УДК 004.056.5:519.2
DOI: 10.37661/1816-0301-2024-21-4-37-45

Оригинальная статья
Original Article

О моделировании случайных данных для оценки качества статистических тестов в криптографии

В. Ю. Палуха✉, Н. А. Прохорчик, Ю. С. Харин

Учреждение Белорусского государственного университета «НИИ прикладных проблем математики и информатики», пр. Независимости, 4, Минск, 220030, Беларусь
✉E-mail: palukha@bsu.by

Аннотация
Цели. Решается задача моделирования вектора вероятностей, распределенного равномерно на гиперсфере заданного радиуса с центром в точке, соответствующей дискретному равномерному распределению. Актуальность задачи состоит в том, что такой вектор вероятностей необходим для генерации случайных последовательностей при анализе вероятностей ошибок первого и второго рода статистических критериев качества криптографических генераторов, проверяющих сложную нулевую гипотезу.
Методы. Используются теория вероятностей и матричный анализ.
Результаты. Разработаны метод и алгоритм моделирования вектора вероятностей, распределенного равномерно на гиперсфере заданного радиуса – точки в K-мерном пространстве, расположенной на пересечении гиперсферы и симплекса.
Заключение. Работоспособность разработанного алгоритма моделирования вектора вероятностей, распределенного равномерно на гиперсфере заданного радиуса, проиллюстрирована компьютерными экспериментами. Генерируемый с помощью разработанного алгоритма вектор вероятностей может быть использован для моделирования псевдослучайной последовательности, позволяющей оценивать вероятности ошибок первого и второго рода статистических тестов, применяемых при анализе качества криптографических генераторов.

Ключевые слова: криптографический генератор, статистическое тестирование, дискретное распределение вероятностей, распределение на гиперсфере, треугольная матрица, математическое моделирование

Благодарности. Работа выполнена при финансовой поддержке в рамках отдельного проекта № 20231671 Министерства образования Республики Беларусь.

Для цитирования. Палуха, В. Ю. О моделировании случайных данных для оценки качества статистических тестов в криптографии / В. Ю. Палуха, Н. А. Прохорчик, Ю. С. Харин // Информатика. – 2024. – Т. 21, № 4. – С. 37–45. – DOI: 10.37661/1816-0301-2024-21-4-37-45.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 20.08.2024
Подписана в печать | Accepted 04.10.2024
Опубликована | Published 30.12.2024

On modeling random data to evaluate the performance of statistical tests in cryptography

Uladzimir Y. Palukha✉, Mikalaj A. Prokharchyk, Yuriy S. Kharin

Research Institute for Applied Mathematics and Informatics
Belarusian State University,
av. Nezavisimosti, 4, Minsk, 220030, Belarus
✉*E-mail: palukha@bsu.by*

Abstract

Objectives. The problem of modeling a probability vector uniformly distributed on a hypersphere of a given radius with a center at a point corresponding to a discrete uniform distribution is solved. The relevance of the problem is that such a probability vector is necessary for generating random sequences when analyzing the probabilities of errors of the 1st and 2nd kind of statistical criteria for the quality of cryptographic generators that test the complex null hypothesis.

Methods. Probability theory and matrix analysis are used.

Results. The method and the algorithm for modeling a probability vector distributed uniformly on a hypersphere of a given radius, that is a point in *K*-dimensional space located at the intersection of the hypersphere and the simplex, have been developed.

Conclusion. The performance of the developed algorithm for modeling a probability vector distributed uniformly on a hypersphere of a given radius is illustrated by computer experiments. The probability vector generated using the developed algorithm can be used to model a pseudo-random sequence that allows one to estimate the probabilities of errors of the first and second kind of statistical tests used in analyzing the quality of cryptographic generators.

Keywords: cryptographic generator, statistical testing, discrete probability distribution, distribution on a hypersphere, triangular matrix, mathematical modeling

Acknowledgements. The work was performed with the financial support within the framework of the separate project No. 20231671 of the Ministry of Education of the Republic of Belarus.

