V. O. Drelikhov, On the constructions of Markov maps, *Mat. Vopr. Kriptogr.*, 2024, Volume 15, Issue 1, 21–34

DOI: 10.4213/mvk460

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2024 Т. 15 № 1 С. 21–34

УДК 519.719.2 DOI https://doi.org/10.4213/mvk460

О конструкциях марковских отображений

В. О. Дрелихов

АО «ИТМиВТ», Москва

Получено 18.V.2023

Аннотация. Модели марковских шифров используются в задачах линейного анализа и разностного анализа блочных шифров. В работе рассматриваются обладающие марковским свойством конструкции отображений $f_k(x)$, зависящих от случайной величины k и действующих на алгебраических объектах различного типа (абелевы группы, векторные пространства и др.). Получена нижняя оценка для мощности конечного множества K значений случайной величины k, $k \in K$, для марковского отображения $f_k(x)$ абелевых групп.

Ключевые слова: марковские шифры, отображения абелевых групп

On the constructions of Markov maps

V. O. Drelikhov

JSC «IPMCE», Moscow

Abstract. Markov cipher models are used in linear analysis and differential analysis of block ciphers. We consider mappings defined on algebraic objects of various types (Abelian groups, vector spaces, etc.) and having Markovian properties. A lower estimate for the cardinality of a set K of values of a random variable k defining the Markov map of Abelian groups $f_k(x)$ is established.

Keywords: Markov ciphers, mappings of Abelian groups

Citation: Matematicheskie Voprosy Kriptografii, 2024, v. 15, № 1, pp. 21–34 (Russian)

Пусть $G^{(0)},\dots,G^{(m)}$, $K^{(0)},\dots,K^{(m-1)}$ – конечные множества, $m\in\mathbb{N}$, $F^{(0)},\dots,F^{(m-1)}$ — последовательность семейств отображений

$$F^{(t)}=\{f^{(t)}_{k^*_t},k^*_t\in K^{(t)}\},\quad f^{(t)}_{k^*_t}\colon G^{(t)}\to G^{(t+1)},\quad t=0,\dots,m-1. \tag{1}$$

Далее рассматриваются случайные отображения

$$f^{(t)}_{k_t}\colon G^{(t)}\to G^{(t+1)},\quad t=0,\dots,m-1, \tag{2}$$

задаваемые случайной величиной k_t, $k_t\in K^{(t)}$. Реализацией случайного отображения $f^{(t)}_{k_t}$ является отображение $f^{(t)}_{k^*_t}$, где k^*_t — значение случайной величины k_t.

Пусть $k_0,\dots,k_{m-1}$, $k_t\in K^{(t)}$, $t=0,\dots,m-1$, — независимые случайные величины, случайный вектор $(x^{(0)}_0,x^{(1)}_0)\in G^{(0)}\times G^{(0)}$ не зависит от $k_0,\dots,k_{m-1}$. Нетрудно убедиться, что задаваемая соотношениями

$$x^{(s)}_t=f^{(t-1)}_{k_{t-1}}(x^{(s)}_{t-1}),\quad s=0,1,\quad t=1,\dots,m,$$

последовательность случайных векторов $(x^{(0)}_t,x^{(1)}_t)\in G^{(t)}\times G^{(t)}$, $t=0,\dots,m$, при любом распределении случайного вектора $(x^{(0)}_0,x^{(1)}_0)$ образует неоднородную цепь Маркова: для произвольных $g^{(s)}_t\in G^{(t)}$, $s=0,1$, $\mathbf{P}((x^{(0)}_t,x^{(1)}_t)=(g^{(0)}_t,g^{(1)}_t))>0$, $t=0,\dots,m$, выполнено равенство

$$\begin{aligned}\mathbf{P}((x^{(0)}_0,x^{(1)}_0)=(g^{(0)}_0,g^{(1)}_0),\dots,(x^{(0)}_m,x^{(1)}_m)=(g^{(0)}_m,g^{(1)}_m))\\ =\mathbf{P}((x^{(0)}_0,x^{(1)}_0)=(g^{(0)}_0,g^{(1)}_0))\\ \times\prod_{t=0}^{m-1}\mathbf{P}((x^{(0)}_{t+1},x^{(1)}_{t+1})=(g^{(0)}_{t+1},g^{(1)}_{t+1})/(x^{(0)}_t,x^{(1)}_t)=(g^{(0)}_t,g^{(1)}_t)).\end{aligned}$$

В разностном методе анализа итеративных шифров рассматривают модели, полученные укрупнением состояний $(x^{(0)}_t,x^{(1)}_t)\in G^{(t)}\times G^{(t)}$, $t=0,\dots,m$, указанной цепи Маркова с использованием разбиений

$$G^{(t)}\times G^{(t)}=\bigcup_{\Delta\in G^{(t)}}A^{\Delta}_t,$$

где

$$A^{\Delta}_t=\bigcup_{u\in G^{(t)}}\{(u,\Delta*u)\},\quad \Delta\in G^{(t)},\quad t=0,\dots,m, \tag{3}$$

при условии, что $(G^{(t)}, *)$, $t = 0, \ldots, m$, — группы (не обязательно абелевы). В рассматриваемых моделях последовательность разностей $x_t^{(0)} * (x_t^{(1)})^{-1}$, $t = 0, \ldots, m$, соответствует последовательности укрупненных состояний, полученных с использованием указанных разбиений.

