Научная статья
DOI 10.66424/2071-8217-2026-2-11
УДК 004.056.55

О ВЛИЯНИИ ДИСКРЕТИЗАЦИИ НА ПРАКТИЧЕСКУЮ СЕКРЕТНОСТЬ КЛЮЧЕЙ, ФОРМИРУЕМЫХ ПО СХЕМЕ ИНТЕРВАЛОВ

Д. С. Богданов*

Национальный исследовательский университет «Высшая школа экономики», Москва, Россия

✉ *bogdanovds@ramlber.ru

ДЛЯ ЦИТИРОВАНИЯ

Богданов Д. С. О влиянии дискретизации на практическую секретность ключей, формируемых по схеме интервалов // Проблемы информационной безопасности. Компьютерные системы. 2026. № 2. С. 138–148.
DOI: 10.66424/2071-8217-2026-2-11

ПОСТУПИЛА 10.02.2026
ПРИНЯТА 07.05.2026
ОПУБЛИКОВАНА 15.06.2026

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Зачастую биты ключа, формируемые физическими генераторами случайных чисел, не являются реализациями независимых в совокупности равномерно распределенных случайных величин, в связи с чем возникает понятие «практическая секретность ключа». Для некоторых физических генераторов случайных чисел указанное отличие обусловлено дискретностью времени, измеряемого электронными компонентами. Для модели физического генератора случайных чисел, построенного по схеме интервалов, получены оценки практической секретности ключей с учетом влияния дискретизации времени измерений.

КЛЮЧЕВЫЕ СЛОВА

Физические генераторы случайных чисел, случайные процессы, теоретико-вероятностная модель, практическая секретность ключей, схема интервалов

Original
DOI 10.66424/2071-8217-2026-2-11

ON THE IMPACT OF DISCRETIZATION ON THE PRACTICAL SECRECY OF KEYS, FORMED BY THE INTERVAL SCHEME

D. S. Bogdanov*

National Research University Higher School of Economics, Moscow, Russia

✉ *bogdanovds@ramlber.ru

FOR CITATION

Bogdanov D. S. On the impact of discretization on the practical secrecy of keys, formed by the interval scheme. *Problems of information security.*

ABSTRACT

Often the key bits generated by physical random number generators are not realizations of jointly independent uniformly distributed random variables, which gives rise to the concept of “practical key secrecy”. For some physical random number generators this deviation is caused by

Computer systems.
2026. No. 2, pp. 138–148.
DOI: 10.66424/2071-8217-2026-2-11
(In Russian)

RECEIVED 10.02.2026
ACCEPTED 07.05.2026
PUBLICATION 15.06.2026

the discreteness of time measured by electronic components. In this paper, for a physical random number generator model based on the interval scheme, we obtain bounds on the practical secrecy of keys taking into account the impact of measurement time discretization.

KEYWORDS

Physical random number generators, random processes, probabilistic model, practical key secrecy, interval scheme

1. ВВЕДЕНИЕ

В практике построения физических генераторов случайных чисел (ФГСЧ) широко применяется подход, основанный на измерении временных интервалов между случайными событиями или от фиксированного начала до момента их наступления. Данная методология, известная как «схема интервалов», рассматривается в обзорных работах [1]. В рамках этой схемы генератор фиксирует моменты наступления некоторых случайных событий (например, приход фотонов на детектор), измеряет интервалы времени между ними с помощью высокочастотного счетчика и формирует выходные биты путем взятия младших разрядов накопленных значений счетчика. Конкретные реализации ФГСЧ, использующие эту схему, можно найти в исследованиях [2–5].

Актуальность разработки надежных ФГСЧ и их строгого анализа подтверждается их критической ролью в современных криптографических системах и постоянным развитием соответствующих стандартов и методов тестирования [6, 7]. Современные исследования в области ФГСЧ направлены как на поиск новых физических принципов [8], так и на углубленный анализ статистических свойств и стойкости существующих конструкций [9, 10].

Как и в случае других физических генераторов, последовательности битов, формируемые по схеме интервалов, часто не обладают свойствами независимости и равновероятности [11]. Это обстоятельство делает необходимым разработку адекватных вероятностных моделей для корректной оценки криптографической стойкости таких ключей. Так, в работе [12] И. М. Арбековым введено понятие практической секретности ключа, характеризующее среднее количество попыток, требуемых для его угадывания. Дальнейшее развитие данной концепции представлено в работах [13, 14]. В частности, в [14] предложена модель, в которой практическая секретность ключа полностью характеризуется параметром ε, определяющим степень отклонения распределения ключей от идеальной равновероятной схемы.

Особенностью ФГСЧ, построенных по схеме интервалов, является то, что отклонение от равновероятности может быть вызвано дискретностью измерения времени электронными компонентами. В работе [4] показано, что конечная частота регистрации сигнала приводит к возникновению зависимостей между соседними значениями выходной последовательности. Схожие эффекты есть и в реализации данной схемы из работы [3].

В настоящей работе с использованием подходов, основанных на исследовании условных распределений и анализе цепей Маркова, аналогичных применяемым в [15], исследуется практическая секретность ключей, формируемых по схеме интервалов. Цель работы – получение оценок сверху отклонения ε для таких ключей с учетом влияния дискретизации времени измерений.

