Math-Net.Ru

Общероссийский математический портал

О. В. Денисов, Спектральный критерий для проверки гипотез о случайных под-
становках, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 3, 19–28

DOI: <https://doi.org/10.4213/mvk193>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.172.240.79

26 апреля 2023 г., 08:26:23

**Спектральный критерий
для проверки гипотез о случайных подстановках**

О. В. Денисов

ООО «Центр сертификационных исследований», Москва

Получено 15.IX.2015

Аннотация. Пусть для каждой из N независимых одинаково распределенных случайных подстановок наблюдается пара, состоящая из случайного равномерно распределенного аргумента и соответствующего значения подстановки. Рассматривается задача проверки гипотезы о равновероятности подстановок против гипотезы о том, что они получены как произведения r независимых подстановок с известным распределением. Предлагается и изучается критерий, который строится по собственным векторам матриц вероятностей переходов аргументов в значения.

Ключевые слова: случайные подстановки, блочные шифрсистемы, атака различения, матрица переходных вероятностей, собственные векторы

Spectral criterion for testing hypotheses on random permutations

O. V. Denisov

Sertification Research Center, LLC, Moscow

Abstract. Suppose that for each of N independent identically distributed random permutations we observe a pair consisting of a random uniformly distributed argument and a corresponding value of permutation. We consider the problem of testing the hypothesis that the distribution of permutations is uniform against the hypothesis that permutations are the products of r independent permutations with known distribution. A test constructed by eigenvectors of matrices of transition probabilities (arguments to values) is proposed and investigated.

Key words: random permutations, block ciphers, distinguishing attack, matrix of the transition probabilities, eigenvectors

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 3, pp. 19–28 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

1. Постановка задачи

Пусть X — конечное множество мощности $|X| = M$, $\mathcal{S}(X)$ — множество всех подстановок на X . При блочном шифровании часто результирующая подстановка F_r вырабатывается как произведение r раундовых подстановок f_k из сравнительно небольшого подмножества $G \subset \mathcal{S}(X)$:

$$F_r(x) = (f_1 \cdots f_r)(x), \quad x \in X, f_k \in G, 1 \leq k \leq r.$$

Частью многих атак на блочные шифрсистемы является атака различения (distinguishing attack), т. е. критерий проверки гипотезы о том, что наблюдаются *переходы* (т. е. пары: аргумент и соответствующее ему значение) случайной подстановки с равномерным распределением на $\mathcal{S}(X)$.

Опишем модель наблюдений и проверяемые гипотезы. Через $U(A)$ будем обозначать равномерное распределение на конечном множестве A . Наблюдаются N переходов $(x(1), y(1)), \dots, (x(N), y(N))$ для N независимых копий $F^{(1)}, \dots, F^{(N)}$ случайной подстановки F :

$$x(t) \sim U(X), \quad y(t) = F^{(t)}(x(t)), \quad F^{(t)} \sim F, \quad 1 \leq t \leq N, \quad (1)$$

где независимые равномерно распределенные на X аргументы не зависят от подстановок. Требуется построить и исследовать критерий для проверки простой гипотезы H_U о равномерности распределения подстановки F

$$H_U: F \sim U(\mathcal{S}(X))$$

против простой альтернативы H_A , состоящей в том, что F имеет такое же распределение, как распределение произведения r независимых копий случайной подстановки f

$$H_A: F = f_1 \cdots f_r, \quad f_k \sim f, \quad 1 \leq k \leq r.$$

Вектор $(p_g = \mathbf{P}\{f = g\}, g \in G)$ распределения f и число раундов r считаются известными.

Отметим, что каждый наблюдаемый переход получен на подстановке, выбираемой независимо от предыдущих. Это условие вместе с условием независимости аргументов обеспечивает независимость наблюдений.

Далее мы построим критерий для проверки H_U против H_A , вероятность $\alpha_U(N)$ ошибки которого (принятия H_A , когда верна H_U) при $N \rightarrow \infty$ стремится к заданному значению α , и оценим число наблюдений N , при котором вероятность $\alpha_A(N)$ ошибки другого рода близка к заданному значению β .