For citation. Palukha U. Y., Prokharchyk M. A., Kharin Y. S. *On modeling random data to evaluate the performance of statistical tests in cryptography.* Informatika [*Informatics*], 2024, vol. 21, no. 4, pp. 37−45 (In Russ.). DOI: 10.37661/1816-0301-2024-21-4-37-45.

Conflict of interest. The authors declare of no conflict of interest.

Введение. Для оценки качества криптографических генераторов используются статистические тесты. В последнее время актуальными становятся тесты, проверяющие сложную нулевую гипотезу [1, 2]. Суть гипотезы заключается в том, что распределение вероятностей последовательности, порождаемой генератором, может отличаться от равномерного на небольшую величину, т. е. вектор распределения вероятностей лежит внутри шара некоторого радиуса с центром в точке, соответствующей равномерному распределению. Для того чтобы проверить работоспособность теста, необходимо смоделировать двоичный временной ряд с *K*-мерным вектором распределения вероятностей, который выбирается случайным равновероятным образом среди расположенных на гиперсфере заданного радиуса. Здесь $K = 2^s$, s – размер s-грамм (s-слов), используемых для тестирования генераторов. Существуют методы генерации случайного вектора, расположенного на гиперсфере и расположенного на симплексе [3]. Данная статья посвящена решению задачи моделирования случайного вектора вероятностей, который расположен на пересечении гиперсферы и симплекса.

Математическая модель и постановка задачи. Введем обозначения: $p = (p_1, \ldots, p_K)'$ – вектор-столбец вероятностей размера K; $\tilde{p} = (p_1, \ldots, p_{K-1})'$ – вектор-столбец, состоящий из первых $K - 1$ координат вектора p; $p_* = \left(\frac{1}{K}, \ldots, \frac{1}{K}\right)'$ – вектор-столбец равномерного распределения

вероятностей размера K; I_K – единичная матрица размера $K \times K$; 1_K – вектор размера K, в котором все элементы равны единице; $1_{K\times K}$ – матрица размера $K \times K$, в которой все элементы равны единице.

Обозначим искомое множество векторов распределений вероятностей как равенство

$$P_0^{\varepsilon} = \left\{ p = (p_k) : p_k \geq 0, \sum_{k=1}^{K} p_k = 1, \sum_{k=1}^{K} \left(p_k - \frac{1}{K} \right)^2 = \varepsilon^2 \right\}, \tag{1}$$

представляющее собой пересечение единичного симплекса и гиперсферы радиуса $\varepsilon > 0$ с центром в точке p_*. Задача заключается в генерации вектора распределения вероятностей p, который равномерно распределен на множестве (1).

Метод и алгоритм моделирования. Обозначим через C_K квадратную матрицу размера $K \times K$ вида

$$C_K = \left(c_{ij}\right) = \begin{pmatrix} 2\,1 \ldots 1 \\ 1\,2 \ldots 1 \\ \ldots\ldots\ldots \\ 1\,1 \ldots 2 \end{pmatrix} = I_K + 1_{K\times K}, \quad c_{ij} = \begin{cases} 2, & i = j; \\ 1, & i \neq j. \end{cases} \tag{2}$$

Представим C_K в виде произведения

$$C_K = \left(C_K^{1/2} \right)' C_K^{1/2}, \tag{3}$$

где $C_K^{1/2}$ – верхнетреугольная матрица, т. е. в виде разложения Холецкого.

Теорема 1. *Для координат вектора p, равномерно распределенного на множестве (1), справедливы выражения*

$$p_k = \begin{cases} \dfrac{1}{K} + \varepsilon \left(C_{K-1}^{-1/2} \xi \right)_k, & k = 1, 2, \ldots, K-1, \\ p_K = 1 - \sum\limits_{i=1}^{K-1} p_i, \end{cases} \tag{4}$$

где ξ – вектор, равномерно распределенный на гиперсфере единичного радиуса в $\mathbb{R}^{K-1}$, и выполняются ограничения

$$p_k \geq 0, \quad \sum_{k=1}^{K-1} p_k \leq 1, \quad k = 1, 2, \ldots, K-1. \tag{5}$$

