МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.23670/IRJ.2023.137.24

МОДЕЛИРОВАНИЕ ГЕНЕРАЦИИ ЦИФРОВОГО ШУМА

Научная статья

Литвинская О.С.[1,] *, Нестеренко С.А.[2]
[1] ORCID : 0000-0002-0041-1542;
[1] Пензенский государственный университет архитектуры и строительства, Пенза, Российская Федерация
[2] КБ «Пульсар-Телеком», Пенза, Российская Федерация

* Корреспондирующий автор (oslit[at]yandex.ru)

Аннотация

Работа посвящена анализу структурных моделей генерации цифрового шума. В статье представлен ряд моделей формирования генерации цифрового шума как средства защиты информации. Представлены структурные схемы на основе кольцевых генераторов, линейных регистров сдвига с обратными связями. В качестве аналогов приводятся физически неклонируемые функции, выполненные на базе кольцевых генераторов импульсов с линией задержки на основе мультиплексоров; гибридных генераторов; на основе алгоритма Box-Muller; на основе кольцевого генератора с метастабильным состоянием и приведена модель на базе FPGA. Приводится описание способов оценки качества генерируемых последовательностей, в частности уточняются графические тесты анализа псевдослучайных последовательностей. В работе приводится результат исследования выбранной структуры генератора цифрового шума на базе кольцевых генераторов. Генератор случайной последовательности на основе кольцевых генераторов синтезирует сигнал с определенной частотой. Частота сигнала в каждом кольцевом генераторе зависит от задержки сигнала в каждом инвертирующем элементе и может быть немного разной в разных кольцевых генераторах из-за небольших отклонений в параметрах элементов. Показаны результаты графических тестов: гистограмма распределения последовательности случайных чисел; распределение элементов последовательности случайных чисел на плоскости; побитовая автокорреляционная функция случайной последовательности; символьная автокорреляционная функция случайной последовательности.

Ключевые слова: сигнал, источник шума, белый шум, моделирование, генератор шума, структура, случайная величина, кольцевой генератор, физически неклонируемая функция, оценка качества сигнала.

MODELLING OF DIGITAL NOISE GENERATION

Research article

Litvinskaya O.S.[1,] *, Nesterenko S.A.[2]
[1] ORCID : 0000-0002-0041-1542;
[1] Penza State University of Architecture and Construction, Penza, Russian Federation
[2] Pulsar-Telecom Design Bureau, Penza, Russian Federation

* Corresponding author (oslit[at]yandex.ru)

Abstract

The work is dedicated to the analysis of structural models of digital noise generation. The article presents a number of models of digital noise generation as a means of information protection. Structural schemes based on ring oscillators, linear shift registers with feedbacks are presented. As analogues the physically unclonable functions made on the basis of ring pulse generators with delay line on the basis of multiplexers; hybrid generators; on the basis of Box-Muller algorithm; on the basis of ring oscillator with metastable state and a model on the basis of FPGA are given. A description of the methods for evaluating the quality of generated sequences is given, in particular, graphical tests for analysing pseudo-random sequences are specified. The work presents the result of research on the selected structure of the digital noise generator based on ring oscillators. The ring oscillator based random sequence generator synthesizes a signal with a certain frequency. The frequency of the signal in each ring oscillator depends on the signal delay in each inverting element, and may be slightly different in different ring oscillators due to small deviations in the element parameters. The results of graphical tests are demonstrated: histogram of the distribution of a sequence of random numbers; distribution of elements of a sequence of random numbers on a plane; bit-by-bit autocorrelation function of a random series; symbolic autocorrelation function of a random sequence.

Keywords: signal, noise source, white noise, modelling, noise generator, structure, random variable, ring oscillator, physically unclonable function, signal quality evaluation.

Введение

Задача получения шумового сигнала с заданными параметрами является актуальной для разработки цифровых систем обработки информации. В зависимости от области применения, требования к шумовому сигналу могут быть разными, например, в радиоэлектронной борьбе может требоваться создание шумовой завесы с определенным спектральным распределением и мощностью, а в криптографии может требоваться создание случайной последовательности с высокой энтропией.

Цифровые источники шума используются в различных областях, включая радиоэлектронную борьбу, где часто используется так называемая «шумовая завеса», в беспроводных коммуникациях они могут использоваться для

защиты от перехвата и расшифровки беспроводных сигналов, в криптографии для создания случайных последовательностей, которые используются для шифрования и дешифрования информации и многих других направлениях.

