В. О. Миронкин, Распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 3, 89–99

DOI: 10.4213/mvk302

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2019 Т. 10 № 3 С. 89–99

УДК 519.212.2+519.719.2 DOI https://doi.org/10.4213/mvk302

Распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений

В. О. Миронкин

Национальный исследовательский университет «Высшая школа экономики», Москва

Получено 29.*IV*.2019

Аннотация. Изучается распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений конечного множества. Получены точные и асимптотические выражения, а также неравенства для распределения, математического ожидания длины отрезка апериодичности и числа вершин с отрезком апериодичности заданной длины.

Ключевые слова: равновероятное случайное отображение, композиция отображений, граф отображения, отрезок апериодичности

Distribution of the length of aperiodicity segment in the graph of independent uniform random mappings composition

V. O. Mironkin

National Research University Higher School of Economics, Moscow

Abstract. We consider graph of independent uniform random mappings composition. The distribution of the length of aperiodicity segment in such graph is studied. Exact and asymptotic expressions as well as inequalities for the probability distribution, mathematical expectation of the length of aperiodicity segment, the number of vertices with aperiodicity segment of given length are obtained.

Keywords: uniform random mapping, composition of mappings, graph of a mapping, aperiodicity segment

Citation: Matematicheskie Voprosy Kriptografii, 2019, v. 10, № 3, pp. 89–99 (Russian)

1. Введение

Исследования, связанные с построением и анализом теоретико-вероятностных моделей функционирования механизмов защиты информации, занимают особое место в современной криптографии. Так, например, в [1–8] изучались характеристики k-кратной итерации равновероятного случайного отображения — объекта, используемого при обосновании криптографических свойств итерационных алгоритмов выработки производных ключей (см. [9,10]), характерной особенностью которых является многократная реализация некоторой фиксированной процедуры. В свою очередь, для повышения криптографической стойкости [11] (в частности, для исключения корреляции между тактами работы) подобные алгоритмы могут быть модифицированы за счет применения не одной, а нескольких процедур либо за счет дополнения некоторой случайности (например, раундовых ключей, векторов инициализации) в каждый такт работы. В таком случае k-кратная итерация одного и того же отображения уже не является адекватной моделью, и имеет смысл рассматривать композиции случайных равновероятных отображений [12–14], лучше описывающие процесс функционирования указанных модификаций итерационных алгоритмов.

Пусть $S = \{1, ..., n\}$, $n > 1$, — конечное множество, $\mathfrak{S}$ — множество всех n^n отображений $g\colon S \to S$.

Далее для произвольного $k \in \mathbb{N}$ рассмотрим последовательность независимых равновероятных отображений $f_1, \ldots, f_k$, имеющих распределение

$$\mathbf{P}\{f_j = g\} = \frac{1}{n^n}, \quad g \in \mathfrak{S}, \quad j = 1, \ldots, k. \tag{1}$$

Через $f_{[k]}$ обозначим композицию отображений: $f_{[k]}(x) = f_k(\ldots(f_1(x))\ldots)$, $x \in S$.

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 в отличие от равновероятного случайного отображения при применении $f_{[k]}$ к исходному множеству S происходит k-кратное сжатие [15].

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

В настоящей статье изучаются распределения длин отрезков апериодичности траекторий в случайных графах $G_{f_{[k]}}$, где $k \geqslant 1$ фиксировано.

2. Длина отрезка апериодичности

Траектория случайного отображения $f_{[k]}$, $k \geqslant 1$, начинающаяся в произвольной вершине $x_0 \in S$ графа $G_{f_{[k]}}$, определяется равенством

$$x_{i+1} = f_{[k]}\left(x_i\right), i = 0, 1, 2, \ldots$$

Вопросы, связанные с описанием момента первого возвращения на пройденную траекторию, представляют как теоретический, так и практический интерес для ряда криптографических задач [16–21], в частности для определения безопасного периода эксплуатации долговременной секретной информации или оценки объема данных, которые могут быть надежно зашифрованы на ключах, вырабатываемых на основе соответствующего итерационного алгоритма.

