http://dx.doi.org/10.35596/1729-7648-2023-29-1-36-47

Оригинальная статья
Original paper

УДК 004.312

КОМБИНИРОВАННЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ НА ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМАХ

А. А. ИВАНЮК

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

Поступила в редакцию 05.10.2022

Аннотация. Показана практическая возможность реализации генераторов случайных чисел на программируемых логических интегральных схемах (англ. FPGA – field programmable gate arrays) путем комбинирования различных физически неклонируемых функций. Предложена компактная и масштабируемая схема цифрового источника случайных чисел на основе асинхронного триггера *D*-типа, сочетающая в себе характеристики физически неклонируемых функций как статической памяти, так и кольцевого осциллятора. В отличие от существующих генераторов случайных чисел предложенная схема может быть использована для решения задачи неклонируемой идентификации цифровых устройств. Приведены экспериментальные результаты, полученные при реализации предложенной схемы генератора на основе программируемых логических интегральных схем типа FPGA Xilinx Zynq. Описаны основные режимы функционирования, вероятностные и статистические характеристики числовых последовательностей, генерируемых предложенной схемой.

Ключевые слова: генератор случайных чисел, физически неклонируемые функции, программируемые логические интегральные схемы.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Благодарность. Автор выражает искреннюю благодарность резиденту Парка высоких технологий компании SK Hynix Memory Solutions Eastern Europe за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

Для цитирования. Иванюк, А. А. Комбинированный генератор случайных чисел на программируемых логических интегральных схемах / А. А. Иванюк // Цифровая трансформация. 2023. Т. 29, № 1. С. 36–47. http://dx.doi.org/10.35596/1729-7648-2023-29-1-36-47.

COMBINED RANDOM NUMBER GENERATOR ON PROGRAMMABLE LOGIC INTEGATED CIRCUITS

ALEXANDER A. IVANIUK

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Submitted 05.10.2022

Abstract. The paper shows the practical possibility of implementing random number generators on field programmable gate arrays (FPGA) by combining various physically unclonable functions. A compact and scalable scheme of a digital random number source based on an asynchronous flip-flop of the *D*-type is proposed, which combines the characteristics of a static memory physically unclonable functions and a ring oscillator physically unclonable functions. Unlike existing random number generators, the proposed scheme can be used to solve the problem of unclonable identification of digital devices. The article presents experimental results obtained by the proposed generator circuit based on the FPGA Xilinx Zynq. The main modes of operation, probabilistic and statistical characteristics of numerical sequences, generated by the proposed scheme are described.

Keywords: random number generator, physically unclonable functions, programmable logic integrated circuits.

Conflict of interests. The author declares no conflict of interests.

Gratitude. The author expresses his sincere gratitude to the HTP resident of the SK Hynix Memory Solutions Eastern Europe company for the equipment provided for carrying out experiments within the framework of the joint laboratory with the Belarusian State University of Informatics and Radioelectronics.

For citation. Ivaniuk A. A. (2023) Combined Random Number Generator on Programmable Logic Integrated Circuits. *Digital Transformation.* 29 (1), 36–47. http://dx.doi.org/10.35596/1729-7648-2023-29-1-36-47 (in Russian).

Введение

Генераторы случайных чисел (ГСЧ) находят широкое применение в таких приложениях, как компьютерное имитационное моделирование, криптографическая защита информации, тестирование и диагностика технических объектов, компьютерные игры, создание и обработка мультимедиа материалов и т. п. Генераторы случайных чисел по своей природе делятся на два класса: генераторы псевдослучайных чисел (ГПСЧ) и генераторы истинно случайных чисел (ГИСЧ). Построение ГПСЧ, как правило, осуществляется на основе некоторого определенного алгебраического правила, позволяющего получать последовательности чисел, близкие по своим характеристикам к случайным, но обладающие свойством воспроизводимости. В свою очередь, ГИСЧ вырабатывают последовательности чисел, каждый элемент которых практически невозможно вычислить либо предсказать, основываясь на информации о предыдущих элементах[1]. Исследованиям в области построения и анализа ГИСЧ посвящены многие работы как зарубежных, так и отечественных ученых, среди которых можно отметить научные школы академика Ю. С. Харина, профессора А. Е. Леусенко, Э. А. Бакановича и др.

В цифровых системах выделяют следующие источники случайности: физические, системные и основанные на действиях оператора[1]. В современных приложениях предпочтительными являются источники случайности, базирующиеся на физических процессах. Среди всего многообразия существующих методов синтеза ГИСЧ можно выделить класс относительно новых методов, основанных на хаотических, непредсказуемых физических процессах, происходящих внутри цифровых интегральных схем при их функционировании. Такие методы используют элементы цифровой схемотехники и не требуют реализации аналого-цифровых преобразований случайных физических величин для получения последовательностей случайных чисел. Методы объединяются под общим названием «физическая криптография» [1], в основе которой лежат физически неклонируемые функции (ФНФ) [2].

В статье рассмотрено новое схемотехническое решение на основе ФНФ для построения генераторов истинно случайных чисел. В отличие от существующих генераторов предлагаемый ГИСЧ обладает незначительной аппаратурной избыточностью, легко масштабируется под различную разрядность генерируемых чисел и может применяться для решения задачи уникальной идентификации цифровых устройств.

Общие подходы к построению генераторов случайных чисел

Генераторы случайных чисел, которые используются в составе готовых устройств, как правило, сертифицируются (стандартизируются) и должны соответствовать определенным рекомендациям (стандартам). Примерами таких рекомендаций могут служить документы NIST [3, 4], в которых описаны возможные подходы к построению аппаратных ГСЧ. На рис. 1 представлена обобщенная структура генераторов случайных чисел, рекомендованная NIST для криптографических приложений.

Согласно представленной на рис. 1 структуре, физически неклонируемые функции являются перспективными источниками цифрового шума, которые не требуют наличия блока оцифровки (аналого-цифровых преобразователей) и могут проектироваться и изготавливаться как составные части цифровых систем на кристалле. Основные свойства ФНФ – неклонируемость и случайность, обусловленные тем, что при изготовлении ФНФ с применением различных технологий невозможно создать две идентичные копии устройства (схемы), обладающие одинаковыми характеристиками.

[1] Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел: СТБ 34.101.47–2017. Введ. 01.09.2017. Минск, 2017. 18 с.