Доказательство. Преобразуем условие в равенстве (1), задающее радиус гиперсферы, воспользовавшись тем, что $p_K = 1 - \sum\limits_{i=1}^{K-1} p_i$, и введенными обозначениями:

$$\begin{aligned} \sum_{k=1}^{K} \left(p_k - \frac{1}{K} \right)^2 &= \sum_{k=1}^{K-1} \left(p_k - \frac{1}{K} \right)^2 + \left(1 - \sum_{i=1}^{K-1} p_i - \frac{1}{K} \right)^2 = \sum_{k=1}^{K-1} \left(p_k - \frac{1}{K} \right)^2 + \\ &+ \left(\sum_{i=1}^{K-1} \frac{1}{K} + \frac{1}{K} - \sum_{i=1}^{K-1} p_i - \frac{1}{K} \right)^2 = \sum_{k=1}^{K-1} \left(p_k - \frac{1}{K} \right)^2 + \left(\sum_{i=1}^{K-1} \left(p_i - \frac{1}{K} \right) \right)^2 = \\ &= (\tilde{p} - \tilde{p}_*)'(\tilde{p} - \tilde{p}_*) + \left((\tilde{p} - \tilde{p}_*)' 1_{K-1} \right)^2 = (\tilde{p} - \tilde{p}_*)' I_{K-1} (\tilde{p} - \tilde{p}_*) + \\ &+ (\tilde{p} - \tilde{p}_*)' 1_{K-1} 1_{K-1}' (\tilde{p} - \tilde{p}_*) = (\tilde{p} - \tilde{p}_*)' (I_{K-1} + 1_{K-1} 1_{K-1}') (\tilde{p} - \tilde{p}_*) = \varepsilon^2. \end{aligned} \tag{6}$$

Тогда с учетом представлений (2) и (3) из выражения (6) получим

$$(\tilde{p}-\tilde{p}_*)'C_{K-1}(\tilde{p}-\tilde{p}_*)=\left(C_{K-1}^{1/2}(\tilde{p}-\tilde{p}_*)\right)'C_{K-1}^{1/2}(\tilde{p}-\tilde{p}_*)=\varepsilon^2$$

или

$$\left(\frac{1}{\varepsilon}C_{K-1}^{1/2}(\tilde{p}-\tilde{p}_*)\right)'\left(\frac{1}{\varepsilon}C_{K-1}^{1/2}(\tilde{p}-\tilde{p}_*)\right)=1. \tag{7}$$

Обозначим

$$\xi=\frac{1}{\varepsilon}C_{K-1}^{1/2}(\tilde{p}-\tilde{p}_*). \tag{8}$$

Из равенства (7) следует, что ξ – вектор, расположенный на гиперсфере единичного радиуса с центром в начале координат в $\mathbb{R}^{K-1}$. Для моделирования случайного вектора ξ воспользуемся алгоритмами из §3.13 или §3.5 [3]. Для моделирования p необходимо его выразить через ξ.

Из равенства (8) получим

$$\tilde{p}-\tilde{p}_*=\varepsilon C_{K-1}^{-1/2}\xi,\quad \tilde{p}=\tilde{p}_*+\varepsilon C_{K-1}^{-1/2}\xi, \tag{9}$$

откуда вытекают выражения (4). ■

Для того чтобы воспользоваться выражениями (4), необходимо вычислить матрицу $C_{K-1}^{-1/2}$. Для этого сначала вычислим $C_{K-1}^{1/2}$.

