

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ УСТРОЙСТВ ИОТ-ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ ПОЛУПРОВОДНИКОВЫХ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

DOI: 10.36724/2072-8735-2026-20-9-27-35

Manuscript received 28 May 2026;

Accepted 07 August 2026

Мосин Сергей Геннадьевич,*Казанский (Приволжский) федеральный университет,
Казань, Россия;**ООО "ЛабСистемс", г. Владимир, Россия;**Рязанский государственный радиотехнический университет
им. В.Ф. Уткина, Рязань, Россия, smosin@ieee.org*

Ключевые слова: Интернет вещей (IoT), беспроводные IoT-устройства, безопасность, физически неклонируемая функция (PUF), схемотехническое моделирование, XOR-вентиль, реконфигурируемый кольцевой генератор

В работе рассмотрена проблема обеспечения безопасности беспроводной инфраструктуры Интернета вещей (IoT – Internet of Things) в контексте Индустрии 4.0. Критическим вызовом является ограниченность ресурсов беспроводных IoT-устройств (автономное энергопотребление, вычислительная мощность, объем памяти), что не позволяет применять сложные криптографические алгоритмы в реальном времени. Для решения этой задачи предложено использование полупроводниковых физически неклонируемых функций (PUF – Physically Unclonable Functions), генерирующих уникальные псевдослучайные последовательности на основе случайных вариаций технологического процесса производства интегральных схем. Представлена системная модель IoT-инфраструктуры в терминах теории множеств, позволяющая выполнять структурный и параметрический синтез в ходе проектирования. Основным научным вкладом является разработка схемотехнической модели XOR-вентилей, оптимизированной для синтеза PUF на основе реконфигурируемых кольцевых генераторов. Модель адаптирована под КМОП-технологии TSMC 180 нм и позволяет на ранних этапах проектирования беспроводных IoT-устройств по заказной технологии выбирать рациональные конфигурации PUF с учетом фактических ограничений. Проведено численное моделирование методом Монте-Карло с учетом коррелированных и некоррелированных технологических вариаций. Реализованы две тестовые обвязки для накопления битовых последовательностей. Полученные результаты верифицированы и продемонстрировали соответствие теоретическим ожиданиям, подтверждая эффективность предложенного подхода для синтеза псевдослучайных битовых последовательностей для целей идентификации и аутентификации беспроводных IoT-устройств. Дальнейшие исследования направлены на оценку надежности и устойчивости к атакам с использованием машинного обучения.

Информация об авторах:

Мосин Сергей Геннадьевич, доктор технических наук, профессор кафедры прикладной математики и искусственного интеллекта, Казанский (Приволжский) федеральный университет, г. Казань, Россия; заместитель генерального директора ООО "ЛабСистемс", г. Владимир, Россия; профессор кафедры САПР ВС, Рязанский государственный радиотехнический университет им. В.Ф. Уткина, г. Рязань, Россия. ORCID 0000-0003-1389-2602

Для цитирования:

Мосин С. Г. Обеспечение безопасности беспроводных устройств IoT-инфраструктуры с помощью полупроводниковых физически неклонируемых функций // T-Comm: Телекоммуникации и транспорт. 2026. Том 20. №9. С. 27-35.

For citation:

S. G. Mosin, "The security ensuring of IoT-infrastructure's wireless devices using semiconductor physically unclonable functions", T-Comm, 2026, vol. 20, no.9, pp. 27-35. (in Russian)

Введение

Переход к четвертой промышленной революции (Индустрия 4.0) обусловлен разработкой и активным внедрением киберфизических систем (КФС, *CPS – Cyber-Physical System*) в различные секторы экономики с целью организации умного производства, под которым понимают взаимодействие между умной фабрикой и умной продукцией. Используемые в работе определения основаны на принятых в российских и международных стандартах понятиях (табл. 1). Умное производство можно охарактеризовать использованием автоматизированных систем управления, взаимодействующих между собой без непосредственного участия человека с применением технологий искусственного интеллекта. А Индустрию 4.0 – как концептуальную модель создания единого цифрового пространства, где физические объекты и нематериальные активы представлены виртуально и могут взаимодействовать друг с другом на протяжении своего жизненного цикла.

Таблица 1

Перечень стандартов, определяющих понятия предметной области

ГОСТ Р 71531-2024 «Системы киберфизические. Термины и определения».
ГОСТ Р 71576-2024 «Системы киберфизические. Общие положения».
ГОСТ Р 59799-2021 «Умное производство. Модель эталонной архитектуры индустрии 4.0 (<i>RAMI 4.0</i>)».
ГОСТ Р 71842-2024 «Цифровая промышленность. Умное производство. Часть 1. Термины и определения»
ISO/IEC 20924-2021 <i>Information technology – Internet of Things (IoT) – Vocabulary</i> .

Каркасом Индустрии 4.0 выступает стек ключевых технологий, который включает: искусственный интеллект (*AI – Artificial Intelligence*) и машинное обучение (*ML – Machine Learning*), большие данные и предиктивную аналитику (*Big Data*), цифровые двойники (*Digital Twins*), интернет вещей (*IoT – Internet of Things*), распределенные и высокопроизводительные вычисления (*HPC – High-Performance Computing*), роботизированные и мехатронные агенты, дополненная и виртуальная реальность (*AR/VR – Augmented/Virtual Reality*) и др.

Технология *IoT* в представленном стеке определяет инфраструктуру взаимосвязанных сущностей, систем и информационных ресурсов, а также служб, позволяющих обрабатывать информацию о физическом и виртуальном мире и реагировать на нее. Такая инфраструктура представлена сетью датчиков, сенсоров, контрольно-измерительных узлов и устройств (КИУУ), собирающих данные о состоянии объектов и параметрах процессов, преобразующих их к удобному формату и передающих в единую систему обработки, которые обладают интерфейсом подключения к проводным сетям или беспроводным каналам связи. Причем беспроводные *IoT*-устройства получают все большее распространение в силу повышения гибкости систем, их мобильности и масштабируемости, а также простоты установки и обслуживания.

Обеспечение кибербезопасности *IoT*-инфраструктуры КФС требует комплексной защиты каналов связи, конечных устройств и обрабатываемых данных. Переход на беспроводные интерфейсы расширяет поверхность атак за счет уязвимостей физического уровня (перехват, глушение, подмена пакетов), что критически повышает риски компрометации по

сравнению с проводными технологиями. Применение недоверенной электронной компонентной базы и несанкционированное подключение сторонних устройств выступают источниками злонамеренных ошибок в виде сторонних атак, провоцирования отказов и сбоев в обслуживании, нелегального доступа к данным, нарушения их целостности и достоверности, что негативно сказывается на безопасности и защищенности *IoT*-инфраструктуры КФС.