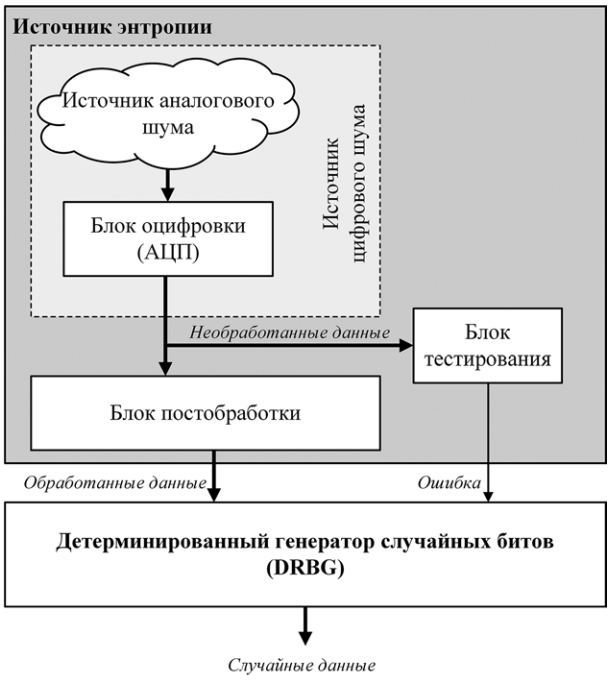


Рис. 1. Структура криптографического генератора случайных чисел согласно рекомендации NIST
Fig. 1. The structure of the cryptographic random number generator according to the recommendation of NIST

Неповторимость значений характеристик обусловлена случайными вариациями физических структур материалов, геометрией межсоединительных проводников и компонент, влияние на которые со стороны изготовителя невозможно. Таким образом, ФНФ являются физическими источниками уникальности (неклонируемости) и случайности. Вырабатываемые ФНФ случайные данные, как правило, не пригодны для применения, особенно в криптографических приложениях. Связано это с тем, что необработанные данные от ФНФ не обладают необходимыми статистическими свойствами. Например, такие данные могут не соответствовать заданному закону распределения для применения в конкретных приложениях.

Для решения описанной проблемы применяются различные методы и алгоритмы постобработки этих данных. В силу того, что происходящие физические процессы при генерации цифрового шума являются неконтролируемыми, могут происходить сбои в генерации случайных данных. Один из распространенных видов сбоев – так называемое залипание генерируемых случайных данных, выражающееся в многократном повторении одного и того же символа либо серии символов. Для обнаружения подобных сбоев, причинами которых могут быть и сторонние атаки злоумышленников, применяют специальные статистические тесты. По рекомендации NIST такими тестами являются Repetition Count Test (тест на последовательность одинаковых бит) и Adaptive Proportion Test (тест на пропорции повторяющихся бит). Если один из тестов не пройден, блок тестирования (рис. 1) генерирует сообщение об ошибке, сигнализирующее о том, что сгенерированные данные неслучайны. При прохождении тестов обработанные случайные данные поступают на блок DRBG (детерминированный генератор случайных битов), который, по сути, представляет собой генератор псевдослучайных чисел [3]. По рекомендациям NIST для реализаций блока DRBG могут быть использованы три криптографических метода – AES, SHA либо HMAC [4], обеспечивающих необходимый уровень криптостойкости.

Для построения схем ГИСЧ (источников цифрового шума) чаще всего применяют схемы ФНФ кольцевого осциллятора [2, 5]. Основная его особенность заключается в генерировании периодических сигналов с уникальной непредсказуемой частотой и фиксировании их случайного значения на триггерных схемах. В статье предлагается схема комбинированного генератора случайных чисел, в которой используются два типа ФНФ – кольцевого осциллятора и статической памяти [2], что позволяет в том числе вырабатывать уникальные идентификаторы цифровых устройств и проводить предварительную постобработку случайных данных.

Схема комбинированного генератора истинно случайных чисел

Основу предлагаемой схемы ГИСЧ составляют асинхронный триггер *D*-типа LDE, инвертор INV, мультиплексор MUX и синхронный триггер *T*-типа TFF. На рис. 2 приведена базовая схема однобитного генератора истинно случайных чисел, имеющая следующие входы и выходы: *DI* – вход для внешних данных; *GE* – управляющий вход загрузки данных в триггер; *LE* – управляющий вход активации режима кольцевого осциллятора; *Q* – диагностический выход и выход для идентификационных данных; *RB* – основной выход случайных данных.

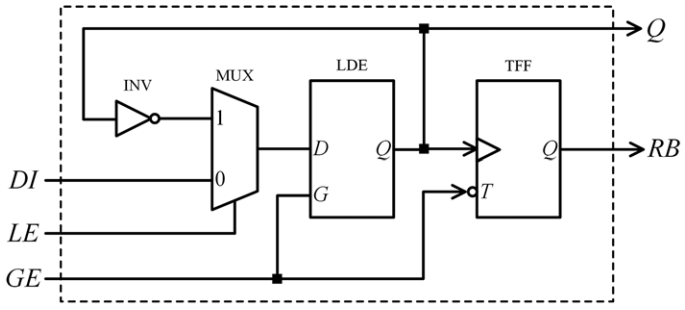


Рис. 2. Базовая схема комбинированного генератора истинно случайных чисел
Fig. 2. The basic scheme of the combined random number generator

Техническая идея, лежащая в основе предложенной схемы, заключается в комбинировании различных схем ФНФ с целью реализации ГИСЧ, обладающего свойством технологической невоспроизводимости и позволяющего, в том числе, решать задачу неклонируемой идентификации. Представленную на рис. 2 схему можно разделить на четыре функциональные части: регистр хранения LDE с возможностью записи внешних данных *DI* и выходом *Q*; источник уникального бита идентификации, которым является триггер LDE в режиме инициализации (выход *Q*); управляемый кольцевой генератор, образующийся при значении *LE* = 1 и включающий в себя схему триггера LDE, инвертора INV и мультиплексора MUX; схема генерирования случайного значения на выходе *RB*, представленная синхронным *T*-триггером TFF. В общем случае вся схема способна вырабатывать случайные значения на обоих выходах *Q* и *RB*.

Следует отметить, что предложенная схема может быть реализована различными способами в зависимости от технологии и библиотечных функциональных элементов. Например, для FPGA-технологии схемная реализация генератора может представлять собой два LUT-блока и два триггера. Однако для обеспечения непредсказуемости поведения схемы в режиме инициализации схему асинхронного триггера лучше реализовать также на LUT-блоках (U0 и U1), как это показано на рис. 3.

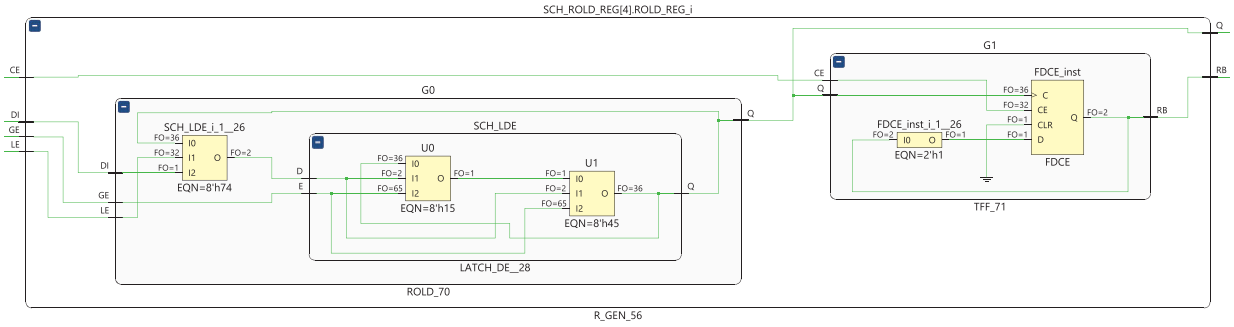


Рис. 3. Схемная реализации генератора на ресурсах FPGA
Fig. 3. Schematic implementation of the generator on FPGA resources

Рассмотрим подробнее режимы функционирования предложенной схемы.