Заметим, что при гипотезе H_A подстановка F лежит в слое G^r группы подстановок, порожденной системой образующих G . Здесь и далее в зависимости от контекста обозначение A^i используется как для декартовой степени множества A , так и для множества i -кратных произведений элементов группы A . В общем случае возможно равенство $G^r = \mathcal{S}(X)$, и если при этом распределение (p_g) индуцирует равномерное распределение на G^r , то гипотезы являются неразличимыми.

2. Построение критерия

2.1. Сведение задачи к проверке гипотез о матрице вероятностей переходов

Обозначим через $Q = \|P\{j = F(i)\}\|_{i,j \in X}$ матрицу вероятностей переходов (аргументов в значения) при действии случайной подстановки F . Равномерную матрицу размера L обозначим через $U = \frac{1}{L} \mathbf{1}$, где $\mathbf{1}$ — матрица, состоящая из всех единиц, ее размер L определяется контекстом. Через $\vec{1}$ и $1^\downarrow$ будем обозначать вектор-строку и вектор-столбец, состоящие из всех единиц. Единичной матрицей размера L будем называть матрицу, являющуюся нейтральным элементом относительно умножения:

$$E = \text{diag}(1, \dots, 1) = \sum_{1 \leq i \leq L} E_{i,i}.$$

Через $E_{i,j}$ здесь и далее обозначаем матрицу, единственный ненулевой элемент которой равен 1 и находится на месте i, j .

Легко показать, что $Q = U = \frac{1}{M} \mathbf{1}$ при гипотезе H_U . При гипотезе H_A при случайном выборе аргумента x , не зависящем от независимых подстановок f_k , $1 \leq k \leq r$, последовательность случайных величин

$$x, f_1(x), (f_1 f_2)(x) = f_2(f_1(x)), \dots \quad (2)$$

образует однородную цепь Маркова с матрицей переходных вероятностей $\mathbb{P} = \sum_{g \in G} p_g \pi_g$ за 1 шаг, где $\pi_g := \|\text{ind}\{g(i) = j\}\|_{i,j \in X}$ — подстановочные матрицы. Поэтому здесь $Q = \mathbb{P}^r$.

Матрицы π_g являются дважды стохастическими 0,1-матрицами; следовательно, их взвешенная сумма $\mathbb{P}$ и ее степени также являются дважды стохастическими:

$$\vec{1} \mathbb{P}^r = \vec{1}, \quad \mathbb{P}^r 1^\downarrow = 1^\downarrow, \quad r \geq 1.$$

Первое равенство означает также, что равномерное распределение на X является стационарным распределением цепи Маркова.

Итак, задача сводится к построению критерия для проверки гипотезы $Q = U$ против гипотезы $Q = \mathbb{P}^r$. Далее везде считаем, что $\mathbb{P}^r \neq U$.

2.2. Построение различающих пар векторов

Для простоты будем считать, что цепь Маркова (2) имеет один класс существенных состояний, и он ациклический. Такое предположение практически всегда выполнено, поскольку в противном случае $\mathbb{P}^r$ содержит нули для любого $r \in \mathbb{N}$, т. е. шифр не является транзитивным.

С помощью теоремы Биркгофа [5, с. 47] несложно доказать, что цепь с дважды стохастической матрицей переходных вероятностей не имеет несущественных состояний. Поэтому предположение о единственности класса существенных состояний эквивалентно тому, что все состояния из X сообщаются. Конъюнкция этого условия и предположения об ациклическости эквивалентна условию эргодичности цепи, т. е. существованию предела $\lim_{r \rightarrow \infty} \mathbb{P}^r$. При этом $\lim_{r \rightarrow \infty} \mathbb{P}^r = \mathbb{U}$ в силу дважды стохастичности матрицы $\mathbb{P}$.

