ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.212.2+519.719.2

ОБ ОБРАЗАХ И ПРООБРАЗАХ В ГРАФЕ КОМПОЗИЦИИ НЕЗАВИСИМЫХ РАВНОВЕРОЯТНЫХ СЛУЧАЙНЫХ ОТОБРАЖЕНИЙ

В. О. Миронкин

Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия

Изучаются вероятностные характеристики графа случайного отображения $f_{[k]}$ — композиции k независимых равновероятных случайных отображений $f_1, \ldots, f_k$, где $f_i\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$, $n, k \in \mathbb{N}$, $i = 1, \ldots, n$. Получены формулы для распределения длины отрезка апериодичности произвольной вершины в графе отображения $f_{[k]}$ с учётом ряда ограничений. Выписаны формулы для вероятностей принадлежности вершины множеству $f_{[k]}(\{1, \ldots, n\})$ и множеству висячих вершин в графе отображения $f_{[k]}$. Вычислены вероятности инцидентности двух произвольных вершин одной компоненте связности, попадания произвольной вершины в множество прообразов другой вершины, а также появления коллизии в указанном графе.

Ключевые слова: *равновероятное случайное отображение, композиция отображений, граф отображения, образ множества, прообраз вершины, висячая вершина, слой в графе, отрезок апериодичности, коллизия.*

DOI 10.17223/20710410/49/1

ON IMAGES AND PRE-IMAGES IN A GRAPH OF THE COMPOSITION OF INDEPENDENT UNIFORM RANDOM MAPPINGS

V. O. Mironkin

National Research University Higher School of Economics, Moscow, Russia

E-mail: mironkin.v@mail.ru

We study the probability characteristics of the random mapping graph $f_{[k]}$ — the composition of k independent equiprobable random mappings $f_1, \ldots, f_k$, where $f_i\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$, $n, k \in \mathbb{N}$, $i = 1, \ldots, n$. The following results are obtained. For any fixed $x, y \in S = \{1, \ldots, n\}$, $x \neq y$,

$$\mathbf{P}\{f_{[k]}(x) = f_{[k]}(y)\} = \sum_{\substack{s_1, \ldots, s_{k-1} \in \mathbb{N}\colon \\ 2 \geqslant s_1 \geqslant \ldots \geqslant s_{k-1}}} \frac{q(2, s_1)}{n^{s_{k-1}-1}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}),$$

where $q(a,b) = \mathrm{C}_n^{n-b}\left(\frac{b}{n}\right)^a \sum\limits_{l=0}^{b} \mathrm{C}_b^l(-1)^l\left(1-\frac{l}{b}\right)^a$. For any fixed $x \in S$,

$$\mathbf{P}\{x \in f_{[k]}(S)\} = \frac{1}{n}\sum_{l=1}^{n}\left(\frac{(n)_l}{n^l}\right)^k + \\ + \sum_{l=1}^{n-2}\sum_{t=1}^{n-l-1}\sum_{m=1}^{n-t-l}(-1)^{m-1}\mathrm{C}_{n-1}^{m}\sum_{\substack{s_1,\ldots,s_{k-1}\in\mathbb{N}:\\ m\geqslant s_1\geqslant\ldots\geqslant s_{k-1}}}\frac{q(m,s_1)}{n^{s_{k-1}}}\prod_{i=1}^{k-2}q(s_i,s_{i+1})V_{s_1,\ldots,s_{k-1}}^{\{k,m\}},$$

where

$$V_{s_1,\ldots,s_{k-1}}^{\{k,m\}} = \mathbf{P}\{x \in H_{f_{[k]}}^{(t,l)} \mid D_{s_1,\ldots,s_{k-1},1}^{\{k\}}(y_1,\ldots,y_m), f_{[k]}(y_1) = x\} = \\ = \frac{1}{n}\prod_{i=m+1}^{t+l+m-1}\left(1-\frac{i}{n}\right)\prod_{i=1}^{k-1}\prod_{j=s_i+1}^{t+l+s_i-2}\left(1-\frac{j}{n}\right)\sum_{v=0}^{k-1}\prod_{u=1}^{v}\left(1-\frac{t+l+s_u-1}{n}\right),$$

$H_f^{(t,l)}$ is t-th layer of cycles of length l in graph G_f, $D_{s_1,\ldots,s_k}^{\{k\}}(y_1,\ldots,y_m) = \bigcap\limits_{i=1}^{k}\{|\{f_{[i]}(y_1),\ldots,f_{[i]}(y_m)\}| = s_i\}$, and $(n)_z = n(n-1)\ldots(n-z+1)$. For any fixed $x \in S \setminus S'$ and for any $r \in \{1,\ldots,n-1\}$, $S' \subseteq S$, $|S'| = r$, $z \in \{1,\ldots,n\}$,

$$\mathbf{P}\{\tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' = \varnothing\} = \\ = \left(1-\left(1-\frac{z}{n}\right)\left(1-\frac{z-1}{n}\right)^{k-1}\right)\left(\frac{(n)_{z-1}}{n^{z-1}}\right)^{k-1}\frac{(n)_{r+z}}{n^{z-1}\,(n)_{r+1}},$$

where $\mathcal{R}_{f_{[k]}}(x)$ is the aperiodicity segment of vertex x in the graph of mapping $f_{[k]}$, $\tau_{f_{[k]}}(x) = \min\{t \in \mathbb{N}\colon {f_{[k]}}^t(x) \in \{x, f_{[k]}(x),\ldots,{f_{[k]}}^{t-1}(x)\}\}$. For any fixed $x, y \in S$, $x \neq y$, and for any $r \in \{1,\ldots,n\}$,

$$\mathbf{P}\{y \in (f_{[k]})^{-r}(x)\} = \frac{1}{n}\left(1-\frac{1}{n-1}\sum_{z\in Q_r\setminus\{1\}}\left(\frac{(n)_z}{n^z}\right)^k\right),$$

where $Q_r = \{m \in \mathbb{N}\colon m|r\}$.