1. *Режим инициализации*. В данный режим схема попадает при включении питания и удержании управляющего сигнала *GE* = 0. При такой конфигурации начальное значение на выходе $Q = X$ ($X \in \{0, 1\}$) будет случайным и непредсказуемым и схожим по поведению с ФНФ статической памяти [2]. С учетом реализации триггера TFF на FPGA с использованием примитива FDCE (рис. 3) начальное значение на выходе *RB* в режиме инициализации будет всегда постоянным и предсказуемым.

2. *Режим кольцевого осциллятора*. Достижим при установке управляющих сигналов *LE* = 1 и *GE* = 1. В данном случае образуется отрицательная обратная связь, соединяющая выход *Q* триггера LDE со входом *D* через схему инвертора INV. При этом на выходе *Q* всей схемы будет наблюдаться последовательная смена значений с частотой F_Q, определяемой задержками распространения сигала через все структурные элементы схемы, включая задержки на линиях межсоединений. Такая конфигурация схемы идентична схеме ФНФ кольцевого осциллятора [2, 5], при этом значение F_Q будет являться уникальным и непредсказуемым.

3. *Режим загрузки данных*. Активируется при установке управляющих сигналов *LE* = 0 и *GE* = 1. При этом значение *d*, поданное на вход *DI*, будет записано в триггер LDE и отображено на выходе *Q* = *d* всей схемы.

4. *Режим хранения*. Схож с режимом инициализации, но отличается тем, что в него схема переходит после режима кольцевого осциллятора либо после режима загрузки данных. В случае переключения сигнала *GE* = 1→0 при *LE* = 0 значение на выходе *Q* будет равно *d*, когда *GE* = 1→0 при *LE* = 1 зафиксированные значения на выходах *Q* и *RB* будут случайными и непредсказуемыми в силу многих факторов, которые описаны ниже.

Предложенная схема может быть расширена до *N*-разрядной путем объединения в регистровую схему с общим управлением по входам *LE* и *GE* и *N*-разрядными выходными шинами *Q* и *RB*. Это позволяет расширить функционал схемы, например, путем построения *N*-разрядных генераторов циклических последовательностей. На рис. 4 представлены некоторые варианты реализации различных схем многоразрядных генераторов на основе базовой схемы однобитного ГИСЧ.

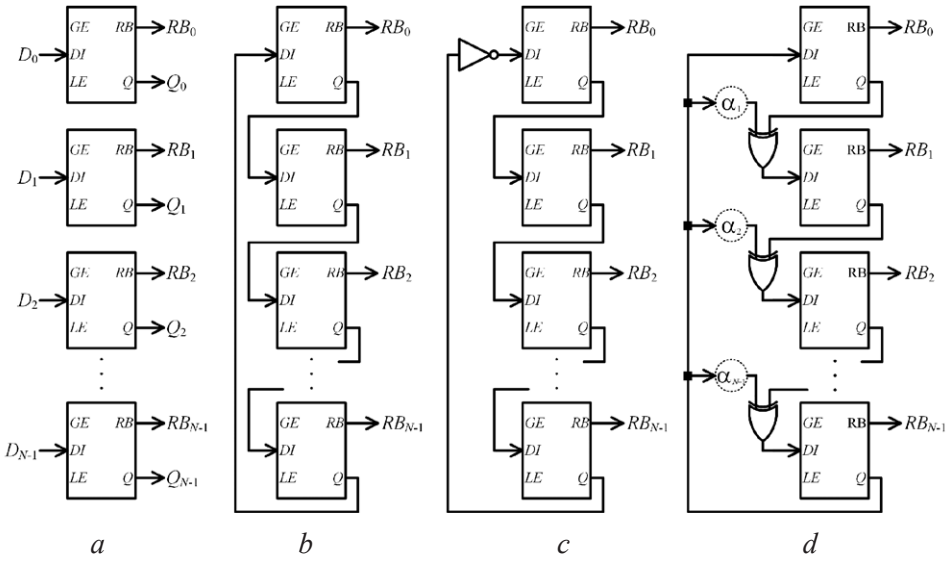


Рис. 4. Примеры схем: *a* – регистра хранения; *b* – генератора циклической последовательности; *c* – генератора последовательности Джонсона; *d* – генератора М-последовательности
Fig. 4. Examples of schemes: *a* – of a storage register; *b* – of a cyclic sequence generator; *c* – of the Johnson sequence generator; *d* – of M-sequence generator

Схема регистра хранения (рис. 4, *a*) может функционировать во всех описанных режимах базовой схемы. В такой конфигурации схема представляет собой *N* независимых однобитных источников случайных данных, выполняющих роль разрядов регистра случайного числа с возможностью загрузки внешних данных. Варианты схем, представленных на рис. 4, *b*–*d*, осуществляют в режиме 3 (загрузка данных) генерацию различных последовательностей: циклической, Джонсона и М-последовательности соответственно.

В режиме 1 (инициализация) все схемы будут находиться в режиме ФНФ статической памяти и вырабатывать уникальные значения на своих выходах Q_0–Q_{N-1}, которые можно использовать для генерирования неклонируемых *N*-разрядных идентификаторов (встроенных аппаратных водяных знаков), позволяющих решать задачу аутентификации цифровых устройств.

В режиме 2 (кольцевой осциллятор) все представленные схемы будут функционировать как *N* независимых ФНФ кольцевого осциллятора, вырабатывая на выходах Q_0–Q_{N-1} случайные символы с различными статистическими и вероятностными характеристиками. Переключая схемы из режима 2 в режим 4 (хранение), сгенерированные случайные значения будут зафиксированы на базовых элементах, которые, в свою очередь, могут служить начальными значениями для схем

генераторов различных детерминированных (псевдослучайных) последовательностей, а на выходах RB_0–RB_{N-1} будут дополнительно вырабатываться случайные символы, отличные от тех, которые появятся на выходах Q_0–Q_{N-1}.

