В. О. Миронкин, Слои в графе k-кратной итерации равновероятного случайного отображения, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 1, 73–82

DOI: 10.4213/mvk277

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2019 Т. 10 № 1 С. 73–82

УДК 519.212.2+519.719.2 DOI https://doi.org/10.4213/mvk277

Слои в графе k-кратной итерации равновероятного случайного отображения

В. О. Миронкин

Национальный исследовательский университет «Высшая школа экономики», Москва

Получено 30.V.2016
Переработанный вариант 30.XI.2018

Аннотация. Изучаются вероятностные характеристики графа k-кратной итерации равновероятного случайного отображения конечного множества. Получены точные выражения и оценки для распределений расстояний вершин от циклов. Приведены формулы для математических ожиданий чисел вершин, находящихся на заданных расстояниях от циклов, и для функции распределения высоты случайной вершины.

Ключевые слова: равновероятное случайное отображение, итерация отображения, граф отображения, слой в графе, циклические вершины

Layers of the graph of k-fold iteration of the uniform random mapping

V. O. Mironkin

National Research University Higher School of Economics, Moscow

Abstract. The probabilistic characteristics of the graph of k-fold iteration of uniform random mapping are studied. Exact expressions and estimates for the distribution of the distances from the vertices to cycles are obtained. Formulas for expected values of the numbers of vertices on the given distance from cycles and for the distribution function of the height of a random vertex are derived.

Key words: uniform random mapping, iteration of random mapping, graph of a mapping, layer in a graph, cyclic vertices

Citation: *Matematicheskie Voprosy Kriptografii*, 2019, v. 10, № 1, pp. 73–82 (Russian)

1. Введение

В рамках исследований итерационных алгоритмов выработки производных (сеансовых) ключей на основе некоторой долговременной информации (см., например, [1]), наряду с оценкой допустимого периода ее эксплуатации [2–4], а также с оценкой мощности образа и прообраза исходного множества ключей [5–8], возникают задачи, связанные с классификацией элементов формируемого ключевого множества по количественным характеристикам реализуемого отображения. В некоторых случаях это объясняется необходимостью задания отношения эквивалентности на множестве ключей, используемого для определения классов эквивалентности и получения оценок криптографической стойкости соответствующих алгоритмов относительно ряда методов опробования [9].

В настоящей статье в качестве классифицирующей характеристики рассматривается значение высоты отдельно взятой вершины графа k-кратной итерации равновероятного случайного отображения, моделирующего процесс функционирования алгоритма выработки ключей.

Отметим, что исследование отношения эквивалентности на множестве вершин графа k-кратной итерации G_{f^k}, где $k > 1$, представляет собой отдельную задачу. Использование при ее решении модели равновероятного случайного отображения позволяет применить имеющуюся теорию [10–14].

Аналогично [2] 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 S в себя, алгебра событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$ является равновероятной:

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

При изложении результатов будем использовать следующие определения для характеристик графа G_f отображения f с множеством вершин S и множеством ориентированных ребер $(x, f(x))$, $x \in S$ (в определениях отображение f считается детерминированным).

О п р е д е л е н и е 1. 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 $C_l(G_f)$.

О п р е д е л е н и е 2. *Высотой* $\alpha_f(x)$ вершины $x \in S$ в графе G_f называется расстояние (число ребер) от этой вершины до ближайшей циклической вершины: $\alpha_f(x) = \min\{m \geqslant 0\colon f^m(x) \in C(G_f)\}$.

Через $\beta_f(x)$ обозначим случайную величину, равную длине цикла компоненты графа G_f, содержащей вершину $x \in S$.

Замечание 1. Следуя обозначениям, принятым в [2, 8], зависимость случайных величин $\alpha_f(x)$, $\beta_f(x)$ от параметра n отражать не будем.

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

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

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

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.

О п р е д е л е н и е 3. Для произвольного $t \in \{0,\ldots,n-1\}$ назовем *t-м слоем* в графе G_f множество вершин $H_f^{(t)} = \{x \in S : \alpha_f(x) = t\}$.

