Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.3, 681.5

ЗАЛИВАКО
Сергей Сергеевич

СИНТЕЗ АППАРАТНЫХ СРЕДСТВ НЕКЛОНИРУЕМОЙ ИДЕНТИФИКАЦИИ И ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМАХ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.05 – Элементы и устройства вычислительной техники и систем управления

Минск 2018

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель	**Иванюк Александр Александрович**, доктор технических наук, доцент, профессор кафедры информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Официальные оппоненты:	**Петровский Александр Александрович**, доктор технических наук, профессор, профессор кафедры электронных вычислительных средств учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
	Мулярчик Константин Сергеевич, кандидат технических наук, доцент, доцент кафедры телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий Белорусского государственного университета
Оппонирующая организация	Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»

Защита состоится «11» октября 2018 г. в 14:00 на заседании совета по защите диссертаций Д 02.15.01 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293–89–89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Автореферат разослан «4» сентября 2018 г.

Ученый секретарь совета
по защите диссертаций, кандидат
технических наук, доцент Ревотюк М. П.

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время цифровые электронные устройства повсеместно используются в различных сферах человеческой деятельности. Основная функциональность данного класса устройств реализована с помощью интегральных схем, проектирование и изготовление которых является длительным и трудоемким процессом. Применение программируемых логических устройств для реализации цифровой электроники позволило сократить сроки проектирования сложных технических систем с 12–18 месяцев до 3–6 месяцев.

Случайные вариации технологического процесса изготовления интегральных схем оказывают негативное влияние на характеристики производительности и надежности реализуемых схемотехнических решений. С другой стороны, данные вариации используются для реализации так называемых физически неклонируемых функций (ФНФ). Основными применениями ФНФ являются идентификация цифровых устройств (ЦУ) и генерирование случайных числовых последовательностей. Например, многие крупные компании, серийно выпускающие программируемые логические интегральные схемы (Xilinx, Intel (Altera), Microsemi и др.), в настоящее время реализовали средства идентификации и аутентификации ЦУ на основе ФНФ. Идентификаторы ЦУ, полученные на основе ФНФ, обладают такими свойствами, как уникальность, случайность и невоспроизводимость (неклонируемость), что позволяет эффективно решать практические задачи аппаратной криптографии.

В силу изменения температуры окружающей среды, а также неизбежного износа и деградации кристалла интегральной схемы, генерируемые ФНФ идентификаторы являются нестабильными, т. е. изменяющими свое значение с течением времени. С другой стороны, ФНФ являются хорошим источником случайности для построения на их основе генераторов случайных числовых последовательностей, однако их вероятностные характеристики не всегда соответствуют криптографическим стандартам. В свою очередь, увеличение стабильности ФНФ приводит к уменьшению ее случайности, что способствует уязвимости к криптографическим атакам.

В этой связи актуальной представляется задача синтеза аппаратных средств идентификации и генерирования случайных числовых последовательностей на основе ФНФ с высокими характеристиками стабильности, уникальности, случайности, а также низкой уязвимостью к криптографическим атакам. Решение данной задачи позволит обеспечить уникальность, аутентичность, структурную целостность и защиту от несанкционированного копирования цифровых устройств.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Диссертационная работа выполнена в соответствии с научно-техническими заданиями и планами работ кафедры «Вычислительные методы и программирование», кафедры «Информатика», научно-исследовательской лаборатории 3.3 «Диагностика средств вычислительной техники» учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», а также научно-исследовательского центра разработок по проектированию интегральных схем «Virtus» (англ. Virtus, IC Design Center of Excellence) Наньянгского технологического университета (НТУ, Сингапур). Работа проводилась в рамках следующих научно-исследовательских проектов: «Моделирование и оптимизация параметров электронных приборов и устройств» (ГБ № 11-2035); «Методы и алгоритмы моделирования структурно сложных объектов с перестраиваемой архитектурой» (ГБ № 16-2017); «Разработка методов и алгоритмов защиты цифровых устройств программируемой логики от несанкционированного использования» (№ Ф14МВ-003), Белорусский республиканский фонд фундаментальных исследований и Министерство образования Республики Беларусь; «Singapore Ministry of Education Academic Research Fund (AcRF) / Tier 1 Grant MOE 2014-T1-002-141» (RG186/14), Министерство образования Республики Сингапур.

Цель и задачи исследования

Целью работы является синтез аппаратных средств неклонируемой идентификации и аутентификации, а также генераторов случайных числовых последовательностей на программируемых логических интегральных схемах.

Для достижения поставленной цели необходимо решить следующие задачи исследования.

1. Разработать метод неклонируемой идентификации на программируемых логических интегральных схемах с улучшенной характеристикой стабильности в условиях изменения температуры окружающей среды.

2. Разработать метод и аппаратные средства снижения уязвимости физически неклонируемой функции типа арбитр к криптографическим атакам.

3. Разработать метод структурного синтеза генераторов случайных числовых последовательностей с равномерным законом распределения на основе известных физически неклонируемых функций с целью их реализации на программируемых логических интегральных схемах.

Объектом исследования являются программируемые логические интегральные схемы. Предмет исследования – физически неклонируемые функции, реализованные на ПЛИС.

Научная новизна

1. Разработана методика обнаружения метастабильного состояния арбитра физически неклонируемой функции, основанная на эффекте затухающего колебания асинхронного RS-триггера, которая в отличие от существующих решений не требует многократного повторения запросов.

2. Предложено оригинальное решение задачи генерирования стабильных неклонируемых идентификаторов цифровых устройств, реализуемых на программируемых логических интегральных схемах, с учетом особенностей задержки распространения сигналов для физически неклонируемой функции типа арбитр.

3. Предложен новый алгоритм классификации запросов физически неклонируемой функции типа арбитр, позволяющий повысить характеристику стабильности ответов без применения дополнительных аппаратурных затрат.

4. Разработан новый метод снижения уязвимости физически неклонируемой функции типа арбитр к криптографическим атакам с помощью машинного обучения, основанный на применении нелинейного преобразования значений запросов.

5. Предложен новый метод структурного синтеза генераторов случайных числовых последовательностей с равномерным законом распределения, основанный на реализации физически неклонируемых функций на программируемых логических интегральных схемах.