Экспериментальная часть

Для проверки статистических и вероятностных характеристик предложенных схем была спроектирована аппаратно-программная система проведения экспериментов на программируемых логических интегральных схемах (ПЛИС) типа FPGA Xilinx Zynq XC7Z010, входящая в состав платы быстрого прототипирования Digilent Zybo Z7[2]. Система построена на основе встроенного процессора ARM Cortex-A9, служащего для управления схемой генератора и обмена данными с рабочей станцией. Схема генератора была спроектирована на языке VHDL с параметром $N = 32$ и дополнена устройством управления, блоками анализа частот каждого вывода генератора.

В первом эксперименте осуществлялась генерация уникального 32-битного идентификатора путем многократного включения системы в режиме инициализации. Для этого использовали четыре идентичные платы Digilent Zybo Z7, сконфигурируемые одним и тем же bit-образом проекта. Для каждого экземпляра экспериментальной схемы оценивалась вероятность встречаемости единичного символа на каждом выходе

$$P_i^1\left(Q_i^d, E\right) = \frac{1}{E}\sum_{e=1}^{E} Q_i^d, \tag{1}$$

где $Q_i^d \in \{0,1\}$ – значение символа на i-м выходе схемы ($i \in [0, N-1]$), реализованной на плате с индексом $d \in [1, D]$; D, E – число плат и экспериментов соответственно.

На рис. 5 приведены значения $P_i^1\left(Q_i^d, E\right)$ для следующих параметров: $N = 32$, $D = 4$, $E = 100$.

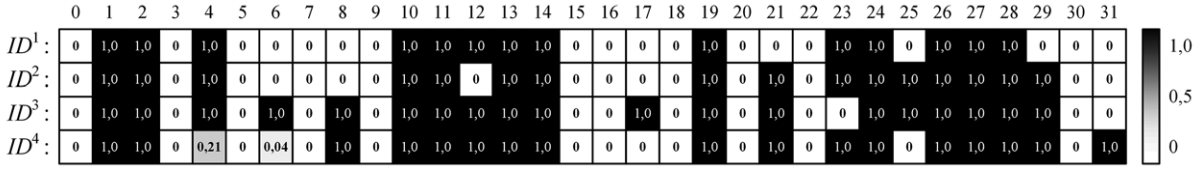


Рис. 5. Тепловая карта значений $P_i^1\left(Q_i^d, E\right)$ для четырех реализованных систем
Fig. 5. Heat map of $P_i^1\left(Q_i^d, E\right)$ values for four implemented systems

Как видно из рис. 5, подавляющее большинство разрядов имеют стабильные значения, для которых $P_i^1(Q_i^d, E) = 0$ либо $P_i^1(Q_i^d, E) = 1$. В силу того, что базовая схема асинхронного D-триггера в своей основе представляет собой управляемый бистабильный элемент (асинхронный RS-триггер), наличие асимметрии в реализации конкретного экземпляра этой схемы определяет его стабильное начальное значение. Меньшая асимметрия внутренней реализации триггера приводит схему в метастабильное состояние, при котором $0 < P_i^1(Q_i^d, E) < 1$. Так, полученное значение $P_4^1(Q_4^4, 100) = 0,21$ свидетельствует о более высокой степени симметрии схемы триггера в сравнении с остальными.

Примем полученные для всех плат значения в качестве значений разрядов их идентификаторов и оценим основные характеристики (стабильность, уникальность, единообразие), которые применяются в том числе для оценки ФНФ [6]. Сперва введем понятие идеального N-разрядного идентификатора устройства, значение которого получается по следующему мажоритарному правилу: $ID^d = \{id_0^d, id_1^d, id_2^d, ..., id_{N-1}^d\}$, где $id_i^d = 0$ – если $P_i^1(Q_i^d, E) < 0,5$, и $id_i^d = 1$ – если $P_i^1(Q_i^d, E) \geq 0,5$. Оценим стабильность идентификаторов по следующей формуле:

$$S\left(ID^d\right) = 1 - \frac{1}{N}\sum_{i=0}^{N-1}\left|id_i^d - P_i^1\left(Q_i^d, E\right)\right|. \tag{2}$$

По сути, значение $S(ID^d)$ есть величина, обратная коэффициенту битовых ошибок BER (Bit Error Rate) при многократном извлечении значения идентификатора. Таким образом, получаем:

[2] ZyboZ7: Zynq-7000 ARM/FPGA SoC Development Board [Electronic Resource]. Mode of access: https://digilent.com/reference/programmable-logic/zybo-z7/start. Date of access: 19.09.2022.

$S(ID^1) = S(ID^2) = S(ID^3) = 1$ и $S(ID^4) = 0{,}9921$. Для оценки уникальности идентификаторов используем удельное расстояние по Хэммингу между двумя бинарными *N*-разрядными векторами

$$HD_N^{a,b} = \frac{1}{N} HD\left(ID^a, ID^b\right), \tag{3}$$

где HD – расстояние по Хэммингу между векторами ID^a и ID^b, $a,b \in [1,D]$.

В ходе анализа экспериментальных данных получены следующие значения: $HD_{32}^{1,2} = 0{,}125$, $HD_{32}^{1,3} = 0{,}21875$, $HD_{32}^{1,4} = HD_{32}^{2,3} = HD_{32}^{2,4} = 0{,}15625$, $HD_{32}^{3,4} = 0{,}1875$. Удельную уникальность вычисляли как среднее арифметическое значений $HD_N^{a,b}$ всех возможных пар C_D^2 идентификаторов из D возможных [6]

$$U^D = \frac{1}{C_D^2} \cdot \sum_{a=1}^{C_D^2-1} \sum_{b=a+1}^{C_D^2} HD_N^{a,b}. \tag{4}$$

Для рассматриваемого случая $U^4 = 0{,}1666$, при этом минимальное значение удельной уникальности для различных четырех 32-битных идентификаторов равно 0,04166. При оценке идентификаторов часто применяют дополнительную метрику единообразия [6], которая отражает в них соотношение нулевых и единичных символов:

$$UF\left(ID^d\right) = 1 - 2 \cdot \left| \frac{WH\left(ID^d\right)}{N} - 0{,}5 \right|, \tag{5}$$

где $WH(ID^d)$ – вес по Хэммингу двоичного вектора ID^d.

Полученные идентификаторы обладают высоким значением данной метрики: $UF(ID^1) = 0{,}875$, $UF(ID^2) = 1{,}0$, $UF(ID^3) = 0{,}8125$, $UF(ID^4) = 0{,}9375$. Приведенные значения стабильности, уникальности и единообразия свидетельствуют о потенциальной возможности практического применения данного подхода для реализации неклонируемых аппаратных идентификаторов, в том числе для решения задач защиты авторских прав на цифровые системы.