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

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

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

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

Через $\beta_f(x)$ обозначим случайную величину, равную длине цикла компоненты $\mathcal{K}_f(x)$. Множество всех циклических вершин графа G_f обозначим $C(G_f)$.

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

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

Через F_k обозначим функцию распределения случайной величины $\tau_{f_{[k]}}$.

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

Для любых $i_0, i_1 \in \mathbb{R} : i_0 > i_1$ положим $\prod\limits_{j=i_0}^{i_1}(\ldots) \equiv 1$.

Теорема. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых $z \in \{0, 1, \ldots, n\}$ и $x \in S$ справедливо равенство*

$$F_k(z) = 1 - \left(1 - \frac{z}{n}\right)\left(\frac{(n)_z}{n^z}\right)^k, \tag{2}$$

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

Доказательство. В случае $z = 0$ очевидно равенство $F_k(0) = 0$. При этом правая часть выражения (2) также обращается в нуль.

Пусть далее $z \in \{1, \ldots, n\}$. Для фиксированных $k \in \mathbb{N}$ и $x \in S$ рассмотрим итерационную процедуру формирования последовательности вершин $x, f_{[k]}(x), f_{[k]}^2(x), \ldots$ в графе $G_{f_{[k]}}$ (см. рисунок), каждая итерация которой состоит из k последовательных переходов по ребрам случайных графов $G_{f_1}, \ldots, G_{f_k}$ с одним и тем же множеством вершин S (далее — промежуточные графы).

Процесс зацикливания траектории в графе $G_{f_{[k]}}$, начинающейся в вершине x, существенно зависит от ее длины.

Пусть $z = 1$. В этом случае в графах G_{f_i} формируется ровно по одной вершине, и зацикливание траектории в $G_{f_{[k]}}$ за один шаг возможно только при условии $f_k(\ldots(f_1(x))\ldots) = x$, что выполняется с вероятностью $\frac{1}{n}$. Следовательно, $\mathbf{P}\left\{\tau_{f_{[k]}}(x) > 1\right\} = 1 - \frac{1}{n}$.

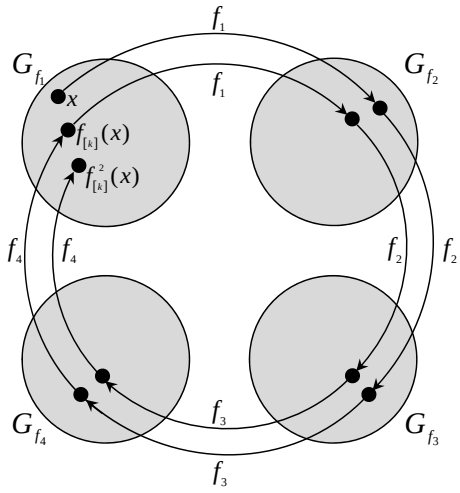

Рис. Процесс формирования компоненты $\mathcal{K}_{f_{[4]}}(x)$

Пусть $z > 1$, тогда незацикливание за z итераций траектории графа $G_{f_{[k]}}$, начинающейся в вершине x, означает, что в каждом отдельном промежуточном графе $G_{f_2}, \ldots, G_{f_k}$ среди z сформированных вершин в точности z различных, а в графе G_{f_1}, содержащем начальную вершину x и z сформированных, различных соответственно $z+1$ вершин. Таким образом, событие $\left\{\tau_{f_{[k]}}(x) > z\right\}$ может быть представлено в следующем виде:

$$\left\{\tau_{f_{[k]}}(x) > z\right\} = \bigcap_{u=1}^{k-1} \bigcap_{\substack{i,j=0 \\ i<j}}^{z-1} \bigcap_{\substack{k,l=0 \\ k<l}}^{z} \left\{ \begin{array}{c} f_u(\ldots(f_1(f^i_{[k]}(x)))\ldots) \neq f_u(\ldots(f_1(f^j_{[k]}(x)))\ldots) \\ f^k_{[k]}(x) \neq f^l_{[k]}(x) \end{array} \right\}.$$