Keywords: *equiprobable random mapping, composition of mappings, graph of a mapping, image of a multitude, pre-image of a vertex, initial vertex, layer in a graph, aperiodicity segment, collision.*

Введение

Настоящая работа продолжает цикл работ [1, 2], посвящённых изучению вероятностных свойств и характеристик композиции независимых равновероятных случайных отображений [3 – 7] — математического объекта, используемого при моделировании итерационных механизмов защиты информации, в том числе алгоритмов выработки производных ключей [8, 9], итерации которых строятся с помощью разных процедур и разных случайных элементов (например, раундовых ключей, векторов инициализации).

Аналогично [1], рассмотрим конечное множество $S = \{1,\ldots,n\}$, $n > 1$, и вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространством элементарных исходов Ω является множество $\mathfrak{S}$ всех n^n отображений $f\colon S \to S$, алгеброй событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$, соответствующая равновероятным случайным отображениям, задана следующим образом:

$$\forall f \in \Omega\ \left(\mathbf{P}(f) = n^{-n}\right). \tag{1}$$

Будем использовать следующие определения для характеристик графа отображения (см. также [10 – 13]; отображение f считается детерминированным).

Определение 1. *Графом отображения* f называется ориентированный граф $G_f = (S, E_f)$ с множеством вершин S и множеством ориентированных рёбер $E_f = \{(x, f(x))\colon x \in S\} \subset S^2$.

Определение 2. *Компонентой связности* $\mathcal{K}_f(x)$ графа G_f, содержащей вершину $x \in S$, называется множество вершин

$$\left\{y \in S\colon f^l(y) = f^k(x) \text{ для некоторых } k, l \geqslant 0\right\}.$$

Определение 3. Вершина $x \in S$ называется *циклической вершиной* графа G_f отображения f, если существует такое $b \geqslant 1$, что $f^b(x) = x$.

Обозначим: $C(G_f)$ — множество циклических вершин графа G_f; $C_l(G_f)$ — множество вершин, лежащих на циклах длины $l \in \{1, \ldots, n\}$; $\beta_f(x)$ — длина цикла компоненты $\mathcal{K}_f(x)$.

Определение 4. *Высотой* $\alpha_f(x)$ вершины $x \in S$ в графе G_f называется расстояние от этой вершины до ближайшей циклической вершины:

$$\alpha_f(x) = \min\{m \geqslant 0\colon f^m(x) \in C(G_f)\}.$$

Определение 5. *Отрезком апериодичности* $\mathcal{R}_f(x)$, начинающимся в вершине $x \in S$ графа G_f, называется отрезок выходящей из x траектории от x до её первого самопересечения.

Через $\tau_f(x)$ обозначим случайную величину, равную длине отрезка апериодичности $\mathcal{R}_f(x)$:

$$\tau_f(x) = \min\left\{t \in \mathbb{N}\colon f^t(x) \in \left\{x, f(x), \ldots, f^{t-1}(x)\right\}\right\}.$$

Как и в [1], зависимость случайных величин $\alpha_f(x)$, $\beta_f(x)$ и $\tau_f(x)$ от параметра n отображать не будем.

Определение 6. Для произвольных $l \in \{1, \ldots, n\}$, $t \in \{0, \ldots, n-l\}$ назовём *t-м слоем циклов длины l* в графе G_f множество вершин

$$H_f^{(t,l)} = \{x \in S\colon \alpha_f(x) = t, \beta_f(x) = l\}.$$

Далее для произвольного $k \in \mathbb{N}$ рассмотрим последовательность независимых отображений $f_1, \ldots, f_k$, имеющих распределение (1) на $\mathfrak{S}$. Через $f_{[k]}$ обозначим композицию отображений: $f_k(\ldots(f_1(x))\ldots)$, $x \in S$; $f_{[0]}$ будем понимать как тождественное отображение.

Отметим, что если случайные отображения $f_1, \ldots, f_k$ имеют равновероятное распределение (1), то распределение $f_{[k]}$ при $k > 1$ не является равновероятным на $\mathfrak{S}$, так как $\left|f_{[1]}(S)\right| \geqslant \left|f_{[2]}(S)\right| \geqslant \ldots$

В настоящей работе изучаются вероятностные характеристики множества $f_{[k]}(S)$ и множества прообразов произвольной вершины $x \in S$ в случае, когда k произвольное и случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$.

1. Образ множества S и коллизии при отображении $f_{[k]}$

В рамках решения задач, связанных с изучением множества $f_{[k]}(S)$, в [4] получены оценки среднего размера образа подмножества множества S при действии композиции случайных отображений.

Результаты, приведённые в данной работе, позволяют выписать точные формулы для ряда вероятностных характеристик образа $f_{[k]}(S)$ исходного множества S, в том числе для его среднего размера.

Для произвольных $k, m, s_1, \ldots, s_k \in \mathbb{N}$, $n \geqslant m \geqslant s_1 \geqslant \ldots \geqslant s_k$, и произвольных фиксированных различных вершин $y_1, \ldots, y_m \in S$ рассмотрим событие

$$D^{\{k\}}_{s_1,\ldots,s_k}(y_1, \ldots, y_m) = \bigcap_{i=1}^{k} \{|\{f_{[i]}(y_1), \ldots, f_{[i]}(y_m)\}| = s_i\}.$$

Лемма 1. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых $m, s_1, \ldots, s_k \in \mathbb{N}$, $n \geqslant m \geqslant s_1 \geqslant \ldots \geqslant s_k$, и любых фиксированных различных $y_1, \ldots, y_m \in S$ справедливо равенство

$$\mathbf{P}\{D^{\{k\}}_{s_1,\ldots,s_k}(y_1, \ldots, y_m)\} = q(m, s_1) \prod_{i=1}^{k-1} q(s_i, s_{i+1}), \tag{2}$$

где $q(a, b) = \mathrm{C}_n^{n-b} \left(\dfrac{b}{n}\right)^a \sum\limits_{l=0}^{b} \mathrm{C}_b^l (-1)^l \left(1 - \dfrac{l}{b}\right)^a$.

