В. О. Миронкин, Коллизии и инцидентность вершин компонентам в графе k-кратной итерации равновероятного случайного отображения, *Дискрет. матем.*, 2019, том 31, выпуск 4, 38–52

DOI: https://doi.org/10.4213/dm1596

Дискретная математика

том 31 выпуск 4 * 2019

УДК 519.212.2+519.719.2 DOI https://doi.org/10.4213/dm1596

Коллизии и инцидентность вершин компонентам в графе k-кратной итерации равновероятного случайного отображения

© 2019 г. В. О. Миронкин*

В работе изучаются вероятностные характеристики графа k-кратной итерации равновероятного случайного отображения. Выписаны формулы для распределения длины отрезка апериодичности произвольной вершины с учетом ряда ограничений. Вычислены вероятности инцидентности двух произвольных вершин одной компоненте связности, попадания произвольной вершины в множество прообразов другой вершины, а также появления коллизии в графе рассматриваемого отображения.

Ключевые слова: равновероятное случайное отображение, итерация отображения, отрезок апериодичности, граф отображения, компонента связности, прообраз, коллизия

Введение

Вопросы, связанные с описанием цикловой структуры различных модификаций случайных отображений [1–3], возникают при решении ряда задач современной криптографии, в частности, при построении теоретико-вероятностных моделей механизмов защиты информации (например, функций сжатия, хэш-функций, регистров сдвига, алгоритмов выработки производных ключей и псевдослучайных последовательностей [4–6]) и обосновании их криптографической стойкости [7], а также при описании некоторых методов дискретного логарифмирования (например, ρ-метод Полларда [8]) и методов балансировки времени–памяти–данных (например, метод Хеллмана [9] и его модификации, использующие особые точки и радужные таблицы [10–14]).

Настоящая статья посвящена исследованию свойств и характеристик графа k-кратной итерации равновероятного случайного отображения [15–19], описывающих особенности взаимного расположения вершин в графе и используемых при обосновании стойкости некоторых итерационных механизмов защиты информации.

Следуя [15], рассмотрим конечное множество $S = \{1, \ldots, n\}$, $n > 1$, и вероятностное пространство равновероятных случайных отображений $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространство элементарных исходов $\Omega = \{f\colon S \to S\}$ — множество всех n^n отображений

Место работы: Национальный исследовательский университет «Высшая школа экономики», e-mail: mironkin.v@mail.ru

S в себя, алгебра событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$ является равновероятной:

$$\mathbf{P}\,(f) = \frac{1}{n^n} \quad \forall\, f \in \Omega. \tag{1}$$

Для произвольного $k \in \mathbb{N}$ обозначим k-кратную итерацию $\underbrace{f(\ldots(f}_{k}(x)\ldots)$ функции f через f^k и введем множества отображений

$$\Omega_k = \bigcup_{f\in\Omega} \{f^k\}.$$

Будем считать, что f^0 — тождественное отображение $S \to S$.

При этом заметим, что Ω_k является собственным подмножеством Ω при любом $k > 1$ и что если случайное отображение f имеет равновероятное распределение (1), то распределение f^k не является равновероятным ни на Ω, ни на Ω_k.

При изложении результатов будем использовать следующие определения для характеристик графа отображения (в определениях отображение f считается детерминированным).

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

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

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

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

Множество циклических вершин графа G_f обозначим $C(G_f)$, а множество вершин, лежащих на циклах длины $l \in \{1, \ldots, n\}$, обозначим $C_l(G_f)$.

Через λ_f обозначим случайную величину, равную общему количеству циклических вершин в графе G_f.

С учетом [20] и того факта, что при переходе от графа G_f к графу G_{f^k} множество циклических вершин остается неизменным, для произвольного $j \in \{1, \ldots, n\}$ имеет место равенство

$$\mathbf{P}\left\{\lambda_{f^k} = j\right\} = \frac{j\,(n)_j}{n^{j+1}}. \tag{2}$$

Далее для любого $x \in S$ множество циклических вершин компоненты связности $\mathcal{K}_f\,(x)$ обозначим $C_f\,(x)$, а через $\beta_f(x)$ обозначим случайную величину, равную длине цикла компоненты $\mathcal{K}_f\,(x)$.

Определение 4. *Подходом* $\mathcal{P}_f\,(x)$, начинающимся в вершине $x \in S$ графа G_f, называется отрезок выходящей из x траектории от x до ее первого попадания в циклическую вершину.

В рамках определения 4 будем считать, что соответствующая циклическая вершина не принадлежит подходу $\mathcal{P}_f\,(x)$.

Через $\alpha_f(x)$ обозначим случайную величину, равную длине подхода $\mathcal{P}_f(x)$, и будем называть ее высотой вершины x в графе G_f:

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

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 ее первого самопересечения.

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

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

Согласно определениям 4, 5 для произвольного $x \in S$ выполняется соотношение

$$\tau_f(x) = \alpha_f(x) + \beta_f(x).$$

Замечание 1. Придерживаясь обозначений, принятых в [15], зависимость случайных величин $\alpha_f(x)$, $\beta_f(x)$, $\tau_f(x)$ от параметра n отражать не будем.

Перейдем к непосредственному рассмотрению вероятностных характеристик графа G_{f^k}, $k \geqslant 1$.

1. Отрезок апериодичности с ограничениями

Согласно [21] в моделях выработки производных ключей типа [22], построенных на основе некоторой секретной долговременной информации с использованием k-кратной итерации равновероятного случайного отображения $f\colon S \to S$, для последовательности различных долговременных ключей $x_1, x_2, \ldots, x_d$, $d > 1$, возможна компрометация формируемого ключевого множества, если $\mathcal{R}_{f^k}(x_i) \cap \mathcal{R}_{f^k}(x_j) \neq \varnothing$, где $1 \leqslant i < j \leqslant d$.