Положения, выносимые на защиту

1. Методика обнаружения метастабильного состояния арбитра физически неклонируемой функции, основанная на эффекте затухающего колебания асинхронного RS-триггера, позволяющая улучшить характеристики стабильности с 0,5648 до 0,9979 и уникальности с 0,4735 до 0,4982 при незначительных аппаратурных затратах (менее 1 % на ПЛИС семейства Xilinx Artix-7 и Zynq-7000).

2. Математическая модель представления задержки распространения сигналов для физически неклонируемой функции типа арбитр, особенностью которой является описание метастабильного состояния арбитра и позволяющая синтезировать аппаратные средства неклонируемой идентификации на программируемых логических интегральных схемах с улучшенной характеристикой стабильности до 1,0.

3. Алгоритм классификации запросов физически неклонируемой функции типа арбитр, позволяющий генерировать уникальные идентификаторы цифровых устройств, реализуемых на программируемых логических интегральных схемах, с улучшением характеристики стабильности с 0,5648 до 1,0 в условиях изменения температуры окружающей среды и без применения дополнительных аппаратурных затрат.

4. Метод снижения уязвимости физически неклонируемой функции типа арбитр к криптографическим атакам, основанный на применении нелинейного преобразования значений запросов, который позволяет уменьшить долю предсказанных злоумышленником ответов с 98 до 50 %, а также сократить аппаратурные затраты на 10 % в сравнении с существующими решениями.

5. Метод структурного синтеза генераторов случайных числовых последовательностей с равномерным законом распределения на основе физически неклонируемых функций, который в сравнении с существующими решениями позволяет на 40 % сократить аппаратурные затраты, а также улучшить качество вырабатываемых случайных последовательностей по характеристикам приблизительной энтропии и некоррелированности при реализации на программируемых логических интегральных схемах.

Личный вклад соискателя ученой степени

Результаты, приведенные в диссертации, и положения, выносимые на защиту, получены соискателем лично. Вклад научного руководителя доктора технических наук, доцента 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 16 международных и республиканских научных конференциях: «Информационные технологии и системы» (ITS’2012, 2013, 2014, 2015, 2016) – Минск, Республика Беларусь, 2012, 2013, 2014, 2015, 2016; научная конференция аспирантов, магистрантов и студентов БГУИР (СНТК’2013, 2014, 2015) – Минск, Республика Беларусь, 2013, 2014, 2015; 2nd Belarus-Korea Forum 2013 – Minsk, The Republic of Belarus, 2013; Международная научно-техническая конференция, приуроченная к 50-летию МРТИ–БГУИР – Минск, Республика Беларусь, 2014; International Symposium on Integrated Circuits (ISIC’2014)

– Singapore, 2014; Международная научно-практическая интернет-конференция «Тенденции и перспективы развития науки и образования в условиях глобализации» – Переяславль-Хмельницкий, Украина, 2015; 21st IEEE Asia and South Pacific Design Automation Conference (ASP-DAC'2016) – Macau, People Republic of China, 2016; 18th IEEE International Symposium on Quality Electronic Design (ISQED'2017) – Santa Clara, CA, United States of America, 2017; IX Международная научно-техническая конефренция «Информационные технологии в промышленности, логистике и социальной сфере» (ITI'2017) – Минск, Республика Беларусь, 2017; 50th IEEE International Symposium on Integrated Circuits and Systems (ISCAS'2017) – Baltimore, MD, United States of America, 2017.

Опубликование результатов диссертации

По материалам диссертации опубликованы 23 печатные работы, в том числе 1 глава в монографии, 5 статей в рецензируемых научных журналах, 6 статей в сборниках материалов научных конференций и 11 тезисов докладов.

Общий объем публикаций по теме диссертации, соответствующий пункту 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, составляет около 12,3 авторского листа.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и трех приложений. Общий объем диссертационной работы составляет 224 страницы, из них 98 страниц основного текста, 62 рисунка на 42 страницах, 18 таблиц на 14 страницах, библиография из 211 наименований, включая 23 публикации автора, на 18 страницах и три приложения на 52 страницах.

ОСНОВНАЯ ЧАСТЬ

Во **введении** обоснована актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, определена область, основные направления, цель и задачи исследования.

В **первой главе** проведен анализ основных методов идентификации цифровых устройств, генерирования случайных числовых последовательностей (ГСЧП), а также существующих реализаций физически неклонируемых функций (ФНФ) на программируемых логических интегральных схемах (ПЛИС).

Эффективность методов идентификации по критериям снижения аппаратурных затрат и повышения криптографической стойкости может быть значительно улучшена за счет применения ФНФ. Методы активной идентификации в отличие от методов пассивной идентификации основаны на использовании

случайности и уникальности вариаций техпроцесса изготовления интегральных схем и, следовательно, в принципе не могут быть реализованы без ФНФ. Реализации ГСЧП в большинстве случаев основаны на физических процессах, задержках цифровых элементов, системах фазовой синхронизации и динамического хаоса. Использование ФНФ в качестве источника случайности позволяет повысить уровень криптографической стойкости проектируемых ГСЧП.

Рассмотрена классификация ФНФ по различным признакам, которая приведена на рисунке 1.