Следующим этапом эксперимента стала оценка частот вырабатываемых сигналов в режиме кольцевого осциллятора. Измерения частот сигналов $F(Q_i^d)$, вырабатываемых на выходах Q_0–$Q_{N\text{-}1}$, проводились дополнительными схемами контроля, реализованными на ПЛИС, во временном окне $MW = kP_{SYS\_CLK} = 1{,}32$ мс для всех четырех экземпляров генератора (k – коэффициент масштабирования, k = 65536; P_{SYS_CLK} – период системного синхросигнала, P_{SYS_CLK} = 20 нс).

На рис. 6 представлены графики значений измеренных частот $F(Q_i^d)$.

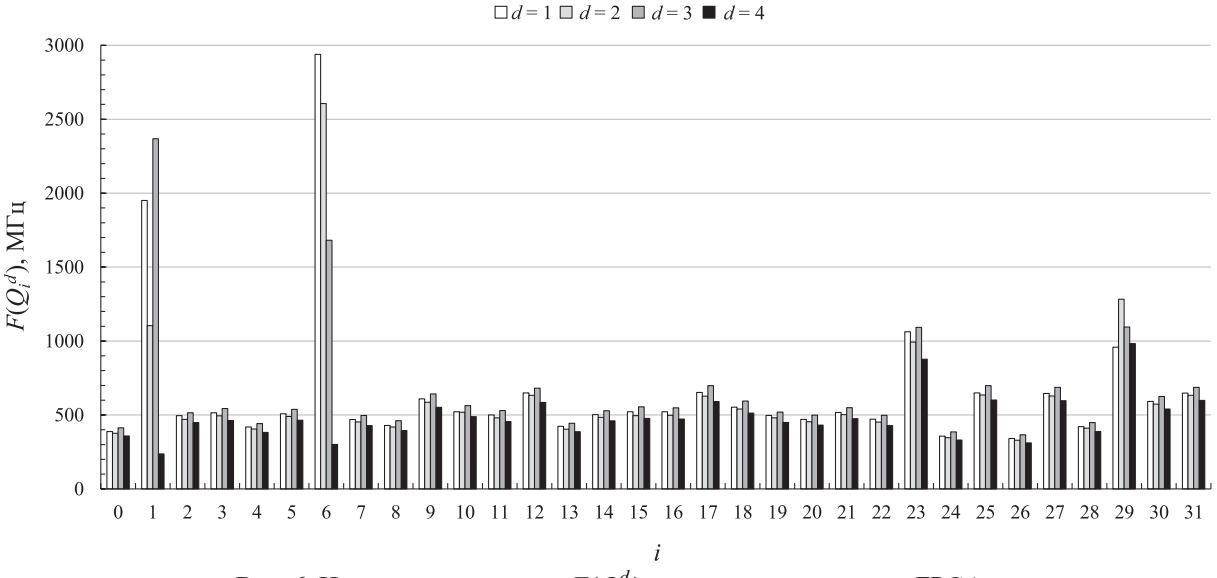


Рис. 6. Измеренные частоты $F(Q_i^d)$ на четырех различных FPGA
Fig. 6. Measured frequency $F(Q_i^d)$ values on four different FPGAs

Как видно из графиков, значения $F(Q_i^d)$ различаются как по разрядам генератора, так и по версиям его реализации на различных ПЛИС. Измерения частот проводились при последовательном переключении генераторов из режима 1 в режим 2 и далее в режим 4.

Присутствующие на графиках рис. 6 выбросы (позиции $i = 1$ и $i = 6$), скорее всего, обусловлены высокочастотными колебаниями, которые, в свою очередь, привели к аномальному функционированию измеряющих счетчиков, реализованных также на ресурсах FPGA. Тем не менее представленные экспериментальные данные являются подтверждением основных положений ФНФ, в частности, уникальности и неклонируемости ФНФ кольцевых генераторов.

При завершении режима осцилляции с дальнейшим переходом в режим хранения на асинхронных триггерах LDE может наблюдаться эффект автоколебаний, вызванный нарушением временных параметров предустановки и удержания сигналов на входах *D* и *G*. Подобный эффект впервые был описан в [7] и использован при анализе поведения ФНФ типа арбитр [8]. Для наблюдения эффекта автоколебаний в предложенной схеме выполнили ряд экспериментов, в которых проводили регистрацию числа передних фронтов автоколебаний $A(Q_i^d, k)$ после завершения режима 2 во временном окне $MW = kP_{SYS\_CLK}$ с переходом в режим 4. В табл. 1 представлены усредненные значения $A(Q_i^d, k)$ для $k = 1$ на повторяющихся 100 запусках четырех систем.

Таблица 1. Средние значения $A(Q_i^d, k)$ для четырех реализаций на различных FPGA
Table 1. Average values of $A(Q_i^d, k)$ for four implementations on different FPGAs

d	*i*															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	26	2	5	4	3	4	1	7	70	3	3	6	2	6	0	2
2	46	1	4	2	3	3	1	3	34	2	7	11	1	42	1	1
3	4	1	11	4	2	1	1	2	9	1	0	13	0	6	3	3
4	11	2	4	3	6	3	2	4	0	3	0	9	0	13	1	3
d	*i*															
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	2	2	1	1	14	6	40	64	6	1	5	1	11	7	4	2
2	2	2	2	2	12	1	5	19	5	1	5	1	33	23	4	1
3	2	0	1	1	11	1	5	8	3	1	3	2	6	4	2	1
4	2	2	2	4	9	4	8	27	14	2	14	2	6	55	4	0

В совокупности с имеющимися различными частотами $F(Q_i^d)$ и подавляющим числом триггеров, обладающих описанным эффектом, для которых значение $A(Q_i^d, k) > 0$, выдвинем предположение, что представленная схема комбинированного генератора может быть использована в качестве источника цифрового шума. Для подтверждения этого предположения при помощи формулы (5) оценим соотношение вырабатываемых нулевых и единичных символов на выходах *Q* и *RB* каждым *i*-м генератором на серии из $E = 1000$ повторяющихся экспериментов для различных значений коэффициента масштабирования *k*. Пусть $q_i^d(e,k) \in \{0,1\}$ и $rb_i^d(e,k) \in \{0,1\}$ есть значения, вырабатываемые генератором с индексом *i* на FPGA с номером *d* в ходе эксперимента $e \in [1, E]$ и коэффициентом масштабирования *k* на выходе *Q* и *RB* соответственно. Оценим значение метрики единообразия (5) для векторов $Q_i^d(E,k) = \{q_i^d(1,k), q_i^d(2,k), q_i^d(3,k), ..., q_i^d(E,k)\}$ и $RB_i^d(E,k) = \{rb_i^d(1,k), rb_i^d(2,k), rb_i^d(3,k), ..., rb_i^d(E,k)\}$, полученных для всех генераторов на четырех FPGA путем их переключения в режим 2, удержания в этом режиме на протяжении *k* периодов P_{SYS_CLK} с дальнейшим переключением в режим 4.