Если при этом исходная ключевая система содержит слабые ключи [7] $y_1, y_2, \ldots, y_t$, $t \geqslant 1$, то в целях обеспечения криптографической стойкости соответствующего итерационного алгоритма на указанные отрезки апериодичности накладывается естественное ограничение

$$\{y_1, y_2, \ldots, y_t\} \cap \left(\bigcup_{i=1}^{d} \mathcal{R}_{f^k}\left(x_1^{(i)}\right)\right) = \varnothing. \tag{3}$$

Таким образом, при оценке надежности алгоритма, а также объема данных, обрабатываемых на заданном секретном ключе, требуется знание распределения соответствующего отрезка апериодичности при отсутствии пересечений с фиксированным подмножеством ключей.

В частности, при $t = d = 1$ событие (3) принимает вид $\left\{y \notin \mathcal{R}_{f^k}(x)\right\}$. Вычислим его вероятность для произвольных элементов $x, y \in S$, $x \neq y$.

Для любых $k, l, i, j \in \mathbb{N}\colon i \leqslant j$ введем обозначения

$$Q_i^j(k,l) = \left\{m \in \mathbb{N}\colon i \leqslant m \leqslant j,\ \frac{m}{(m,k)} = l\right\}, \tag{4}$$

$$\tilde{Q}_i^j(k,l) = \{m \in \mathbb{N}\colon i \leqslant m \leqslant j,\ \frac{m}{(m,k)} < l\}, \tag{5}$$

где (m,k) — наибольший общий делитель чисел m и k.

Далее для произвольных $i_0, i_1 \in \mathbb{Z}$, $i_0 > i_1$, положим $\sum\limits_{j=i_0}^{i_1}(\ldots) = 0$ и $\prod\limits_{j=i_0}^{i_1}(\ldots) = 1$.

Теорема 1. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на Ω. Тогда при любых $k \in \mathbb{N}$, $x, y \in S$, $x \neq y$, и $z \in \{2,\ldots,n\}$ справедливо равенство*

$$\mathbf{P}\left\{\tau_{f^k}(x) = z; y \in \mathcal{R}_{f^k}(x)\right\} = (z-1)\left[\sum_{m\in Q_2^n(k,z)} \frac{(n-2)_{m-2}}{n^m} + \sum_{m\in\tilde{Q}_1^{n-1}(k,z)} \sum_{v=1}^{\min(k,n-r)} \frac{(n-2)_{r+v-2}}{n^{r+v}}\right],$$

где $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$, а $Q_2^n(k,z)$ и $\tilde{Q}_1^{n-1}(k,z)$ определяются соотношениями (4), (5).

Доказательство. Зафиксируем произвольную пару вершин $x, y \in S$, $x \neq y$, и для любого $z \in \{2,\ldots,n\}$ рассмотрим более широкое событие

$$\left\{\tau_{f^k}(x) = z; y \in \mathcal{R}_f(x)\right\},$$

для выполнения которого в случае $x \in C(G_f)$ и $\beta_f(x) = m$, где $m \in \{2,\ldots,n\}$, существует в точности $m-1$ вариантов прохождения случайной траектории $\mathcal{R}_f(x)$ через вершину y, а в случае $\alpha_f(x) = t$, где $t \in \{1,2,\ldots,n-m\}$, $m \in \{1,\ldots,n-1\}$, существует $m+t-1$ вариантов.

Повторяя рассуждения [15] с учетом расположения вершины y на $\mathcal{R}_f(x)$ и обозначая $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$, по формуле полной вероятности [23] получаем цепочку равенств

$$\begin{aligned}
&\mathbf{P}\left\{\tau_{f^k}(x) = z; y \in \mathcal{R}_f(x)\right\} = \mathbf{P}\left\{x \in C_z\left(G_{f^k}\right); y \in C_f(x)\right\} \\
&\quad + \mathbf{P}\left\{\tau_{f^k}(x) = z; x \notin C(G_f); y \in \mathcal{R}_f(x)\right\} = \sum_{m\in Q_2^n(k,z)} \frac{m-1}{n^2} \prod_{i=2}^{m-1}\left(1 - \frac{i}{n}\right) \\
&\quad + \sum_{m\in\tilde{Q}_1^{n-1}(k,z)} \sum_{t=\left(z-\frac{m}{(m,k)}-1\right)k+1}^{\min\left(\left(z-\frac{m}{(m,k)}\right)k,n-m\right)} \frac{m+t-1}{n^2} \prod_{i=2}^{m+t-1}\left(1 - \frac{i}{n}\right) \\
&\quad = \sum_{m\in Q_2^n(k,z)} \frac{(m-1)(n-2)_{m-2}}{n^m} \\
&\quad + \sum_{m\in\tilde{Q}_1^{n-1}(k,z)} \sum_{v=1}^{\min(k,n-r)} \frac{(r+v-1)(n-2)_{r+v-2}}{n^{r+v}}.
\end{aligned} \tag{6}$$

Далее следует учесть, что доля вершин y, лежащих на соответствующих траекториях длины m в графе G_f (для первой группы слагаемых в (6)) и длины $r+v$

(для второй группы слагаемых), при которых $y \in \mathcal{R}_{f^k}(x)$, составляет $\frac{z-1}{m-1}$ и $\frac{z-1}{r+v-1}$ соответственно. Таким образом, из (6) следует

$$\begin{aligned}
&\mathbf{P}\left\{\tau_{f^k}(x)=z; y\in\mathcal{R}_{f^k}(x)\cap\mathcal{R}_f(x)\right\}\\
&\qquad=\sum_{m\in Q_2^n(k,z)}\frac{z-1}{m-1}\cdot\frac{(m-1)(n-2)_{m-2}}{n^m}\\
&\quad+\sum_{m\in\tilde{Q}_1^{n-1}(k,z)}\sum_{v=1}^{\min(k,n-r)}\frac{z-1}{r+v-1}\cdot\frac{(r+v-1)(n-2)_{r+v-2}}{n^{r+v}}\\
&\quad=(z-1)\left[\sum_{m\in Q_2^n(k,z)}\frac{(n-2)_{m-2}}{n^m}+\sum_{m\in\tilde{Q}_1^{n-1}(k,z)}\sum_{v=1}^{\min(k,n-r)}\frac{(n-2)_{r+v-2}}{n^{r+v}}\right],
\end{aligned}$$

откуда с использованием соотношения

$$\mathbf{P}\left\{\tau_{f^k}(x)=z; y\in\mathcal{R}_{f^k}(x)\right\}=\mathbf{P}\left\{\tau_{f^k}(x)=z; y\in\mathcal{R}_{f^k}(x)\cap\mathcal{R}_f(x)\right\}.$$

приходим к утверждению теоремы. Теорема доказана. □

Пусть $]z[=\min\{n\in\mathbb{Z}\colon n\geqslant z\}$.