Доказательство. Для произвольных $i \in \{1, \ldots, k\}$, $a \in \{1, \ldots, m\}$ и $b \in \{1, \ldots, a\}$ определим событие

$$D^{(i)}(a, b) = \{|\{f_i(1), \ldots, f_i(a)\}| = b\},$$

вероятность которого, согласно [14], равна

$$q^{(i)}(a, b) = \mathbf{P}\{D^{(i)}(a, b)\} = \mathbf{P}\{\mu_0(a, n) = n - b\} = \mathrm{C}_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^{b} \mathrm{C}_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a, \tag{3}$$

где случайная величина $\mu_0(a, n)$ — число пустых ячеек в схеме равновероятных размещений, в которой a частиц независимо друг от друга размещаются в n ячейках [14].

Поскольку из полученного выражения следует, что $q^{(i)}(a, b)$ не зависят от i, верхний индекс в обозначении $q^{(i)}(a, b)$ опустим.

С учётом (3) в силу независимости отображений $f_1, \ldots, f_k$ для произвольного $m \in \mathbb{N}$, произвольных фиксированных различных вершин $y_1, \ldots, y_m \in S$ и произвольного набора $(s_1, \ldots, s_k)$, такого, что $n \geqslant m \geqslant s_1 \geqslant \ldots \geqslant s_k$, получаем равенство (2). ■

Определение 7. *Коллизией* в графе отображения G_f называется произвольная пара вершин $x, y \in S$, $x \neq y$, для которых $f(x) = f(y)$.

Лемма 1 позволяет вычислить вероятность события, состоящего в том, что произвольные фиксированные вершины $x, y \in S$, $x \neq y$, образуют коллизию в графе отображения $G_{f_{[k]}}$.

Теорема 1. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, справедливо равенство

$$\mathbf{P}\{f_{[k]}(x) = f_{[k]}(y)\} = \sum_{\substack{s_1,\ldots,s_{k-1}: \\ 2 \geqslant s_1 \geqslant \ldots \geqslant s_{k-1}}} \frac{q(2, s_1)}{n^{s_{k-1}-1}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}),$$

где $q(a, b) = \mathrm{C}_n^{n-b} \left(\dfrac{b}{n}\right)^a \sum\limits_{l=0}^{b} \mathrm{C}_b^l (-1)^l \left(1 - \dfrac{l}{b}\right)^a$.

Доказательство. Для произвольных фиксированных $x, y \in S$, $x \neq y$, с учётом леммы 1 имеет место цепочка соотношений

$$\mathbf{P}\{f_{[k]}(x) = f_{[k]}(y)\} = \sum_{\substack{s_1,\ldots,s_{k-1}:\\ 2\geqslant s_1\geqslant\ldots\geqslant s_{k-1}}} \mathbf{P}\{D^{\{k\}}_{s_1,\ldots,s_{k-1},1}(x,y)\} =$$

$$= \sum_{\substack{s_1,\ldots,s_{k-1}:\\ 2\geqslant s_1\geqslant\ldots\geqslant s_{k-1}}} q(2,s_1)q(s_{k-1},1)\prod_{i=1}^{k-2} q(s_i,s_{i+1}) = \sum_{\substack{s_1,\ldots,s_{k-1}:\\ 2\geqslant s_1\geqslant\ldots\geqslant s_{k-1}}} \frac{q(2,s_1)}{n^{s_{k-1}-1}}\prod_{i=1}^{k-2} q(s_i,s_{i+1}).$$

Теорема доказана. ■

Замечание 1. Согласно теореме 1, в силу равноправия вершин из S среднее число коллизий в графе $G_{f_{[k]}}$ определяется величиной

$$\mathrm{C}_n^2\mathbf{P}\{f_{[k]}(x) = f_{[k]}(y)\}.$$

Определение 8. Вершина $x \in S$ в графе G_f называется *висячей*, если не существует $y \in S$, для которого $f(y) = x$.

Теорема 2. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ справедливо равенство

$$\mathbf{P}\{x \in f_{[k]}(S)\} = \frac{1}{n}\sum_{l=1}^{n}\left(\frac{(n)_l}{n^l}\right)^k +$$
$$+\sum_{l=1}^{n-2}\sum_{t=1}^{n-l-1}\sum_{m=1}^{n-t-l}(-1)^{m-1}\mathrm{C}_{n-1}^m \sum_{\substack{s_1,\ldots,s_{k-1}:\\ m\geqslant s_1\geqslant\ldots\geqslant s_{k-1}}} \frac{q(m,s_1)}{n^{s_{k-1}}}\prod_{i=1}^{k-2} q(s_i,s_{i+1})V^{\{k,m\}}_{s_1,\ldots,s_{k-1}},$$

где $q(a,b) = \mathrm{C}_n^{n-b}\left(\dfrac{b}{n}\right)^a \displaystyle\sum_{l=0}^{b}\mathrm{C}_b^l(-1)^l\left(1-\frac{l}{b}\right)^a$; $V^{\{k,m\}}_{s_1,\ldots,s_{k-1}}$ определяется соотношением (9) (см. далее); $(n)_z = n(n-1)\ldots(n-z+1)$ — z-я факториальная степень числа n.

