Math-Net.Ru

Общероссийский математический портал

В. О. Дрелихов, Вероятностные свойства статистических связей между входом и выходом марковского итеративного шифра с раундовыми отображениями на абелевых группах, *Матем. вopr. криптогр.*, 2021, том 12, выпуск 1, 59–82

DOI: <https://doi.org/10.4213/mvk348>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.135.184

26 апреля 2023 г., 13:53:41

**Вероятностные свойства статистических связей
между входом и выходом марковского итеративного
шифра с раундовыми отображениями
на абелевых группах**

В. О. Дрелихов

АО «ИТМиВТ», Москва

Получено 15.V.2020

Аннотация. Исследуются статистические связи между входом и выходом в модели итеративного шифра, в которой раундовые ключи — независимые случайные величины, раундовые преобразования действуют на абелевых группах и зависят от раундового ключа и номера раунда. Если вход и выход шифра равновероятны, то статистические связи имеют смысл коэффициентов корреляции между значениями характеров. Показано, что для такой модели шифра матрица вторых моментов рассматриваемых характеристик равна произведению матриц, соответствующих раундовым отображениям. Получены верхние и нижние оценки математических ожиданий абсолютных значений исследуемых характеристик.

Ключевые слова: итеративный шифр, марковские модели, отображения абелевых групп, вероятностные связи

Probabilistic properties of statistical dependencies between input and output of Markovian iterative cipher with round transformations on Abelian groups

V. O. Drelikhov

JSC «IPMCE», Moscow

Abstract. We investigate the statistical dependencies between the input and output of an iterative cipher model, in which round keys are independent random variables, round transformations act on Abelian groups and depend on the round key and the round number. If the input and output of the cipher are uniformly distributed, then the statistical dependencies correspond the correlation coefficients between values of the characters. It is shown that for a cipher model with Markovian round mappings on Abelian groups the matrix of the second moments of the considered characteristics is equal to the product of the corresponding matrices constructed for round

mappings. Upper and lower estimates for the expectations of absolute values of studied characteristics are obtained.

Keywords: iterative cipher, Markovian models, mapping of Abelian groups, statistical dependencies

Введение

В ряде задач теоретической криптографии исследуется поведение статистических характеристик, связывающих вход и выход итеративного алгоритма шифрования. В случае когда раундовые отображения действуют на абелевых группах, например на группах типа Z_2^n , в качестве статистических характеристик рассматриваются коэффициенты корреляции между значениями характеров входа и выхода итеративного шифра (либо его части, не содержащей начальных и финальных преобразований).

Пусть $G^{(0)}, \dots, G^{(m)}$ — конечные абелевы группы, $K^{(0)}, \dots, K^{(m-1)}$ — конечные множества, $m \in \mathbb{N}$. Для заданных семейств $F^{(t)}$ раундовых отображений $F^{(t)} = \{f_{k_t^*}^{(t)}, k_t^* \in K^{(t)}\}$, $f_{k_t^*}^{(t)}: G^{(t)} \rightarrow G^{(t+1)}$, $t = 0, \dots, m-1$, каждый набор раундовых ключей $k_t^* \in K^{(t)}$, $t = 0, \dots, m-1$, задает преобразование итеративного шифра, представляющего собой композицию раундовых отображений $f_{k_{m-1}^*}^{(m-1)} \circ \dots \circ f_{k_0^*}^{(0)}$.

Пусть x_0 — случайная величина со значениями в множестве $G^{(0)}$. Введем в рассмотрение характеристики $\Delta_{k_0^*, \dots, k_{m-1}^*}^{(m,0)}(\alpha_m, \alpha_0)$ отображения $f_{k_{m-1}^*}^{(m-1)} \circ \dots \circ f_{k_0^*}^{(0)}$:

$$\Delta_{k_0^*, \dots, k_{m-1}^*}^{(m,0)}(\alpha_m, \alpha_0) = \mathbf{E}_{x_0} \chi_{\alpha_m}^{(m)}(x_m) \chi_{\alpha_0}^{(0)}(x_0), \quad (1.1)$$

где $\chi_{\alpha}^{(t)}$, $\alpha_t \in G^{(t)}$, — характер группы $G^{(t)}$, $t = 0, \dots, m$, обозначение $\mathbf{E}_{x_0}$ указывает, что усреднение выполняется по распределению случайной величины x_0 , случайная величина x_m со значениями в $G^{(m)}$ определяется соотношениями

$$x_{t+1} = f_{k_t^*}^{(t)}(x_t), \quad t = 0, \dots, m-1. \quad (1.2)$$

Отметим, что в случае $\mathbf{E}_{x_0} \chi_{\alpha_0}^{(0)}(x_0) = 0$, $\mathbf{E}_{x_0} \chi_{\alpha_m}^{(m)}(x_m) = 0$ характеристика (1.1) — коэффициент корреляции между комплексными случайными величинами $\chi_{\alpha_0}^{(0)}(x_0)$ и $\chi_{\alpha_m}^{(m)}(x_m)$.

Несмотря на то что алгоритм развертывания ключа определяет функциональные зависимости между раундовыми ключами, в некоторых задачах криптографического анализа используют упрощенные вероятностные модели итеративных шифров. Например, предположение о том, что раундовые ключи — реализации независимых случайных величин, используется в разностном анализе блочных шифров ([1, 2]) при оценке средних значений вероятностей разностей между блоками шифрованного текста итеративного шифра при заданных значениях разностей между блоками открытого текста.

В данной работе рассматривается упрощенная вероятностная модель итеративного шифра, в которой раундовые ключи $k_0^*, \dots, k_{m-1}^*$ — реализации независимых случайных величин $k_0, \dots, k_{m-1}$. С учетом сделанного допущения определим случайные величины $\Delta_{k_0, \dots, k_{t-1}}^{(t,0)}(\alpha_1, \alpha_0)$, $1 \leq t \leq m-1$, $\alpha_0 \in G^{(0)}$, $\alpha_1 \in G^{(t)}$, которые при $k_0 = k_0^*, \dots, k_{t-1} = k_{t-1}^*$ принимают значения

$$\Delta_{k_0^*, \dots, k_{t-1}^*}^{(t,0)}(\alpha_t, \alpha_0) = \mathbf{E}_{x_0} \chi_{\alpha_t}^{(t)}(x_t) \overline{\chi_{\alpha_0}^{(0)}(x_0)},$$

случайная величина x_0 и случайные величины $k_0, \dots, k_{m-1}$ независимы, случайные величины $x_1, \dots, x_m$ определены соотношениями (1.2).

В рамках данной вероятностной модели итеративного шифра рассматриваются свойства усредненных характеристик

$$\mathbf{E}_{k_0, \dots, k_{m-1}} \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_1, \alpha_0), \quad \mathbf{E}_{k_0, \dots, k_{m-1}} \left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_1, \alpha_0) \right|^2.$$

Отметим, что рассмотрение упрощенной вероятностной модели позволяет получить оценки средних значений соответствующих характеристик отображения $f_{k_{m-1}}^{(m-1)} \circ \dots \circ f_{k_0}^{(0)}$ итеративного шифра, полученных путем усреднения по ключу итеративного шифра.

Нам потребуются некоторые сведения из теории характеров. Любая конечная абелева группа $(G, +)$ представляется в виде прямой суммы циклических примарных подгрупп единственным способом, с точностью до перестановки слагаемых ([3, глава 12]):

$$G = G_1 + \dots + G_s, \quad G_i = \langle g_i \rangle, \quad i = 1, 2, \dots, s.$$

Пусть $w_i, w_i \in \mathbb{C}$, — первообразный корень степени $|G_i|$ из единицы, $i = 1, 2, \dots, s$. Действие характера χ_g , $g \in G$, на группе $(G, +)$ задается равенствами

$$g = \sum_{i=1}^s t_i g_i, \quad 0 \leq t_i < |G|, \quad i = 1, 2, \dots, s,$$

$$\chi_g \left(\sum_{i=0}^s a_i g_i \right) = \prod_{i=1}^s w_i^{t_i a_i}, \quad 0 \leq a_i < |G_i|, \quad i = 1, 2, \dots, s.$$

Для характеров χ_g , $g \in G$, выполнены соотношения взаимности, сопряженности и ортогональности (см. [3, глава 12, § 4]):

- 1) $\chi_g(h) = \chi_h(g)$, $g, h \in G$, — соотношение взаимности,
- 2) $\chi_g(-h) = \overline{\chi_g(h)}$, $g, h \in G$, — соотношение сопряженности,
- 3) $\sum_{g \in G} \chi_g(h_1) \overline{\chi_g(h_2)} = |G| I(h_1 = h_2)$, $h_1, h_2 \in G$, — соотношение ортогональности.