Теорема 2. *Пусть случайное отображение $f\colon S\to S$ имеет распределение* (1) *на* Ω. *Тогда при любых $k\in\mathbb{N}$, $x,y\in S$, $x\neq y$, и $z\in\{2,\ldots,n\}$ справедливо равенство*

$$\begin{aligned}
&\mathbf{P}\left\{\tau_{f^k}(x)\leqslant z; y\in\mathcal{R}_{f^k}(x)\right\}\\
&\qquad=\sum_{m\in\tilde{Q}_1^n(k,z+1)}\sum_{t=m}^{\min(r,n)}\frac{\left(\left]\frac{t-m}{k}\right[+\frac{m}{(m,k)}-1\right)(n-2)_{t-2}}{n^t},
\end{aligned}\tag{7}$$

где $r=m+\left(z-\frac{m}{(m,k)}\right)k$, а $\tilde{Q}_1^n(k,z)$ определяется соотношением (5).

Доказательство. Для произвольной фиксированной пары вершин $x,y\in S$, $x\neq y$, с учетом результатов [15, 21] находим, что

$$\begin{aligned}
&\mathbf{P}\left\{\tau_{f^k}(x)\leqslant z; y\in\mathcal{R}_f(x)\right\}=\mathbf{P}\left\{\tau_{f^k}(x)\leqslant z; x\in C(G_f); y\in C_f(x)\right\}\\
&\quad+\mathbf{P}\left\{\tau_{f^k}(x)\leqslant z; x\notin C(G_f); y\in\mathcal{R}_f(x)\right\}=\sum_{m\in\tilde{Q}_2^n(k,z+1)}\frac{m-1}{n^2}\prod_{i=2}^{m-1}\left(1-\frac{i}{n}\right)\\
&\qquad+\sum_{m\in\tilde{Q}_1^{n-1}(k,z+1)}\sum_{t=1}^{\min(r,n)-m}\frac{t+m-1}{n^2}\prod_{i=2}^{t+m-1}\left(1-\frac{i}{n}\right)\\
&\qquad=\sum_{m\in\tilde{Q}_2^n(k,z+1)}\frac{(m-1)(n-2)_{m-2}}{n^m}\\
&\qquad\quad+\sum_{m\in\tilde{Q}_1^{n-1}(k,z+1)}\sum_{t=1}^{\min(r,n)-m}\frac{(t+m-1)(n-2)_{t+m-2}}{n^{t+m}}.
\end{aligned}\tag{8}$$

При этом из равенства

$$\tau_{f^k}(x) = \left]\frac{y-\beta_f(x)}{k}\right[+ \frac{\beta_f(x)}{(\beta_f(x),k)}$$

следует, что при фиксированном $m \in \tilde{Q}_2^n(k, z+1)$ (для первой группы слагаемых в (8)), а также при такой фиксированной паре (m,t) (для второй группы слагаемых), что $m \in \tilde{Q}_1^{n-1}(k, z+1)$ и $t \in \{1, \ldots, \min(r,n)-m\}$, доли вершин $y \in \mathcal{R}_f(x)$, для которых $y \in \mathcal{R}_{f^k}(x)$, составляют $\frac{\frac{m}{(m,k)}-1}{m-1}$ и $\frac{\left]\frac{t}{k}\right[+\frac{m}{(m,k)}-1}{t+m-1}$ соответственно. Таким образом, из (8) вытекает выражение

$$\mathbf{P}\left\{\tau_{f^k}(x) \leqslant z; y \in \mathcal{R}_{f^k}(x)\right\} = \sum_{m \in \tilde{Q}_2^n(k,z+1)} \frac{\left(\frac{m}{(m,k)}-1\right)(n-2)_{m-2}}{n^m}$$
$$+ \sum_{m \in \tilde{Q}_1^{n-1}(k,z+1)} \sum_{t=1}^{\min(r,n)-m} \frac{\left(\left]\frac{t}{k}\right[+\frac{m}{(m,k)}-1\right)(n-2)_{t+m-2}}{n^{t+m}},$$

из которого путем объединения первой и второй групп слагаемых получаем искомую формулу. Теорема доказана. □

Замечание 2. Из теорем 1, 2 с учетом выражений для $\mathbf{P}\left\{\tau_{f^k}(x) = z\right\}$ и $\mathbf{P}\left\{\tau_{f^k}(x) \leqslant z\right\}$, полученных в [15], следуют формулы для величин $\mathbf{P}\left\{\tau_{f^k}(x) = z; y \notin \mathcal{R}_{f^k}(x)\right\}$ и $\mathbf{P}\left\{\tau_{f^k}(x) \leqslant z; y \notin \mathcal{R}_{f^k}(x)\right\}$.

Следствие 1. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на Ω. Тогда при любых $k \in \mathbb{N}$, $x, y \in S$, $x \neq y$, справедливо равенство*

$$\mathbf{P}\left\{y \notin \mathcal{R}_{f^k}(x)\right\} = 1 - \sum_{m=1}^{n}\sum_{t=m}^{n} \frac{\left(\left]\frac{t-m}{k}\right[+\frac{m}{(m,k)}-1\right)(n-2)_{t-2}}{n^t}.$$

Доказательство. Для искомой вероятности справедлива формула

$$\mathbf{P}\left\{y \notin \mathcal{R}_f(x)\right\} = 1 - \mathbf{P}\left\{y \in \mathcal{R}_f(x)\right\} = 1 - \mathbf{P}\left\{\tau_{f^k}(x) \leqslant n; y \in \mathcal{R}_f(x)\right\}. \tag{9}$$

