МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.23

СПЕКТРАЛЬНЫЙ ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКИЙ АНАЛИЗ МАРКОВСКИХ ШИФРОВ

О. В. Денисов

ООО «Инновационные телекоммуникационные технологии», г. Москва, Россия

Изучаются вероятностные модели блочных шифрсистем, в которых случайные раундовые ключи независимы и одинаково распределены. Они называются марковскими шифрами, если последовательность раундовых разностей образует простую однородную цепь Маркова. Описаны (при условиях доминирования второго собственного значения матрицы P вероятностей переходов разностей и одной координаты соответствующих собственных векторов) элементы и строки матриц P^R вероятностей переходов разностей за R раундов, наиболее удалённые от равновероятных значений при всех достаточно больших R. Предложенный в 2016 г. автором спектральный критерий для проверки гипотез о случайных подстановках применён для построения и расчёта атак различения в модели независимых двублочных текстов и в новой модели независимых полных кодовых книг.

Ключевые слова: *марковские блочные шифры, атака различения, спектр матриц, переходные вероятности разностей, второе доминирующее собственное значение, независимые полные кодовые книги.*

DOI 10.17223/20710410/53/2

SPECTRAL PROBABILISTIC AND STATISTICAL ANALYSIS OF MARKOV CIPHERS

O. V. Denisov

Innovative Telecommunication Technologies, LLC, Moscow, Russia

E-mail: denisovOleg@yandex.ru

Let an Abelian group $(\mathcal{X}, +)$ be the alphabet of R-round Markov block cipher with matrix P of transition probabilities of differentials; matrix size equals $M = |\mathcal{X}'|$, $\mathcal{X}' = \mathcal{X} \setminus \{0\}$. Suppose spectrum of P satisfies the condition $\lambda_1 = 1 > |\lambda_2| > |\lambda_3| \geqslant \geqslant \ldots \geqslant \lambda_M$.

1. Extremal transition probabilities $p_{ab}(R)$ and rows P^R for a large number of rounds. Let P be diagonalizable: $BPC = D = \operatorname{diag}(1, \lambda_2, \ldots, \lambda_M)$, $B = C^{-1}$, and there exist $a, b \in \mathcal{X}'$ such that $|C_{a2}| > |C_{i2}|$, $|B_{2b}| > |B_{jb}|$ for all $i \neq a$, $j \neq b$. Then $\arg\max\limits_{(i,j)\in\mathcal{X}'\times\mathcal{X}'} |p_{ij}(R) - \dfrac{1}{M}| = (a, b)$ and $\arg\max\limits_{i\in\mathcal{X}'} |\mathbf{P}_i^{(R)} - \dfrac{1}{M}\mathbf{1}| = a$ for all sufficiently large R, $p_{ab}(R) - \dfrac{1}{M} \sim C_{a2}B_{2b}\lambda_2^R$ and $|\mathbf{P}_a(R) - \dfrac{1}{M}\mathbf{1}| \sim |C_{a2}|\,|\mathbf{B}_2|\,|\lambda_2|^R$ as $R \to \infty$.

2. Distinguishing attack by independent full codebooks. Let the cipher with alphabet $\mathcal{X} = \mathbb{Z}_2^n$ be Markovian (provided random uniformly distributed set of round keys

$\mathbf{k} \sim U(\mathscr{K}^R)$) with matrix P, $z_i = z_i(\mathbf{k})$ be the result of block $i \in \mathcal{X}$ transformation either by cipher (hypothesis H_2) or random uniformly distributed substitution $z(\mathbf{k})$ (hypothesis H_1). Let (λ_2, u) or (λ_2, v) be left or right eigenpair of P, $|u| = |v| = 1$, $\mu_2(R) = \mathbf{u}P^R v^{\downarrow} \neq 0$, $S(\mathbf{k}) = M \sum\limits_{\{i,j\} \subset \mathcal{X}} u_{j-i} v_{z_j - z_i}$. We prove that mean and variance of statistic $S(\mathbf{k})$ equal 0 and $M^2 \dfrac{M+1}{2(M-2)}$ respectively under hypothesis H_1. If sets $\mathbf{k}(1), \ldots, \mathbf{k}(N_b) \sim U(\mathscr{K}^R)$ are independent, $N_b \to \infty$, then for all $0 < \alpha < 1$ criterion $d:\ S'(N_b)\ \mathrm{sign}(\mu_2(R)) > \varkappa_{1-\alpha} \sqrt{\dfrac{NM}{M-2}} \Longrightarrow H_2$, where $N = \dbinom{M+1}{2} N_b$, has error probability $\alpha_1(d) \to \alpha$. We show that $\alpha_2(d) \approx \beta$ for large values of R and $N_b \approx \dfrac{2(\varkappa_{1-\alpha} + \varkappa_{1-\beta})^2}{(2^n \mu_2(R))^2}$.

Keywords: *Markov block ciphers, distinguishing attack, matrix spectrum, transition probabilities of differentials, second dominant eigenvalue, independent full codebooks.*

Введение

Пусть $\mathcal{X}$ — входной и выходной алфавит блочного шифра, $(\mathcal{X}, +)$ — абелева группа с нейтральным элементом 0. Как принято в дифференциальном (разностном) анализе, величины вида $x^* - x$ будем называть *разностями* блоков $x, x^* \in \mathcal{X}$. Через $\mathcal{X}' = \mathcal{X} \setminus \{0\}$ обозначим множество ненулевых блоков, $M = |\mathcal{X}| - 1$ — его мощность, через $S(\mathcal{X})$ — множество всех подстановок на множестве $\mathcal{X}$.

Рассмотрим итеративный R-раундовый шифр, в котором промежуточные раундовые блоки формируются по правилу

$$x^r = f(x^{r-1}, k^r), \quad 1 \leqslant r \leqslant R,$$

где $x = x^0 \in \mathcal{X}$ — входной блок; k^r — ключ r-го раунда из некоторого множества $\mathscr{K}$ раундовых ключей; f — функция шифрования на одном раунде; $y = x^R \in \mathcal{X}$ — выходной блок.

Рассмотрим также вероятностную модель шифрования, в которой шифруется случайно выбираемый двублочный открытый текст $(X, X^*) \in \mathcal{X}^2$, случайно выбираемые раундовые ключи $K^1, \ldots, K^R \in \mathscr{K}$ не зависят от текста, независимы между собой и одинаково распределены. Заглавные буквы здесь и далее обозначают случайные блоки и ключи.

Тогда последовательность (X^r, X^{*r}), $r = 0, \ldots, R$, пар раундовых блоков является простой однородной цепью Маркова (далее рассматриваем только такие цепи). Но не всякая функция от последовательности состояний цепи Маркова (и, в частности, разность компонент пар) образует цепь Маркова. Поэтому содержательно следующее определение [1 – 3]: введённая модель шифрования называется *марковским шифром* (относительно операции + при заданных распределениях входной пары (X, X^*) и раундового ключа K^1), если последовательность случайных *раундовых разностей*

$$\Delta X = X^* - X,\ \Delta X^1 = X^{*1} - X(1),\ \ldots,\ \Delta Y = \Delta X^R = X^{*R} - X^R \tag{1}$$

образует цепь Маркова.

Известно [1; 3, теорема 1], что матрица P вероятностей переходов такой цепи является дважды стохастической. Поэтому цепь не имеет несущественных состояний [4]. Будем считать, что цепь Маркова (1) является эргодической, т. е. имеет один класс существенных состояний, и он ациклический. Такое предположение практически всегда

выполнено, поскольку в противном случае матрица $\|p_{ij}(R)\|_{i,j\in\mathcal{X}'} = P^R$ вероятностей переходов за R раундов содержит нули для любого $R \geqslant 1$. Тогда в силу дважды стохастичности

$$\lim_{R\to\infty} P^R = \mathbb{U},$$

где $\mathbb{U} = \dfrac{1}{M} 1^{\downarrow}\mathbf{1}$ — *равномерная матрица* размера M; $\mathbf{1}$ и $1^{\downarrow}$ — вектор-строка и вектор-столбец, состоящие из всех единиц.

Для матрицы A строку с номером i, столбец с номером j и элемент на месте i, j будем обозначать $\mathbf{A}_i$, $A_j^{\downarrow}$ и A_{ij} соответственно. Единичной матрицей будем называть матрицу, являющуюся нейтральным элементом относительно умножения:

$$E = \operatorname{diag}(1, \ldots, 1) = \sum_{1\leqslant i\leqslant M} E_{i,i}.$$

Через $E_{i,j} = e_i^{\downarrow}\mathbf{e}_j$ обозначаем матрицу, единственный ненулевой элемент которой равен 1 и находится на месте i, j; e_k — k-й вектор стандартного базиса $\mathbb{R}^M$. Для вектора $\mathbf{u}$ будем обозначать через $|\mathbf{u}|$ его евклидову норму.

Пусть $\lambda_1 = 1, \lambda_2, \ldots, \lambda_M \in \mathbb{C}$ — *спектр* матрицы переходных вероятностей разностей (МПВР) P, т. е. набор всех её различных собственных чисел (комплексных корней её характеристического многочлена) с учётом их кратностей. Известно [5, с. 266], что спектральный радиус стохастической матрицы равен 1. Поэтому можем считать, что

$$\lambda_1 = 1 \geqslant |\lambda_2| \geqslant \ldots \geqslant |\lambda_M|.$$

Тогда с учётом отсутствия несущественных состояний предположение об эргодичности цепи эквивалентно [6, теорема 6] тому, что кратность корня 1 равна 1, т. е. $1 > |\lambda_2|$.

В п. 1 рассматривается ситуация диагонализуемой матрицы P при условиях доминирования собственного значения λ_2 над остальными и модуля одной из компонент левого и правого собственных векторов (соответствующих значению λ_2) над остальными. Доказано, что тогда для всех достаточно больших R наибольшее значение отклонения от $1/M$ имеет элемент матрицы, координаты которого соответствуют компонентам $\mathbf{B}_2$, $C_2^{\downarrow}$ с наибольшими модулями; для значения отклонения получена асимптотическая формула. Аналогичный результат получен для строк матрицы P^R, наиболее удалённых от равномерного распределения.