Объектом предлагаемого исследования выступает безопасность беспроводных *IoT*-устройств. Проблема – ограниченные ресурсы и возможности беспроводных *IoT*-устройств (слабые процессоры/микроконтроллеры, мало памяти, узкий канал связи, лимит энергопотребления и др.) для использования сложных защитных механизмов в реальном времени. Предмет исследования – подходы к внутрисхемной реализации уникальных защитных механизмов с учетом фактических ограничений беспроводных *IoT*-устройств.

Цель предложенной работы – реализация и исследование генераторов уникальных псевдослучайных битовых последовательностей на основе полупроводниковых физически неклонированных функций для обеспечения идентификации и аутентификации беспроводных *IoT*-устройств.

Основные результаты:

1. Предложена системная модель *IoT*-инфраструктуры в терминах теории множеств.
2. Определена совокупность требований к беспроводным *IoT*-устройствам и обозначено перспективное направление формирования уникальных псевдослучайных последовательностей на основе полупроводниковых физически неклонированных функций (*PUF – Physically Unclonable Functions*).
3. Предложена схмотехническая модель *XOR*-вентиля, которая позволяет синтезировать, моделировать и выбирать рациональные конфигурации *PUF* для реализации в специализированных интегральных схемах (*ASIC*).
4. Проведено численное моделирование реконфигурируемых кольцевых генераторов (*RO*), выступающих в качестве полупроводниковой *PUF*, и исследование характеристик сформированных ими псевдослучайных битовых последовательностей. Полученные результаты продемонстрировали соответствие теоретическим ожиданиям и результатам других авторов, но для базиса программируемых логических интегральных схем (ПЛИС).

1 Архитектура и особенности *IoT*-инфраструктуры

В общем случае *IoT*-инфраструктуру можно рассматривать как систему гетерогенных систем, которые различаются видом взаимодействия с окружающими системами, степенью связности, топологией и технологией связи, назначением, техническими и функциональными ограничениями и др. (рис. 1). Математически архитектуру *IoT*-инфраструктуры представим кортежем множеств физических *IoT*-устройств – **E**, сетей связи – **N**, форматов накапливаемых данных – **D**, вычислительных ресурсов – **C**, приложений – **App**, технологий обеспечения комплексной безопасности – **S** и технических / функциональных требований и ограничений – **R**.

$$\text{Arch}_{\text{IoT}} = [\mathbf{E}, \mathbf{N}, \mathbf{D}, \mathbf{C}, \text{App}, \mathbf{S}, \mathbf{R}]. \quad (1)$$

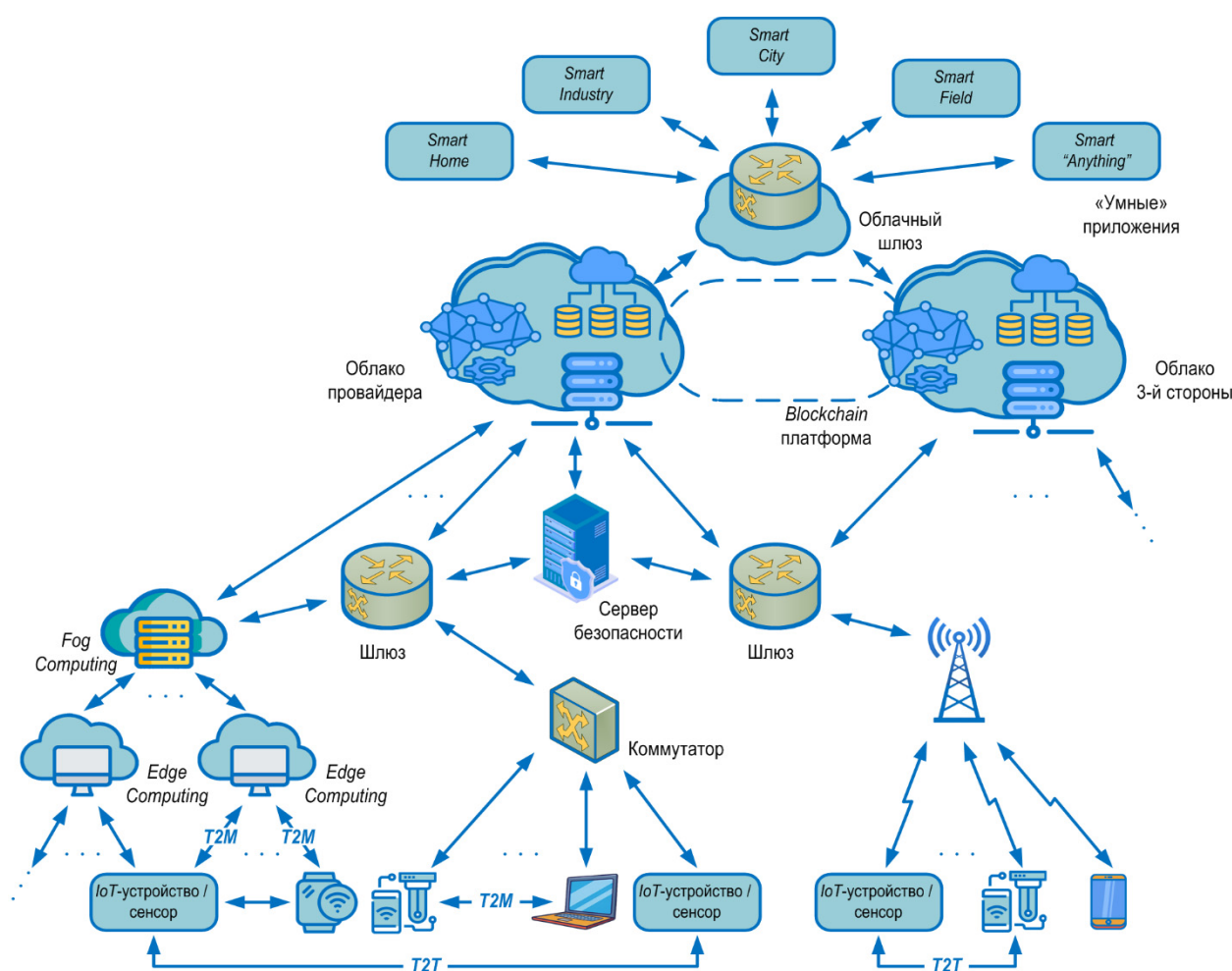


Рис. 1. Архитектура IoT-инфраструктуры

Множество IoT-устройств (**E**) включает элементы сбора данных (датчики/сенсоры, КИУУ и т.п.) и актуаторы – элементы, выполняющие действия над объектами управления (регуляторы, переключатели, сервоприводы, клапаны и т. д.) и отвечающие за взаимодействие киберпространства IoT с физическим миром.