Пусть $G^{(1)}, G^{(2)}$ — конечные абелевы группы, $\chi_\beta^{(1)}, \beta \in G^{(1)}, \chi_\alpha^{(2)}, \alpha \in G^{(2)}$, — характеры групп $G^{(1)}, G^{(2)}$ соответственно. Для произвольного отображения $F, F: G^{(1)} \rightarrow G^{(2)}$, выполнено равенство

$$\chi_\alpha^{(2)}(F(x)) = \sum_{\beta \in G^{(1)}} c_{\alpha, \beta}^{(F)} \chi_\beta^{(1)}(x), \quad \alpha \in G^{(2)}, \quad (1.3)$$

где коэффициенты $c_{\alpha, \beta}^{(F)}, c_{\alpha, \beta}^{(F)} \in \mathbb{C}$, имеют вид

$$c_{\alpha, \beta}^{(F)} = \frac{1}{|G^{(1)}|} \sum_{x \in G^{(1)}} \chi_\alpha^{(2)}(F(x)) \overline{\chi_\beta^{(1)}(x)}, \quad \alpha \in G^{(2)}, \beta \in G^{(1)}. \quad (1.4)$$

Также нам потребуется формула обращения:

$$I(F(x) = y) = \frac{1}{|G^{(2)}|} \sum_{\beta \in G^{(1)}, \alpha \in G^{(2)}} c_{\alpha, \beta}^{(F)} \chi_\beta^{(1)}(x) \overline{\chi_\alpha^{(2)}(y)}, \quad x \in G^{(1)}, y \in G^{(2)}. \quad (1.5)$$

Соотношение (1.5) доказывается цепочкой равенств

$$\begin{aligned} & \frac{1}{|G^{(2)}|} \sum_{\alpha \in G^{(2)}} \sum_{\beta \in G^{(1)}} c_{\alpha, \beta}^{(F)} \chi_\beta^{(1)}(x) \overline{\chi_\alpha^{(2)}(y)} \\ &= \frac{1}{|G^{(2)}|} \sum_{\alpha \in G^{(2)}} \sum_{\beta \in G^{(1)}} \frac{1}{|G^{(1)}|} \sum_{z \in G^{(1)}} \chi_\alpha^{(2)}(F(z)) \overline{\chi_\beta^{(1)}(z)} \chi_\beta^{(1)}(x) \overline{\chi_\alpha^{(2)}(y)} \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{|G^{(2)}|} \frac{1}{|G^{(1)}|} \sum_{\alpha \in G^{(2)}} \sum_{\beta \in G^{(1)}} \sum_{z \in G^{(1)}} \chi_{\alpha}^{(2)}(F(z) - y) \chi_{\beta}^{(1)}(x - z) \\
&= \sum_{z \in G^{(1)}} \frac{1}{|G^{(2)}|} \sum_{\alpha \in G^{(2)}} \chi_{\alpha}^{(2)}(F(z) - y) \frac{1}{|G^{(1)}|} \sum_{\beta \in G^{(1)}} \chi_{\beta}^{(1)}(x - z) \\
&= \sum_{z \in G^{(1)}} I(F(z) = y) I(x = z) = I(F(x) = y).
\end{aligned}$$

С целью упрощения формул здесь и далее используются единые обозначения для операций в различных абелевых группах, в данном случае — в группах $G^{(1)}$, $G^{(2)}$. Полагаем это допустимым, так как нетрудно проследить, к каким элементам какая групповая операция применяется.

2. О средних значениях $\Delta_{k_0, \dots, k_{i-1}}^{(t,0)}(\alpha_1, \alpha_0)$

Для семейства функций $\chi_{\alpha_{t+1}}^{(t+1)}(f_{k_t^*}^{(t)}(x))$, $\alpha_{t+1} \in G^{(t+1)}$, $k_t^* \in K_t$, $0 \leq t < m$, запишем соотношения (1.3) и (1.4) в параметрическом виде:

$$\chi_{\alpha_{t+1}}^{(t+1)}(f_{k_t^*}^{(t)}(x)) = \sum_{\alpha_t \in G^{(t)}} c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t^*] \chi_{\alpha_t}^{(t)}(x), \quad x \in G^{(t)}, \quad (2.1)$$

$$c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t^*] = \frac{1}{|G^{(t)}|} \sum_{x \in G^{(t)}} \chi_{\alpha_{t+1}}^{(t+1)}(f_{k_t^*}^{(t)}(x)) \overline{\chi_{\alpha_t}^{(t)}(x)}, \quad \alpha_t \in G^{(t)}, \alpha_{t+1} \in G^{(t+1)}. \quad (2.2)$$

Зададим случайные матрицы $M_{k_0, \dots, k_{t-1}}^{(t)}$, $0 \leq t \leq m$, и $C_{k_t}^{(t)}$, $0 \leq t \leq m-1$, размерностей $|G^{(t)}| \times |G^{(0)}|$ и $|G^{(t+1)}| \times |G^{(t)}|$ соответственно. Реализациями случайных матриц $M_{k_0, \dots, k_{t-1}}^{(t)}$ и $C_{k_t}^{(t)}$ являются матрицы $M_{k_0^*, \dots, k_{t-1}^*}^{(t)}$ и $C_{k_t^*}^{(t)}$ соответственно, элементы которых имеют вид

$$M_{k_0^*, \dots, k_{t-1}^*}^{(t)}(\alpha_1, \alpha_0) = \Delta_{k_0^*, \dots, k_{t-1}^*}^{(t,0)}(\alpha_1, \alpha_0), \quad \alpha_t \in G^{(t)}, \alpha_0 \in G^{(0)}, 1 \leq t \leq m-1,$$

$$M^{(0)}(\alpha, \beta) = \mathbf{E}_{x_0} \chi_{\alpha-\beta}^{(0)}(x_0), \quad \alpha, \beta \in G^{(0)},$$

$$C_{k_t^*}^{(t)}(\alpha_{t+1}, \alpha_1) = c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t^*], \quad \alpha_{t+1} \in G^{(t+1)}, \alpha_t \in G^{(t)}, 0 \leq t \leq m-1.$$

Теорема 1. В условиях рассматриваемой вероятностной модели справедливы матричные равенства

$$M_{k_0^*, \dots, k_t^*}^{(t+1)} = C_{k_t^*}^{(t)} C_{k_{t-1}^*}^{(t-1)} \dots C_{k_0^*}^{(0)} M^{(0)}, \quad t = 0, 1, \dots, m-1,$$

$$\mathbf{E}_{k_0, \dots, k_t} M_{k_0, \dots, k_t}^{(t+1)} = \left(\mathbf{E}_{k_t} C_{k_t}^{(t)} \right) \left(\mathbf{E}_{k_{t-1}} C_{k_{t-1}}^{(t-1)} \right) \dots \left(\mathbf{E}_{k_0} C_{k_0}^{(0)} \right) M^{(0)},$$

$$t = 0, 1, \dots, m-1,$$

где математическое ожидание $\mathbf{E}_{k_0, \dots, k_t}$ понимается как усреднение по распределениям случайных величин $k_0, \dots, k_t$.

Доказательство. Докажем соотношения

$$\Delta_{k_0^*, \dots, k_t^*}^{(t+1, 0)}(\alpha_{t+1}, \alpha_0) = \sum_{\alpha_t \in G^{(t)}} c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t^*] \Delta_{k_0^*, \dots, k_{t-1}^*}^{(t, 0)}(\alpha_t, \alpha_0), \quad (2.3)$$

$$\mathbf{E}_{k_0, \dots, k_t} \Delta_{k_0, \dots, k_t}^{(t+1, 0)}(\alpha_{t+1}, \alpha_0) = \sum_{\alpha \in G^{(t)}} \mathbf{E}_{k_t} c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t] \mathbf{E}_{k_0, \dots, k_{t-1}} \Delta_{k_0, \dots, k_{t-1}}^{(t, 0)}(\alpha_1, \alpha_0), \quad (2.4)$$

из которых следуют утверждения теоремы 1.

Используя (2.1), нетрудно убедиться в справедливости равенств

$$\begin{aligned} \Delta_{k_0^*}^{(1, 0)}(\alpha_1, \alpha_0) &= \mathbf{E}_{x_0} \chi_{\alpha_1}^{(1)} \left(f_{k_0^*}^{(0)}(x_0) \right) \overline{\chi_{\alpha_0}^{(0)}(x_0)} \\ &= \mathbf{E}_{x_0} \sum_{\beta \in G^{(0)}} c_{\alpha_1, \beta}^{(0)} [k_0^*] \chi_{\beta}^{(0)}(x_0) \overline{\chi_{\alpha_0}^{(0)}(x_0)} = \sum_{\beta \in G^{(0)}} c_{\alpha_1, \beta}^{(0)} [k_0^*] \mathbf{E}_{x_0} \chi_{\beta - \alpha_0}^{(0)}(x_0) \\ &= \sum_{\beta \in G^{(0)}} c_{\alpha_1, \beta}^{(0)} [k_0^*] M^{(0)}(\beta, \alpha_0), \quad \alpha_1 \in G^{(1)}, \alpha_0 \in G^{(0)}, \\ \Delta_{k_0^*, \dots, k_t^*}^{(t+1, 0)}(\alpha_{t+1}, \alpha_0) &= \mathbf{E}_{x_0} \chi_{\alpha_{t+1}}^{(t+1)} \left(f_{k_t^*}^{(t)}(x_t) \right) \overline{\chi_{\alpha_0}^{(0)}(x_0)} \\ &= \sum_{\alpha_t \in G^{(t)}} c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t^*] \mathbf{E}_{x_0} \chi_{\alpha_t}^{(t)}(x_t) \overline{\chi_{\alpha_0}^{(0)}(x_0)} \\ &= \sum_{\alpha_t \in G^{(t)}} c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t^*] \Delta_{k_0^*, \dots, k_{t-1}^*}^{(t, 0)}(\alpha_t, \alpha_0), \quad t \geq 0. \end{aligned}$$

Соотношение (2.4) следует из равенства

$$\begin{aligned} \mathbf{E}_{k_0, \dots, k_t} \Delta_{k_0, \dots, k_t}^{(t+1, 0)}(\alpha_{t+1}, \alpha_0) &= \sum_{\alpha_t \in G^{(t)}} \sum_{k_t^* \in K_t} \mathbf{P}(k_t = k_t^*) c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t^*] \\ &\times \sum_{k_{t-1}^* \in K_{t-1}, \dots, k_0^* \in K_0} \mathbf{P}(k_{t-1} = k_{t-1}^*, \dots, k_0 = k_0^* | k_t = k_t^*) \Delta_{k_0^*, \dots, k_{t-1}^*}^{(t, 0)}(\alpha_t, \alpha_0) \end{aligned}$$

и того, что компоненты случайного вектора $(k_t, \dots, k_0)$, а также x_0 и $(k_t, \dots, k_0)$ независимы. $\square$

Следствие 1. Пусть $0 \leq t \leq m-1$. Если для произвольного $x \in G^{(t)}$ распределение случайной величины $f_{k_t}^{(t)}(x)$ равномерно на $G^{(t+1)}$, то

$$\mathbf{E}_{k_t} \Delta_{k_0, \dots, k_t}^{(t+1, 0)}(\alpha_{t+1}, \alpha_0) = 0, \quad \alpha_{t+1} \in G^{(t+1)} \setminus \{0\}, \quad \alpha_0 \in G^{(0)}. \quad (2.5)$$