В статье [1] введено определение итеративного марковского шифра (марковской модели итеративного шифра). Приведем его ниже с одним незначительным изменением, связанным с тем, что случайные величины $k_0, \ldots, k_{m-1}$ могут иметь разные распределения, кроме того, в [1] распределение случайных величин $k_0, \ldots, k_{m-1}$ полагалось равномерным, иными словами, марковское свойство относилось только к семейству отображений вида (1). Однако при варьировании распределений случайных величин $k_0, \ldots, k_{m-1}$ марковские свойства случайных отображений $f_k(x)$ не обязательно сохраняются.

Определение 1 (марковский итеративный шифр)**.** Пусть k – случайная величина, K – множество ее значений, $F = \{f_{k^*}, k^* \in K\}$ – семейство отображений, $f_k : G^{(1)} \to G^{(2)}$, $(G^{(1)}, *)$, $(G^{(2)}, *)$ – конечные группы. Пара (k, F) обладает марковским свойством, если выполнено условие инвариантности.

Условие инвариантности. Для произвольных $\Delta_1 \in G^{(1)}$, $\Delta_2 \in G^{(2)}$ вероятности

$$\mathbf{P}(f_k(\Delta_1 * x) = \Delta_2 * f_k(x)) \tag{4}$$

одинаковы для всех $x \in G^{(1)}$.

Композиция $f_{k_{m-1}}^{(m-1)} \circ \ldots \circ f_{k_0}^{(0)}$ введенных в (2) случайных раундовых отображений $f_{k_t}^{(t)} : G^{(t)} \to G^{(t+1)}$, $k_t \in K^{(t)}$, $t = 0, \ldots, m-1$, называется марковским итеративным шифром, если случайные величины $k_0, \ldots, k_{m-1}$ независимы и все пары $(k_t, F^{(t)})$, $t = 0, \ldots, m-1$, обладают марковским свойством. Далее, с целью упрощения терминологии, марковским отображением (отображением с марковским свойством) будем называть случайное отображение $f_{k_t}^{(t)} : G^{(t)} \to G^{(t+1)}$, задаваемое случайной величиной k_t, если пара $(k_t, F^{(t)})$ обладает марковским свойством.

Рассмотрим дополнительные условия для марковского итеративного шифра:

– $K^{(0)} = \cdots = K^{(m-1)} = K$, $G^{(0)} = \cdots = G^{(m)}$,

– случайные величины $k_0, \ldots, k_{m-1}$ одинаково распределены;

– для любого $\theta \in K$ отображения $f_\theta^{(0)}, \ldots, f_\theta^{(m-1)}$ совпадают (т. е. $f_\theta^{(t)}$ не зависит от $t \in \{0, \ldots, m-1\}$).

В [2] показано, что выполнение свойства однородной цепи Маркова для последовательности разностей $x_t^{(0)} * (x_t^{(1)})^{-1}$, $t = 0, \ldots, m$, следует из возможности укрупнения состояний однородной цепи Маркова [3]. Одним из приложений результатов [3] является следующий критерий наличия марковского свойства для последовательности разностей, справедливый при выполнении указанных выше дополнительных условий: заданное в определении 1 условие инвариантности (4) для раундовых отображений является необходимым и достаточным условием того, что последовательность разностей $x_t^{(0)} * (x_t^{(1)})^{-1}$, $t = 0, \ldots, m$, образует цепь Маркова при любом распределении случайного вектора $(x_0^{(0)}, x_0^{(1)})$.

Отметим, что марковское свойство для отображений не обязательно абелевых групп было сформулировано в [4, теорема 1, формула 7] как один из критериев марковости шифра с такими раундовыми отображениями. В этой же статье [4, стр. 29] данный критерий и еще два подобных критерия названы «условиями инвариантности распределения разностей подстановки относительно фиксации входного блока».

В [5, раздел 3] рассмотрены возможности укрупнения состояний неоднородных цепей Маркова в общем случае, без указанных выше дополнительных условий, при этом группы $G^{(0)}, \ldots, G^{(m)}$ не обязательно абелевы, и показано, что приведенное выше в определении итеративного марковского шифра условие (4) является достаточным условием того, что последовательность разностей $x_t^{(0)} * (x_t^{(1)})^{-1}$, $t = 0, \ldots, m$, образует неоднородную цепь Маркова при любом распределении случайного вектора $(x_0^{(0)}, x_0^{(1)})$.

Установлено [5, стр. 71, следствие 3], что композиция марковских отображений $f_{k_0}^{(0)}, f_{k_1}^{(1)}$ сохраняет марковское свойство (4) отображений в условиях независимости случайных величин k_0, k_1. Точнее, если случайные величины k_0, k_1 независимы и случайные отображения групп $f_{k_0}^{(0)} : G^{(0)} \to G^{(1)}$, $f_{k_1}^{(1)} \colon G^{(1)} \to G^{(2)}$ обладают марковским свойством, то случайное отображение $f_{k_0}^{(0)} \circ f_{k_1}^{(1)} : G^{(0)} \to G^{(2)}$ также обладает марковским свойством.