Множество сетей связи (**N**) включает стандарты и протоколы передачи информации с использованием проводных и беспроводных технологий, а также устройства, обеспечивающие сетевое взаимодействие – коммутаторы, шлюзы, точки доступа, базовые станции и др. Правила организации и функционирования сетей связи определяет стек протоколов от физического уровня до прикладного. Взаимодействие IoT-устройств с другими элементами инфраструктуры рассматривают как межмашинную коммуникацию (*M2M* – *Machine-to-Machine*) в рамках которой в зависимости от цели и уровня интеграции выделяют две модели:

- *Things-to-Machine (T2M)*, которая описывает сценарий взаимодействия оконечных устройств сбора данных (*Things*) с интеллектуальной системой (*Machine*) в виде контроллера, компьютера/сервера или облачного сервиса (ЦОД – центр обработки данных) для постоянной или периодической передачи накопленной информации. Как правило, этот сценарий предусматривает односторонний обмен данными.

- *Things-to-Things (T2T)*, которая описывает сценарий взаимодействия IoT-устройств между собой без прямого участия человека для совместного решения задач или создания сложной, динамической и, зачастую, самоорганизующейся сети – двухсторонний обмен.

Множество форматов данных (**D**) включает правила представления накапливаемой и передаваемой информации, которые непосредственно связаны с используемыми протоколами передачи (табл. 2).

Множество вычислительных ресурсов (**C**) включает централизованные или распределенные информационно-вычислительные средства обработки данных, поступающих от оконечных устройств. Простейшие вычисления могут выполняться на микроконтроллере IoT-устройства (при наличии). Интеллектуальный анализ данных выполняют на специальных вычислительных ресурсах согласно выбранной вычислительной модели:

- Граничные вычисления (*Edge Computing*) – модель распределенных вычислений, в которой обработка информации происходит в непосредственной близости к месту, где данные были получены и будут использованы в дальнейшем (на «границе» сети) [1, 2].

- Облачные вычисления (*Cloud Computing*) – модель централизованных вычислений в ЦОД и дата-центрах на удаленных

серверах и/или высокопроизводительных вычислительных системах, которые предоставляет провайдер облачных сервисов [3]. Возможно использование коммерческих облачных сервисов по подписке или сервисов с открытым доступом, которые могут быть предоставлены не только ключевым провайдером, но и сторонним поставщиком. Интеграция облачных вычислений и технологии *Blockchain* позволяет организовать распределенную доверенную вычислительную сеть, узлами которой выступают «облака». Использование распределенного реестра устраняет единую точку отказа, повышает прозрачность операций и защищает данные от фальсификации [4].

- Туманные вычисления (*Fog Computing*) – модель децентрализованных вычислений, в которой вычислительные ресурсы, хранилища данных и сетевые сервисы размещены ближе к конечным устройствам и источникам данных, формируя промежуточный слой между ними и облаком для балансировки вычислительной нагрузки и пропускной способности сети [5].

Таблица 2

Форматы данных и протоколы передачи в IoT-инфраструктуре

Название	Источник
Форматы данных	
<i>Текстовые форматы для хранения и обмена структурированными данными</i>	
<i>XML (eXtensible Markup Language)</i>	<i>RFC 3023: XML Media Types. January 2001. 39 p. https://datatracker.ietf.org/doc/html/rfc3023</i>
<i>JSON (JavaScript Object Notation)</i>	<i>ISO/IEC 21778:2017 Information technology – The JSON data interchange syntax</i>
<i>CSV (Comma-Separated Values)</i>	<i>RFC 4180: Common Format and MIME Type for Comma-Separated Values (CSV) Files. October 2005. 6 p. https://datatracker.ietf.org/doc/html/rfc4180</i>
<i>Двоичные форматы для хранения и обмена структурированными данными</i>	
<i>Protobuf (Protocol Buffers)</i>	<i>Protocol Buffers v35.1 https://github.com/protocolbuffers/protobuf/releases/tag/v35.1</i>
<i>Apache Avro</i>	<i>Avro 1.12.1 https://avro.apache.org/blog/releases/</i>
<i>Apache Parquet</i>	<i>Parquet 2.13.0 https://parquet.apache.org/blog/</i>
Протоколы передачи	
<i>CoAP (Constrained Application Protocol)</i>	<i>RFC 7252: The Constrained Application Protocol (CoAP). June 2014, IETF Trust and the Document Authors. 112 p. http://www.rfc.fr/rfc/en/rfc7252.pdf</i>
<i>MQTT (Message Queuing Telemetry Transport)</i>	<i>ISO/IEC 20922:2016 Information technology – Message Queuing Telemetry Transport (MQTT) v3.1.1. ГОСТ Р 58603–2019 Информационные технологии. Интернет вещей. Протокол организации очередей доставки телеметрических сообщений MQTT. Вер. 3.1.1.</i>
<i>Data Distribution Service</i>	<i>Object Management Group. Data distribution service for real-time systems, 2004.</i>
<i>AMQP (Advanced Message Queuing Protocol)</i>	<i>ISO/IEC 19464:2014 Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification</i>
<i>XMPP (Extensible Messaging and Presence Protocol)</i>	<i>RFC 3920 & 3921: Extensible Messaging and Presence Protocol (XMPP): Core. October 2004. 91 p. http://www.rfc.fr/rfc/en/rfc3920.pdf</i>

Множество приложений (**App**) включает программные решения под различное аппаратное обеспечение (смартфоны, сенсорные панели, настольные/переносные компьютеры и серверы, и др.), представленные в плоскости пользователя и плоскости разработчика. В первом случае это мобильные приложения, web-страницы, программы визуализации и обработки запросов, доступные в использовании даже для неквалифицированных пользователей. Во втором случае это библиотеки программных компонентов, программные интерфейсы приложений (*API – Application Programming Interface*), БД и СУБД, т.е. специализированные средства, предназначенные для разработчиков программного обеспечения. Можно выделить иерархию приложений от уровня отдельных пользователей до бизнес-уровня и уровня отраслей промышленности с учетом масштаба востребованности и универсальности.

Множество технологий обеспечения комплексной безопасности (**S**) включает методы и инструменты, обеспечивающие защиту всех элементов IoT-инфраструктуры, предотвращение уязвимостей и несанкционированный доступ при их использовании в разных сценариях взаимодействия [6]. На уровне обеспечения безопасности IoT-устройств важными средствами выступают: идентификация – распознавание устройства и его свойств по уникальному признаку [7, 8], аутентификация – проверка подлинности пользователя, устройства или системы [9-11] и авторизация – предоставление прав на осуществление определенных действий и доступа к ресурсам. Аутентификация использует открытые / закрытые ключи и специализированные протоколы [12, 13]. В основе аутентификации как процесса установления, что устройство (пользователь) действительно является тем, за кого себя выдает, лежат различные решения:

- Факторная аутентификация (*FA – Factor Authentication*) – метод подтверждения подлинности устройства (пользователя), при котором требуется использование нескольких независимых факторов из разных категорий. Распространена двухфакторная аутентификация (*2FA*) – частный случай многофакторной аутентификации (*MFA*), использующий только два фактора.