Использование цифровых источников шума имеет ряд преимуществ перед пассивными компонентами, таких как резисторы и диоды. В частности, цифровой генератор шума позволяет получить равномерный спектральный состав шума, имеет более высокую стабильность и контролируемость параметров.

Случайный процесс, получаемый в цифровом генераторе шума, действительно является псевдослучайным, так как основан на алгоритмах генерации случайных чисел. В частности, цифровой генератор шума позволяет получить равномерный спектральный состав шума, имеет более высокую стабильность и контролируемость параметров.

Методы и принципы исследования

Рассмотрим структурные модели генерации цифрового шума. Псевдослучайная последовательность (m-последовательность) может формироваться с помощью линейных регистров сдвига с обратными связями (ЛРСОС). Такая последовательность двоичных символов используется для получения шума с равномерной спектральной плотностью в рабочем диапазоне частот, который является «белым» [1].

Последовательность, генерируемая с помощью ЛРСОС обладает рядом свойств:

1) период последовательности предполагает распределение единиц и нулей в соотношении: количество нулей в последовательности на 1 меньше количества единиц;

2) сумма двух последовательностей, которые являются результатом циклического сдвига исходной m-последовательности, является результатом циклического сдвига исходной последовательности;

3) при скольжении окна шириной r бит вдоль m-последовательности каждая серия из r бит появляется один раз за исключением серии из r нулей.

Для любой m-последовательности свойственно: одна серия из единиц длиной r; одна серий из нулей длиной r-1; одна серия единиц и одна серия нулей длиной r-2; две серии из единиц и две серии из нулей длиной r-3; четыре серии единиц и четыре серии нулей длиной r-4; 2r-3 серий единиц и 2r-3 серий нулей длиной 1.

Другим подходом к получению цифрового шума является использование физически неклонируемых функций [2]. Каждый кольцевой генератор создается на основе уникальных физических свойств, таких как различия в технологическом процессе изготовления или в параметрах материалов. Принцип воспроизведения таких функций основан на неравномерности задержек распространения сигналов по каскадам множества кольцевых генераторов. Изменение задержек невозможно проконтролировать, следовательно, частоты генераторов будут отличаться. Данная особенность и используется для формирования значений функций.

Известны также гибридные генераторы шума, сочетающие цифровой источник первичного шума с прецизионными цифроаналоговыми преобразователями (рисунок 1) [3].

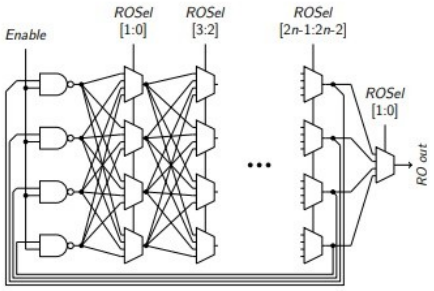

Рисунок 1 - Структура кольцевого генератора импульсов с линией задержки на основе мультиплексоров

DOI: https://doi.org/10.23670/IRJ.2023.137.24.1

В работе [4] внимания заслуживает описание метода Box-Muller, который позволяет получить практически Гауссово распределение шума и сократить сложность реализации такого источника шума, например, на программируемой пользователем вентильной матрице. Метод основан на центральной предельной теореме и гласит, что сумма независимых случайных величин имеет распределение, близкое к Гауссовому.

Белый шум может быть получен, используя лишь два независимых случайных значения. Пара независимых случайных величин является аргументами для трансцендентных функций, значения которых невозможно вычислить с помощью полиномиальных выражений. Следовательно, для аппаратной реализации потребуется только два ЛРСОС. Результаты вычислений по алгоритму Box-Mueller могут храниться в памяти, а её адресация происходит псевдослучайным образом. Дальнейшая обработка случайных значений подразумевает умножение с накоплением и преобразование интегрированного потока в аналоговую форму. Такие процедуры позволяют сгладить неравномерности Гауссового распределения. Качество такого шума можно оценить, используя функцию плотности вероятности.

В работе [5] в качестве источника шума предложен кольцевой генератор импульсов, способный перейти в метастабильное состояние. Данный метод получения энтропии в системе позволяет увеличить пропускной диапазон генератора случайных чисел при меньшем времени накопления.

Основой такого генератора является инвертор, замкнутый петлёй обратной связи, через переключатель (рисунок 2).