В этой же работе [5, стр. 69] приведен пример, показывающий, что в общем случае условие марковости шифра не является необходимым для того, чтобы последовательность разностей $x_t^{(0)} * (x_t^{(1)})^{-1}$, $t = 0, \ldots, m$, образовывала неоднородную марковскую цепь при любом

распределении случайного вектора $(x_0^{(0)}, x_0^{(1)})$.

Заметим также, что при укрупнении состояний марковской цепи вместо блоков (3) можно рассматривать блоки

$$A_t^{\Delta} = \bigcup_{u \in G^{(t)}} \{(u, u * \Delta)\}, \quad \Delta \in G^{(t)}, t = 0, \ldots, m,$$

но при этом необходимо изменить условие инвариантности, рассмотрев вместо вероятности (4) вероятность $\mathbf{P}(f_k(x * \Delta_1) = f_k(x) * \Delta_2)$.

Конструкций марковских отображений известно не так много, но марковские модели отображений широко используются в задачах разностного анализа блочных шифров, сфера их применения расширяется, например в [5] показана возможность использования свойств марковских отображений в задачах линейного анализа. Рассмотрим примеры марковских отображений.

Пример 1 ([4, стр. 31])**.** Пусть $(G^{(1)}, *)$, $(G^{(2)}, *)$ – конечные группы, $k^{(1)}$, $k^{(2)}$ – независимые случайные величины, $k^{(1)} \in K^{(1)}$, $K^{(1)}$ – конечное множество, случайная величина $k^{(2)}$ имеет равномерное распределение на множестве $G^{(1)}$, $g_{k^{(1)}} \colon G^{(1)} \to G^{(2)}$ — случайное отображение, зависящее только от $k^{(1)}$. Тогда отображение $f_{(k^{(1)},k^{(2)})} \colon G^{(1)} \to G^{(2)}$,

$$f_{(k^{(1)},k^{(2)})}(x) = g_{k^{(1)}}(x * k^{(2)}), \quad x \in G^{(1)},$$

является марковским.

Пример 2. Пусть $(G^{(1)}, *)$, $(G^{(2)}, *)$ – конечные группы, h_1, h_2 – гомоморфизмы, $h_i : G^{(i)} \to G^{(i)}$, $i = 1, 2$. Если задаваемое случайной величиной k, $k \in K$, случайное отображение $f_k : G^{(1)} \to G^{(2)}$ – марковское, то для произвольного $g \in G^{(1)}$ случайное отображение

$$h_2(f_k(h_1(x) * g)), x \in G^{(1)}, k \in K,$$

также является марковским.

Доказательство. Справедливы равенства

$$\begin{aligned} &\mathbf{P}\big(h_2(f_k(h_1(\Delta_1 * x) * g)) = \Delta_2 * h_2(f_k(h_1(x) * g))\big) \\ &= \mathbf{P}\big(h_2\big(f_k(h_1(\Delta_1) * h_1(x) * g) * (f_k(h_1(x) * g))^{-1}\big) = \Delta_2\big) \\ &= \sum_{\Delta_2' \in h_2^{(-1)}(\Delta_2)} \mathbf{P}(f_k(h_1(\Delta_1) * h_1(x) * g) * (f_k(h_1(x) * g))^{-1} = \Delta_2') \end{aligned}$$

$$= \sum_{\Delta_2' \in h_2^{(-1)}(\Delta_2)} \pi^{(f_k)}_{h_1(\Delta_1),\Delta_2'},$$

где первое равенство получено с использованием свойства гомоморфизмов h_1, h_2, корректность обозначения

$$\pi^{(f_k)}_{h_1(\Delta_1),\Delta_2'} = \mathbf{P}(f_k(h_1(\Delta_1) * h_1(x) * g) * (f_k(h_1(x) * g))^{-1} = \Delta_2')$$

следует из марковского свойства случайного отображения f_k. □

Пример 3. Пусть k_1 и k_2 – независимые случайные величины, $(G^{(1)}, +)$, $(G^{(2)}, +)$ — конечные абелевы группы. Если случайные отображения $f^{(j)}_{k_j} : G^{(1)} \to G^{(2)}$, $j = 1, 2$, марковские, то задаваемое случайным вектором $k = (k_1, k_2)$ отображение $f_{(k_1,k_2)} : G^{(1)} \times G^{(1)} \to G^{(2)}$,

$$f_{(k_1,k_2)}(x_1, x_2) = f^{(1)}_{k_1}(x_1) + f^{(2)}_{k_2}(x_2), \quad x_1, x_2 \in G^{(1)},$$

также является марковским.

Доказательство. Пусть $\Delta_{1,1}, \Delta_{1,2} \in G^{(1)}$, $\Delta_2 \in G^{(2)}$. Справедливы равенства

$$\mathbf{P}_k(f^{(1)}_{k_1}(x_1 + \Delta_{1,1}) + f^{(2)}_{k_2}(x_2 + \Delta_{1,2}) - f^{(1)}_{k_1}(x_1) - f^{(2)}_{k_2}(x_2) = \Delta_2)$$

$$= \sum_{\substack{\Delta_{2,1},\Delta_{2,2} \in G^{(2)}, \\ \Delta_{2,1}+\Delta_{2,2}=\Delta_2}} \mathbf{P}_k(f^{(1)}_{k_1}(x_1 + \Delta_{1,1}) - f^{(1)}_{k_1}(x_1) = \Delta_{2,1}, \; f^{(2)}_{k_2}(x_2 + \Delta_{1,2}) - f^{(2)}_{k_2}(x_2) = \Delta_{2,2})$$