О п р е д е л е н и е 4. Для произвольных $l \in \{1,\ldots,n\}$, $t \in \{0,\ldots,n-l\}$ назовем *t-м слоем циклов длины l* в графе G_f множество вершин

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

Настоящая статья посвящена изучению вероятностных характеристик слоев в случайных графах G_{f^k} в случае, когда f имеет равновероятное распределение на Ω, а $k > 1$ фиксировано.

2. Вероятность попадания случайной вершины на цикл заданной длины

Из определений 3 и 4 для отображения f^k при $t = 0$ вытекают равенства множеств $H_{f^k}^{(0)} = C\left(G_{f^k}\right)$ и $H_{f^k}^{(0,l)} = C_l\left(G_{f^k}\right)$. Так, в частности, в случае $k=1$ множества вершин $H_{f^k}^{(0)}$ и $H_{f^k}^{(0,l)}$ подробно изучены в [12, 15, 16].

Учитывая, что при переходе от графа G_f к графу G_{f^k}, $k > 1$, множество циклических вершин остается неизменным, для произвольного $x \in S$ получаем следующую цепочку равенств:

$$\mathbf{P}\left\{x \in H_{f^k}^{(0)}\right\} = \mathbf{P}\left\{x \in H_{f^{k-1}}^{(0)}\right\} = \cdots = \mathbf{P}\left\{x \in H_f^{(0)}\right\} = \sum_{l=1}^{n} \frac{(n)_l}{n^{l+1}},$$

где $(n)_l = n(n-1)\ldots(n-l+1)$ — l-я факториальная степень числа n.

Распределение числа циклических вершин по компонентам графа G_{f^k} зависит от величины k. Поэтому в общем случае для произвольных $k \in \mathbb{N}$, $x \in S$ и $l \in \{1, \ldots, n\}$ величины

$$\mathbf{P}\left\{x \in H_{f^{k-i}}^{(0,l)}\right\} \quad \text{и} \quad \mathbf{P}\left\{x \in H_{f^{k-j}}^{(0,l)}\right\}, \quad \text{где} \quad i, j \in \{0, 1, \ldots, k\}, \quad i \neq j,$$

не совпадают. Это объясняется тем, что при переходе от f к f^k каждый цикл графа G_f длины $m \in \{1, \ldots, n\}$ распадается на (m, k) отдельных циклов графа G_{f^k} длины $m/(m, k)$. Здесь и далее (m, k) — наибольший общий делитель чисел m и k.

Для произвольных $k, l, i, j \in \mathbb{N}: \ i \leqslant j$ введем обозначение

$$Q_i^j(k, l) = \left\{m \in \mathbb{N} : i \leqslant m \leqslant j, \ \frac{m}{(m, k)} = l\right\}. \tag{2}$$

Замечание 2. Мощность множества $Q_i^j(k, l)$ не превосходит количества делителей d числа k, для которых $ld \leqslant j$. В частности, для простого k множество $Q_i^j(k, l)$ состоит не более чем из двух элементов.

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

$$\mathbf{P}\left\{x \in C_l\left(G_{f^k}\right)\right\} = \sum_{m \in Q_1^n(k,l)} \frac{(n)_m}{n^{m+1}}, \tag{3}$$

где $Q_1^n(k, l)$ определяется соотношением (2).

Доказательство. Зафиксируем вершину $x \in S$ и обозначим через m длину цикла компоненты графа G_f, где $m \leqslant n$. Тогда соответствующая компонента в графе G_{f^k}, содержащая вершину x, имеет цикл длины $l = m/(m, k)$. Используя обозначение (2), для произвольных $k \in \mathbb{N}$, $l \in \{1, \ldots, n\}$ можно записать совпадение событий

$$\left\{x \in C_l\left(G_{f^k}\right)\right\} = \bigcup_{m \in Q_1^n(k,l)} \{\alpha_f(x) = 0, \beta_f(x) = m\}. \tag{4}$$