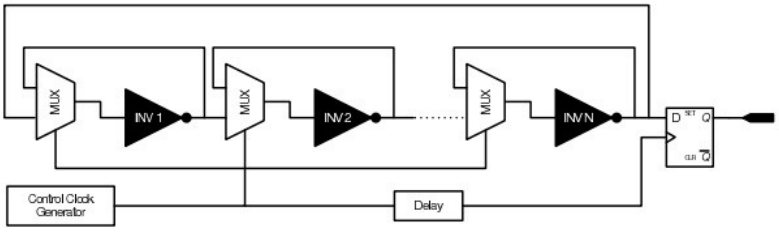

Рисунок 2 - Кольцевой генератор с метастабильным состоянием
DOI: https://doi.org/10.23670/IRJ.2023.137.24.2

Такой кольцевой генератор состоит из последовательно соединенных мультиплексоров и инверторов, причём выход инвертора соединён со следующим мультиплексором и с предыдущим. Блок управления может переводить генератор в одно из двух состояний: генерация, либо метастабильность (при отключении инверторов друг от друга). В данном случае каждый инвертор представляет собой независимый источник шума, так как в данном случае на входе находится пороговое напряжение. После этого происходит переход в режим генерации. При этом мгновенные значения напряжения внутри генератора распределены случайным образом, что приводит к высокой энтропии системы. Чередуя режимы метастабильности и генерации возможно получение случайных значений на выходе.

В случае, когда переключатель замкнут, инвертор находится в метастабильном состоянии и напряжение на его выходе колеблется вследствие теплового шума. Если из таких элементов состоит кольцевой генератор, то его начальное состояние будет зависеть от энтропии, которая возникает при колебаниях выходного напряжения.

Существуют также способы создания генераторов случайных чисел на базе программируемых логических интегральных схем. Идея состоит в том, чтобы использовать кольцевой генератор импульсов в качестве узла, задающего тактовую частоту. Кроме того, используется так называемый хаотический генератор, состоящий из последовательной цепи инверторов, охваченной обратной связью через элемент «Исключающее ИЛИ». Производительность такого генератора может быть увеличена повышением тактовой частоты, либо добавлением каскадов, соединенных параллельно. Для усиления статистических свойств могут применяться блоки последующей обработки, которые представляют собой ЛРСОС на выходе каждого хаотического генератора [6], [7], [9], [10].

Основные результаты

Анализируя представленные выше модели генерации цифрового шума, и основываясь на субъективном выборе, предлагается принять к рассмотрению модель на основе кольцевого генератора шума, используя особенность метастабильности триггера как источника энтропии в цифровой системе обработки информации.

На основе рассмотренных структурных моделей генерации цифрового шума, предлагается для дальнейшего исследования выбрать собственную структуру генератора цифрового шума на базе кольцевых генераторов (рисунок 3 а).

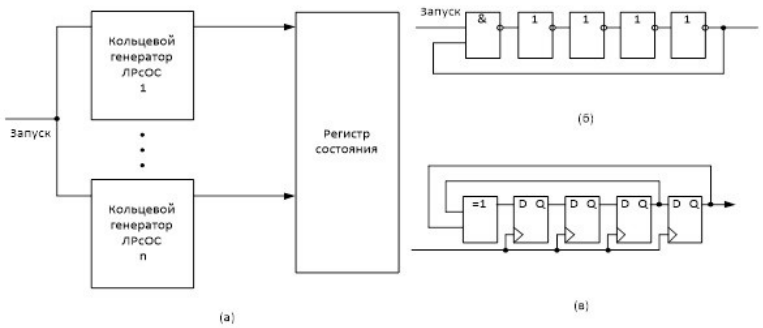

Рисунок 3 - Генератор шума:
а) общая структура генератора цифрового шума; *б)* кольцевой генератор импульсов; *в)* ЛРСОС
DOI: https://doi.org/10.23670/IRJ.2023.137.24.3

Источником метастабильного состояния триггера является кольцевой генератор импульсов, представляющий собой цепь инверторов с обратной связью. Число инверторов может быть нечётным, либо структура генератора может состоять из единственного инвертора с обратной связью через линию задержки для обеспечения режима генерации. При этом может использоваться множество отводов с каждого каскада генератора. Сокращение среднего времени между сбоями на выходе генератора позволяет формировать шум со спектральной плотностью в заданном диапазоне частот.