$$= \sum_{\substack{\Delta_{2,1},\Delta_{2,2} \in G^{(2)}, \\ \Delta_{2,1}+\Delta_{2,2}=\Delta_2}} \mathbf{P}_{k_1}(f^{(1)}_{k_1}(x_1 + \Delta_{1,1}) - f^{(1)}_{k_1}(x_1) = \Delta_{2,1}) \times \mathbf{P}_{k_2}(f^{(2)}_{k_2}(x_2 + \Delta_{1,2}) - f^{(2)}_{k_2}(x_2) = \Delta_{2,2})$$

$$= \sum_{\substack{\Delta_{2,1},\Delta_{2,2} \in G^{(2)}, \\ \Delta_{2,1}+\Delta_{2,2}=\Delta_2}} \phi_1(\Delta_{1,1}, \Delta_{2,1})\phi_1(\Delta_{1,2}, \Delta_{2,2}),$$

где корректность обозначения

$$\phi_j(\Delta_{1,j}, \Delta_{2,j}) = \mathbf{P}_{k_j}(f^{(j)}_{k_j}(x_j + \Delta_{1,j}) - f^{(j)}_{k_j}(x_j) = \Delta_{2,j})$$

следует из марковских свойств отображений $f^{(j)}_{k_j}(x)$, $j = 1, 2$. Пусть $\mathbf{P}_k(.)$ обозначает вероятность случайного события, задаваемую распределением случайной величины k. Из правой части равенства следует,

что вероятность

$$\mathbf{P}_{(k_1,k_2)}\left(f^{(1)}_{k_1}(x_1+\Delta_{1,1})+f^{(2)}_{k_2}(x_2+\Delta_{1,2})-f^{(1)}_{k_1}(x_1)-f^{(2)}_{k_2}(x_2)=\Delta_2\right)$$

не зависит от (x_1, x_2), так как функции ϕ_1, ϕ_2 не зависят от аргументов x_1, x_2. □

Следствие 1. *В условиях примера* 3 *случайное отображение* $f_{(k_1,k_2)}\colon G^{(1)} \to G^{(2)}$,

$$f_{(k_1,k_2)}(x) = f^{(1)}_{k_1}(x) + f^{(2)}_{k_2}(x), \quad x \in G^{(1)},$$

обладает марковским свойством.

Доказательство следствия проводится аналогично при $x_1 = x_2 = x$.

Пример 4. Пусть $G^{(1)}_i$, $G^{(2)}_i$ – конечные группы, $i = 1, \ldots, r$, $k = (k_1, \ldots, k_r)$ — случайный вектор с независимыми компонентами, случайные отображения $f^{(i)}_{k_i} : G^{(1)}_i \to G^{(2)}_i$, $i = 1, \ldots, r$, являются марковскими. Тогда случайное отображение

$$F_k\colon G^{(1)}_1\times\ldots\times G^{(1)}_r\to G^{(2)}_1\times\ldots\times G^{(2)}_r,\, F_k(x_1,\ldots,x_r)=(f^{(1)}_{k_1}(x_1),\ldots,f^{(r)}_{k_r}(x_r)),$$

$x_i \in G^{(1)}_i$, $i = 1, \ldots, r$, является марковским.

Пример 5 ([5, стр. 78])**.** Рассмотрим вероятностную модель итеративного шифра на основе m-раундовой обобщенной схемы Фейстеля

$$y_{t+u+1} = h^{(t)}_{k^*_{t,0}}(y_{t+u} + k^*_{t,u}, \ldots, y_{t+1} + k^*_{t,1}) + y_t, \quad t = 0, \ldots, m-1,$$

где $u \geqslant 1$, векторы $k^*_t = (k^*_{t,0}, \ldots, k^*_{t,u}) \in G^{u+1}$, $t = 0, \ldots, m-1$, —- раундовые ключи, реализации независимых случайных векторов $k_0, \ldots, k_{m-1}$ соответственно, $(G, +)$ — конечная абелева группа, $\{h^{(t)}_s, s \in G\}$ — семейство произвольных функций усложнения, $h^{(t)}_s : G^u \to G$, $t = 0, \ldots, m-1$. Задаваемое случайным вектором $(k_0, \ldots, k_{m-1})$ отображение $(y_u, \ldots, y_0) \mapsto (y_{m+u}, \ldots, y_m)$ является марковским, где вектор $(y_u, \ldots, y_0) \in G^{u+1}$ — вход схемы Фейстеля, вектор $(y_{m+u}, \ldots, y_m) \in G^{u+1}$ — выход схемы Фейстеля.

Пример 6. Пусть F – поле, F_n – множество векторов над полем F размерности n. Задаваемое случайной величиной k, $k \in K$, случайное

отображение $f_k(\mathbf{x}) = \mathbf{x}\mathbf{B}_k + \mathbf{c}_k$ является марковским, если $\mathbf{B}_k$ – зависящая от k матрица размера $n \times n$ над полем F, вектор $\mathbf{c}_k$ также зависит от k, $\mathbf{x}, \mathbf{c}_k \in F_n$.