Лемма 1. Для элементов матрицы $C_K^{1/2}=\left(u_{ij}\right)$ справедливо представление

$$u_{ij}=\begin{cases}\dfrac{1}{\sqrt{i(i+1)}}, & i<j;\\ 0, & i>j;\\ \sqrt{\dfrac{i+1}{i}}, & i=j.\end{cases} \tag{10}$$

Доказательство. Для разложения Холецкого справедливы выражения [4]

$$u_{ij}=\begin{cases}\dfrac{1}{u_{ii}}\left(c_{ij}-\sum\limits_{k=1}^{i-1}u_{ki}u_{kj}\right), & i<j;\\ 0, & i>j;\\ \sqrt{c_{ii}-\sum\limits_{k=1}^{i-1}u_{ki}^2}, & i=j.\end{cases} \tag{11}$$

Докажем представление (10) методом математической индукции. При $K = 2$ из выражений (11) получим

$$u_{11} = \sqrt{2}, \quad u_{12} = \frac{1}{\sqrt{2}}, \quad u_{22} = \sqrt{2 - \frac{1}{2}} = \sqrt{\frac{3}{2}}, \quad u_{21} = 0,$$

что согласуется с представлением (10).

Согласно формуле (4.1.4.2) из работы [5] справедливо равенство

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}, \quad n \in \mathbb{N}. \tag{12}$$

Пусть для матриц C_k размерностей $k = 2, \ldots, K$ выражения (10) выполняются. Покажем их выполнение для матрицы C_{K+1}. Из выражений (11) видно, что вычисление элементов матрицы $C_k^{1/2}$ происходит последовательно по столбцам слева направо и внутри столбца сверху вниз от первой строки до диагонали, а все элементы под диагональю заполняются нулями. Для последовательного вычисления элементов матрицы $C_k^{1/2}$, расположенных над диагональю, используются элементы этой матрицы, расположенные в уже вычисленном ранее столбце и в текущем столбце; элементы, расположенные выше и поэтому уже вычисленные, а также соответствующий элемент матрицы C_k. Для вычисления элемента на диагонали используются элементы матрицы $C_k^{1/2}$, расположенные выше в этом столбце, и соответствующий элемент матрицы C_k. Поэтому при увеличении размерности матрицы C_K с K до $K + 1$ необходимо лишь вычислить $(K + 1)$-й столбец матрицы $C_{K+1}^{1/2}$ и дополнить ее $(K + 1)$-й строкой, где все элементы, кроме последнего, будут нулевыми. Следовательно, вычислим элементы $u_{i\,K+1}, i = 1, \ldots, K+1$, воспользовавшись свойством (12) и индуктивным предположением.

Сначала снова воспользуемся методом математической индукции, чтобы вычислить $u_{i\,K+1}, i = 1, \ldots, K$. При $i = 1$ получим $u_{1\,K+1} = \frac{c_{1K+1}}{u_{11}} = \frac{1}{\sqrt{2}}$. Полагаем далее, что для $i = 1, \ldots, j,\ j < K$, выполняется $u_{i\,K+1} = \frac{1}{\sqrt{i(i+1)}}, i = 1, \ldots, K$. Покажем для $i = j + 1$:

$$u_{j+1\,K+1} = \frac{1}{u_{j+1\,j+1}}\left(c_{j+1\,K+1} - \sum_{k=1}^{j} u_{k\,j+1} u_{k\,K+1}\right) = \sqrt{\frac{j+1}{j+2}}\left(1 - \sum_{k=1}^{j} \frac{1}{\sqrt{k(k+1)}} \cdot \frac{1}{\sqrt{k(k+1)}}\right) =$$

$$= \sqrt{\frac{j+1}{j+2}}\left(1 - \sum_{k=1}^{j} \frac{1}{k(k+1)}\right) = \sqrt{\frac{j+1}{j+2}}\left(1 - \frac{j}{j+1}\right) = \sqrt{\frac{j+1}{j+2}} \cdot \frac{1}{j+1} = \frac{1}{\sqrt{(j+1)(j+2)}}.$$

Теперь вычислим элемент матрицы $u_{K+1\,K+1}$:

$$u_{K+1\,K+1} = \sqrt{c_{K+1\,K+1} - \sum_{k=1}^{K} u_{k\,K+1}^2} = \sqrt{2 - \sum_{k=1}^{K} \frac{1}{k(k+1)}} = \sqrt{2 - \frac{K}{K+1}} = \sqrt{\frac{K+2}{K+1}},$$

