Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет информатики и радиоэлектроники

УДК 004.312

Бурко
Лиана Александровна

МЕТОДЫ, АЛГОРИТМЫ И СРЕДСТВА УНИКАЛЬНОЙ ИДЕНТИФИКАЦИИ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМ

АВТОРЕФЕРАТ
на соискание степени магистра

по специальности 7-06-0611-05 – Компьютерная инженерия. Хранение и обработка данных

_____

Научный руководитель:
Иванюк Александр Александрович
доктор технических наук,
профессор каф. информатики, БГУИР

_____

Минск 2026

ВВЕДЕНИЕ

Методы цифровой обработки сигналов, машинного обучения и Рынок ПЛИС (программируемых логических интегральных схем) типа FPGA (Field Programmable Gate Array) демонстрирует уверенный рост, обусловленный растущим спросом на реконфигурируемые и высокопроизводительные вычислительные системы в центрах обработки данных, телекоммуникациях и автомобильной промышленности. Распространение задач искусственного интеллекта и машинного обучения, наряду с быстрым расширением сетей 5G, ускоряет внедрение FPGA благодаря их возможностям параллельной обработки и низкой задержке. Кроме того, достижения в области систем на кристалле (SoC) FPGA и интеграции встроенных FPGA расширяют возможности применения в периферийных вычислениях и устройствах IoT (Интернета вещей). Поскольку отрасли отдают приоритет гибкости, энергоэффективности и ускоренному прототипированию, FPGA становятся краеугольной технологией для интеллектуальных аппаратных систем следующего поколения.

Ярким примером практического применения ПЛИС является марсоход Perseverance, в котором используются радиационно-стойкие FPGA семейства Xilinx Virtex для реализации высокопроизводительных алгоритмов компьютерного зрения и автономной навигации. FPGA обеспечивают обработку изображений в реальном времени, включая коррекцию, фильтрацию и стереоанализ, что позволяет марсоходу непрерывно перемещаться по поверхности планеты без остановок на вычисления. Высокая надёжность и устойчивость к радиационному воздействию делают ПЛИС ключевым элементом длительных космических миссий, демонстрируя их эффективность в критически важных системах.

Дополнительным преимуществом FPGA в составе космических аппаратов является возможность их удалённой реконфигурации. В отличие от специализированных интегральных схем (ASIC), функциональность ПЛИС может быть изменена после запуска аппарата посредством передачи обновлённой конфигурации с Земли. Это позволяет корректировать алгоритмы обработки данных, устранять выявленные ошибки проектирования, адаптировать систему к новым условиям эксплуатации и даже восстанавливать работоспособность при частичных отказах, вызванных радиационным воздействием.

По прогнозам, мировой рынок FPGA вырастет с 11,73 млрд долларов США в 2025 году до 19,34 млрд долларов США к 2030 году при среднегодовом темпе роста 10,5%.

Клонирование является серьёзной проблемой для ПЛИС, так как их проекты легко скопировать или изменить. Поскольку многие ПЛИС теряют данные при выключении питания, их конфигурация каждый раз загружается заново из внешней памяти. Если злоумышленник имеет физический доступ к устройству, он может перехватить эти данные и использовать их для копирования проекта на другие ПЛИС. Для защиты применяют шифрование, при котором внутри ПЛИС должен храниться секретный ключ. Однако для этого часто требуется дополнительная память, что увеличивает стоимость и размеры

устройства. Кроме того, постоянно хранимый ключ может быть уязвим для атак.

Физически неклонируемые функции (ФНФ) устраняют недостатки цифрового хранения ключей, при котором секретный ключ постоянно хранится в энергонезависимой памяти. В ФНФ ключ формируется динамически на основе присущих и неклонируемых мезоскопических физических характеристик устройства, которые крайне сложно или практически невозможно воспроизвести.

Физические свойства каждого кремниевого устройства определяются с помощью набора запросов (входов) и соответствующего набора ответов (выходов). ФНФ могут использоваться в различных протоколах безопасности, таких как генерацию секретных ключей, генерацию случайных чисел, защиту интеллектуальной собственности ПЛИС, идентификацию устройств, аутентификацию микросхем, протоколы обмена и согласования ключей, защиту от подделок и безопасность Интернета вещей. Ряд ФНФ уже реализован в ASIC (Application-Specific Integrated Circuit) и, в частности, в ПЛИС типа FPGA. Широкое применение ПЛИС во встраиваемых системах и возможность быстрой кастомизации продуктов указывают на целесообразность реализации PUF непосредственно в ПЛИС.

