, \ldots, e_m)$, $e_i$ — нейтральные элементы групп $\mathcal{X}_i$. Нейтральный элемент $e$ образует одноэлементный класс существенных состояний, и добавление его в множество состояний приводит к появлению соответствующего блока единичного размера на диагонали $\mathbb{P}$, не влияя на дважды стохастичность матрицы.

Найдём переходные вероятности. Для $a = (a_1, \ldots, a_m) \in \mathcal{X}$ и $b' = (b_1, \ldots, b_m) = \pi^{-1}(b) \in \mathcal{X}$ — прообраза блока $b$ относительно действия $\pi$ — имеем с учётом гомоморфности $\pi$

$$g_\gamma(ax) g_\gamma^{-1}(x) = \pi\left(f_\gamma(ax\delta)\right) \pi\left(f_\gamma(x\delta)\right)^{-1} = \pi\left(f_\gamma(ax\delta) f_\gamma(x\delta)^{-1}\right).$$

Отсюда с учётом независимости случайных векторов $(\delta_i, \varepsilon_i)$, $1 \leqslant i \leqslant m$, получаем

$$p_{a,b} = \mathsf{P}\left\{f_\gamma(ax\delta) f_\gamma(x\delta)^{-1} = b'\right\} =$$
$$= \prod_{1 \leqslant i \leqslant m} \mathsf{P}\left\{f_{i,\varepsilon_i}(a_i \odot_i x_i \odot_i \delta_i) f_{i,\varepsilon_i}(x_i \odot_i \delta_i)^{-1} = b_i\right\} = p_{a_1,b_1}^{(1)} \ldots p_{a_m,b_m}^{(m)}.$$

Теорема 2 доказана. ■

Рассмотрим случай, когда все компонентные группы одинаковы, т. е. $(\mathcal{X}, \odot)$ — прямое произведение $m$ групп $(\mathcal{X}_1, \odot)$, S-боксы выбираются из набора $(f_j : \mathcal{X}_1 \to \mathcal{X}_1, j \in J)$:

$$g_\gamma(x) = \pi\left(f_{\varepsilon_1}(\delta_1 \odot x_1), \ldots, f_{\varepsilon_m}(\delta_m \odot x_m)\right), \quad x = (x_1, \ldots, x_m) \in \mathcal{X} = \mathcal{X}_1^m. \tag{15}$$

Если при этом индексы выбора одинаково распределены, то очевидно, что тензорное произведение матриц становится тензорной степенью одной матрицы.

**Следствие 2.** Пусть при условиях (1) и (2) в каждом раунде (15) раундовый ключ $\gamma$ состоит из независимых в совокупности случайных величин $\delta_1, \ldots, \delta_m, \varepsilon_1, \ldots, \varepsilon_m$, где $\delta_i \sim U(\mathcal{X}_1)$, а $\varepsilon_i$ одинаково распределены. Пусть также подстановка $\pi$ с матрицей $\Pi$ является гомоморфизмом группы $(\mathcal{X}, \odot)$. Тогда при любом распределении $(X, X^*)$ последовательность (5) образует однородную цепь Маркова с дважды стохастической матрицей

$$\mathbb{P} = \mathbb{P}_1^{[m]}\Pi, \quad \mathbb{P}_1 = \| \mathsf{P}\{f_{\varepsilon_1}(ax) f_{\varepsilon_1}(x)^{-1} = b\|_{a,b\in\mathcal{X}_1},$$

где вероятности вычисляются в предположении независимости $x \sim U(\mathcal{X}_1)$ и $\varepsilon_1$.

Отметим, что если в (15) операция $\odot$ — сложение по модулю 2, то $\pi$ является гомоморфизмом как в SP-сети, где $\pi$ выбирается из группы перестановок координат векторов, так и в XSL-сети, где $\pi$ выбирается из группы невырожденных линейных преобразований двоичных векторов.