Заметим, что события, стоящие под знаком объединения в (4), несовместны и что при фиксированных l и m вероятность каждого из них равна $(n)_m/n^{m+1}$ [14]. Поэтому, переходя в (4) к вероятностям событий, получаем

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

что соответствует утверждению теоремы. □

Следствие 1. *Пусть случайное отображение* $f\colon S \to S$ *имеет распределение* (1) *на* Ω. *Тогда при любых* $k \in \mathbb{N}$, $x \in S$ *и* $l \in \{1, \ldots, n\}$ *справедлива двусторонняя оценка*

$$\frac{1}{n} \sum_{m \in Q_1^n(k,l)} e^{-\left(1+\frac{m}{n}\right)\frac{m(m-1)}{2n}} \leqslant \mathbf{P}\left\{x \in C_l\left(G_{f^k}\right)\right\} \leqslant \frac{1}{n} \sum_{m \in Q_1^n(k,l)} e^{-\frac{(m-1)^2}{2n}}.$$

Доказательство. С учетом вытекающего из [17] двустороннего неравенства

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

справедливого для $1 \leqslant m \leqslant n$, получаем искомую двустороннюю оценку. $\square$

Замечание 3. Теорема 1 позволяет найти выражение для среднего значения мощности множества $C_l\left(G_{f^k}\right)$. Действительно, так как

$$\left|C_l\left(G_{f^k}\right)\right| = \sum_{x \in S} I\left\{x \in C_l\left(G_{f^k}\right)\right\},$$

то в силу равноправия всех $x \in S$

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

Далее для случайного $k \in \mathbb{N}$ и случайных вершин $x, y \in S$, $x \neq y$, вычислим совместную вероятность их попадания на циклы фиксированной длины в графе G_{f^k}.

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* $l_1, l_2 \in \{1, \ldots, n\}$: $l_1 + l_2 \leqslant n\,(1+\delta_{l_1,l_2})$, *справедливо равенство*

$$\begin{aligned}&\mathbf{P}\{x \in C_{l_1}(G_{f^k}), y \in C_{l_2}(G_{f^k})\} = \\ &= \delta_{l_1,l_2} \sum_{m \in Q_2^n(k,l_1)} \frac{(m-1)\,(n-2)_{m-2}}{n^m} + \sum_{m_1 \in Q_1^n(k,l_1)} \sum_{m_2 \in Q_1^{n-m_1}(k,l_2)} \frac{(n-2)_{m_1+m_2-2}}{n^{m_1+m_2}},\end{aligned}$$

где

$$\delta_{l_1,l_2} = \begin{cases} 1, & l_1 = l_2, \\ 0, & l_1 \neq l_2, \end{cases}$$

— символ Кронекера, а $Q_1^n(k,l), Q_2^n(k,l)$ *определяются соотношением* (2).

Доказательство. Для произвольных $x, y \in S$ определим индикатор

$$I_{x,y} = \begin{cases} 1, & \text{если } x, y \text{ лежат на одном цикле графа } G_f, \\ 0 & \text{в противном случае.} \end{cases}$$

Рассмотрим случай $l_1 = l_2 = l$. По формуле полной вероятности

$$\begin{aligned} &\mathbf{P}\{x, y \in C_l(G_{f^k})\} = \\ &= \mathbf{P}\{x, y \in C_l(G_{f^k}), I_{x,y}=1\} + \mathbf{P}\{x, y \in C_l(G_{f^k}), I_{x,y}=0\}. \end{aligned} \tag{5}$$

Вычислим первое слагаемое в правой части (5). Зафиксируем вершину $x \in S$. При этом для произвольной вершины $y \in S \setminus \{x\}$ существует в точности $m-1$ вариантов ее расположения на цикле длины m в графе G_f, содержащем x. Тогда, рассуждая, как и в теореме 1 (с учетом не одной, а двух вершин x, y), получаем равенство

$$\begin{aligned} &\mathbf{P}\left\{x, y \in C_l(G_{f^k}), I_{x,y} = 1\right\} = \\ &= \sum_{m \in Q_2^n(k,l)} \frac{m-1}{n^m} \prod_{i=2}^{m-1} (n-i) = \sum_{m \in Q_2^n(k,l)} \frac{(m-1)\,(n-2)_{m-2}}{n^m}. \end{aligned} \tag{6}$$