В п. 2 и 3 изучаются спектральные атаки различения в двух моделях наблюдений. *Атакой различения на R раундов* шифрсистемы называют статистический критерий для проверки гипотезы H_2 о том, что при шифровании применялись R раундов данной шифрсистемы, против гипотезы H_1 о том, что использовалась случайная подстановка. Для марковских шифров традиционно считается, что МПВР Q равна $\mathbb{U}$ при гипотезе H_1 и P^R — при H_2. Но при шифровании случайно выбранной пары блоков (X, X^*) на фиксированном наборе $\mathbf{k} = (k^1, \ldots, k^R)$ раундовых ключей последовательность (1) раундовых разностей не образует цепь Маркова в общем случае, и МПВР за R раундов не равна P^R. Поэтому возникает вопрос о существовании модели наблюдений, в которой разностная атака различения будет приводить в точности к такой статистической модели.

Автором в [7] предложена такая модель наблюдений — независимые «двублочные тексты». Условия модели отличаются от традиционных и фактически означают, что при гипотезе H_2 каждая пара входных блоков шифруется на своём случайно выбираемом ключе $\mathbf{K}$, а при H_1 — на своей случайно равновероятно выбираемой подстановке.

Это близко к ситуации, когда криптоаналитик наблюдает много коротких открытых сообщений и результатов их шифрования. Тогда непосредственно с помощью атаки различения может проверяться гипотеза о том, что шифрование осуществляется заданной системой. В этой модели без использования эвристических предположений получены оценки вероятностей ошибок атак различения, основанных на разностных и мультиразностных статистиках. В частности, для ситуации фиксированной входной разности и сближения гипотез рассчитаны асимптотические вероятности ошибок критерия отношения правдоподобий [8], основанного на частотах всех выходных разностей.

В п. 2 в модели независимых двублочных текстов со случайной ненулевой равновероятной входной разностью на основе [4] построен спектральный критерий. В п. 3 введена вторая модель наблюдений, развивающая модель [8], — случайные полные кодовые книги, в которой также построена и рассчитана аналогичная атака.

1. Экстремальные вероятности переходов за большое число раундов

Одной из важных задач классического разностного анализа является поиск *экстремальных вероятностей*, под которыми будем понимать вероятности с наибольшим отклонением $|p_{ij}(R) - 1/M|$. При небольших R оно достигается обычно на элементах с максимальным значением $p_{ij}(R)$, для поиска которых в криптографической литературе предлагаются в основном эвристические алгоритмы. Мы будем использовать методы спектрального матричного анализа [5] для описания поведения таких вероятностей, предполагая для простоты, что P диагонализуема над $\mathbb{C}$, т. е. существует такая невырожденная матрица C, что

$$BPC = D = \operatorname{diag}(1, \lambda_2, \ldots, \lambda_M), \quad B = C^{-1}. \tag{2}$$

Усилим условие эргодичности цепи условием доминирования собственного значения λ_2:

$$\lambda_1 = 1 > |\lambda_2| > |\lambda_3| \tag{3}$$

и введём условия доминирования модуля одной компоненты собственных векторов $C_2^{\downarrow}$ и $\mathbf{B}_2$ матрицы P, соответствующих λ_2:

$$\exists a \in \mathcal{X}' \, \forall i \neq a \; (|C_{a2}| > |C_{i2}|); \tag{4}$$

$$\exists b \in \mathcal{X}' \, \forall j \neq b \; (|B_{2b}| > |B_{jb}|). \tag{5}$$

Из условия (3) вытекает, в частности, что спектр не содержит числа, сопряжённого к λ_2, поэтому λ_2 вещественно, как и соответствующие ему собственные векторы $\mathbf{B}_2$, $C_2^{\downarrow}$.

Теорема 1. Пусть выполнены условие (2) диагонализуемости МПВР P и условие (3) доминирования $\lambda_{1,2}$. Тогда существуют такие R_0, R_1, что:

1) при условиях (4) и (5) доминирования модуля одной компоненты

$$\operatorname*{arg\,max}_{(i,j)\in\mathcal{X}'\times\mathcal{X}'} \left| p_{ij}(R) - \frac{1}{M} \right| = (a, b), \quad R \geqslant R_0,$$

$$p_{ab}(R) - \frac{1}{M} \sim C_{a2} B_{2b} \lambda_2^R, \quad R \to \infty; \tag{6}$$

2) при условии (4) для строк $\mathbf{P}_i^{(R)}$ матрицы P^R имеем

$$\arg\max_{i\in\mathcal{X}'}\left|\mathbf{P}_i^{(R)}-\frac{1}{M}\mathbf{1}\right|=a,\quad R\geqslant R_1,$$
$$\left|\mathbf{P}_a^{(R)}-\frac{1}{M}\mathbf{1}\right|\sim|C_{a2}|\,|\mathbf{B}_2|\,|\lambda_2|^R,\quad R\to\infty. \tag{7}$$

Доказательство. В силу равенств $PC=CD$ и $BP=DB$, $D=\operatorname{diag}(\cdot)$, векторы $C_i^{\downarrow}$ и $\mathbf{B}_i$ — собственные, соответствующие λ_i. При $i=1,2$ эти векторы определены однозначно с точностью до мультипликативной константы, поскольку алгебраическая и геометрическая кратности собственных значений λ_1, λ_2 равны 1. С учётом дважды стохастичности матрицы это означает, что $C_1^{\downarrow}$ и $\mathbf{B}_1$ параллельны вектору $1^{\downarrow}$.

Условие $BC=E$ равносильно тому, что $\mathbf{B}_iC_j^{\downarrow}=\mathbb{I}\{i=j\}$, $i,j\in\mathcal{X}'$. Оно сохранится, если одновременно любую строку $\mathbf{B}_i$ умножить, а столбец $C_i^{\downarrow}$ с тем же номером разделить на произвольное число $\lambda\neq0$. Поэтому без ограничения общности считаем, что $(C_1^{\downarrow})^{\top}=\mathbf{B}_1=\dfrac{1}{\sqrt{M}}\mathbf{1}$. Тогда, согласно теореме [5, с. 64] о спектральном разложении, получаем

$$P^R=CD^RB=\sum_{1\leqslant k\leqslant M}\lambda_k^RC_k^{\downarrow}\mathbf{B}_k=\mathbb{U}+\lambda_2^RG_2+\ldots+\lambda_M^RG_M,\ G_k=C_k^{\downarrow}\mathbf{B}_k. \tag{8}$$

1. Докажем сначала формулу (6). Из (8) для всех $i,j\in\mathcal{X}'$ находим

$$p_{ij}(R)=\mathbf{e}_iP^Re_j^{\downarrow}=\sum_{1\leqslant k\leqslant M}\lambda_k^RC_{ik}B_{kj}=\frac{1}{M}+\lambda_2^R\big(C_{i2}B_{2j}+\varepsilon_{ij}(R)\big),$$
$$\text{где}\quad\varepsilon_{ij}(R)=\sum_{3\leqslant k\leqslant M}C_{ik}B_{kj}(\lambda_k/\lambda_2)^R,$$

и $|\varepsilon_{ij}(R)|\leqslant|\lambda_3/\lambda_2|^R\sum\limits_{3\leqslant k\leqslant M}|C_{ik}B_{kj}|\to0$ при $R\to\infty$. Поэтому $\left(p_{ab}(R)-1/M\right)/\lambda_2^R\to$ $\to C_{a2}B_{2b}\neq0$, что равносильно (6).

Из полученных асимптотических представлений и условий (4), (5) следует, что при всех $(i,j)\neq(a,b)$

$$\left|\frac{p_{ij}(R)-1/M}{p_{ab}(R)-1/M}\right|=\left|\frac{C_{i2}B_{2j}+\varepsilon_{ij}(R)}{C_{a2}B_{2b}+\varepsilon_{ab}(R)}\right|\to\left|\frac{C_{i2}}{C_{a2}}\right|\left|\frac{B_{2j}}{B_{2b}}\right|<1,$$

поэтому, начиная с некоторого R_0, модуль числителя меньше модуля знаменателя.

2. Пункт 2 доказывается аналогично; установим сначала формулу (7). Из (8) для всех $i\in\mathcal{X}'$ находим

$$\mathbf{P}_i^{(R)}=\mathbf{e}_iP^R=\sum_{1\leqslant k\leqslant M}\lambda_k^RC_{ik}\mathbf{B}_k=\frac{1}{M}\mathbf{1}+\lambda_2^R\big(C_{i2}\mathbf{B}_2+\varepsilon_i(R)\big),$$
$$\text{где}\quad\varepsilon_i(R)=(\varepsilon_{ij}(R),j\in\mathcal{X}')=\sum_{3\leqslant k\leqslant M}C_{ik}\mathbf{B}_k(\lambda_k/\lambda_2)^R,$$

и при $R\to\infty$

$$|\varepsilon_i(R)|\leqslant|\lambda_3/\lambda_2|^R\sum_{3\leqslant k\leqslant M}|C_{ik}||\mathbf{B}_k|\to0.$$

Здесь для последовательности векторов $\mathbf{u}(R)$ пишем $\mathbf{u}(R)=o(1)$, если $|\mathbf{u}(R)|=o(1)$. Так как

$$\big||\mathbf{u}+o(1)|-|\mathbf{u}|\big|\leqslant|\mathbf{u}+o(1)-\mathbf{u}|=o(1),$$

то $|\mathbf{u}+o(1)|=|\mathbf{u}|+o(1)$, и тогда

$$\left|\mathbf{P}_a^{(R)}-\frac{1}{M}\mathbf{1}\right|=|\lambda_2|^R(|C_{a2}|\,|\mathbf{B}_2|+o(1)),$$

что с учётом неравенства $|C_{a2}|\,|\mathbf{B}_2|>0$ равносильно (7).