Пусть $\lambda_1 = 1, \lambda_2, \dots, \lambda_s \in \mathbb{C}$ — спектр матрицы $\mathbb{P}$, т. е. множество всех ее различных собственных чисел (комплексных корней $\chi_{\mathbb{P}}(x)$); здесь и далее через $\chi_A(x)$ обозначаем характеристический многочлен матрицы A . Спектральный радиус [4, с. 188] стохастической матрицы равен 1 (см., например, [3, с. 105] или [4, с. 266]). Эргодичность цепи эквивалентна тому (см., например, [3, с. 108]), что

$$\text{кратность корня } 1 \text{ равна } 1, \quad \lambda_1 = 1 > |\lambda_2| \geq \dots \geq |\lambda_s|. \quad (3)$$

Далее предположим также наличие еще одного, кроме λ_1 , ненулевого действительного собственного значения:

$$0 \neq \lambda_i \in \mathbb{R} \text{ для некоторого } 2 \leq i \leq s, \quad (4)$$

и обозначим через l его кратность. Заметим, что тогда спектр матрицы $\mathbb{P}^r$ содержит λ_i^r (см., например, [4, с. 65]), и так как $\chi_{\mathbb{U}}(x) = x^{M-1}(x-1)$, то при $\mathbb{P}^r = \mathbb{U}$ условие (4) не может быть выполнено.

Обозначим через $|\vec{u}|$ евклидову норму вектора $\vec{u}$.

Теорема 1. Пусть спектр дважды стохастической матрицы $\mathbb{P}$ удовлетворяет условиям (3) и (4). Тогда существует такая пара векторов $\vec{u}, v^\perp \in \mathbb{R}^M$, что

$$\vec{u}\mathbb{P}^r v^\perp = \lambda_i^r, \quad \vec{u}\mathbb{U} v^\perp = 0. \quad (5)$$

Доказательство. Рассмотрим линейное преобразование $\varphi : \vec{a} \mapsto \vec{a}\mathbb{P}$ пространства $(\mathbb{R}^M, +)_{\mathbb{R}}$. Так как $\chi_{\mathbb{P}}(x) = (x-1)(x-\lambda_i)^l \chi_1(x)$ — произведение трех взаимно простых многочленов, то пространство раскладывается в прямую сумму соответствующих многочленам подпространств [3, с. 77], инвариантных относительно φ .

Выберем во втором подпространстве жорданов базис и обозначим через s минимальный размер жордановых клеток $J_{s_i}(\lambda_i)$ с корнем λ_i , на которые распадается матрица линейного преобразования подпространства в этом базисе. Здесь и ниже через $J_k(\lambda)$ обозначаем жорданову клетку размера k с корнем λ . Тогда с учетом [3, с. 77] получаем, что $\mathbb{P}$ подобна (над $\mathbb{R}$) блочно-диагональной матрице D :

$$C^{-1}\mathbb{P}C = D = \text{Diag}(J_1(1), J_s(\lambda_i), A). \quad (6)$$

Обозначая далее $B = C^{-1}$, из равенства $BC = E$ получаем соотношение $\vec{B}_i C_j^\downarrow = \text{ind } \{i=j\}$, $i, j \in \{1, \dots, M\}$, означающее *биортогональность базисов* $\{\vec{B}_i\}$ и $\{C_j^\downarrow\}$ [4, с. 67], т. е. наборов строк матрицы B и столбцов матрицы C .

Из (6) следует, что $\mathbb{P}C = CD$. Так как первые два столбца произведений матриц из левой и правой частей этого равенства равны соответственно $\mathbb{P}C_1^\downarrow, \mathbb{P}C_2^\downarrow$ и $C_1^\downarrow, \lambda_i C_2^\downarrow$, то $C_1^\downarrow, C_2^\downarrow$ являются правыми собственными векторами матрицы $\mathbb{P}$, соответствующими собственным значениям 1 и λ_i .

Из (6) также следует, что $B\mathbb{P} = DB$. Первая и $(s+1)$ -я строки этих матриц равны соответственно $\vec{B}_1\mathbb{P}, \vec{B}_{s+1}\mathbb{P}$ и $\vec{B}_1, \lambda_i \vec{B}_{s+1}$. Поэтому векторы $\vec{B}_1, \vec{B}_{s+1}$ являются левыми собственными векторами матрицы $\mathbb{P}$, соответствующими собственным значениям 1 и λ_i . Таким образом,

$$\vec{B}_{s+1}\mathbb{P}^r = \lambda_i \vec{B}_{s+1}\mathbb{P}^{r-1} = \dots = \lambda_i^r \vec{B}_{s+1}, \quad \mathbb{P}^r C_2^\downarrow = \lambda_i^r C_2^\downarrow. \quad (7)$$