- Взаимная аутентификация (*MA – Mutual authentication*) – метод, при котором подлинность подтверждают обе стороны соединения до начала обмена данными.

- Аутентификации через отдельный канал (*OOBA – Out-of-Band Authentication*) – метод подтверждения подлинности с использованием отдельного независимого канала связи, отличного от основного канала передачи данных.

Множество технических / функциональных требований и ограничений (**R**) включает разрешенные или допустимые диапазоны для параметров системы и используемых ресурсов, обязательные и опциональные возможности, нормативную базу и т.п. Например технические требования задают энергоэффективность, пропускную способность, совместимость, устойчивость, возможности вертикального и горизонтального масштабирования; функциональные требования определяют сценарии сбора и передачи данных, логику их обработки и формирования управляющих воздействий для актуаторов, аспекты визуализации и интерфейса пользователя для приложений; нормативная база регламентирует обработку персональных данных, взаимодействие с критическими инфраструктурами (здравоохранение, правоохранительные

службы, энергетика и др.), разрешения на использование определенных технологий и сервисов, договорные отношения между провайдером и пользователем.

В ходе проектирования *IoT*-инфраструктуры осуществляют структурный и параметрический синтез, а также анализ и оптимизацию получаемых решений, которые на ранних стадиях основаны на совокупности теоретико-множественных операций над элементами кортежа Arch_{IoT} (1), что позволяет определять состав необходимых компонентов, распределять нагрузку и осуществлять балансировку между шлюзами и ресурсами граничных, туманных и облачных вычислений, моделировать связи и отношения один-ко-многим / многие-ко-многим, масштабировать и управлять подсистемами и др.

2 Безопасность *IoT*-устройств с использованием полупроводниковых *PUF*

К беспроводным *IoT*-устройствам в отличие от проводных предъявляют особые требования к энергопотреблению и длительности автономной работы, производительности встроенных вычислительных ресурсов, к дальности и скорости передачи данных, а также к безопасности, что связано с уязвимостями и атаками – возможностью перехвата радиосигнала, подмены данных и несанкционированной интеграцией стороннего устройства в систему.

Оценка энергопотребления в течение цикла эксплуатации *IoT*-устройства может быть выполнена на ранних стадиях проектирования *IoT*-инфраструктуры с учетом особенностей используемой технологии беспроводной связи [14-16]. Минимальная производительность встроенных вычислителей также выступает ограничением на использование надежных, но вычислительно сложных технологий шифрования данных и аутентификации. Поэтому для обеспечения безопасности беспроводных *IoT*-устройств рассматривают варианты с учетом обозначенных ограничений. Одно из перспективных направлений формирования уникальных псевдослучайных

последовательностей и цифровых ключей с их использованием – внутрисхемная реализация полупроводниковых физически неклонируемых функций (*PUF* – *Physically Unclonable Functions*), в основе которых лежат случайные вариации технологического процесса производства интегральных схем [17, 18]. В общем случае *PUF* определена множеством пар запрос-ответ (*CPR* – *Challenge-Response Pair*), которые непредсказуемы и не поддаются клонированию. Применение реконфигурируемых схем *PUF* позволяет на ограниченном множестве электронных компонентов, занимающих минимально необходимую площадь кристалла ИС, формировать семейство потенциально полезных *CPR*, где запросы (*C*) активируют конкретную конфигурацию, которой соответствует уникальный ответ (*R*).

Вентиль «Исключающее-ИЛИ» (*XOR*) – эффективный базис реализации реконфигурируемых *PUF* с точки зрения функциональных возможностей и минимизации занимаемой площади на кристалле (рис. 2). Если входы *XOR*-вентиля рассматривать как управляющий (*Cx*) и информационный (*Ix*), то в силу функциональных особенностей в зависимости от значения управляющего входа вентиль можно рассматривать как инвертор (*Cx* = 1) или как буфер (*Cx* = 0). Это обстоятельство позволяет формировать структуры, реконфигурируемые с помощью значений управляющих входов, совокупность которых определяет уникальный запрос *PUF* (*C*).

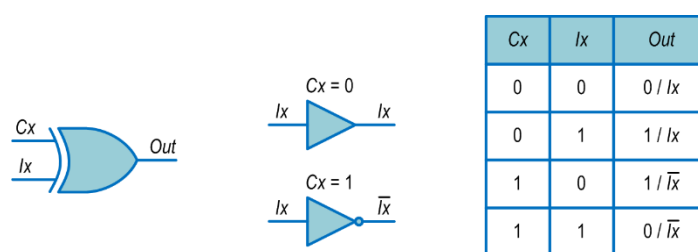


Рис. 2. *XOR*-вентиль и варианты реконфигурирования

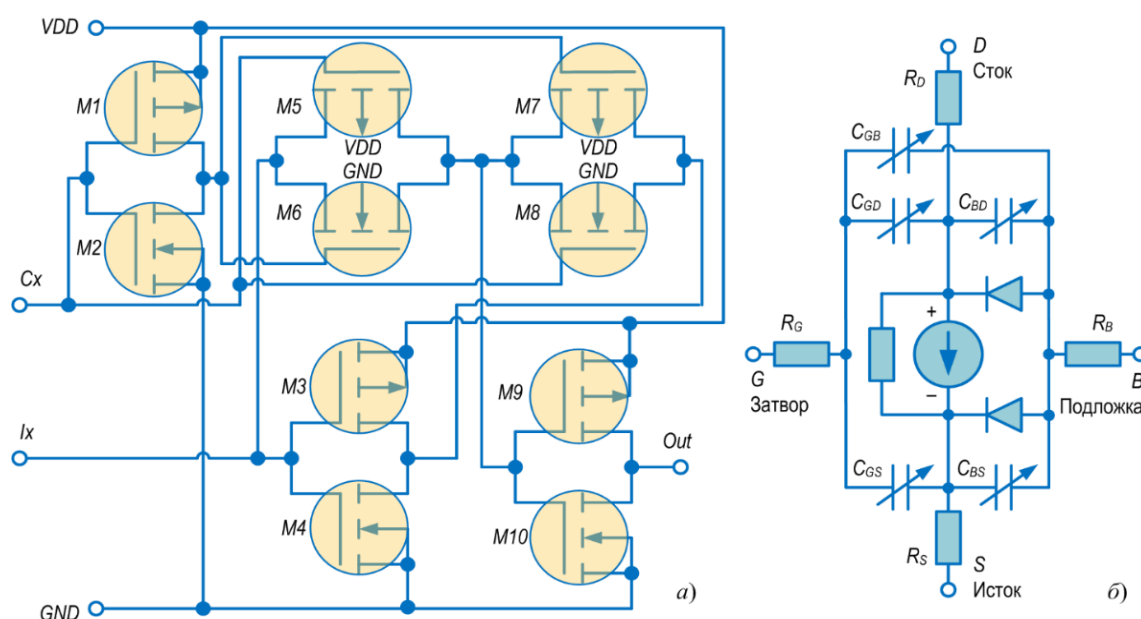


Рис. 3. Схема электрическая: *XOR*-вентиль (а), модель транзистора (б)