Для случая когда вершины x, y лежат на различных циклах длин $m_1, m_2 \in \{1, \ldots, n\}$, $m_1 + m_2 \leqslant n$, в графе G_f, имеем

$$\begin{aligned} \mathbf{P}\left\{\begin{matrix} x, y \in C_l\left(G_{f^k}\right) \\ I_{x,y} = 0 \end{matrix}\right\} &= \sum_{m_1 \in Q_1^n(k,l)} \sum_{m_2 \in Q_1^{n-m_1}(k,l)} \frac{1}{n^{m_1+m_2}} \prod_{i=2}^{m_1+m_2-1} (n-i) = \\ &= \sum_{m_1 \in Q_1^n(k,l)} \sum_{m_2 \in Q_1^{n-m_1}(k,l)} \frac{(n-2)_{m_1+m_2-2}}{n^{m_1+m_2}}. \end{aligned} \tag{7}$$

Подставив (6) и (7) в равенство (5), получим выражение для искомой вероятности в случае $l_1 = l_2 = l$.

Пусть теперь $l_1 \neq l_2$. В этом случае вершины x, y могут лежать только на разных циклах в графе G_{f^k} и в графе G_f. Поэтому

$$\begin{aligned} &\mathbf{P}\left\{x \in C_{l_1}\left(G_{f^k}\right), y \in C_{l_2}\left(G_{f^k}\right), l_1 \neq l_2\right\} = \\ &= \sum_{m_1 \in Q_1^n(k,l_1)} \sum_{m_2 \in Q_1^{n-m_1}(k,l_2)} \frac{(n-2)_{m_1+m_2-2}}{n^{m_1+m_2}}. \end{aligned} \tag{8}$$

Объединяя выражения (5) и (8) с использованием символа Кронекера, получаем утверждение теоремы. □

Следуя рассуждениям теоремы 2, можно вывести аналогичные формулы для совместных вероятностей $\mathbf{P}\{x_1 \in C_{l_1}(G_{f^k}), x_2 \in C_{l_2}(G_{f^k}), \ldots, x_s \in C_{l_s}(G_{f^k})\}$ при заданных значениях $l_1, \ldots, l_s \in \{1, \ldots, n\}$, где $s \leqslant n$, а также для дисперсии мощности множества $C_l(G_{f^k})$, $l \in \{1, \ldots, n\}$.

3. Вероятность попадания вершины в заданный слой

Поскольку для произвольного заданного $l \in \{1, \ldots, n\}$ множества вершин $H_{f^k}^{(t,l)}$ при $t = 0$ и $t \neq 0$ имеют принципиально различную структуру, опишем вероятностные характеристики множеств $H_{f^k}^{(t,l)}$, $t \in \{1, \ldots, n-1\}$.

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

$$\mathbf{P}\{x \in H_{f^k}^{(t,l)}\} = \sum_{s=0}^{k-1} \sum_{m \in Q_1^{n-tk+s}(k,l)} \frac{(n)_{m+tk-s}}{n^{m+tk-s+1}}, \tag{9}$$

где $Q_1^j(k,l)$ определяются соотношением (2).