Кроме того, в силу первого условия в (3) векторы $\vec{B}_1$ и $C_1^\downarrow$ коллинеарны вектору $\vec{1}$, что с учетом биортогональности дает равенства

$$\vec{B}_{s+1}\mathbb{U} = \vec{B}_{s+1} \frac{1}{M} \mathbf{1}^\downarrow \vec{1} = 0\vec{1} = \vec{0}, \quad \mathbb{U}C_2^\downarrow = 0^\downarrow.$$

Отсюда с учетом (7) получаем, что следующие две пары векторов

$$\vec{B}_{s+1} \text{ и } (\vec{B}_{s+1})^T / |\vec{B}_{s+1}|^2, \quad (C_2^\downarrow)^T / |C_2^\downarrow|^2 \text{ и } C_2^\downarrow, \quad (8)$$

каждая из которых построена с использованием одного собственного вектора, удовлетворяют условиям (5).

Заметим также, что если $l = 1$, то $s = 1$, $\vec{B}_{s+1} = \vec{B}_2$, и с учетом биортогональности пара векторов

$$\vec{B}_2 \text{ и } C_2^\downarrow, \quad (9)$$

построенная с использованием двух собственных векторов, также удовлетворяет условиям (5).

Теорема 1 доказана. $\square$

2.3. Статистика и вид критерия

Рассмотрим матричную статистику $\hat{Q} = \frac{M}{N} \sum_{1 \leq t \leq N} E_{x(t), y(t)}$. Согласно модели наблюдений (1) она является суммой независимых матриц, распределенных как случайная матрица $E_{x, F(x)}$, $x \sim U(X)$. Поэтому математическое ожидание статистики равно

$$\begin{aligned} \mathbf{E}\hat{Q} &= M\mathbf{E}E_{x, F(x)} = M \|\mathbf{P}\{x = i, F(x) = j\}\|_{i, j \in X} = \\ &= M \|\mathbf{P}\{x = i\}\mathbf{P}\{F(i) = j\}\|_{i, j \in X} = Q, \end{aligned}$$

т. е. $\hat{Q}$ является несмещенной оценкой для Q при каждой гипотезе.

Любую пару векторов $\vec{u}, v^\downarrow$, удовлетворяющую условиям (5), далее будем называть *различающей*; теорема 1 дает достаточные условия существования различающей пары. Для произвольной фиксированной различающей пары векторов определим скалярную статистику

$$S(N) = N\vec{u}\hat{Q}v^\downarrow = M \sum_{1 \leq t \leq N} u_{x(t)}v_{y(t)}. \quad (10)$$

Согласно (1), $S(N)$ — сумма независимых случайных величин, имеющих такое же распределение, как случайная величина $\zeta = Mu_x v_{F(x)}$. Дисперсия ζ в силу независимости слагаемых равна $\frac{\mathbf{D}S(N)}{N}$, и это значение обозначаем через σ_U^2 и σ_A^2 при гипотезах H_U и H_A соответственно.

Из несмещенности статистики $\hat{Q}$ и условий (5) находим

$$\mathbf{E}S(N) = N\vec{u}Qv^\downarrow = \begin{cases} 0 & \text{при гипотезе } H_U, \\ N\lambda_i^r & \text{при гипотезе } H_A. \end{cases} \quad (11)$$

Таким образом, слагаемые здесь являются оценками элемента спектра матрицы $Q \in \{\mathbb{U}, \mathbb{P}^r\}$; поэтому статистику $S(N)$ и основанный на ней критерий можно назвать *спектральными*.

Обозначим далее через $\Phi(x)$ функцию распределения стандартного нормального закона $N(0, 1)$, а через $\varkappa_\varepsilon$ квантили этого распределения, т. е. корни уравнения $\Phi(x) = \varepsilon$.

Выражения для среднего (11) и центральная предельная теорема (ЦПТ) позволяют описать поведение статистики $S(N)$ при больших N следующим образом. При гипотезе H_U с большой вероятностью значение $S(N)$ лежит в некоторой окрестности нуля, радиус которой определяется величиной σ_U . При гипотезе H_A с большой вероятностью $S(N)$ имеет знак, совпадающий со знаком λ_i^r .