В работе предложена схемотехническая модель *XOR*-вентилей, которая учитывает особенности используемой интегральной технологии при производстве ИС беспроводных *IoT*-устройств и позволяет уже на ранних стадиях проектирования (до создания топологии) синтезировать, моделировать и выбирать рациональные конфигурации *PUF*, обеспечивающие формирование полезных *CRP*. Модель *XOR*-вентилей представлена списком соединений в формате *PSpice*, соответствующим схемной реализации в базе КМОП-транзисторов (рис. 3). Модель позволяет задавать параметры вариаций технологического процесса, необходимые для последующих статистических испытаний методом Монте-Карло, в ходе которых оцениваются динамические характеристики как самого вентилей, так и реконфигурируемых схем *PUF* на его основе.

В качестве таких схем рассмотрены реконфигурируемые кольцевые генераторы (*RO* – *Ring Oscillator*) с изменяемым количеством каскадов (рис. 4) [19-21]. Обязательное требование к *RO* – конфигурирование нечетного числа инверторов в схеме. Для *n*-стадийного каскада возможно формирование 2^{n-1} уникальных схем кольцевых генераторов.

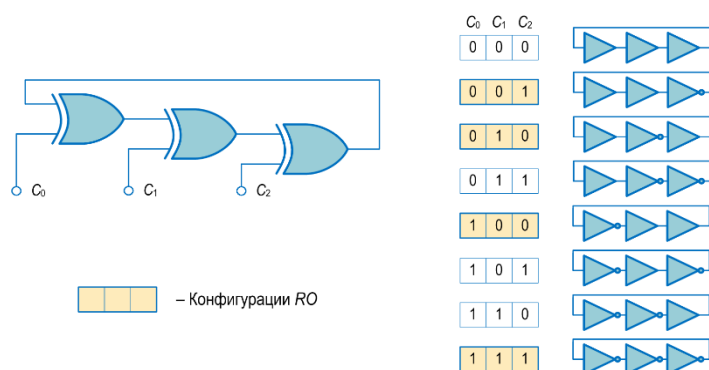


Рис. 4. Структура кольцевого генератора на трех *XOR*-вентилей и варианты реконфигурирования

3 Экспериментальные исследования

Для подтверждения достижения цели работы – реализации и исследования генераторов уникальных псевдослучайных битовых последовательностей на основе полупроводниковых физически неклонированных функций (*PUF*), предназначенных для идентификации и аутентификации беспроводных *IoT*-устройств, – проведена серия численных экспериментов. В ходе исследований выполнена верификация схемотехнической модели *XOR*-вентилей. Реконфигурируемые кольцевые генераторы (*RO*), выступающие в качестве полупроводниковой *PUF*, реализованы на четырех *XOR*-вентилей. Моделирование *RO* выполнено методом Монте-Карло во временной области с использованием *EDA*-среды *PSpice A/D (CADENCE)* при 3 000 итерациях. Параметры модели *XOR*-вентилей настроены под КМОП-технологии *TSMC* 180 нм; случайные вариации технологического процесса заданы независимым разбросом параметров (3% по нормальному закону от номиналов) и коррелированным разбросом в партии (5% по равномерному закону). Расчеты проводились на вычислительной системе с процессором *Intel Core i5-7000* (3.4 ГГц, x64) и 32 Гб ОЗУ.

Для накопления псевдослучайных последовательностей предложены и реализованы две тестовые обвязки – счетчик импульсов на выходе *RO* (разрядность 10 бит) и сдвиговый

регистр с варьiruемой длиной от 8 до 16 разрядов для накопления отсчетов выходного сигнала *RO* с прореживанием внутри временного окна. В процессе верификации подтверждены статические и динамические характеристики *XOR*-вентилей.

По итогам статистических испытаний построены гистограммы числовых значений, накопленных в счетчике и сдвиговом регистре, которые отражают широкий диапазон изменения частоты *RO* при вариации технологических параметров, что свидетельствует о чувствительности предложенной структуры к технологическим флуктуациям (рис. 5).

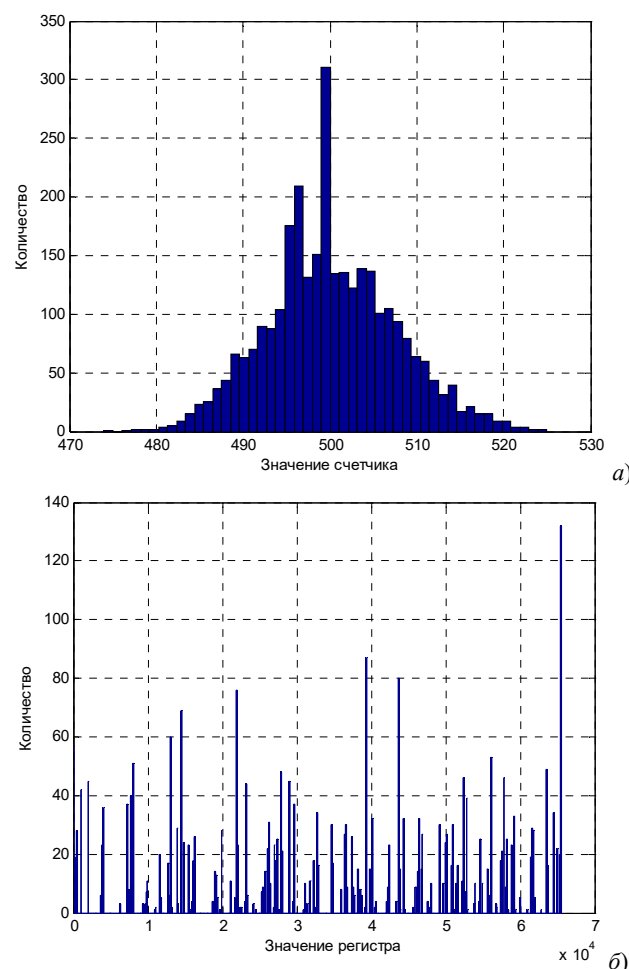


Рис. 5. Гистограмма накопленных значений при длине временного окна 150 нс: в счетчике (а), в сдвиговом 16-разрядном регистре (б)

На основе полученных выборок рассчитаны ключевые характеристики *PUF* – уникальность (U_q – *Uniqueness*), однородность (U_f – *Uniformity*) и общая минимальная энтропия (E) – для обеих обвязок при длинах сдвигового регистра 8, 10, 12, 14 и 16 разрядов (табл. 3). Результаты для сдвигового регистра демонстрируют соответствие ожидаемым теоретическим значениям: U_q и U_f стремятся к 0.5, а E – к 1, что подтверждает статистическую независимость и равномерность выходных последовательностей. Эти данные коррелируют с результатами других авторов для *PUF* на основе программируемых логических интегральных схем (ПЛИС), что дополнительно валидирует сходимость предложенной модели и реконфигурируемых схем на ее основе (табл. 4).