Тогда, переходя к вероятности, получаем цепочку равенств:

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) > z\right\} = \prod_{i=1}^{z}\left(1-\frac{i}{n}\right)\cdot\left(\prod_{i=1}^{z-1}\left(1-\frac{i}{n}\right)\right)^{k-1} =$$

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

отсюда и из соотношения $F_k(z) = 1 - \mathbf{P}\left\{\tau_{f_{[k]}}(x) > z\right\}$ следует искомый результат.

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

$$\mathbf{E}\tau_{f_{[k]}}(x) = \sum_{z=0}^{n-1} \left(1 - \frac{z}{n}\right) \left(\frac{(n)_z}{n^z}\right)^k.$$

Доказательство. С учетом равенства $\mathbf{E}\xi = \sum\limits_{z=0}^{\infty} \mathbf{P}\{\xi > z\}$ для математического ожидания неотрицательной случайной величины ξ (см., например, [22])

$$\mathbf{E}\tau_{f_{[k]}}(x) = \sum_{z=0}^{\infty} \mathbf{P}\left\{\tau_{f_{[k]}}(x) > z\right\} = \sum_{z=0}^{n-1} \left(1 - \frac{z}{n}\right) \left(\frac{(n)_z}{n^z}\right)^k.$$

Теорема позволяет выписать асимптотику распределения случайной величины $\tau_{f_{[k]}}(x)$ для любого $x \in S$.

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 любых $u \geqslant 0$ и $x \in S$, где $|S| = n$, справедливо равенство*

$$\lim_{n\to\infty} \mathbf{P}\left\{\tau_{f_{[k]}}(x) > u\sqrt{2n}\right\} = e^{-ku^2}.$$

Доказательство. Согласно [23] для произвольного $m \in \{0, 1, \ldots, n\}$ выполняется двойное неравенство

$$e^{-\left(1+\frac{m}{n}\right)\frac{m(m-1)}{2n}} \leqslant \frac{(n)_m}{n^m} = \prod_{i=1}^{m-1}\left(1 - \frac{i}{n}\right) \leqslant e^{-\frac{m(m-1)}{2n}}. \tag{3}$$

Из него и из формулы $\mathbf{P}\left\{\tau_{f_{[k]}}(x) > m\right\} = \left(1 - \frac{m}{n}\right)\left(\frac{(n)_m}{n^m}\right)^k$ следует двусторонняя оценка

$$\left(1 - \frac{m}{n}\right) e^{-k\left(1+\frac{m}{n}\right)\frac{m(m-1)}{2n}} \leqslant \mathbf{P}\left\{\tau_{f_{[k]}}(x) > m\right\} \leqslant \left(1 - \frac{m}{n}\right) e^{-k\frac{m(m-1)}{2n}}. \tag{4}$$

Полагая $m = u\sqrt{2n}$ и переходя в (4) к пределу при $n \to \infty$, получаем утверждение следствия.

Замечание 2. Согласно следствию 2 для произвольного $x \in S$ случайная величина $\frac{\tau_{f_{[k]}}(x)}{\sqrt{2n}}$ при $n \to \infty$ асимптотически распределена по закону Рэлея [24] с модой $\sigma = \frac{1}{\sqrt{2k}}$. Пользуясь этим фактом, несложно вывести предельные выражения для численных характеристик случайной величины $\tau_{f_{[k]}}(x)$, представляющих криптографический интерес. Так, в частности, при $n \to \infty$

$$\mathbf{E}\tau_{f_{[k]}}(x) \sim \sqrt{\frac{\pi n}{2k}},$$

$$\mathbf{D}\tau_{f_{[k]}}(x) \sim \frac{2n}{k}\left(1 - \frac{\pi}{4}\right).$$

Следствие 3. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых $z \in \{1, \ldots, n\}$ и $x \in S$ справедливо равенство*