На основе данных положений выделим две структуры генератора цифрового шума. Первая предполагает в качестве источников шума использовать множество ЛРСОС, состояние которых в дальнейшем фиксируется в регистре, работающем на системной частоте (рис 3, б). Вторая структура использует в качестве источников шума кольцевые генераторы импульсов, обладающие более высокой спектральной плотностью мощности и подверженные влиянию питающего напряжения, температуры, а также технологического разброса параметров кристалла (рисунок 3, в).

В дальнейшем планируется провести исследование статистических свойств подобной структуры генератора с использованием графических тестов анализа псевдослучайных последовательностей.

Обсуждение

Реализуем генератор случайной последовательности из шестнадцати кольцевых генераторов с нечётным количеством каскадов от 3 до 33 (Рисунок 3, б), работающих параллельно.

Оценку качества генерируемых последовательностей можно выполнить с помощью набора тестов. Имеется ряд графических тестов, позволяющих провести анализ последовательности:

– тест на равномерность распределения в виде гистограммы, на которой отображаются частоты появления каждого значения;

– тест на автокорреляцию, представляющий собой график автокорреляции, на котором отображается корреляция между каждым значением и его задержанным экземпляром;

– тест на серийность, который используется для проверки наличия серий (последовательностей одинаковых значений) в последовательности. Для этого используется график серийности, на котором отображается количество серий заданной длины в последовательности;

– тест на частоту битов используется для проверки равномерности распределения нулей и единиц в последовательности. Для этого используется график частоты битов, на котором отображается количество нулей и единиц в последовательности;

– тест на длину последовательности использует график длины последовательности, на котором отображается количество вхождений последовательностей заданной длины в сгенерированную последовательность;

– тест на повторение блоков в виде графика повторения блоков, на котором отображается количество повторов каждого блока в последовательности;

– тест на случайность перестановок использует график перестановок, на котором отображается количество циклов в перестановке.

Проект выполнен на отладочной плате Sipeed Tang Nano 9K с FPGA Gowin GW1NR-LV9QN88PC6/I5, язык описания аппаратуры Verilog HDL.

Каждую секунду состояние генератора фиксируется в регистре и отправляется в последовательный порт компьютера (рисунок 4).

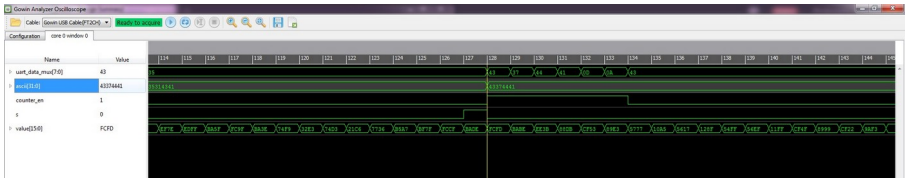

Рисунок 4 - Состояние генератора

DOI: https://doi.org/10.23670/IRJ.2023.137.24.4

В процессе эксперимента было получено и обработано 10843 отсчёта состояний генератора. Построены графические характеристики качества случайной последовательности с использованием среды GNU Octave 7.3.0 (рисунок 5, 6, 7).

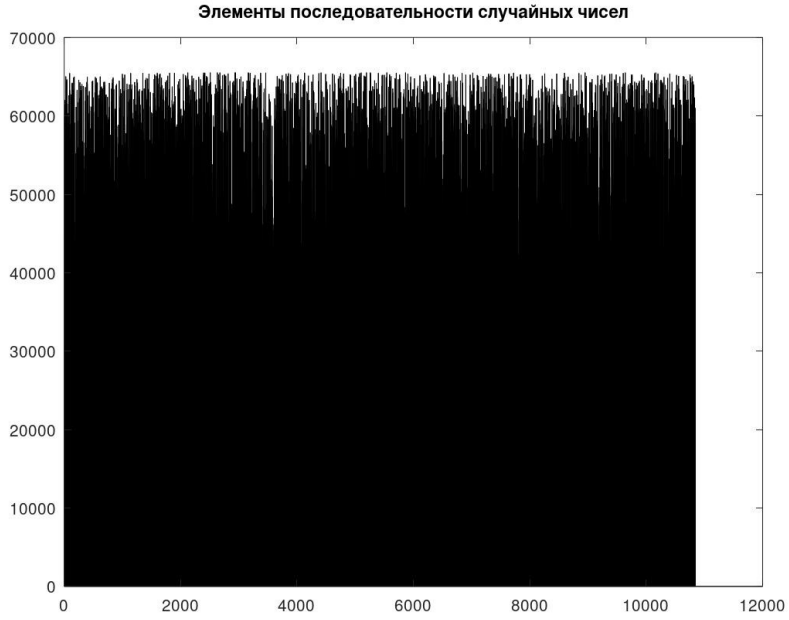

Рисунок 5 - Графические характеристики качества случайной последовательности — элементы последовательности случайных чисел