На рис. 7 приведены значения метрик $UF(Q_i^d(E,k))$ и $UF(RB_i^d(E,k))$ для $k = 1$ и $k = 64$. Так, для $k = 1$ наблюдается подавляющее большинство нулевых значений (87 из 128 возможных) $UF(Q_i^d(E,k)) = 0$, обусловленных выработкой постоянного значения на выходах *Q*. Одновременное измерение значений на выходах *RB* дало всего лишь 21 значение $UF(RB_i^d(E,k)) = 0$. При увеличении коэффициента масштабирования до $k = 64$ число значений $UF(Q_i^d(E,k)) = 0$ сократилось до четырех, а $UF(RB_i^d(E,k)) = 0$ – до нуля. При этом абсолютные значения $UF(RB_i^d(E,k))$ близки к максимальному единичному значению, что удовлетворяет условию прохождения теста на пропорцию повторяющихся бит.

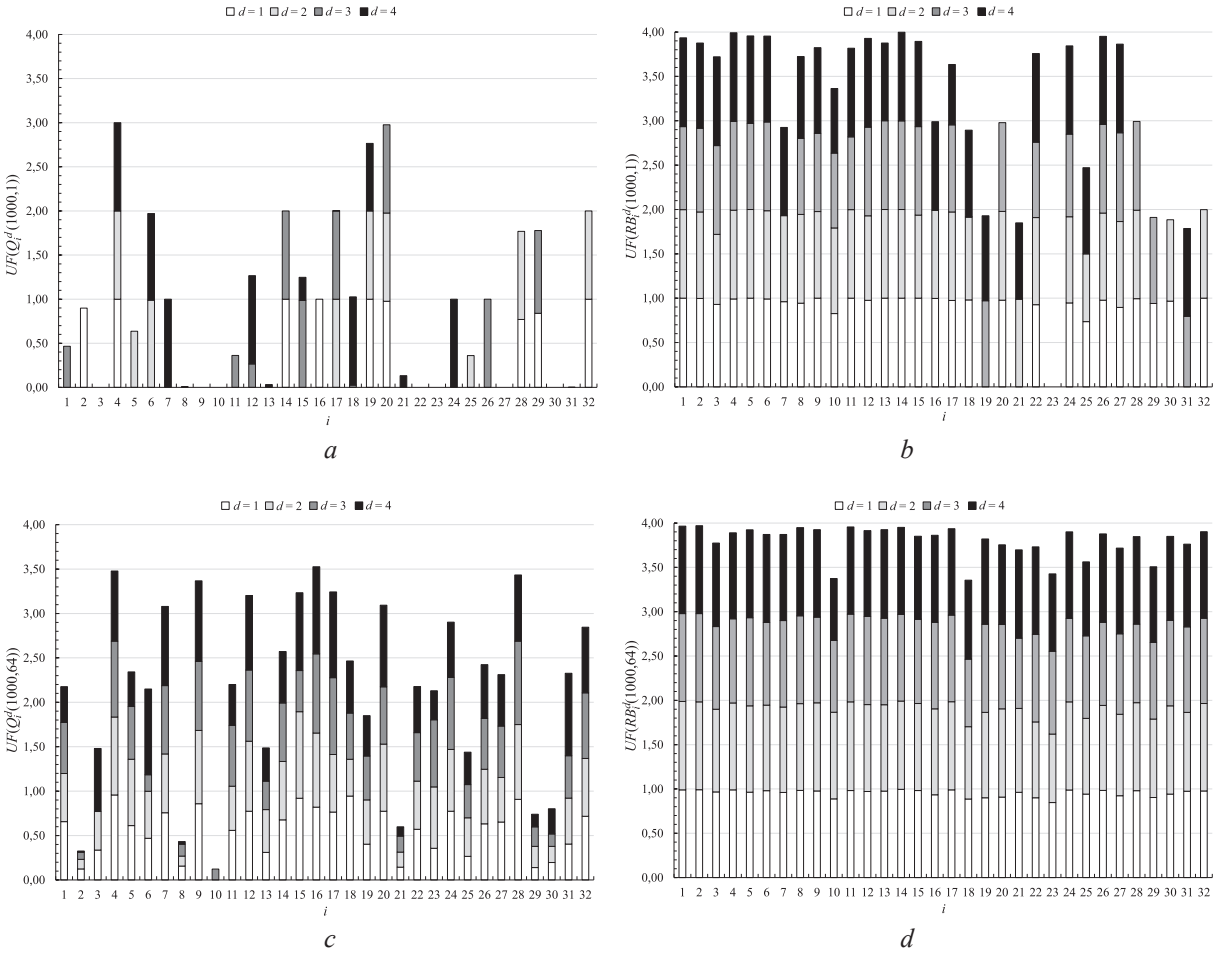


Рис. 7. Гистограммы с накоплением значений метрики единообразия для векторов:
$a - Q_i^d(1000,1)$; $b - RB_i^d(1000,1)$; $c - Q_i^d(1000,64)$; $d - RB_i^d(1000,64)$

Fig. 7. Stacked histograms of uniformity metric values for vectors:
$a - Q_i^d(1000,1)$; $b - RB_i^d(1000,1)$; $c - Q_i^d(1000,64)$; $d - RB_i^d(1000,64)$