Поэтому для заданного значения $\alpha \in (0, 1)$ будем исследовать односторонние критерии вида

$$S(N) \operatorname{sign}(\lambda_i^r) > \kappa_{1-\alpha} \sigma_U \sqrt{N} \implies H_A. \quad (12)$$

Таким образом, будем отвергать H_U , если модуль $S(N)$ значительно отклоняется от нуля в сторону математического ожидания, соответствующего альтернативе. Ниже в теореме 3 доказано, что при гипотезе H_U вероятность ошибки критерия (12) стремится к α при $N \rightarrow \infty$.

3. Расчет критерия

Будем обозначать через $\vec{u}^a := (u_1^a, \dots, u_M^a)$ вектор-строку, полученный возведением в степень a каждой компоненты вектора $\vec{u}$; степень вектор-столбца обозначаем $v^{\downarrow a}$. Тогда, в частности, $\vec{u}^2 1^{\downarrow} = |\vec{u}|^2$, $1 v^{\downarrow 2} = |\vec{v}|^2$.

Теорема 2. Пусть при условиях (1), (3) и (4) различающая пара векторов $\vec{u}, v^{\downarrow}$ удовлетворяет условию (5). Тогда при всех $N \geq 1$

$$\sigma_U^2 = |\vec{u}|^2 |\vec{v}|^2, \quad \sigma_A^2 = M \vec{u}^2 \mathbb{P}^r v^{\downarrow 2} - \lambda_i^{2r}.$$

Если пара имеет вид (8), то $\sigma_U^2 = 1$.

Доказательство. Из определения случайной величины ζ и соотношения $\mathbf{P}\{x=i, F(x)=j\} = M^{-1} \mathbf{P}\{F(i)=j\}$ имеем

$$\mathbf{E} \zeta^2 = M^2 \sum_{i,j \in X} \mathbf{P}\{x=i, F(x)=j\} u_i^2 v_j^2 = M \sum_{i,j \in X} u_i^2 Q_{ij} v_j^2 = M \vec{u}^2 Q v^{\downarrow 2}.$$

Отсюда с учетом (11) получаем указанное в теореме выражение для σ_A^2 .

Выражение для σ_U^2 находим подстановкой $Q = \mathbb{U}$ в крайнюю правую часть последнего равенства:

$$\sigma_U^2 = M \vec{u}^2 \frac{1}{M} 1^{\downarrow} 1 v^{\downarrow 2} = (\vec{u}^2 1^{\downarrow})(1 v^{\downarrow 2}) = |\vec{u}|^2 |\vec{v}|^2.$$

Для двух пар (8), построенных с использованием одного собственного вектора, имеем $|\vec{u}| = |\vec{v}|^{-1}$, и тогда $\sigma_U^2 = 1$. Теорема 2 доказана. $\square$

Замечания. 1) Из первого равенства в (5) следует, что в любой различающей паре оба вектора ненулевые, и $\sigma_U^2 > 0$ согласно теореме 2.

2) Если выполнено условие эргодичности (3) и M фиксировано, то матрица $\mathbb{P}^r$ при $r \rightarrow \infty$ сходится к $\mathbb{U}$, и $\sigma_A^2 \rightarrow \sigma_U^2$.

Обозначим через $\alpha_U(N)$ и $\alpha_A(N)$ вероятности ошибок критерия (12) при гипотезах H_U и H_A соответственно и получим для них асимптотические оценки.

Теорема 3. Пусть выполнены условия теоремы 2 и $N \rightarrow \infty$. Тогда $\alpha_U(N) = \alpha + O\left(\frac{1}{\sqrt{N}}\right)$, а если $\sigma_{\mathcal{A}}^2 > 0$, то

$$\alpha_{\mathcal{A}}(N) = \Phi\left(-\frac{\sqrt{N}|\lambda_i|^r - \varkappa_{1-\alpha}\sigma_U}{\sigma_{\mathcal{A}}}\right) + O\left(\frac{1}{\sqrt{N}}\right).$$

Доказательство. Согласно центральной предельной теореме для сумм независимых одинаково распределенных случайных величин, формуле (11) и теореме 2 при гипотезе H_U

$$\tilde{S}(N) = \frac{S(N)}{\sigma_U \sqrt{N}} \xrightarrow{D} N(0, 1), \quad N \rightarrow \infty.$$