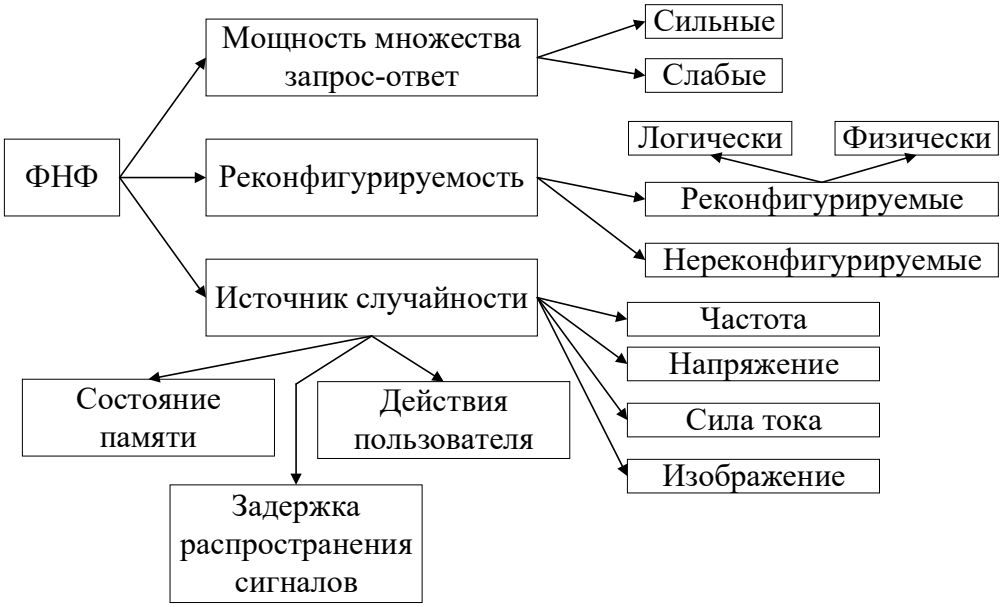


Рисунок 1. – Классификация ФНФ по различным признакам

Выделяют две основные области применения ФНФ: идентификация/аутентификация цифровых устройств и генерирование случайных числовых последовательностей. Актуальной проблемой существующих реализаций ФНФ является нестабильность их ответов при изменяющихся внешних условиях, а также внутреннем износе и деградации кристалла интегральной схемы. Повышение характеристики стабильности ФНФ, в свою очередь, приводит к ухудшению ее случайности, что повышает уязвимость к криптографическим атакам.

ПЛИС типа FPGA имеет три класса источников извлечения уникальных вариаций технологического процесса изготовления: конфигурируемые элементы, встроенные блоки статической памяти и память конфигурации. Следовательно, данная технологическая платформа подходит для схемотехнических испытаний различных типов ФНФ.

Во **второй главе** предложена методика обнаружения метастабильности, математическая модель задержки распространения сигналов, алгоритм класси-

фикации запросов для ФНФ типа арбитр (АФНФ), предназначенные для реализации методов идентификации и аутентификации цифровых устройств. Структурная схема АФНФ приведена на рисунке 2.

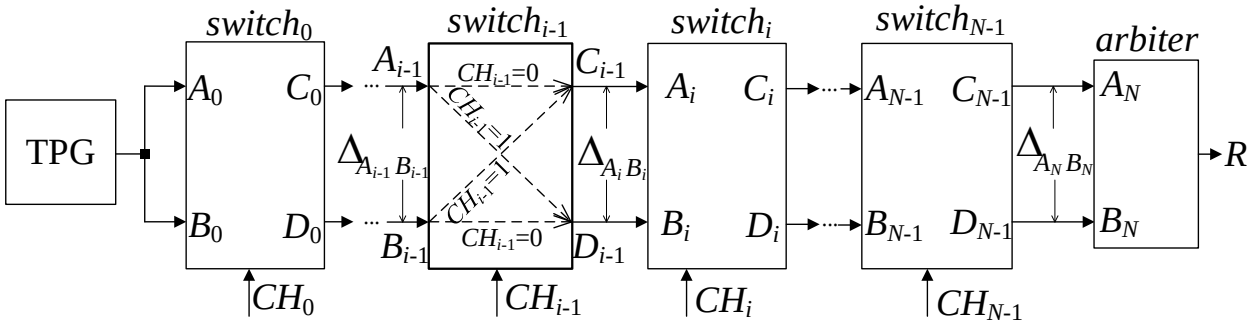


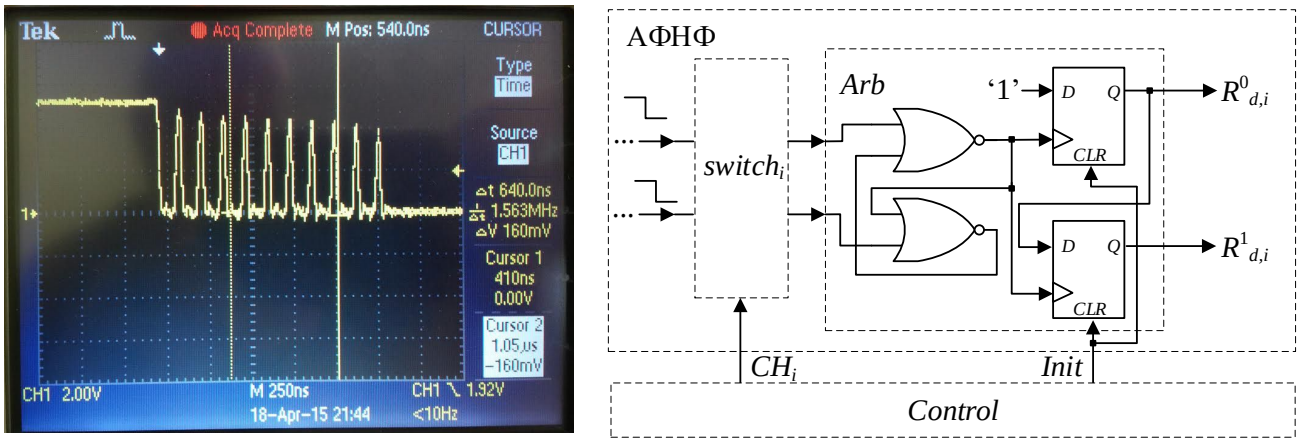
Рисунок 2. – Структурная схема ФНФ типа арбитр

Анализ существующих ФНФ показал, что АФНФ является наиболее подходящей для реализации как методов идентификации, так и методов генерирования случайных числовых последовательностей. В сравнении с другими типами ФНФ АФНФ имеет более высокие значения характеристик уникальности и случайности. С другой стороны, значение характеристики стабильности АФНФ ниже, чем у ФНФ кольцевых генераторов и ФНФ на основе памяти по причине эффекта метастабильности арбитра. Данный эффект наблюдается в случае, если разность временных задержек передних фронтов сигналов на входе данных и входе синхронизации не попадает в интервал от -t_{hold} (времени удержания) до t_{setup} (времени предустановки). Параметры t_{hold} и t_{setup} являются уникальными и определяются используемой технологией и особенностями реализации арбитра.