Поэтому для получения результата достаточно подставить выражение (7) в (9) и учесть, что в случае $z = n$ пределы и множества суммирования слагаемых в (7) принимают вид

$$\min(r,n) = \min\left(\left(n - \frac{m}{(m,k)}\right)k, n-m\right) + m = n,$$

$$\tilde{Q}_1^n(k, n+1) = \{1, \ldots, n\}.$$

В итоге приходим к искомому равенству. Следствие доказано. □

2. Инцидентность вершин одной компоненте связности

Вопросы, связанные с оценкой вероятности попадания случайных вершин в одну компоненту связности графа отображения $f\colon S \to S$, изучались в ряде публикаций. Так, в частности, в [24] для произвольных различных вершин $x_1, x_2, \ldots, x_d \in S$, $d > 1$, получено следующее предельное значение этой вероятности при $n \to \infty$

$$\mathbf{P}\left\{x_1, x_2, \ldots, x_d \in \mathcal{K}_f\left(x_1\right)\right\} = \frac{(2d-2)!!}{(2d-1)!!}. \tag{10}$$

Отметим, что указанная характеристика описывает возможность компрометации производных ключей, вырабатываемых с использованием случайного отображения $f\colon S \to S$, поскольку событие $\{x_1, x_2, \ldots, x_d \in \mathcal{K}_f\left(x_1\right)\}$ совпадает с упомянутым выше событием $\left\{\bigcap_{i=1}^{d} \mathcal{R}_f\left(x_i\right) \neq \varnothing\right\}$.

Рассмотрим граф G_{f^k}, $k \in \mathbb{N}$, и для произвольной пары вершин $x, y \in S$, $x \neq y$, вычислим $\mathbf{P}\left\{y \in \mathcal{K}_{f^k}\left(x\right)\right\}$.

Для любых $m \in \mathbb{N}$ и $s,\ t \in \mathbb{N} \cup \{0\}$ положим

$$\Delta_m^{s,t} = \begin{cases} 1, & s_{\bmod m} \geqslant t_{\bmod m} > 0, \\ 0 & \text{в противном случае,} \end{cases} \tag{11}$$

здесь и далее используется обозначение $s_{\bmod m} = s - m[\frac{s}{m}]$ для наименьшего неотрицательного вычета s по модулю m.

Теорема 3. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на Ω. Тогда при любых $k \in \mathbb{N}$, $x, y \in S$, $x \neq y$, справедливо равенство*

$$\mathbf{P}\left\{y \in \mathcal{K}_{f^k}\left(x\right)\right\} = \sum_{m=1}^{n} \sum_{v=m}^{n} \sum_{s=0}^{n-v} \frac{\left(\left]\frac{v}{(m,k)}\right[- \omega_{m,v,s}\right)(n-2)_{v+s-2}}{n^{v+s}},$$

где $\omega_{m,v,s} = \begin{cases} 1, & \text{если } s = 0, \\ \Delta_{(m,k)}^{s,v} & \text{в противном случае.} \end{cases}$

Доказательство. Зафиксируем произвольную пару вершин $x, y \in S$, $x \neq y$. Тогда по формуле полной вероятности

$$\mathbf{P}\left\{y \in \mathcal{K}_{f^k}\left(x\right)\right\} = \mathbf{P}\left\{y \in \mathcal{K}_{f^k}\left(x\right), x \in C_f\left(x\right)\right\} + \mathbf{P}\left\{y \in \mathcal{K}_{f^k}\left(x\right), x \notin C_f\left(x\right)\right\}. \tag{12}$$

Вычислим первое слагаемое в (12). Зафиксируем длину $m \in \{1, \ldots, n\}$ цикла $C_f\left(x\right)$. Заметим, что существует в точности $\frac{m}{(m,k)} - 1$ вариантов расположения вершины $y \neq x$ на цикле $C_f\left(x\right)$, при которых выполняется событие $\left\{y \in \mathcal{K}_{f^k}\left(x\right)\right\}$. Вероятность каждого такого варианта составляет $\frac{1}{n^2} \prod\limits_{i=2}^{m-1} \left(1 - \frac{i}{n}\right)$ [25].

Если же $\alpha_f\left(y\right) = s \in \{1, \ldots, n-m\}$, то для каждого такого фиксированного s существует ровно $\frac{m}{(m,k)}$ вариантов точки вхождения подхода $\mathcal{P}_f\left(y\right)$ в цикл $C_f\left(x\right)$,

при которых также выполняется событие $\{y \in \mathcal{K}_{f^k}(x)\}$, а вероятность каждого из них равна $\frac{1}{n^2}\prod\limits_{i=2}^{m+s-1}\left(1-\frac{i}{n}\right)$. Таким образом,

$$\mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x), x \in C_f(x)\right\} = \sum_{m=2}^{n} \frac{\frac{m}{(m,k)}-1}{n^2} \prod_{i=2}^{m-1}\left(1-\frac{i}{n}\right) + \sum_{m=1}^{n}\sum_{s=1}^{n-m} \frac{\frac{m}{(m,k)}}{n^2} \prod_{i=2}^{m+s-1}\left(1-\frac{i}{n}\right). \quad (13)$$

Рассмотрим второе слагаемое в (12). В этом случае, помимо m, зафиксируем длину подхода $t = \alpha_f(x) > 0$. Если $y \in \mathcal{R}_f(x)$, то существует $\left]\frac{t+m}{(m,k)}\right[- 1$ вариантов (исключается вершина x) расположения вершины $y \neq x$ на отрезке апериодичности $\mathcal{R}_f(x)$, при которых выполняется событие $\{y \in \mathcal{K}_{f^k}(x)\}$. Вероятность каждого такого варианта $\frac{1}{n^2}\prod\limits_{i=2}^{m+t-1}\left(1-\frac{i}{n}\right)$.