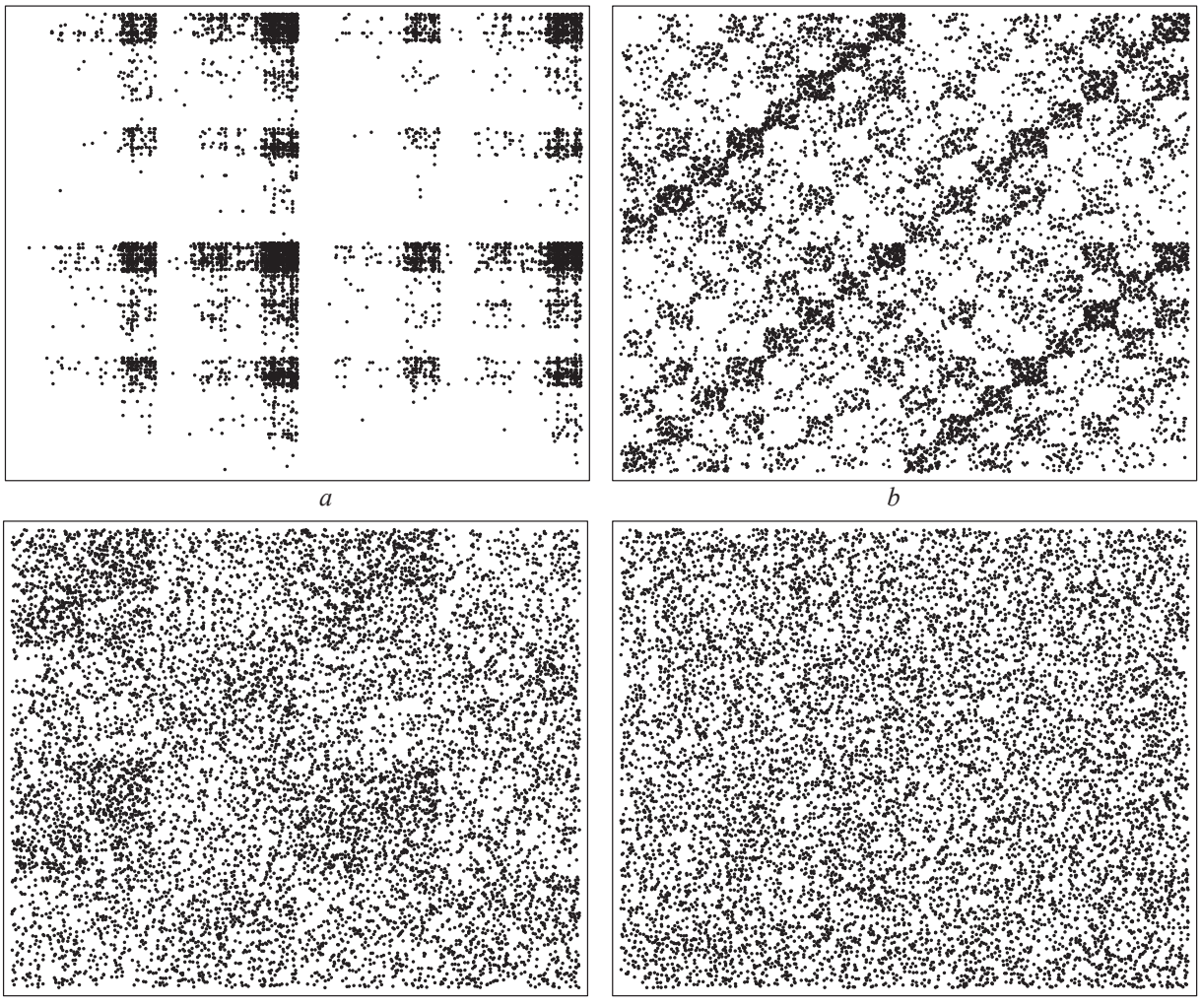
Проведенные эксперименты для различных значений k свидетельствуют о целесообразности использования выходов *RB* генераторов в качестве источников цифрового шума. Установлено, что при $k \geq 16$ все генераторы, реализованные на четырех FPGA, дают значение $UF(RB_i^d(E,k)) \neq 0$, тем самым способны успешно пройти тест на последовательность одинаковых бит.

В табл. 2 приведены данные о числе нулевых метрик $UF(Q_i^d(E,k))$ и $UF(RB_i^d(E,k))$ для различных значений k. Следует отметить, что дальнейшее увеличение k не способствует регистрации ненулевой метрики $UF(Q_i^d(E,k))$ на выходах четырех генераторов Q_3^3, Q_{10}^1, Q_{10}^2 и Q_{10}^4.

Таблица 2. Число нулевых значений метрик единообразия для различных k
Table 2. Number of zero values of uniformity metrics for different k

d	$UF(Q_i^d(E,k))=0$ / $UF(RB_i^d(E,k))=0$						
	k						
	1	2	4	8	16	32	64
1	23/4	14/2	6/0	8/1	1/0	1/0	1/0
2	23/4	14/3	8/0	4/0	2/0	1/0	1/0
3	20/7	20/6	12/2	4/0	3/0	1/0	1/0
4	21/6	16/5	15/4	4/1	4/0	1/0	1/0

Оценим поведение генераторов в старт-стопном режиме последовательной выработки 32-разрядных случайных чисел с выходов *Q* и *RB*, давая всем схемам работать во временном окне *MW* в режиме 2 с последующим переключением в режим 4. Для быстрой и визуальной оценки качества вырабатываемых последовательностей использовали графический тест «Распределение на плоскости» для 10^4 последовательно полученных чисел. На рис. 8 изображены результаты графических тестов для FPGA с индексом $d = 1$ для $k = 64$.



a *b* *c* *d*

Рис. 8. Результаты графических тестов в различных режимах для значений: *a*, *b* – с выходов *Q* и *RB*; *c*, *d* – с выходов *RB* в режимах счетчика Джонсона и генератора М-последовательности соответственно
Fig. 8. Results of graphics tests in various modes for values: *a*, *b* – from outputs *Q* and *RB*; *c*, *d* – from *RB* outputs in the Johnson counter mode and in M-sequence generator mode respectively

Как показали эксперименты, выход *RB* предложенной схемы генератора является предпочтительным в сравнении с выходом *Q* (рис. 8, *a*, *b*). Обусловлено это наличием *T*-триггера, выполняющего роль сумматора по модулю 2 значений, которые вырабатываются на выходе асинхронного триггера LDE в режиме остановки функционирования с наблюдаемым эффектом автоколебания. Для устранения неравномерности вырабатываемых значений можно сконфигурировать генераторы в схемы многоразрядных генераторов (рис. 4). Так, на рис. 8, *c* представлен результат тестирования генератора в режиме счетчика Джонсона, а на рис. 8, *d* – в режиме генератора М-последовательности, реализованного по порождающему полиному $\varphi(x) = 1 + x + x^5 + x^6 + x^{32}$, показавшему наилучший результат.

На рис. 9 представлены гистограммы распределения сгенерированных 32-разрядных случайных чисел четырьмя описанными выше модификациями генераторов. Объем выборки для всех генераторов составил $2 \cdot 10^5$, число интервалов для построения гистограмм выбрано равным 50.