Отсюда и из условия (4) следует, что при всех $i\neq a$

$$\frac{\left|\mathbf{P}_i^{(R)}-\frac{1}{M}\mathbf{1}\right|}{\left|\mathbf{P}_a^{(R)}-\frac{1}{M}\mathbf{1}\right|}=\frac{|C_{i2}\mathbf{B}_2+o(1)|}{|C_{a2}\mathbf{B}_2+o(1)|}\to\frac{|C_{i2}|\,|\mathbf{B}_2|}{|C_{a2}|\,|\mathbf{B}_2|}<1,$$

поэтому, начиная с некоторого R_1, модуль числителя меньше модуля знаменателя.

Теорема 1 доказана. ■

Фактически теорема 1 даёт условия, достаточные для единственности наиболее неравномерного элемента (соответственно строки) матрицы P^R при росте R, а также для возникновения *эффекта стабилизации позиции* таких элемента и строки. Из п. 1 теоремы 1 легко получить следующие достаточные условия стабилизации позиции максимальных элементов P^R.

Следствие 1. Пусть выполнены условия (2)–(5) и ограничение

$$(C_{a2}B_{2b}>0 \text{ при } \lambda_2>0) \text{ либо } \left((-1)^R=\operatorname{sign}(C_{a2}B_{2b}) \text{ при } \lambda_2<0\right).$$

Тогда элемент $p_{ab}(R)$ — максимальный в матрице P^R для всех достаточно больших R.

Доказательство. Из доказательства п. 1 теоремы 1 следует, что $\operatorname{sign}(p_{ab}(R)-1/M)=\operatorname{sign}(C_{a2}B_{2b}\lambda_2^R)$ для всех достаточно больших R. При каждом из условий ограничения этот знак равен 1, поэтому с учётом доказательства п. 1 теоремы 1

$$p_{ab}(R)-1/M=|p_{ab}(R)-1/M|>|p_{ij}(R)-1/M|\geqslant p_{ij}(R)-1/M$$

для всех $(i,j)\neq(a,b)$. ■

Возможно, условие (2) диагонализуемости в теореме 1 можно ослабить, преодолевая возникающие при этом трудности с помощью более общих блочно-диагональных матричных представлений типа [9, с. 184] и аппарата матричных норм.

Условие (3) доминирования λ_2 представляется в этом смысле более существенным: при отказе от него может появиться, например, сопряжённая доминирующая пара $|\lambda_{2,3}|>\lambda_4$, которая даст осцилляцию множеств координат с экстремальными значениями. Простейшим примером этого является циркулянт $P=T=\left(\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right)$ — дважды стохастическая матрица, соответствующая полноцикловой подстановке. Как известно [5, с. 245], его спектр совпадает с группой Γ_n корней из 1 степени n. Здесь $n=3$ и спектр $\operatorname{sp}(T)=\{1,\gamma,\gamma^*\}$, $\gamma=e^{2\pi i/3}$. Так как $T^2=\left(\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right)$, $T^3=E$, то при нумерации позиций в матрице элементами группы вычетов $(\mathbb{Z}_n,\oplus)$ получаем

$$p_{ij}(R)-\frac{1}{3}=\begin{cases}2/3 & \text{при } j\equiv i\oplus R \pmod 3,\\ -1/3 & \text{иначе.}\end{cases}$$

Таким образом, соответствующая экстремальным позициям трансверсаль будет изменяться периодически с периодом 3.

Развивая эту идею, построим пример, в котором соответствующая матрице цепь Маркова будет эргодической.

Пример 1. При произвольном n элементы циркулянта, соответствующего вектору $(a_0,\dots,a_{n-1})$, задаются равенством $p_{ij}=a_{j\ominus i}$, $i,j\in\mathbb{Z}_n$, $\ominus$ — вычитание по модулю n. Рассмотрим параметрическое семейство дважды стохастических матриц $P(p)$ — циркулянтов вектора $(p,1-p,0,\dots,0)$, $0\leqslant p\leqslant 1$.

Заметим, что $P(p)=pE+(1-p)T$ — многочлен от циркулянта T, соответствующего полноцикловой подстановке. Спектр матрицы $P(p)$ есть результат применения этого многочлена к спектру T [5, с. 245], поэтому состоит из чисел $z_k(p)=p+(1-p)\gamma^k$, $k\in\mathbb{Z}_n$, $\gamma=e^{2\pi i/n}$. Числу $z_k(p)$ соответствует правый собственный вектор $v_k=(\gamma^{jk}\big|\, j\in\mathbb{Z}_n)$ и левый $v_k^*=v_{n-1-k}$, $k\in\mathbb{Z}_n$. Следовательно, $G_{k+1}=\dfrac{1}{\sqrt{n}}v_k^{\downarrow}\dfrac{1}{\sqrt{n}}\mathbf{v}_k^*$ в разложении (8).

Геометрически описать изменение спектра можно так: при $p=0$ спектр $\operatorname{sp}(P(0))=\operatorname{sp}(T)=\Gamma_n$ является правильным многоугольником, вписанным в единичную окружность. Так как равенства

$$z_k(p)-1=(1-p)(\gamma^k-1),\ k\in\mathbb{Z}_n,\ 0\leqslant p\leqslant 1,$$

означают гомотетию с центром в вершине $z_0(p)=1=\lambda_1$ и коэффициентом подобия $1-p$ (векторы, соединяющие 1 и $z_k(p)$, пропорциональны векторам, соединяющим 1 и γ^k), то при увеличении p этот многоугольник уменьшается (длина сторон равна $(1-p)|\gamma-1|$), оставаясь подобным исходному, и при $p=1$ вырождается в точку 1. Таким образом, при $0<p<1$ все точки, кроме λ_1, лежат внутри единичного круга, $|\lambda_2|<1$, поэтому цепь эргодическая [6, теорема 6].

При $n=3$ найдем p, при котором сопряжённая пара будет лежать на мнимой оси. Из условия $\operatorname{Re}z_1(p)=p+(1-p)\cos(2\pi/3)=0$ получаем $p=1/3$, $P=\frac{1}{3}\left(\begin{smallmatrix}1&2&0\\0&1&2\\2&0&1\end{smallmatrix}\right)$, $\lambda_{2,3}=\pm i/\sqrt{3}$.

Так как здесь

$$G_2=\frac{1}{\sqrt{3}}v_1^{\downarrow}\frac{1}{\sqrt{3}}\mathbf{v}_2=\frac{1}{3}\begin{pmatrix}1\\ \gamma\\ \gamma^2\end{pmatrix}\begin{pmatrix}1 & \gamma^2 & \gamma\end{pmatrix}=\frac{1}{3}\begin{pmatrix}1 & \gamma^2 & \gamma\\ \gamma & 1 & \gamma^2\\ \gamma^2 & \gamma & 1\end{pmatrix}$$

и $G_3=\dfrac{1}{3}v_2^{\downarrow}\mathbf{v}_1=G_2^*$, то, согласно разложению (8),

$$P^R-\mathbb{U}=\lambda_2^RG_2+\lambda_3^RG_3=\lambda_2^RG_2+(\lambda_2^*)^RG_2^*=2\operatorname{Re}(\lambda_2^RG_2)=\frac{2}{3^{R/2}}\operatorname{Re}(i^RG_2).$$

Итак, конфигурация мест максимальных элементов P^R будет изменяться периодически с периодом 4, а экстремальных — с периодом 2. Действительно, это наименьшие периоды последовательностей $\operatorname{Re}(i^Rz)$, $0\neq z\in\mathbb{C}$, и $|\operatorname{Re}(i^Rz)|$, $\arg z\notin\{\pm\pi/4,\pm3\pi/4\}$, $R=1,2,\dots$ Поэтому эффекты стабилизации позиций максимальных и экстремальных элементов здесь отсутствуют.

2. Спектральные атаки различения на марковские шифры по двублочным текстам

2.1. Несмещённая оценка МПВР и билинейная функция от неё

Наблюдаются входные разности $\Delta X(t)=X^*(t)-X(t)$ случайных независимых двублочных открытых текстов $(X(t),X^*(t))$ и выходные разности $\Delta Y(t)=Y^*(t)-Y(t)$ соответствующих им шифртекстов $(Y(t),Y^*(t))$, причём

$$\text{пары } (X(t),X^*(t)) \text{ независимы},\ \Delta X(t)\sim U(\mathcal{X}'),\ 1\leqslant t\leqslant N, \tag{9}$$

т. е. разности $\Delta X(1), \ldots, \Delta X(N)$ независимы и равномерно распределены на $\mathcal{X}'$.

Гипотеза H_1 заключается в том, что шифртексты получены в результате применения подстановок, выбираемых независимо равновероятно из $S(\mathcal{X})$. Гипотеза H_2 заключается в том, что шифртексты получены R-раундовым применением марковского шифра с дважды стохастической МПВ ненулевых разностей P за 1 раунд. Обозначим через Q матрицу вероятностей переходов цепи из раундовых разностей за R шагов, и тогда задача сводится к построению критерия для проверки гипотезы $Q = \mathbb{U}$ против гипотезы $Q = P^R$. Такая постановка соответствует условиям работы [4], и можно воспользоваться построенным в ней спектральным критерием. Далее через P_i, E_i, D_i, $\alpha_i(N)$ обозначаем соответственно вероятностное распределение, математическое ожидание и дисперсию статистик, вероятности ошибок критериев при гипотезе H_i, $i = 1, 2$.

Рассмотрим матричнозначную статистику

$$\hat{Q} = \frac{M}{N} \sum_{1 \leqslant t \leqslant N} E_{\Delta X(t), \Delta Y(t)}.$$

Согласно модели наблюдений (9), она является суммой независимых одинаково распределённых как случайная матрица $E_{x,y}$ матриц, где распределение случайной пары (x, y) задаётся условием

$$x \sim U(\mathcal{X}'),\ \mathsf{P}\{y = j \mid x = i\} = Q_{ij}. \tag{10}$$

Поэтому математическое ожидание статистики равно

$$\mathsf{E}\hat{Q} = M\mathsf{E}E_{x,y} = M\|\,\mathsf{P}\{x = i, y = j\}\|_{i,j \in \mathcal{X}'} = M\|\,\mathsf{P}\{x = i\}Q_{ij}\|_{i,j \in \mathcal{X}'} = Q,$$

то есть $\hat{Q}$ является несмещённой оценкой для Q при каждой гипотезе.