Для улучшения характеристики стабильности АФНФ предложено исследовать не только передний фронт тестового импульса, а весь импульс целиком. Предложенная модификация схемы арбитра на основе четырех D-триггеров позволяет выделить около 1 % значений запросов, для которых длительность тестовых импульсов значительно отличается, а также около 9 % запросов, ответы на которые попадают в метастабильное состояние. Остальные 90 % запросов порождают два устойчивых состояния D-триггеров, соответствующие стабильному логическому нолю и стабильной логической единице в классической реализации АФНФ.

Как было показано в работе T. Kacprzak “Analysis of oscillatory metastable operation of an RS flip-flop”, при функционировании асинхронного RS-триггера на выходе наблюдается высокочастотное затухающее колебание (рисунок 3, а) при переходе из запрещенного состояния в состояние хранения. Данный эффект был использован для обнаружения метастабильного состояния асинхрон-

ного RS-триггера с помощью схемы, приведенной на рисунке 3, б.



а) б)

Рисунок 3. – Высокочастотное затухающее колебание RS-триггера (а); предлагаемая схема арбитра (б)

Предложенные модификации арбитра позволили улучшить характеристики стабильности с 0,5648 до 0,9979 и уникальности с 0,4735 до 0,4982 при незначительных аппаратурных затратах (менее 1 % на ПЛИС семейства Xilinx Artix-7 и Zynq-7000).

Предложена математическая модель временной разности задержек двух сигналов $\Delta_{A_N B_N}$, распространяемых по симметричным путям АФНФ. Значение $\Delta_{A_N B_N}$ может быть представлено с помощью соотношения

$$\Delta_{A_N B_N}(CH_{N-1}, CH_{N-2}, \ldots, CH_0) = \sum_{j=0}^{N-1}(\delta_j \prod_{i=0}^{j} Sign_i), \quad (1)$$

где CH_i – i-й разряд двоичного значения запроса; δ_j – уникальное значение задержки для звена j АФНФ; $Sign_i$ – знак задержки, определяемый значением CH_i ($i, j \in [0, N-1]$, N – разрядность АФНФ).

В итоге значение ответа на выходе R = {0, 1, X} (X – метастабильное состояние) зависит от результирующей разницы между фронтами сигналов $\Delta_{A_N B_N}$:

$$R = \begin{cases} 0, & \text{если } \Delta_{A_N B_N} \leq -t_{hold}, \\ 1, & \text{если } \Delta_{A_N B_N} \geq t_{setup}, \\ X, & \text{если } -t_{hold} < \Delta_{A_N B_N} < t_{setup}. \end{cases} \quad (2)$$

На основе предложенной модели разработан алгоритм классификации запросов, основанный на изменении старшего и младшего бита запроса CH^{Ω}

($\Omega \in [0, 2^N - 1]$). На рис. 4 показан график зависимости значений задержек от двоичных значений запросов CH^{Ω} (начальный запрос), $CH^{\Omega'}$ (запрос с измененным младшим битом), $CH^{\Omega''}$ (запрос с измененным старшим битом), $CH^{\Omega'''}$ (запрос с измененными старшим и младшим битами).

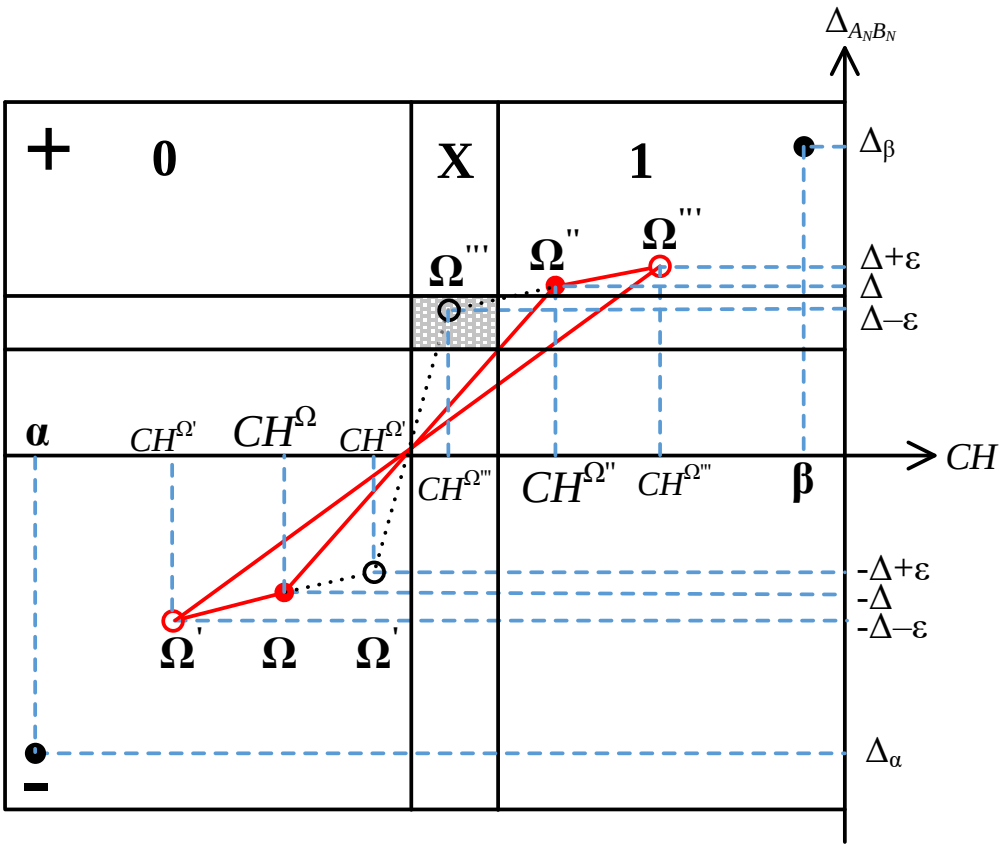


Рисунок 4. – График зависимости значений задержки $\Delta_{A_N B_N}$ от значений запросов CH

В общем случае изменение старшего бита произвольного запроса CH^{Ω} приводит к изменению знака задержки $\Delta_{A_N B_N}$, что, в свою очередь, вызывает инверсию значения ответа R с высокой вероятностью. При изменении младшего бита запроса, напротив, инверсия значения R маловероятна. В связи с этим определены два типа запросов: сильные (CH_s) и слабые (CH_w). Сильным запросом CH_s назовем такой запрос, для которого справедливо соотношение:

$$R_0 = R_1 = \overline{R_2} = \overline{R_3}, \tag{3}$$

где $R_0 = PUF(CH_s^{\Omega})$; $R_1 = PUF(CH_s^{\Omega'})$; $R_2 = PUF(CH_s^{\Omega''})$; $R_3 = PUF(CH_s^{\Omega'''})$.