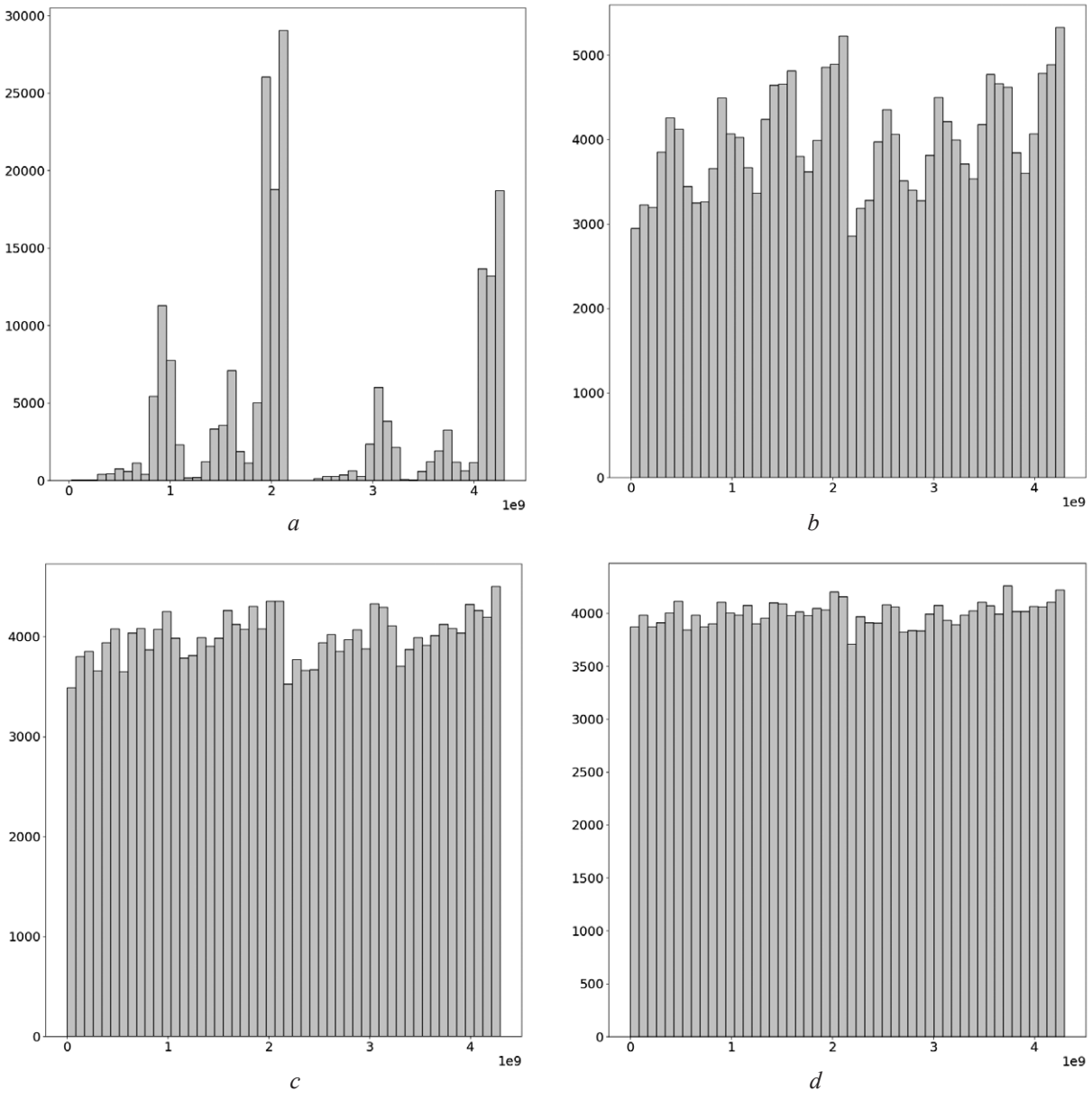


Рис. 9. Гистограммы распределения случайных чисел, полученных с выходов: *a*, *b* – *Q* и *RB*; *c*, *d* – *RB* в режимах счетчика Джонсона и генератора М-последовательности
Fig. 9. Histograms of distribution of random numbers obtained: *a*, *b* – from outputs *Q* and *RB*; *c*, *d* – from *RB* outputs in the Johnson counter mode and in M-sequence generator mode

Заключение

1. Предложена схема комбинированного генератора случайных чисел, основанная на двух типах физически неклонируемых функций – статической памяти и кольцевого осциллятора. В режиме физически неклонируемых функций статической памяти генератор способен вырабатывать уникальные неклонируемые идентификаторы, которые могут быть использованы как в схемах аутентификации, так и для защиты авторских прав на разрабатываемые цифровые устройства. В старт-стопном режиме кольцевого осциллятора генератор вырабатывает случайные значения, которые фиксируются схемой асинхронного триггера и могут храниться для последующего использования, например, для построения не только регистровых схем, но и схем генераторов псевдослучайных последовательностей. При завершении осцилляции на выходе асинхронного триггера фиксируются случайные автоколебания, которые детектируются и обрабатываются дополнительным синхронным *T*-триггером, входящим в состав схемы генератора. Эксперименты,

проведенные на кристаллах FPGA, показали, что случайные значения, вырабатываемые на выходе *T*-триггера, обладают лучшим показателем соотношения нулевых и единичных символов в генерируемых последовательностях по сравнению со схемой кольцевого осциллятора.

2. Базовая схема предложенного генератора может быть использована для построения схем постобработки случайных данных. Построенная таким образом схема генератора М-последовательности способна вырабатывать равномерные случайные данные с успешным прохождением базовых тестов Repetition Count Test и Adaptive Proportion Test.

References

1. Costiuc M., Maimut D., Teseleanu G. (2019) Physical Cryptography. *IACR Cryptology ePrint Archive.* Available: https://eprint.iacr.org/2019/1235.pdf (Accessed 19 September 2021).
2. Yarmolik V. N., Vashinko Ju. G. (2011) Physically Unclonable Functions. *Informatika*. 30 (2), 92–103 (in Russian).
3. Barker E., Kelsey J. (2015) Recommendation for Random Number Generation Using Deterministic Random Bit Generators. *NIST Special Publication 800-90A*. Available: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1 (Accessed 19 September 2022).
4. Turan M. S., Barker E., Kelsey J., McKay K. A., Baish M. L., Boyle M. (2018) Recommendation for the Entropy Sources Used for Random Bit Generation. NIST *Special Publication 800-90B*. Available: https://doi.org/10.6028/NIST.SP.800-90B (Accessed 19 September 2022).
5. Buchovecka S., Lorencz R., Kodytek F., Buček J. (2017) True Random Number Generator Based on Ring Oscillator PUF Circuit. *Microprocessors and Microsystems*. 53, 33–41.
6. Athanas P., Pnevmatikatos D., Sklavos N. (eds.) (2013) A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions. *Embedded Systems Design with FPGAs*. New York, Springer. 245–267.
7. Kacprzak T. (1988) Analysis of Oscillatory Metastable Operation of an RS Flip-Flop. *IEEE Journal of Solid-State Circuits*. 23 (1), 260–266.
8. Zalivaka S. S., Ivaniuk A. A., Chang Ch. H. (2018) Reliable and Modeling Attack Resistant Authentication of Arbiter PUF in FPGA Implementation with Trinary Quadruple Response. *IEEE Transactions on Information Forensics and Security*. 14 (4), 1109–1123.

Сведения об авторе

Иванюк А. А., д. т. н., доцент, профессор кафедры информатики, заведующий совместной учебной лабораторией «СК хайникс мемори солюшнс Восточная Европа» Белорусского государственного университета информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: + 375 17 293-80-66
E-mail: ivaniuk@bsuir.by
Иванюк Александр Александрович

Information about the author

Ivaniuk A. A., Dr. of Sci. (Eng.), Associate Professor, Professor at the Comp. Sci. Department, Head of the Joint Educational Laboratory “SK Hynix memory solutions Eastern Europe” of the Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 17 293-80-66
E-mail: ivaniuk@bsuir.by
Ivaniuk Alexander Alexandrovich