Тогда с учетом равенства $\varkappa_{1-\alpha} = -\varkappa_{\alpha}$ имеем при $\lambda_i^r > 0$

$$\alpha_U(N) = \mathbf{P}\{\tilde{S}(N) > \varkappa_{1-\alpha}\} \rightarrow 1 - \Phi(\varkappa_{1-\alpha}) = \alpha.$$

При $\lambda_i^r < 0$ аналогично

$$\begin{aligned} \alpha_U(N) &= \mathbf{P}\{-\tilde{S}(N) > \varkappa_{1-\alpha}\} = \mathbf{P}\{\tilde{S}(N) < -\varkappa_{1-\alpha}\} = \\ &= \mathbf{P}\{\tilde{S}(N) < \varkappa_{\alpha}\} \rightarrow \Phi(\varkappa_{\alpha}) = \alpha. \end{aligned}$$

Оценивая остаточный член с помощью теоремы Берри–Эссеена [1, с. 449], получаем указанное в условии теоремы выражение для $\alpha_U(N)$.

2. Обозначая $\mu = \lambda_i^r$, при гипотезе $H_{\mathcal{A}}$ имеем $\tilde{S}(N) = \frac{S(N) - N\mu}{\sigma_{\mathcal{A}} \sqrt{N}} \xrightarrow{D} N(0, 1)$. Тогда в случае $\mu > 0$

$$\begin{aligned} \alpha_{\mathcal{A}}(N) &= \mathbf{P}\{S(N) \leq \varkappa_{1-\alpha}\sigma_U \sqrt{N}\} = \\ &= \mathbf{P}\left\{\tilde{S}(N) \leq \frac{1}{\sigma_{\mathcal{A}} \sqrt{N}}(\varkappa_{1-\alpha}\sqrt{N}\sigma_U - N\mu)\right\}, \end{aligned}$$

что отличается от $\Phi\left(-\frac{1}{\sigma_{\mathcal{A}}}(\sqrt{N}\mu - \varkappa_{1-\alpha}\sigma_U)\right)$ на величину $O(1/\sqrt{N})$, если $N \rightarrow \infty$. При $\mu < 0$ выкладки аналогичны. Теорема 3 доказана. $\square$

Заметим, что невыполнение условия $\sigma_{\mathcal{A}}^2 > 0$ теоремы означает, что при гипотезе $H_{\mathcal{A}}$ распределение ζ вырождено, и $S(N) = N\lambda_i^r$ с вероятностью 1. Тогда $\alpha_{\mathcal{A}}(N) = 0$ при всех таких N , что $\sqrt{N}|\lambda_i^r| > \varkappa_{1-\alpha}\sigma_U$.

Приравнивая первое слагаемое в выражении для $\alpha_{\mathcal{A}}(N)$ теоремы к $\beta \in (0, 1)$, получаем приближенную формулу для объема материала, достаточного для различения гипотез с заданными вероятностями ошибок:

$$N_1^*(\alpha, \beta, r) = \frac{(\varkappa_{1-\alpha}\sigma_U + \varkappa_{1-\beta}\sigma_{\mathcal{A}})^2}{|\lambda_i|^{2r}}.$$

Главным членом здесь является знаменатель, и с учетом замечания 2 к теореме 2 получаем, что значение $N_1^*(\cdot)$ увеличивается примерно в $|\lambda_i|^{-2}$ раз при увеличении r на 1.

В доказательстве теоремы 1 на основе левого и правого собственных векторов $\vec{B}_{s+1}$ и $C_2^\downarrow$ были построены две различающие пары (8), а при $l = 1$ также третья пара (9). Если $\vec{B}_{s+1}$ и $C_2^\downarrow$ параллельны, то все три критерия вида (12), соответствующие разным парам, совпадают, поскольку неравенства в них равносильны. В противном случае возникает вопрос: какая из пар предпочтительнее для использования?

