# ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ СИСТЕМ
## INFORMATION PROTECTION AND SYSTEM RELIABILITY



УДК 004.312
DOI: 10.37661/1816-0301-2025-22-4-65-81

*Оригинальная статья*
*Original Article*

# Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого осциллятора

**А. А. Иванюк✉, Л. А. Бурко**

*Белорусский государственный университет информатики и радиоэлектроники,*
*ул. П. Бровки, 6, 220013, Минск, Беларусь*
✉*E-mail: ivaniuk@bsuir.by*

**Аннотация**

Цели. Целью работы является рассмотрение особенностей функционирования цифровой схемы, анализирующей частоту выходного сигнала конфигурируемого кольцевого осциллятора в пределах фиксированного окна измерения.

Методы. Используются методы синтеза и анализа цифровых устройств, в том числе на программируемых логических интегральных схемах (ПЛИС), основы цифровой схемотехники, методы анализа случайных нормально распределенных величин.

Результаты. Разработана цифровая схема регистрации периода конфигурируемого кольцевого осциллятора в зависимости от временного окна измерения и значения его конфигурации. Проведены экспериментальные исследования периодов вырабатываемых сигналов при реализации разработанной схемы на программируемых логических интегральных схемах FPGA Xilinx ZYNQ 7000. Показано, что при многократном повторении измерения периода для регистрирующего счетчика можно выделить три группы разрядов: группу $G_2$ стабильных разрядов, значения которых остаются неизменными на протяжении всех измерений; группу $G_1$ слабо стабильных разрядов, искажения которых незначительны, и группу $G_0$ сильно нестабильных разрядов, вероятность искажения которых от измерения к измерению близка к 1. Было выдвинуто предположение, что группа разрядов $G_0$ представляет собой оцифрованные значения шумовой составляющей значения измеряемого периода. Предполагается, что в силу наличия многих независимых компонентов схем конфигурируемого кольцевого осциллятора и цифрового регистратора, девиаций питающего напряжения, температуры кристалла и окружающей среды, ошибок квантования и др. данная шумовая составляющая нормально распределена. Аналитически было доказано, что нормально распределенная величина, квантованная многоразрядными двоичными числами, при определенных значениях математического ожидания $\mu$ и среднеквадратического отклонения $\sigma$ порождает только две группы – $G_2$ и $G_0$. Доказано, что вероятность появления единичного символа на всех разрядах группы $G_0$ близка к 0,5, а размерность группы можно оценить как $3+\lfloor \log_2 \sigma \rfloor$. Разряды группы $G_1$ можно привести к группе $G_2$ различными

способами, в том числе методом максимального правдоподобия либо нормализацией значения каждого измерения до теоретически обоснованного разделения на группы $G_2$ и $G_0$. Значения разрядов группы $G_2$ можно интерпретировать как детерминированный ответ на запрос, представляющий собой конфигурацию схемы кольцевого осциллятора в заданном окне измерения, формируя новый тип многоразрядных физически неклонируемых функций, обладающих высокой стабильностью. В свою очередь, разряды $G_0$ могут быть использованы как однобитные источники случайных величин, распределение которых близко к равномерному, формируя основу для построения генераторов случайных чисел.
Заключение. Полученные результаты могут быть применены во встроенных средствах обеспечения неклонируемой идентификации цифровых систем и генерации случайных данных. Применение синхронного двоичного счетчика в качестве схемы регистратора частоты конфигурируемого кольцевого осциллятора открывает новые возможности для построения многоразрядных схем физически неклонируемых функций с улучшенными показателями стабильности, уникальности и случайности.

**Ключевые слова:** физическая криптография, физически неклонируемые функции, конфигурируемый кольцевой осциллятор, стабильная идентификация, генерация случайных данных

**Благодарности.** Авторы выражают искреннюю благодарность резиденту ПВТ компании «Инженерный Центр Ядро», которая является одним из центров разработки YADRO, за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

**Для цитирования.** Иванюк, А. А. Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого осциллятора / А. А. Иванюк, Л. А. Бурко // Информатика. – 2025. – Т. 22, № 4. – С. 65–81. – DOI: 10.37661/1816-0301-2025-22-4-65-81.

**Конфликт интересов.** Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 22.09.2025
Подписана в печать | Accepted 13.10.2025
Опубликована | Published 30.12.2025

# Generation of deterministic identifiers and random numbers using a configurable ring oscillator circuit

**Alexander A. Ivaniuk✉, Liana A. Burko**

*Belarusian State University of Informatics and Radioelectronics, st. P. Brovki, 6, Minsk, 220013, Belarus*
✉*E-mail: ivaniuk@bsuir.by*

**Abstract**
Objectives. The purpose of the study is to examine the operational characteristics of a digital circuit designed to analyze the output signal frequency of a configurable ring oscillator within a fixed measurement window.
Methods. Methods of digital device synthesis and analysis were employed, including implementation on programmable logic integrated circuits (FPGAs), fundamentals of digital circuit design, and methods for analyzing normally distributed random variables.
Results. A digital circuit for recording the period of a configurable ring oscillator, depending on the measurement time window and the value of its configuration has been developed. Experimental studies of the generated signal periods were conducted using Xilinx ZYNQ 7000 series FPGAs. It was demonstrated that upon repeated period measurements the bits of the recording counter can be categorized into three groups: group $G_2$: stable bits retaining constant values across all measurements; group $G_1$: weakly stable bits exhibiting minor distortions; group $G_0$: strongly unstable bits with a distortion probability approaching 1 between measurements. It was hypothesized that group $G_0$ represents the digitized noise component of the measured period value. Due to numerous independent factors (components within the configurable ring oscillator and digital recorder, supply voltage deviations, die and ambient temperature variations, quantization errors, etc.), it is assumed that this noise component follows a normal

distribution. Analytical proof established that a normally distributed variable, quantized using multi-bit binary numbers under specific values of mathematical expectation $\mu$ and standard deviation $\sigma$, generates only two groups: $G_2$ and $G_0$. It was proven that the probability of a '1' appearing in any bit of group $G_0$ approaches 0,5, and the group size can be estimated as $3+\lfloor \log_2 \sigma \rfloor$. The bits of group $G_1$ can be converted to group $G_2$ using various methods, such as maximum likelihood estimation or by normalizing each measurement value to a theoretically justified separation into $G_2$ and $G_0$. The values of group $G_2$ bits can be interpreted as a response to a challenge defined by the ring oscillator circuit configuration and measurement window, forming a novel type of multi-bit Physical Unclonable Function (PUF) characterized by high stability. Conversely, the $G_0$ bits can serve as single-bit sources of random variables with near-uniform distribution, providing a foundation for building random number generators.

Conclusion. The obtained results can be utilized in embedded systems for providing unclonable identification of digital devices and for random data generation. The application of a synchronous binary counter as a frequency recording circuit for a configurable ring oscillator opens new avenues for designing multibit physical unclonable function architectures with enhanced performance metrics in terms of stability, uniqueness, and randomness.

**Keywords:** physical cryptography, physically unclonable functions, configurable ring oscillator, stable identification, random numbers generation

**Acknowledgments.** The authors sincerely thank "Engineering Center Yadro" (a resident of the Belarus High-Tech Park / HTP and an R&D center within the YADRO Group) for providing the experimental equipment used in this work through our joint educational laboratory with the Belarusian State University of Informatics and Radioelectronics.

**For citation.** Ivaniuk A. A., Burko L. A. *Generation of deterministic identifiers and random numbers using a configurable ring oscillator circuit*. Informatika [*Informatics*], 2025, vol. 22, no. 4, pp. 65–81 (In Russ.). DOI: 10.37661/1816-0301-2025-22-4-65-81.

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

**Введение.** Цифровые физически неклонируемые функции (ФНФ) [1–3], составляющие основу современной аппаратной криптографии, лежат в основе методов уникальной идентификации, аутентификации, защиты от клонирования и генерации случайных чисел и по-прежнему находятся в фокусе внимания как проектировщиков, так и исследователей. Среди большого разнообразия видов схем ФНФ выделяются схемы типа «Арбитр» [4, 5] и ФНФ кольцевых осцилляторов (КО) [6], основные характеристики которых наряду с простотой реализации привлекают разработчиков защищенных цифровых устройств. Данные типы ФНФ основаны на сравнении задержек распространения сигналов по симметричным путям, уникально выбираемым по поступающему запросу *CH*. По результату сравнения формируется бинарный ответ *R*, а сами схемы реализуют функцию вида $R = PUF(CH)$. Все множество пар «запрос – ответ» является уникальным, неклонируемым, непредсказуемым и случайным, что характеризует конкретный воплощенный в кремнии экземпляр схемы ФНФ.

Развитием классической архитектуры ФНФ КО являются схемы, основанные на применении конфигурируемых кольцевых осцилляторов (ККО) [7–12]. Это дает возможность извлекать уникальность не только по результату сравнения частот, выбранных из реализованного множества КО, но и из каждой схемы КО путем конфигурации внутренних путей прохождения сигнала. Данная особенность позволяет применять ФНФ КО как для заказных СБИС, так и для ПЛИС, обеспечивая для последних приемлемые показатели стабильности, надежности, случайности и внутрикристальной уникальности [10]. Компактность схем ФНФ ККО наряду с расширенными возможностями извлечения уникальных признаков делает их перспективными для дальнейших исследований и реализации на различных технологиях.