что согласуется с представлением (10). ■

Лемма 2. Для элементов матрицы $C_K^{-1/2} = \left(\gamma_{ij}\right)$ справедливо представление

$$\gamma_{ij} = \begin{cases} -\dfrac{1}{\sqrt{j(j+1)}}, & i < j; \\ 0, & i > j; \\ \sqrt{\dfrac{i}{i+1}}, & i = j. \end{cases} \tag{13}$$

Доказательство. Для элементов матрицы, обратной к верхнетреугольной, справедливы выражения [6]

$$\gamma_{ij} = \begin{cases} -\dfrac{1}{u_{jj}} \sum\limits_{k=i}^{j-1} \gamma_{ik} u_{kj}, & i < j; \\ 0, & i > j; \\ \dfrac{1}{u_{ii}}, & i = j. \end{cases} \tag{14}$$

Докажем представление (13) методом математической индукции. При $K = 2$ из (14) получим

$$\gamma_{11} = \frac{1}{\sqrt{2}}, \quad \gamma_{12} = -\sqrt{\frac{2}{3}} \cdot \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = -\frac{1}{\sqrt{6}}, \quad u_{22} = \sqrt{\frac{2}{3}}, \quad u_{21} = 0,$$

что согласуется с (13).

Пусть для матриц $C_k^{1/2}$ размерностей $k = 2, \ldots, K$ выражения (13) выполняются. Покажем их выполнение для матрицы $C_{K+1}^{1/2}$. Из выражений (14) видно, что вычисление элементов матрицы $C_k^{-1/2}$ происходит последовательно по столбцам слева направо и внутри столбца сверху вниз от первой строки до диагонали, а все элементы под диагональю заполняются нулями. Для последовательного вычисления элементов матрицы $C_k^{-1/2}$, расположенных над диагональю, используются элементы этой матрицы, расположенные в текущей строке левее, а также элементы из текущего столбца матрицы $C_k^{1/2}$, расположенные не ниже соответствующего. Для вычисления элемента на диагонали применяется соответствующий элемент матрицы $C_k^{1/2}$. Поэтому при увеличении размерности матрицы $C_K^{1/2}$ с K до $K + 1$ необходимо лишь вычислить $(K + 1)$-й столбец матрицы $C_{K+1}^{-1/2}$ и дополнить ее $(K + 1)$-й строкой, где все элементы, кроме последнего, будут нулевыми. Следовательно, вычислим элементы $\gamma_{i\,K+1}, i = 1, \ldots, K+1$, воспользовавшись леммой 1, свойством (12) и индуктивным предположением:

$$\gamma_{i\,K+1} = -\frac{1}{u_{K+1\,K+1}} \sum_{k=i}^{K} \gamma_{ik} u_{k\,K+1} = -\sqrt{\frac{K+1}{K+2}} \left(\sqrt{\frac{i}{i+1}} \cdot \frac{1}{\sqrt{i(i+1)}} + \sum_{k=i+1}^{K} \left(-\frac{1}{\sqrt{k(k+1)}} \right) \cdot \frac{1}{\sqrt{k(k+1)}} \right) =$$

$$= -\sqrt{\frac{K+1}{K+2}} \left(\frac{1}{i+1} - \sum_{k=i+1}^{K} \frac{1}{k(k+1)} \right) = -\sqrt{\frac{K+1}{K+2}} \left(\frac{1}{i+1} - \sum_{k=1}^{K} \frac{1}{k(k+1)} + \sum_{k=1}^{i} \frac{1}{k(k+1)} \right) =$$

$$= -\sqrt{\frac{K+1}{K+2}}\left(\frac{1}{i+1} - \frac{K}{K+1} + \frac{i}{i+1}\right) = -\sqrt{\frac{K+1}{K+2}}\left(1 - \frac{K}{K+1}\right) = -\frac{1}{\sqrt{(K+1)(K+2)}}, i = 1, \ldots, K;$$

$$\gamma_{K+1\,K+1} = \frac{1}{u_{K+1\,K+1}} = \sqrt{\frac{K+1}{K+2}},$$

что согласуется с представлением (13). ■

Отметим, что приведенное доказательство является конструктивным. Справедливость леммы 2 можно также проверить прямым перемножением матриц $U = (u_{ij})$, $\Gamma = (\gamma_{ij})$, определяемых представлениями (10) и (13), и сравнением результата с единичной матрицей: $U\Gamma = I_K$.