Доказательство марковского свойства следует из равенства $f_k(\mathbf{x} + \Delta_1) - f_k(\mathbf{x}) = \Delta_1\mathbf{B}_k$, $\Delta_1 \in F_n$, показывающего независимость вероятности $\mathbf{P}(f_k(\mathbf{x} + \Delta_1) - f_k(\mathbf{x}) = \Delta_2)$ от вектора $\mathbf{x}$ для всех пар (Δ_1, Δ_2).

Пример 7. Пусть $(L, +)$ — подгруппа аддитивной группы поля $GF(q)$, φ — гомоморфизм группы $(GF(q), +)$ в L. Выберем произвольные $h_1, h_2 \in GF(q)\backslash L$ так, что $h_1 + h_2 \notin L$. Пусть k — случайная величина, имеющая равномерное распределение на смежном классе $K = h_1 + L$, тогда задаваемое случайной величиной k отображение $f_k : L \to L$,

$$f_k(x) = \varphi\left(\frac{x + h_2}{(x + h_2 + k)k}\right), \quad x \in L,$$

обладает марковским свойством.

Доказательство. Пусть $\Delta_1 \in L$. Из выбора области значений k, x, h_1, h_2 следует справедливость соотношений

$$k \neq 0, \quad x + h_2 + k \in h_1 + h_2 + L, \quad x + h_2 + k \neq 0,$$

$$x + \Delta_1 + h_2 + k \in h_1 + h_2 + L, \quad x + \Delta_1 + h_2 + k \neq 0.$$

Из равенств

$$\begin{aligned} f_k(x + \Delta_1) - f_k(x) &= \varphi\left(\frac{x + \Delta_1 + h_2}{(x + \Delta_1 + h_2 + k)k}\right) - \varphi\left(\frac{x + h_2}{(x + h_2 + k)k}\right) \\ &= \varphi\left(\frac{x + \Delta_1 + h_2}{(x + \Delta_1 + h_2 + k)k} - \frac{x + h_2}{(x + h_2 + k)k}\right) \\ &= \varphi\left(\frac{\Delta_1}{(x + h_2 + k)(x + h_2 + k + \Delta_1)}\right) \end{aligned}$$

следует справедливость при произвольном $\Delta_2 \in L$ равенств

$$|L|\,\mathbf{P}(f_k(x+\Delta_1)-f_k(x)=\Delta_2)$$
$$=\sum_{t\in h_1+L} I\left(\varphi\left(\frac{\Delta_1}{(x+h_2+t)(x+h_2+t+\Delta_1)}\right)=\Delta_2\right)$$
$$=\sum_{t\in L} I\left(\varphi\left(\frac{\Delta_1}{(x+t+h_1+h_2)(x+t+h_1+h_2+\Delta_1)}\right)=\Delta_2\right)$$
$$=\sum_{t\in L} I\left(\varphi\left(\frac{\Delta_1}{(t+h_1+h_2)(t+h_1+h_2+\Delta_1)}\right)=\Delta_2\right),$$

где $I(A)$ – функция-индикатор события A, корректность изменения области суммирования в последнем равенстве следует из условия $t, x \in L$. Правая часть последнего равенства указывает, что вероятность $\mathbf{P}(f_k(x+\Delta_1)-f_k(x)=\Delta_2)$ не зависит от $x \in L$. □

Пример 8. Пусть $(F_n, +)$ — группа n-мерных векторов над полем $GF(q)$, характеристика поля больше трех. Рассмотрим случайное отображение $f_k\colon F_n \to F_n$,

$$f_k(\mathbf{x})=(y_1,\ldots,y_n),\quad y_i=\mathbf{x}\mathbf{A}_k^{(i)}\mathbf{x}^\top+\mathbf{b}_k^{(i)}\mathbf{x}^\top+c_k^{(i)},\quad i=1,\ldots,n, \tag{5}$$

где K — конечное множество, k — случайная величина со значениями в K, удовлетворяющая условию

$$\mathbf{P}(k=\theta)>0 \text{ для всех } \theta\in K, \tag{6}$$

$c_\theta^{(i)} \in F$, $\theta \in K$, $\mathbf{A}_\theta^{(i)}$, $\mathbf{b}_\theta^{(i)}$ —- зависящие от $\theta \in K$ симметричные $n\times n$-матрицы над полем F, вектор размерности n над полем F соответственно, $i=1,\ldots,n$.

Теорема 1. *Пусть распределение случайной величины k удовлетворяет условию* (6). *Заданное в* (5) *отображение $f_k : F_n \to F_n$ обладает марковским свойством тогда и только тогда, когда $\mathbf{A}_k^{(i)} \equiv 0$, $i=1,\ldots,n$, $k\in K$.*

Доказательство. Пусть случайное отображение $f_k(\mathbf{x})$ обладает марковским свойством. Пусть $\mathbf{c}_k=(c_k^{(1)},\ldots,c_k^{(n)})$, $\mathbf{B}_k$ —- матрица размера $n\times n$, образованная строками $\mathbf{b}_k^{(1)},\ldots,\mathbf{b}_k^{(n)}$. Непосредственной проверкой условия инвариантности (4) нетрудно убедиться, что из марковского свойства отображения $f_k(\mathbf{x})$ следует марковское свойство случайного отображения $g_k(\mathbf{x})=f_k(\mathbf{x})-\mathbf{B}_k\mathbf{x}^\top-\mathbf{c}_k$.