Одним из основных блоков цифровых схем ФНФ КО и ККО является блок измерения частоты выбранного осциллятора. Как правило, такие блоки представляют собой синхронные двоичные счетчики, регистрирующие число фронтов генерируемого КО сигнала в фиксированном временном окне *MW*. В классической схеме ФНФ КО по определенному запросу *CH* выбирается пара осцилляторов из множества имеющихся, для которых производятся измерения, а их результаты сравниваются между собой, формируя бинарный ответ *R* всей схемы ФНФ. В схеме ФНФ ККО,

помимо воспроизведения более компактной версии ФНФ КО [9], запросом могут выступать значение конфигурации *CF* самой схемы и размер временного окна измерения *MW*, при этом многоразрядный результат измерения числа фронтов является уникальным ответом. В данном случае схема реализует функцию вида $\boldsymbol{R} = PUF(CF, MW)$. В силу многих факторов получаемое значение $\boldsymbol{R}$ является нестабильным, что проявляется при повторяющихся измерениях с одними и теми же значениями *CF* и *MW* и негативно сказывается на таких характеристиках ФНФ, как надежность и стабильность [13, 14].

Настоящая статья посвящена исследованию поведения регистрирующего счетчика ФНФ ККО с целью выделения группы стабильных разрядов, значения которых в дальнейшем могут быть применены для повышения надежности ответов ФНФ (например, для генерации детерминированных идентификаторов), и группы нестабильных (шумовых) разрядов, которые могут стать основой для генерации случайных чисел.

**Схема конфигурируемого кольцевого осциллятора.** Объектом исследования является схема, состоящая из ККО и регистратора количества передних фронтов, сгенерированных ККО в фиксированном временном окне измерения *MW*. Период вырабатываемого сигнала зависит от управляемых и неуправляемых (случайных) факторов. Управляемым фактором является конфигурация ККО, задаваемая значением на многоразрядной входной шине *CF*. К неуправляемым факторам можно отнести уникальные задержки сигналов на структурных элементах ККО, зависящие от технологии изготовления, девиации уровня питающего напряжения, температуры кристалла и т. п. [15]. В совокупности это приводит к неуправляемым случайным разбросам фронтов генерируемых сигналов [16], что можно наблюдать на многоразрядном выходе схемы регистратора. При этом многократно регистрируемое значение числа фронтов при фиксированных *MW* и *CF* можно представить как сумму постоянной и случайной (шумовой) составляющей, к которой в том числе можно отнести несовершенство схемы регистратора, порождающей шум квантования. Если в качестве схемы регистратора использовать синхронный многоразрядный ($N=C+L$ разрядов) двоичный счетчик с разрешением, то по окончании измерения старшая часть разрядов *C* будет характеризовать постоянную составляющую результата измерения $R_{id}$, а младшая часть разрядов *L* – шумовую составляющую $R_{rnd}$ (рис. 1).

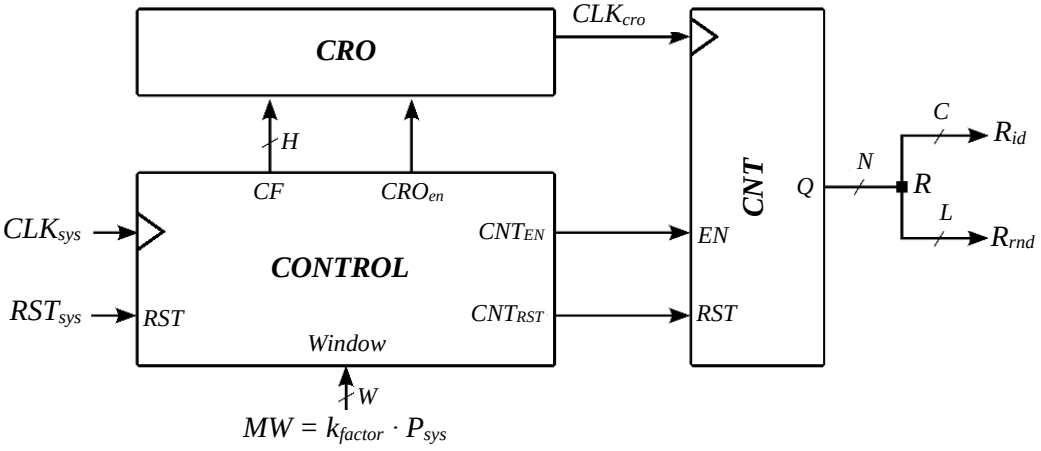


Рис. 1. Структурная схема измерения сигналов ККО

*Fig. 1. Block diagram of the CRO signal measurement*

В общем случае регистрация числа фронтов выполняется в следующей последовательности: сначала на устройство управления *CONTROL* по *W*-разрядной шине подается значение желаемого окна измерения *MW*, далее выбранным значением *CF* конфигурируется схема ККО (configurable ring oscillator, CRO) одной из $2^H$ возможных конфигураций, после чего схема переходит в режим генерирования периодического сигнала $CLK_{cro}$, который подается на вход синхронизации двоичного счетчика *CNT* (Counter). Сигналы разрешения функционирования ККО $CRO_{en}$ и счетчика $CNT_{en}$ являются активными на протяжении всего временного окна измерения, по

окончании которого значение $R$ на счетчике равно числу зарегистрированных фронтов сигнала $CLK_{cro}$. При многократном измерении в значениях $\boldsymbol{R}$ можно выделить старшие разряды $R_{id}$ со стабильными значениями и младшие разряды $R_{rnd}$ с нестабильными оцифрованными значениями шумовой составляющей. Таким образом, предложенная схема может выполнять роль двух схем: ФНФ с многоразрядным ответом $R_{id} = PUF(CF, MW)$, обладающей достаточно высоким уровнем стабильности, и ФНФ, выполняющей роль генератора случайных чисел $R_{rnd} = PUF(CF, MW)$.

Покажем на практике, что подобным свойством обладают схемы ККО, реализованные на ПЛИС типа FPGA, а шумовая составляющая $R_{rnd}$ может быть представлена как случайная нормально распределенная величина.

**Экспериментальное исследование периодов сигналов ККО.** Во многих цифровых системах с кристаллами ПЛИС сигналы системной частоты $CLK_{sys} = P_{sys}^{-1}$ выбираются со значениями, которые гораздо ниже, чем максимально возможная рабочая частота реализуемых схем, $F_{sch} > CLK_{sys}$. Так, на плате быстрого прототипирования Digilent ZYBO-Z7 для части кристалла с программируемой логикой $CLK_{sys} = 50$ МГц, а максимальная частота функционирования 32-разрядного синхронного счетчика, реализованного на программируемой логике, оценивается как $F_{sch} \approx 180$ МГц (для кристалла Xilinx ZYNQ xc7z010-1, выполненного по 28-нанометровому техпроцессу). Согласно теореме Котельникова системная частота может быть применена для измерения периодов схем ККО, частоты выходных сигналов которых не превышают 25 МГц ($P_{cro} = 40$ нс). Для повышения разрешающей способности схемы измерения будем производить оценку периода $P_{cro}$ (частоты $F_{cro} = P_{cro}^{-1}$) сигнала ККО, подавая его на вход синхронизации двоичного синхронного счетчика во временном окне измерения $MW = k_{factor} \cdot P_{sys}$, кратном стационарному периоду $P_{sys}$ системного сигнала синхронизации, где $k_{factor}$ – целочисленный множитель, задаваемый системой измерения. Подобный метод измерения позволит оценивать частоты $F_{cro} \le 180$ МГц.

На точность измерения периода сигнала ККО будут влиять ширина окна измерения (множитель $k_{factor}$) и разрядность регистрирующего счетчика $N=C+L$ (см. рис. 1). Предположим, что $\lambda \cdot P_{cro} = P_{sys}$. Если $\lambda \ge 1$, для регистрации первого фронта сигала ККО достаточно минимального окна измерения при $k_{factor} = 1$. В случае если $\lambda < 1$, для регистрации первого фронта необходимо, чтобы $k_{factor} = 2 \cdot \lceil \lambda \rceil$. Так как значение $P_{cro}$ заранее неизвестно, измерение можно начинать со значения $k_{factor} = 1$. Если при этом значение регистрирующего счетчика $R \ge 1$, то принимается, что $\lambda \ge 1$. В противном случае, если $R = 0$, то измерение повторяется для большего значения $k_{factor}$ до тех пор, пока не будет достигнуто условие $R \ge 1$. Далее временное окно измерения можно увеличивать, экспоненциально изменяя множитель $k_{factor} = 2^i$, $i \in \mathbb{Z}$. На каждой новой итерации происходит более точное измерение периода ККО $P_{croi} = \dfrac{MW_i}{R_i} = 2^i \cdot \dfrac{P_{sys}}{R_i}$ либо значения $\lambda_i = \dfrac{P_{sys}}{P_{croi}} = \dfrac{R_i}{2^i}$. Увеличение степенного показателя $i$ заканчивается при достижении необходимого значения точности: $\varepsilon \le \left|\lambda_{i+1} - \lambda_i\right|$.