Следствие 1. *Алгоритм моделирования вектора K-мерного распределения вероятностей, который выбирается случайным равновероятным образом среди расположенных на гиперсфере радиуса ε, состоит из следующих шагов:*

1) вычислить матрицу $C_{K-1}^{-1/2}$ *по формуле (13);*

2) сгенерировать вектор ξ, равномерно распределенный на гиперсфере единичного радиуса в $\mathbb{R}^{K-1}$*, методом из §3.13 либо §3.5 [3];*

3) методом исключения сгенерировать вектор p по формуле (4): в случае, если не выполняется условие (5), вернуться к шагу 2.

Отметим, что разработанный алгоритм применим для $\forall K \geq 2$, а не только для $K = 2^s$.

Результаты компьютерного моделирования. Для демонстрации работы алгоритма произведено моделирование векторов при $K = 3$. Данное значение K позволяет графически отобразить сгенерированные точки. В соответствии с алгоритмом двумя способами в зависимости от метода на шаге 2 сгенерировано 1000 векторов при $K = 3$ и $\varepsilon = 0{,}05$. Как следует из формулы (1), при $K = 3$ искомые векторы лежат на окружности радиуса ε с центром в точке (1/3, 1/3, 1/3) на плоскости $x + y + z = 1$. Расположение K сгенерированных точек в пространстве показано на рис. 1. Видно, что точки действительно лежат на заданной выше окружности.

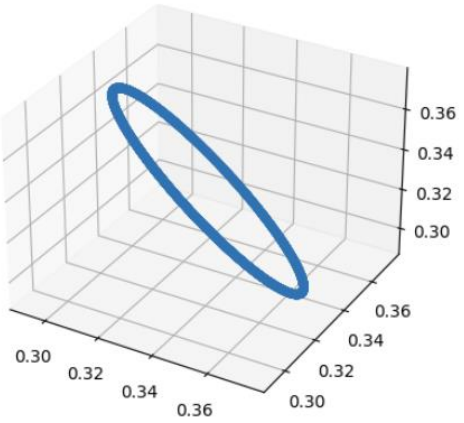

Рис. 1. Расположение в пространстве сгенерированных векторов

Fig. 1. The spatial arrangement of generated vectors

Для того чтобы убедиться, что сгенерированные точки действительно расположены равномерно на допустимом множестве, перейдем к полярным координатам и построим гистограмму значений угла φ. Для этого нужно преобразовать декартовы координаты таким образом, чтобы точки лежали на окружности с центром в начале координат на плоскости *Oxy*. Сначала вычтем из каждой координаты 1/3 и получим окружность радиуса ε с центром в точке (0, 0, 0) на плоскости $x + y + z = 0$. Данная плоскость пересекает плоскость $z = 0$ по прямой $y = -x$. Найдем угол ψ между плоскостями. Согласно п. 14.6 [7] $\cos\psi = \frac{1}{\sqrt{3}}$. Для того чтобы преобразовать плоскость

$x + y + + z = 0$ к плоскости $z = 0$, необходимо выполнить композицию поворотов: на угол $\frac{\pi}{4}$ по оси Oz и на угол $\psi = \arccos\frac{1}{\sqrt{3}}$ по оси Ox. Матрица поворота согласно работе [8] равна

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & -\frac{\sqrt{2}}{\sqrt{3}} \\ 0 & \frac{\sqrt{2}}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{\sqrt{2}}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}. \quad (15)$$

После умножения нормированных векторов на матрицу (15) их третьи координаты будут равны 0. Теперь можно перейти к полярным координатам в соответствии с формулами из п. 6.4 [9], заменив диапазон $[-\pi, \pi]$ на $[0, 2\pi]$. Гистограммы значений угла φ полученных точек изображены на рис. 2 и 3. На рисунках видно, что распределение точек действительно близко к равномерному.