Слабым запросом CH_w назовем такой запрос, для которого соотношение (3) не соблюдается. Было экспериментально показано, что сильные запросы обладают гораздо более высоким уровнем стабильности. Предложен тест на под-

тверждение стабильности ответов, заключающийся в изменении дополнительных произвольных $k < N$ бит сильного запроса CH_s всеми возможными 2^k способами. Если значение ответа R остается неизменным, то запрос CH_s классифицируется как устойчиво стабильный. Результаты тестирования стабильности ответов P_{stable} при k = 0,. . ., 4, N = 128 и изменениях значений температуры от –40 до +90 °C приведены на рисунке 5.

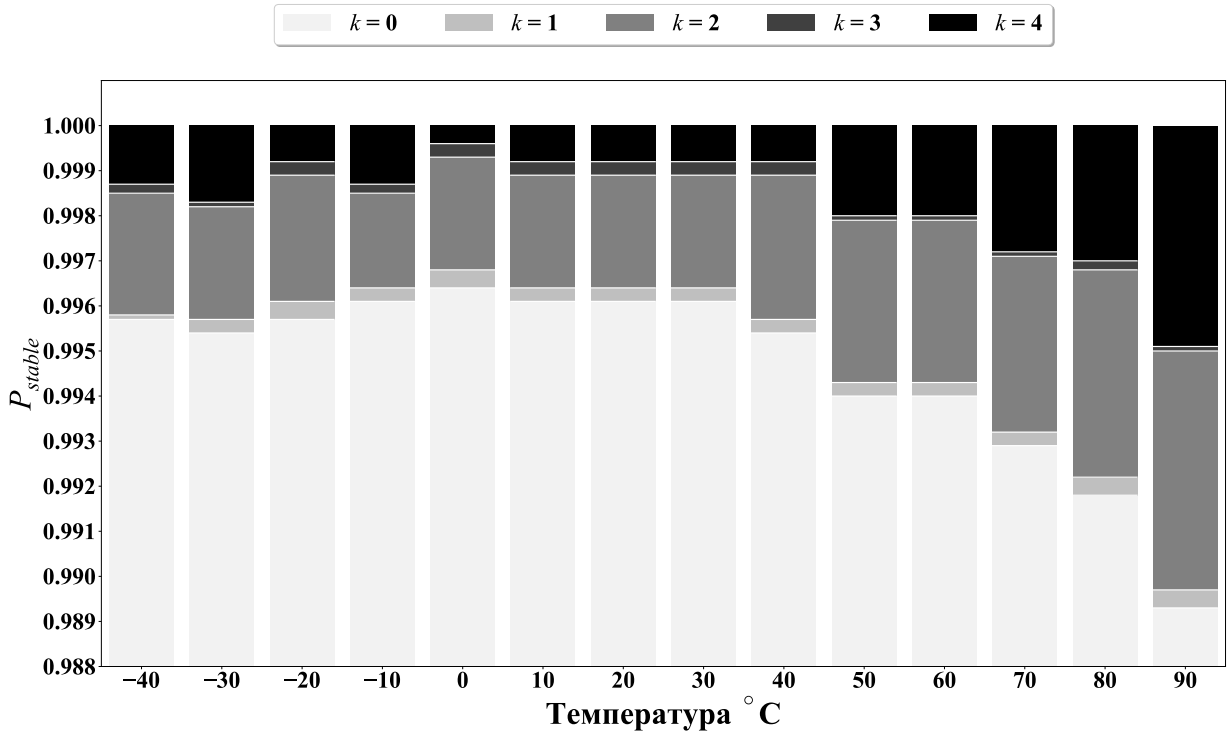


Рисунок 5. – График зависимости значения стабильности P_{stable} от температуры

Установлено, что параметры региона метастабильности отличаются значительно между компонентами АФНФ как внутри одного кристалла, так и между кристаллами различных семейств ПЛИС. Эксперимент был проведен с использованием 8 идентичных компонент АФНФ на 21 плате быстрого прототипирования двух различных семейств ПЛИС (Xilinx Artix-7 и Xilinx Zynq-7000). Результаты данного эксперимента приведены на рисунке 6.

Третья глава посвящена методам снижения уязвимости АФНФ к криптографическим атакам. Анализ существующих протоколов аутентификации показал, что методы, основанные на нелинейном преобразовании значений запросов, являются менее уязвимыми к криптографическим атакам и требуют меньших аппаратурных затрат.

Предложены три метода структурной модификации АФНФ на основе нелинейного преобразования значений запросов: алгоритм хеширования SHA-256, регистр синхронных T-триггеров, а также многоканальный сигнатурный анализатор (англ. Multiple Input Signature Register, MISR). Последний метод показал