Доказательство. Заметим, что произвольная фиксированная вершина $x \in S$ лежит в множестве $f_{[k]}(S)$ в случаях, когда она либо является циклической в графе $G_{f_{[k]}}$, либо лежит на подходах к циклу и при этом не является висячей. Таким образом, выполняется равенство

$$\{x \in f_{[k]}(S)\} = \{x \in C(G_{f_{[k]}})\} \cup \bigcup_{l=1}^{n-2}\bigcup_{t=1}^{n-l-1}\{x \in H^{(t,l)}_{f_{[k]}}, |(f_{[k]})^{-1}(x)| \geqslant 1\},$$

где под знаком объединения стоят несовместные события. Тогда, переходя к вероятностям событий, получаем

$$\mathbf{P}\{x \in f_{[k]}(S)\} = \mathbf{P}\{x \in C(G_{f_{[k]}})\} + \sum_{l=1}^{n-2}\sum_{t=1}^{n-l-1}\mathbf{P}\{x \in H^{(t,l)}_{f_{[k]}}, |(f_{[k]})^{-1}(x)| \geqslant 1\}. \qquad (4)$$

Согласно [2], первое слагаемое в правой части (4) равно

$$\mathbf{P}\{x \in C(G_{f_{[k]}})\} = \frac{1}{n}\sum_{l=1}^{n}\left(\frac{(n)_l}{n^l}\right)^k. \qquad (5)$$

Рассмотрим отдельно величины, стоящие под знаками суммирования в (4), при фиксированных $l \in \{1,\dots,n-2\}$, $t \in \{1,\dots,n-l-1\}$. По формуле включения-исключения в силу равноправия всех вершин $y \in S \setminus \{x\}$ имеем

$$\begin{gathered}\mathbf{P}\{x \in H^{(t,l)}_{f_{[k]}}, |(f_{[k]})^{-1}(x)| \geqslant 1\} = \mathbf{P}\{\bigcup_{y \in S\setminus\{x\}} \{x \in H^{(t,l)}_{f_{[k]}}, y \in (f_{[k]})^{-1}(x)\}\} = \\ = \sum_{m=1}^{n-t-l} (-1)^{m-1} \mathrm{C}^m_{n-1} \mathbf{P}\left\{\begin{array}{c} x \in H^{(t,l)}_{f_{[k]}}, f_{[k]}(y_1) = \ldots = f_{[k]}(y_m) = x, \\ y_1,\dots,y_m \in S\setminus\{x\} \text{ — различны} \end{array}\right\}.\end{gathered} \tag{6}$$

Рассмотрим вероятность, стоящую под знаком суммирования в правой части (6), при фиксированном значении $m \in \{1,\dots,n-l-t\}$. Для произвольных фиксированных различных $y_1,\dots,y_m \in S \setminus \{x\}$ по формуле полной вероятности имеем

$$\begin{gathered}\mathbf{P}\{x \in H^{(t,l)}_{f_{[k]}}, f_{[k]}(y_1) = \ldots = f_{[k]}(y_m) = x\} = \\ = \sum_{\substack{s_1,\dots,s_{k-1}: \\ m \geqslant s_1 \geqslant \ldots \geqslant s_{k-1}}} \mathbf{P}\{D^{\{k\}}_{s_1,\dots,s_{k-1},1}(y_1,\dots,y_m), f_{[k]}(y_1) = x, x \in H^{(t,l)}_{f_{[k]}}\} = \\ = \sum_{\substack{s_1,\dots,s_{k-1}: \\ m \geqslant s_1 \geqslant \ldots \geqslant s_{k-1}}} \mathbf{P}\{x \in H^{(t,l)}_{f_{[k]}} \mid D^{\{k\}}_{s_1,\dots,s_{k-1},1}(y_1,\dots,y_m), f_{[k]}(y_1) = x\} \times \\ \times \mathbf{P}\{D^{\{k\}}_{s_1,\dots,s_{k-1},1}(y_1,\dots,y_m), f_{[k]}(y_1) = x\}.\end{gathered} \tag{7}$$

При этом в силу независимости отображений $f_1,\dots,f_k$ с учётом леммы 1

$$\begin{gathered}\mathbf{P}\{D^{\{k\}}_{s_1,\dots,s_{k-1},1}(y_1,\dots,y_m), f_{[k]}(y_1) = x\} = \\ = \frac{1}{n^{s_{k-1}}} \mathbf{P}\{D^{\{k-1\}}_{s_1,\dots,s_{k-1}}(y_1,\dots,y_m)\} = \frac{q(m,s_1)}{n^{s_{k-1}}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}).\end{gathered} \tag{8}$$

Далее заметим, что вычисление условной вероятности, стоящей под знаком суммирования в правой части (7), проводится аналогично [2] с поправкой на наличие дополнительных $s_1,\dots,s_{k-1},m$ вершин в множествах $f_{[1]}(S),\dots,f_{[k]}(S)$ соответственно, а именно:

$$\begin{gathered}V^{\{k,m\}}_{s_1,\dots,s_{k-1}} = \mathbf{P}\{x \in H^{(t,l)}_{f_{[k]}} \mid D^{\{k\}}_{s_1,\dots,s_{k-1},1}(y_1,\dots,y_m), f_{[k]}(y_1) = x\} = \\ = \frac{1}{n} \prod_{i=m+1}^{t+l+m-1} \left(1 - \frac{i}{n}\right) \prod_{i=1}^{k-1} \prod_{j=s_i+1}^{t+l+s_i-2} \left(1 - \frac{j}{n}\right) \sum_{v=0}^{k-1} \prod_{u=1}^{v} \left(1 - \frac{t+l+s_u-1}{n}\right).\end{gathered} \tag{9}$$

Подставив (8) и (9) в (7), с учётом (4)–(6) получим искомый результат. ■

Следствие 1. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1,\dots,f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда

$$\mathbf{E}\left|f_{[k]}(S)\right| = n\mathbf{P}\{x \in f_{[k]}(S)\}.$$

Из определения 8 следует, что множество висячих вершин графа G_f совпадает с множеством вершин, не имеющих прообразов.

Через $T_{f_{[k]}}$ обозначим множество висячих вершин в графе $G_{f_{[k]}}$, $k \in \mathbb{N}$. Множество T_f исследовано, например, в [13]. Рассмотрим случай $k \geqslant 2$. Найдём вероятность попадания случайной вершины графа $G_{f_{[k]}}$ в множество $T_{f_{[k]}}$.