2. МЕТОДЫ ИССЛЕДОВАНИЙ

Приведем основные определения, используемые в работе. В источнике [12] И. М. Арбековым введено понятие практической секретности ключа. Пусть ключ шифра принимает значения в конечном

множестве K с распределением вероятностей $P_K(k)$, $k \in K$. Практической секретностью ключа называется среднее число опробованных ключей до определения истинного ключа шифрования при использовании оптимального усеченного алгоритма перебора [12, 13]. Пусть злоумышленник, обладая некоторой априорной информацией, формирует упорядоченный список ключей в порядке убывания их условных вероятностей и перебирает их последовательно, пока не найдет верный. Если $p_{(1)} \geq p_{(2)} \geq \ldots \geq p_{(|K|)}$ – упорядоченные по убыванию вероятности ключей (при заданной дополнительной информации), то практическая секретность выражается как

$$S = \sum_{i=1}^{|K|} i p_{(i)}.$$

Данный подход формализует классическую идею К. Шеннона о «среднем объеме работы, необходимой для определения ключа», переводя ее на язык строгих вероятностных оценок. В отличие от энтропийных критериев, практическая секретность непосредственно измеряет стойкость ключа к атакам перебором с использованием всей доступной противнику информации о распределении ключей.

В контексте физических генераторов случайных чисел ключ формируется как последовательность знаков (символов), генерируемых устройством. Поэтому распределение ключа P_K полностью определяется совместным распределением выходных знаков ФГСЧ. В работе [14] предложена модель, в которой практическая секретность ключа полностью определяется параметром ε, задающим степень отклонения распределения отдельных знаков и их наборов от идеальной равновероятной схемы. При этом ε-представление позволяет получить достижимые и легко вычислимые оценки практической секретности без непосредственного анализа переборных алгоритмов.

Определение 1. Пусть $\gamma_1, \gamma_2, \ldots$ – случайные величины со значениями в $\{0,1,\ldots,m-1\}$.

Тогда через ε обозначим число, при котором для любого $k \in N$, любых попарно различных $t_1, t_2, \ldots, t_k \in N$ и любых $x_1, x_2, \ldots, x_k \in \{0,1,\ldots,m-1\}$ выполняется

$$\left(\frac{1}{m} - \varepsilon\right)^k \leq P(\gamma_{t_1} = x_1, \ldots, \gamma_{t_k} = x_k) \leq \left(\frac{1}{m} + \varepsilon\right)^k. \quad (1)$$

При $k = 1$ условие (1) означает, что каждое отдельное значение последовательности отклоняется от равномерного распределения не более чем на ε. При $k > 1$ оно ограничивает степень зависимости между элементами последовательности, не позволяя совместному распределению слишком сильно отличаться от произведения маргинальных.

3. ОЦЕНКА ВЛИЯНИЯ ДИСКРЕТИЗАЦИИ НА ПРАКТИЧЕСКУЮ СЕКРЕТНОСТЬ КЛЮЧЕЙ

Определение 2. Пусть $_i$, $i \in N$ – независимые неотрицательные одинаково распределенные случайные величины с плотностью $f(x)$. Через S_n, $n = 0,1,\ldots$, обозначим случайные величины

$$S_0 = 0,\ S_1 = \xi_1, \ldots, S_n = \sum_{i=1}^{n} \xi_i,$$

а через $\tau > 0$ – частоту регистрации сигнала.

Пусть $m \in N$, $m \geq 2$. Через γ_i обозначим случайные величины

$$\gamma_i = \left[\frac{S_i}{\tau}\right] \mod m,$$

где $i \in N$.

Значения γ_i называются «выходной последовательностью», полученной по схеме интервалов. Приведем пример ФГСЧ, построенного по схеме интервалов.

Пример 1: квантовый ФГСЧ на основе подсчета длительности интервалов времени до прилета фотона [3]. Рассмотрим ФГСЧ, работающий по следующему принципу. Источник испускает фотоны в моменты времени, являющиеся случайными величинами. Пусть ξ_n – время между испусканием $(n-1)$-го и n-го фотона. В соответствии с модельным предположением, случайные величины $\{\xi_n\}_{n=1}^{\infty}$

независимы, неотрицательны и одинаково распределены.

В момент регистрации n-го фотона считывается значение счетчика, который инкрементируется с фиксированной частотой $\tau > 0$. Формируемый знак равен младшему биту считанного значения, т.е.

$$\gamma_n = \left[\frac{S_n}{\tau}\right] \bmod 2,$$

где $S_n = \xi_1 + \ldots + \xi_n$ – момент прихода n-го фотона; $[x]$ – целая часть числа x. Таким образом, последовательность $\{\gamma_n\}$ формируется в точном соответствии со схемой интервалов (определение 2) при $m = 2$.

Для оценки сверху ε воспользуемся следующим замечанием.

Утверждение 1. Пусть $\gamma_1, \gamma_2, \ldots$ – случайные величины со значениями в $\{0,1,\ldots,m-1\}$. Условие (1) очевидным образом выполняется, если для любого $k \in N$, для любых попарно различных $t_1, t_2, \ldots, t_k \in N$, для любых $x_1 \in \{0,1,\ldots,m-1\}$,

$$\left| P(\gamma_{t_1} = x_1 \mid \gamma_{t_2} = x_2, \ldots, \gamma_{t_k} = x_k) - \frac{1}{m} \right| \le \varepsilon. \quad (2)$$

При $k = 1$ понимается безусловная вероятность, т.е. $P(\gamma_{t_1} = x_1)$.

Вместо рассмотрения условных вероятностей перейдем к условным математическим ожиданиям и изучим их существенные верхние грани.