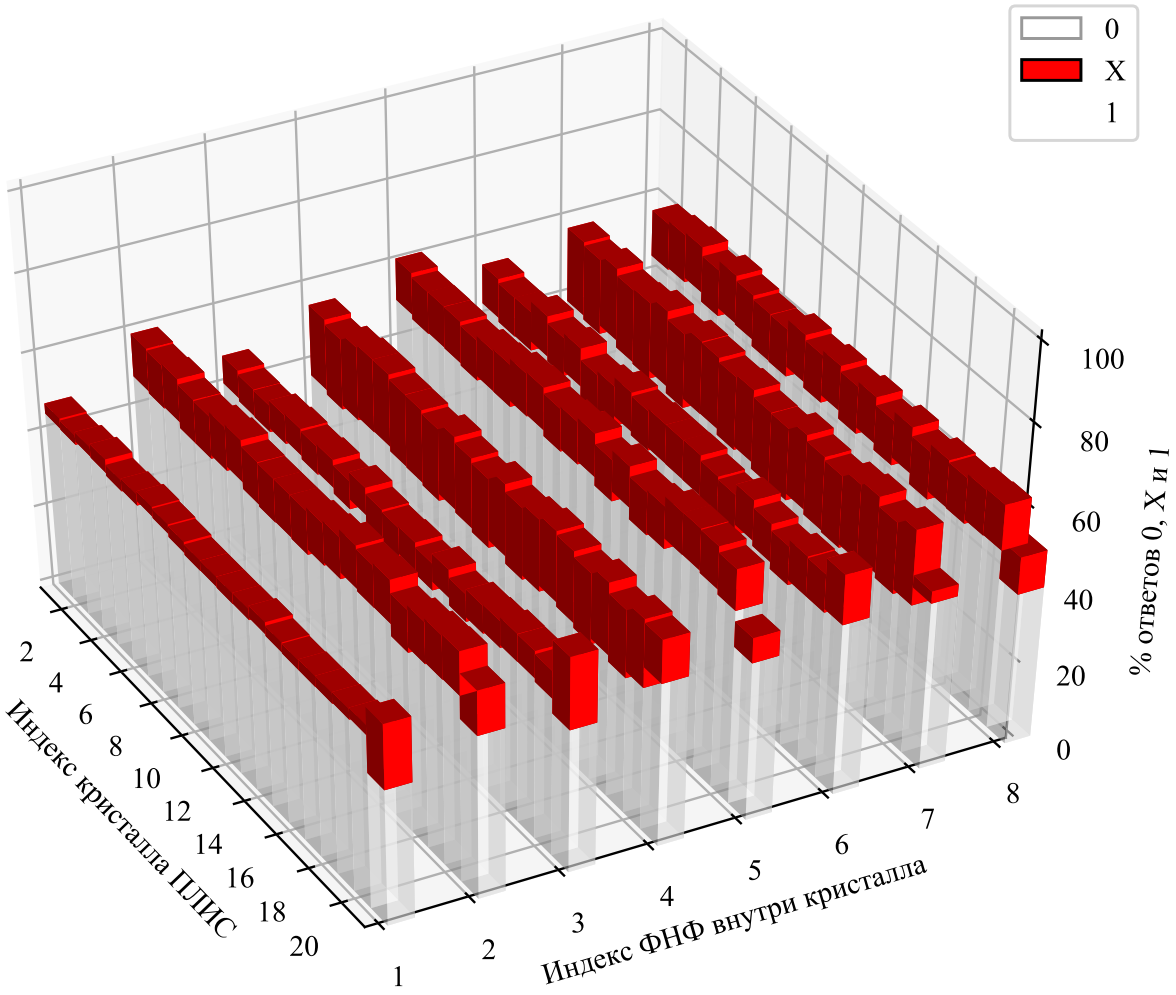


Рисунок 6. – Диаграмма распределения ответов 0, X и 1 для множества идентичных компонент АФНФ, реализованных на различных ПЛИС

наименьшую уязвимость к криптографическим атакам при небольших аппаратурных затратах. Схемная реализация предложенного метода приведена на рисунке 7.

В данной главе был также предложен протокол аутентификации на основе структурной модификации АФНФ (рисунок 8), который включает в себя три этапа: регистрация параметров, собственно аутентификация, обновление параметров.

Предлагаемый метод позволяет снизить точность моделей, построенных с помощью метода опорных векторов, градиентного бустинга и эволюционной стратегии адаптации ковариационных матриц. Таким образом, реализация модифицированной АФНФ на базе ПЛИС может быть использована в качестве средства идентификации с высокими характеристиками стабильности, уникальности, случайности и низкой уязвимостью к криптографическим атакам.

В **четвертой главе** предложены реализации ГСЧП на основе ФНФ. Существует два основных класса методов проектирования ГСЧП на основе ФНФ:

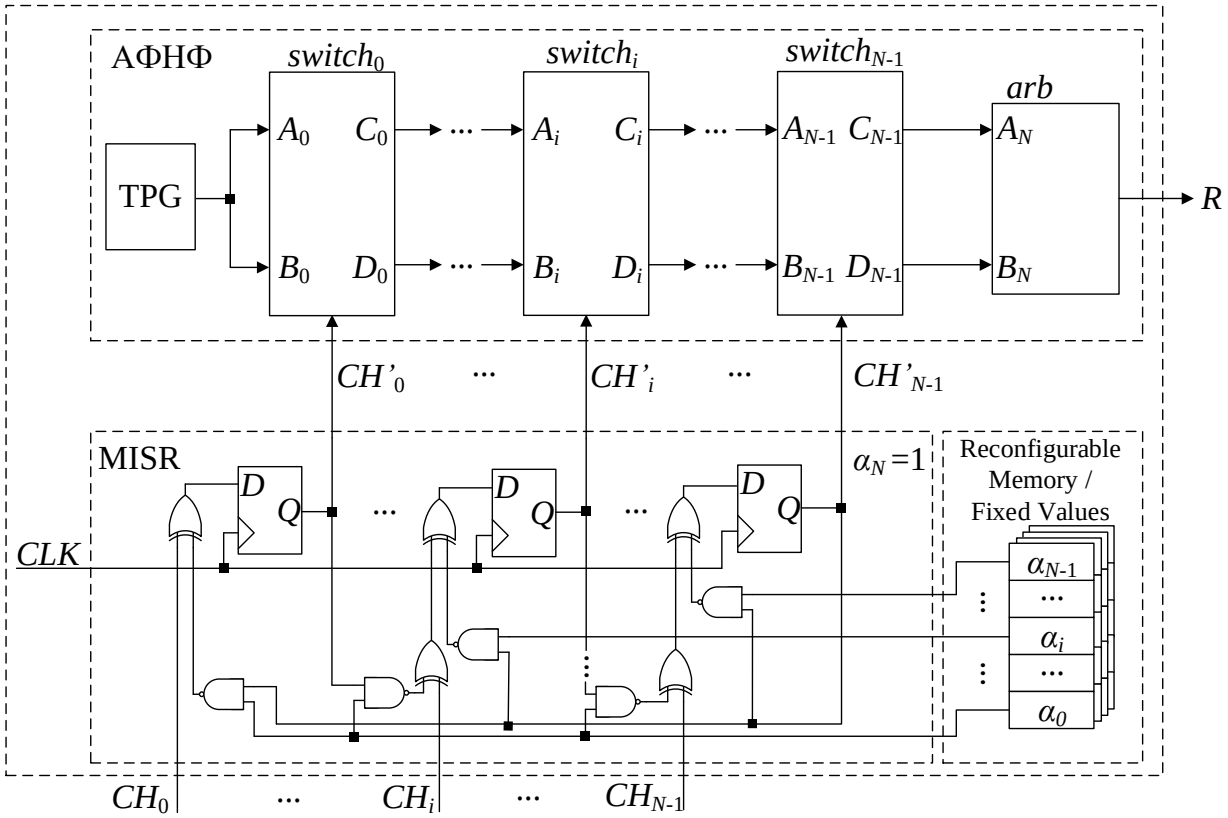


Рисунок 7. – Предлагаемая модификация схемы АФНФ на основе MISR

улучшение статистических характеристик случайной последовательности, вырабатываемой ФНФ, с помощью генератора псевдослучайных числовых последовательностей; отбор запросов ФНФ, ответы на которые являются менее стабильными. Предложенный метод синтеза ГСЧП позволяет проектировать ЦУ, работающие в режимах идентификации и ГСЧП. Обобщенная структурная схема данного класса устройств приведена на рисунке 9.

Предложены реализации ГСЧП как на основе первого класса методов (ФНФ кольцевых генераторов, комбинированная ФНФ, АФНФ), так и на основе второго – использование слабых запросов АФНФ. Улучшение статистических характеристик исходных последовательностей было осуществлено с помощью дерева элементов XOR, линейного сдвигового регистра с обратной связью, адаптивного сигнатурного анализатора, MISR.

Показано, что использование АФНФ в качестве источника случайности позволяет реализовать ГСЧП с равномерным законом распределения с наименьшими аппаратурными затратами. Последовательности, вырабатываемые генератором, успешно проходят тесты статистического пакета NIST. Следовательно, АФНФ, реализованная на ПЛИС, может быть использована как средство идентификации, так и компактный генератор случайных числовых последовательностей.

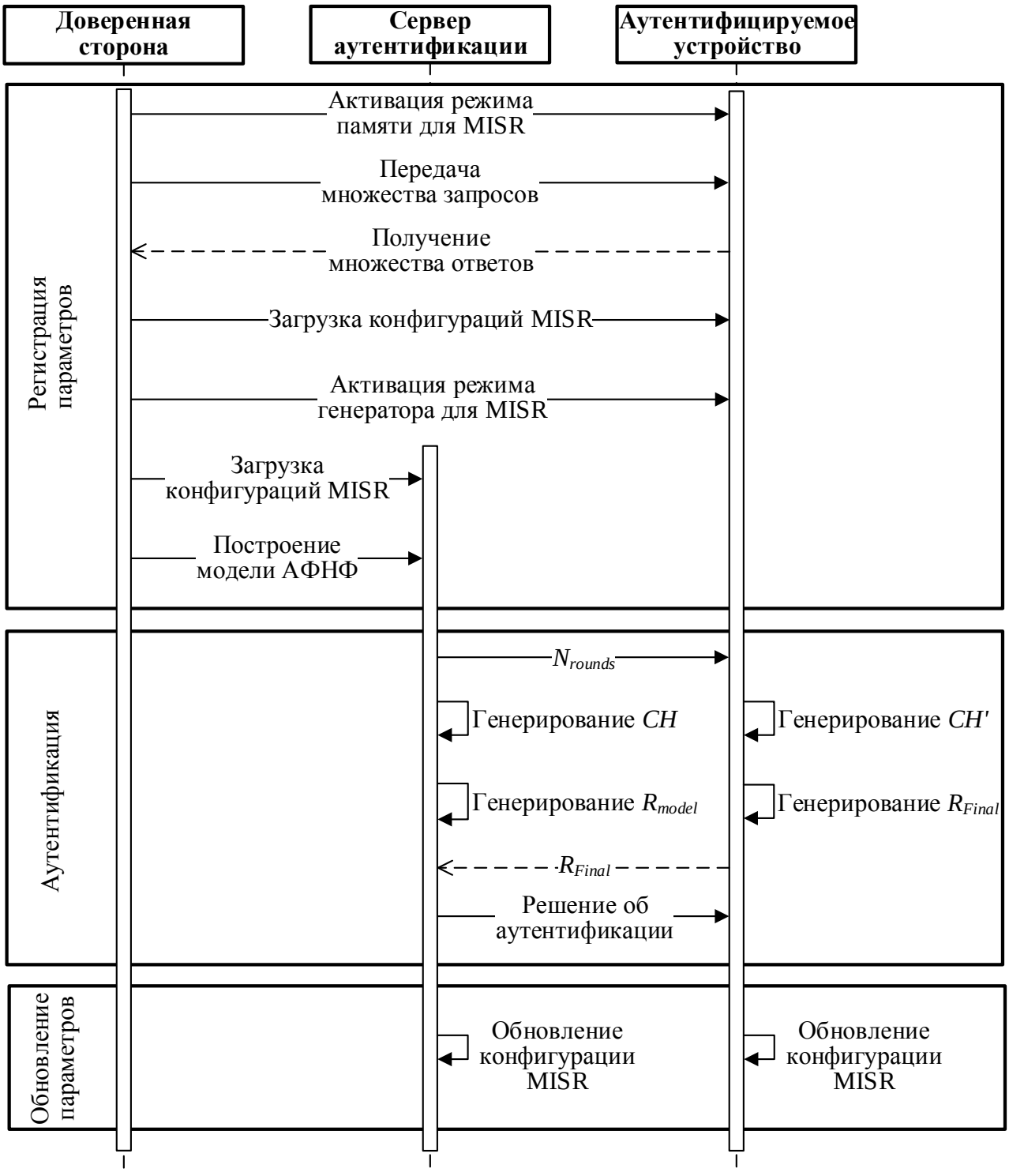


Рисунок 8. – Протокол аутентификации на основе модифицированной АФНФ

В **приложениях** приведены таблицы результатов тестирования случайных последовательностей с помощью пакета статистических тестов NIST и документы о внедрении результатов диссертационной работы. Описаны аппаратно-программные комплексы для исследования характеристик разработанных ФНФ и верификации предложенных в работе методов идентификации/аутентификации