Выберем произвольный ненулевой вектор $\mathbf{\Delta}_1 \in F_n$ и, используя симметричность матриц $\mathbf{A}_k^{(i)}$, представим разность $g_k(\mathbf{x}+\mathbf{\Delta}_1) - g_k(\mathbf{x})$, $\mathbf{x} \in F_n$, в виде:

$$g_k(\mathbf{x}+\mathbf{\Delta}_1) - g_k(\mathbf{x}) = (z_1, \ldots, z_n),$$
$$z_i = (\mathbf{x}+\mathbf{\Delta}_1)\mathbf{A}_k^{(i)}(\mathbf{x}+\mathbf{\Delta}_1)^\top - \mathbf{x}\mathbf{A}_k^{(i)}\mathbf{x}^\top = 2\mathbf{x}\mathbf{A}_k^{(i)}\mathbf{\Delta}_1^\top + \mathbf{\Delta}_1\mathbf{A}_k^{(i)}\mathbf{\Delta}_1^\top,\ i=1,\ldots,n. \tag{7}$$

Подставив в (7) значение $\mathbf{x}^* = -\mathbf{\Delta}_1/2$, получим равенство $g_k(\mathbf{x}^* + \mathbf{\Delta}_1) - g_k(\mathbf{x}^*) = 0$. Зафиксируем $\mathbf{\Delta}_2 \in F_n$ и рассмотрим вероятность $\mathbf{P}(g_k(\mathbf{x}^* + \mathbf{\Delta}_1) - g_k(\mathbf{x}^*) = \mathbf{\Delta}_2)$,

$$\mathbf{P}(g_k(\mathbf{x}^* + \mathbf{\Delta}_1) - g_k(\mathbf{x}^*) = \mathbf{\Delta}_2) = I(\mathbf{\Delta}_2 = 0).$$

Так как случайное отображение $g_k(\mathbf{x})$ обладает марковским свойством, то из условия инвариантности (4) следует равенство $\mathbf{P}(g_k(\mathbf{x}+\mathbf{\Delta}_1) - g_k(\mathbf{x}) = 0) = 1$ для всех $\mathbf{x} \in F_n$. Из последнего равенства и условия (6) следует равенство $g_\theta(\mathbf{x}+\mathbf{\Delta}_1) - g_\theta(\mathbf{x}) = 0$ для всех $x \in F_n$, $\theta \in K$. Используя равенство (7), получим, что для произвольных $\mathbf{x}, \mathbf{\Delta}_1 \in F_n$ выполнено соотношение

$$2\mathbf{x}\mathbf{A}_\theta^{(i)}\mathbf{\Delta}_1^\top + \mathbf{\Delta}_1\mathbf{A}_\theta^{(i)}\mathbf{\Delta}_1^\top = 0$$

для всех $i = 1, \ldots, n$, $\theta \in K$.

Если в качестве векторов $\mathbf{x}, \mathbf{\Delta}_1$ выбрать векторы $\mathbf{e}(j_1)$, $\mathbf{e}(j_2)$ с нулевыми компонентами, кроме единичных компонент с номерами j_1, j_2 соответственно, $1 \leqslant j_1, j_2 \leqslant n$, то для каждого $1 \leqslant i \leqslant n$ будут выполнены соотношения для элементов $\mathbf{A}_\theta^{(i)}(j_1, j_2)$ в матрицах $\mathbf{A}_\theta^{(i)}$:

для $j_1 = j_2$

$$0 = 2\mathbf{e}(j_1)\mathbf{A}_\theta^{(i)}\mathbf{e}(j_1)^\top + \mathbf{e}(j_1)\mathbf{A}_\theta^{(i)}\mathbf{e}(j_1)^\top = 3\mathbf{A}_\theta^{(i)}(j_1, j_1), \quad \theta \in K, \tag{8}$$

для $j_1 \neq j_2$

$$0 = 2\mathbf{A}_\theta^{(i)}(j_1, j_2) + \mathbf{A}_\theta^{(i)}(j_2, j_2) = 2\mathbf{A}_\theta^{(i)}(j_1, j_2), \quad \theta \in K. \tag{9}$$

Последнее равенство в (9) получено с использованием (8), учитывая, что характеристика поля F больше трех. Из соотношений (3), (4) следуют равенства $\mathbf{A}_k^{(i)} \equiv 0$, $i = 1, \ldots, n$, $k \in K$.

Докажем обратную импликацию. Пусть для всех $k \in K$, $\mathbf{x} \in F_n$ выполнено $\mathbf{A}_k^{(i)} \equiv 0$, $i = 1, \ldots, n$. Тогда набор квадратичных форм $f_k(\mathbf{x})$ принимает вид $f_k(\mathbf{x}) = \mathbf{B}_k\mathbf{x}^\top + \mathbf{c}_k$, где матрица $\mathbf{B}_k$ и вектор $\mathbf{c}_k$ определены выше в доказательстве теоремы. Марковское свойство случайного отображения $f_k(\mathbf{x})$ устанавливается так же, как и в примере 6. □

В примере 1 рассмотрена конструкция марковского отображения f_k, $k \in K$, действующего на заданных группах $G^{(1)}, G^{(2)}$, для которого мощность множества K значений случайной величины k, принимаемых с положительными вероятностями, может быть сколь угодно большой. Приведенная ниже теорема задает нетривиальную нижнюю оценку мощности множества K для марковского отображения f_k, $k \in K$, действующего на абелевых группах.