Определение 3. Пусть ξ – случайная величина, заданная на вероятностном пространстве (Ω, F, P). Через $\operatorname{ess\,sup}\xi$ обозначим существенную верхнюю грань случайной величины ξ, т.е. такое число, что $P(\omega : \xi > \operatorname{ess\,sup}\xi) = 0$ и $P(\omega : \xi > \operatorname{ess\,sup}\xi - \varepsilon) > 0$ для любого $\varepsilon > 0$. Дальнейшая цель – получить оценки вида:

$$\operatorname{ess\,sup} \left| P(\gamma_{t_1} = x_1 \mid \gamma_{t_2}, \ldots, \gamma_{t_k}) - \frac{1}{m} \right| \le \varepsilon.$$

Тогда для любого набора значений $(x_2, \ldots, x_k)$, для которого множество $\{\omega : \gamma_{t_2}(\omega) = x_2, \ldots, \gamma_{t_k}(\omega) = x_k\}$ имеет положительную вероятность, почти наверное на этом множестве выполняется

$$\left| P(\gamma_{t_1} = x_1 \mid \gamma_{t_2} = x_2, \ldots, \gamma_{t_k} = x_k) - \frac{1}{m} \right| \le \varepsilon,$$

и, следовательно, будут получены оценки практической секретности ключей.

Справедлива следующая лемма.

Лемма 1 [15]. Пусть (Ω, F, P) вероятностное пространство и ξ – случайная величина на нем. Пусть $\mathcal{B}_1$, $\mathcal{B}_2$ – две σ-алгебры, такие что $\mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \mathcal{F}$:

$$\operatorname{ess\,sup} E(\xi \mid \mathcal{B}_1) \le \operatorname{ess\,sup} E(\xi \mid \mathcal{B}_2). \quad (3)$$

Из нее можно получить важное следствие: пусть γ_n, $n \in N$ – последовательность, полученная по схеме интервалов. Зафиксируем некоторые $n \in N$ и $r \in \{0,1,\ldots,m-1\}$.

Пусть $\mathcal{B}_1$, $\mathcal{B}_2$ – две σ-алгебры, такие что $\mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \mathcal{F}$:

$$\operatorname{ess\,sup} \left| P(\gamma_n = r \mid \mathcal{B}_1) - \frac{1}{m} \right| \le$$

$$\le \operatorname{ess\,sup} \left| P(\gamma_n = r \mid \mathcal{B}_2) - \frac{1}{m} \right|.$$

Доказательство. Обозначим через $\xi = I_{\{\gamma_n = r\}} - \frac{1}{m}$, где $I_{\{\gamma_n = r\}}$ – индикатор события $\{\gamma_n = r\}$. Тогда по определению условного математического ожидания:

$$P(\gamma_n = r \mid \mathcal{B}_1) - \frac{1}{m} = E(\xi \mid \mathcal{B}_1),$$

$$P(\gamma_n = r \mid \mathcal{B}_2) - \frac{1}{m} = E(\xi \mid \mathcal{B}_2).$$

Поскольку $\mathcal{B}_1 \subseteq \mathcal{B}_2$, по телескопическому свойству условных математических ожиданий имеем:

$$E(\xi \mid \mathcal{B}_1) = E(E(\xi \mid \mathcal{B}_2) \mid \mathcal{B}_1).$$

Для любой случайной величины η и σ-алгебры $\mathcal{B}$ выполняется неравенство $|E(\eta \mid \mathcal{B})| \le E(|\eta| \mid \mathcal{B})$ почти наверное (частный случай неравенства Йенсена для условного математического ожидания). Применяя его к $\eta = E(\xi \mid \mathcal{B}_2)$, получаем:

$$|E(\xi \mid \mathcal{B}_1)| = |E(E(\xi \mid \mathcal{B}_2) \mid \mathcal{B}_1)| \le$$

$$\le E(|E(\xi \mid \mathcal{B}_2)| \mid \mathcal{B}_1).$$

Пусть $C = \operatorname{ess\,sup} |E(\xi \mid \mathcal{B}_2)|$. По определению существенной верхней грани $|E(\xi \mid \mathcal{B}_2)| \le C$ почти наверное. Тогда, используя монотонность условного математического ожидания, имеем:

$$E(|E(\xi \mid \mathcal{B}_2)| \mid \mathcal{B}_1) \le E(C \mid \mathcal{B}_1) = C$$

почти наверное. Следовательно, $|E(\xi \mid \mathcal{B}_1)| \le C$ почти наверное.

Таким образом,

$$\operatorname{ess\,sup}\left|E\left(\xi \mid \mathcal{B}_1\right)\right| \le C = \\ = \operatorname{ess\,sup}\left|E\left(\xi \mid \mathcal{B}_2\right)\right|.$$

Возвращаясь к условным вероятностям, получаем требуемое неравенство.

Введем последовательность случайных величин $\theta_1,\theta_2,\ldots$ по следующему правилу:

$$\theta_i = \left\{\frac{S_i}{m\tau}\right\}, \qquad (4)$$

где $\{x\}$ – дробная часть числа x.

Заметим, что

$$\gamma_i = \left[m\theta_i\right], \qquad (5)$$

$i \in N$.

Действительно

$$\frac{S_n}{\tau} = \left[\frac{S_n}{m\tau}\right]m + \left\{\frac{S_n}{m\tau}\right\}m.$$

Выражение $\left[\frac{S_n}{m\tau}\right]m$ является целым числом кратным m, тогда

$$\gamma_i = \left[\frac{S_i}{\tau}\right] \mod m = \left[\left\{\frac{S_n}{m\tau}\right\}m\right] \\ \mod m = \left[m\theta_i\right] \mod m.$$