Пусть теперь $s = \min\{w \in \mathbb{N} \cup \{0\} : f^w(y) \in \mathcal{R}_f(x)\} > 0$. Тогда для всех t, кратных (m,k), существует ровно $\left]\frac{t+m}{(m,k)}\right[$ вариантов точки вхождения траектории, начинающейся в вершине y, в отрезок апериодичности $\mathcal{R}_f(x)$, при которых выполняется событие $\{y \in \mathcal{K}_{f^k}(x)\}$. Если же $(m,k) \nmid t$, то для $s_{\mathrm{mod}\,(m,k)} < t_{\mathrm{mod}\,(m,k)}$ число таких вариантов составляет $\left]\frac{t+m}{(m,k)}\right[$, а для $s_{\mathrm{mod}\,(m,k)} \geqslant t_{\mathrm{mod}\,(m,k)}$ — соответственно $\left]\frac{t+m}{(m,k)}\right[- 1$. Вероятность каждого такого вхождения равна $\frac{1}{n^2}\prod\limits_{i=2}^{m+s+t-1}\left(1-\frac{i}{n}\right)$. Следовательно,

$$\mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x), x \notin C_f(x)\right\} = \sum_{m=1}^{n}\sum_{t=1}^{n-m} \frac{\left]\frac{t+m}{(m,k)}\right[- 1}{n^2} \prod_{i=2}^{m+t-1}\left(1-\frac{i}{n}\right) + \sum_{m=1}^{n}\sum_{t=1}^{n-m}\sum_{s=1}^{n-m-t} \frac{\left]\frac{t+m}{(m,k)}\right[- \Delta^{s,t}_{(m,k)}}{n^2} \prod_{i=2}^{m+t+s-1}\left(1-\frac{i}{n}\right). \quad (14)$$

Далее, подставив (13) и (14) в (12) и преобразовав полученное выражение за счет замены переменной $t = v - m$ с учетом равенства $\Delta^{s,v}_{(m,k)} = \Delta^{s,t}_{(m,k)}$, придем к искомому результату. Теорема доказана. □

Замечание 3. Теорема 3 позволяет выписать выражение для средней мощности компоненты произвольной не зависящей от f вершины $x \in S$ в графе G_{f^k}. Действительно, из соотношения

$$\mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\} = \sum_{r=2}^{n} \mathbf{P}\left\{|\mathcal{K}_{f^k}(x)| = r\right\} \mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x) \;\middle|\; |\mathcal{K}_{f^k}(x)| = r\right\} = \sum_{r=2}^{n} \frac{r-1}{n-1} \mathbf{P}\left\{|\mathcal{K}_{f^k}(x)| = r\right\} = \frac{1}{n-1}\mathbf{E}\left(|\mathcal{K}_{f^k}(x)| - 1\right)$$

следует равенство

$$\mathbf{E}|\mathcal{K}_{f^k}(x)| = (n-1)\,\mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\} + 1.$$

Замечание 4. В силу равноправия вершин графа G_f согласно теореме 3 среднее число пар $(x, y) \in S \times S\colon x \neq y$, сохраняющих инцидентность одной компоненте связности при переходе от графа G_f к графу G_{f^k}, определяется равенством $n\,(n-1)\,\mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\}$.

Следствие 2. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на Ω. Тогда при любых $k \in \mathbb{N}$, $x, y \in S$, $x \neq y$, справедливо двустороннее неравенство*

$$\frac{1}{3k} < \lim_{n\to\infty} \mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\} \leqslant \frac{2}{3}.$$

Доказательство. Из соотношения (13) и очевидного неравенства $\frac{m}{2k} < \frac{m}{(m,k)}$, справедливого для произвольных $m \in \{1, \ldots, n\}$ и $k \in \mathbb{N}$, получаем

$$\frac{1}{2k}\mathbf{P}\left\{y \in \mathcal{K}_f(x), x \in C_f(x)\right\} < \mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x), x \in C_f(x)\right\}. \tag{15}$$

В свою очередь, из определения $\Delta^{s,t}_{(m,k)}$ и соотношения $\frac{t+m}{(m,k)} \geqslant 1$, справедливого для произвольных $m \in \{1, \ldots, n\}$, $t \in \{0, \ldots, n-m\}$, $s \in \{0, \ldots, n-m-t\}$ и $k \in \mathbb{N}$, следует неравенство

$$\frac{t+m}{2k} < \left]\frac{t+m}{(m,k)}\right[- \Delta^{s,t}_{(m,k)}, \tag{16}$$

из которого получаем

$$\frac{1}{2k}\mathbf{P}\left\{y \in \mathcal{K}_f(x), x \notin C_f(x)\right\} < \mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x), x \notin C_f(x)\right\} \tag{17}$$

и, следовательно, для произвольного $k \in \mathbb{N}$ можем записать двустороннюю оценку

$$\frac{1}{2k}\mathbf{P}\left\{y \in \mathcal{K}_f(x)\right\} < \mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\} \leqslant \mathbf{P}\left\{y \in \mathcal{K}_f(x)\right\}.$$

Таким образом, переходя к пределу в полученном неравенстве при $n \to \infty$, с использованием формулы $\lim\limits_{n\to\infty} \mathbf{P}\left\{y \in \mathcal{K}_f(x)\right\} = \frac{2}{3}$, [24] получаем искомый результат. Следствие доказано. □

Отметим также, что теорема 3 иллюстрирует возможность уменьшения вероятности компрометации ключей посредством использования не всех последовательно вырабатываемых производных ключей, а отобранных с некоторым фиксированным шагом k (за счет распада компонент связности графа G_f при переходе к графу G_{f^k}). Исключение составляет случай, когда граф G_{f^k} является связным, и, как следствие, любой набор вершин из S сохраняет инцидентность соответствующей компоненте.

Обозначим через η_f случайную величину, равную числу компонент связности в графе G_f.

Теорема 4. *Пусть случайное отображение* $f\colon S \to S$ *имеет распределение* (1) *на* Ω. *Тогда при любом* $k \in \mathbb{N}$ *справедливо равенство*

$$\mathbf{P}\left\{\eta_{f^k} = 1\right\} = \sum_{j \in D_k} \frac{(n)_j}{n^{j+1}},$$

где $D_k = \{j \in \{1, \ldots, n\} : \ (k, j) = 1\}$.