На основе принципа биортогональности [9] проще докажем следующее обобщение теоремы 1 [4].

Лемма 1. Пусть P — дважды стохастическая матрица размера M, $u, v \in \mathbb{R}^M$ — векторы длины 1. Тогда:

1) если (λ, u) или (λ, v) — собственная пара P, $\lambda \neq 1$, то $\mathbf{u}\,\mathbb{U}v^{\downarrow} = 0$;
2) если (λ, u) — левая или (λ, v) — правая собственная пара P, то $\mathbf{u}P^R v^{\downarrow} = \lambda^R \cos(u, v)$;
3) если u, v — левый и правый собственные векторы для значения λ кратности 1, то $\cos(u, v) \neq 0$.

Доказательство.

1) Пусть v — правый собственный вектор (ситуации, когда v — левый собственный или u — собственный, рассматриваются аналогично). Напомним *принцип биортогональности* [9, с. 78]: если $(\lambda_i, \mathbf{x})$ и $(\lambda_j, v^{\downarrow})$ — собственные пары вещественной матрицы A и $\lambda_i \neq \lambda_j$, то $x \perp v$. Действительно, вычитая из равенства $(\mathbf{x}A)v^{\downarrow} = \lambda_i \mathbf{x}v^{\downarrow}$ равенство $\mathbf{x}(Av^{\downarrow}) = \mathbf{x}\lambda_j v^{\downarrow}$, получаем $(\lambda_i - \lambda_j)\langle x, v\rangle = 0$, откуда $\langle x, v\rangle = 0$.

Осталось заметить, что из дважды стохастичности P следует $\mathbf{1}P = \mathbf{1}$, т. е. $(1, \mathbf{1})$ — собственная пара, $\lambda_1 = 1 \neq \lambda$, поэтому

$$\langle \mathbf{1}, \mathbf{v}\rangle = 0, \quad \mathbb{U}v^{\downarrow} = \tfrac{1}{M}1^{\downarrow}\mathbf{1}v^{\downarrow} = \tfrac{1}{M}1^{\downarrow}0 = 0^{\downarrow}.$$

2) Пусть v — правый собственный вектор (ситуация, когда u — левый собственный, рассматривается аналогично). Из определения собственного вектора получаем

$$\mathbf{u}(P^R v^{\downarrow}) = \mathbf{u}\lambda^R v^{\downarrow} = \lambda^R \langle u, v\rangle.$$

Заметим, что $\langle u, v\rangle = \cos(u, v)$ согласно условиям нормированности векторов.

3) Если u, v — левый и правый собственные, соответствующие простому значению λ, то $\langle u, v\rangle \neq 0$ по лемме о неортогональности [9, с. 412].

Лемма 1 доказана. ■

Пусть $\lambda \in \mathbb{R} \setminus \{0, 1\}$ — вещественное собственное значение P. Зафиксируем произвольно пару векторов $(u, v) \in \mathbb{R}^M$, удовлетворяющую условиям п. 1 леммы 1. Она определяет скалярную статистику

$$S(N) = N\mathbf{u}\hat{Q}v^{\downarrow} = N\mathbf{u}\left(\frac{M}{N}\sum_{1\leqslant t\leqslant N} E_{\Delta X(t),\Delta Y(t)}\right)v^{\downarrow} = M\sum_{1\leqslant t\leqslant N} u_{\Delta X(t)}v_{\Delta Y(t)}. \tag{11}$$

Согласно модели наблюдений (9), $S(N)$ — сумма независимых случайных величин, имеющих такое же распределение, как случайная величина

$$\tau = Mu_x v_y,$$

где распределение (x, y) задано условием (10). Из несмещённости статистики $\hat{Q}$ и п. 1 леммы 1 с учётом марковости шифра находим

$$\mathsf{E}S(N) = N\mathbf{u}Qv^{\downarrow} = \begin{cases} 0 & \text{при } H_1, \\ N\mu_2(R) & \text{при } H_2, \text{ где } \mu_2(R) = \mathbf{u}P^R v^{\downarrow}. \end{cases} \tag{12}$$

Далее считаем $\mu_2(R) \neq 0$. Это выполнено, например, при условии п. 3 леммы 1.

2.2. Критерий и его расчёт

Из (11) и (12) следует, что $\mathsf{E}_i\tau = \mathbb{I}\{i = 2\}\mu_2(R)$, $i = 1, 2$. Дисперсия случайной величины τ в силу независимости слагаемых в правой части (11) равна $\mathsf{D}_i S(N)/N$ при гипотезе H_i, это значение обозначим через σ_i^2, $i = 1, 2$. Выражения (12) для среднего и центральная предельная теорема позволяют описать поведение статистики $S(N)$ при больших N следующим образом. При гипотезе H_1 с большой вероятностью значение $S(N)$ лежит в некоторой окрестности нуля, радиус которой определяется величиной σ_1. При гипотезе H_2 с большой вероятностью $S(N)$ имеет знак, совпадающий со знаком величины $\mu_2(R)$. Поэтому для заданного значения $\alpha \in (0, 1)$ рассматриваем односторонние критерии вида

$$d: \; S(N)\,\operatorname{sign}(\mu_2(R)) > \varkappa_{1-\alpha}\sqrt{N} \Longrightarrow H_2. \tag{13}$$

Здесь и далее $\varkappa_\gamma$ — квантиль уровня γ стандартного нормального распределения $\mathcal{N}(0, 1)$.

Будем обозначать через $v^2 = (v_1^2, \ldots, v_M^2)$ векторы, полученные возведением в квадрат каждой компоненты исходного вектора. С учётом леммы 1 аналогично теоремам 2 и 3 из [4] доказывается следующая

Теорема 2. Пусть в модели наблюдений (9) при гипотезе H_2 шифр является марковским с МПВР P,

$$\begin{gathered} (\lambda_2, u) \text{ или } (\lambda_2, v) \text{ — собственная пара } P, \\ \lambda_2 \in \mathbb{R},\ |\lambda_2| \neq 0, 1,\ |u| = |v| = 1,\ \mu_2(R) = \mathbf{u}P^R v^{\downarrow} \neq 0. \end{gathered} \tag{14}$$

Тогда:

1) $\sigma_1^2 = 1,\ \sigma_2^2(R) = M\mathbf{u}^2 P^R v^{2\downarrow} - \mu_2^2(R)$;
2) при $N \to \infty$ критерий (13) имеет асимптотический размер α и

$$\alpha_2(d) = \Phi\left(-\frac{\sqrt{N}|\mu_2(R)| - \varkappa_{1-\alpha}}{\sigma_2(R)}\right) + O\left(\frac{1}{\sqrt{N}}\right).$$

Доказательство.

1) При обеих гипотезах из равенства $\mathsf{P}\{x = i, y = j\} = \dfrac{1}{M}Q_{ij}$ имеем

$$\mathsf{E}\tau^2 = M^2\mathsf{E}(u_x v_y)^2 = M^2 \sum_{i,j\in\mathcal{X}'} \mathsf{P}\{x = i, y = j\} u_i^2 v_j^2 = M \sum_{i,j\in\mathcal{X}'} u_i^2 Q_{ij} v_j^2 = M\mathbf{u}^2 Q v^{2\downarrow}.$$

Отсюда с учётом (12) получаем $\sigma_2^2 = \mathsf{E}\tau^2 - \mu^2$, как и указано в теореме, $\mu = \mu_2(R)$.

При H_1 подставляем $Q = \mathbb{U}$:

$$\sigma_1^2 = M\mathbf{u}^2 \frac{1}{M} 1^{\downarrow}\mathbf{1}v^{2\downarrow} = (\mathbf{u}^2 1^{\downarrow})(\mathbf{1}v^{2\downarrow}) = |u|^2\,|v|^2 = 1.$$

2) При гипотезе H_1, согласно центральной предельной теореме для сумм независимых одинаково распределенных случайных величин, с учётом (12) и равенства $\sigma_1^2 = 1$ имеем

$$\tilde{S}(N) = \frac{S(N)}{\sqrt{N}} \xrightarrow{w} \mathcal{N}(0,1), \quad N \to \infty.$$

Тогда с учётом равенства $\varkappa_{1-\alpha} = -\varkappa_\alpha$ при $\mu > 0$

$$\alpha_1(d) = \mathsf{P}_1\{\tilde{S}(N) > \varkappa_{1-\alpha}\} \to 1 - \Phi(\varkappa_{1-\alpha}) = \alpha.$$

При $\mu < 0$ аналогично

$$\alpha_1(d) = \mathsf{P}_1\{-\tilde{S}(N) > \varkappa_{1-\alpha}\} = \mathsf{P}_1\{\tilde{S}(N) < -\varkappa_{1-\alpha}\} = \mathsf{P}_1\{\tilde{S}(N) < \varkappa_\alpha\} \to \Phi(\varkappa_\alpha) = \alpha.$$

При гипотезе H_2 имеем $\tilde{S}(N) = \dfrac{S(N) - N\mu}{\sigma_2\sqrt{N}} \xrightarrow{w} \mathcal{N}(0,1)$. Тогда в случае $\mu > 0$

$$\alpha_2(d) = \mathsf{P}_2\{S(N) \leqslant \varkappa_{1-\alpha}\sqrt{N}\} = \mathsf{P}_2\left\{\tilde{S}(N) \leqslant \frac{1}{\sigma_2\sqrt{N}}\left(\varkappa_{1-\alpha}\sqrt{N}\sigma_2 - N\mu\right)\right\},$$

что при $N \to \infty$ по теореме Берри — Эссеена [10, с. 449] отличается от значения $\Phi\left(-\dfrac{1}{\sigma_2}(\sqrt{N}\mu - \varkappa_{1-\alpha})\right)$ на величину $O(1/\sqrt{N})$. Отсюда вытекает указанное в условии теоремы выражение для $\alpha_2(d)$. При $\mu < 0$ расчёт $\alpha_2(d)$ проводится аналогично.