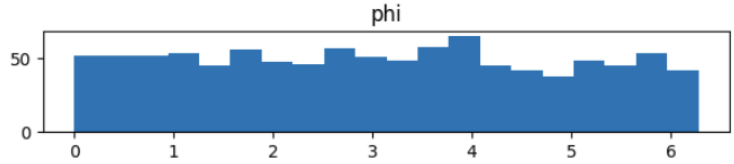

Рис. 2. Гистограмма угла φ, алгоритм из §3.13 [3]

Fig. 2. Histogram of angle φ, algorithm from §3.13 [3]

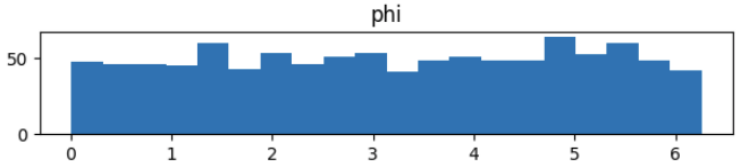

Рис. 3. Гистограмма угла φ, алгоритм из §3.5 [3]

Fig. 3. Histogram of angle φ, algorithm from §3.5 [3]

Заключение. В статье разработаны метод и алгоритм моделирования вектора вероятностей, распределенного равномерно на гиперсфере заданного радиуса с центром в точке, соответствующей равномерному распределению. Проведены компьютерные эксперименты, демонстрирующие работоспособность разработанного алгоритма.

Вклад авторов. *В. Ю. Палуха*, *Ю. С. Харин* обосновали теоретическую часть и подготовили текст статьи; *Н. А. Прохорчик* реализовал алгоритм моделирования на языке Python и компьютерные эксперименты.

Список использованных источников

1. Харин, Ю. С. О статистической проверке сложных гипотез об *s*-мерном равномерном распределении вероятностей двоичных последовательностей / Ю. С. Харин, А. М. Зубков // Дискретная математика. – 2024. – Т. 36, вып. 1. – С. 116–135. – DOI: 10.4213/dm1806.

2. Палуха, В. Ю. Статистическое тестирование криптографических генераторов на основе сложной нулевой гипотезы / В. Ю. Палуха, Ю. С. Харин // Теоретическая и прикладная криптография : материалы II Междунар. науч. конф., Минск, 19–20 окт. 2023 г. / Белорус. гос. ун-т ; редкол.: Ю. С. Харин (гл. ред.) [и др.]. – Минск : БГУ, 2023. – С. 185–193.

3. Харин, Ю. С. Практикум на ЭВМ по математической статистике / Ю. С. Харин, М. Д. Степанова. – Минск : Университетское, 1987. – 304 с.

4. Воеводин, В. В. Матрицы и вычисления / В. В. Воеводин, Ю. А. Кузнецов. – М. : Наука, 1984. – 320 с.

5. Прудников, А. П. Интегралы и ряды / А. П. Прудников, Ю. А. Брычков, О. И. Маричев. – М. : Наука, 1981. – 800 с.

6. Каплан, И. А. Практические занятия по высшей математике : в 5 ч. / И. А. Каплан. – Харьков : Изд-во Харьковского университета, 1972. – Ч. V. – 413 с.

7. Милованов, М. В. Алгебра и аналитическая геометрия : в 2 ч. / М. В. Милованов, Р. И. Тышкевич, А. С. Феденко. – Минск : Вышэйшая школа, 1984. – Ч. 1. – 302 с.

8. Лурье, А. И. Аналитическая механика / А. И. Лурье. – М. : Физматлит, 1961. – 824 с.

9. Torrence, B. F. The Student's Introduction to Mathematica® / B. F. Torrense, E. A. Torrence. – N. Y. : Cambridge University Press, 2009. – 483 p.