Замечание 2. Из равенства $S = T_{f_{[k]}} \cup f_{[k]}(S)$, где $T_{f_{[k]}} \cap f_{[k]}(S) = \varnothing$, вытекает выражение для вероятности попадания произвольной вершины x в множество висячих вершин в графе $G_{f_{[k]}}$:

$$\mathbf{P}\{x \in T_{f_{[k]}}\} = 1 - \mathbf{P}\{x \in f_{[k]}(S)\}.$$

При этом в силу равноправия вершин из S выполняются соотношения

$$\mathbf{E}\left|T_{f_{[k]}}\right| = n\mathbf{P}\{x \in T_{f_{[k]}}\} = n - n\mathbf{P}\{x \in f_{[k]}(S)\}.$$

2. Инцидентность вершин одной компоненте связности в графе отображения $f_{[k]}$

Для вычисления вероятности попадания вершин из S в одну компоненту связности графа $G_{f_{[k]}}$ докажем ряд вспомогательных утверждений.

Выделим в исходном множестве S некоторое подмножество вершин $S' = \{y_1, \ldots, y_r\} \subseteq S$, где $r < n$. Для данного множества вычислим вероятность события, заключающегося в том, что отрезок апериодичности $\mathcal{R}_{f_{[k]}}(x)$ произвольной вершины $x \in S \setminus S'$ не проходит через вершины множества S'.

Теорема 3. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S \setminus S'$ и любых $r \in \{1, \ldots, n-1\}$, $S' \subseteq S$ ($|S'| = r$) и $z \in \{1, \ldots, n\}$ справедливо равенство

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' = \varnothing\right\} =$$
$$= \left(1 - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^{k-1}\right)\left(\frac{(n)_{z-1}}{n^{z-1}}\right)^{k-1} \frac{(n)_{r+z}}{n^{z-1}\,(n)_{r+1}}.$$

Доказательство. Зафиксируем $S' = \{y_1, \ldots, y_r\} \subseteq S$ и $x \in S \setminus S'$. По формуле условной вероятности

$$\mathbf{P}\{\tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' = \varnothing\} = \mathbf{P}\{\tau_{f_{[k]}}(x) = z\}\mathbf{P}\{\mathcal{R}_{f_{[k]}}(x) \cap S' = \varnothing \mid \tau_{f_{[k]}}(x) = z\} =$$
$$= \left(F_{[k]}(z) - F_{[k]}(z-1)\right)\frac{(n-r-1)_{z-1}z}{(n-1)_{z-1}z},$$

где $(n-1)_{z-1}\,z$ — общее число отрезков апериодичности длины z графа $G_{f_{[k]}}$, начинающихся в вершине $x \in S$. Преобразовав полученное выражение с учётом равенства [1]

$$F_k(z) = 1 - \left(1 - \frac{z}{n}\right)\left(\frac{(n)_z}{n^z}\right)^k,$$

получим искомое равенство. ■

Следствие 2. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S \setminus S'$ и любых $r \in \{1, \ldots, n-1\}$, $S' \subseteq S$, $|S'| = r$, справедливо равенство

$$\mathbf{P}\{\mathcal{R}_{f_{[k]}}(x) \cap S' = \varnothing\} =$$
$$= \sum_{z=1}^{n-r-1}\left(1 - \left(1 - \frac{z+1}{n}\right)\left(1 - \frac{z}{n}\right)^{k-1}\right)\left(\frac{(n)_z}{n^z}\right)^{k-1}\frac{(n)_{r+z+1}}{n^z(n)_{r+1}}. \tag{10}$$

Формулы, полученные в теореме 3 и следствии 2, могут быть использованы при решении задачи оценки допустимого периода эксплуатации долговременных ключей в процессе функционирования итерационных алгоритмов типа [8] при наличии информации о «слабых» ключах.

Далее для случая $r = 1$ вычислим вероятность того, что вершина $y = y_1$, соответствующая некоторому «слабому» ключу, попадёт в компоненту связности $\mathcal{K}_{f_{[k]}}(x)$, где $x \in S \setminus \{y\}$ — произвольный фиксированный.

Теорема 4. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, справедливо равенство

$$\begin{gathered}\mathbf{P}\{y \in \mathcal{K}_{f_{[k]}}(x)\} = 1 - \sum_{z=1}^{n-2} \left(1 - \left(1 - \frac{z+1}{n}\right)\left(1 - \frac{z}{n}\right)^{k-1}\right) \left(\frac{(n)_z}{n^z}\right)^k \frac{\mathrm{C}_{n-z}^2}{\mathrm{C}_n^2} + \\ + \sum_{z=1}^{n-1} \sum_{u=1}^{n-z} \frac{z^2}{n-1} \left(\frac{(n)_{z+u}}{n^{z+u}}\right)^k + \sum_{z=1}^{n-1} \sum_{u=0}^{n-z-1} \sum_{s=1}^{k-1} \sum_{t=1}^{k-1} \chi(z,u,s,t) + \\ + \sum_{z=1}^{n-1} \sum_{u=z}^{n-1} \frac{(z^2-z)(n-u)}{u(n-1)} \left(\frac{(n)_u}{n^u}\right)^k \left(1 - \left(1 - \frac{u}{n}\right)^{k-1}\right),\end{gathered}$$

где $\chi(z,u,s,t)$ определяется соотношением (16) (см. далее).

Доказательство. Для произвольной фиксированной пары вершин $x, y \in S$, $x \neq y$, выполняется равенство событий

$$\{y \in \mathcal{K}_{f_{[k]}}(x)\} = \{y \in \mathcal{R}_{f_{[k]}}(x)\} \cup \bigcup_{z=1}^{n-1} \bigcup_{u=0}^{n-z-1} \{\tau_{f_{[k]}}(x) = z, f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x)\},$$

где под знаками объединения стоят несовместные события. Поэтому, переходя к вероятностям с учётом равноправия всех вершин из S, получаем

$$\begin{gathered}\mathbf{P}\{y \in \mathcal{K}_{f_{[k]}}(x)\} = \mathbf{P}\{y \in \mathcal{R}_{f_{[k]}}(x)\} + \\ + \sum_{z=1}^{n-1} \sum_{u=0}^{n-z-1} \mathbf{P}\{\tau_{f_{[k]}}(x) = z, f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x)\}.\end{gathered} \tag{11}$$