Доказательство. Для произвольного $x \in S$ случайная величина $\alpha_{f^k}(x)$ удовлетворяет соотношению

$$\alpha_{f^k}(x) = \left[\frac{\alpha_f(x) + k - 1}{k}\right].$$

Поэтому при $l \in S$ и $t \in \{1, \ldots, n-l\}$ событие $\{x \in H_{f^k}^{(t,l)}\}$ может быть выражено через события $\{x \in H_f^{(j,m)}\}$, $j \in \overline{(t-1)k+1, tk}$, при подходящих значениях m:

$$\begin{aligned}
&\{x \in H_{f^k}^{(t,l)}\} = \\
&= \bigcup_{m \in Q_1^{n-tk}(k,l)} \{x \in H_f^{(tk,m)}\} \cup \bigcup_{m \in Q_1^{n-tk+1}(k,l)} \{x \in H_f^{(tk-1,m)}\} \cup \cdots \\
&\quad \cdots \cup \bigcup_{m \in Q_1^{n-(t-1)k+1}(k,l)} \{x \in H_f^{((t-1)k+1,m)}\} = \\
&= \bigcup_{s=0}^{k-1} \bigcup_{m \in Q_1^{n-tk+s}(k,l)} \{x \in H_f^{(tk-s,m)}\},
\end{aligned} \tag{10}$$

где под знаками объединения стоят несовместные события.

Из [14] известно, что для произвольных $v \in \{1, \ldots, n\}$ и $u \in \{1, \ldots, n-v\}$ справедливо равенство

$$\mathbf{P}\{x \in H_f^{(u,v)}\} = \frac{(n)_{u+v}}{n^{u+v+1}}. \tag{11}$$

Тогда, переходя в (10) к вероятностям событий и подставляя (11), получаем искомое утверждение. □

На основе рассуждений, проведенных при доказательстве теорем 2 и 3, несложно вывести точные выражения (см. [18]) для совместной вероятности

$$\mathbf{P}\{x \in H_{f^k}^{(t_1,l_1)}, y \in H_{f^k}^{(t_2,l_2)}\}.$$

Замечание 4. Аналогично замечанию 3 получаем формулу для математического ожидания

$$\mathbf{E}\left|H_{f^k}^{(t,l)}\right| = n\,\mathbf{P}\{x \in H_{f^k}^{(t,l)}\},$$

для которого с поправкой на коэффициент n справедливо утверждение теоремы 3.

Через $F_{\alpha_{f^k}(x)}(z)$, $z \in \{1, \ldots, n-1\}$, обозначим функцию распределения случайной величины $\alpha_{f^k}(x)$.

Тогда имеет место следующий результат.

Следствие 2. *Пусть случайное отображение*

$$f\colon S \to S$$

имеет распределение (1) *на* Ω. *Тогда при любых* $k \in \mathbb{N}$, $x \in S$ *и* $z \in \{1, \ldots, n-1\}$ *справедливы равенства*

$$\mathbf{P}\{x \in H_{f^k}^{(z)}\} = \sum_{l=1}^{n-z}\sum_{s=0}^{k-1}\sum_{m \in Q_1^{n-zk+s}(k,l)} \frac{(n)_{m+zk-s}}{n^{m+zk-s+1}},$$

$$F_{\alpha_{f^k}(x)}(z) = \sum_{m \in Q_1^n(k,l)} \frac{(n)_m}{n^{m+1}} + \sum_{u=1}^{z}\sum_{l=1}^{n-u}\sum_{s=0}^{k-1}\sum_{m \in Q_1^{n-uk+s}(k,l)} \frac{(n)_{m+uk-s}}{n^{m+uk-s+1}}.$$

Доказательство. Из равенства множеств

$$H_{f^k}^{(z)} = \bigcup_{l=1}^{n-z} H_{f^k}^{(z,l)}, \quad \text{где} \quad H_{f^k}^{(z,l_1)} \bigcap H_{f^k}^{(z,l_2)} = \varnothing \quad \text{при} \quad l_1 \neq l_2,$$

вытекают искомые соотношения для $\mathbf{P}\{x \in H_{f^k}^{(z)}\}$ и $F_{\alpha_{f^k}(x)}(z)$. □