Текущие лидеры рынка ПЛИС, а именно AMD (бывший Xilinx), Intel (бывшая Altera) и Microsemi, уже начали интеграцию ФНФ в свои серийные продукты для целей безопасности. В настоящее время ПЛИС Xilinx UltraScale+ позволяют пользователю реализовывать программные ядра ФНФ (используемые как ключ ФНФ) для защиты пользовательского ключа (red key) в процессе конфигурации. Аналогично, ПЛИС Intel Stratix 10 предоставляют пользователю доступ к PUF как части процесса конфигурации устройства для защиты пользовательского ключа и идентификации устройства.

Кроме того, отдельные ПЛИС Microsemi PolarFire могут использоваться в качестве корня доверия (Root of Trust) для безопасной аутентификации, а также для защиты интеллектуальной собственности заказчика. Также возможно приобретение программных ФНФ у сторонних разработчиков, таких как Intrinsic-ID Inc, Lewis Innovative Technology, QuantumTrace и Helion Technology Ltd и др.

Несмотря на активное внедрение ФНФ в коммерческие ПЛИС, остаются открытыми вопросы, связанные с особенностями их реализации, стабильностью ответов и пригодностью для практических приложений. В связи с этим задача исследования и реализации ФНФ в архитектуре ПЛИС с целью повышения уровня аппаратной безопасности является актуальной.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью исследования является разработка и экспериментальное исследование архитектуры физически неклонируемой функции на основе конфигурируемых кольцевых осцилляторов, обеспечивающей формирование уникальных идентификаторов и пригодной для задач генерации истинно случайных чисел.

Для достижения поставленной цели необходимо решить следующие задачи:

– Провести анализ существующих архитектур физически неклонируемых функций и методов их реализации на FPGA.

– Разработать архитектуру ФНФ на основе конфигурируемых кольцевых осцилляторов и реализовать её на платформе Xilinx ZYNQ-7000.

– Выполнить экспериментальное исследование статистических характеристик периодов сигналов ККО.

– Разработать аналитическую модель распределения значений регистрирующего счётчика и исследовать структуру групп разрядов.

– Исследовать характеристики межкристальной и внутрикристальной уникальности идентификаторов.

– Провести сравнительный анализ методов постобработки на основе аддитивного и мультипликативного скремблирования.

Объектом исследования является схема генерирования неклонируемых идентификаторов и случайных чисел на основе конфигурируемого кольцевого осциллятора.

Предметом исследования является частота сигналов, вырабатываемая схемами ККО, реализованными на ПЛИС.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа соответствует п.1 «Цифровые технологии и искусственный интеллект» (подпункты «программное обеспечение и программно-технические средства», «математические теории и методы, высокопроизводительные вычислительные системы, цифровые модели и двойники») приоритетных направлений научной, научно-технической и инновационной деятельности на 2026-2030 годы.

Научная новизна

Предложена схема генерации стабильных уникальных идентификаторов и истинно случайных чисел на базе схемы регистрации числа импульсов конфигурируемого кольцевого осциллятора в фиксированном временном окне

измерения, реализованной на программируемой логической интегральной схеме (ПЛИС).

Предложена программная аналитическая модель поведения конфигурируемого кольцевого осциллятора.

Личный вклад соискателя ученой степени

Результаты, приведенные в диссертации, и положения, выносимые на защиту, получены соискателем лично. Вклад научного руководителя профессора А. А. Иванюка связан с постановкой целей и задач исследования, определением возможных путей решения и обсуждением результатов исследований, проводимых автором. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертации результатов.

Апробация диссертации и информация об использовании ее результатов

Основные результаты диссертационной работы докладывались и обсуждались на 6 международных и республиканских научных конференциях, проводимых в Минске, Республика Беларусь: «Информационные технологии и системы» (2024, 2025), «Научная конференция аспирантов, магистрантов и студентов БГУИР» (2025, 2026), «17th International Conference on Pattern Recognition and Information Processing» (2025), «Технические средства защиты информации» (2026).

Опубликование результатов диссертации

По материалам диссертации опубликованы 7 печатных работ, 1 статья в рецензируемом научном журнале, 6 статей в сборниках материалов научных конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, пяти глав, заключения, библиографического списка и трех приложений. Общий объем диссертационной работы составляет 109 страниц, из них 76 страниц основного текста, 39 рисунков на 30 страницах, 3 таблицы на 4 страницах, библиография из 47 наименований, включая 7 публикации автора, на 4 страницах и 3 приложения на 17 страницах.

Проверка на уникальность

Проведена экспертиза диссертационной работы на корректность использования заимствованных материалов с применением сетевого ресурса

«Антиплагиат» (адрес доступа: https://antiplagiat.ru) в online режиме.