Полученная формула для $N_1^*(\cdot)$ позволяет осуществить приближенную оптимизацию критериев по различающим парам. При достаточно больших r минимальное значение $N_1^*(\cdot)$ будет давать пара, соответствующая вещественному λ_i с наибольшим модулем. Ограничимся случаем, когда все имеющиеся пары соответствуют одному значению $|\lambda_i|$, и соответствующие j -й паре, $j \geq 1$, среднеквадратичные отклонения обозначим $\sigma_U^{(j)}$, $\sigma_A^{(j)}$. Тогда, например, 1-ю пару можно считать лучше 2-й при фиксированном r , если

$$\sigma_U^{(1)} < \sigma_U^{(2)}, \quad \sigma_A^{(1)} < \sigma_A^{(2)}, \quad (13)$$

поскольку для 1-й пары значение $N_1^*(\alpha, \beta, r)$ будет меньше, чем для 2-й, при всех α, β . Замечание 2 к теореме 2 указывает, что при условии эргодичности (3), как правило, неравенства в (13) выполнены или не выполнены одновременно при всех достаточно больших r .

4. Замечания

Вероятностные аспекты проблемы близости распределения итеративно получаемых случайных подстановок к равномерному распределению глубоко исследовались как в отечественной, так и в зарубежной литературе. В ряде случаев скорость сходимости распределения к равномерному оценивается величиной $O(\lambda_2^r)$, λ_2 — наибольшее по модулю собственное значение матрицы переходных вероятностей случайной подстановки. В нашей работе рассматривается статистический аспект данной проблемы, т. е. в некотором смысле обратная задача: при каком N возможно построение критерия, выявляющего с заданными вероятностями ошибок имеющуюся неравномерность распределения случайной подстановки? Предлагается строить критерий на основе наибольшего по модулю действительного собственного значения λ_i ($i = 2$, если $\lambda_2 \in \mathbb{R}$).

В криптографической литературе предлагался ряд критериев (атак различения) для подстановок, возникающих в блочных шифрсистемах. В основном они строились для конкретных криптосистем и их расчет, как правило, носил эвристический характер. Это вызвано сложностью случайных подстановок как объекта исследования и большой степенью $M = 2^n$, где $n \geq 32$ — длина блока. В нашей работе изучается вероятностная модель блочной шифрсистемы со случайным независимым выбором раундовых ключей и равновероятных входных блоков, рассматривавшаяся ранее в [6] и ряде других работ. Для предложенного критерия удастся получить строгие асимптотические оценки вероятностей ошибок и оценку объема материала порядка $|\lambda_i|^{-2r}$. Условие (1) применения критерия отличается от традиционных условий и фактически означает, что каждый входной блок шифруется на своем наборе случайно равновероятно выбираемых раундовых ключей. Это близко к ситуации, когда криптоаналитик наблюдает много коротких открытых сообщений и результатов их шифрования.

Главной проблемой для построения критерия становится поиск хотя бы одного собственного вектора стохастической матрицы, соответствующего выбранному собственному значению λ_i . Это известная алгебраическая *частичная проблема собственных значений*. Для ряда шифрсистем матрица переходных вероятностей разностей блоков является тензорным произведением [2, с. 10] и поэтому имеет много нулей. Для некоторых реальных масштабируемых SP-сетей при $n = 16$ матрицы размера $M = 2^{16} - 1$ имеют около 1% ненулевых элементов, что позволяет находить любое заданное число их собственных значений и векторов на персональных ЭВМ с помощью алгоритмов анализа разреженных матриц. Вопрос о сложности поиска одной собственной пары для таких матриц при больших n остается открытым.

Автор благодарен А. М. Зубкову за ряд полезных замечаний, способствовавших улучшению статьи.

Список литературы

- [1] Боровков А. А., *Теория вероятностей*, М.: Эдиториал УРСС, 1999, 472 с.
- [2] Глухов М. М., “О рассеивающих линейных преобразованиях для блочных шифрсистем”, *Матем. вопр. криптогр.*, **2**:2 (2011), 5–39.
- [3] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, **2**, М.: Гелиос АРВ, 2003, 416 с.
- [4] Ланкастер П., *Теория матриц*, М.: Наука, 1978, 280 с.
- [5] Минк Х., *Перманенты*, М.: Мир, 1982, 211 с.
- [6] Lai X., Massey J., Murphy S., “Markov ciphers and differential cryptanalysis”. In: “*EURO-CRYPT’91*”, Lect. Notes Comput. Sci., **547**, 1991, 17–38.