Замечание 5. Полученные в теоремах 1, 3 выражения могут быть использованы при описании численных характеристик итерационных алгоритмов выработки производных ключей на базе некоторого отображения $f : S \to S$ (см., например, алгоритм выработки ключа «CryptoPro Key Meshing» [1, 19]), в которых на основе долговременного ключа $x \in S$ формируется последовательность производных ключей с заданным фиксированным шагом $k \in \mathbb{N}$:

$$x,\ f^k(x),\ f^{2k}(x), \ldots$$

Так, в частности, с учетом разбиения исходного множества S долговременных ключей вида

$$S = \bigcup_{u=1}^{n} \left[\bigcup_{t=0}^{u-1} H_{f^k}^{(t,u-t)} \right]$$

и полученных выражений для

$$\mathbf{P}\left\{x \in H_{f^k}^{(t,l)}\right\}, \qquad l \in \{1, \ldots, n\}, \quad t \in \{0, 1, \ldots, n-l\},$$

можно оценить число вырабатываемых производных ключей, при котором обеспечивается криптографически стойкое шифрование (значение случайной величины $\alpha_f(x) + \beta_f(x)$), а следовательно, и объем информации, которую можно надежно зашифровать на соответствующих ключах с заданной вероятностью.

В заключение автор благодарит А. М. Зубкова и Д. В. Пильщикова за интерес к работе и полезные замечания.

Список литературы

[1] Миронкин В. О., “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”, *Проблемы информационной безопасности. Компьютерные системы*, № 4 (2015), 140–146.

[2] 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.

[3] Миронкин В. О., “Об оценках распределения длины отрезка апериодичности в графе k-кратной итерации равновероятного случайного отображения”, *Прикл. дискретн. матем.*, № 42 (2018), 6–17.

[4] Миронкин В. О., “Исследование свойств и характеристик степени случайного отображения”, *Обозрение прикладной и промышленной математики*, **21**:1 (2014), 70–73.

[5] Зубков А. М., Серов А. А., “Совокупность образов подмножества конечного множества при итерациях случайных отображений”, *Дискретная математика*, **26**:4 (2014), 43–50.

[6] Пильщиков Д. В., “Асимптотическое поведение мощности полного прообраза случайного множества при итерациях отображений конечного множества”, *Математические вопросы криптографии*, **8**:1 (2017), 95–106.

[7] Зубков А. М., Серов А. А., “Предельная теорема для мощности образа подмножества при композиции случайных отображений”, *Дискретная математика*, **29**:1 (2017), 17–26.

[8] Миронкин В. О., Михайлов В. Г., “О множестве образов k-кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **9**:3 (2018), 99–108.

[9] Погорелов Б. А., Сачков В. Н., *Словарь криптографических терминов*, М.: МЦНМО, 2006, 94 с.

[10] Колчин В. Ф., *Случайные отображения*, М.: Наука, 1984, 208 с.

[11] Колчин В. Ф., Севастьянов Б. А., Чистяков В. П., *Случайные размещения*, М.: Наука, 1976, 224 с.

[12] Сачков В. Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.

[13] Flajolet P., Odlyzko A., “Random mapping statistics”, Lect. Notes Comput. Sci., **434**, 1989, 329–354.

[14] Harris B., “Probability distributions related to random mapping”, *Ann. Math. Statist.*, **31**:4 (1960), 1045–1062.

[15] Зубков А. М., “Вычисление распределения характеристик числа компонент и циклических точек случайного отображения”, *Математические вопросы криптографии*, № 2 (2010), 5–18.

[16] Михайлов В. Г., “Исследование числа циклических точек автомата из регистров с неравномерным движением”, В кн.: *Труды по дискретной математике*, М.: ФИЗМАТЛИТ, 2002, 167–172.

[17] Токарева Н. Н., *Симметричная криптография*, Новосибирск: Новосиб. гос. ун-т, 2012, 234 с.

[18] Миронкин В. О., “Об особенностях строения графа степени случайного отображения”, *Обозрение прикладной и промышленной математики*, **23**:1 (2016), 57–62.

[19] Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., Smyshlyaev S. V., Sonina L. A., “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*, **8**:2 (2017), 39–50.