Теорема 2 доказана. ■

Приравнивая первое слагаемое в выражении для $\alpha_2(d)$ теоремы 2 к $\beta \in (0,1)$, получаем приближённую формулу для объёма материала, достаточного для различения гипотез с заданными вероятностями ошибок:

$$N_1^*(\alpha,\beta,R) = \frac{(\varkappa_{1-\alpha} + \varkappa_{1-\beta}\sigma_2(R))^2}{\mu_2^2(R)}.$$

Главным членом здесь является знаменатель, поскольку $P^R \to \mathbb{U}$ при $R \to \infty$, $\sigma_2^2(R) \to 1$. Ниже показано, что при ограничении парами векторов, удовлетворяющими

условиям п. 2 леммы 1, максимальное по парам значение модуля $\mu_2(R)$ равно $|\lambda_2|^R$ — см. (17). При таком выборе пары значение $N_1^*(\cdot)$ увеличивается примерно в $|\lambda_2|^{-2}$ раз при увеличении числа R раундов шифрования на 1.

Значение второго наибольшего по модулю собственного числа λ_2 МПВР как характеристики устойчивости марковского шифра к разностным атакам впервые рассмотрел X. Lai в диссертации [11]. После 24-летнего перерыва Lai продолжил исследование с соавторами: в [12] рассмотрены два способа получения верхних оценок $|\lambda_2|$, а также их применения к анализу мини-моделей шифрсистемы IDEA с длинами блока 8 и 16 бит. Получена следующая оценка [12, теорема 2]: шифрсистема с длиной блока n является «практически стойкой к разностному криптоанализу», если $|\lambda_2|^{R-2} < 2^{-(n-1)}$ (заметим, что в оригинале пропущен знак модуля у λ_2).

Эта оценка имеет эвристический характер, поскольку понятие «практической стойкости» строго не определено. Спектральный критерий (13) и его расчёт в теореме 2 позволяют дать более строгую и точную характеристику спектрально-разностной атаки — формулу для объёма материала в зависимости от вероятностей ошибок обоих родов. Она показывает, что в модели независимых двублочных текстов при любом числе раундов на достаточном объёме материала может быть построена атака различения со сколь угодно малыми вероятностями ошибок.

2.3. Оптимизация выбора пары векторов

1. С некоторой точки зрения спектральная атака есть обобщение традиционной. Действительно, при традиционном подходе для отличения гипотезы $Q = P^R$ от гипотезы $Q = \mathbb{U}$ используется статистическая оценка одного (желательно наибольшего по модулю) выделенного элемента матрицы $P^R - \mathbb{U}$:

$$p_{ab}(R) - 1/M = \mathbf{e}_a(P^R - \mathbb{U})e_b^{\downarrow}. \tag{15}$$

Правая часть равенства (15) может рассматриваться как значение билинейной формы из семейства

$$\left\{\mathbf{u}\,(P^R - \mathbb{U})v^{\downarrow} : u, v \in \mathbb{R}^M,\ |u| = |v| = 1\right\}. \tag{16}$$

Спектральный критерий основан на разнице средних значений статистики при разных гипотезах, которую при нормировании также можно записать в виде (16):

$$\frac{1}{N}(\mathsf{E}_2 S(N) - \mathsf{E}_1 S(N)) = \mathbf{u}(P^R - \mathbb{U})v^{\downarrow} = \mu_2(R).$$

Здесь последнее равенство выполнено для пар, удовлетворяющих условиям п. 1 леммы 1. Поэтому логично поставить вопрос о поиске пары (u, v), при которой модуль билинейной формы (16) максимален.

2. Пусть выполнено условие (3) доминирования λ_2.

2*а*) При ограничении парами, удовлетворяющими условиям п. 2 леммы 1, из неравенства Коши — Буняковского получаем, что модуль $\mu_2(R)$ максимизируется при выборе

$$u = v \in \{\mathbf{B}_2/|\mathbf{B}_2|, C_2^{\downarrow}/|C_2^{\downarrow}|\},\ \text{при этом } \mu_2(R) = \lambda_2^R, \tag{17}$$

где $\mathbf{B}_2$, $C_2^{\downarrow}$ — левый и правый собственные векторы матрицы P. Выбор (17) можно назвать *одновекторным построением* спектральной статистики. Из простоты λ_2 вытекает, что таких оптимальных пар (с точностью до знака векторов) будет не более двух.

2*б*) В ситуации выбора произвольной нормированной пары векторов можно предложить следующий путь асимптотически оптимального выбора пары векторов при

условии (2) диагонализуемости P над $\mathbb{C}$. Из спектрального разложения (8) следует, что при больших R главный член значений билинейных форм (16) равен

$$\lambda_2^R \mathbf{u}\, C_2^{\downarrow} \mathbf{B}_2 v^{\downarrow} = \lambda_2^R \langle \mathbf{u}, C_2^{\downarrow} \rangle \langle \mathbf{B}_2 v^{\downarrow} \rangle = \lambda_2^R \cos(u, C_2^{\downarrow}) |C_2^{\downarrow}| \cos(v, \mathbf{B}_2) |\mathbf{B}_2|,$$

что по модулю не превосходит $|\mathbf{B}_2||C_2^{\downarrow}||\lambda_2|^R$. При этом равенство достигается тогда и только тогда, когда u параллелен $C_2^{\downarrow}$, v — параллелен $\mathbf{B}_2$. Это условие обеспечивается выбором

$$u = C_2^{\downarrow}/|C_2^{\downarrow}|,\ v = \mathbf{B}_2/|\mathbf{B}_2|, \quad \text{тогда } \mu_2(R) \approx |\mathbf{B}_2||C_2^{\downarrow}|\lambda_2^R. \tag{18}$$

Порядок последней величины совпадает с порядком значения $|\lambda_2|^R$ из (17).

Такое использование правого собственного вектора матрицы в качестве левого вектора билинейной формы (и наоборот) несколько неожиданно, но, согласно неравенству Коши — Буняковского, значение коэффициента

$$|\mathbf{B}_2||C_2^{\downarrow}| \geqslant \langle \mathbf{B}_2, C_2^{\downarrow} \rangle = 1$$

не меньше 1. Поэтому, возможно, при больших R именно пара векторов (18) будет близка к оптимальной.

3. Спектральные атаки по независимым кодовым книгам

Условие наличия у аналитика полной кодовой книги малоразмерного блочного шифра рассмотрено в [8]. Как представляется, оно является достаточно естественным (например, использовалось блочное шифрование в режиме счётчика) и удобным для проведения экспериментов. В [8] предложена, рассчитана (для 50 % атакуемых ключей) и осуществлена атака, основанная на критерии отношения правдоподобий, на последний раунд Present$(16, R)$ для $7 \leqslant R \leqslant 9$ по одной кодовой книге.

Покажем, что спектральный метод позволяет рассматривать более общую ситуацию наличия нескольких случайных полных кодовых книг.

Будем считать, что ненулевые элементы группы $(\mathcal{X}, +)$ пронумерованы числами от 1 до M, и отождествлять элементы с числами при нумерации координат, описании области суммирования и т. д.

Пусть $\mathscr{K}$ — множество значений одного раундового ключа, $B = B(\mathbf{k}) = (z_0, \ldots, z_M)$ — книга, соответствующая набору $\mathbf{k} \in \mathscr{K}^R$ раундовых ключей, т. е. $z_i = F_R(i, \mathbf{k})$ — результат R-раундового шифрования блока $i \in \mathcal{X}$. Книге соответствует матрица переходных вероятностей разностей

$$P(\mathbf{k}) = \|\mathsf{P}\{F_R(X + a, \mathbf{k}) - F_R(X, \mathbf{k}) = b\}\|_{a,b \in \mathcal{X}'},\ X \sim U(\mathcal{X}).$$

В следующей лемме (достаточно простой, но имеющей важный методический смысл) утверждается, что в модели с выбором случайного набора $\mathbf{K}$ раундовых ключей матрица $P^{(R)}$ переходных вероятностей разностей шифра (за R раундов) есть результат усреднения матриц $P(\mathbf{k})$. Элементы МПВР равны при $a, b \in \mathcal{X}'$:

$$P_{ab}^{(R)} = \mathsf{P}\{F_R(X + a, \mathbf{K}) - F_R(X, \mathbf{K}) = b\}, \quad X \sim U(\mathcal{X}).$$

Лемма 2. Пусть случайный набор $\mathbf{K}$ выбирается из $\mathscr{K}^R$ независимо от входного блока X. Тогда $\mathsf{E}P(\mathbf{K}) = P^{(R)}$. Если при этом компоненты $\mathbf{K}$ независимы и одинаково распределены так, что шифр является марковским с матрицей P переходных вероятностей разностей за 1 раунд, то $\mathsf{E}P(\mathbf{K}) = P^R$.

Доказательство. Обозначим $\xi(x,\mathbf{k}) = \mathbb{I}\{F_R(x+a,\mathbf{k}) - F_R(x,\mathbf{k}) = b\}$ при фиксированных $a, b \neq 0$. С учётом независимости $\mathbf{K}$ и X имеем

$$P_{ab}^{(R)} = \sum_{\mathbf{k}\in\mathscr{K}^R, x\in\mathcal{X}} \mathsf{P}\{\mathbf{K}=\mathbf{k}, X=x\}\xi(x,\mathbf{k}) = \sum_{\mathbf{k}\in\mathscr{K}^R} \mathsf{P}\{\mathbf{K}=\mathbf{k}\} \sum\nolimits_{x\in\mathcal{X}} \mathsf{P}\{X=x\}\xi(x,\mathbf{k}) =$$
$$= \sum_{\mathbf{k}\in\mathscr{K}^R} \mathsf{P}\{\mathbf{K}=\mathbf{k}\}P(\mathbf{k})_{ab} = \mathsf{E}P(\mathbf{K})_{ab},$$

что требовалось доказать. ■

Замечание 1. В [13, с. 264] доказан аналогичный лемме 2 результат о произведениях R элементов матриц; вероятность перехода разностей за R раундов является суммой таких произведений.