Таблица 3

Полученные характеристики PUF

Характеристика	Счетчик	Устройство				
		Сдвиговый регистр (разрядность, бит)				
		8-	10-	12-	14-	16-
Уникальность	0.3105	0.4962	0.4963	0.4965	0.4967	0.4968
Однородность	0.6413	0.5442	0.5437	0.5424	0.5409	0.5403
Общая минимальная энтропия	0.5037	0.8780	0.8793	0.8827	0.8866	0.8884

Таблица 4

Сравнение результатов с референсными работами

Источник	Уникальность	Однородность	Энтропия
[19]	0.4220	0.4674	–
[20]	–	–	0.9870
[21]	0.5018	0.4755	–
[22]	0.4805	0.5091	0.7825
[23]	0.4200	0.5697	–
[24]	0.4974	0.5466	–
[25]	0.4479	0.4974	–
Предложенное решение:			
сдвиговый регистр 16-бит	0.4968	0.5403	0.8884

Ключевые характеристики для счетчика уступают теоретическим ожиданиям в силу ограниченного диапазона накапливаемых значений (рис. 5, а). Прямое использование этих значений в качестве уникальных ответов PUF нецелесообразно по сравнению со значениями из сдвигового регистра. Близость ключевых характеристик ответов сдвигового регистра различной длины подтверждают возможность внутрисхемного синтеза уникальных битовых последовательностей требуемой длины с минимальными затратами площади кристалла.

4 Заключение

В работе предложена системная модель IoT-инфраструктуры, представленная кортежем конечных множеств, позволяющая выполнять структурный и параметрический синтез в ходе проектирования. Обозначены источники уязвимостей беспроводных IoT-устройств и совокупность функциональных и технологических ограничений, которые осложняют обеспечение безопасности. Определена совокупность требований к беспроводным IoT-устройствам и представлено перспективное направление формирования уникальных псевдослучайных последовательностей на основе полупроводниковых PUF. Предложена схемотехническая модель XOR-вентилей, которая позволяет уже на ранних стадиях проектирования IoT-устройств по заказной интегральной технологии осуществлять выбор рациональной конфигурации PUF, адаптируя параметры обвязки под требования конкретного приложения. Выполнено численное моделирование реконфигурируемых кольцевых генераторов, реализованных на основе XOR-вентилей и выступающих в качестве полупроводниковой PUF. Проведено исследование характеристик получен-

ных псевдослучайных битовых последовательностей. Экспериментальные результаты продемонстрировали соответствие теоретическим ожиданиям и результатам других авторов, что позволяет судить о достижении поставленной в данной работе цели.

Дальнейшее развитие исследований видится в расширении возможностей модели XOR-вентилей для оценки надежности (*reliability*) реконфигурируемых PUF, а также в реализации средств анализа устойчивости к атакам с использованием машинного обучения (*ML*-атаки).

Литература

1. Kumar A., Singh D. Reinforcement learning based security method for IoT-Edge computing // *Wireless Networks*, 2026, vol. 32, pp. 1547–1567, doi: 10.1007/s11276-026-04123-5.
2. Jinchuan W., Ming N., Qiaojin G., Zhiwei Y., Suhang L. Design of an Intelligent IoT Platform Based on the Synergy of Edge Computing and Cloud Computing // *Journal of Big Data and Computing*, 2026, vol. 4, no. 1, pp. 27–33, doi: 10.62517/jbdc.202601104.
3. Andriulo F.C., Fiore M., Mongiello M., Traversa E., Zizzo V. Edge Computing and Cloud Computing for Internet of Things: A Review // *Informatics*, 2024, vol. 11, no. 4: 71. 22 p., doi: 10.3390/informatics11040071.
4. Jhariya M.K., Dehalwar V., Bharti J. Blockchain-enabled secure, lightweight self-sovereign identification and authentication framework for access management of IoT devices // *Cluster Computing*, 2026, vol. 29, Paper ID 291, 25 p., doi: 10.1007/s10586-026-06005-z.
5. Apat H.K., Goswami V., Sahoo B. et al. An Adaptive Queueing Model for Optimizing IoT Application Performance in Fog-Cloud Computing Environment // *SN Computer Science*, 2026, vol. 7, Paper ID 486, 15 p., doi: 10.1007/s42979-026-04997-4.
6. Минаев В.А., Швырев Б.А., Ромашикин Т.Р. Безопасность интернета вещей: основные решения // *Информация и безопасность*. 2023. Т. 26. Вып. 2. С. 163–168. doi: 10.36622/VSTU.2023.26.2.001.
7. Dou Y. Current Status and Challenges of IoT Device Identity Authentication Technology // *Computers and Artificial Intelligence*, 2026, vol. 3, no. 2, pp. 65–77, doi: 10.70267/cai.26v3n2.6577.
8. Weibing Li, Shenggang Wu, Wei Han. Blockchain-based IoT device identity authentication and data traceability // *International Journal of Computer Information Systems and Industrial Management Applications*, 2025, vol. 17, p. 17, doi: 10.70917/ijcisim-2025-0316.
9. Бойко А. А., Быков М. Ю., Куцев С. С., Перегудов М. А. Аутентификация в сетях сотовой связи: обзор математических моделей // *Системы управления, связи и безопасности*. 2025. № 1. С. 187–219. doi: 10.24412/2410-9916-2025-1-187-219.
10. Миронов А. М. Новая математическая модель протоколов аутентификации и основанный на ней метод верификации // *Интеллектуальные системы. Теория и приложения*. 2018. Т. 22, № 4. С. 79–98.
11. Kang J.H., Seo M. Enhanced Authentication for Decentralized IoT Access Control Architecture // *Cryptography*, 2023, vol. 7, no. 3, Paper ID 42, 17 p., doi: 10.3390/cryptography7030042.
12. Chan Suet Yan S., Tang Su Wei A., Bong J. H., Teh Q. L., Sivalingam S., Khoo S. Y., Nafy T. M. Authentication of IoT device with the enhancement of One-time Password (OTP) // *Journal of IT in Asia*, 2021, vol. 9, no. 1, pp. 29–40, doi: 10.33736/jita.3841.2021.
13. Malik A., Kushwah R. A Secure Authentication and Key Establishment Protocol for IoT Devices Using ECCMD // *SN Computer Science*, 2025, vol. 6, Paper ID 803, 16 p., doi: 10.1007/s42979-025-04354-x.
14. Mosin S. A Model of LoRaWAN Communication in Class A for Design Automation of Wireless Sensor Networks Based on the IoT Paradigm // *2018 IEEE East-West Design & Test Symposium (EWDTS)*, Kazan, 2018, pp. 1–6. doi: 10.1109/EWDTS.2018.8524618.
15. Mosin S. A Model for Univariate and Multivariate Simulating the Battery Lifetime of UE NB-IoT // *2024 International Russian Automation*

Conference (RusAutoCon), Sochi, Russian Federation, 2024, pp. 13–18, Paper ID 10694326, doi: 10.1109/RusAutoCon61949.2024.