***Пример 1.*** Для реализованной схемы ККО, конфигурации $CH$=0 и для $k_{factor} = 1$ ($i$=0) значение счетчика $R_0 = 3$. При этом $P_{cro0} = \dfrac{MW_0}{R_0} = \dfrac{P_{sys}}{3}$, т. е. $\lambda_0 = 3$. Дальнейшие измерения на увеличенных окнах $MW_i$ дают следующие результаты: $\lambda_1 = \dfrac{6}{2} = 3$, $\lambda_2 = \dfrac{12}{4} = 3$, $\lambda_3 = \dfrac{23}{8} = 3 - \dfrac{1}{8}$,

$\lambda_4 = \frac{46}{16} = 3 - \frac{1}{8}$, $\lambda_5 = \frac{91}{32} = 3 - \frac{5}{32}$ и т. д. На рис. 2 приведены значения $\lambda_i$ для $i \in [0,30]$. Видно, что с увеличением $i$ значение $\lambda_i$ асимптотически приближается к 2,84 по мере увеличения окна измерения и для $i = 30$ принимает значение 2,842 954.

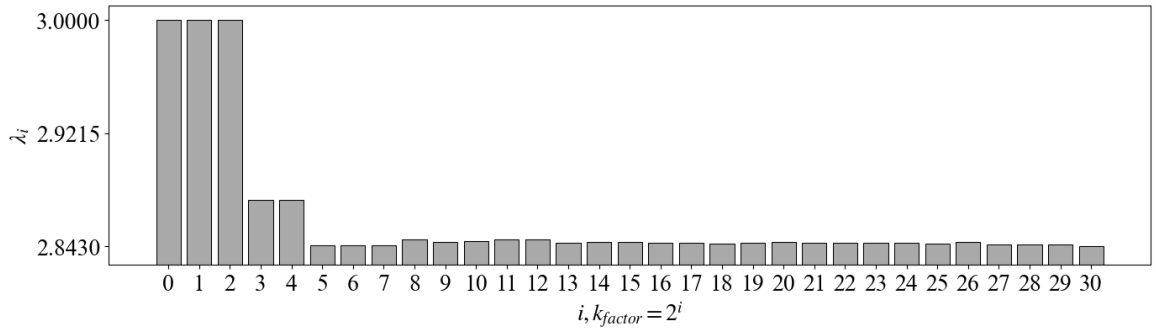


Рис. 2. Значения $\lambda^i$ для $i \in [0,30]$

*Fig. 2.* $\lambda^i$ *values for* $i \in [0,30]$

В примере 1 были использованы значения, полученные путем однократных измерений в соответствующих временных окнах.

При многократно повторяемых измерениях $M$ на одном и том же временном окне $MW_i$ наблюдаются различные значения регистрирующего счетчика, вызванные разными факторами, к которым можно отнести нестабильность питающего напряжения, тепловой шум окружающей среды и кристалла FPGA, несовершенство измерительного оборудования и т. п. Так, для $M = 10^3$ повторяющихся измерений и для различных окон $MW_i$ были оценены математические ожидания (МО) $\mu(\lambda_i)$ и среднеквадратические отклонения (СКО) $\sigma(\lambda_i)$ регистрируемых величин $\lambda_i$. На рис. 3 изображена столбчатая гистограмма значений величины $\eta_i = \frac{\sigma(\lambda_i)}{\mu(\lambda_i)} \cdot 100\,\%$, определяющей удельный вес шумовой составляющей $\lambda_i$ при измерениях на различных окнах $MW_i$.

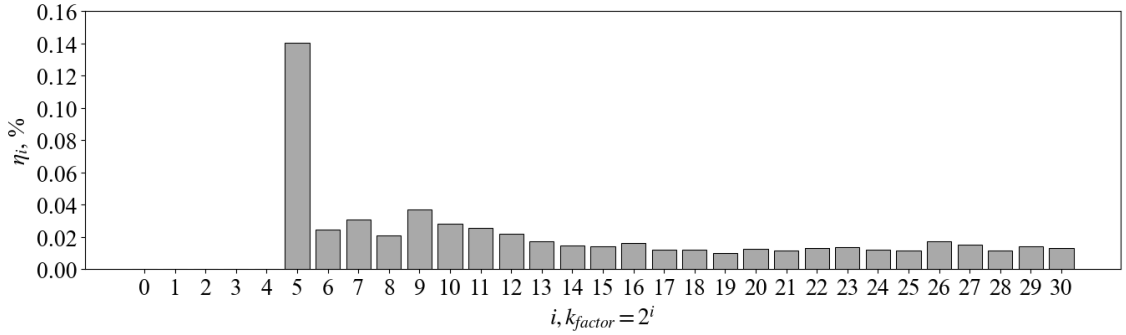


Рис. 3. Зависимость величины $\eta_i$ от окна измерения

*Fig. 3. Dependence of the* $\eta_i$ *value on the measurement window*

Как показали проведенные эксперименты, регистрируемые значения на $M$ повторяющихся измерениях можно представить вероятностями появления единичного символа в каждом $j$-м разряде счетчика $R_i^j$:

$$P_i^j = \frac{1}{M} \sum_{m=0}^{M-1} R_{i,m}^j, \quad (1)$$

где $R_{i,m}^{j} \in \{0,1\}$ – значение *j*-го разряда счетчика ( $j \in [0, N_i - 1]$ ) на *m*-м измерении в фиксированном окне $MW_i$. В качестве примера на рис. 4 приведены значения $P_{17}^{j}$ для $M = 10^3$, *i*=17 ($k_{factor} = 2^{17}$), $N_i = 19$, $j \in [0,18]$.

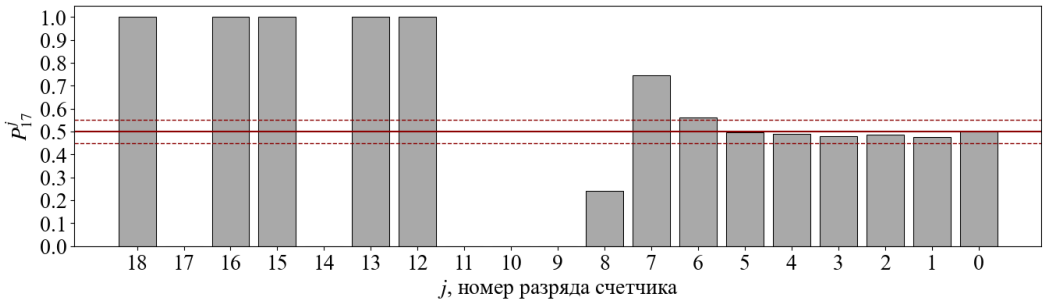


Рис. 4. Значения $P_{17}^{j}$ для каждого из разрядов регистрирующего счетчика при $k_{factor} = 2^{17}$

*Fig. 4. Values of* $P_{17}^{j}$ *for each of the digits of the register counter at* $k_{factor} = 2^{17}$

На рис. 5 показана тепловая карта значений $P_i^{j}$ для $i \in [0,30]$.

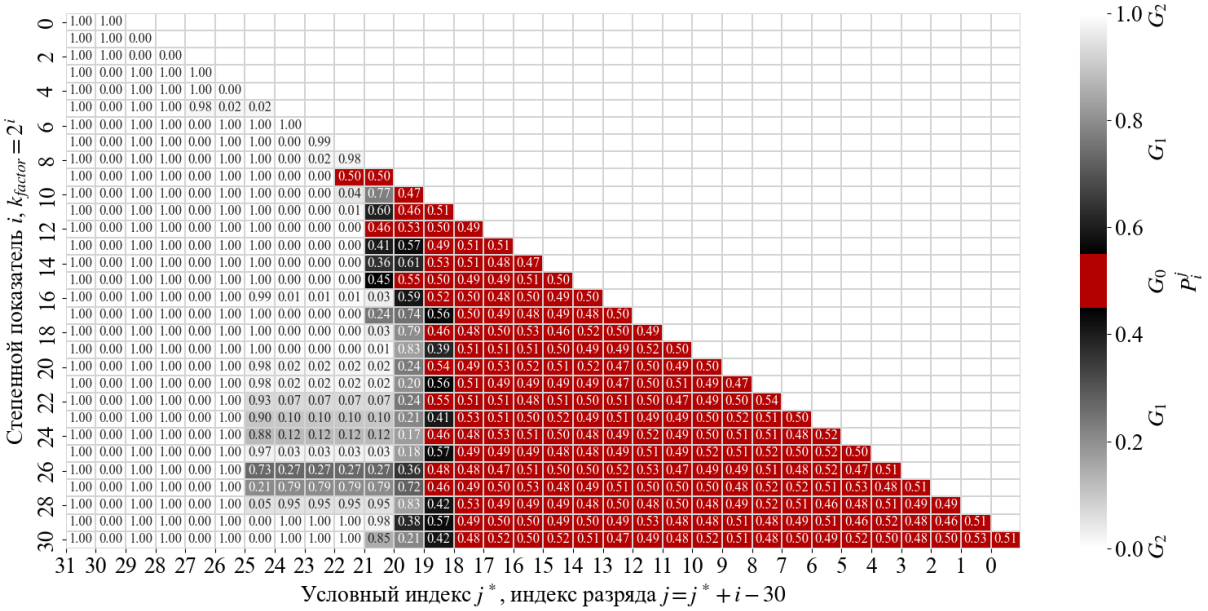


Рис. 5. Значения $P_i^{j}$, $\forall i \in [0,30]$ и $\xi = 0,05$

*Fig. 5. Values of* $P_i^{j}$, $\forall i \in [0,30]$ *and* $\xi = 0,05$

Как видно на представленной карте, значения всех значимых разрядов можно условно разделить на три подмножества:

1. Группу стабильных разрядов $G_2$, включающую разряды (на рис. 5 отмечены белым цветом), для которых $P_i^{j} = 1$ либо $P_i^{j} = 0$.