Доказательство. Учитывая, что случайная величина x_t функционально зависит от $x_0, k_0, \dots, k_{t-1}$ и не зависит от k_t , выполним преобразования

$$\begin{aligned} \mathbf{E}_{k_t} c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t] &= \mathbf{E}_{k_t} \left(\mathbf{E}_{x_t} \chi_{\alpha_{t+1}}^{(t+1)} \left(f_{k_t}^{(t)}(x_t) \right) \overline{\chi_{\alpha_t}^{(t)}(x_t)} \right) \\ &= \mathbf{E}_{x_t} \left(\overline{\chi_{\alpha_t}^{(t)}(x_t)} \mathbf{E}_{k_t} \chi_{\alpha_{t+1}}^{(t+1)} \left(f_{k_t}^{(t)}(x_t) \right) \right) = I(\alpha_{t+1} = 0) \mathbf{E}_{x_t} \overline{\chi_{\alpha_t}^{(t)}(x_t)} = 0, \end{aligned}$$

из которых ввиду равенства (2.4) следует соотношение (2.5). $\square$

Пример 1. Пусть $k_0, \dots, k_{m-1}$, $k_t = (k_{t,0}, k_{t,1})$, $t = 0, 1, \dots, m-1$, — независимые случайные векторы со значениями в G^2 , где $(G, +)$ — конечная абелева группа. Рассмотрим вероятностную модель итеративного шифра на основе m -раундовой обобщенной схемы Фейстеля

$$y_{t+u+1} = h_{k_{t,0}^*}^{(t)}(y_{t+u}, y_{t+u-1}, \dots, y_{t+1}) + y_t + k_{t,1}^*, \quad t = 0, \dots, m-1, \quad (2.6)$$

где $u \geq 1$, $k_t^* = (k_{t,0}^*, k_{t,1}^*) \in G^2$, $t = 0, \dots, m-1$, — раундовые ключи (реализации независимых случайных векторов $k_0, \dots, k_{m-1}$ соответственно), $h_s^{(t)}: G^u \rightarrow G$, $s \in G$, — семейство функций усложнения, $t = 0, \dots, m-1$. Входом обобщенной схемы Фейстеля является вектор $(y_u, \dots, y_0)$, $(y_u, \dots, y_0) \in G^{u+1}$, выходом — вектор $(y_{m+u}, \dots, y_m)$, $(y_{m+u}, \dots, y_m) \in G^{u+1}$.

Обобщенную схему Фейстеля (2.6) представим в виде соотношений (1.2), задав группы $G^{(t)}$ и классы отображений $f_{k_t^*}^{(t)}$ следующим образом:

$$\begin{aligned} x_t &= (x_{t,1}, \dots, x_{t,u+1}) = (y_{t+u}, \dots, y_t), \quad t = 0, \dots, m, \\ f_{k_t^*}^{(t)}(x_t) &= \left(h_{k_{t,0}^*}^{(t)}(x_{t,1}, \dots, x_{t,u}) + x_{t,u+1} + k_{t,1}^*, x_{t,1}, \dots, x_{t,u} \right), \\ &t = 0, \dots, m-1. \end{aligned} \quad (2.7)$$

Используя характеры группы G^{u+1} , определим характеристики $\Delta_{k_0^*, \dots, k_{t-1}^*}^{(t, 0)}((\alpha_{(t,1)}, \dots, \alpha_{(t,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}))$,

$\alpha_{(t,1)}, \dots, \alpha_{(t,u+1)}, \alpha_{(0,1)}, \dots, \alpha_{(0,u+1)} \in G$, $1 \leq t \leq m$, аналогичные (1.1):

$$\begin{aligned} & \Delta_{k_0^*, \dots, k_{t-1}^*}^{(t,0)} \left((\alpha_{(t,1)}, \dots, \alpha_{(t,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}) \right) \\ &= \mathbf{E}_{x_0} \chi_{\alpha_{(t,1)}}(x_{t,1}) \dots \chi_{\alpha_{(t,u+1)}}(x_{t,u+1}) \overline{\chi_{\alpha_{(0,1)}}(x_{0,1}) \dots \chi_{\alpha_{(0,u+1)}}(x_{0,u+1})}, \end{aligned} \quad (2.8)$$

где x_0 — случайный вектор со значениями в G^{u+1} , не зависящий от $k_0, \dots, k_{m-1}$.

Введем в рассмотрение случайные величины

$$\Delta_{k_0, \dots, k_t}^{(t+1,0)} \left((\alpha_{(t+1,1)}, \dots, \alpha_{(t+1,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}) \right),$$

реализациями которых при $(k_0, \dots, k_t) = (k_0^*, \dots, k_t^*)$ являются $\Delta_{k_0^*, \dots, k_t^*}^{(t+1,0)} \left((\alpha_{(t+1,1)}, \dots, \alpha_{(t+1,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}) \right)$.

Следствие 2. Если распределения случайных векторов $k_0, \dots, k_{m-1}$ таковы, что при произвольных $0 \leq t \leq m-1$ и $k_{t,0}^* \in G$ распределение случайной величины $k_{t,1}$ при условии $\{k_{t,0} = k_{t,0}^*\}$ равномерно на G , то для $\alpha_{(t+1,1)}, \dots, \alpha_{(t+1,u+1)}, \alpha_{(0,1)}, \dots, \alpha_{(0,u+1)} \in G$, $\alpha_{(t+1,1)} \neq 0$, выполнено

$$\mathbf{E}_{k_t} \Delta_{k_0, \dots, k_t}^{(t+1,0)} \left((\alpha_{(t+1,1)}, \dots, \alpha_{(t+1,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}) \right) = 0.$$

Доказательство. Используя (2.7), представим правую часть (2.8) в виде

$$\begin{aligned} & \Delta_{k_0^*, \dots, k_t^*}^{(t+1,0)} \left((\alpha_{(t+1,1)}, \dots, \alpha_{(t+1,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}) \right) \\ &= \mathbf{E}_{x_0} \chi_{\alpha_{t+1,1}} \left(h_{k_{t,0}^*}^{(t)}(x_{t,1}, \dots, x_{t,u}) \right) \\ & \times \chi_{\alpha_{t+1,1}}(x_{t,u+1} + k_{t,1}^*) \prod_{s=2}^{u+1} \chi_{\alpha_{(t+1,s)}}(x_{t,s}) \prod_{r=1}^{u+1} \overline{\chi_{\alpha_{(0,r)}}(x_{0,r})}. \end{aligned}$$

Справедливы соотношения

$$\begin{aligned} & \mathbf{E}_{k_t} \Delta_{k_0, \dots, k_t}^{(t+1,0)} \left((\alpha_{(t+1,1)}, \dots, \alpha_{(t+1,u+1)}), (\alpha_{(0,1)}, \dots, \alpha_{(0,u+1)}) \right) \\ &= \mathbf{E}_{x_{0,1}, \dots, x_{0,u}} \prod_{s=2}^{u+1} \chi_{\alpha_{(t+1,s)}}(x_{t,s}) \prod_{r=1}^{u+1} \overline{\chi_{\alpha_{(0,r)}}(x_{0,r})} \\ & \times \mathbf{E}_{k_t} \chi_{\alpha_{t+1,1}} \left(h_{k_{t,0}^*}^{(t)}(x_{t,1}, \dots, x_{t,u}) \right) \chi_{\alpha_{t+1,1}}(x_{t,u+1} + k_{t,1}) = 0. \end{aligned}$$

Последнее соотношение следует из равномерности распределения $k_{t,1}$ при условии $\{k_{t,0} = k_{t,0}^*\}$. $\square$

3. Укрупнение неоднородной цепи Маркова и марковская модель неоднородного итеративного шифра

Нам потребуются некоторые результаты об укрупнении неоднородной цепи Маркова с помощью разбиения множества исходов.

Пусть $x_0, x_1, \dots$ — некоторая последовательность случайных величин, связанных в неоднородную цепь Маркова с вектором начального распределения $(p_{u_0}, u_0 \in U^{(0)})$ и матрицами вероятностей переходов $\pi^{(i)} = (\pi_{u_{i-1}u_i}^{(i)}, u_{i-1} \in U^{(i-1)}, u_i \in U^{(i)}), i = 1, 2, \dots$, где $U^{(i)}$ — множество значений случайной величины $x_i, i = 0, 1, \dots$. Иными словами, для произвольных $n \in \mathbb{N}, u_i \in U^{(i)}, i = 0, 1, \dots, n$, выполнено соотношение

$$\mathbf{P}(x_0 = u_0, \dots, x_n = u_n) = p_{u_0} \prod_{i=1}^n \pi_{u_{i-1}, u_i}^{(i)}. \quad (3.1)$$

Пусть заданы разбиения множеств $U^{(i)}$

$$U^{(i)} = A_i^{(1)} \cup \dots \cup A_i^{(l_i)}, \quad i = 0, 1, \dots \quad (3.2)$$

Определяемая соотношениями (3.1) неоднородная цепь Маркова допускает укрупнение состояний с использованием разбиений (3.2), если существуют матрицы $\Pi^{(i)} = (\Pi_{j_{i-1}, j_i}^{(i)}, 1 \leq j_{i-1} \leq l_{i-1}, 1 \leq j_i \leq l_i), i = 1, 2, \dots$, удовлетворяющие условию: для произвольных $n \in \mathbb{N}, j_0, j_1, \dots, j_n, 1 \leq j_i \leq l_i, i = 0, 1, \dots, n$, выполнено равенство

$$\mathbf{P}(x_0 \in A_0^{(j_0)}, \dots, x_n \in A_n^{(j_n)}) = \mathbf{P}(x_0 \in A_0^{(j_0)}) \prod_{i=1}^n \Pi_{j_{i-1}, j_i}^{(i)}. \quad (3.3)$$

Из равенства (3.3) следует, что матрицы $\Pi^{(i)}, i = 1, 2, \dots$, задают вероятности $\mathbf{P}(x_i \in A_i^{(j_i)} | x_{i-1} \in A_{i-1}^{(j_{i-1})})$ переходов между укрупненными состояниями.