DOI: https://doi.org/10.23670/IRJ.2023.137.24.5

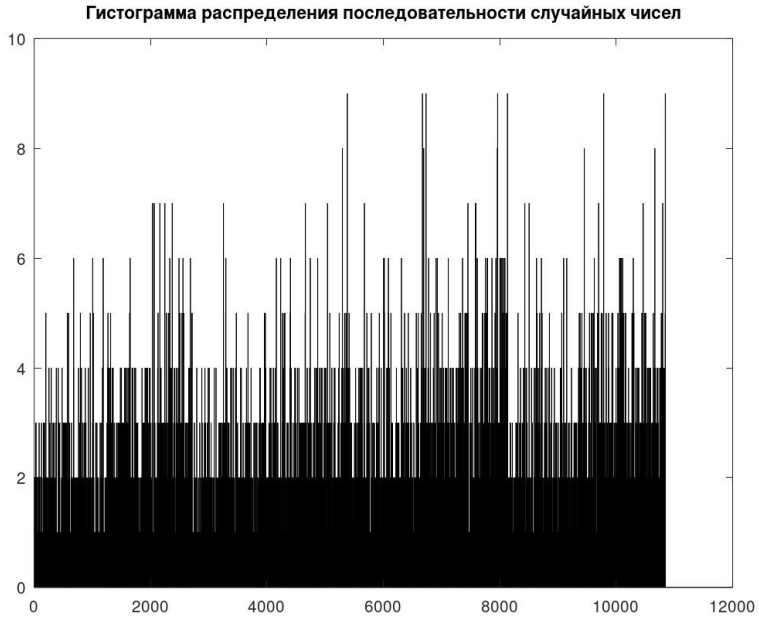

Рисунок 6 - Графические характеристики качества случайной последовательности — гистограмма распределения последовательности случайных чисел

DOI: https://doi.org/10.23670/IRJ.2023.137.24.6

Рисунок 7 - Графические характеристики качества случайной последовательности — распределение элементов последовательности случайных чисел на плоскости

DOI: https://doi.org/10.23670/IRJ.2023.137.24.7

Представление элементов случайной последовательности в виде пиксельного рисунка, полученного из битовых значений состояний генераторов(фрагмент) представлен на рисунке 8.

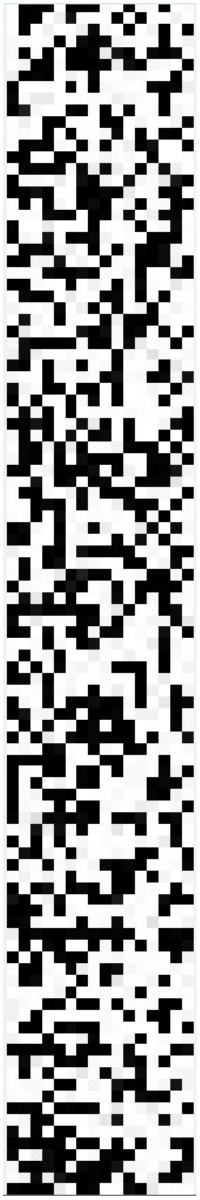

Рисунок 8 - Пиксельное изображение случайной последовательности
DOI: https://doi.org/10.23670/IRJ.2023.137.24.8

Побитовая и символьная автокорреляционная (АКФ) функция на фрагменте данных в 10240 бит представлена на рисунке 9.