Но $m\theta_i \in \left[0,m\right)$, значит

$$\left[m\theta_i\right] \mod m = \left[m\theta_i\right].$$

Поскольку значения θ_i однозначно определяют значения γ_i, верно следующее включение:

$$\mathcal{B}_\gamma^{(n)} \subseteq \mathcal{B}_\theta^{(n)},$$

где $\mathcal{B}_\gamma^{(n)}$ – σ-алгебра, порожденная случайными величинами $\gamma_1,\ldots,\gamma_{n-2},\gamma_{n-1},\gamma_{n+1},\gamma_{n+2},\ldots$; $\mathcal{B}_\theta^{(n)}$ – σ-алгебра, порожденная случайными величинами $\theta_1,\theta_2,\ldots,\theta_{n-2},\theta_{n-1},\theta_{n+1},\theta_{n+2},\ldots$. Тогда по следствию 1 получаем, что

$$\sup_n \max_{r=0}^{m-1} \operatorname{ess\,sup}\left|P\left(\gamma_n = r \mid \gamma_1,\ldots,\gamma_{n-2},\gamma_{n-1},\gamma_{n+1},\gamma_{n+2},\ldots\right) - \frac{1}{m}\right| \le \\ \le \sup_n \max_{r=0}^{m-1} \operatorname{ess\,sup}\left|P\left(\left[m\theta_n\right] = r \mid \theta_1,\theta_2,\ldots,\theta_{n-2},\theta_{n-1},\theta_{n+1},\theta_{n+2},\ldots\right) - \frac{1}{m}\right|.$$

Докажем некоторые свойства последовательности θ_n, которые позволят оценить указанные условные вероятности.

Лемма 2. Случайные величины θ_n образуют цепь Маркова со значениями в $\left[0,1\right]$.

Доказательство. Возьмем произвольное измеримое множество $A \in \mathcal{B}\left(\left[0,1\right]\right)$, произвольные $n \in N$, $x_{n-1},x_{n-2},\ldots \in \left[0,1\right]$. Заметим, что

$$\theta_n - \theta_{n-1} = \left\{\frac{S_n}{m\tau}\right\} - \left\{\frac{S_{n-1}}{m\tau}\right\} = \left\{\frac{S_n - S_{n-1}}{m\tau}\right\} = \left\{\frac{\xi_n}{m\tau}\right\},$$

где под $\theta_n - \theta_{n-1}$ понимается вычитание по модулю 1. Тогда все разности $\theta_n - \theta_{n-1}$ независимы между собой, независимы с θ_i, $i < n$, и одинаково распределены. Следовательно

$$P\left(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n-2} = x_{n-2},\ldots\right) = \\ = P\left(\theta_n - \theta_{n-1} \in A - x_{n-1} \mid \theta_{n-1} = x_{n-1}, \theta_{n-2} = x_{n-2},\ldots\right) = \\ = P\left(\theta_n - \theta_{n-1} \in A - x_{n-1} \mid \theta_{n-1} = x_{n-1}\right) = \\ = P\left(\theta_n \in A \mid \theta_{n-1} = x_{n-1}\right).$$

Значит, последовательность θ_n, $n \in N$, действительно образует цепь Маркова и, следовательно, существует функция $p(s,x)$, такая что

$$P\left(\theta_n \in A \mid \theta_{n-1} = s\right) = \int_A p(s,x)dx,$$

для любого $n \in N$, $A \in \mathcal{B}\left(\left[0,1\right]\right)$, $s \in \left[0,1\right]$.

Неформально говоря, случайная величина θ_n характеризует «остаток» $\left\{\frac{S_n}{\tau}\right\}$, который влияет на подсчет длительности следующего интервала. При этом сами остатки образуют цепь Маркова – вероятность следующего интервала (и, следовательно, его остатка) зависит от значения предыдущего остатка и не зависит от более «старых» остатков.

Лемма 2 и формула (5) демонстрируют заявленную зависимость знаков выходной последовательности. Действительно, распределение знака γ_i определяется значением θ_i, которые зависимы между собой.

В силу марковского свойства для любого $n \in N$, любого $r \in \{0,1,\ldots,m-1\}$, любых $x_1, x_2, \ldots, x_{n-1} \in [0,1]$ выполнено

$$P([m\theta_n] = r \mid \theta_1 = x_1, \theta_2 = x_2, \ldots, \theta_{n-1} = x_{n-1}) = \\ = P([m\theta_n] = r \mid \theta_{n-1} = x_{n-1}).$$

Однако нужно искать вероятности при условии фиксации не только конечного «прошлого», но и бесконечного «будущего».

Лемма 3. Пусть $\{\theta_n\}_{n \in N}$ – цепь Маркова со значениями в $[0,1]$ с переходной плотностью $p(s,x)$. Тогда для любого $n \in N$, любого измеримого множества $A \subseteq [0,1]$, любого со события $B \in \mathcal{F}_{N \setminus \{n\}}$ и любых $x_{n-1}, x_{n+1} \in [0,1]$, таких что $P(B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) > 0$, справедливо равенство

$$P(\theta_n \in A \mid B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = P(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}).$$

Рассмотрим сначала случай, когда B – цилиндрическое множество, т.е. представимое в виде

$$B = \{\theta_1 \in B_1\} \cap \{\theta_2 \in B_2\} \cap \ldots \cap \{\theta_{n-1} \in B_{n-1}\} \cap \\ \cap \{\theta_{n+1} \in B_{n+1}\} \cap \ldots \cap \{\theta_{n+t} \in B_{n+t}\}, \quad (6)$$

где $t \in N$ и $B_1, \ldots, B_{n+t} \in \mathcal{B}([0,1])$.

Для такого B имеем:

$$P(\theta_n \in A, B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = \int_{B_1} \cdots \int_{B_{n-2}} \int_{A} \int_{B_{n+1}} \cdots \int_{B_{n+t}} f_{\theta_1}(z_1) \times \\ \times \prod_{i=2}^{n} p(z_{i-1}, z_i) \prod_{i=n}^{n+t} p(z_i, z_{i+1}) dz_{n+t} \cdots dz_{n+1} dz_n dz_{n-2} \cdots dz_1,$$

где $z_{n-1} = x_{n-1}$, $z_{n+1} = x_{n+1}$; f_{θ_1} – плотность распределения θ_1.