2. Группу условно стабильных разрядов $G_1$, включающую все разряды $R_i^{j}$ (отмечены оттенками серого цвета), для которых $1 > P_i^{j} > 0,5 + \xi$ либо $0,5 - \xi > P_i^{j} > 0$, где $\xi$ – малая величина, характеризующая отклонение от значения 0,5 (на рис. 4 $\xi = 0,05$).

3. Группу сильно нестабильных разрядов $G_0$ (отмечены красным цветом), для которых $0,5+\xi \geq P_i^j \geq 0,5-\xi$.

Для данных на рис. 4 и значения $\xi = 0,05$ группы разрядов выглядят следующим образом: $G_2 = \{R_{17}^{18}, R_{17}^{17}, R_{17}^{16}, R_{17}^{15}, R_{17}^{14}, R_{17}^{13}, R_{17}^{12}, R_{17}^{11}, R_{17}^{10}, R_{17}^{9}\}$, $G_1 = \{R_{17}^{8}, R_{17}^{7}, R_{17}^{6}\}$ и $G_0 = \{R_{17}^{5}, R_{17}^{4}, R_{17}^{3}, R_{17}^{2}, R_{17}^{1}, R_{17}^{0}\}$.

Сумма размерностей представленных групп равна минимально необходимому числу разрядов счетчика $N_i$, регистрирующего целое число периодов ККО в заданном окне измерения: $N_i = |G_2| + |G_1| + |G_0| = \lceil \log_2 R_i \rceil = \lceil \log_2 (\lambda_i \cdot 2^i) \rceil = \lceil \log_2 \lambda_i \rceil + i$. Для рассматриваемого примера (*i*=17) $N_i = \lceil \log_2 \lambda_i \rceil + i = 2 + 17 = 19$, а $|G_2| = 10$, $|G_1| = 3$ и $|G_0| = 6$, что также в сумме дает 19 разрядов.

Как видно из представленных данных (см. рис. 5), ненулевое число разрядов в группе $G_1$ начинается с индекса *i*=5, что коррелируется с первым ненулевым значением $\eta_i$ (см. рис. 3). Начиная с индекса *i*=9, наблюдается ненулевая численность сильно нестабильных разрядов группы $G_0$, которая асимптотически линейно возрастает по мере увеличения окна $MW_i$. При этом общее число разрядов двух групп $|G_2| + |G_1|$, начиная с индекса *i*=13, практически остается стационарным (принимает значение 12 либо 13). Кроме того, начиная с того же индекса *i*=13, распределение сгенерированных значений счетчика становится близким к нормальному распределению.

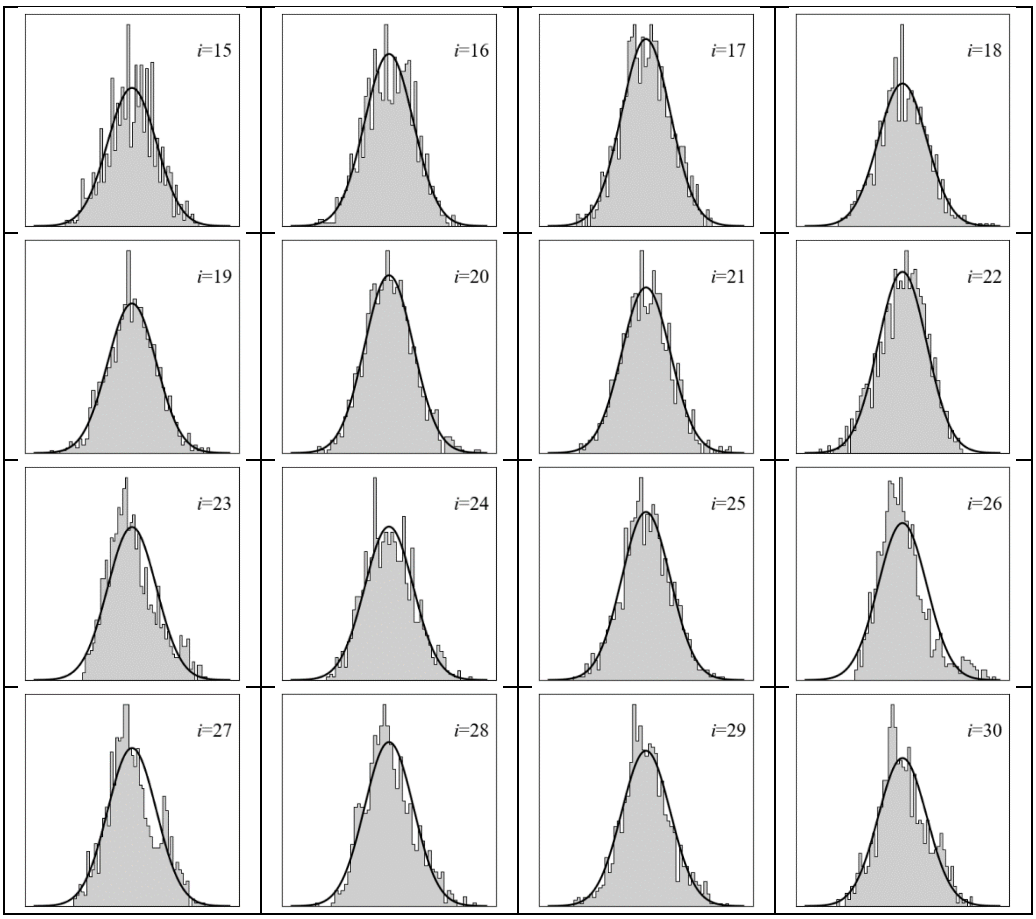


Рис. 6. Гистограммы распределения значений счетчика на различных окнах измерения для $i \in [15, 30]$

*Fig. 6. Histograms of the distribution of counter values on different measurement windows for* $i \in [15, 30]$

На рис. 6 представлены гистограммы распределения значений счетчика в различных окнах измерения для $i \in [15,30]$ совместно с графиками нормального распределения, построенными по экспериментальным значениям МО и СКО. Большое сходство с нормальным распределением дает основание использовать разряды регистрирующего счетчика из группы $G_0$ для генерирования случайных данных.

Проведем аналитическое исследование случайных нормально распределенных положительных целочисленных значений, алгоритмически сгенерированных по экспериментально полученным величинам МО и СКО. Для этого создадим программную модель, позволяющую оценивать распределение разрядов регистрирующего счетчика на группы $G_2$, $G_1$ и $G_0$, и сравним полученные распределения с реальными экспериментальными.

**Моделирование поведения групп разрядов регистрирующего счетчика.** Целью данного исследования будет служить установление закономерностей по распределению групп $G_2$, $G_1$ и $G_0$ на множестве положительных целочисленных значений, полученных путем квантования и округления случайных нормально распределенных величин, в зависимости от задаваемых значений МО и СКО. Для этого была реализована программная модель на языке Python функционального поведения двоичного счетчика, регистрирующего передние фронты сигналов ККО. Входными данными для модели служат параметры $\mu(R_i)$(МО) и $\sigma(R_i)$(СКО) значений регистрирующего счетчика $R_i$, полученных экспериментальным путем для $i \in [9,30]$. Для имитации поведения двоичного счетчика параметры $\mu(R_i)$, $\sigma(R_i)$ и вырабатываемые значения округлялись до ближайших меньших целых чисел. При этом первое ненулевое значение $\sigma(R_i)$ появляется для *i*=9, что коррелируется с первой ненулевой размерностью группы $G_0$ (см. рис. 5).

Для генерирования $M = 10^3$ целочисленных нормально распределенных значений по заданным параметрам использовалась функция truncnorm из библиотечного пакета scipy.stats. Далее сгенерированные значения переводились в двоичное представление. Для этих значений вычислялись вероятности $P_i^j$ и проводилась оценка размерностей групп $G_2$, $G_1$ и $G_0$.

Определим отклонение модельных оценок от экспериментальных при помощи расстояния Евклида. Пусть $V_i^{\text{e}} = (P_i^0; P_i^1; P_i^2; ...; P_i^{N_i-1})$ – вектор, компонентами которого $V_i^e(j) = P_i^j$, $j \in [0, N_i - 1]$, являются экспериментальные данные, полученные для *i*-го степенного коэффициента окна измерения. Тогда $V_i^m$ – вектор той же размерности, сформированный из модельных оценок значений $P_i^j$.

С учетом того что все значения $P_i^j \in [0,1]$, максимальное расстояние Евклида между векторами $V_i^e$ и $V_i^m$ можно выразить как $D_{em}^{\max}(i) = \sqrt{N_i}$. Введем меру сходства двух векторов $V_i^e$ и $V_i^m$ через их нормированное расстояние Евклида:

$$S_{em}(i) = 1 - D_{em}^{norm}(i) = 1 - \frac{1}{D_{em}^{\max}(i)} \cdot \sqrt{\sum_{j=0}^{N_i-1} \left(V_i^e(j) - V_i^m(j)\right)^2}. \quad (2)$$

Очевидно, что $S_{em}(i) \in [0,1]$ и $S_{em}(i) = 0$ соответствуют случаю максимального расстояния (различия) векторов, а $S_{em}(i) = 1$ – полного подобия векторов $V_i^e = V_i^m$.

***Пример 2.*** Для *i*=9 ($k_{factor} = 2^9$, $D_{em}^{\max}(i) = \sqrt{11} \approx 3{,}3166$) векторы принимают следующие значения: $V_i^e = (1;0;1;1;0;1;1;0;0;0,496;0,503)$, $V_i^m = (1;0;1;1;0;1;0,943;0,057;0,068;0,334;0,486)$.