Теорема 2. Если матрицы вероятностей переходов неоднородной цепи Маркова удовлетворяют условию: для произвольных $n \in \mathbb{N}, 1 \leq j_n \leq l_n, 1 \leq j_{n-1} \leq l_{n-1}, u', u'' \in A_{n-1}^{(j_{n-1})}$ выполнено равенство

$$\mathbf{P}(x_n \in A_n^{(j_n)} | x_{n-1} = u') = \mathbf{P}(x_n \in A_n^{(j_n)} | x_{n-1} = u''), \quad (3.4)$$

то неоднородная цепь Маркова допускает укрупнение состояний с использованием разбиений (3.2) при произвольном векторе начального

распределения. При этом матрицы в равенстве (3.3) можно выбрать независимыми от начального распределения.

Доказательство. Для каждого j_i , $1 \leq j_i \leq l_i$, $i = 1, 2, \dots$, выберем произвольно элемент $u_{i-1}^* \in A_{i-1}^{(j_{i-1})}$ и положим $\Pi_{j_{i-1}, j_i}^{(i)} = \mathbf{P} \left(x_i \in A_i^{(j_i)} \mid x_{i-1} = u_{i-1}^* \right)$. Из (3.4) следует, что матрицы $\Pi_{j_{i-1}, j_i}^{(i)}$ определены однозначно. Если для заданных $i \geq 1$, $1 \leq j_{i-1} \leq l_{i-1}$, $1 \leq j_i \leq l_i$ выполнено условие $\mathbf{P} \left(x_{i-1} \in A_{i-1}^{(j_{i-1})} \right) > 0$, то из равенств

$$\begin{aligned} & \mathbf{P} \left(x_i \in A_i^{(j_i)}, x_{i-1} \in A_{i-1}^{(j_{i-1})} \right) \\ &= \sum_{u_{i-1}^* \in A_{i-1}^{(j_{i-1})}} \mathbf{P} \left(x_{i-1} = u_{i-1}^* \right) \mathbf{P} \left(x_i \in A_i^{(j_i)} \mid x_{i-1} = u_{i-1}^* \right) \\ &= \mathbf{P} \left(x_{i-1} \in A_{i-1}^{(j_{i-1})} \right) \mathbf{P} \left(x_i \in A_i^{(j_i)} \mid x_{i-1} = u_{i-1}^* \right) \end{aligned}$$

следует соотношение

$$\begin{aligned} \mathbf{P} \left(x_i \in A_i^{(j_i)} \mid x_{i-1} \in A_{i-1}^{(j_{i-1})} \right) &= \frac{\mathbf{P} \left(x_{i-1} \in A_{i-1}^{(j_{i-1})}, x_i \in A_i^{(j_i)} \right)}{\mathbf{P} \left(x_{i-1} \in A_{i-1}^{(j_{i-1})} \right)} \\ &= \mathbf{P} \left(x_i \in A_i^{(j_i)} \mid x_{i-1} = u_{i-1}^* \right) = \Pi_{j_{i-1}, j_i}^{(i)}. \end{aligned}$$

При $n \geq 1$ удовлетворяющие условиям $\mathbf{P} \left(x_{n-1} \in A_{n-1}^{(j_{n-1})} \right) = 0$, $1 \leq j_{n-1} \leq l_{n-1}$, слагаемые суммы

$$\mathbf{P} \left(x_0 \in A_0^{(j_0)}, \dots, x_n \in A_n^{(j_n)} \right) = \sum_{u_0 \in A_0^{(j_0)}, \dots, u_n \in A_n^{(j_n)}} \mathbf{P} (x_0 = u_0, \dots, x_n = u_n)$$

равны нулю. Для суммы остальных слагаемых выполнены равенства

$$\begin{aligned} & \mathbf{P} \left(x_0 \in A_0^{(j_0)}, \dots, x_n \in A_n^{(j_n)} \right) \\ &= \sum_{u_0 \in A_0^{(j_0)}, \dots, u_{n-1} \in A_{n-1}^{(j_{n-1})}} \mathbf{P} (x_0 = u_0, \dots, x_{n-1} = u_{n-1}) \\ & \quad \times \sum_{u_n \in A_n^{(j_n)}} \mathbf{P} (x_n = u_n \mid x_{n-1} = u_{n-1}) \end{aligned}$$

$$\begin{aligned}
&= \sum_{u_0 \in A_0^{(j_0)}, \dots, u_{n-1} \in A_{n-1}^{(j_{n-1})}} \mathbf{P}(x_0 = u_0, \dots, x_{n-1} = u_{n-1}) \\
&\quad \times \mathbf{P}(x_n \in A_n^{(j_n)} | x_{n-1} \in A_{n-1}^{(j_{n-1})}) \\
&= \mathbf{P}(x_0 \in A_0^{(j_0)}, \dots, x_{n-1} \in A_{n-1}^{(j_{n-1})}) \mathbf{P}(x_n \in A_n^{(j_n)} | x_{n-1} \in A_{n-1}^{(j_{n-1})}). \quad (3.5)
\end{aligned}$$

Доказательство теоремы 2 следует из справедливости равенства (3.5) для произвольного $n \geq 1$. $\square$

В [4] доказаны необходимость и достаточность условия (3.4) для возможности укрупнения однородной цепи Маркова при произвольном начальном распределении. Приведенное здесь доказательство достаточности условия (3.4) для неоднородной цепи Маркова фактически повторяет доказательство из [4]. Покажем, что для неоднородной марковской цепи условие (3.4) уже не является необходимым: условие (3.4) не следует из равенства (3.3).

Пусть $n = 2$, $U^{(0)} = U^{(1)} = U^{(2)} = \{1, 2, 3, 4\}$, $A_0^{(1)} = A_1^{(1)} = A_2^{(1)} = \{1, 2\}$, $A_0^{(2)} = A_1^{(2)} = A_2^{(2)} = \{3, 4\}$. Зададим матрицы $\pi^{(1)}$, $\pi^{(2)}$, $\Pi^{(1)}$, $\Pi^{(2)}$:

$$\begin{aligned}
\pi^{(1)} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \pi^{(2)} = \begin{pmatrix} 0 & 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0.5 & 0 \\ 0.5 & 0.5 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \\
\Pi^{(1)} &= \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad \Pi^{(2)} = \begin{pmatrix} 0 & 1 \\ 0.5 & 0.5 \end{pmatrix}.
\end{aligned}$$

Для последовательности случайных величин x_0, x_1, x_2 , связанных в неоднородную цепь Маркова с матрицами $\pi^{(1)}$, $\pi^{(2)}$ вероятностей переходов, условие (3.3) выполнено для матриц $\Pi^{(1)}$, $\Pi^{(2)}$ при произвольном начальном распределении, при этом матрица $\pi^{(2)}$ не удовлетворяет (3.4).

Пусть $G^{(0)}, \dots, G^{(m)}$ — конечные множества, $m \in \mathbb{N}$, $k_0, \dots, k_{m-1}$ — независимые случайные величины, принимающие значения в конечных множествах $K^{(0)}, \dots, K^{(m-1)}$ соответственно. Пусть $\{f_{k_t^*}^{(t)}, k_t^* \in K^{(t)}\}$, $t = 0, \dots, m-1$, — семейства отображений $f_{k_t^*}^{(t)}: G^{(t)} \rightarrow G^{(t+1)}$, биграмма $(x_0^{(0)}, x_0^{(1)})$, $(x_0^{(0)}, x_0^{(1)}) \in G^{(0)} \times G^{(0)}$ — случайный вектор, не зависящий

от случайных величин $k_0, \dots, k_{m-1}$. Нетрудно убедиться, что задаваемые соотношениями

$$x_t^{(s)} = f_{k_{t-1}}^{(t-1)} \left(x_{t-1}^{(s)} \right), \quad s = 0, 1, \quad (3.6)$$

биграммы $\left(x_t^{(0)}, x_t^{(1)} \right), \left(x_t^{(0)}, x_t^{(1)} \right) \in G^{(t)} \times G^{(t)}, t = 0, \dots, m$, образуют неоднородную цепь Маркова:

$$\begin{aligned} \mathbf{P} \left(\left(x_0^{(0)}, x_0^{(1)} \right) = \left(g_0^{(0)}, g_0^{(1)} \right), \dots, \left(x_m^{(0)}, x_m^{(1)} \right) = \left(g_m^{(0)}, g_m^{(1)} \right) \right) \\ = \mathbf{P} \left(\left(x_0^{(0)}, x_0^{(1)} \right) = \left(g_0^{(0)}, g_0^{(1)} \right) \right) \\ \times \prod_{t=0}^{m-1} \mathbf{P} \left(\left(x_{t+1}^{(0)}, x_{t+1}^{(1)} \right) = \left(g_{t+1}^{(0)}, g_{t+1}^{(1)} \right) \mid \left(x_t^{(0)}, x_t^{(1)} \right) = \left(g_t^{(0)}, g_t^{(1)} \right) \right), \end{aligned} \quad (3.7)$$

$g_t^{(s)} \in G^{(t)}, s = 0, 1, t = 0, \dots, m$, даже в случае, если на множествах $G^{(t)}$ не заданы операции групп.

В разностном анализе итеративных шифров для укрупнения значений биграмм $\left(x_t^{(0)}, x_t^{(1)} \right) \in G^{(t)} \times G^{(t)}, t = 0, \dots, m$, используются разбиения

$$G^{(t)} \times G^{(t)} = \bigcup_{\Delta \in G^{(t)}} A_t^\Delta, \quad A_t^\Delta = \bigcup_{u \in G^{(t)}} \{(u, u + \Delta)\}, \quad \Delta \in G^{(t)}, \quad t = 0, \dots, m, \quad (3.8)$$

при условии, что $(G^{(t)}, +)$ — группы (не обязательно абелевы), $t = 0, \dots, m$.