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} = \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k\right)\left(\frac{(n)_{z-1}}{n^{z-1}}\right)^k. \tag{5}$$

Доказательство. С учетом (2) для случайной величины $\tau_{f_{[k]}}$ имеем цепочку преобразований

$$\begin{aligned}\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} &= F_k(z) - F_k(z-1) = \\ &= 1 - \left(1 - \frac{z}{n}\right)\prod_{i=1}^{z-1}\left(1 - \frac{i}{n}\right)^k - \left(1 - \left(1 - \frac{z-1}{n}\right)\prod_{i=1}^{z-2}\left(1 - \frac{i}{n}\right)^k\right) = \\ &= \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k\right)\prod_{i=1}^{z-2}\left(1 - \frac{i}{n}\right)^k.\end{aligned}$$

Замечание 3. Величины (5) могут быть использованы при реализации ряда методов криптографического анализа (например, метода последовательного опробования [11]) итерационных алгоритмов выработки производных ключей.

Зачастую в реальных механизмах защиты информации значение n довольно велико. Как следствие, наряду с точными выражениями

исследуемых характеристик на практике существенную роль играют оценки, имеющие более простой аналитический вид и допускающие эффективное вычисление на ЭВМ.

Следствие 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 $z \in \{1, \ldots, n\}$ и $x \in S$ справедливы неравенства*

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} \geqslant \geqslant \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k\right) e^{-k\left(1+\frac{z}{n}\right)\frac{(z-1)(z-2)}{2n}}, \quad (6)$$

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} \leqslant \leqslant \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k\right) e^{-k\frac{(z-1)(z-2)}{2n}}. \quad (7)$$

Если при этом $z > 1$ и $kz \leqslant n$, то

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} > > \left(1 - \frac{z-1}{n}\right)\left(\frac{k(z-1)}{n} - C_k^2\frac{(z-1)^2}{n^2}\right) e^{-k\left(1+\frac{z}{n}\right)\frac{(z-1)(z-2)}{2n}},$$

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} \leqslant \frac{1}{n}\left(1 + k(z-1)\left(1 - \frac{z}{n}\right)\right) e^{-k\frac{(z-1)(z-2)}{2n}}.$$

Доказательство. С учетом двойного неравенства (3) и формулы (5) получаем искомые оценки (6) и (7).

Далее рассмотрим неравенство [25]

$$1 - kx \leqslant (1-x)^k \leqslant 1 - kx + C_k^2 x^2, \quad (8)$$

справедливое при $-1 < x < 1$, точность которого обратно пропорциональна абсолютному значению kx. При этом в условиях настоящего следствия и левая и правая части данного неравенства являются нетри-

виальными для $x = \frac{z-1}{n}$. Согласно (8) имеет место цепочка соотношений

$$1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k > \\ > 1 - \frac{z-1}{n} - \left(1 - \frac{z-1}{n}\right)\left(1 - \frac{k\,(z-1)}{n} + C_k^2 \frac{(z-1)^2}{n^2}\right) = \\ = \left(1 - \frac{z-1}{n}\right)\left(\frac{k\,(z-1)}{n} - C_k^2 \frac{(z-1)^2}{n^2}\right),$$

откуда следует оценка снизу для $\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\}$.