Как видно, пять компонент векторов из 11 различаются, но их отличия незначительные, что выражается в значениях нормированного расстояния $D_{em}^{norm}(9) \approx 0,0585$ и меры сходства $S_{em}(9) = 0,9415$.

На рис. 7 показаны значения $S_{em}(i)$, вычисленные для $i \in [9,30]$.

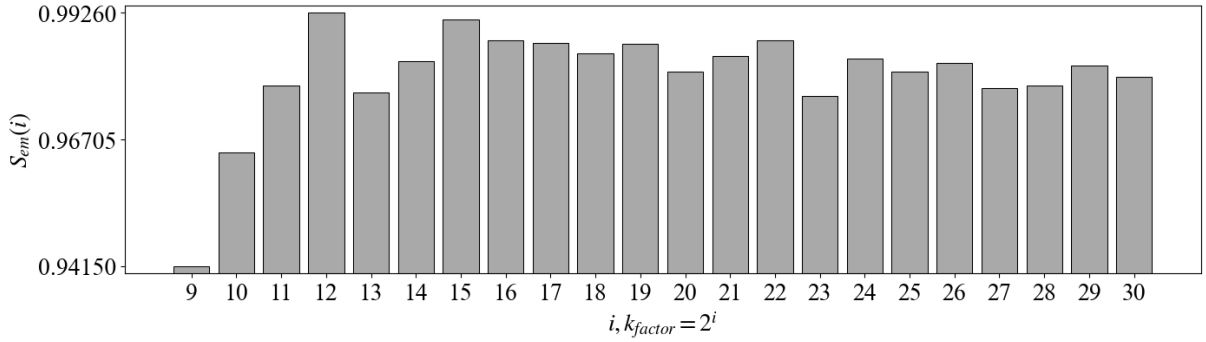


Рис. 7. Значения меры сходства $S_{em}(i)$ для $i \in [9,30]$

*Fig. 7. Similarity measure values* $S_{em}(i)$ *for* $i \in [9,30]$

Из представленных значений видно, что для всех окон измерений ($i \in [9,30]$) наблюдаются незначительные отличия экспериментальных данных от данных, полученных на программной модели. Это может служить подтверждением гипотезы о распределении многократно измеряемых значений $R_i$, близком к нормальному распределению случайной величины.

Рассмотрим непрерывную случайную нормально распределенную величину $Q$: $Q \sim N(\mu_Q, \sigma_Q{}^2)$. Пусть $Q$ равномерно квантована $T = 2^L$ уровнями и кодируется $L$-разрядными положительными двоичными числами, каждое из которых будем рассматривать в следующей нотации: $b^t = (b_{L-1}^t, b_{L-2}^t, b_{L-3}^t, ..., b_0^t)$, где $b_l^t \in \{0,1\}$ есть $l$-й разряд двоичного числа $b^t$, кодирующего уровень квантования $t$, при этом $t \in [0, T-1]$, $l \in [0, L-1]$, $T \in \mathbb{Z}$, $L \in \mathbb{Z}$. В общем случае $b^t$ есть двоичное представление уровня квантования $t$. Например, для $L$=4 и $t$=5 имеется $T$=16 уровней квантования, а $b^5 = (b_3^5, b_2^5, b_1^5, b_0^5) = (0,1,0,1)$.

Диапазон значений, в который будут попадать большинство чисел (99,9937 %), представим как $D_Q = [\mu_Q - 4 \cdot \sigma_Q, \mu_Q + 4 \cdot \sigma_Q]$, тогда шаг квантования будет равен $\Delta_Q = \dfrac{8 \cdot \sigma_Q}{T} = 2^{3-L} \cdot \sigma_Q$.

Произвольное значение $q$ случайной величины $Q$ принадлежит одному из уровней квантования $t$ из $T$ возможных и лежит в диапазоне $\mu_Q - 4\sigma_Q + t \cdot \Delta_Q \le q < \mu_Q - 4\sigma_Q + (t+1) \cdot \Delta_Q$. Если применить квантование с использованием усечения, то значение $q$ будет соответствовать целому числу $t$ либо его двоичному представлению $b^t$. Так, для предыдущего примера случайная величина $q$ из диапазона $[\mu_Q - \dfrac{3}{2}\sigma_Q, \mu_Q - \sigma_Q)$ будет представлена двоичным числом $b^5$.

С учетом сказанного выше можно рассматривать эквивалентную случайную величину $B \sim N(\mu_B, \sigma_B{}^2)$, для которой диапазон большинства принимаемых значений равен $D_B = [\mu_B - 4 \cdot \sigma_B, \mu_B + +4 \cdot \sigma_B] = [0, 2^L)$, при этом $\mu_B = 2^{L-1}$, $\sigma_B = 2^{L-3}$, $\Delta_B = 1$. Произвольное значение $b$ случайной величины $B$ принадлежит одному из диапазонов $D_B^t = [t, t + \Delta_B)$, а квантованное с усечением значение будет равно $t$ ($b^t$ в двоичном представлении) (рис. 8).

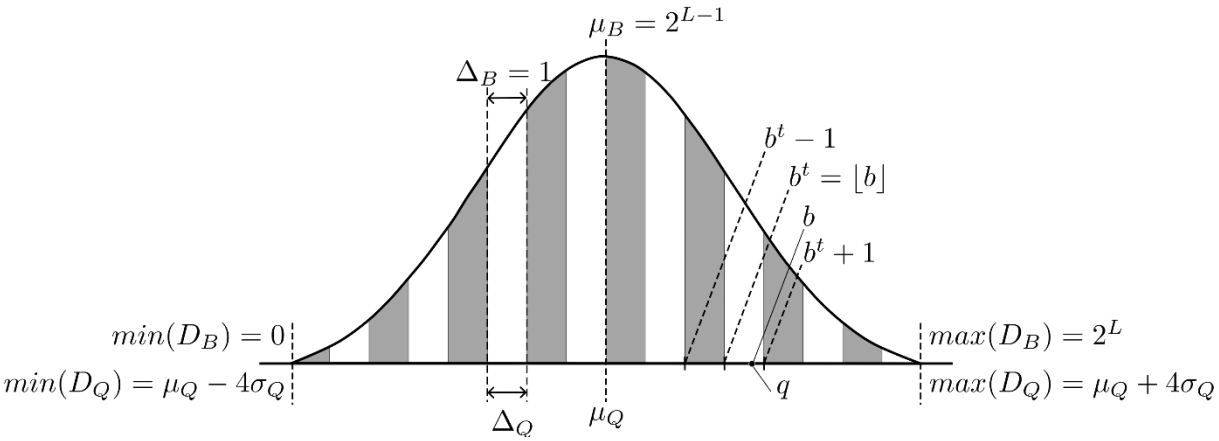


Рис. 8. Основные параметры величин *Q* и *B*
*Fig. 8. Basic parameters of the quantities Q and B*

Так как $\Delta_B = 1$, то записи вида $t + \Delta_B$ и $t + 1$ являются эквивалентными. В силу симметрии функции распределения случайной величины *B* диапазон $D_B$ можно представить двумя равновеликими диапазонами $D_B = D_{LB} \bigcup D_{HB}$, где $D_{LB} = [0, \mu_B)$, а $D_{HB} = [\mu_B, 2^L)$, для которых выполняется равенство вероятностей принадлежности $P(B \in D_{LB}) = P(B \in D_{HB})$.

Оценим вероятность появления единичного бита в старшем разряде $P(B_{L-1} = 1)$ при квантовании и двоичном кодировании величины *Q*.

Утверждение 1. *Вероятность появления единичного бита в старшем разряде* $P(B_{L-1} = 1) = P(B \in D_{HB}) = 0,5$.

Доказательство. Все двоичные числа, для которых $b^t_{L-1} = 1$, принадлежат диапазону $D_{HB}$, что для непрерывной величины *B* соответствует вероятности попадания в диапазон $P(\mu_B \le B < \mu_B + 4\sigma_B)$. Стандартизуем случайную величину *B* относительного стандартного нормального распределения *Z*~*N*(0,1): $Z = \frac{B - \mu_B}{\sigma_B}$. Для нижней границы диапазона $Z_{\min} = \frac{\mu_B - \mu_B}{\sigma_B} = 0$, а для верхней – $Z_{\max} = \frac{\mu_B + 4\sigma_B - \mu_B}{\sigma_B} = 4$.

Тогда вероятность попадания случайной величины в заданный диапазон вычисляется как $P(0 \le Z < 4) = \Phi(Z_{\max}) - \Phi(Z_{\min}) = \Phi(4) - \Phi(0) = 0,9999 - 0,5 = 0,4999$, где Ф – функция стандартного нормального распределения. Таким образом, $P(B_{L-1} = 1) \approx 0,5$, что и требовалось доказать.

Изменим принимаемые кодированные значения величины *B* в двоичном представлении путем добавления одного старшего разряда с константным значением $B_L = 1$: $b^t = (\underline{b^t_L}, b^t_{L-1}, b^t_{L-2}, ..., b^t_0)$, $\forall t \in [0, T-1]$, при этом число *T* квантованных уровней и значение $\sigma_B$ остаются прежними. В таком случае значение матожидания будет равным $\mu^*_B = 2^L + \mu_B$, а диапазон принимаемых значений будет выглядеть следующим образом: $D^*_{HB} = [2^L, 2^{L+1})$.