Прокомментируем теорему 2. Известно [6, следствие 1], что при шифровании набором параллельных S-боксов и покоординатном аддитивном наложении раундового ключа вероятность перехода разности равна произведению вероятностей переходов её составных частей. Другими словами, матрица вероятностей перехода разностей при таком шифровании является тензорным произведением соответствующих матриц переходов частей разностей, соответствующих S-боксам [2; 7, с. 11]. Но при этом были сформулированы не все вероятностные условия (в частности, не было условия (1)), при которых такая матрица является матрицей вероятностей переходов разностной цепи Маркова; в теореме 2 этот недочёт устранён. С другой стороны, часть ключа, управляющая выбором индексов S-боксов, либо отсутствовала [7] (и тогда этот набор постоянен в раунде), либо считалась равномерно распределённой [4]. Теорема 2 показывает, что условие равномерной распределённости необязательно.

## 3. Обсуждение результатов

### 3.1. Об определениях марковского шифра

В [1] шифр называется марковским, если для всех $a, b \in \mathcal{X}'$

$$\begin{gathered}\text{при равномерном распределении } \gamma \\ \mathsf{P}\left\{g_\gamma(\Delta X\, X) g_\gamma(X)^{-1} = b \mid \Delta X = a,\, X = x\right\} \text{ не зависит от выбора } x \in \mathcal{X}.\end{gathered} \tag{16}$$

Заметим, что при условии (1) независимости входных блоков и раундовых ключей вторая строка условия (16) становится условием (7).

Доказано [1, теорема 2], что из (16) при условии (2) следует марковость последовательности разностей (5). Но в формулировке и в доказательстве теоремы имеются некоторые изъяны. В формулировке нет условия (1), без которого в общем случае даже последовательность пар блоков (4) не является цепью Маркова. В доказательстве показана марковость лишь отрезка из первых трёх разностей, не обоснована возможность исключения условия $\Delta X = \alpha$ при переходе от строки 3 к строке 4 в цепочке равенств. В тезисах [8] указан ещё один некорректный переход в доказательстве теоремы 2 [1].

В работе [2] выбран другой подход к доказательству марковости, основанный на теореме 6.3.2 [3] о возможности укрупнения состояний цепи Маркова, что позволило фактически доказать необходимость и достаточность условия (16) для марковости (5). В теореме 1 данной работы установлено, что доказательство [2] может быть проведено

в условиях, когда раундовые ключи могут выбираться не обязательно равновероятно. Но для получения критерия условие марковости последовательности разностей должно быть усилено требованием его выполнения при любом распределении входной пары блоков, иначе остаётся потенциальная возможность слабого укрупнения состояний [3, с. 169]. Доказанная дважды стохастичность $\mathbb{P}$ равносильна установленной в теореме 2 [1] стационарности равномерного распределения разностей. Заметим, что в нашей работе в качестве определения марковского шифра выбрано условие марковости (5) как более естественное по сравнению с близким к нему условием (16).

Достаточное условие (11) нашей работы является ослаблением условия [4, теорема 6], поскольку не требует равномерности распределения второй части раундового ключа. При этом доказательство его достаточности значительно проще доказательства теоремы 6 [4, с. 44]. До работы [4] марковость моделей шифрсистем доказывалась лишь в частных случаях для DES [6, лемма 1, теорема 1], PES [1, лемма 1], а также для шифрсистемы IPES, позже названной IDEA [4, с. 57]. Заметим, что условие (11) позволяет рассматривать другие вероятностные модели IDEA, в которых часть $(Z_5^{(1)}, Z_6^{(1)})$ [4, с. 65] раундового ключа не обязательно равномерно распределена, что может способствовать построению атак на слабые части ключа.

### 3.2. О критике марковской модели

Марковская модель блочных шифрсистем активно используется в англоязычной литературе с начала 1990-х гг. Примерно с 2006 г. интерес к ней стали проявлять украинские авторы [9 – 11], а в последние годы и российские. Вместе с тем имеются и критики этой модели, поскольку она, естественно, далека от совершенства. Они обычно выдвигают следующий аргумент:

«в реальности ключ всегда один и фиксирован, а не случаен». (17)

Приведём контраргументы.