16. Мосин С.Г. Поиск оптимальной конфигурации радиоресурсов линии вверх для снижения энергопотребления UE NB-IoT при передаче данных // Динамика сложных систем. 2025. Т. 19. № 2. С. 40–49. doi: 10.18127/j19997493-202502-06.

17. Lata K., Cenkeramaddi L.R. FPGA-Based PUF Designs: A Comprehensive Review and Comparative Analysis // Cryptography, 2023, vol. 7, no. 4, Paper ID 55, 30 p., doi: 10.3390/cryptography7040055.

18. Karmakar M., Naz S.F., Shah A.P. Fault-Tolerant Reversible Logic Gate-Based RO-PUF Design // Memories - Materials, Devices, Circuits and Systems, 2023, vol. 4, Paper ID 100055, 6 p., doi: 10.1016/j.memori.2023.100055.

19. Tanamoto T., Yasuda S., Takaya S., Fujita S. Physically Unclonable Function Using an Initial Waveform of Ring Oscillators // IEEE Transactions on Circuits and Systems II: Express Briefs, 2017, vol. 64, no. 7, pp. 827–831, doi: 10.1109/TCSII.2016.2602828.

20. Rojas-Muñoz L.F., Sánchez-Solano S., Martínez-Rodríguez M.C., Brox P. True Random Number Generation Capability of a Ring Oscillator PUF for Reconfigurable Devices // Electronics, 2022, vol. 11, Paper ID 4028, 24 p., doi: 10.3390/electronics11234028.

21. Zulfikar Z., Soin N., Wan Muhamad Hatta S.F., Abu Talip M.S., Jaafar A. Routing Density Analysis of Area-Efficient Ring Oscillator Physically Unclonable Functions // Applied Sciences, 2021, vol. 11, no. 20, Paper ID 9730, 15 p., doi: 10.3390/app11209730.

22. Gu C., Chang C.H., Liu W. et al. A large-scale comprehensive evaluation of single-slice ring oscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs // Journal of Cryptographic Engineering, 2021, vol. 11, pp. 227–238, doi: 10.1007/s13389-020-00244-5.

23. Zulfikar Z., Walidainy H., Rahman A., Muchtar K. Reliability Improvement of 28 nm Intel FPGA Ring Oscillator PUF for Chip Identification // Cryptography, 2025, vol. 9, Paper ID 36, 16 p., doi: https://doi.org/10.3390/cryptography9020036.

24. Casado-Galán A., Núñez J., Tena-Sánchez E., Potestad-Ordóñez F.E., Acosta A.J. Assessment of an FPGA Implementation of a Hybrid PUF Based on a Configurable Transient Effect Ring Oscillator and Ring Oscillator (TERORO-PUF) // Electronics, 2026, vol. 15, no. 3, Paper ID 661, pp. 1–23, doi: https://doi.org/10.3390/electronics15030661.

25. Cui Y., Li J., Chen Y., Wang C., Gu C., O'Neill M., Liu W. An efficient Ring Oscillator PUF using programmable delay units on FPGA // ACM Transactions on Design Automation of Electronic Systems, 2023, vol. 29, no. 1, Article No.: 2, pp. 1–20, doi: 10.1145/3593807.

THE SECURITY ENSURING OF IOT-INFRASTRUCTURE'S WIRELESS DEVICES USING SEMICONDUCTOR PHYSICALLY UNCLONABLE FUNCTIONS

Sergey G. Mosin, Kazan Federal University, Kazan, Russia; LabSystems LLC, Vladimir, Russia;
Ryazan State Radio Engineering University, Ryazan, Russia, smosin@ieee.org

Abstract

The paper examines the security of wireless IoT-infrastructure in the context of Industry 4.0. A critical challenge is the limited resources of wireless IoT-devices (power consumption, computing power, and memory capacity), which precludes the use of complex cryptographic algorithms in real time. The use of semiconductor physically unclonable functions (PUFs) that generate unique pseudorandom sequences based on random variations in the integrated circuit manufacturing process is proposed to address this issue. A system model of IoT-infrastructure is presented in terms of set theory, enabling structural and parametric synthesis during design. The main scientific contribution is the development of a circuit model of an XOR-gate optimized for PUF synthesis based on reconfigurable ring oscillators. The model is adapted for TSMC 180 nm CMOS technology and enables the selection of rational PUF configurations at the early stages of designing wireless IoT-devices using custom integrated technology taking into account actual constraints. The Monte Carlo simulations were conducted considering correlated and uncorrelated technological variations. Two testbenches for a pseudorandom bit sequence accumulation were implemented. The obtained results were verified and demonstrated compliance with theoretical expectations, confirming the effectiveness of the proposed approach for synthesizing pseudorandom bit sequences for identification and authentication of wireless IoT-devices. Further research aims to assess the reliability and resilience to machine learning attacks.

Keywords: Internet of Things (IoT), wireless IoT-devices, security, physically unclonable function (PUF), circuit simulation, XOR-gate, reconfigurable ring oscillator.

References

- [1] A. Kumar, D. Singh, "Reinforcement learning based security method for IoT-Edge computing," *Wireless Networks*, 2026, vol. 32, pp. 1547–1567, doi: 10.1007/s11276-026-04123-5.
- [2] W. Jinchuan, N. Ming, G. Qiaojin, Y. Zhiwei, L. Suhang, "Design of an Intelligent IoT Platform Based on the Synergy of Edge Computing and Cloud Computing," *Journal of Big Data and Computing*, 2026, vol. 4, no. 1, pp. 27–33, doi: 10.62517/jbdc.202601104.
- [3] F.C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: A Review," *Informatics*, 2024, vol. 11, no. 4: 71. 22 p., doi: 10.3390/informatics11040071.