Выражение для первого слагаемого в (11) следует из (10) при $r = 1$:

$$\begin{gathered}\mathbf{P}\{y \in \mathcal{R}_{f_{[k]}}(x)\} = 1 - \mathbf{P}\{y \notin \mathcal{R}_{f_{[k]}}(x)\} = \\ = 1 - \sum_{z=1}^{n-2} \left(1 - \left(1 - \frac{z+1}{n}\right)\left(1 - \frac{z}{n}\right)^{k-1}\right) \left(\frac{(n)_z}{n^z}\right)^k \frac{\mathrm{C}_{n-z}^2}{\mathrm{C}_n^2}.\end{gathered} \tag{12}$$

Вычислим вероятность события, стоящего под знаками суммирования в (11) при фиксированных значениях $z \in \{1, \ldots, n-1\}$ и $u \in \{0, \ldots, n-z-1\}$. Для указанных значений z, u определим события

$$A_{z,s}^{\{x\}} = \left\{ \min_{j \in \{1,\ldots,k\}} \{j \colon f_{[j]}(f_{[k]}^{z-1}(x)) \in \{f_{[j]}(f_{[k]}^m(x)), m = 0, \ldots, z-2\}\} = s \right\},$$

$$B_{u,s}^{\{x,y\}} = \left\{ \min_{j \in \{1,\ldots,k\}} \{j \colon f_{[j]}(f_{[k]}^u(y)) \in \{f_{[i]}(f_{[k]}^m(x)), m = 0, \ldots, z-1, i = 1, \ldots, k\}\} = s \right\}.$$

Тогда выполняется равенство

$$\{\tau_{f_{[k]}}(x)=z, f^u_{[k]}(y)\notin\mathcal{R}_{f_{[k]}}(x), f^{u+1}_{[k]}(y)\in\mathcal{R}_{f_{[k]}}(x)\}=$$
$$=\bigcup_{s=1}^{k}\bigcup_{t=1}^{k}\left\{\begin{array}{c}\tau_{f_{[k]}}(x)=z, A^{\{x\}}_{z,s}, B^{\{x,y\}}_{u,t},\\ f^u_{[k]}(y)\notin\mathcal{R}_{f_{[k]}}(x), f^{u+1}_{[k]}(y)\in\mathcal{R}_{f_{[k]}}(x)\end{array}\right\}.$$

Вычислим вероятности $p_{z,u,s,t}$ событий, стоящих под знаком объединения, при фиксированных значениях $s\in\{1,\ldots,k\}$, $t\in\{1,\ldots,k\}$.

В случае $s=t=k$:

$$p_{z,u,k,k}=\frac{z^2}{n}\prod_{i=2}^{z+u}\left(1-\frac{i}{n}\right)\prod_{i=1}^{z+u}\left(1-\frac{i}{n}\right)^{k-1}=\frac{z^2}{n-1}\left(\frac{(n)_{z+u+1}}{n^{z+u+1}}\right)^k. \tag{13}$$

В случае $s=k$, $t<k$:

$$\begin{aligned}p_{z,u,k,t}&=\frac{z(z-1)}{n}\prod_{i=2}^{z+u}\left(1-\frac{i}{n}\right)\prod_{i=1}^{z+u-1}\left(1-\frac{i}{n}\right)^{k-1}\left(1-\frac{z+u}{n}\right)^{t-1}=\\&=\frac{z(z-1)}{n-1}\left(\frac{(n)_{z+u}}{n^{z+u}}\right)^k\left(1-\frac{z+u}{n}\right)^t.\end{aligned} \tag{14}$$

В случае $s<k$, $t=k$:

$$\begin{aligned}p_{z,u,s,k}&=\frac{z(z-1)}{n}\prod_{i=2}^{z+u}\left(1-\frac{i}{n}\right)\prod_{i=1}^{z+u-1}\left(1-\frac{i}{n}\right)^{k-1}\left(1-\frac{z+u}{n}\right)^{s-1}=\\&=\frac{z(z-1)}{n-1}\left(\frac{(n)_{z+u}}{n^{z+u}}\right)^k\left(1-\frac{z+u}{n}\right)^s.\end{aligned} \tag{15}$$

В случае $s<k$, $t<k$:

$$\begin{aligned}\chi(z,u,s,t)=p_{z,u,s,t}&=\frac{(z-1)^2}{n}\prod_{i=2}^{z+u}\left(1-\frac{i}{n}\right)\prod_{i=1}^{z+u-2}\left(1-\frac{i}{n}\right)^{k-1}\times\\\times\left(1-\frac{z+u-1}{n}\right)^{s-1}&\left(1-\frac{z+u}{n}\right)^{\min(t,s)-1}\left(1-\frac{z+u-1}{n}\right)^{t-\min(t,s)}=\\=\frac{(z-1)^2}{n-1}&\left(\frac{(n)_{z+u-1}}{n^{z+u-1}}\right)^k\left(1-\frac{z+u-1}{n}\right)^{s+t-\min(t,s)}\left(1-\frac{z+u}{n}\right)^{\min(t,s)}.\end{aligned} \tag{16}$$

В итоге, подставив выражения (12)–(16) в (11) и сгруппировав слагаемые, получим искомую формулу. ■

Замечание 3. Для средней мощности компоненты связности произвольной фиксированной вершины $x\in S$ в графе $G_{f_{[k]}}$ справедливо равенство

$$\mathbf{E}|\mathcal{K}_{f_{[k]}}(x)|=(n-1)\mathbf{P}\{y\in\mathcal{K}_{f_{[k]}}(x)\}+1.$$

3. Прообразы случайной вершины в графе отображения $f_{[k]}$

Для произвольного фиксированного $x\in S$ и произвольного $r\in\mathbb{N}$ через $\left(f_{[k]}\right)^{-r}(x)$ обозначим множество $\{y\in S\colon f^r_{[k]}(y)=x\}$. Дополнительно для произвольных $j,r\in\mathbb{N}$ определим

$$Q_r=\{m\in\mathbb{N}\colon m|r\}. \tag{17}$$

Заметим, что для произвольного фиксированного $x \in S$ вероятность события $\{y \in \in \left(f_{[k]}\right)^{-r}(x)\}$ зависит от выбора $y \in S$, а именно от выполнения и невыполнения условия $y = x$. Так, в частности, в случае $y = x$ выполняется равенство

$$\{x \in \left(f_{[k]}\right)^{-r}(x)\} = \bigcup_{m \in Q_r} \{x \in C_m(G_{f_{[k]}})\},$$

где под знаком объединения стоят несовместные события, и поэтому для равновероятных независимых случайных отображений $f_1, \ldots, f_k$ с учётом [1]

$$\mathbf{P}\{x \in \left(f_{[k]}\right)^{-r}(x)\} = \frac{1}{n} \sum_{m \in Q_r} \left(\frac{(n)_m}{n^m}\right)^k.$$

В случае $y \neq x$ справедлив следующий результат.