1. Существует ряд ситуаций, в которых наблюдаются несколько шифртекстов, выработанных на разных ключах шифрования, например:

а) ключи получены из одного долговременного и различных разовых ключей;
б) ключи получены из фиксированного ключа и различных известных инициализирующих векторов (tweakable ciphers);
в) связанные ключи.

2. При некоторых алгоритмах развертывания ключа раундовые ключи, полученные на первых раундах, слабо зависимы, т. е. они близки к случайным независимым равновероятным векторам при случайном равновероятном выборе ключа шифрования. Модель случайного выбора ключа позволяет привлекать аппарат теории вероятностей для изучения характеристик «типичной» случайной подстановки, реализуемой блочной шифрсистемой, а также для изучения распределения вероятностей отклонений от таких характеристик.

3. Очевидно, аргумент (17) относится не к марковским шифрам как таковым, а вообще к неавтономным вероятностным моделям блочных шифрсистем. Но, например, в теории поточных шифрсистем давно используется и не вызывает возражений аналогичная модель для фильтрующего генератора, когда линейная рекуррентная последовательность, определяемая ключевым начальным заполнением, заменяется на последовательность независимых равновероятных битов. Для блочных шифрсистем увеличивается только размерность задачи и последовательность раундовых ключей,

определяемая ключом шифрования, заменяется на последовательность независимых равновероятных двоичных векторов.

Теория марковских шифров, как уже сказано выше, всего лишь изучает условия, при которых пары шифруемых блоков могут быть укрупнены в их разности с сохранением марковского свойства, которое даёт затем удобное равенство Колмогорова — Чепмена $\mathbb{P}^{(r)} = \mathbb{P}^r$ для матрицы переходных вероятностей за $r$ тактов.

Подводя итог, перечислим достоинства (+) неавтономных моделей и некоторые их недостатки (−) как естественные продолжения достоинств:

(+) возможность исследования вероятностей переходов блоков и пар блоков за $r$ раундов методами цепей Маркова, простое вычисление $\mathbb{P}^{(r)} = \mathbb{P}^r$; (−) возникновение вопроса об адекватности модели;

(+) результаты анализа устойчивы к модификации АРК; (−) теряется информация о возможной связи между раундовыми ключами;

(+) в марковских алгоритмах шифрования: возможность сокращения в два раза размерности состояния при переходе в неавтономной модели от пар блоков к их разностям.

Автор выражает признательность Б. А. Погорелову за постановку задачи и внимание к работе и Ф. М. Малышеву, чьи замечания способствовали существенному упрощению формулировок и доказательств результатов.

## ЛИТЕРАТУРА

1. *Lai X., Massey J., and Murphy S.* Markov ciphers and differential cryptanalysis // Eurocrypt-1991. LNCS. 1991. V. 547. P. 17–38.
2. *Погорелов Б. А., Пудовкина М. А.* Разбиения на биграммах и марковость алгоритмов блочного шифрования // Математические вопросы криптографии. 2017. Т. 8. Вып. 1. С. 107–142.
3. *Кемени Дж., Снелл Дж.* Конечные цепи Маркова. М.: Наука, 1970. 271 с.
4. *Lai X.* On the Design and Security of Block Ciphers: dissertation for the degree of Doctor of Technical Sciences. Swiss Federal Institute of Technology, Zurich, 1992. 118 p.
5. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // CRYPTO-1990. LNCS. 1991. V. 537. P. 2–21.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. No. 1. P. 3–72.
7. *Глухов М. М.* О рассеивающих линейных преобразованиях для блочных шифрсистем // Математические вопросы криптографии. 2011. Т. 2. Вып. 2. С. 5–40.
8. *Дрелихов В. О., Никифоров М. С.* О марковских свойствах усредненных разностных характеристик итеративных блочных шифров // Тез. докл. на конф. РУСКРИПТО, 2017. `www.ruscrypto.ru/accociation/archive/rc2017.html`
9. *Алексейчук А. Н.* Верхние границы параметров, характеризующих стойкость немарковских блочных шифров относительно методов разностного и линейного криптоанализа // Науково-технічний журнал «Захист інформації». 2006. Вып. 3. С. 20–28.
10. *Ковальчук Л. В.* Обобщенные марковские шифры: построение оценок практической стойкости к дифференциальным атакам // Сб. материалов 2-й Междунар. научн. конф. по проблемам безопасности и противодействия терроризму, 25–26 октября 2006 г. М.: МЦНМО, 2006.
11. *Лисицкая И. В., Долгов В. И.* Блочные симметричные шифры и марковские процессы // Прикладная радиоэлектроника. 2012. Т. 11. Вып. 2. С. 137–143.