Доказательство. По формуле полной вероятности

$$\mathbf{P}\left\{\eta_{f^k} = 1\right\} = \sum_{j=1}^{n} \mathbf{P}\left\{\eta_{f^k} = 1 \;\middle|\; \lambda_f = j\right\} \mathbf{P}\left\{\lambda_f = j\right\}. \tag{18}$$

При фиксированном $j \in \{1, \ldots, n\}$ величину $\mathbf{P}\left\{\eta_{f^k} = 1 \;\middle|\; \lambda_f = j\right\}$ можно интерпретировать как вероятность того, что k-кратная итерация равновероятной случайной подстановки $\pi \in S_j$ содержит ровно 1 цикл. Тогда с учетом [20]

$$\mathbf{P}\left\{\eta_{f^k} = 1 \;\middle|\; \lambda_f = j\right\} = \begin{cases} \frac{1}{j}, & \text{если } (k, j) = 1, \\ 0 & \text{в противном случае.} \end{cases}$$

В итоге, подставив (2) в (18), получим требуемый результат. Теорема доказана. □

Следствие 3. *Пусть случайное отображение* $f\colon S \to S$ *имеет распределение* (1) *на* Ω. *Тогда при любом* $k \in \mathbb{N}$ *справедливы следующие оценки*:

$$\frac{1}{n} \sum_{j \in D_k} e^{-\left(1+\frac{j}{n}\right)\frac{j(j-1)}{2n}} \leqslant \mathbf{P}\left\{\eta_{f^k} = 1\right\} \leqslant \frac{1}{n} \sum_{j \in D_k} e^{-\frac{j(j-1)}{2n}}.$$

Доказательство. С учетом двустороннего неравенства, вытекающего из [26]:

$$e^{-\left(1+\frac{j}{n}\right)\frac{j(j-1)}{2n}} \leqslant \frac{(n)_j}{n^j} = \prod_{i=1}^{j-1} \left(1 - \frac{i}{n}\right) \leqslant e^{-\frac{j(j-1)}{2n}},$$

справедливого для $j \in \{1, \ldots, n\}$, получаем искомую двустороннюю оценку. Следствие доказано. □

3. Прообразы и коллизии

Неотъемлемой составляющей криптографического анализа хэш-функций и функций сжатия, а также механизмов защиты информации, построенных на их основе, являются задачи, связанные с поиском коллизий и описанием множества прообразов произвольной вершины соответствующего графа отображения [19]. Указанные задачи находят свое применение в том числе и при оптимизации методов балансировки времени–памяти–данных [12].

Через $\left(f^k\right)^{-1}(x)$ обозначим множество непосредственных прообразов случайной вершины $x \in S$ в графе G_{f^k}, $k \geqslant 1$.

Теорема 5. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на* Ω. *Тогда при любых* $k \in \mathbb{N}$, $x, y \in S$, $x \neq y$, *справедливо равенство*

$$\mathbf{P}\left\{y \in \left(f^k\right)^{-1}(x)\right\} = \sum_{m \in \overline{Q}_2^n(k,1)} \frac{(n-2)_{m-2}}{n^m} + \sum_{t=1}^{n-1} \sum_{m=t+1}^{n} \frac{(n-2)_{m-2}}{n^m},$$

где $\overline{Q}_2^n(k,1) = \{2,\ldots,n\} \setminus Q_2^n(k,1)$, $Q_2^n(k,1)$ *определяется соотношением* (4).

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

$$\mathbf{P}\left\{y \in \left(f^k\right)^{-1}(x)\right\} = \mathbf{P}\left\{f^k(y) = x, x \in C_f(x)\right\} + \mathbf{P}\left\{f^k(y) = x, x \notin C_f(x)\right\}. \quad (19)$$

Рассмотрим первое слагаемое в (19). На цикле $C_f(x)$ с фиксированной длиной $m \in \{2,\ldots,n\}$ в случае $m \nmid k$ существует единственный вариант расположения вершины y, при котором выполняется событие $\left\{y \in \left(f^k\right)^{-1}(x)\right\}$, и его вероятность составляет $\frac{1}{n^2}\prod\limits_{i=2}^{m-1}\left(1-\frac{i}{n}\right)$. В случае $m \mid k$ таких вариантов не существует.

Если же $s = \alpha_f(y) \in \{1,\ldots,k\}$, то для любого $\beta_f(x) = m \in \{1,\ldots,n-s\}$ также существует единственный вариант расположения вершины y, при котором выполняется событие $\left\{y \in \left(f^k\right)^{-1}(x)\right\}$, и его вероятность равна $\frac{1}{n^2}\prod\limits_{i=2}^{m+s-1}\left(1-\frac{i}{n}\right)$.

Объединив указанные случаи, приходим к выражению для первого слагаемого в (19)

$$\mathbf{P}\left\{f^k(y) = x, x \in C_f(x)\right\} = \frac{1}{n^2}\sum_{m \in \overline{Q}_2^n(k,1)} \prod_{i=2}^{m-1}\left(1-\frac{i}{n}\right) + \frac{1}{n^2}\sum_{s=1}^{k}\sum_{m=1}^{n-s}\prod_{i=2}^{m+s-1}\left(1-\frac{i}{n}\right), \quad (20)$$

где $\overline{Q}_2^n(k,1) = \{2,\ldots,n\} \setminus Q_2^n(k,1)$.

Перейдем к вычислению второго слагаемого в (19). Запишем равенство

$$\left\{f^k(y) = x, x \notin C_f(x)\right\} = \bigcup_{t=1}^{n-k-1}\bigcup_{m=1}^{n-k-t}\left\{\alpha_f(x) = t, \beta_f(x) = m, f^k(y) = x\right\},$$

где под знаками объединения стоят несовместные события, и при фиксированных t, m вероятность соответствующего события равна $\frac{1}{n^2}\prod\limits_{i=2}^{t+m+k-1}\left(1-\frac{i}{n}\right)$. Тогда, переходя к вероятностям, получаем

$$\mathbf{P}\left\{f^k(y) = x, x \notin C_f(x)\right\} = \frac{1}{n^2}\sum_{t=1}^{n-k-1}\sum_{m=1}^{n-k-t}\prod_{i=2}^{t+m+k-1}\left(1-\frac{i}{n}\right) = \frac{1}{n^2}\sum_{t=k+1}^{n-1}\sum_{m=1}^{n-t}\prod_{i=2}^{t+m-1}\left(1-\frac{i}{n}\right). \quad (21)$$

В итоге, подставив (20) и (21) в (19), приходим к искомому выражению. Теорема доказана. □