Заметим, что подынтегральное выражение факторизуется в произведение трех частей: часть, зависящая только от $z_1, \ldots, z_{n-2}$ и x_{n-1}; зависящая только от x_{n-1}, z_n, x_{n+1}: $p(x_{n-1}, z_n) p(z_n, x_{n+1})$; зависящая только от $x_{n+1}, z_{n+2}, \ldots, z_{n+t}$.

При интегрировании по $z_1, \ldots, z_{n-2}$ и $z_{n+2}, \ldots, z_{n+t}$ получаем множители, не зависящие от z_n. Поэтому

$$P(\theta_n \in A, B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = C_1(x_{n-1}) \int_A p(x_{n-1}, z_n) p(z_n, x_{n+1}) dz_n C_2(x_{n+1}),$$

где $C_1(x_{n-1})$ и $C_2(x_{n+1})$ – некоторые константы (зависящие от B и x_{n-1}, x_{n+1}, но не от A). Аналогично,

$$P(B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = C_1(x_{n-1}) \int_0^1 p(x_{n-1}, z_n) p(z_n, x_{n+1}) dz_n C_2(x_{n+1}).$$

Следовательно,

$$P(\theta_n \in A \mid B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = \frac{\int_A p(x_{n-1}, z_n) p(z_n, x_{n+1}) dz_n}{\int_0^1 p(x_{n-1}, z_n) p(z_n, x_{n+1}) dz_n},$$

что совпадает с $P(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1})$.

Таким образом, утверждение леммы доказано для всех цилиндрических множеств B (образующих π-систему в P).

Теперь докажем, что класс L всех множеств $B \in \mathcal{F}_{N \setminus \{n\}}$, для которых или выполняется утверждение леммы, или B имеет нулевую вероятность $P(B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = 0$, является λ-системой.

Проверим свойства λ-системы:

1. $\Omega \in \mathcal{L}$, так как $P(\Omega, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) > 0$ и утверждение леммы для $B = \Omega$ тривиально выполняется.

2. Пусть $B_1, B_2 \in \mathcal{L}$ и $B_1 \subseteq B_2$. Рассмотрим три случая. Если $P(B_2 \setminus B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = 0$, то $B_2 \setminus B_1 \in \mathcal{L}$ по определению. Если $P(B_2) > 0$, а $P(B_1) = 0$, то очевидно, что $B_2 \setminus B_1 \in \mathcal{L}$. Пусть теперь $P(B_2, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) > 0$ и $P(B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) > 0$. Тогда

$$P(\theta_n \in A, B_2 \setminus B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = P(\theta_n \in A, B_2, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) - \\ - P(\theta_n \in A, B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = P(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) \times \\ \times \left(P(B_2, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) - \right. \\ \left. - P(B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) \right).$$

Аналогично

$$P(B_2 \setminus B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) = \\ = P(B_2, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}) - \\ - P(B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}).$$

Следовательно,

$$P\left(\theta_n \in A \mid B_2 \setminus B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) =$$
$$= \frac{P\left(\theta_n \in A, B_2 \setminus B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right)}{P\left(B_2 \setminus B_1, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right)} =$$
$$= P\left(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right).$$

Значит, $B_2 \setminus B_1 \in \mathcal{L}$.

3. Пусть $B_k \in \mathcal{L}$, $k \geq 1$, и $B_k \uparrow B$. Рассмотрим два случая. Если $P\left(B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) = 0$, то $B \in \mathcal{L}$ по определению.

Если $P\left(B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) > 0$, то найдется k_0 такое, что $P\left(B_{k_0}, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) > 0$. По непрерывности вероятности:

$$P\left(\theta_n \in A \mid B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) =$$
$$= \lim_{k\to\infty} P\left(\theta_n \in A \mid B_k, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) =$$
$$= \lim_{k\to\infty} P\left(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) =$$
$$= P\left(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right).$$

Значит, $B \in \mathcal{L}$.

Таким образом, L – λ-система, содержащая π-систему P цилиндрических множеств. По теореме о $\pi - \lambda$ системах [16, С. 205, теорема 2], $\sigma(\mathcal{P}) \subseteq \mathcal{L}$. Но $\sigma(\mathcal{P}) = \mathcal{F}_{N\setminus\{n\}}$.

Следовательно, для любого $B \in \mathcal{F}_{N\setminus\{n\}}$, если $P\left(B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) > 0$, то

$$P\left(\theta_n \in A \mid B, \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right) =$$
$$= P\left(\theta_n \in A \mid \theta_{n-1} = x_{n-1}, \theta_{n+1} = x_{n+1}\right).$$

Таким образом, оценка практической секретности сводится к оценке выражения

$$\sup_n \max_{r=0}^{m-1} \sup_{x,y\in[0,1]} \left| P\left([m\theta_n] = r \mid \theta_{n-1} = x, \theta_{n+1} = y\right) - \frac{1}{m} \right|.$$

Справедлива следующая лемма.

Лемма 4. Пусть функция $f(x)$ из определения 2 является ограниченной, дифференцируемой на $(0,\infty)$ и $f(x)$ имеет на $(0,\infty)$ ограниченную вариацию. Тогда

$$\sup_{x,y\in[0,1]} \left| p(x,y) - 1 \right| \leq m\tau Var_f,$$

где

$$Var_f = \sup_{0=t_0<t_1<\ldots} \sum_{k\geq 1} \left| f(t_k) - f(t_{k-1}) \right|.$$

Доказательство. Заметим, что из определения случайных величин θ_n следует равенство

$$p(x,y) = p(0, \{y - x\}),$$

где под $\{x\}$ понимается дробная часть числа x. Значит для доказательства леммы достаточно рассмотреть случай $x = 0$.