Замечание 2. Из доказательства леммы 2 видно, что она справедлива и для неравномерного распределения X.

Для фиксированных $u, v \in \mathbb{R}^M$ аналогично статистике (11) из модели двублочных текстов при суммировании по всем возможным $N_0 = \binom{M+1}{2}$ парам разностей книги строим статистику

$$S(\mathbf{k}) = N_0 \mathbf{u} P(\mathbf{k}) v^{\downarrow} = M \sum_{a,b\in\mathcal{X}'} u_a \frac{M+1}{2} P(\mathbf{k})_{ab} v_b,$$

которую назовём *книжным вкладом*.

Ограничимся далее ситуацией $(\mathcal{X}, +) = (\mathbb{Z}_2^n, \oplus)$. Тогда для пар входных блоков $(i, i+a)$, $(i+a, i)$ разности совпадают,

$$\frac{M+1}{2} P(\mathbf{k})_{ab} = \frac{1}{2} \sum_{0\leqslant i\leqslant M} \mathbb{I}\{F_R(i+a,\mathbf{k}) - F_R(i,\mathbf{k}) = b\} =$$
$$= \sum_{i<j} \mathbb{I}\{j = i+a, F_R(j,\mathbf{k}) - F_R(i,\mathbf{k}) = b\} = \sum_{i<j} \mathbb{I}\{a = j-i\}\mathbb{I}\{b = z_j - z_i\},$$

и получаем

$$S(\mathbf{k}) = M \sum_{a,b} \sum_{i<j} \mathbb{I}\{a = j-i\}\mathbb{I}\{b = z_j - z_i\} u_a v_b = M \sum_{0\leqslant i<j\leqslant M} u_{j-i} v_{z_j - z_i}. \tag{19}$$

При условиях леммы 2 книжный вклад является случайной величиной, среднее значение которой при гипотезе H_2 находим из леммы 2 с учётом свойства линейности математического ожидания случайной матрицы

$$\mathsf{E}_2 S(\mathbf{k}) = N_0 \mathbf{u} P^R v^{\downarrow} = N_0 \mu_2(R),$$

что совпадает с выражением $N\mu_2(R)$ в (12) при $N = N_0$. Объяснить это совпадение можно так: при условиях теоремы 2 независимые слагаемые суммы $S(N)$ имеют такое же распределение, как случайная величина $\tau = M u_{\Delta X} v_{\Delta Y}$ при случайном равновероятном выборе разности ΔX. Но при случайном равновероятном выборе пары мест $\{i, j\}$ в книге B распределения случайных величин $u_{j-i} v_{z_j - z_i}$ и τ совпадают.

Если будем предполагать, как в [8], что распределение $S(\mathbf{k})$ близко к нормальному, то получим, что среднее значение $\mathsf{E}_2 S(\mathbf{k})$ близко к медиане распределения. Поэтому примерно для 50 % ключей модули величин $S(\mathbf{k})$ не меньше $|\mathsf{E}_2 S(\mathbf{k})|$. Тогда односторонний критерий

$$d: \; S(\mathbf{K}) \operatorname{sign}(\mu_2(R)) > \varkappa_{1-\alpha}\sqrt{N_0} \Longrightarrow H_2$$

размера, близкого к α, будет выявлять суммарный шифр не менее чем для примерно 50 % ключей (т. е. $\alpha_2(d) \leqslant \beta \approx 0{,}5$) при условии $\varkappa_{1-\alpha}\sqrt{N_0} \leqslant N_0|\mu_2(R)|$. Оно близко к условию $|\mathcal{X}| \geqslant \dfrac{\varkappa_{1-\alpha}}{|\mu_2(R)|}$.

Обобщая модель [8], будем предполагать, что имеется N_b случайных независимых кодовых книг $B(t) = (z_0^t, \ldots, z_M^t)$, $1 \leqslant t \leqslant N_b$. Гипотеза H_1 заключается в том, что они получены как нижние строки N_b независимых подстановок с равновероятным распределением на $S(\mathcal{X})$. Гипотеза H_2 заключается в том, что книги соответствуют R-раундовому шифрованию при независимом выборе случайных равновероятных наборов $\mathbf{K}(t) \sim U(\mathscr{K}^R)$ раундовых ключей, $1 \leqslant t \leqslant N_b$.

Обозначим далее через $P(t)$ МПВР, соответствующую книге $B(t)$, $1 \leqslant t \leqslant N_b$, и перейдём к рассмотрению статистики

$$S'(N_b) = S_1 + \ldots + S_{N_b}, \quad S_t = N_0 \mathbf{u} P(t) v^{\downarrow}. \tag{20}$$

Временная сложность её вычисления пропорциональна $|\mathcal{X}|^2 N_b$. Тогда с учётом леммы 2 при условиях п. 1 леммы 1, согласно (12),

$$\mathsf{E}_i S'(N_b) = N_b N_0 \mu_2(R)\, \mathbb{I}\{i = 2\}. \tag{21}$$

3.1. Дисперсия книжного вклада при гипотезе H_1

В теореме 2 при обеих гипотезах найдены дисперсии $N\sigma_i^2$ случайной величины $S(N)$ как суммы независимых случайных величин. Статистика $S(\mathbf{k})$ книжного вклада является суммой зависимых случайных величин в силу зависимости выбора пар входных блоков, что значительно усложняет вычисление её дисперсии.

Это удаётся сделать при гипотезе H_1 для группы $\mathcal{X} = \mathbb{Z}_2^n$. Здесь возникают следующие интересные вероятностные конструкции.

Обозначим: $(M)_k = M(M-1)\ldots(M-k+1)$ — факториальная степень числа M для $k \geqslant 1$.

Лемма 3. Пусть случайная величина ξ задана на пространстве элементарных событий Ω мощности $M \geqslant 2$ с классической вероятностью, $\mathsf{E}\xi = 0$. Тогда при случайном выборе $\omega = (\omega_1, \omega_2)$ из Ω^2 для случайной величины $\eta(\omega) = \xi(\omega_1)\xi(\omega_2)$ имеем:

1) $\mathsf{E}\eta = -\dfrac{\mathsf{D}\xi}{M-1}$, если ω_1, ω_2 извлекаются из Ω равновероятно без возвращения;
2) $\mathsf{E}\eta = \dfrac{2\mathsf{D}\xi}{(M-1)(M-2)}$, если ω извлекается из Ω^2 в соответствии с мерой $\mathsf{P}\{\omega\} = \dfrac{M-3+2\mathbb{I}\{\omega_1=\omega_2\}}{(M)_3}$.

Доказательство. В вероятностных схемах обоих пунктов компоненты ω распределены равномерно на Ω в силу симметрии исходов.

1. В схеме п. 1

$$\mathsf{E}\eta = \frac{1}{(M)_2}\sum_{\omega_1\neq\omega_2}\xi(\omega_1)\xi(\omega_2) = \frac{1}{(M)_2}\Big(\sum_{\omega_1}\xi(\omega_1)\sum_{\omega_2}\xi(\omega_2) - \sum_{\omega_1}\xi^2(\omega_1)\Big) = -\frac{M\mathsf{E}\xi^2}{(M)_2} = -\frac{\mathsf{D}\xi}{M-1},$$

поскольку $\sum\limits_{\omega_1}\xi(\omega_1) = M\mathsf{E}\xi = 0$.

2. В схеме п. 2 имеем $\mathsf{P}\{\omega_1 = \omega_2\} = M\dfrac{M-1}{(M)_3} = \dfrac{1}{M-2}$, условное математическое ожидание случайной величины η при условии события $\{\omega_1 = \omega_2\}$ равно

$$\mathsf{E}(\eta \,|\, \omega_1 = \omega_2) = \mathsf{E}\xi^2(\omega) = \mathsf{D}\xi.$$

Условие $\{\omega_1 \neq \omega_2\}$ порождает равномерную условную меру на множестве выборок объёма 2 без возвращения, поэтому, согласно п. 1, $\mathsf{E}(\eta \,|\, \omega_1 \neq \omega_2) = -\dfrac{\mathsf{D}\xi}{M-1}$. Тогда по формуле полного математического ожидания [10, с. 68]

$$\mathsf{E}\eta(\omega) = \mathsf{P}\{\omega_1 = \omega_2\}\mathsf{E}(\eta \,|\, \omega_1 = \omega_2) + \mathsf{P}\{\omega_1 \neq \omega_2\}\mathsf{E}(\eta \,|\, \omega_1 \neq \omega_2) =$$
$$= \frac{1}{M-2}\mathsf{D}\xi + \frac{M-3}{M-2}\,\frac{(-\mathsf{D}\xi)}{M-1} = \frac{\mathsf{D}\xi}{M-2}\left(1 - \frac{M-3}{M-1}\right) = \frac{2\mathsf{D}\xi}{(M-1)(M-2)}.$$

Лемма 3 доказана. ■

Пример 2. Пусть $\xi(\omega) = \omega$. Тогда: а) при $\Omega = \{-1, 1\}$ имеем $\mathsf{D}\xi = 1$, и в схеме п. 1 $\eta \equiv -1$, $\mathsf{E}\eta = -1 = -\dfrac{\mathsf{D}\xi}{2-1}$; б) при $\Omega = \{-1, 0, 1\}$ имеем $\mathsf{D}\xi = 2/3$, и в схеме п. 1 $\eta \sim \begin{pmatrix} 0 & -1 \\ 2/3 & 1/3 \end{pmatrix}$, $\mathsf{E}\eta = -\dfrac{1}{3} = -\dfrac{\mathsf{D}\xi}{3-1}$. В схеме п. 2 имеем $\mathsf{P}\{\omega_1 = \omega_2\} = 1$, поэтому η имеет распределение Бернулли с вероятностью успеха $\dfrac{2}{3} = \mathsf{E}\eta = \dfrac{2\mathsf{D}\xi}{3-1}$, что тоже согласуется с формулой леммы 3.