Оценим вероятность $P(B_L = 1)$ как вероятность попадания величины *B* в диапазон $D^*_{HB}$: $P(B \in D^*_{HB}) = P(2^L \le B < 2^{L+1})$. Стандартизуем случайную величину *B* относительного стандартного нормального распределения *Z*~*N*(0,1): $Z = \frac{B - \mu^*_B}{\sigma_B}$.

Для нижней границы диапазона $Z_{\min} = \frac{2^L - 2^L - \mu_B}{\sigma_B} = -\frac{\mu_B}{\sigma_B} = -4$, а для верхней – $Z_{\max} = \frac{2^{L+1} - 2^L - \mu_B}{\sigma_B} = \frac{\mu_B}{\sigma_B} = 4$. Тогда вероятность $P(2^L \le B < 2^{L+1}) = \Phi(4) - \Phi(-4) = 1 - 1 + \Phi(4) = 1$. Таким образом, $P(B^L = 1) = 1$.

В общем случае расширение кодированных значений величины $B$ на $C$ константных разрядов с произвольными значениями $b^t = (\underline{b^t_{L+C-1}, b^t_{L+C-2}, ..., b^t_{L+1}, b^t_L}, b^t_{L-1}, b^t_{L-2}, ..., b^t_0)$, $\forall t \in [0, T-1]$ также дадут $P(B_{l-1} = 1) = 1$ либо $P(B_{l-1} = 0) = 1$, $\forall l \in [L, L+C-1]$. Иными словами, все старшие добавленные константные разряды $b^t_l$ образуют группу $G_2$. На основании этого сформулируем следующее следствие.

***Следствие 1.*** *Если случайная нормально распределенная величина* $B \sim N(\mu_B, {\sigma_B}^2)$, *для которой* $\sigma_B = 2^{L-3}$, $\mu_B = H_C + 2^{L-1}$, *где* $H_C > 2^{L-1}$, *и* $\mu_B \equiv 0 (\mathrm{mod}\ \ 2^L)$, *квантуется* $T = 2^L$ *уровнями, кодирующимися* (C+L)*-разрядными двоичными числами, то C старших разрядов (кодирующих значение* $H_C$*) являются неизменными и образуют группу* $G_2$.

Для следующего утверждения введем понятие инверсного диапазона: для произвольного диапазона $D^t_B = [b^t, b^t + 1)$ его инверсия $\overline{D^t_B} = [\overline{b^t}, \overline{b^t} + 1)$, где $\overline{b^t}$ есть поразрядная инверсия значения $b^t$, $\forall t \in [0, T-1]$.

Утверждение 2. *Вероятности принадлежности случайной величины B к произвольному диапазону* $D^t_B$ *и его инверсии* $\overline{D^t_B}$ *равны:* $P(B \in D^t_B) = P(B \in \overline{D^t_B})$.

Данное утверждение верно в силу симметрии функции распределения относительно значения $\mu_B = 2^{L-1}$.

Доказательство. Инверсию произвольного двоичного $L$-разрядного числа $b^t$ можно представить выражением $\overline{b^t} = (\overline{b^t_{L-1}}, \overline{b^t_{L-2}}, \overline{b^t_{L-3}}, ..., \overline{b^t_0})$ либо в десятичном представлении выражением $\bar{t} = 2^L - 1 - t = 2\mu_B - 1 - t$.

В общем случае вероятность $P(B \in D^t_B)$ представим как равенство

$$P(B \in D^t_B) = P(t \le B < t + 1) = \Phi(Z_{\max}) - \Phi(Z_{\min}), \tag{3}$$

где $Z_{\min} = \frac{t - \mu_B}{\sigma_B}$, а $Z_{\max} = \frac{t + 1 - \mu_B}{\sigma_B} = Z_{\min} + \frac{1}{\sigma_B}$ – стандартизованные значения.

Выразим аналогичным образом вероятность $P(B \in \overline{D^t_B})$:

$$P(B \in \overline{D^t_B}) = P(2\mu_B - 1 - t \le B < 2\mu_B - t) = \Phi(Z^*_{\max}) - \Phi(Z^*_{\min}). \tag{4}$$

Рассмотрим стандартизованные значения инверсного диапазона $Z^*_{\max}$ и $Z^*_{\min}$:

$$\begin{aligned} Z^*_{\max} &= \frac{2\mu_B - t - \mu_B}{\sigma_B} = -\frac{t - \mu_B}{\sigma_B} = -Z_{\min}, \\ Z^*_{\min} &= \frac{2\mu_B - 1 - t - \mu_B}{\sigma_B} = -\frac{t + 1 - \mu_B}{\sigma_B} = -Z_{\max} = -(Z_{\min} + \frac{1}{\sigma_B}). \end{aligned} \tag{5}$$

Тогда согласно симметрии функции стандартного нормального распределения относительно нуля вероятность (4) можно выразить следующим образом: $\Phi(Z^*_{\max}) - \Phi(Z^*_{\min}) = \Phi(-Z_{\min}) - -\Phi(-Z_{\max}) = \Phi(Z_{\max}) - \Phi(Z_{\min}) = P(B \in D^t_B)$, что и требовалось доказать.

Обозначим составной диапазон $D^{(l,1)}_B = \bigcup_{t=0}^{T-1} D^t_B$ как совокупность диапазонов квантования, для которых выполняется условие $b^t_l = 1$, $l \in [0, L-2]$. По аналогии введем составной диапазон $D^{(l,0)}_B = \bigcup_{t=0}^{T-1} D^t_B$, $\forall b^t_l = 0$. Произвольный диапазон $D^{(l,1)}_B$ можно представить следующим образом: $D^{(l,1)}_B = D^{(l,1)}_{LB} \bigcup D^{(l,1)}_{HB}$, где $D^{(l,1)}_{LB} = \bigcup_{t=0}^{\mu_B - 1} D^t_B$ при $b^t_{L-1} = 0$, а $D^{(l,1)}_{HB} = \bigcup_{t=\mu_B}^{T-1} D^t_B$ при $b^t_{L-1} = 1$, $\forall b^t_l = 1$, $l \in [0, L-2]$. Тогда вероятность принадлежности случайной величины диапазону $D^{(l,1)}_B$ можно выразить как $P(B \in D^{(l,1)}_B) = P(B \in D^{(l,1)}_{LB}) + P(B \in D^{(l,1)}_{HB})$.

Утверждение 3. *Вероятность принадлежности случайной величины B диапазону* $D^{(l,1)}_B$ *равна* $P(B \in D^{(l,1)}_B) = 0,5$ *для всех* $l \in [0, L-2]$.

Доказательство. Произведем инверсию составного диапазона $D^{(l,1)}_{LB}$: $\overline{D^{(l,1)}_{LB}} = \bigcup_{t=0}^{\mu_B - 1} \overline{D^t_B} = \bigcup_{t=\mu_B}^{M-1} D^t_B = D^{(l,0)}_{HB}$. В свою очередь, объединение диапазонов $D^{(l,1)}_{HB}$ и $D^{(l,0)}_{HB}$ дает диапазон $D_{HB}$: $D^{(l,1)}_{HB} \bigcup D^{(l,0)}_{HB} = D_{HB}$. Основываясь на утверждении 2, $P(B \in D^{(l,1)}_{LQ}) = P(B \in \overline{D^{(l,1)}_{LQ}}) = P(B \in D^{(l,0)}_{HQ})$. Тогда в разложении $P(B \in D^{(l,1)}_B) = P(B \in D^{(l,1)}_{LQ}) + P(B \in D^{(l,1)}_{HQ})$ произведем замену вероятности $P(B \in D^{(l,1)}_{LQ})$ на вероятность $P(B \in D^{(l,0)}_{HQ})$ в силу их равенства: $P(B \in D^{(l,0)}_{HQ}) + +P(B \in D^{(l,1)}_{HQ}) = P(B \in D_{HQ})$. Согласно утверждению 1 $P(B \in D_{HQ}) = 0,5$, что и требовалось доказать.

***Пример 3.*** Пусть $L$=3, тогда $T$=8, $\mu_B = 4$, $\sigma_B = 1$, $D_B = [0,8)$. Оценим вероятность $P(B \in D^{(l,1)}_B)$ для $l$=0. Весь диапазон принимаемых значений $D_B$ условно разделим на симметричные диапазоны $D_{LB} = [0,4)$ и $D_{HB} = [4,8)$. Тогда $D^{(0,1)}_B = D^1_B \bigcup D^3_B \bigcup D^5_B \bigcup D^7_B$, $D^{(0,1)}_{LB} = D^1_B \bigcup D^3_B$, а $D^{(0,1)}_{HB} = D^5_B \bigcup D^7_B$. Инверсия составного диапазона выглядит как $\overline{D^{(0,1)}_{LB}} = D^6_B \bigcup D^4_B = D^{(0,0)}_{HB}$. Согласно утверждению 2 следующее равенство является верным: $P(B \in D^{(0,1)}_{LB}) = P(B \in \overline{D^{(0,1)}_{LB}}) = P(B \in D^{(0,0)}_{HB})$. Тогда вероятность принадлежности составному диапазону $D^{(0,1)}_B$ представим как $P(B \in (D^6_B \bigcup D^4_B \bigcup D^5_B \bigcup D^7_B)) = P(B \in D_{HQ}) = 0,5$.