Заметим, что плотность случайной величины θ_1 равна $p(0,y)$. Выведем формулу

$$p(0,y) = \frac{d}{dy} P\left(\theta_1 \leq y\right) = \frac{d}{dy} P\left(\left\{\frac{\xi_1}{m\tau}\right\} \leq y\right) =$$
$$= \frac{d}{dy} \sum_{k=0}^{\infty} P\left(k < \frac{\xi_1}{m\tau} \leq k + y\right) =$$
$$= \frac{d}{dy}\left[\sum_{k=0}^{\infty} P\left(\frac{\xi_1}{m\tau} \leq k + y\right) - \sum_{k=0}^{\infty} P\left(\frac{\xi_1}{m\tau} < k\right)\right] =$$
$$= m\tau \sum_{k=0}^{\infty} f(m\tau(y+k)).$$

Тогда для любого $z \in [0,1]$

$$\left|p(0,y) - p(0,z)\right| \leq$$
$$\leq m\tau \left| \sum_{k=0}^{\infty} f(m\tau(y+k)) - \sum_{k=0}^{\infty} f(m\tau(z+k)) \right| \leq$$
$$\leq m\tau \sum_{k=0}^{\infty} \left| f(m\tau(y+k)) - f(m\tau(z+k)) \right| \leq m\tau Var_f.$$

Кроме того

$$1 = \int_0^1 p(0,z)dz = \int_0^1 \left(p(0,z) - p(0,y) + p(0,y)\right)dz \leq$$
$$\leq \int_0^1 p(0,y)dz + m\tau Var_f = p(0,y) + m\tau Var_f.$$

Значит, $p(0,y) \geq 1 - m\tau Var_f$. Аналогично доказывается, что $p(0,y) \leq 1 + m\tau Var_f$.

Теорема 1. Пусть в терминах определения 2 функция $f(x)$ является ограниченной, дифференцируемой на $(0,\infty)$, и $f(x)$ имеет на $(0,\infty)$ ограниченную вариацию Var_f, причем $m\tau Var_f < 1$. Тогда

$$\sup_n \max_{r=0}^{m-1} \operatorname{ess\,sup} \left| P\left(\gamma_n = r \mid \gamma_1, \ldots, \gamma_{n-1}, \gamma_{n+1}, \ldots\right) - \right.$$
$$\left. - \frac{1}{m} \right| \leq \frac{4\tau Var_f}{(1 - m\tau Var_f)^2}.$$

Доказательство. Из следствия 1 и леммы 3 следует, что

$$\sup_n \max_{r=0}^{m-1} \operatorname{ess\,sup} \left| P(\gamma_n = r | \gamma_1, \ldots, \gamma_{n-1}, \gamma_{n+1}, \ldots) - \frac{1}{m} \right| \le$$

$$\le \sup_n \max_{r=0}^{m-1} \sup_{x,y \in [0,1]} \left| P([m\theta_n] = r | \theta_{n-1} = x, \theta_{n+1} = y) - \frac{1}{m} \right|.$$

Из доказательства леммы 3 имеем:

$$P\left([m\theta_n] = r \mid \theta_{n-1} = x, \theta_{n+1} = y\right) =$$

$$= \frac{\int_{r/m}^{(r+1)/m} p(x,s)p(s,y)ds}{\int_0^1 p(x,z)p(z,y)dz}.$$

Из леммы 4 следует, что для любых $s, x, y \in [0,1]$ выполняется

$$1 - m\tau Var_f \le p(x,s), p(s,y) \le 1 + m\tau Var_f.$$

Используя эти оценки, получаем верхнюю границу для числителя:

$$\int_{r/m}^{(r+1)/m} p(x,s)p(s,y)ds \le \frac{1}{m}(1 + m\tau Var_f)^2,$$

и нижнюю границу для знаменателя:

$$\int_0^1 p(x,z)p(z,y)dz \ge (1 - m\tau Var_f)^2.$$

Следовательно,

$$P\left([m\theta_n] = r | \theta_{n-1} = x, \theta_{n+1} = y\right) \le \frac{(1 + m\tau Var_f)^2}{m(1 - m\tau Var_f)^2}.$$

Аналогично получаем нижнюю оценку:

$$P\left([m\theta_n] = r | \theta_{n-1} = x, \theta_{n+1} = y\right) \ge \frac{(1 - m\tau Var_f)^2}{m(1 + m\tau Var_f)^2}.$$

Таким образом,

$$\left| P\left([m\theta_n] = r | \theta_{n-1} = x, \theta_{n+1} = y\right) - \frac{1}{m} \right| \le$$

$$\le \max\left\{ \frac{(1 + m\tau Var_f)^2}{m(1 - m\tau Var_f)^2} - \frac{1}{m}, \frac{1}{m} - \frac{(1 - m\tau Var_f)^2}{m(1 + m\tau Var_f)^2} \right\}.$$

Обозначим $x = m\tau Var_f$, где $0 < x < 1$. Рассмотрим два отклонения:

$$A = \frac{(1+x)^2}{m(1-x)^2} - \frac{1}{m}, \quad B = \frac{1}{m} - \frac{(1-x)^2}{m(1+x)^2}.$$

Умножим оба выражения на m:

$$mA = \frac{(1+x)^2}{(1-x)^2} - 1, \quad mB = 1 - \frac{(1-x)^2}{(1+x)^2}.$$

Вычислим

$$mA = \frac{(1+x)^2 - (1-x)^2}{(1-x)^2} = \frac{4x}{(1-x)^2}$$

и

$$mB = \frac{(1+x)^2 - (1-x)^2}{(1+x)^2} = \frac{4x}{(1+x)^2}.$$

Поскольку $(1-x)^2 < (1+x)^2$ при $0 < x < 1$, то $mA > mB$, а значит $A > B$. Следовательно, максимум достигается на первом выражении.