В результате проверки установлена корректность использования заимствованных материалов. Оригинальность диссертационной работы составляет 90,51%, а также 4,27% цитирования и 2,01% самоцитирования.

ОСНОВНОЕ СОДЕРЖАНИЕ

В первой главе рассмотрены теоретические основы физически неклонируемых функций (ФНФ). Выполнен анализ принципов их функционирования, основанных на использовании технологических вариаций полупроводниковых структур. Приведена классификация ФНФ по технологии реализации и уровню безопасности, рассмотрены основные архитектурные типы ФНФ на базе ПЛИС, включая ФНФ с задержкой и ФНФ с памятью. Особое внимание уделено ключевым характеристикам и метрикам оценки ФНФ, таким как стабильность, надежность, воспроизводимость, уникальность и единообразие ответов.

Во второй главе исследованы архитектура и принципы функционирования физически неклонируемой функции на основе конфигурируемого кольцевого осциллятора (ФНФ ККО). Рассмотрены симметричные и конфигурируемые симметричные пути как базовые элементы построения ФНФ, проанализированы классические архитектуры ФНФ на кольцевых осцилляторах и их модификации. Предложена новая архитектура ФНФ ККО с использованием одного регистрирующего счетчика, позволяющая одновременно получать стабильные идентификаторы и данные для генерации истинно случайных чисел. Также описаны экспериментальный стенд, используемая аппаратная платформа Xilinx ZYNQ-7000 и программные средства проведения исследований.

В третьей главе проведено экспериментальное исследование статистических характеристик периодов сигналов конфигурируемого кольцевого осциллятора. Выполнен анализ распределения значений регистрирующего счетчика, исследованы вероятностные характеристики отдельных разрядов и предложен подход к их классификации на стабильные, условно стабильные и случайные группы. Полученные результаты позволили выявить закономерности формирования различных групп разрядов и определить их пригодность для задач идентификации устройств и генерации случайных чисел.

В четвертой главе разработана аналитическая модель поведения периодов сигналов конфигурируемого кольцевого осциллятора. Выполнено моделирование различных групп разрядов регистрирующего счетчика и дано теоретическое обоснование причин их формирования. Предложен метод коррекции данных, направленный на устранение условно стабильной группы разрядов, а также проведено исследование особенностей метастабильной группы. Разработанная модель позволила объяснить наблюдаемые экспериментальные результаты и установить связь между физическими процессами в ККО и статистическими характеристиками выходных данных.

В пятой главе представлены методы получения уникальных идентификаторов на основе разработанной архитектуры ФНФ ККО. Выполнено исследование межкристальной и внутрикристальной уникальности идентификаторов, проведена оценка их качества с использованием стандартных метрик идентификации. Рассмотрены методы постобработки данных на основе

аддитивного и мультипликативного скремблирования, выполнен их сравнительный анализ и исследовано влияние на характеристики уникальности и случайности формируемых последовательностей. На основании проведенных экспериментов определены наиболее эффективные способы формирования стабильных идентификаторов и истинно случайных чисел.

ЗАКЛЮЧЕНИЕ

В рамках данной магистерской диссертации был проведён анализ существующих архитектур физически неклонируемых функций (ФНФ) и было показано, что ФНФ являются перспективным механизмом аппаратной безопасности, позволяющим реализовать идентификацию устройств, генерацию и восстановление криптографических ключей, а также формирование доверенной вычислительной среды без необходимости хранения секретной информации в явном виде. Установлено, что основой функционирования ФНФ являются случайные технологические вариации, определяющие уникальность физических характеристик каждого кристалла.

На основе анализа существующих решений была рассмотрена и реализована архитектура физически неклонируемой функции на базе конфигурируемого кольцевого осциллятора. Показано, что использование конфигурируемых симметричных путей позволяет получать множество частотных состояний при фиксированном количестве осцилляторов, что снижает аппаратные затраты по сравнению с классическими архитектурами ФНФ КО.

Разработана и экспериментально исследована схема ФНФ ККО, использующая один регистрирующий счётчик для формирования многобитного ответа, зависящего от параметра окна измерения. Полученный выходной вектор позволяет выделять как стабильную часть, пригодную для идентификации устройств, так и нестабильную шумовую компоненту, потенциально пригодную для генерации истинно случайных последовательностей.

Для проведения экспериментальных исследований была создана аппаратно-программная инфраструктура на базе FPGA Xilinx ZYNQ-7000 и плат Digilent ZYBO Z7-10. Средства Vivado использовались для проектирования и реализации аппаратной части, Vitis – для разработки встроенного программного обеспечения и управления экспериментом, Tera Term – для сбора экспериментальных данных через последовательный интерфейс, а Python (Jupyter Notebook) – для автоматизированной обработки, визуализации и статистического анализа результатов.