REFERENCES

1. *Lai X., Massey J., and Murphy S.* Markov ciphers and differential cryptanalysis. Eurocrypt-1991, LNCS, 1991, vol. 547, pp. 17–38.
2. *Pogorelov B. A. and Pudovkina M. A.* Razbieniya na bigrammah i markovost' algoritmov blochnogo shifrovaniya [Partitions on bigrams and Markov property of block ciphers]. Matematicheskie Voprosy Kriptografii, 2017, vol. 8, iss. 1, pp. 107–142. (in Russian)
3. *Kemeny J. G. and Snell J. L.* Finite Markov Chains. The University Series in Undergraduate Mathematics. Princeton, Van Nostrand, 1960. 271 p.
4. *Lai X.* On the Design and Security of Block Ciphers: dissertation for the degree of Doctor of Technical Sciences. Swiss Federal Institute of Technology, Zurich, 1992. 118 p.
5. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems. CRYPTO-1990, LNCS, 1991, vol. 537, pp. 2–21.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems. J. Cryptology, 1991, vol. 4, no. 1, pp. 3–72.
7. *Gluhov M. M.* O rasseivayushchih linejnyh preobrazovaniyah dlya blochnyh shifrsistem [On mixing linear transforms for block ciphers]. Matematicheskie Voprosy Kriptografii, 2011, vol. 2, iss. 2, pp. 5–40. (in Russian)
8. *Drelikhov V. O. and Nikiforov M. S.* O markovskih svojstvah usrednennyh raznostnyh harakteristik iterativnyh blochnyh shifrov [On Markov properties of averaged difference characteristics of iterative block ciphers]. Proc. RUSCRIPTO-2017, `www.ruscrypto.ru/accociation/archive/rc2017.html` (in Russian)
9. *Aleksejchuk A. N.* Verhnie granicy parametrov, harakterizuyushchih stojkost' nemarkovskih blochnyh shifrov otnositel'no metodov raznostnogo i linejnogo kriptoanaliza [Upper limits of parameters characterizing the stability of non-Markov block ciphers with respect to the methods of difference and linear cryptanalysis]. Naukovo-tekhnichnij zhurnal «Zahist Informacii», 2006, iss. 3, pp. 20–28. (in Russian)
10. *Koval'chuk L. V.* Obobshchennye markovskie shifry: postroenie ocenok prakticheskoj stojkosti k differencial'nym atakam [Generalized Markov ciphers: construction of estimates of practical resistance to differential attacks]. Proc. 2nd Intern. Conf. on Security and Counter-Terrorism, October 25–26, 2006. Moscow, MCCME Publ., 2006. (in Russian)
11. *Lisickaya I. V. and Dolgov V. I.* Blochnye simmetrichnye shifry i markovskie processy [Block symmetric ciphers and Markov processes]. Prikladnaya Radioehlektronika, 2012, vol. 11, iss. 2, pp. 137–143. (in Russian)