Последовательность разностей $x_t^{(0)} - x_t^{(1)}, t = 0, \dots, m$, соответствует последовательности укрупненных состояний, полученных с использованием разбиений (3.8) множества значений случайных биграмм $\left(x_t^{(0)}, x_t^{(1)} \right)$.

Понятие итеративного марковского шифра (марковской модели итеративного шифра) введено в [1]. Необходимые и достаточные условия выполнения марковских свойств для последовательности разностей $x_t^{(0)} - x_t^{(1)}, t = 0, \dots, m$, промежуточных состояний итеративного шифра установлены в [5] методами анализа однородных цепей Маркова с укрупненными состояниями. Различные подходы к расширению достаточных условий марковости алгоритмов блочного шифрования приведены в [6].

Условие (3.4) для рассматриваемой неоднородной марковской цепи и разбиений множества значений случайных биграмм $(x_t^{(0)}, x_t^{(1)})$ на классы с заданными разностями $x_t^{(0)} - x_t^{(1)}$, $t = 0, \dots, m$, формулируется следующим образом.

Определение 1. Пусть k — случайная величина со значениями в множестве K , реализацией которой является раундовый ключ $k^*, k^* \in K$, $F = \{f_{k^*}, k^* \in K\}$ — семейство раундовых отображений, $f_{k^*} : U \rightarrow V$, U, V — конечные группы. Пара (k, F) обладает марковским свойством, если выполнено условие: для любых $\Delta_1 \in U$, $\Delta_2 \in V$ вероятность $\mathbf{P}(f_k(x + \Delta_1) = f_k(x) + \Delta_2)$ не зависит от $x, x \in U$.

Сформулируем достаточное условие марковости неоднородного итеративного шифра с раундовыми отображениями, действующими на группах.

Следствие 3. Если пары (k_t, F_t) обладают марковским свойством, $t = 0, \dots, m-1$, где $F_t = \{f_{k_t^*}^{(t)}, k_t^* \in K^{(t)}\}$, то неоднородная цепь Маркова, образуемая случайными биграммами $(x_t^{(0)}, x_t^{(1)})$ со значениями в $G^{(t)} \times G^{(t)}$, $t = 0, \dots, m-1$, задаваемыми соотношениями (3.6), допускает укрупнение состояний с использованием разбиений (3.8).

Доказательство следствия использует теорему 2 и эквивалентность достаточного условия укрупнения определению 1 марковского свойства.

4. О среднем значении $\left| \Delta_{k_0, \dots, k_{t-1}}^{(t,0)}(\alpha_t, \alpha_0) \right|^2$

Пусть $(G^{(1)}, +)$, $(G^{(2)}, +)$ — конечные абелевы группы, $\chi_\beta^{(1)}$, $\beta \in G^{(1)}$, $\chi_\alpha^{(2)}$, $\alpha \in G^{(2)}$, — характеры групп $G^{(1)}$, $G^{(2)}$ соответственно. Для отображения $f, f: G^{(1)} \times K \rightarrow G^{(2)}$, выполнены соотношения, аналогичные (2.1) и (2.2):

$$\chi_\alpha^{(2)}(f(x, k^*)) = \sum_{\beta \in G^{(1)}} c_{\alpha, \beta} [k^*] \chi_\beta^{(1)}(x), \quad \alpha \in G^{(2)}, \quad k^* \in K, \quad (4.1)$$

$$c_{\alpha, \beta} [k^*] = \frac{1}{|G^{(1)}|} \sum_{x \in G^{(1)}} \chi_\alpha^{(2)}(f(x, k^*)) \overline{\chi_\beta^{(1)}(x)}, \quad \beta \in G^{(1)}, \quad \alpha \in G^{(2)}, \quad k^* \in K. \quad (4.2)$$

Теорема 3. Пусть k — случайная величина со значениями в конечном множестве K .

В обозначениях (4.1), (4.2) следующие условия эквивалентны:

1) Для $\alpha \in G^{(2)}$, $\beta_1, \beta_2 \in G^{(1)}$, $\beta_1 \neq \beta_2$, выполнено

$$\sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha, \beta_1}[k^*] \overline{c_{\alpha, \beta_2}[k^*]} = 0. \quad (4.3)$$

2) Пара (k, f) обладает марковским свойством.

Доказательство. Докажем импликацию 1) $\Rightarrow$ 2).

Применяя равенство (1.5) к отображению $f(x_2, k) - f(x_1, k)$, действующему из $G^{(1)} \times G^{(1)}$ в $G^{(2)}$, получим

$$\begin{aligned} I(f(x_2, k) - f(x_1, k) = \Delta_2) \\ = \frac{1}{|G^{(2)}|} \sum_{\substack{\alpha \in G^{(2)} \\ \beta_1, \beta_2 \in G^{(1)}}} c_{\alpha, \beta_2}[k] \chi_{\beta_2}^{(1)}(x_2) \overline{c_{\alpha, \beta_1}[k] \chi_{\beta_1}^{(1)}(x_1) \chi_{\alpha}^{(2)}(\Delta_2)}. \end{aligned}$$

Используя последнее соотношение, выполним преобразование

$$\begin{aligned} \mathbf{P}(f(x_2, k) - f(x_1, k) = \Delta_2) \\ = \sum_{k^* \in K} \mathbf{P}(k = k^*) I(f(x_2, k^*) - f(x_1, k^*) = \Delta_2) \\ = \frac{1}{|G^{(2)}|} \sum_{\substack{\alpha \in G^{(2)} \\ \beta_1, \beta_2 \in G^{(1)}}} \overline{\chi_{\alpha}^{(2)}(\Delta_2) \chi_{\beta_1}^{(1)}(x_1) \chi_{\beta_2}^{(1)}(x_2)} \\ \times \sum_{k^* \in K} \mathbf{P}(k = k^*) \overline{c_{\alpha, \beta_1}[k^*]} c_{\alpha, \beta_2}[k^*]. \end{aligned}$$

В частности, задав $x_2 = x_1 + \Delta_1$, $\Delta_1 \in G^{(1)}$, получим

$$\begin{aligned} \mathbf{P}(f(x_1 + \Delta_1, k^*) - f(x_1, k^*) = \Delta_2) \\ = \frac{1}{|G^{(2)}|} \sum_{\substack{\alpha \in G^{(2)} \\ \beta_1, \beta_2 \in G^{(1)}}} \overline{\chi_{\alpha}^{(2)}(\Delta_2) \chi_{\beta_2 - \beta_1}^{(1)}(x_1) \chi_{\beta_2}^{(1)}(\Delta_1)} \\ \times \sum_{k^* \in K} \mathbf{P}(k = k^*) \overline{c_{\alpha, \beta_1}[k^*]} c_{\alpha, \beta_2}[k^*]. \end{aligned}$$

Обозначив $\beta = \beta_2 - \beta_1$, с учетом равенства $\beta_2 = \beta + \beta_1$ продолжим преобразования:

$$\begin{aligned} & \mathbf{P} (f (x_1 + \Delta_1, k^*) - f (x_1, k^*) = \Delta_2) \\ &= \frac{1}{|G^{(2)}|} \sum_{\beta \in G^{(1)}} \chi_{\beta}^{(1)} (x_1) \sum_{\substack{\alpha \in G^{(2)} \\ \beta_1 \in G^{(1)}}} \overline{\chi_{\alpha}^{(2)} (\Delta_2)} \chi_{\beta + \beta_1}^{(1)} (\Delta_1) \\ & \quad \times \sum_{k^* \in K} \mathbf{P} (k = k^*) \overline{c_{\alpha, \beta_1} [k^*]} c_{\alpha, \beta + \beta_1} [k^*]. \end{aligned} \quad (4.4)$$

Из условия (4.3) следует, что для $\beta \neq 0$ слагаемые в сумму (4.4) входят с нулевыми множителями, поэтому

$$\begin{aligned} & \mathbf{P} (f (x_1 + \Delta_1, k) - f (x_1, k) = \Delta_2) \\ &= \frac{1}{|G^{(2)}|} \sum_{\beta \in G^{(1)}, \alpha \in G^{(2)}} \chi_{\beta}^{(1)} (\Delta_1) \overline{\chi_{\alpha}^{(2)} (\Delta_2)} \sum_{k^* \in K} \mathbf{P} (k = k^*) |c_{\alpha, \beta} [k^*]|^2. \end{aligned} \quad (4.5)$$

Наличие марковского свойства следует из равенства (4.5).

Докажем импликацию 2) $\Rightarrow$ 1). Введем в рассмотрение отображение $p_{\alpha, \Delta_1}: G^{(1)} \rightarrow \mathbb{C}$, $\alpha \in G^{(2)}$, $\Delta_1 \in G^{(1)}$:

$$p_{\alpha, \Delta_1} (x_1) = \mathbf{E}_k \chi_{\alpha}^{(2)} (f (x_1 + \Delta_1, k) - f (x_1, k)).$$

Из соотношений

$$\begin{aligned} p_{\alpha, \Delta_1} (x_1) &= \sum_{k^* \in K} \mathbf{P} (k = k^*) \chi_{\alpha}^{(2)} (f (x_1 + \Delta_1, k^*) - f (x_1, k^*)) \\ &= \sum_{k^* \in K} \mathbf{P} (k = k^*) \sum_{\Delta_2 \in G^{(2)}} \chi_{\alpha}^{(2)} (\Delta_2) I (f (x_1 + \Delta_1, k^*) - f (x_1, k^*) = \Delta_2) \\ &= \sum_{\Delta_2 \in G^{(2)}} \chi_{\alpha}^{(2)} (\Delta_2) \mathbf{P} (f (x_1 + \Delta_1, k) - f (x_1, k) = \Delta_2) \end{aligned}$$

следует, что $p_{\alpha, \Delta_1} (x_1)$ не зависит от x_1 , поскольку по условию 2) вероятность $\mathbf{P} (f (x_1 + \Delta_1, k) - f (x_1, k) = \Delta_2)$ не зависит от x_1 . Из (4.2) следует, что коэффициенты $c_{\alpha, \beta}^{(p)}$, $\beta \neq 0$, разложения $p_{\alpha, \Delta_1} (x_1)$ по характеристам:

$$\begin{aligned} p_{\alpha, \Delta_1} (x_1) &= \sum_{\beta \in G^{(1)}} \chi_{\beta}^{(1)} (x_1) c_{\alpha, \beta}^{(p)}, \\ c_{\alpha, \beta}^{(p)} &= \frac{1}{|G^{(1)}|} \sum_{x \in G^{(1)}} p_{\alpha, \Delta_1} (x) \overline{\chi_{\beta}^{(1)} (x)}, \end{aligned}$$

удовлетворяют условиям $c_{\alpha,\beta}^{(p)} = 0$, $\beta \neq 0$.