В ходе экспериментов исследовано влияние параметра окна измерения на статистические характеристики регистрируемых значений. Установлено, что распределения значений счётчика при определённых параметрах близки к нормальному распределению, что подтверждено графическим анализом и статистическими критериями проверки гипотезы нормальности.

На основании анализа вероятностей появления единичных битов предложено разделение разрядов регистрирующего счётчика на три группы: стабильные разряды G2, условно стабильные разряды G1 и нестабильные разряды G1. Разработана аналитическая модель, объясняющая формирование группы G1 эффектами арифметических переносов, возникающих при квантовании и округлении нормально распределённых значений.

Предложен метод коррекции экспериментальных данных, направленный на устранение условно стабильной группы G1. Показано, что применение данной процедуры позволяет преобразовать структуру выходных данных к

двухгрупповой модели G2-G0 , что упрощает дальнейшее формирование идентификаторов и случайных последовательностей.

Проведена оценка характеристик межкристальной и внутрикристальной уникальности идентификаторов, формируемых предложенной архитектурой ФНФ ККО. Установлено, что исходные идентификаторы без постобработки не обеспечивают достижения оптимальных значений метрик уникальности и характеризуются наличием корреляции между последовательностями.

Для повышения статистических характеристик идентификаторов исследованы методы постобработки на основе аддитивного и мультипликативного скремблирования. Показано, что аддитивный скремблер улучшает значения расстояния Хэмминга, однако не обеспечивает устойчивого приближения метрик уникальности к теоретически оптимальному значению 0,5. Наилучшие результаты продемонстрировала схема мультипликативного скремблирования, обеспечивающая значения межкристальной и внутрикристальной уникальности, стабильно близкие к 0,5, а также отсутствие нулевых значений исследуемых метрик.

Дополнительно установлено, что применение постобработки существенно улучшает статистические характеристики выходных последовательностей и повышает их пригодность для генерации истинно случайных чисел.

Таким образом, результаты работы подтверждают практическую применимость предложенной архитектуры физически неклонируемой функции на основе конфигурируемого кольцевого осциллятора для задач аппаратной идентификации устройств, генерации уникальных идентификаторов и формирования аппаратных источников энтропии в системах аппаратной безопасности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1] Бурко, Л. А. Исследование поведения кольцевого осциллятора / Л. А. Бурко, А. А. Иванюк // Информационные технологии и системы 2024 (ИТС 2024) = Information Technologies and Systems 2024 (ITS 2024) : материалы международной научной конференции, Минск, 20 ноября 2024 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2024. – С. 81–82.

[2] Бурко, Л. А. Исследование ФНФ кольцевого осциллятора как источника случайности / Л. А. Бурко // Компьютерные системы и сети: материалы 61-й научной конференции аспирантов, магистрантов и студентов, Минск, 22–26 апреля 2025 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2025. – С. 464–466.

[3] Бурко, Л. А. Генерация случайных чисел на основе схемы фнф конфигурируемого кольцевого осциллятора / Л. А. Бурко, А. А. Иванюк // Информационные технологии и системы 2025 (ИТС 2025) : материалы Международной научной конференции, Минск, 19 ноября 2025 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск, 2025. – С. 143–144.

[4] Иванюк А.А., Бурко Л.А. Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого осциллятора. *Информатика*. 2025;22(4):65-81. https://doi.org/10.37661/1816-0301-2025-22-4-65-81

[5] Ivaniuk, A. Unclonable Identification and True Random Number Generation Based on CRO PUF / A. Ivaniuk, L. Burko // Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference, September 16-18, 2025, Minsk, Belarus / UIIP NASB. – Minsk, 2025.– pp. 103-107.

[6] Бурко Л.А., Иванюк А.А. Метод повышения уникальности аппартных идентификаторов плис на основе физически неклонируемых функций типа конфигурируемого кольцевого осциллятора / Технические средства защиты информации: материалы XXIV Международной научно-технической конференции, Минск, 8 апреля 2026 года / Белорусский государственный университет информатики и радиоэлектроники [и др.] ; редкол.: О. В. Бойправ [и др.]. – Минск, 2026. – 436 с.

[7] Бурко, Л. А. Статистическое исследование данных, полученных с фнф на конфигурируемых кольцевых осцилляторах / Л. А. Бурко // Компьютерные системы и сети: материалы 62-й научной конференции аспирантов, магистрантов