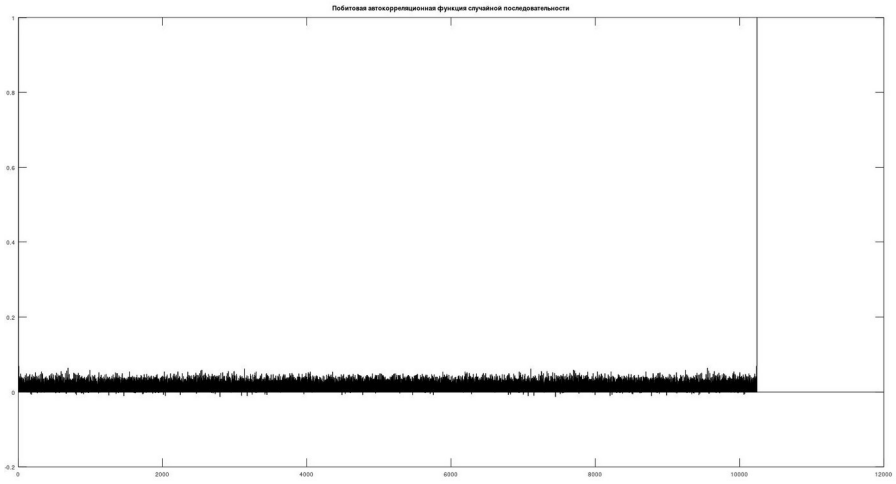

Рисунок 9 - Побитовая автокорреляционная функция случайной последовательности
DOI: https://doi.org/10.23670/IRJ.2023.137.24.9

Символьная АКФ на всей последовательности случайных чисел в 10843 отсчёта по 16 бит представлена на рисунке 10.

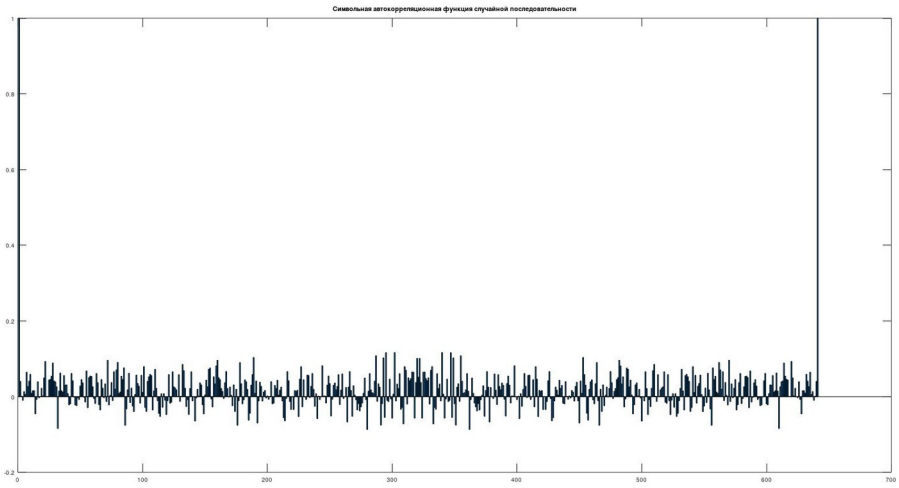

Рисунок 10 - Символьная автокорреляционная функция случайной последовательности
DOI: https://doi.org/10.23670/IRJ.2023.137.24.10

Заключение

Исходя из анализа результатов исследования видно, что выбранная структура генератора цифрового шума формирует случайную последовательность и может быть использована для задач подобного направления. В дальнейшем исследование может быть дополнено другими методами анализа. Например, для повышения безопасности генераторов цифрового шума на основе ЛРСОС могут использоваться такие методы, как добавление шума к начальному состоянию регистра, использование нескольких ЛРСОС с разными начальными состояниями и обратной связью, а также применение криптографических преобразований к выходной последовательности.

Конфликт интересов

Не указан.

Рецензия

Гибадуллин Р.Ф., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация
DOI: https://doi.org/10.23670/IRJ.2023.137.24.11

Conflict of Interest

None declared.

Review

Gibadullin R.F., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation
DOI: https://doi.org/10.23670/IRJ.2023.137.24.11

Список литературы / References

1. Мардер М. Цифровые генераторы шума / М. Мардер, В. Федосов // Радио. — 1990. — 8.

2. Заливако С.С.. Схемная реализация комбинированной физически неклонируемой функции для генерирования действительно случайных числовых последовательностей / С.С. Заливако, А.А. Иванюк // Доклады БГУИР; — 2013: БГУИР, 2013.