Используя равенство

$$\begin{aligned} \chi_{\alpha}^{(2)}(f(x_1 + \Delta_1, k) - f(x_1, k)) \\ = \sum_{\beta_1, \beta_2 \in G^{(1)}} c_{\alpha, \beta_1}[k] \chi_{\beta_1}^{(1)}(x_1) \chi_{\beta_1}^{(1)}(\Delta_1) \overline{c_{\alpha, \beta_2}[k] \chi_{\beta_2}^{(1)}(x_1)}, \end{aligned}$$

проведем формальные преобразования:

$$\begin{aligned} c_{\alpha, \beta}^{(p)} &= \frac{1}{|G^{(1)}|} \sum_{x_1 \in G^{(1)}} \mathbf{E} k \chi_{\alpha}^{(2)}(f(x_1 + \Delta_1, k) - f(x_1, k)) \overline{\chi_{\beta}^{(1)}(x_1)} \\ &= \frac{1}{|G^{(1)}|} \sum_{\beta_1, \beta_2, x \in G^{(1)}} \chi_{\beta_1 - \beta_2 - \beta}^{(1)}(x_1) \chi_{\beta_1}^{(1)}(\Delta_1) \sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha, \beta_1}[k^*] \overline{c_{\alpha, \beta_2}[k^*]} \\ &= \sum_{\beta_1, \beta_2} I(\beta = \beta_1 - \beta_2) \chi_{\beta_1}^{(1)}(\Delta_1) \sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha, \beta_1}[k^*] \overline{c_{\alpha, \beta_2}[k^*]} \\ &= \sum_{\beta_1 \in G^{(1)}} \chi_{\beta_1}^{(1)}(\Delta_1) \sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha, \beta_1}[k^*] \overline{c_{\alpha, \beta - \beta_1}[k^*]}. \end{aligned} \quad (4.6)$$

Из равенств

$$\sum_{\beta_1 \in G^{(1)}} \chi_{\beta_1}^{(1)}(\Delta_1) \sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha, \beta_1}[k^*] \overline{c_{\alpha, \beta - \beta_1}[k^*]} = 0, \quad \Delta_1 \in G^{(1)},$$

и соотношений ортогональности характеров следует условие 1):

$$\sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha, \beta_1}[k^*] \overline{c_{\alpha, \beta - \beta_1}[k^*]} = 0 \text{ при } \beta_1 \neq 0, \alpha \in G^{(2)}.$$

□

Последовательно применяя к композиции отображений

$$G^{(0)} \xrightarrow{f_{k_0^*}^{(0)}} G^{(1)} \xrightarrow{f_{k_1^*}^{(1)}} G^{(2)} \rightarrow \dots \rightarrow G^{(m-1)} \xrightarrow{f_{k_{m-1}^*}^{(m-1)}} G^{(m)}$$

равенства (2.1) для значений $t = m - 1, \dots, 0$, получим равенство

$$\chi_{\alpha_m}^{(m)}(x_m) = \sum_{\alpha_0 \in G^{(0)}, \dots, \alpha_{m-1} \in G^{(m-1)}} \chi_{\alpha_0}^{(0)}(x_0) \prod_{t=0}^{m-1} c_{\alpha_{t+1}, \alpha_t}^{(t)}[k^*], \quad \alpha_m \in G^{(m)}, \quad (4.7)$$

позволяющее вычислить значение $\Delta_{k_0^*, \dots, k_{m-1}^*}^{(m,0)}(\alpha_m, \beta)$, $\alpha_m \in G^{(m)}$, $\beta \in G^{(0)}$:

$$\Delta_{k_0^*, \dots, k_{m-1}^*}^{(m,0)}(\alpha_m, \beta) = \sum_{\alpha_0 \in G^{(0)}, \dots, \alpha_{m-1} \in G^{(m-1)}} \prod_{t=0}^{m-1} c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t^*] \mathbf{E}_{x_0} \chi_{\alpha_0 - \beta}^{(0)}(x_0). \quad (4.8)$$

Теорема 4. Если для итеративного шифра (1.2) пары $(k_t, \{f_{k_t^*}^{(t)}, k_t^* \in K^{(t)}\})$, $t = 0, \dots, m-1$, обладают марковским свойством, то в условиях рассматриваемой вероятностной модели с учетом обозначений (4.2) выполнены соотношения:

1)

$$\mathbf{E}_{k_0, \dots, k_{m-1}} \prod_{t=0}^{m-1} c_{\alpha_{t+1}^{(1)}, \alpha_t^{(1)}}^{(t)}[k_t] \overline{c_{\alpha_{t+1}^{(2)}, \alpha_t^{(2)}}^{(t)}[k_t]} = 0, \quad (4.9)$$

где $(\alpha_{m-1}^{(j)}, \dots, \alpha_0^{(j)})$, $j = 1, 2$, — различные наборы индексов слагаемых суммы (4.8),

2)

$$\begin{aligned} & \mathbf{E}_{k_0, \dots, k_{m-1}} \left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_m, \beta) \right|^2 \\ &= \sum_{\alpha_0 \in G^{(0)}, \dots, \alpha_{m-1} \in G^{(m-1)}} \prod_{t=0}^{m-1} \mathbf{E}_{k_t} \left| c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t] \right|^2 \left| \mathbf{E}_{x_0} \chi_{\alpha_0 - \beta}^{(0)}(x_0) \right|^2. \end{aligned} \quad (4.10)$$

Замечание. Введем в рассмотрение матрицы $V^{(t)}$, $0 \leq t \leq m$, и $D^{(t)}$, $0 \leq t \leq m-1$, размерностей $|G^{(t)}| \times |G^{(t)}|$ и $|G^{(t+1)}| \times |G^{(t)}|$ соответственно. Элементы этих матриц имеют вид

$$\begin{aligned} V^{(t)}(\alpha_t, \alpha_0) &= \mathbf{E}_{k_0, \dots, k_{t-1}} \left| \Delta_{k_0, \dots, k_{t-1}}^{(t,0)}(\alpha_t, \alpha_0) \right|^2, \quad \alpha_t \in G^{(t)}, \alpha_0 \in G^{(0)}, t > 0, \\ V^{(0)}(\alpha_0, \beta) &= \left| \mathbf{E}_{x_0} \chi_{\alpha_0 - \beta}^{(0)}(x_0) \right|^2, \quad \alpha_0, \beta \in G^{(0)}, \\ D^{(t)}(\alpha_{t+1}, \alpha_t) &= \sum_{k_t^* \in K^{(t)}} \mathbf{P}(k_t = k_t^*) \left| c_{\alpha_{t+1}, \alpha_t}^{(t)}[k_t^*] \right|^2, \quad \alpha_{t+1} \in G^{(t+1)}, \alpha_t \in G^{(t)}. \end{aligned}$$

Равенство (4.10) представляется в виде равенства матриц

$$V^{(t)} = D^{(t)} D^{(t-1)} \dots D^{(0)} V^{(0)}, \quad t = 0, 1, \dots, m-1. \quad (4.11)$$

Доказательство теоремы 4. Поскольку наборы $(\alpha_{m-1}^{(j)}, \dots, \alpha_0^{(j)})$, $j = 1, 2$, различны, то существует такое τ , $0 < \tau \leq m$, что $\alpha_{m-1}^{(1)} = \alpha_{m-1}^{(2)}, \dots, \alpha_{m-\tau+1}^{(1)} = \alpha_{m-\tau+1}^{(2)}, \alpha_{m-\tau}^{(1)} \neq \alpha_{m-\tau}^{(2)}$.

Из марковского свойства пары $k_{m-\tau}$ и $\left\{ f_{k_{m-\tau}^*}^{(m-\tau)}, k_{m-\tau}^* \in K^{(m-\tau)} \right\}$ следуют равенства

$$\begin{aligned} \mathbf{E}_{k_{m-\tau}} c_{\alpha_{m-\tau+1}^{(1)}, \alpha_{m-\tau}^{(1)}}^{(m-\tau)} [k_{m-\tau}] \overline{c_{\alpha_{m-\tau+1}^{(2)}, \alpha_{m-\tau}^{(2)}}^{(m-\tau)} [k_{m-\tau}]} &= 0, \\ \mathbf{E}_{k_0, \dots, k_{m-1}} \prod_{t=0}^{m-1} c_{\alpha_{t+1}^{(1)}, \alpha_t^{(1)}}^{(t)} [k_t] \overline{c_{\alpha_{t+1}^{(2)}, \alpha_t^{(2)}}^{(t)} [k_t]} &= \\ &= \prod_{t=0}^{m-1} \mathbf{E}_{k_t} c_{\alpha_{t+1}^{(1)}, \alpha_t^{(1)}}^{(t)} [k_t] \overline{c_{\alpha_{t+1}^{(2)}, \alpha_t^{(2)}}^{(t)} [k_t]} = 0. \end{aligned}$$