Предварительно приведем некоторые сведения о характерах абелевых групп (см. учебник [6]). Представим группу $(G, +)$ в виде прямой суммы циклических примарных подгрупп $G = H_1 + \ldots + H_s$, $H_i =< g_i >$, $i = 1, \ldots, s$, такое представление единственно, с точностью до перестановки слагаемых. Пусть $w_i \in \mathbb{C}$ — первообразный корень степени $|H_i|$ из единицы, $i = 1, \ldots, s$, и для элементов $a, b \in G$ выполнено представление

$$a = \sum_{i=0}^{s} t_i^{(a)} g_i,\ b = \sum_{i=0}^{s} t_i^{(b)} g_i,\ 0 \leqslant t_i^{(a)} < |H_i|\,,\ 0 \leqslant t_i^{(b)} < |H_i|\,,\ i = 1, \ldots, s.$$

Значение характера χ_a на элементе b задается уравнением

$$\chi_a(b) = \prod_{i=1}^{s} w_i^{t_i^{(a)} t_i^{(b)}}.$$

Пусть $(G^{(1)}, +)$, $(G^{(2)}, +)$ — конечные абелевы группы. Рассмотрим характеры $\chi_\beta^{(1)}$, $\chi_\alpha^{(2)}$ групп $G^{(1)}, G^{(2)}$, $\beta \in G^{(1)}$, $\alpha \in G^{(2)}$. Для произвольного отображения $f\colon G^{(1)} \to G^{(2)}$ справедливо разложение функции $\chi_\alpha^{(2)}(f(x))$, $\alpha \in G^{(2)}$, $x \in G^{(1)}$, по базисным функциям-характерам

$$\chi_\alpha^{(2)}(f(x)) = \sum_{\beta \in G^{(1)}} c_{\alpha,\beta} \chi_\beta^{(1)}(x), \tag{10}$$

коэффициенты $c_{\alpha,\beta}$ имеют вид

$$c_{\alpha,\beta} = \frac{1}{|G^{(1)}|} \sum_{x \in G^{(1)}} \chi_\alpha^{(2)}(f(x)) \overline{\chi_\beta^{(1)}}(x), \quad \alpha \in G^{(2)}, \beta \in G^{(1)}. \tag{11}$$

Пусть $f_k : G^{(1)} \to G^{(2)}$ — случайное отображение, задаваемое случайной величиной k, $k \in K$, и набором функций $\{f_\theta : G^{(1)} \to G^{(2)}, \theta \in K\}$. Равенство (10) для функции $\chi_\alpha^{(2)}(f_\theta(x))$, $\alpha \in G^{(2)}$, $\alpha \neq 0$, $x \in G^{(1)}$, представим в параметрическом виде

$$\chi_\alpha^{(2)}(f_\theta(x)) = \sum_{\beta \in G^{(1)}} c_{\alpha,\beta}[\theta] \chi_\beta^{(1)}(x), \quad \theta \in K.$$

Обозначим через $n_{\alpha,\theta}$ количество ненулевых значений в наборе коэффициентов $\{c_{\alpha,\beta}[\theta], \beta \in G^{(1)}\}$, $\alpha \in G^{(2)}$, $\alpha \neq 0$, $\theta \in K$.

Теорема 2. *Пусть* $f_k : G^{(1)} \to G^{(2)}$, $k \in K$, — *марковское отображение, действующее на конечных абелевых группах, и выполнено условие* $\mathbf{P}(k = \theta) > 0$ *для всех* $\theta \in K$. *Тогда для произвольных* $\alpha \in G^{(2)}$, $\alpha \neq 0$, $\theta \in K$, *справедливо неравенство* $|K| \geqslant n_{\alpha,\theta}$.

Доказательство. Зафиксируем произвольные значения $\theta \in K$, $\alpha \in G^{(2)}$, $\alpha \neq 0$. Рассмотрим множество B,

$$B = \{\beta \in G^{(1)} : c_{\alpha,\beta}[\theta] \neq 0\}, \quad |B| = n_{\alpha,\theta},$$

и связанный со множеством B набор векторов $\mathbf{z}(s)$, $s \in B$, размерности $|K|$,

$$\mathbf{z}(s) = (c_{\alpha,s}[k^*]\sqrt{\mathbf{P}(k = k^*)},\ k^* \in K).$$

Из марковского свойства отображения f_k следует, что векторы $\mathbf{z}(s)$, $s \in B$, ортогональны над $\mathbb{C}$ (см. [5, теорема 3]):

$$\mathbf{z}(s_1)\mathbf{z}(s_2)^\top = \sum_{k^* \in K} \mathbf{P}(k = k^*) c_{\alpha,s_1}[k^*]\overline{c_{\alpha,s_2}[k^*]} = 0$$

для всех $s_1 \neq s_2, s_1, s_2 \in B$.