С другой стороны, из (8) получаем

$$1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k \leqslant \\ \leqslant 1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{k\,(z-1)}{n}\right) = \\ = \frac{1}{n} + \frac{k\,(z-1)}{n} - \frac{kz\,(z-1)}{n^2} = \frac{1}{n}\left(1 + k\,(z-1)\left(1 - \frac{z}{n}\right)\right),$$

и поэтому

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} \leqslant \frac{1}{n}\left(1 + k\,(z-1)\left(1 - \frac{z}{n}\right)\right) e^{-k\frac{(z-1)(z-2)}{2n}}.$$

Через $\nu_{f_{[k]}}(z)$ обозначим случайную величину, равную числу вершин в графе $G_{f_{[k]}}$, для которых длина отрезка апериодичности равна $z \in \{1, \ldots, n\}$.

Следствие 5. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого $z \in \{1, \ldots, n\}$ справедливо равенство*

$$\mathbf{E}\nu_{f_{[k]}}(z) = n\left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k\right)\left(\frac{(n)_{z-1}}{n^{z-1}}\right)^k.$$

Доказательство. Зафиксируем $z \in \{1, \ldots, n\}$ и представим случайную величину $\nu_{f_{[k]}}(z)$ в виде суммы индикаторов:

$$\nu_{f_{[k]}}(z) = \sum_{x \in S} I\left\{\tau_{f_{[k]}}(x) = z\right\}.$$

Тогда в силу равноправия всех вершин множества S

$$\mathbf{E}\nu_{f_{[k]}}(z) = \sum_{x\in S}\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} = n\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\},$$

откуда с учетом равенства (5) следует искомое выражение.

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

Список литературы

[1] 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.

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

[3] Миронкин В.О., “Об оценках распределения длины отрезка апериодичности в графе k-кратной итерации равновероятного случайного отображения”, *Прикладная дискретная математика*, **42** (2018), 6–17.

[4] Миронкин В.О., “Слои в графе k-кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **10**:1 (2019), 73–82.

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

[6] Михайлов В.Г., “О повторяемости состояний датчика псевдослучайных чисел при его многократном использовании”, *Теория вероятн. и её примен.*, **40**:4 (1995), 786–797.

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

[8] Пильщиков Д.В., “Исследование сложности метода радужных таблиц с маркерами цепочек”, *Математические вопросы криптографии*, **8**:4 (2017), 99–116.

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

[10] 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.

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

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

[13] Зубков А.М., Серов А.А., “Оценки среднего размера образа подмножества при композиции случайных отображений”, *Дискретная математика*, **30**:2 (2018), 27–36.

[14] Серов А.А., "Образы конечного множества при итерациях двух случайных зависимых отображений", *Дискретная математика*, **27**:4 (2015), 133–140.

[15] Flajolet P., Odlyzko A., "Random mapping statistics", EUROCRYPT'89, Lect. Notes Comput. Sci., **434**, 1989, 329–354.

[16] Hellman M.E., "A cryptanalytic time-memory trade-off", *IEEE Trans. Inf. Theory*, 1980, 401–406.

[17] Hong J., Ma D., "Success probability of the Hellman trade-off", *Inf. Process. Lett.*, **109**:7 (2009), 347–351.

[18] McSweeney J.K., Pittel B.G., "Expected coalescence time for a nonuniform allocation process", *Adv. Appl. Probab.*, **40**:4 (2008), 1002–1032.

[19] Oechslin P., "Making a faster cryptanalytic time-memory trade-off", *Lect. Notes Comput. Sci.*, **2729** (2003), 617–630.

[20] 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.

[21] 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.

[22] Лагутин М.Б., *Наглядная математическая статистика*: *учебное пособие* (2-*е изд.*), М. : БИНОМ. Лаборатория знаний, 2009, 472 с.

[23] Токарева Н.Н., *Симметричная криптография. Краткий курс*: *учебное пособие*, Новосибирск: Новосиб. гос. ун-т, 2012, 234 с.

[24] Вадзинский Р.Н., *Справочник по вероятностным распределениям*, СПб. : Наука, 2001, 295 с.

[25] Феллер В., *Введение в теорию вероятностей и ее приложения*, *т.* 2, М. : Мир, 1984, 738 с.