Замечание 3. Если при условии леммы 3 элементы ω_1, ω_2 выбираются независимо равновероятно из Ω, то $\mathsf{E}\eta = \operatorname{cov}(\xi(\omega_1), \xi(\omega_2)) = 0$. В схеме п. 1 вероятность диагонали нулевая (понижена по сравнению с независимым выбором), поэтому случайные величины $\xi(\omega_1)$, $\xi(\omega_2)$ отрицательно коррелированы. В схеме п. 2 вероятность диагонали повышена по сравнению с независимым выбором: $\dfrac{1}{M-2} > \dfrac{1}{M}$, поэтому $\xi(\omega_1)$, $\xi(\omega_2)$ положительно коррелированы.

Изучим отдельно линейно связанную с книжным вкладом (19) статистику

$$S = \sum_{0 \leqslant i < j \leqslant M} u_{j-i} v_{z_j - z_i}.$$

Теорема 3. Пусть подстановка z с нижней строкой $(z_0, \ldots, z_M)$ выбирается случайно равновероятно из $S(\mathcal{X})$, векторы $u, v \in \mathbb{R}^M$ евклидовой длины 1 ортогональны вектору $\mathbf{1}$. Тогда $\mathsf{E}S = 0$, а при $(\mathcal{X}, +) = (\mathbb{Z}_2^n, \oplus)$, $n \geqslant 2$

$$\mathsf{D}S = \frac{M+1}{2(M-2)} = \frac{2^{n-1}}{2^n - 3}.$$

Доказательство. Для различных $i, j \in \mathcal{X}$ положим $\xi = \xi(i,j) = z_j - z_i$. Легко видеть, что эта случайная величина равномерно распределена на $\mathcal{X}'$. Поэтому

$$\mathsf{E}v_\xi = \sum_{a \in \mathcal{X}'} \frac{1}{M} v_a = \frac{1}{M}\langle v, \mathbf{1}\rangle = 0,\ \mathsf{E}v_\xi^2 = \sum_{a \in \mathcal{X}'} \frac{1}{M} v_a^2 = \frac{1}{M}|v|^2 = \frac{1}{M}, \tag{22}$$

и $\mathsf{E}S = \sum\limits_{i<j} u_{j-i}\mathsf{E}v_{\xi(i,j)} = 0$. Вычислим $\mathsf{D}S = \mathsf{E}S^2$. Представим

$$S^2 = \sum_{i<j} u_{j-i} v_{\xi(i,j)} \sum_{k<l} u_{l-k} v_{\xi(k,l)} = \Sigma_2 + \Sigma_1 + \Sigma_0, \tag{23}$$

где Σ_m — сумма случайных величин $u_{j-i}u_{l-k}v_{\xi(i,j)}v_{\xi(k,l)}$ по всем таким парам пар $(i,j), (k,l)$, что

$$0 \leqslant i < j \leqslant M,\ 0 \leqslant k < l \leqslant M,\ |\{i,j\} \cap \{k,l\}| = m, \tag{24}$$

$m = 0, 1, 2$. Вычислим средние значения этих сумм.

1. Легко видеть, что $\Sigma_2 = \sum\limits_{i<j} u_{j-i}^2 v_{\xi(i,j)}^2$, и с учётом (22)

$$\mathsf{E}\Sigma_2 = \sum_{i<j} u_{j-i}^2 \frac{1}{M} = \frac{1}{M}\sum_{i<j} u_{i+j}^2 = \frac{1}{2M}\sum_{i\neq j} u_{i+j}^2,$$

где во втором переходе использовано равенство $-i = i$ для $i \in \mathbb{Z}_2^n$. Для любого фиксированного $a \in \mathcal{X}'$ уравнение $i + j = a$ имеет ровно $M + 1$ решений относительно $(i, j) \in \mathcal{X}^2$, поэтому

$$\mathsf{E}\Sigma_2 = \frac{M+1}{2M}\sum_{a\in\mathcal{X}'} u_a^2 = \frac{M+1}{2M}. \tag{25}$$

2. Для вычисления $\mathsf{E}\Sigma_1$ найдём совместное распределение случайных величин $\xi = \xi(i, j)$ и $\eta = \xi(k, l)$. С учётом симметрии, не ограничивая общности, считаем $\xi = z_0 + z_1$, $\eta = z_0 + z_2$. Так как $z_1 \neq z_2$, то $\mathsf{P}\{\xi = \eta\} = 0$.

Далее, для любых $c \neq d$ из $\mathcal{X}'$ в событии $\{\xi = c, \eta = d\}$ при фиксации $z_0 = a$ определяются однозначно значения $z_1 = a + c$, $z_2 = a + d$. Поэтому $\mathsf{P}\{\xi = c, \eta = d\} = \dfrac{M}{(M+1)_3} = \dfrac{1}{(M)_2}$. Таким образом, $\omega = (\xi, \eta)$ имеет распределение выборки без возвращения из $\mathcal{X}'$, и с учётом (22) по п. 1 леммы 3 получим

$$\mathsf{E}v_{\xi(i,j)}v_{\xi(k,l)} = \frac{-\mathsf{E}v_\xi^2}{|\mathcal{X}'|} = -\frac{1}{M(M-1)},\ |\{i,j\}\cap\{k,l\}| = 1. \tag{26}$$

Это равенство поможет вычислить возникающую сумму $S_1 = \sum u_{i+j}u_{k+l}$ по индексам (24) при $m = 1$. Одной тройке $0 \leqslant a < b < c \leqslant M$ соответствует ровно шесть индексов со свойством $\{i, j\} \cup \{k, l\} = \{a, b, c\}$: тремя способами из $\{a, b, c\}$ выбираем повторяющийся элемент и двумя — суммируемый с ним индекс в u_{i+j}. Сумму соответствующих шести слагаемых можно записать в виде $\sum\limits_{(i,j,k)\in\mathcal{P}\{a,b,c\}} u_{i+j}u_{i+k}$ по всем перестановкам множества $\{a, b, c\}$. Интерпретируя (i, j, k) как реализацию случайного вектора (z_0, z_1, z_2), находим

$$S_1 = \sum_{(i,j,k)} u_{i+j}u_{i+k} = (M+1)_3\mathsf{E}u_{\xi(0,1)}u_{\xi(0,2)} = (M+1)_3\frac{-1}{M(M-1)} = -(M+1),$$

где в предпоследнем переходе использовано выражение (26). Итак,

$$\mathsf{E}\Sigma_1 = \sum u_{i+j}u_{k+l}\mathsf{E}v_{\xi(i,j)}v_{\xi(k,l)} = S_1\frac{-1}{M(M-1)} = \frac{M+1}{M(M-1)}. \tag{27}$$

3. Вычисление $\mathsf{E}\Sigma_0$ проведём аналогично п. 2. Исследуем совместное распределение случайных величин $\xi = z_0 + z_1$ и $\eta = z_2 + z_3$. Здесь для $c = d \in \mathcal{X}'$ в событии $\{\xi = \eta = c\}$ при фиксации $z_0 = a$, $z_2 = b$ определяются однозначно значения $z_1 = a + c$, $z_3 = b + c$, и в четвёрке (z_0, z_1, z_2, z_3) все элементы различны тогда и только тогда, когда $b \notin \{a, a + c\}$. Следовательно,

$$\mathsf{P}\{\xi = \eta = c\} = \frac{(M+1)(M-1)}{(M+1)_4} = \frac{M-1}{(M)_3}.$$

При $c \neq d$ из $\mathcal{X}'$ в событии $\{\xi = c, \eta = d\}$ при фиксации z_0, z_2 значениями $a, b \in \mathcal{X}$ четвёрка $(z_0, z_1, z_2, z_3) = (a, a+c, b, b+d)$ состоит из различных элементов тогда и только

тогда, когда $b \notin \{a, a+c, a+c+d, a+d\}$. Отсюда $\mathsf{P}\{\xi = c, \eta = d\} = \dfrac{(M+1)(M-3)}{(M+1)_4} = \dfrac{M-3}{(M)_3}$.

Заметим, что:

а) сумма вероятностей распределения (ξ, η) равна

$$M\frac{M-1}{(M)_3} + M(M-1)\frac{M-3}{(M)_3} = \frac{1}{M-2} + \frac{M-3}{M-2} = 1;$$

б) при $n = 2$ имеем $M = 3$, и распределение (ξ, η) сосредоточено на диагонали.

Таким образом, $\omega = (\xi, \eta)$ имеет распределение, как в п. 2 леммы 3, поэтому здесь с учётом (22)

$$\mathsf{E}v_{\xi(i,j)}v_{\xi(k,l)} = \frac{2/M}{(M-1)(M-2)} = \frac{2}{(M)_3}, \ \{i,j\} \cap \{k,l\} = \varnothing. \tag{28}$$

Далее находим

$$S_0 = \sum u_{i+j}u_{k+l} = \frac{1}{4}\sum_{i\neq j, k\neq l} u_{i+j}u_{k+l} = \frac{(M+1)_4}{4}\mathsf{E}u_{\xi(0,1)}u_{\xi(2,3)} = \frac{(M+1)_4}{4}\frac{2}{(M)_3} = \frac{M+1}{2},$$

где в предпоследнем переходе использовано (28). Итак,

$$\mathsf{E}\Sigma_0 = S_0\mathsf{E}v_{\xi(0,1)}v_{\xi(2,3)} = \frac{M+1}{2}\frac{2}{(M)_3} = \frac{M+1}{(M)_3}. \tag{29}$$

Окончательно из представления (23) с учётом (25), (27) и (29) находим

$$\mathsf{E}S^2 = \frac{M+1}{2M} + \frac{M+1}{M(M-1)} + \frac{M+1}{(M)_3} = \frac{M+1}{M}\left(\frac{1}{2} + \frac{1}{M-1} + \frac{1}{(M-1)(M-2)}\right) = \frac{M+1}{2(M-2)}.$$

Теорема 3 доказана. ■

Замечание 4. Величина $\mathsf{E}S^2 = \dfrac{1}{2}\left(1 + \dfrac{3}{M-2}\right)$ монотонно убывает от 1 к $1/2$ при $M = 5, 6, \ldots$

Замечание 5. Если бы слагаемые в определении S были независимы, то дисперсия с учётом п. 1 доказательства теоремы 3 была бы равна $\sum\limits_{i<j} u_{i+j}^2/M = (M+1)/(2M)$, что равно доле $(M-2)/M$ реального значения.