Соотношение

$$\begin{aligned} \mathbf{E}_{k_0, \dots, k_t} \left| \Delta_{k_0, \dots, k_t}^{(t+1,0)} (\alpha_{t+1}, \alpha_0) \right|^2 &= \sum_{\alpha_t^{(1)}, \alpha_t^{(2)} \in G^{(t)}} \mathbf{E}_{k_t} c_{\alpha_{t+1}^{(1)}, \alpha_t^{(1)}}^{(t)} [k_t] \overline{c_{\alpha_{t+1}^{(2)}, \alpha_t^{(2)}}^{(t)} [k_t]} \\ &\times \mathbf{E}_{k_0, \dots, k_{t-1}} \Delta_{k_0, \dots, k_{t-1}}^{(t,0)} \left(\alpha_t^{(1)}, \alpha_0 \right) \overline{\Delta_{k_0, \dots, k_{t-1}}^{(t,0)} \left(\alpha_t^{(2)}, \alpha_0 \right)} \quad (4.12) \end{aligned}$$

следует из (2.3) и из независимости $k_0, \dots, k_{t-1}$ и k_t . Из теоремы 3 следует, что слагаемые с ненулевыми коэффициентами в сумме (4.12) должны удовлетворять условию $\alpha_t^{(1)} = \alpha_t^{(2)}$, при этом будет выполнено равенство

$$\begin{aligned} \mathbf{E}_{k_0, \dots, k_t} \left| \Delta_{k_0, \dots, k_t}^{(t+1,0)} (\alpha_{t+1}, \alpha_0) \right|^2 &= \sum_{\alpha_t \in G^{(t)}} \mathbf{E}_{k_t} \left| c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t] \right|^2 \mathbf{E}_{k_0, \dots, k_{t-1}} \left| \Delta_{k_0, \dots, k_{t-1}}^{(t,0)} \left(\alpha_t^{(1)}, \alpha_0 \right) \right|^2. \end{aligned}$$

Из последнего соотношения несложно получить равенство (4.10). $\square$

Следствие 4. В условиях теоремы 4 выполнено неравенство

$$\begin{aligned} &\left(\mathbf{E}_{k_0, \dots, k_{m-1}} \left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)} (\alpha_m, \beta) \right| \right)^2 \\ &\leq \sum_{\alpha_0 \in G^{(0)}, \dots, \alpha_{m-1} \in G^{(m-1)}} \prod_{t=0}^{m-1} \mathbf{E}_{k_t} \left| c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t] \right|^2 \left| \mathbf{E}_{x_0} \chi_{\alpha_0 - \beta}^{(0)} (x_0) \right|^2. \quad (4.13) \end{aligned}$$

Неравенство (4.13) обращается в равенство только в случае, когда $\left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_m, \alpha_0) \right|$ не зависит от $k_0, \dots, k_{m-1}$.

Доказательство следует из неравенства

$$\left(\mathbf{E}_{k_0, \dots, k_{m-1}} \left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_m, \beta) \right| \right)^2 \leq \mathbf{E}_{k_0, \dots, k_{m-1}} \left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_m, \beta) \right|^2,$$

равенство возможно только при $\mathbf{D}_{k_0, \dots, k_{m-1}} \left| \Delta_{k_0, \dots, k_{m-1}}^{(m,0)}(\alpha_m, \beta) \right| = 0$.

Следствие 5. В условиях теоремы 4 матрица $D^{(t)}$ является стохастической, $0 \leq t \leq m-1$. Если $G^{(t)} = G^{(t+1)}$ и для каждого фиксированного $k_t^* \in K^{(t)}$ отображение $f_{k_t^*}^{(t)}(x)$ задает подстановку, то матрица $D^{(t)}$ дважды стохастическая, $0 \leq t \leq m-1$.

Доказательство. Стохастичность матрицы $D^{(t)}$ следует из равенства Парсеваля

$$\begin{aligned} & \sum_{\alpha_t \in G^{(t)}} |c_{\alpha_{t+1}, \alpha_t}^{(t)}|^2 \\ &= \frac{1}{|G^{(t)}|^2} \sum_{x_1, x_2 \in G^{(t)}} \chi_{\alpha_{t+1}}^{(t+1)}(f_{k_t^*}^{(t)}(x_1)) \overline{\chi_{\alpha_{t+1}}^{(t+1)}(f_{k_t^*}^{(t)}(x_2))} \sum_{\alpha_t \in G^{(t)}} \overline{\chi_{\alpha_1}^{(t)}(x_1)} \chi_{\alpha_t}^{(t)}(x_2) \\ &= \frac{1}{|G^{(t)}|} \sum_{x \in G^{(t)}} \left| \chi_{\alpha_{t+1}}^{(t)}(f_{k_t^*}^{(t)}(x)) \right|^2 = 1 \end{aligned} \quad (4.14)$$

и соотношения

$$\sum_{\alpha_t \in G^{(t)}} D^{(t)}(\alpha_{t+1}, \alpha_t) = \sum_{k_t^* \in K^{(t)}} \mathbf{P}(k_t = k_t^*) \sum_{\alpha_t \in G^{(t)}} |c_{\alpha_{t+1}, \alpha_t}^{(t)}|^2 = 1. \quad (4.15)$$

Пусть $h_{k_t^*}$ — обратное отображение к отображению $f_{k_t^*}^{(t)}$, $0 \leq t \leq m-1$. Из соотношений (4.1), (4.2) следует, что для коэффициентов $\lambda_{\alpha, \beta}[k_t^*]$ разложений $\chi_{\alpha}^{(t+1)}(h_{k_t^*}(x))$ по характерам

$$\chi_{\alpha}^{(t+1)}(h_{k_t^*}(x)) = \sum_{\beta \in G^{(t)}} \lambda_{\alpha, \beta}[k_t^*] \chi_{\beta}^{(t)}(x), \quad \alpha \in G^{(t)}, k_t^* \in K^{(t)},$$

выполнены соотношения

$$\begin{aligned}\lambda_{\alpha,\beta}[k_t^*] &= \frac{1}{|G^{(t)}|} \sum_{x \in G^{(t)}} \chi_{\alpha}^{(t+1)} \left(f_{k_t^*}^{(t)}(x) \right) \overline{\chi_{\beta}^{(t)}(x)} \\ &= \frac{1}{|G^{(t)}|} \sum_{y \in G^{(t)}} \chi_{\alpha}^{(t+1)}(y) \overline{\chi_{\beta}^{(t)}(h_{k_t^*}(y))} = c_{\beta,\alpha}^{(t)}[k_t^*], \\ \beta &\in G^{(t)}, \quad \alpha \in G^{(t)}, \quad k_t^* \in K^{(t)}.\end{aligned}$$

Доказательство дважды стохастичности матрицы $D^{(t)}$ следует из тождества $c_{\alpha_{t-1},\alpha_t}^{(t)}[k_t^*] = \lambda_{\alpha_t,\alpha_{t+1}}[k_t^*]$, $\alpha_t, \alpha_{t+1} \in G^{(t)}$, и соотношений, аналогичных (4.14), (4.15), для отображения $h_{k_t^*}$. $\square$

Пример 2. Пусть $k_0, \dots, k_{m-1}$, $k_t = (k_{t,0}, \dots, k_{t,u})$, $u \geq 1$, $t = 0, 1, \dots, m-1$, — независимые случайные векторы, принимающие значения в G^{u+1} , $(G, +)$ — конечная абелева группа. Рассмотрим вероятностную модель итеративного шифра на основе m -раундовой обобщенной схемы Фейстеля

$$y_{t+u+1} = h_{k_{t,0}^*}^{(t)}(y_{t+u} + k_{t,u}^*, \dots, y_{t+1} + k_{t,1}^*) + y_t, \quad t = 0, \dots, m-1, \quad (4.16)$$

где $k_t^* = (k_{t,0}^*, \dots, k_{t,u}^*) \in G^{u+1}$, $t = 0, \dots, m-1$, — раундовые ключи (реализации независимых случайных векторов $k_0, \dots, k_{m-1}$ соответственно), $\{h_s^{(t)}: G^u \rightarrow G, s \in G\}$, — семейство функций усложнения, $t = 0, \dots, m-1$. Входом схемы Фейстеля является случайный вектор $(y_u, \dots, y_0)$ со значениями в G^{u+1} . Выходом схемы Фейстеля является вектор $(y_{m+u}, \dots, y_m)$.

Представим соотношения (4.16) обобщенной схемы Фейстеля в виде (1.1), задав группы $G^{(t)}$ и классы отображений $f_{k_t^*}^{(t)}$ следующим образом:

$$\begin{aligned}G^{(t)} &= G^{u+1}, \quad x_t = (x_{t,1}, \dots, x_{t,u+1}) = (y_{t+u}, \dots, y_t), \quad t = 0, \dots, m, \\ f_{k_t^*}^{(t)}(x_t) &= \left(h_{k_{t,0}^*}^{(t)}(x_{t,1} + k_{t,u}^*, \dots, x_{t,u} + k_{t,1}^*) + x_{t,u+1}, \quad x_{t,1}, \dots, x_{t,u} \right), \\ &t = 0, \dots, m-1. \quad (4.17)\end{aligned}$$

Пусть для вероятностной модели итеративного шифра на основе m -раундовой обобщенной схемы Фейстеля (4.16) распределение $(k_{t,1}, \dots, k_{t,u})$ равномерно на G^u при условии фиксации $k_{t,0} = k_{t,0}^*$, $k_{t,0}^* \in G$, $t = 0, \dots, m$. Тогда в условиях фиксации $k_{t,0} = k_{t,0}^*$, $k_{t,0}^* \in G$,