References

1. Kharin Yu. S., Zubkov A. M. *On statistical testing of composite hypotheses on s-dimensional uniform probability distribution of binary sequences*. Diskretnaya Matematika [*Discrete Mathematics*], 2024, vol. 36, iss. 1, pp. 116–135 (In Russ.). DOI: 10.4213/dm1806.

2. Palukha U. Yu., Kharin Yu. S. *Statistical testing of cryptographic generators based on a complex null hypothesis*. Teoreticheskaja i prikladnaja kriptografija : materialy II Mezhdunarodnoj nauchnoj konferencii, Minsk, 19–20 oktjabrja 2023 g. [*Theoretical and Applied Cryptography : Proceedings of the II International Scientific Conference, Minsk, 19–20 October 2023*]. Ed. board: Yu. S. Kharin, V. I. Bernik, P. V. Kuchinsky, A. N. Kurbatsky. Minsk, Belorusskij gosudarstvennyj universitet, 2023, pp. 185–193 (In Russ.).

3. Kharin Yu. S., Stepanova M. D. Praktikum na EVM po matematicheskoy statistike. *Computer Workshop on Mathematical Statistics*. Minsk, Universitetskoe, 1987, 304 p. (In Russ.).

4. Voevodin V. V., Kuznecov Yu. A. Matricy i vychisleniya. *Matrices and Calculations*. Moscow, Nauka, 1984, 320 p. (In Russ.).

5. Prudnikov A. P., Brychkov Yu. A., Marichev O. I. Integraly i rjady. *Integrals and Series*. Moscow, Nauka, 1981, 800 p. (In Russ.).

6. Kaplan I. A. Prakticheskiye zaniatiya po vysshej matematike : v 5 chastjah. *Practical Classes in Higher Mathematics : in 5 Parts.* Kharkov, Izdatel'stvo Har'kovskogo universiteta, 1972, part V, 413 p. (In Russ.)

7. Mikovanov M. V., Tyshkevich R. I., Fedenko A. S. Algebra i analiticheskaya geometriya : v 2 chastjah. *Algebra and Analytic Geometry: in 2 Parts.* Minsk, Vysheyshaya shkola, 1984, part 1, 302 p. (In Russ.).

8. Lurje A. I. Analiticheskaya mekhanika. *Analytical Mechanics*. Moscow, Fizmatlit, 1961, 824 p. (In Russ.).

9. Torrence B. F., Torrence E. A. *The Student's Introduction to Mathematica®*. New York, Cambridge University Press, 2009, 483 p.

Информация об авторах

Палуха Владимир Юрьевич, кандидат физико-математических наук, доцент, заведующий НИЛ математических методов защиты информации, НИИ прикладных проблем математики и информатики, Белорусский государственный университет.
E-mail: palukha@bsu.by
https://orcid.org/0009-0007-8474-1146

Прохорчик Николай Анатольевич, младший научный сотрудник, НИЛ математических методов защиты информации, НИИ прикладных проблем математики и информатики, Белорусский государственный университет.
E-mail: prohorchikna@bsu.by

Харин Юрий Семенович, доктор физико-математических наук, профессор, академик НАН Беларуси, директор, НИИ прикладных проблем математики и информатики, Белорусский государственный университет.
E-mail: kharin@bsu.by
https://orcid.org/0000-0003-4226-2546

Information about the authors

Uladzimir Y. Palukha, Ph. D. (Phys.-Math.), Assoc. Prof., Head of the Research Laboratory of Mathematical Methods of Information Security, Research Institute for Applied Mathematics and Informatics, Belarusian State University.
E-mail: palukha@bsu.by
https://orcid.org/0009-0007-8474-1146

Mikalay A. Prokharchyk, Junior Researcher, Research Laboratory of Mathematical Methods of Information Security, Research Institute for Applied Mathematics and Informatics, Belarusian State University.
E-mail: prohorchikna@bsu.by

Yuriy S. Kharin, D. Sc. (Phys.-Math.), Prof., Acad. of the National Academy of Sciences of Belarus, Dir., Research Institute for Applied Mathematics and Informatics, Belarusian State University.
E-mail: kharin@bsu.by
https://orcid.org/0000-0003-4226-2546