Возвращаясь к A, получаем:

$$A = \frac{1}{m} \cdot \frac{4x}{(1-x)^2} = \frac{4m\tau Var_f}{m(1 - m\tau Var_f)^2} = \frac{4\tau Var_f}{(1 - m\tau Var_f)^2}.$$

Таким образом,

$$\sup_n \max_{r=0}^{m-1} \operatorname{ess\,sup} \left| P(\gamma_n = r | \gamma_1, \ldots, \gamma_{n-1}, \gamma_{n+1}, \ldots) - \right.$$

$$\left. - \frac{1}{m} \right| \le \frac{4\tau Var_f}{(1 - m\tau Var_f)^2}.$$

Пример 2. В соответствии с модельными предположениями работы [17] время до прилета n-го фотона есть случайная величина ξ_n, причем случайные величины ξ_i, $i = 1, 2, \ldots$, являются независимыми, неотрицательными и одинаково распределенными с экспоненциальным распределением $Exp(\lambda)$, где параметр λ определяется из характеристик лазера, испускающего фотоны.

Пусть параметр m из определения 2 равен двум. Для экспоненциального распределения $Exp(\lambda)$ плотность $f(x) = \lambda e^{-\lambda x}$ является убывающей функцией на $(0, \infty)$, поэтому ее полная вариация равна $Var_f = \lambda$. Для обеспечения выполнения условия теоремы 1 $m\tau Var_f = 2\tau\lambda < 1$ необходимо соответствующим образом подбирать параметры τ и λ (см. таблицу). Приведем оценки параметра ε для различных значений λ и τ, рассчитанные по формуле из теоремы 1:

$$\varepsilon \le \frac{4\tau\lambda}{(1 - 2\tau\lambda)^2}.$$

Все представленные комбинации параметров удовлетворяют условию $2\tau\lambda < 1$,

Оценки на ε при различных значениях параметра λ и τ для $m=2$, вычисленные по формуле $\varepsilon \leqslant 4\tau\lambda/(1-2\tau\lambda)^2$

Estimates for ε at different values of the parameter λ and τ for $m = 2$, , calculated by the formula $\varepsilon \leq 4\tau\lambda/(1-2\tau\lambda)^2$

λ\τ	0,05	0,01	0,0065	10^{-4}
0,25	$5{,}27\cdot10^{-2}$	$1{,}01\cdot10^{-2}$	$6{,}54\cdot10^{-3}$	$1{,}00\cdot10^{-4}$
0,5	$1{,}11\cdot10^{-1}$	$2{,}04\cdot10^{-2}$	$1{,}32\cdot10^{-2}$	$2{,}00\cdot10^{-4}$
1	$2{,}47\cdot10^{-1}$	$4{,}17\cdot10^{-2}$	$2{,}69\cdot10^{-2}$	$4{,}00\cdot10^{-4}$

а полученные оценки ε не превышают 0,247. Наибольшее значение $\varepsilon \approx 0{,}247$ соответствует $\lambda = 1$, $\tau = 0{,}05$ $(2\tau\lambda = 0{,}1)$. Как видно из таблицы, уменьшение τ приводит к существенному снижению оценки ε. Например, при $\tau = 10^{-4}$ даже для $\lambda = 1$ получаем $\varepsilon \approx 4 \cdot 10^{-4}$, что свидетельствует о высокой практической секретности ключа.

4. ЗАКЛЮЧЕНИЕ

Предложен подход к оценке практической секретности ключей, формируемых по схеме интервалов с учетом дискретизации времени. Основной результат заключается в сведении исходной криптографической задачи к анализу цепи Маркова, образованной остатками от деления накопленных интервалов времени.

Доказано, что для случайных величин с ограниченной вариацией плотности распределения величина ε может быть сделана сколь угодно малой за счет увеличения частоты регистрации сигнала τ. Представленный пример с экспоненциальным распределением демонстрирует работоспособность подхода и позволяет получить конкретные численные оценки.

Полученные оценки позволяют количественно обосновать требования к параметрам ФГСЧ (частота дискретизации τ и параметры распределения ξ_i) для достижения заданного уровня практической секретности, что является важным шагом на пути к стандартизуемому и верифицируемому проектированию подобных устройств [6, 10].

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Автор заявляет об отсутствии конфликта интересов / The author declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. **Богданов Д. С., Логачев А. С., Миронкин В. О.** Теоретико-вероятностные модели физических генераторов случайных чисел // Проблемы информационной безопасности. Компьютерные системы. 2024. Т. 61. № 3. С. 9–19.
2. **Killmann W., Schindler W.** A Design for a Physical RNG with Robust Entropy Estimators // Cryptographic Hardware and Embedded Systems–CHES 2008: 10th International Workshop, 10–13 August 2008, Washington, DC, USA. 2008. P. 146–163.
3. **Dynes J. F., Yuan Z. L., Sharpe A. W., Shields A. J.** A High Speed, Post-Processing Free, Quantum Random Number Generator // Applied Physics Letters. 2008. Vol. 93. № 3. P. 031109.
4. **Stipcevic M., Rogina B. M.** Quantum random number generator based on photonic emission in semiconductors // Rev. Sci. Instrum. 2007. Vol. 78. P. 1–7.
5. **Nie Y.-Q., Zhang H.-F., Zhang Z. et al.** Practical and fast quantum random number