$t = 0, \dots, m-1$, семейство раундовых отображений (4.16) также задает вероятностную модель итеративного шифра. Для произвольных $\Delta_1, \Delta_2 \in G^{u+1}$, $\Delta_1 = (\Delta_{1,1}, \dots, \Delta_{1,u+1})$, $\Delta_2 = (\Delta_{2,1}, \dots, \Delta_{2,u+1})$ из соотношений

$$\begin{aligned} & \mathbf{P} \left(f_{k_{t,0}^*, k_{t,1}, \dots, k_{t,u}}^{(t)} (x_t + \Delta_1) - f_{k_{t,0}^*, k_{t,1}, \dots, k_{t,u}}^{(t)} (x_t) = \Delta_2 \right) \\ &= \frac{1}{|G|^u} \sum_{k_{t,1}^*, \dots, k_{t,u}^* \in G} \left(I \left(h_{k_{t,0}^*}^{(t)} (x_{t,1} + \Delta_{1,1} + k_{t,u}^*, \dots, x_{t,u} + \Delta_{1,u} + k_{t,1}^*) + \Delta_{1,u+1} \right. \right. \\ & \quad \left. \left. - h_{k_{t,0}^*}^{(t)} (x_{t,1} + k_{t,u}^*, \dots, x_{t,u} + k_{t,1}^*) = \Delta_{2,1} \right) \right) I (\Delta_{1,1} = \Delta_{2,2}, \dots, \Delta_{1,u} = \Delta_{2,u+1}) \\ &= \frac{1}{|G|^u} \sum_{k_{t,1}^*, \dots, k_{t,u}^* \in G} \left(I \left(h_{k_{t,0}^*}^{(t)} (\Delta_{1,1} + k_{t,u}^*, \dots, \Delta_{1,u} + k_{t,1}^*) + \Delta_{1,u+1} \right. \right. \\ & \quad \left. \left. - h_{k_{t,0}^*}^{(t)} (x_{t,1} + k_{t,u}^*, \dots, x_{t,u} + k_{t,1}^*) = \Delta_{2,1} \right) \right) I (\Delta_{1,1} = \Delta_{2,2}, \dots, \Delta_{1,u} = \Delta_{2,u+1}) \\ &= \mathbf{P} \left(f_{k_{t,0}^*, k_{t,1}, \dots, k_{t,u}}^{(t)} (\Delta_1) - f_{k_{t,0}^*, k_{t,1}, \dots, k_{t,u}}^{(t)} (0) = \Delta_2 \right) \end{aligned}$$

следует равенство для безусловных вероятностей

$$\begin{aligned} \mathbf{P} \left(f_{k_{t,0}, k_{t,1}, \dots, k_{t,u}}^{(t)} (x_t + \Delta_1) - f_{k_{t,0}, k_{t,1}, \dots, k_{t,u}}^{(t)} (x_t) = \Delta_2 \right) &= \\ &= \mathbf{P} \left(f_{k_{t,0}, k_{t,1}, \dots, k_{t,u}}^{(t)} (\Delta_1) - f_{k_{t,0}, k_{t,1}, \dots, k_{t,u}}^{(t)} (0) = \Delta_2 \right), \end{aligned}$$

которое означает, что случайный вектор k_t и семейство отображений $f_{k_t}^{(t)}$, $t = 0, \dots, m-1$, обладают марковским свойством.

Вернемся к представлению (4.8) характеристики $\Delta_{k_0^*, \dots, k_{m-1}^*}^{(m,0)} (\alpha_m, \beta)$, $\alpha_m \in G^{(m)}$, $\beta \in G^{(0)}$. Пусть $L = G^{(m-1)} \times \dots \times G^{(0)}$, L_1 — непустое подмножество L , $L_2 = L \setminus L_1$.

С целью упрощения записи выражений введем обозначения: $k^* = (k_0^*, \dots, k_{m-1}^*)$, $k = (k_0, \dots, k_{m-1})$, $K = K^{(0)} \times \dots \times K^{(m-1)}$, при этом вектор k^* — реализация случайного вектора k .

Сумму (4.8) разобьем на два слагаемых

$$\begin{aligned} \Delta_{k^*}^{(m,0)} (\alpha_m, \beta) &= \xi_{k^*} (L_1) + \xi_{k^*} (L_2), \\ \xi_{k^*} (L_j) &= \sum_{(\alpha_{m-1}, \dots, \alpha_0) \in L_j} \prod_{t=0}^{m-1} c_{\alpha_{t+1}, \alpha_t}^{(t)} [k_t^*] \mathbf{E}_{x_0} \chi_{\alpha_0 - \beta}^{(0)} (x_0), \quad j = 1, 2. \end{aligned}$$

Теорема 5. Пусть для итеративного шифра (1.2) пары $(k_t, \{f_{k_t^*}^{(t)}, k_t^* \in K^{(t)}\})$, $t = 0, \dots, m-1$, обладают марковским свойством. Тогда в условиях рассматриваемой вероятностной модели выполнено неравенство

$$\max_{k^* \in K} |\xi_{k^*}(L_1)| \mathbf{E}_k \left| \Delta_k^{(m,0)}(\alpha_m, \beta) \right| \geq \mathbf{E}_k |\xi_k(L_1)|^2. \quad (4.18)$$

Доказательство. Выполнены неравенства

$$\begin{aligned} & \max_{k^* \in K} |\xi_{k^*}(L_1)| \mathbf{E}_k \left| \Delta_k^{(m,0)}(\alpha_m, \beta) \right| \\ &= \sum_{k^* \in K} \mathbf{P}(k = k^*) \max_{k^* \in K} |\xi_{k^*}(L_1)| |\xi_{k^*}(L_1) + \xi_{k^*}(L_2)| \\ &\geq \sum_{k^* \in K} \mathbf{P}(k = k^*) |\xi_{k^*}(L_1)| |\xi_{k^*}(L_1) + \xi_{k^*}(L_2)| \\ &= \sum_{k^* \in K} \mathbf{P}(k = k^*) \left| \overline{\xi_{k^*}(L_1)} \xi_{k^*}(L_1) + \overline{\xi_{k^*}(L_1)} \xi_{k^*}(L_2) \right|. \end{aligned} \quad (4.19)$$

Из равенства (4.9) теоремы 4 следуют соотношения

$$\begin{aligned} \sum_{k^* \in K} \mathbf{P}(k = k^*) \prod_{t=0}^{m-1} c_{\alpha_{t+1}^{(1)}, \alpha_t^{(1)}}^{(t)} [k_t^*] \mathbf{E}_{x_0} \chi_{\alpha_0^{(1)} - \beta}^{(0)}(x_0) \\ \times \prod_{t=0}^{m-1} \overline{c_{\alpha_{t+1}^{(2)}, \alpha_t^{(2)}}^{(t)} [k_t^*] \mathbf{E}_{x_0} \chi_{\alpha_0^{(2)} - \beta}^{(0)}(x_0)} = 0, \end{aligned}$$

где $\alpha_m^{(1)} = \alpha_m^{(2)} = \alpha_m$, $(\alpha_{m-1}^{(j)}, \dots, \alpha_0^{(j)}) \in L_j$, $j = 1, 2$,

$$\sum_{k^* \in K} \mathbf{P}(k = k^*) \overline{\xi_{k^*}(L_1)} \xi_{k^*}(L_2) = 0. \quad (4.20)$$

Оценим сумму (4.19), используя неравенство

$$\sum_{i=1}^n |w_i| \geq \left| \sum_{i=1}^n w_i \right|, \quad w_1, \dots, w_n \in \mathbb{C},$$

следующее по индукции из неравенства треугольника

$|w_0| + |w_1| \geq |w_0 + w_1|$, $w_1, w_2 \in \mathbb{C}$:

$$\begin{aligned} & \max_{k^* \in K} |\xi_{k^*}(L_1)| \mathbf{E}_k \left| \Delta_k^{(m,0)}(\alpha_m, \beta) \right| \\ & \geq \left| \sum_{k^* \in K} \mathbf{P}(k = k^*) |\xi_{k^*}(L_1)|^2 + \sum_{k^* \in K} \mathbf{P}(k = k^*) \overline{\xi_{k^*}(L_1)} \xi_{k^*}(L_2) \right|. \end{aligned}$$

Из (4.20) следует, что правая часть неравенства равна $\mathbf{E}_k |\xi_k(L_1)|^2$. $\square$

Пусть Λ — класс подмножеств L_1 , $L_1 \in \Lambda$, удовлетворяющих условию: случайная величина $|\xi_k(L_1)|$ имеет вырожденное распределение.

Следствие 6. Если класс Λ не пустой, то при условиях теоремы 5 выполнено неравенство

$$\mathbf{E}_k \left| \Delta_k^{(m,0)}(\alpha_m, \beta) \right| \geq \max_{L_1 \in \Lambda} |\xi_{k^*}(L_1)|, \quad k^* \in K. \quad (4.21)$$

Доказательство. Неравенство (4.21) выполнено, если $\max_{L_1 \in \Lambda} |\xi_{k^*}(L_1)| = 0$.

Пусть для некоторого L_1 , $L_1 \in \Lambda$, выполнено $|\xi_{k^*}(L_1)| > 0$. Из вырожденности распределения случайной величины $|\xi_k(L_1)|$ следуют соотношения

$$\max_{k^* \in K} |\xi_{k^*}(L_1)| = |\xi_{k^*}(L_1)|, \quad \mathbf{E}_k |\xi_k(L_1)|^2 = |\xi_{k^*}(L_1)|^2, \quad k^* \in K,$$

позволяющие из (4.18) получить неравенство

$$\mathbf{E}_k \left| \Delta_k^{(m,0)}(\alpha_m, \beta) \right| \geq |\xi_{k^*}(L_1)|. \quad (4.22)$$

Неравенство (4.21) следует из (4.22) и произвольности выбора L_1 , $L_1 \in \Lambda$. $\square$

Список литературы

- [1] Lai X., Massey J., Murphy S., “Markov ciphers and differential cryptanalysis”, EURO-CRYPT’1991, Lect. Notes Comput. Sci., **547**, 1991, 17–38.
- [2] Lai X., *Diss. for the degree of Doctor of Techn. Sci.*, Swiss Federal Inst. Technology, Zürich, 1992, 118 pp.
- [3] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра: Учебник. 2-е изд., испр. и доп.*, СПб.: Лань, 2015, 608 с.
- [4] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М.: Наука, 1970, 272 с.

- [5] Погорелов Б.А., Пудовкина М.А., “Разбиения на биграммах и марковость алгоритмов блочного шифрования”, *Математические вопросы криптографии*, **8:1** (2017), 107–142.
- [6] Денисов О.В., “Критерии марковости алгоритмов блочного шифрования”, *Прикладная дискретная математика*, 2018, № 41, 28–37.