***Следствие 2.*** *Если случайная нормально распределенная величина* $B \sim N(\mu_B, {\sigma_B}^2)$, *для которой* $\sigma_B = 2^{L-3}$, *а* $\mu_B \geq 2^{L-1}$ *и* $\mu_B \equiv 0 (\mathrm{mod}\ \ 2^L)$, *квантуется* $T = 2^L$ *уровнями, кодирующимися* (*C*+*L*)*-разрядными двоичными числами, то L младших разрядов образуют группу* $G_0$.

Следствие 2 дополняет следствие 1 на основании утверждения 3.

Для подтверждения приведенных теоретических выводов были проведены эксперименты на программной модели, позволяющие оценить разделение на группы $G_2$ и $G_0$ при параметрах случайной величины, указанных в следствиях 1 и 2.

Рассмотренный случай является идеализированным по таким параметрам, как матожидание и СКО, значения которых на практике могут быть произвольными. Так, если в рассмотренной модели значение $\mu_Q = H_C + 2^{L-1} + \chi$, $H_C > 2^{L-1}$, $\chi < 2^{L-1}$, то при подсчете числа передних фронтов на синхронном счетчике могут возникать случаи, когда происходит арифметический перенос в разряды, порядковые индексы которых больше чем $\lceil \log_2 \chi \rceil$. Это влияет на значения вероятностей $P_i^j$ (1) для разрядов в окрестности $\mu_B = 2^{L-1}$.

Искажения могут затронуть и разряды из группы $G_0$, в этом случае $P_i^j \neq 0,5$, и (или) разряды из группы $G_2$, что даст $1,0 < P_i^j < 0,5$ либо $0,5 < P_i^j < 1,0$, формируя группу $G_1$.

Обобщая вышесказанное, можно утверждать, что для определенных значений множителя многократно регистрируемое значение счетчика, вероятнее всего, будет содержать три ненулевые группы разрядов $G_2$, $G_1$ и $G_0$. Методом максимального правдоподобия группу $G_1$ можно преобразовать в часть дополнительных разрядов группы $G_2$ либо вычесть значение шумовой составляющей матожидания $\chi < 2^{L-1}$ из регистрируемых счетчиком значений для приведения к виду $(G_2, G_0)$.

**Эксперимент по устранению группы $G_1$.** Основной целью эксперимента является искусственное устранение условно стабильной группы $G_1$ (нахождение значения $\chi < 2^{L-1}$). Ранее (см. рис. 5) были получены экспериментальные данные со счетчика для $\forall i \in [0,30]$. Для каждой выборки значений счетчика $R_i$ на повторяющихся *k* измерениях ($R_{i,1}, R_{i,2}, R_{i,3}, ..., R_{i,k}$) производилась оценка математического ожидания (округление до ближайшего целого) $\mu_i$ и среднеквадратичного отклонения $\sigma_i$. Согласно следствию 2 возможна оценка размерности нестабильной части $G_0$, которая показывает, какое количество младших бит можно считать шумовой составляющей: $|G_0| = 3 + \lfloor \log_2 \sigma_i \rfloor$. После этого выделяется информативная, или стабильная, часть математического ожидания $H_C$, размерность которой можно оценить как $|H_C| = N_i - |G_0|$. Эта часть демонстрирует стабильность в рамках всей выборки и не изменяется под действием случайных шумов. Далее информативные биты $H_C$ используются для формирования нового модифицированного среднего значения $\mu_i^*$, состоящего из трех частей: $|H_C|$ значащих старших бит, разделяющего бита «1» и $|G_0| - 1$ нулевых младших бит ($\mu_i^* = [H_C : 1 : 0^{|G_0|-1}]_2$). Разделительный бит «1» предотвращает влияние шумовой составляющей на стабильные разряды. Таким образом, результирующее значение $\mu_i^*$ представляет собой математическое ожидание, очищенное от влияния условно нестабильной группы $G_1$, а полученная ненулевая разница $\Delta_i = \mu_i - \mu_i^*$ интерпретируется как влияние этой группы. Вычитание из каждого элемента выборки $R_i$ значения $\Delta_i$ равносильно исключению группы $G_1$ из статистики, поскольку ее вклад компенсируется в каждом значении, образуя новую модифицированную выборку, состоящую только из двух групп: стабильной $G_2$ и нестабильной $G_0$.

***Пример 4.*** Для полученных ранее значений имеем $i = 19$, $\mu_{19} = 1491607$, $\sigma_{19} = 148{,}18$. Оценим размерность нестабильной группы: $|G_0| = 3 + \lfloor \log_2 \sigma_{19} \rfloor = 10$. Переведем $\mu_{19}$ в бинарный вид: $\mu_{19} = [10110110000101001011 1]_2$, $N_{19} = 21$.

Для формирования нового значения $\mu_{19}^{*}$ берется стабильная $\mu_{19}$ часть размером $|H_C| = N_i - |G_0| = 11$ бит: $H_C = [10110110000]_2$. Тогда $\mu_{19}^{*} = [H_C : 1 : 0^9]$, а значение $\Delta_{19} = \mu_{19} - \mu_{19}^{*} = 151_{10}$. Скорректировав каждое значение выборки $R_{19}$ на $\Delta_{19}$, получим распределение по группам (рис. 9).

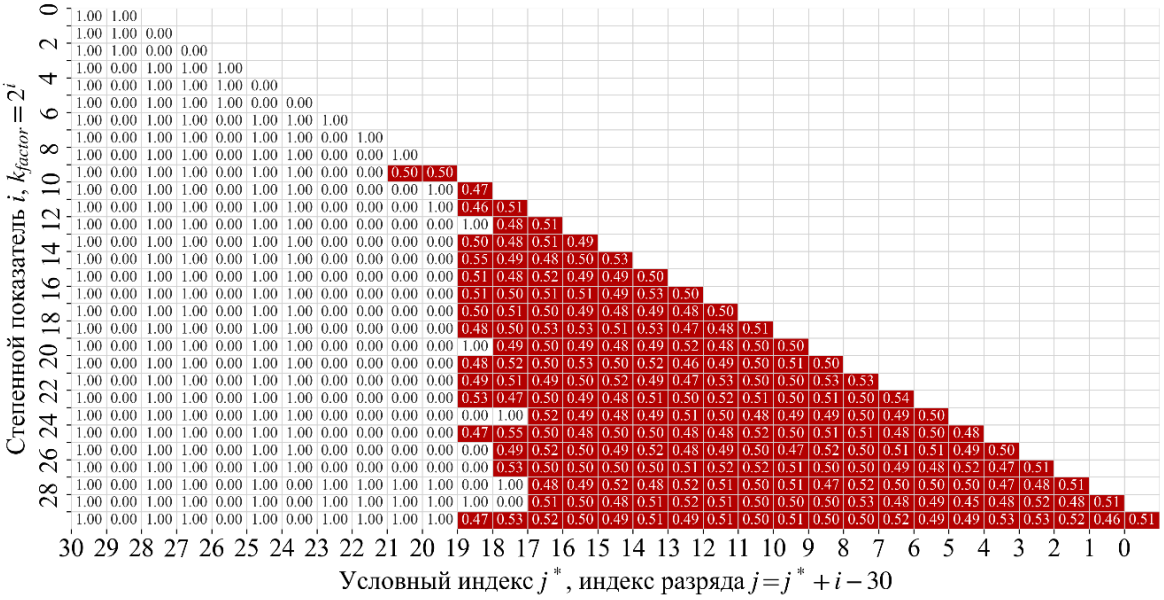


Рис. 9. Значения $P_i^j$, $\forall i \in [0, 30]$ и $\xi = 0,05$ после обработки

*Fig. 9. Values of* $P_i^j$, $\forall i \in [0, 30]$ *and* $\xi = 0,05$ *after postprocessing*

На рис. 9 видно, что для всех значений *i* удалось нивелировать группу $G_1$, оставив распределение значений регистрируемого счетчика на две группы: $G_2$ и $G_0$. Следует отметить, что для значений $3 + \log_2 \sigma_i \le 0$ коррекция значения выборок не проводилась.

**Заключение.** В статье представлены результаты исследования поведения схемы регистрации числа импульсов конфигурируемого кольцевого генератора в фиксированном временном окне. Было показано, что разряды регистрируемого счетчика можно условно разделить на три группы: старшие стабильные разряды, условно стабильные разряды и младшие сильно нестабильные разряды, вероятность появления единичного символа в которых близка к значению 0,5. Анализ собранных экспериментальных данных и проведенное исследование программной модели рассматриваемой схемы показали схожесть генерируемых значений со значениями случайной нормально распределенной величины. Теоретически и практически была показана возможность нивелирования группы условно стабильных разрядов, что открывает перспективы для исследования новых подходов к генерации уникальных идентификаторов, повышения стабильности ФНФ и генерации случайных чисел на основе цифровых схем.

**Вклад авторов.** *А. А. Иванюк* выдвинул гипотезу об использовании разрядов двоичного счетчика, регистрирующего сигналы от схемы конфигурируемого кольцевого осциллятора для генерирования уникальных стабильных идентификаторов и случайных чисел. *Л. А. Бурко* провела экспериментальные исследования и приняла участие в обобщении, анализе и оформлении полученных результатов.

## Список использованных источников

1. Secure System Design and Trustable Computing / ed.: Ch. H. Chang, M. Potkonjak – Switzerland : Springer, 2016. – 549 p. – DOI: 10.1007/978-3-319-14971-4.

2. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – Т. 30, № 2. – С. 92–103.