Отметим, что в наборе векторов $\mathbf{z}(s)$, $s \in B$, отсутствует нулевой вектор, поскольку компоненты $c_{\alpha,s}[\theta]$, $s \in B$, не равны нулю и $\mathbf{P}(k = \theta) > 0$. С учетом сделанных замечаний ненулевые векторы $\mathbf{z}(s)$, $s \in B$, ортогональны и, следовательно, линейно независимы над полем $\mathbb{C}$. Для доказательства утверждения теоремы осталось заметить, что количество линейно независимых векторов не может превышать их размерность. □

Приведем численный пример, показывающий достижимость нижней оценки из теоремы 2 для мощности множества K значений случайной величины k.

Пример 9. Пусть $G^{(1)} = G^{(2)} = K = \mathbb{Z}/4$, случайная величина k, имеющая равномерное распределение на множестве K. Строки приведенной ниже матрицы $\mathbf{M}$ задают векторы значений $f_\theta(x)$ случайного отображения $f_k : G^{(1)} \to G^{(2)}$ для различных значений θ случайной величины k,

$$\mathbf{M} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 3 & 2 & 0 \\ 3 & 1 & 1 & 0 \\ 2 & 2 & 3 & 0 \end{pmatrix}, \tag{12}$$

где номер строки в матрице $\mathbf{M}$ соответствует значению $\theta = 0, \ldots, 3$, номер столбца — значению $x = 0, \ldots, 3$.

Прямыми расчетами нетрудно убедиться, что случайное отображение f_k является марковским, матрица $\mathbf{P}$ переходных вероятностей разностей приведена ниже

$$\mathbf{P} = \frac{1}{4} \begin{pmatrix} 4 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Для значений $\theta = 0$, $\alpha = 1$ выполнено равенство $n_{\alpha,\theta} = |K| = 4$, поскольку набор коэффициентов $\{c_{\alpha,\beta}[\theta], \beta \in G^{(1)}\}$ имеет вид

$$\{0.25 + 0.25\mathrm{i}, -0.25 + 0.75\mathrm{i}, 0.25 + 0.25\mathrm{i}, -0.25 - 0.25\mathrm{i}\}.$$

Далее, используя конструкцию из следствия 1 примера 3, рассмотрим случайное отображение $F_{(k_1,\ldots,k_r)} : \left(G^{(1)}\right)^r \to G^{(2)}$,

$$F_{(k_1,\ldots,k_r)}(x_1, \ldots, x_r) = f_{k_1}(x_1) + \cdots + f_{k_r}(x_r), \tag{13}$$

где отображения $f_\theta(x)$, $\theta \in G^{(1)}$, заданы таблично в (12), компоненты случайного вектора $(k_1, \ldots, k_r)$ — независимые копии случайной величины k.

Из марковского свойства отображения f_k следует, что случайное отображение $F_{(k_1,\ldots,k_r)}$ является марковским, при этом для значений $\theta = 0$, $\alpha = 1$ разложение функции $\chi_\alpha(f_\theta(x_1) + \cdots + f_\theta(x_r))$ по системе базисных функций-характеров

$$\{\chi_{\beta_1}(x_1) \ldots \chi_{\beta_r}(x_r), (\beta_1, \ldots, \beta_r) \in \left(G^{(1)}\right)^r\} \tag{14}$$

следует из равенства

$$\chi_\alpha(f_\theta(x_1) + \cdots + f_\theta(x_r)) = \prod_{i=1}^{r} \chi_\alpha(f_\theta(x_r)) = \prod_{i=1}^{r} \left(\sum_{\beta \in G^{(1)}} c_{\alpha,\beta}[\theta] \chi_\beta(x_i) \right),$$

количество ненулевых коэффициентов в указанном разложении равно $|K|^r = 4^r$.

Рассмотрим случайное отображение $h_k : (G^{(1)})^r \to G^{(2)}$, $k \in K_r$, конечное множество K_r не содержит элементов, принимаемых случайной величиной k с нулевой вероятностью. Пусть в набор функций $\{h_\theta(x_1, \ldots, x_r), \theta \in K_r\}$ входит заданная в (13) функция $f_0(x_1) + \cdots + f_0(x_r)$. Тогда, учитывая, что вектор коэффициентов разложения функции $\chi_1(f_0(x_1) + \cdots + f_0(x_r))$ по системе базисных функций-характеров (14) содержит 4^r ненулевых компонент, согласно теореме 2, для выполнения марковского свойства случайного отображения h_k необходимо, чтобы множество K_r содержало не менее 4^r элементов.

Список литературы

[1] Lai X., Massey J. L., Murphy S., “Markov ciphers and differential cryptanalysis”, EuroCrypt 1991, Lect. Notes Comput. Sci., **547**, 1991, 17–38.

[2] Погорелов Б. А., Пудовкина М. А., “Разбиения на биграммах и марковость алгоритмов блочного шифрования”, *Математические вопросы криптографии*, **8**:1 (2017), 107–142.

[3] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М.: Наука, 1970, 272 с.

[4] Денисов О. В., “Критерии марковости алгоритмов блочного шифрования”, *Прикладная дискретная математика*, 2018, № 41, 28–37.

[5] Дрелихов В. О., “Вероятностные свойства статистических связей между входом и выходом марковского итеративного шифра с раундовыми отображениями на абелевых группах”, *Математические вопросы криптографии*, **12**:1 (2021), 59–82.

[6] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*: *Учебник для вузов*, 5-е изд., стер., СПб.: Лань, 2024, 608 с.