- [4] M.K. Jhariya, V. Dehalwar, J. Bharti, "Blockchain-enabled secure, lightweight self-sovereign identification and authentication framework for access management of IoT devices," *Cluster Computing*, 2026, vol. 29, Paper ID 291, 25 p., doi: 10.1007/s10586-026-06005-z.
- [5] H.K. Apat, V. Goswami, B. Sahoo et al., "An Adaptive Queueing Model for Optimizing IoT Application Performance in Fog-Cloud Computing Environment," *SN Computer Science*, 2026, vol. 7, Paper ID 486, 15 p., doi: 10.1007/s42979-026-04997-4.
- [6] V.A. Minaev, B.A. Shvyrev, T.R. Romashkin, "Internet of things security: key solutions," *Informacija i bezopasnost'*, 2023, vol. 26, no. 2, pp. 163-168. doi: 10.36622/VSTU.2023.26.2.001 (in Russian).
- [7] Y. Dou, "Current Status and Challenges of IoT Device Identity Authentication Technology," *Computers and Artificial Intelligence*, 2026, vol. 3, no. 2, pp. 65-77, doi: 10.70267/cai.26v3n2.6577.
- [8] Li Weibing, Wu Shenggang, Han Wei, "Blockchain-based IoT device identity authentication and data traceability," *International Journal of Computer Information Systems and Industrial Management Applications*, 2025, vol. 17, p. 17, doi: 10.70917/ijcism-2025-0316.
- [9] A. A. Boyko, M. Yu. Bykov, S. S. Kushev, M. A. Peregodov, "Authentication in cellular networks: overview of mathematical models," *Systems of Control, Communication and Security*, 2025, no. 1, pp. 187-219, doi: 10.24412/2410-9916-2025-1-187-219 (in Russian).
- [10] A. M. Mironov, "New mathematical model of authentication protocols and verification method based on this model," *Intelligent systems. Theory and applications*, 2018, vol. 22, no. 4, pp. 79-98 (in Russian).
- [11] J.H. Kang, M. Seo, "Enhanced Authentication for Decentralized IoT Access Control Architecture," *Cryptography*, 2023, vol. 7, no. 3, Paper ID 42, 17 p., doi: 10.3390/cryptography7030042.
- [12] S. Chan Suet Yan, A. Tang Su Wei, J. H. Bong, Q. L. Teh, S. Sivalingam, S. Y. Khoo, T. M. Nafy, "Authentication of IoT device with the enhancement of One-time Password (OTP)," *Journal of IT in Asia*, 2021, vol. 9, no. 1, pp. 29-40, doi: 10.33736/jita.3841.2021.
- [13] A. Malik, R. Kushwah, "A Secure Authentication and Key Establishment Protocol for IoT Devices Using ECCMD," *SN Computer Science*, 2025, vol. 6, Paper ID 803, 16 p., doi: 10.1007/s42979-025-04354-x.
- [14] S. Mosin, "A Model of LoRaWAN Communication in Class A for Design Automation of Wireless Sensor Networks Based on the IoT Paradigm," in *2018 IEEE East-West Design & Test Symposium (EWDTS)*, Kazan, 2018, pp. 1-6. doi: 10.1109/EWDTS.2018.8524618.
- [15] S. Mosin, "A Model for Univariate and Multivariate Simulating the Battery Lifetime of UE NB-IoT," in *2024 International Russian Automation Conference (RusAutoCon)*, Sochi, Russian Federation, 2024, pp. 13-18, Paper ID 10694326, doi: 10.1109/RusAutoCon61949.2024.
- [16] S. G. Mosin, "Search of optimal uplink radio resources configuration for reducing power consumption of UE NB-IoT at data transmission," *Dynamics of complex systems*, 2025, vol. 19, no. 2, pp. 40-49, doi: 10.18127/j19997493-202502-06 (in Russian).
- [17] K. Lata, L.R. Cenkeramaddi, "FPGA-Based PUF Designs: A Comprehensive Review and Comparative Analysis," *Cryptography*, 2023, vol. 7, no. 4, Paper ID 55, 30 p., doi: 10.3390/cryptography7040055.
- [18] M. Karmakar, S.F. Naz, A.P. Shah, "Fault-Tolerant Reversible Logic Gate-Based RO-PUF Design," *Memories - Materials, Devices, Circuits and Systems*, 2023, vol. 4, Paper ID 100055, 6 p., doi: 10.1016/j.memori.2023.100055.
- [19] T. Tanamoto, S. Yasuda, S. Takaya, S. Fujita, "Physically Unclonable Function Using an Initial Waveform of Ring Oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2017, vol. 64, no. 7, pp. 827-831, doi: 10.1109/TCSII.2016.2602828.
- [20] L.F. Rojas-Munoz, S. Sanchez-Solano, M.C. Martinez-Rodriguez, P. Brox, "True Random Number Generation Capability of a Ring Oscillator PUF for Reconfigurable Devices," *Electronics*, 2022, vol. 11, Paper ID 4028, 24 p., doi: 10.3390/electronics11234028.
- [21] Z. Zulfikar, N. Soin, S.F. Wan Muhamad Hatta, M.S. Abu Talip, A. Jaafar, "Routing Density Analysis of Area-Efficient Ring Oscillator Physically Unclonable Functions," *Applied Sciences*, 2021, vol. 11, no. 20, Paper ID 9730, 15 p., doi: 10.3390/app11209730.
- [22] C. Gu, CH. Chang, W. Liu et al., "A large-scale comprehensive evaluation of single-slice ring oscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs," *Journal of Cryptographic Engineering*, 2021, vol. 11, pp. 227-238, doi: 10.1007/s13389-020-00244-5.
- [23] Z. Zulfikar, H. Walidainy, A. Rahman, K. Muchtar, "Reliability Improvement of 28 nm Intel FPGA Ring Oscillator PUF for Chip Identification," *Cryptography*, 2025, vol. 9, Paper ID 36, 16 p., doi: <https://doi.org/10.3390/cryptography9020036>.
- [24] A. Casado-Galán, J. Nájera, E. Tena-Sánchez, F.E. Potestad-Ordóñez, A.J. Acosta, "Assessment of an FPGA Implementation of a Hybrid PUF Based on a Configurable Transient Effect Ring Oscillator and Ring Oscillator (TERORO-PUF)," *Electronics*, 2026, vol. 15, no. 3, Paper ID 661, pp. 1-23, doi: <https://doi.org/10.3390/electronics15030661>.
- [25] Y. Cui, J. Li, Y. Chen, C. Wang, C. Gu, M. O'Neill, W. Liu, "An efficient Ring Oscillator PUF using programmable delay units on FPGA," *ACM Transactions on Design Automation of Electronic Systems*, 2023, vol. 29, no. 1, Article No.: 2, pp. 1-20, doi: 10.1145/3593807.

Information about author:

Sergey G. Mosin, Kazan Federal University, Professor, Kazan, Russia; LabSystems LLC, Deputy Director General, Vladimir, Russia; Ryazan State Radio Engineering University, Professor, Ryazan, Russia. ORCID 0000-0003-1389-2602