Отметим, что для произвольного $k \in \mathbb{N}$ в случае $y = x$ выполняется равенство событий

$$\left\{x \in \left(f^k\right)^{-1}(x)\right\} = \left\{x \in C_1\left(G_{f^k}\right)\right\},$$

откуда с учетом [21]

$$\mathbf{P}\left\{x \in \left(f^k\right)^{-1}(x)\right\} = \sum_{m \in Q_1^n(k,1)} \frac{(n)_m}{n^{m+1}}.$$

В частности, для простого $k \in \mathbb{N}$ получаем выражение

$$\mathbf{P}\left\{x \in \left(f^k\right)^{-1}(x)\right\} = \frac{1}{n}\left(1 + \frac{(n)_k}{n^k}\right),$$

вырождающееся при $k > n$ в равенство $\mathbf{P}\left\{x \in \left(f^k\right)^{-1}(x)\right\} = \frac{1}{n}$.

Замечание 5. Теорема 5 позволяет выписать выражение для среднего числа прообразов произвольной вершины $x \in S$ в графе G_{f^k}. А именно, так как

$$\left|\left(f^k\right)^{-1}(x)\right| = \sum_{y \in S} I\left\{y \in \left(f^k\right)^{-1}(x)\right\},$$

то в силу равноправия всех $y \in S$

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

Определение 6. *Коллизией* в графе отображения G_f называется произвольная пара вершин $x, y \in S$, $x \neq y$, для которых $f(x) = f(y)$.

Теорема 6. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на Ω. Тогда при любых $k \in \mathbb{N}$, $x, y \in S$, $x \neq y$, справедливо равенство*

$$\mathbf{P}\left\{f^k(x) = f^k(y)\right\} = \sum_{t=1}^{k}\sum_{s=0}^{n-1}\sum_{m=t+1}^{n-s} \frac{(1+\delta_{s,0})\,(n-2)_{m+s-2}}{n^{m+s}}$$
$$+ \sum_{t=1}^{k}\sum_{m=t+1}^{n}\sum_{i=0}^{t-1}\sum_{j=\delta_{i,0}}^{\left[\frac{k-t}{m-t}\right]} \frac{(n-2)_{m+i+jm-2}}{n^{m+i+jm}},$$

где $\delta_{i,j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases}$ — *символ Кронекера.*

Доказательство. Зафиксируем $x, y \in S\colon x \neq y$. Тогда по формуле полной вероятности

$$\mathbf{P}\left\{f^k(x) = f^k(y)\right\} = \mathbf{P}\left\{f^k(x) = f^k(y), x \in C_f(x)\right\}$$
$$+ \mathbf{P}\left\{f^k(x) = f^k(y), x \notin C_f(x)\right\}. \quad (22)$$

Рассмотрим первое слагаемое в (22). Заметим, что в случае $x \in C_f(x)$ событие $\{f^k(x) = f^k(y)\}$ может быть выполненным только при $s = \alpha_f(y) \in \{1, \ldots, k\}$. При этом для любого $\beta_f(x) = m \in \{1, \ldots, n-s\}$ существует единственный вариант расположения вершины y, и его вероятность составляет $\frac{1}{n^2} \prod\limits_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right)$. Таким образом,

$$\mathbf{P}\left\{f^k(x) = f^k(y), x \in C_f(x)\right\} = \frac{1}{n^2} \sum_{s=1}^{k} \sum_{m=1}^{n-s} \prod_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right). \tag{23}$$

Вычислим второе слагаемое в (22). Запишем равенство событий

$$\begin{aligned}\left\{f^k(x) = f^k(y), x \notin C_f(x)\right\} \\ = \left\{f^k(x) = f^k(y), \alpha_f(x) > k\right\} \cup \left\{f^k(x) = f^k(y), 1 \leqslant \alpha_f(x) \leqslant k\right\}\end{aligned}$$

и рассмотрим отдельно события, стоящие в его правой части.

Пусть $\alpha_f(x) = t \in \{k+1, \ldots, n-1\}$. В этом случае $s = \min\{w \in \mathbb{N} \cup \{0\} : f^w(y) \in \mathcal{R}_f(x)\} \in \{1, \ldots, k\}$, и для произвольного $\beta_f(x) = m \in \{1, \ldots, n-s-t\}$ существует единственный вариант расположения вершины y, при котором выполняется событие $\{f^k(x) = f^k(y)\}$, и его вероятность составляет $\frac{1}{n^2} \prod\limits_{i=2}^{m+s+t-1} \left(1 - \frac{i}{n}\right)$.

Пусть теперь $\alpha_f(x) = t \in \{1, \ldots, k\}$. Тогда для произвольного $s \in \{0, \ldots, k\}$ существует единственный вариант вхождения траектории, начинающейся в вершине y, в цикл $C_f(x)$ длины $m \in \{1, \ldots, n-s-t\}$, при котором $\{f^k(x) = f^k(y)\}$. Вероятность каждого такого варианта также равна $\frac{1}{n^2} \prod\limits_{i=2}^{m+s+t-1} \left(1 - \frac{i}{n}\right)$.

Определим множество вариантов расположения вершины y, при которых траектория, начинающаяся в этой вершине, входит в подход $\mathcal{P}_f(x)$, и выполняется равенство $\{f^k(x) = f^k(y)\}$. Соответствующее множество M имеет вид

$$M = \left\{y \in S \backslash \{x\} \colon f^{i+jm}(y) = f^i(x),\ i = 0, \ldots, t-1,\ j = 0, \ldots, \left[\frac{k-t}{m}\right]\right\},$$