3. Vinagrero Gutierrez, S. Physical Unclonable Functions (PUFs): foundations, evaluation, and testing for secure hardware systems / S. Vinagrero Gutierrez, G. Di Natale, I. Vatajelu // 30th IEEE European Test Symp. (ETS 2025), Tallinn, Estonia, May 2025. – URL: https://hal.science/hal-05111870 (date of access: 28.08.2025).

4. Hemavathy, S. Arbiter PUF – a review of design, composition, and security aspects / S. Hemavathy, V. S. K. Bhaaskaran // IEEE Access. – 2023. – Vol. 11. – P. 33979–34004. – DOI: 10.1109/ACCESS.2023.3264016.

5. Иванюк, А. А. Синтез симметричных путей физически неклонируемой функции типа арбитр на FPGA / А. А. Иванюк // Информатика. – 2019. – Т. 16, № 2. – С. 99–108.

6. Maiti, A. Improved ring oscillator PUF: an FPGA-friendly secure primitive / A. Maiti, P. Schaumont // Journal of Cryptology. – 2011. – Vol. 24. – P. 375–397. – DOI: 10.1007/s00145-010-9088-4.

7. Configurable ring oscillator PUF using hybrid logic gates / D. Deng, S. Hou, Z. Wang, Y. Guo // IEEE Access. – 2020. – Vol. 8. – P. 161427–161437. – DOI: 10.1109/ACCESS.2020.3021205.

8. Иванюк, А. А. Конфигурируемый кольцевой осциллятор с управляемыми межсоединениями / А. А. Иванюк, В. Н. Ярмолик // Безопасность информационных технологий. – 2024. – Т. 31, № 2. – С. 121–133. – DOI: 10.26583/bit.2024.2.08.

9. Иванюк, А. А. Физически неклонируемые функции на базе управляемого кольцевого осциллятора / А. А. Иванюк, В. Н. Ярмолик // Безопасность информационных технологий. – 2023. – Т. 30, № 3. – С. 90–103. – DOI: 10.26583/bit.2023.3.06.

10. Иванюк, А. А. Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора / А. А. Иванюк // Информатика. – 2025. – Т. 22, № 1. – С. 73–89. – DOI: 10.37661/1816-0301-2025-22-1-73-89.

11. Xin, X. A configurable ring-oscillator-based PUF for Xilinx FPGAs / X. Xin, J.-P. Kaps, K. Gaj // 14th Euromicro Conf. on Digital System Design, Oulu, Finland, 31 Aug. – 02 Sept. 2011. – Oulu, 2011. – P. 651–657. – DOI: 10.1109/DSD.2011.88.

12. Hardware-efficient configurable ring-oscillator-based physical unclonable function/true random number generator module for secure key management / S. Sánchez-Solano, L. F. Rojas-Muñoz, C. Martínez-Rodríguez, P. Brox // Sensors. – 2024. – Vol. 24. – P. 5674–5707. – DOI: 10.3390/s24175674.

13. A large scale characterization of RO-PUF / A. Maiti, J. Casarona, L. McHale, P. Schaumont // 2010 IEEE Intern. Symp. on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, USA, 13–14 June 2010. – Anaheim, 2010 – P. 94–99. – DOI: 10.1109/HST.2010.5513108.

14. Kulagin V. Optimizing RO-PUFs: a filtering approach to reliability and entropy trade-offs / V. Kulagin, G. Di Natale, I. Vatajelu // IEEE 30th European Test Symp. (ETS 2025), Tallinn, Estonia, May 2025. – URL: https://hal.science/hal-05111852v1 (date of access: 28.08.2025).

15. Vinagrero Gutierrez, S. On-line method to limit unreliability and bit-aliasing in RO-PUF / S. Vinagrero Gutierrez, G. Di Natale, I. Vatajelu // IEEE 29th Intern. Symp. on On-Line Testing and Robust System Design (IOLTS 2023), Crete, Greece, July 2023. – URL: https://hal.science/hal-04193294/file/IOLTS___RO_Reliability_and_Bitaliasing.pdf (date of access: 28.08.2025). – DOI: 10.1109/IOLTS59296.2023.10224877.

16. Jitter and phase noise in ring oscillators // The Design of Low Noise Oscillators. – Boston, MA : Springer, 1999. – P. 79–110. – DOI: 10.1007/0-306-48199-5_5.

## References

1. Chang Ch. H., Potkonjak M. (eds.). *Secure System Design and Trustable Computing*. Switzerland, Springer, 2016, 549 p. DOI: 10.1007/978-3-319-14971-4.

2. Yarmolik V. N., Vashynko Yu. G. *Physically unclonable functions.* Informatika [*Informatics*], 2011, vol. 30, no. 2, pp. 92–103 (In Russ.).

3. Vinagrero Gutierrez S., Di Natale G., Vatajelu I. Physical Unclonable Functions (PUFs): foundations, evaluation, and testing for secure hardware systems. *30th IEEE European Test Symposium (ETS 2025), Tallinn, Estonia, May 2025*. Available at: https://hal.science/hal-05111870 (accessed 28.08.2025).

4. Hemavathy S., Bhaaskaran V. S. K. Arbiter PUF – a review of design, composition, and security aspects. *IEEE Access*, 2023, vol. 11, pp. 33979–34004. DOI: 10.1109/ACCESS.2023.3264016.

5. Ivaniuk A. A. *Synthesis of symmetric paths of arbiter physically unclonable function on FPGA.* Informatika [*Informatics*], 2019, vol. 16, no. 2, pp. 99–108 (In Russ.).

6. Maiti A., Schaumont P. Improved ring oscillator PUF: an FPGA-friendly secure primitive. *Journal of Cryptology*, 2011, vol. 24, pp. 375–397. DOI: 10.1007/s00145-010-9088-4.

7. Deng D., Hou S., Wang Z., Guo Y. Configurable ring oscillator PUF using hybrid logic gates. *IEEE Access*, 2020, vol. 8, pp. 161427–161437. DOI: 10.1109/ACCESS.2020.3021205.

8. Ivaniuk A. A., Yarmolik V. N. *Configurable ring oscillator with controlled interconnections.* Bezopasnost` informatsionnykh tekhnologiy [*IT Security (Russia)*], 2024, vol. 31, no. 2, pp. 121–133 (In Russ.). DOI: 10.26583/bit.2024.2.08.

9. Ivaniuk A. A., Yarmolik V. N. *Physically unclonable functions based on a controlled ring oscillator.* Bezopasnost` informatsionnykh tekhnologiy [*IT Security (Russia)*], 2023, vol. 30, no. 3, pp. 90–103 (In Russ.). DOI: 10.26583/bit.2023.3.06.

10. Ivaniuk A. A. *Investigation of the physically unclonable function of a configurable ring oscillator.* Informatika [*Informatics*], 2025, vol. 22, no. 1, pp. 73–89 (In Russ.). DOI: 10.37661/1816-0301-2025-22-1-73-89.

11. Xin X., Kaps J.-P., Gaj K. A configurable ring-oscillator-based PUF for Xilinx FPGAs. *14th Euromicro Conference on Digital System Design, Oulu, Finland, 31 August – 02 September 2011.* Oulu, 2011, pp. 651–657. DOI: 10.1109/DSD.2011.88.

12. Sánchez-Solano S., Rojas-Muñoz L. F., Martínez-Rodríguez C., Brox P. Hardware-efficient configurable ring-oscillator-based physical unclonable function/true random number generator module for secure key management. *Sensors*, 2024, vol. 24, pp. 5674–5707. DOI: 10.3390/s24175674.

13. Maiti A., Casarona J., McHale L., Schaumont P. A large scale characterization of RO-PUF. 2010 *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, USA, 13–14 June 2010.* Anaheim, 2010, pp. 94–99. DOI: 10.1109/HST.2010.5513108.

14. Kulagin V., Di Natale G., Vatajelu I. Optimizing RO-PUFs: a filtering approach to reliability and entropy trade-offs. *30th IEEE European Test Symposium (ETS 2025), May 2025, Tallinn, Estonia.* Available at: https://hal.science/hal-05111852v1 (accessed 28.08.2025).

15. Vinagrero Gutierrez S., Di Natale G., Vatajelu I. On-line method to limit unreliability and bit-aliasing in RO-PUF. *IEEE 29th International Symposium on On-Line Testing and Robust System Design (IOLTS 2023), Crete, Greece, July 2023.* Available at: https://hal.science/hal-04193294/file/IOLTS___RO_Reliability_and_Bitaliasing.pdf (accessed 28.08.2025). DOI: 10.1109/IOLTS59296.2023.10224877.

16. Jitter and phase noise in ring oscillators. *The Design of Low Noise Oscillators*. Springer, Boston, MA, 1999, pp. 79–110. DOI: 10.1007/0-306-48199-5_5.

## Информация об авторах

*Иванюк Александр Александрович*, доктор технических наук, профессор, профессор кафедры информатики, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: ivaniuk@bsuir.by

*Бурко Лиана Александровна*, магистрант, факультет компьютерных систем и сетей, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: burkoliana@gmail.com

## Information about the authors

*Alexander A. Ivaniuk*, D. Sc. (Eng.), Prof., Prof. of Comp. Sci. Department, Belarusian State University of Informatics and Radioelectronics.
E-mail: ivaniuk@bsuir.by

*Liana A. Burko*, Undergraduate, the Faculty of Computer Systems and Networks, Belarusian State University of Informatics and Radioelectronics.
E-mail: burkoliana@gmail.com