Замечание 6. При $n = 2, 3$ равенства (26), (28) и утверждение теоремы 3 проверены перебором на ЭВМ всех подстановок степеней 4 и 8 соответственно при некоторых u, v. Так, при $n = 2$ использовались $u = (1, -1, 0)/\sqrt{2}$, $v = (2, 1, -1)/\sqrt{6}$; если здесь целочисленные векторы не нормировать, то результаты будут больше соответственно в $|v|^2 = 6$ и в $|u|^2|v|^2 = 12$ раз.

Из теоремы 3 вытекает, что при гипотезе H_1

$$\mathsf{D}_1 S(\mathbf{k}) = M^2\frac{M+1}{2(M-2)} = N_0\frac{M}{M-2}, \quad M = 2^n - 1, \tag{30}$$

что немного (в $M/(M-2)$ раз) больше дисперсии суммы $\mathsf{D}_1 S(N_0) = N_0$ с таким же количеством независимых слагаемых, имеющих такое же распределение.

3.2. Критерий и оценка требуемого числа книг

С учётом формулы (30) для дисперсии книжного вклада при гипотезе H_1 рассматриваем критерий

$$d:\ S'(N_b)\ \mathrm{sign}(\mu_2(R)) > \varkappa_{1-\alpha}\sqrt{\frac{NM}{M-2}} \Longrightarrow H_2, \tag{31}$$

где $N = N_0 N_b$.

Теорема 4. Пусть при $\mathbf{K} \sim U(\mathscr{K}^R)$ шифр с алфавитом $(\mathcal{X}, +) = (\mathbb{Z}_2^n, \oplus)$ является марковским с МПВР P, удовлетворяющей условию (3) доминирования λ_2, и векторы статистики $S'(N_b)$ выбраны согласно (14). Тогда для любого α, $0 < \alpha < 1$, при $N_b \to \infty$ критерий (31) имеет асимптотический размер α и

$$\alpha_2(d) = \Phi\Big(-\frac{\sqrt{N}|\mu_2(R)| - \varkappa_{1-\alpha}\sqrt{M/(M-2)}}{\sqrt{\mathsf{D}_2 S(\mathbf{k})/N_0}}\Big) + O\left(\frac{1}{\sqrt{N_b}}\right).$$

Доказательство. Слагаемые в представлении (20) для $S'(N_b)$ при обеих гипотезах являются независимыми одинаково распределёнными случайными величинами и, согласно центральной предельной теореме, распределения нормированных сумм $\dfrac{S'(N_b) - \mathsf{E}_i S'(N_b)}{\sqrt{N_b \mathsf{D}_i S(\mathbf{k})}}$ сходятся к $\mathcal{N}(0,1)$, $i = 1, 2$. Далее асимптотические вероятности ошибок критерия рассчитываются стандартным способом с учётом равенств (21) и (30). В частности, при $\mu_2(R) > 0$ с учётом неравенства Берри — Эссеена

$$\alpha_2(d) = \mathsf{P}_2\left\{S' \leqslant \varkappa_{1-\alpha}\sqrt{\frac{NM}{M-2}}\right\} =$$

$$= \mathsf{P}_2\Big\{\frac{S' - N\mu_2(R)}{\sqrt{N_b \mathsf{D}_2 S(\mathbf{k})}} \leqslant \frac{\varkappa_{1-\alpha}\sqrt{NM/(M-2)} - N\mu_2(R)}{\sqrt{N_b \mathsf{D}_2 S(\mathbf{k})}}\Big\} =$$

$$= \Phi\Big(\frac{\varkappa_{1-\alpha}\sqrt{M/(M-2)} - \sqrt{N}\mu_2(R)}{\sqrt{\mathsf{D}_2 S(\mathbf{k})/N_0}}\Big) + O\left(\frac{1}{\sqrt{N_b}}\right).$$

Теорема 4 доказана. ■

Предполагая, что при больших R шифрование даёт подстановки, близкие к случайным равновероятным, и поэтому $\mathsf{D}_2 S(\mathbf{k}) \approx \mathsf{D}_1 S(\mathbf{k})$, приравниваем главный член в $\alpha_2(d)$ к β. Таким образом получаем оценку для числа кодовых книг при больших значениях N_b, $M = 2^n - 1$:

$$\sqrt{N}|\mu_2(R)| - \varkappa_{1-\alpha}\sqrt{\frac{M}{M-2}} \approx \varkappa_{1-\beta}\sqrt{\frac{M}{M-2}},$$

$$N_b \approx \frac{(\varkappa_{1-\alpha} + \varkappa_{1-\beta})^2 \dfrac{M}{M-2}}{\dbinom{M+1}{2}\mu_2^2(R)} \approx \frac{2(\varkappa_{1-\alpha} + \varkappa_{1-\beta})^2}{(2^n \mu_2(R))^2}.$$

Отметим, что в 50 %-й атаке для обоснования этой оценки не требуется предположения о дисперсии $\mathsf{D}_2 S(\mathbf{k})$ и $\varkappa_{1-\beta} = 0$. Тогда при одновекторном построении (17) статистики имеем $\mu_2(R) = \lambda_2^R$, $N_{b,50\,\%} \approx \dfrac{\varkappa_{1-\alpha}^2}{2^{2n-1}\lambda_2^{2R}}$.

ЛИТЕРАТУРА

1. *Lai X., Massey J., and Murphy S.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
2. *Погорелов Б. А., Пудовкина М. А.* Разбиения на биграммах и марковость алгоритмов блочного шифрования // Матем. вопр. криптогр. 2017. Т. 8. Вып. 1. С. 107–142.
3. *Денисов О. В.* Критерии марковости алгоритмов блочного шифрования // Прикладная дискретная математика. 2018. № 41. С. 28–37.
4. *Денисов О. В.* Спектральный критерий для проверки гипотез о случайных подстановках // Матем. вопр. криптогр. 2016. Т. 7. Вып. 3. С. 19–28.
5. *Ланкастер П.* Теория матриц. М.: Наука, 1978. 280 с.
6. *Альпин Ю. А., Альпина В. С.* Теорема Перрона — Фробениуса: доказательство с помощью цепей Маркова // Зап. научн. сем. ПОМИ. 2008. Т. 359. С. 5–16.
7. *Денисов О. В.* Атаки различения на блочные шифрсистемы по разностям двублочных текстов // Прикладная дискретная математика. 2020. № 48. С. 43–62.
8. *Albrecht M. and Leander G.* An all-in-one approach to differential cryptanalysis for small block ciphers // LNCS. 2013. V. 7707. P. 1–15.
9. *Хорн Р., Джонсон Ч.* Матричный анализ. М.: Мир, 1989. 655 с.
10. *Боровков А. А.* Теория вероятностей. М.: Эдиториал УРСС, 1999. 472 с.
11. *Lai X.* On the Design and Security of Block Ciphers: Dissertation for the degree of Doctor of Technical Sciences. Swiss Federal Institute of Technology, Zurich, 1992. 118 p.
12. *Xue W., Lin T., Shun X., et al.* On the estimation of the second largest eigenvalue of Markov ciphers // Security Comm. Networks. 2016. V. 9. P. 2093–2099.
13. *Vaudenay S.* On the security of CS-cipher // LNCS. 1999. V. 1636. P. 260–274.

REFERENCES

1. *Lai X., Massey J., and Murphy S.* Markov ciphers and differential cryptanalysis. LNCS, 1991, vol. 547, pp. 17–38.
2. *Pogorelov B. A. and Pudovkina M. A.* Razbieniya na bigrammah i markovost' algoritmov blochnogo shifrovaniya [Partitions on bigrams and Markov property of block ciphers]. Matematicheskie Voprosy Kriptografii, 2017, vol. 8, iss. 1, pp. 107–142. (in Russian)
3. *Denisov O. V.* Kriterii markovosti algoritmov blochnogo shifrovaniya [Criteria for Markov block ciphers]. Prikladnaya Diskretnaya Matematika, 2018, no. 41, pp. 28–37. (in Russian)
4. *Denisov O. V.* Spektral'nyj kriterij dlya proverki gipotez o sluchajnyh podstanovkah [Spectral criterion for testing hypotheses about random substitutions]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, iss. 3, pp. 19–28. (in Russian)
5. *Lankaster P.* Theory of Matrices. N.Y.; London, Academic Press, 1969.
6. *Al'pin Yu. A. and Al'pina V. S.* Teorema Perrona — Frobeniusa: dokazatel'stvo s pomoshch'yu cepej Markova [Perron — Frobenius theorem: proof using Markov chains]. Zapiski Nauchnyh Seminarov POMI, 2008, vol. 359, pp. 5–16. (in Russian)
7. *Denisov O. V.* Ataki razlicheniya na blochnye shifrsistemy po raznostyam dvublochnyh tekstov [Distinguishing attacks on block ciphers by differentials of 2-blocks texts]. Prikladnaya Diskretnaya Matematika, 2020, no. 48, pp. 43–62. (in Russian)
8. *Albrecht M. and Leander G.* An all-in-one approach to differential cryptanalysis for small block ciphers. LNCS, 2013, vol. 7707, pp. 1–15.
9. *Horn R. and Johnson C.* Matrix Analysis. Cambridge University Press, 1986.
10. *Borovkov A. A.* Teoriya veroyatnostej [Probability Theory]. Moscow, URSS, 1999. 472 p. (in Russian)

11. *Lai X.* On the Design and Security of Block Ciphers: Dissertation for the degree of Doctor of Technical Sciences. Swiss Federal Institute of Technology, Zurich, 1992. 118 p.
12. *Xue W., Lin T., Shun X., et al.* On the estimation of the second largest eigenvalue of Markov ciphers // Security Comm. Networks, 2016, vol. 9, pp. 2093–2099.
13. *Vaudenay S.* On the security of CS-cipher. LNCS, 1999, vol. 1636, pp. 260–274.