а вероятность каждого варианта составляет $\frac{1}{n^2} \prod\limits_{i=2}^{m+t+i+jm-1} \left(1 - \frac{i}{n}\right)$. Следовательно,

$$\begin{aligned}\mathbf{P}\left\{f^k(x) = f^k(y), x \notin C_f(x)\right\} &= \frac{1}{n^2} \sum_{t=k+1}^{n-1} \sum_{s=1}^{k} \sum_{m=1}^{n-t-s} \prod_{i=2}^{m+t+s-1} \left(1 - \frac{i}{n}\right) \\ &+ \frac{1}{n^2} \sum_{t=1}^{k} \sum_{s=0}^{k} \sum_{m=1}^{n-t-s} \prod_{i=2}^{m+t+s-1} \left(1 - \frac{i}{n}\right) \\ &+ \frac{1}{n^2} \sum_{t=1}^{k} \sum_{m=1}^{n-t} \sum_{i=0}^{t-1} \sum_{j=\delta_{i,0}}^{\left[\frac{k-t}{m}\right]} \prod_{i=2}^{m+t+i+jm-1} \left(1 - \frac{i}{n}\right). \end{aligned} \tag{24}$$

Подставив выражения (23) и (24) в (22) и проведя элементарные преобразования, получим искомую формулу. Теорема доказана. □

Замечание 6. Согласно теореме 6 в силу равноправия вершин из S среднее число коллизий в графе G_{f^k} определяется величиной $C_n^2\mathbf{P}\left\{f^k(x) = f^k(y)\right\}$.

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

Список литературы

1. Зубков А. М., "Вычисление распределений характеристик чисел компонент и циклических точек случайного отображения", *Математические вопросы криптографии*, **1**:2 (2010), 5-18.
2. Зубков А. М., Серов А. А., "Предельная теорема для мощности образа подмножества при композиции случайных отображений", *Дискретная математика*, **29**:1 (2017), 17-26; англ. пер.: Zubkov A. M., Serov A. A., "Limit theorem for the size of an image of subset under compositions of random mappings", *Discrete Math. Appl.*, **28**:2 (2018), 131–138.
3. Зубков А. М., Серов А. А., "Оценки среднего размера образа подмножества при композиции случайных отображений", *Дискретная математика*, **30**:2 (2018), 27-36; англ. пер.: Zubkov A. M., Serov A. A., "Estimates of the mean size of the subset image under composition of random mappings", *Discrete Math. Appl.*, **28**:5 (2018), 331–338.
4. Михайлов В. Г., "О повторяемости состояний датчика псевдослучайных чисел при его многократном использовании", *Теория вероятн. и ее примен.*, **40**:4 (1995), 786-797; англ. пер.: Mikhailov V. G., "Repetition of states of a random-number generator under multiple access", *Theory Probab. Appl.*, **40**:4 (1995), 679–689.
5. Михайлов В. Г., "Исследование комбинаторно-вероятностной модели автоматов из регистров с неравномерным движением", *Труды по дискретной математике*, 2002, 139-149.
6. Михайлов В. Г., "Исследование числа циклических точек автомата из регистров с неравномерным движением", *Труды по дискретной математике*, 2002, 167-172.
7. Погорелов Б. А., Сачков В. Н. (ред.), *Словарь криптографических терминов*, М. : МЦНМО, 2006, 94 с.
8. Василенко О. Н., *Теоретико-числовые алгоритмы в криптографии*, М.: МЦНМО, 2003, 328 с.
9. Hellman M. E., "A cryptanalytic time-memory trade-off", *IEEE Trans. Inf. Theory*, 1980, 401-406.
10. Pilshchikov D. V., "Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number of particles and the total number of particles in the Galton-Watson process", *Математические вопросы криптографии*, **5**:2 (2014), 103-108.
11. Pilshchikov D. V., "On the limiting mean values in probabilistic models of time-memory-data tradeoff methods", *Математические вопросы криптографии*, **6**:2 (2015), 59-65.
12. Пильщиков Д. В., "Исследование сложности метода радужных таблиц с маркерами цепочек", *Математические вопросы криптографии*, **8**:4 (2017), 99-116.
13. Avoine G., Junod P., Oechslin P., "Characterization and improvement of time-memory trade-off based on perfect tables", *Trans. Inf. Syst. Secur.*, **11**:17 (2008), 1-17.
14. Oechslin P., "Making a faster cryptanalytic time-memory trade-off", *Lect. Notes Comput. Sci.*, **2729** (2003), 617-630.
15. Зубков А. М., Миронкин В. О., "Распределение длины отрезка апериодичности в графе k-кратной итерации случайного равновероятного отображения", *Математические вопросы криптографии*, **8**:4 (2017), 63-74.
16. Зубков А. М., Серов А. А., "Совокупность образов подмножества конечного множества при итерациях случайных отображений", *Дискретная математика*, **26**:4 (2014), 43-50; англ. пер.: Zubkov A. M., Serov A. A., "Images of subset of finite set under iterations of random mappings", *Discrete Math. Appl.*, **25**:3 (2015), 179–185.

17. Миронкин В. О., Михайлов В. Г., “О множестве образов k-кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **9**:3 (2018), 99-108.
18. Миронкин В. О., “Об оценках распределения длины отрезка апериодичности в графе k-кратной итерации равновероятного случайного отображения”, *Прикладная дискретная математика*, **42** (2018), 6-17.
19. Пильщиков Д. В., “Асимптотическое поведение мощности полного прообраза случайного множества при итерациях отображений конечного множества”, *Математические вопросы криптографии*, **8**:1 (2017), 95-106.
20. Rubin H., Sitgreaves R., “Probability distributions related to random transformations of a finite set”, Tech. Rept. № 19A, Appl. Math. and Statist. Lab., Stanford Univ., 1954, 50 с.
21. Миронкин В. О., “Слои в графе k-кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **10**:1 (2019), 73-82.
22. Миронкин В. О., “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”, *Проблемы информационной безопасности. Компьютерные системы*, 2015, № 4, 140-146.
23. Чистяков В. П., *Курс теории вероятностей* (7-*е изд.*), М.: Дрофа, 2007, 253 с.
24. Халипов П. В., *Вероятность покрытия конечного множества компонентой случайного отображения*, Дипломная работа, мех-мат МГУ им. М.В. Ломоносова, 2008.
25. Harris B., “Probability distributions related to random mapping”, *Ann. Math. Statist.*, **31**:4 (1960), 1045-1062.
26. Токарева Н. Н., *Симметричная криптография. Краткий курс*: *учебное пособие*, Новосиб. гос. ун-т. Новосибирск, 2012, 234 с.

Статья поступила 12.07.2019.
Переработанный вариант поступил 24.11.2019.