Теорема 5. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $r \in \{1, \ldots, n\}$ справедливо равенство

$$\mathbf{P}\{y \in \left(f_{[k]}\right)^{-r}(x)\} = \frac{1}{n}\left(1 - \frac{1}{n-1} \sum_{z \in Q_r \setminus \{1\}} \left(\frac{(n)_z}{n^z}\right)^k\right),$$

где Q_r определяется соотношением (17).

Доказательство. Для произвольных фиксированных $x, y \in S$, $x \neq y$, по формуле полной вероятности

$$\begin{gathered}\mathbf{P}\{y \in \left(f_{[k]}\right)^{-r}(x)\} = \sum_{z \in Q_r \setminus \{1\}} \mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x\} + \\ + \sum_{z \in \overline{Q}_r} \mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x\} + \sum_{z=r+1}^{n} \mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x\},\end{gathered} \tag{18}$$

где $\overline{Q}_r = \{1, \ldots, r\} \setminus Q_r$. Заметим, что в случае $z \in Q_r \setminus \{1\}$

$$\mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x, y \in C(G_{f_{[k]}})\} = 0.$$

Тогда для величин, стоящих под первым знаком суммирования в (18), имеем

$$\begin{gathered}\mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x\} = \mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x, y \notin C(G_{f_{[k]}})\} = \\ = \mathbf{P}\{\tau_{f_{[k]}}(y) = z, y \notin C(G_{f_{[k]}})\}\mathbf{P}\{f^r_{[k]}(y) = x \mid \tau_{f_{[k]}}(y) = z, y \notin C(G_{f_{[k]}})\} = \\ = \left(\mathbf{P}\{\tau_{f_{[k]}}(y) = z\} - \mathbf{P}\{y \in C_z(G_{f_{[k]}})\}\right)\frac{(n-2)_{z-2}(z-1)}{(n-1)_{z-1}(z-1)} = \\ = \frac{1}{n-1}\mathbf{P}\{\tau_{f_{[k]}}(y) = z\} - \frac{1}{n-1}\mathbf{P}\{y \in C_z(G_{f_{[k]}})\}.\end{gathered} \tag{19}$$

В случае $z \in \overline{Q}_r \cup \{r+1, \ldots, n\}$ на расположение вершины $y \in \mathcal{K}_{f_{[k]}}(x)$ никаких дополнительных ограничений не накладывается, поэтому

$$\begin{gathered}\mathbf{P}\{\tau_{f_{[k]}}(y) = z, f^r_{[k]}(y) = x\} = \mathbf{P}\{\tau_{f_{[k]}}(y) = z\}\mathbf{P}\{f^r_{[k]}(y) = x \mid \tau_{f_{[k]}}(y) = z\} = \\ = \mathbf{P}\{\tau_{f_{[k]}}(y) = z\}\frac{(n-2)_{z-2}}{(n-1)_{z-1}} = \frac{1}{n-1}\mathbf{P}\{\tau_{f_{[k]}}(y) = z\}.\end{gathered} \tag{20}$$

Подставив выражения (19) и (20) в (18), с учётом равенства [2]

$$\mathbf{P}\{\tau_{f_{[k]}}(y) > z\} = \left(1 - \frac{z}{n}\right)\left(\frac{(n)_z}{n^z}\right)^k$$

и равенства [1]

$$\mathbf{P}\{x \in C_z(G_{f_{[k]}})\} = \frac{1}{n}\left(\frac{(n)_z}{n^z}\right)^k$$

получаем искомую формулу

$$\mathbf{P}\{y \in (f_{[k]})^{-r}(x)\} = \frac{1}{n-1}\left(\sum_{z=2}^{n}\mathbf{P}\{\tau_{f_{[k]}}(y) = z\} - \sum_{z\in Q_r\setminus\{1\}}\mathbf{P}\{y \in C_z(G_{f_{[k]}})\}\right) =$$

$$= \frac{1}{n-1}\mathbf{P}\{\tau_{f_{[k]}}(y) > 1\} - \frac{1}{n-1}\sum_{z\in Q_r\setminus\{1\}}\mathbf{P}\{y \in C_z(G_{f_{[k]}})\} =$$

$$= \frac{1}{n}\left(1 - \frac{1}{n-1}\sum_{z\in Q_r\setminus\{1\}}\left(\frac{(n)_z}{n^z}\right)^k\right).$$

Теорема доказана. ■

Замечание 4. Для среднего числа прообразов произвольной фиксированной вершины $x \in S$ в графе $G_{f_{[k]}}$ справедлива цепочка соотношений

$$\mathbf{E}\left|(f_{[k]})^{-r}(x)\right| = \mathbf{E}\sum_{y\in S} I\{y \in (f_{[k]})^{-r}(x)\} = (n-1)\mathbf{P}\{y \in (f_{[k]})^{-r}(x)\} + \mathbf{P}\{x \in (f_{[k]})^{-r}(x)\}.$$

Заключение

Полученные результаты позволяют описать строение и вероятностные свойства графа $G_{f_{[k]}}$, $k \geqslant 1$, существенно используемые в рамках синтеза и анализа итерационных механизмов защиты информации в части формирования ключей, в принцип функционирования которых заложено применение различных преобразований или источника случайности в каждый отдельный такт работы.