3. Gaussian Noise Generator (GNG) Reference Design // Altera Corporation. — 2016. — URL: https://cdrdv2-public.intel.com/654047/gaussian-noise-generator-reference-design.pdf (accessed: 12.09.2023)

4. Çağlan A.. FPGA Implementation of AWGN Noise Generator Using Box-Muller Method / A. Çağlan, E. İnceöz, E. Balcısoy, M. E. Özbek, E. Çavuş; — Turkey: Zonguldak, 2016.

5. Vasyltsov I. Fast Digital TRNG Based on Metastable Ring Oscillator / I. Vasyltsov, E. Hambardzumyan, Y.S. Kim, B. Karpinskyy. — 2008. — №5154. — URL: https://doi.org/10.1007/978-3-540-85053-3_11 (accessed: 22.07.2023)

6. Чулков В. А. Кольцевые генераторы импульсов в цифровых преобразователях информации / В. А. Чулков // Известие вузов. Приборостроение. — 2019. — 62-1.

7. Ramji G. Efficient Design of Chaos Based 4 Bit True Random Number Generator on FPGA / G. Ramji, A. Pandey, R. K. Baghel // International Journal of Engineering & Technology. — 2018. — 7(3).

8. Чулков В. А. Кольцевые генераторы импульсов на ПЛИС / В. А. Чулков, А. В. Медведев // Известие вузов. Приборостроение. — 2009. — 12.

9. Чулков В. А. Интерполирующие устройства синхронизации и преобразователи информации / В. А. Чулков — М: Физматлит, 2010. — 320 с.

10. Чулков В.А. Функциональные генераторы на основе прямого цифрового синтеза / В.А. Чулков // XXI век: итоги прошлого и проблемы настоящего плюс. — 2022. — 3(59).

Список литературы на английском языке / References in English

1. Marder M. Tsifrovye generatory shuma [Digital Noise Generators] / M. Marder, V. Fedosov // Radio. — 1990. — 8. [in Russian]

2. Zalivako S.S.. Shemnaja realizatsija kombinirovannoj fizicheski nekloniruemoj funktsii dlja generirovanija dejstvitel'no sluchajnyh chislovyh posledovatel'nostej [Schematic Implementation of a Combined Physically Unclonable Function for Generating Truly Random Numerical Sequences] / S.S. Zalivako, A.A. Ivanjuk // Reports of BSUIR; — 2013: BGUIR, 2013. [in Russian]

3. Gaussian Noise Generator (GNG) Reference Design // Altera Corporation. — 2016. — URL: https://cdrdv2-public.intel.com/654047/gaussian-noise-generator-reference-design.pdf (accessed: 12.09.2023)

4. Çağlan A.. FPGA Implementation of AWGN Noise Generator Using Box-Muller Method / A. Çağlan, E. İnceöz, E. Balcısoy, M. E. Özbek, E. Çavuş; — Turkey: Zonguldak, 2016.

5. Vasyltsov I. Fast Digital TRNG Based on Metastable Ring Oscillator / I. Vasyltsov, E. Hambardzumyan, Y.S. Kim, B. Karpinskyy. — 2008. — №5154. — URL: https://doi.org/10.1007/978-3-540-85053-3_11 (accessed: 22.07.2023)

6. Chulkov V. A. Kol'tsevye generatory impul'sov v tsifrovyh preobrazovateljah informatsii [Ring Pulse Generators in Digital Information Converters] / V. A. Chulkov // News of Universities. Instrumentation. — 2019. — 62-1. [in Russian]

7. Ramji G. Efficient Design of Chaos Based 4 Bit True Random Number Generator on FPGA / G. Ramji, A. Pandey, R. K. Baghel // International Journal of Engineering & Technology. — 2018. — 7(3).

8. Chulkov V. A. Kol'tsevye generatory impul'sov na PLIS [Ring Pulse Generators on FPGA] / V. A. Chulkov, A. V. Medvedev // News of Universities. Instrumentation. — 2009. — 12. [in Russian]

9. Chulkov V. A. Interpolirujuschie ustrojstva sinhronizatsii i preobrazovateli informatsii [Interpolating Synchronization Devices and Information Converters] / V. A. Chulkov — M: Fizmatlit, 2010. — 320 p. [in Russian]

10. Chulkov V.A. Funktsional'nye generatory na osnove prjamogo tsifrovogo sinteza [Functional Generators Based on Direct Digital Synthesis] / V.A. Chulkov // XXI Century: the Results of the Past and the Problems of the Present Plus. — 2022. — 3(59). [in Russian]