generation based on photon arrival time relative to external reference // Applied Physics Letters. 2014. Vol. 104. № 5. P. 051110.
6. **Turan M. S., Barker E., Kelsey J. et al.** Recommendation for the Entropy Sources Used for Random Bit Generation // NIST Special Publication (SP) 800-90B. 2018. 84 p.
7. **Killmann W., Schindler W.** A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators // Bundesamt für Sicherheit in der Informationstechnik (BSI). 2002. 38 p.
8. **Marangon D. G., Vallone G., Villoresi P.** Source-Device-Independent Ultrafast Quantum Random Number Generation // Physical Review Letters. 2017. Vol. 118. P. 060503.
9. **Saini A., Tsokanos A., Kirner R.** Quantum randomness in cryptography – a survey of cryptosystems, RNG-based ciphers, and QRNGs // Information. 2022. Vol. 13. № 8. P. 358.
10. **Sunar B., Martin W. J., Stinson D. R.** A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks // IEEE Transactions on Computers. 2019. Vol. 56. № 1. P. 109–119.
11. **Арбеков И. М.** Элементарная квантовая криптография: для криптографов, не знакомых с квантовой механикой. М. : URSS, 2022. 168 с.
12. **Арбеков И. М.** Критерии секретности ключа // Математические вопросы криптографии. 2016. Т. 7. № 1. С. 39–56.
13. **Arbekov I. M.** Lower bounds for the practical secrecy of a key // Mathematical Questions of Cryptography. 2017. Vol. 8. № 2. P. 29–38.
14. **Логачев А. С., Миронкин В. О**. О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа // Прикладная дискретная математика. 2024. Т. 65. С. 66–83.
15. **Богданов Д. С.** О практической секретности ключей, формируемых из мгновенных значений стационарного гауссовского процесса // Предварительные материалы конференции «CTCrypt 2025». 2025. С. 170–183.
16. **Ширяев А. Н.** Вероятность. В 2-х кн. 7-е изд., стер. М. : МЦНМО, 2021. 416 с.
17. **Furst M., Weier H., Nauerth S. et al.** High speed optical quantum random number generation // Optics Express. 2010. Vol. 18. № 12. P. 13029–13037.

REFERENCES

1. **Bogdanov D. S., Logachev A. S., Mironkin V. O.** The probabilitic-theoretic models of physical random number generators. *Problems of information security. Computer systems*. 2024. No. 3, pp. 9–19. DOI: 10.48612/jisp/m3bn-24ap-6tn8. (In Russian)
2. **Killmann W., Schindler W.** A Design for a Physical RNG with Robust Entropy Estimators. Cryptographic Hardware and Embedded Systems–CHES 2008: 10th International Workshop, 10–13 August 2008, Washington, DC, USA. 2008, pp. 146–163.
3. **Dynes J. F., Yuan Z. L., Sharpe A. W., Shields A. J.** A High Speed, Post-Processing Free, Quantum Random Number Generator. *Applied Physics Letters*. 2008. Vol. 93. No. 3, pp. 031109.
4. **Stipcevic M., Rogina B. M.** Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum*. 2007. Vol. 78, pp. 1–7.
5. **Nie Y.-Q., Zhang H.-F., Zhang Z. et al.** Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Applied Physics Letters*. 2014. Vol. 104. No. 5, pp. 051110.
6. **Turan M. S., Barker E., Kelsey J. et al.** Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication (SP) 800-90B. 2018, 84 p.
7. **Killmann W., Schindler W.** A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators. Bundesamt für Sicherheit in der Informationstechnik (BSI). 2002, 38 p.
8. **Marangon D. G., Vallone G., Villoresi P.** Source-Device-Independent Ultrafast Quantum Random Number Generation. *Physical Review Letters*. 2017. Vol. 118, pp. 060503.
9. **Saini A., Tsokanos A., Kirner R.** Quantum randomness in cryptography – a survey of cryptosystems, RNG-based ciphers, and

QRNGs. *Information*. 2022. Vol. 13. No. 8, pp. 358.
10. **Sunar B., Martin W. J., Stinson D. R.** A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks. *IEEE Transactions on Computers*. 2019. Vol. 56. No. 1, pp. 109–119.
11. **Arbekov I. M.** Elementary Quantum Cryptography: for Cryptographers Unfamiliar with Quantum Mechanics. Moscow : URSS, 2022, 168 p. (In Russian)
12. **Arbekov I. M.** Key secrecy criteria. *Mathematical Questions of Cryptography*. 2016. Vol. 7. No. 1, pp. 39–56. (In Russian)
13. **Arbekov I. M.** Lower bounds for the practical secrecy of a key. Mathematical Questions of Cryptography. 2017. Vol. 8. No. 2, pp. 29–38.
14. **Logachev A. S., Mironkin V. O.** On the influence of probabilistic characteristics of discrete sources forming cryptographic keys on the practical secrecy of a key. *Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics)*. 2024. Vol. 65, pp. 66–83. (In Russian)
15. **Bogdanov D. S.** On the practical secrecy of keys generated from instantaneous values of a stationary Gaussian process. Preliminary materials of the conference “CTCrypt 2025”. 2025, pp. 170–183. (In Russian)
16. **Shiryaev A. N.** Probability. In 2 books. 7th ed., stereotype. Moscow: MCNMO, 2021, 416 p. (In Russian)
17. **Furst M., Weier H., Nauerth S. et al.** High speed optical quantum random number generation. *Optics Express*. 2010. Vol. 18. No. 12, pp. 13029–13037.

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT AUTHOR

БОГДАНОВ Дмитрий Сергеевич – преподаватель, Национальный исследовательский университет «Высшая школа экономики», Россия, 109028, Москва, Покровский бульвар, д.11
E-mail: bogdanovds@rambler.ru
ORCID: 0000-0001-6178-6420

BOGDANOV Dmitry S. – Lecturer, National Research University Higher School of Economics, Russia, 109028, Moscow, Pokrovksy Bulvar, 11