В частности, найдены средние значения мощностей образа исходного множества вершин при действии случайного отображения $f_{[k]}$ и множества вершин, не имеющих прообразов. Получены точные формулы для вероятностей принадлежности указанным множествам фиксированного элемента. Выписаны формулы для распределения длины отрезка апериодичности произвольной фиксированной вершины, не проходящего через заданное множество вершин, вероятностей инцидентности любых двух фиксированных вершин одной компоненте связности и попадания произвольной фиксированной вершины в множество прообразов другой произвольной фиксированной вершины. Вычислена вероятность формирования коллизии произвольной парой фиксированных вершин в случайном графе $G_{f_{[k]}}$.

Автор благодарит А. М. Зубкова за интерес к работе и полезные замечания.

ЛИТЕРАТУРА

1. *Миронкин В. О.* Распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений // Математические вопросы криптографии. 2019. Т. 10. № 3. С. 89–99.
2. *Миронкин В. О.* Слои в графе композиции независимых равновероятных случайных отображений // Математические вопросы криптографии. 2020. Т. 11. № 1. С. 101–114.

3. *Зубков А. М., Серов А. А.* Предельная теорема для мощности образа подмножества при композиции случайных отображений // Дискретная математика. 2017. Т. 29. № 1. С. 17–26.
4. *Зубков А. М., Серов А. А.* Оценки среднего размера образа подмножества при композиции случайных отображений // Дискретная математика. 2018. Т. 30. № 2. С. 27–36.
5. *Серов А. А.* Образы конечного множества при итерациях двух случайных зависимых отображений // Дискретная математика. 2015. Т. 27. № 4. С. 133–140.
6. *Dalal A. and Schmutz E.* Compositions of random functions on a finite set // Electr. J. Comb. 2002. V. 9. No. R26. P. 1–7.
7. *Fill J. A.* On compositions of random functions on a finite set // 2002. P. 1–15. `http://www.mts.jhu.edu/~fill/`
8. *Миронкин В. О.* О некоторых вероятностных характеристиках алгоритма выработки ключа “CRYPTOPRO KEY MESHING” // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 140–146.
9. *Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., et al.* On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing // Математические вопросы криптографии. 2017. Т. 8. № 2. С. 39–50.
10. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984. 208 с.
11. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978. 288 с.
12. *Harris B.* Probability distributions related to random mapping // Ann. Math. Statist. 1960. V. 31. No. 4. P. 1045–1062.
13. *Flajolet P. and Odlyzko A.* Random mapping statistics // LNCS. 1989. V. 434. P. 329–354.
14. *Колчин В. Ф., Севастьянов Б. А., Чистяков В. П.* Случайные размещения. М.: Наука, 1976. 224 с.

REFERENCES

1. *Mironkin V. O.* Raspredelenie dlini otrezka aperiodichnosti v grafe kompozicii nezavisimih ravnoveroyatnih sluchaynih otobrazeniy [Distribution of the length of aperiodicity segment in the graph of independent uniform random mappings composition]. Mat. Vopr. Kriptogr., 2019, vol. 10, no. 3, pp. 89–99. (in Russian)
2. *Mironkin V. O.* Sloyi v grafe kompozicii nezavisimih ravnoveroyatnih sluchaynih otobrazeniy [Layers in a graph of the composition of independent uniform random mappings]. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 1, pp. 101–114. (in Russian)
3. *Zubkov A. M. and Serov A. A.* Predelnaya teorema dlya moshnosti obraza podmnozestva pri kompozicii sluchaynih otobrazeniy [Limit theorem for the size of an image of subset under compositions of random mappings]. Discrete Math., 2017, vol. 29, no. 1, pp. 17–26. (in Russian)
4. *Zubkov A. M. and Serov A. A.* Ocenki srednego razmera obraza podmnozestva pri kompozicii sluchaynih otobrazeniy [Estimates of the mean size of the subset image under composition of random mappings]. Discrete Math., 2018, vol. 30, no. 2, pp. 27–36. (in Russian)
5. *Serov A. A.* Obrazi konechnogo mnozestva pri iteraciyah dvuh sluchaynih zavisimih otobrazeniy [Images of a finite set under iterations of two random dependent mappings]. Discrete Math., 2015, vol. 27, no. 4, pp. 133–140. (in Russian)
6. *Dalal A. and Schmutz E.* Compositions of random functions on a finite set. Electr. J. Comb., 2002, vol. 9, no. R26, pp. 1–7.
7. *Fill J. A.* On compositions of random functions on a finite set. 2002, pp. 1–15. `http://www.mts.jhu.edu/~fill/`

8. *Mironkin V. O.* O nekotorih veroyatnostnih harakteristikah algoritma virabotki klucha “CRYPTOPRO KEY MESHING” [On some probabilistic characteristics of key derevation function “CRYPTOPRO KEY MESHING”]. Problemy Informacionnoj Bezopasnosti. Komp’yuternye Sistemy, 2015, no. 4, pp. 140–146. (in Russian)
9. *Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., et al.* On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing. Mat. Vopr. Kriptogr., 2017, vol. 8, no. 2, pp. 39–50.
10. *Kolchin V. F.* Sluchaynie otobrazeniya [Random Mappings]. Moscow, Nauka Publ., 1984. (in Russian)
11. *Sachkov V. N.* Veroyatnostnie metodi v kombinatornom analize [Probabilistic Methods in Combinatorial Analysis]. Moscow, Nauka Publ., 1978. (in Russian)
12. *Harris B.* Probability distributions related to random mapping. Ann. Math. Statist., 1960, vol. 31, no. 4, pp. 1045–1062.
13. *Flajolet P. and Odlyzko A.* Random mapping statistics. LNCS, 1989, vol. 434, pp. 329–354.
14. *Kolchin V. F., Sevastyanov B. A., and Chistyakov V. P.* Sluchaynie razmesheniya [Random Assignments]. Moscow, Nauka Publ., 1976. (in Russian)