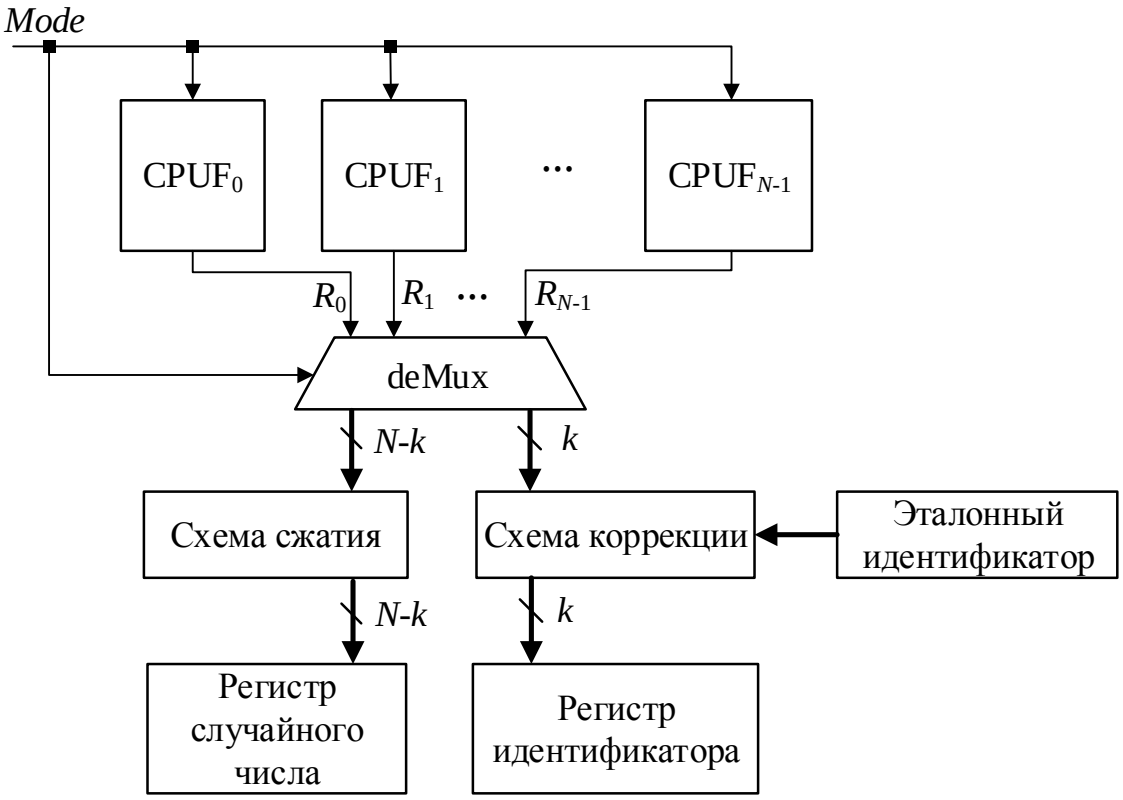


Рисунок 9. – Структурная схема ЦУ с режимами идентификации и ГСЧП

и генераторов случайных числовых последовательностей на основе ПЛИС. Обобщенная схема одного из разработанных аппаратно-программных комплексов приведена на рисунке 10.

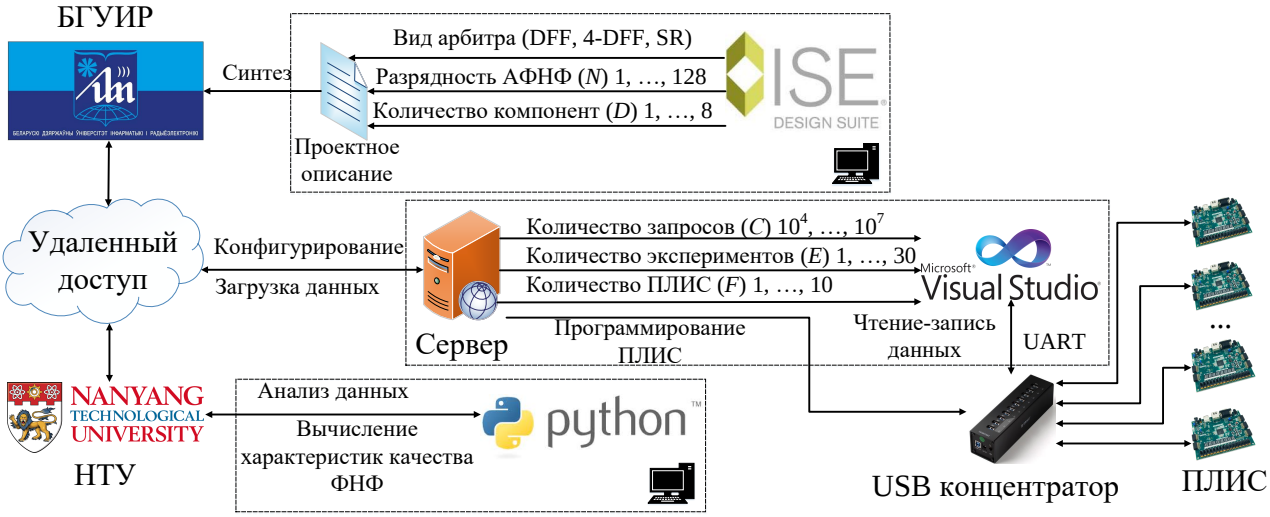


Рисунок 10. – Обобщенная схема распределенного аппаратно-программного комплекса

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Разработана методика обнаружения метастабильных состояний арбитра физически неклонируемой функции, основанная на эффекте затухающего колебания асинхронного RS-триггера, позволяющая улучшить характеристики стабильности с 0,5648 до 0,9979 и уникальности с 0,4735 до 0,4982 при незначительных аппаратурных затратах (менее 1 % на ПЛИС семейства Xilinx Artix-7 и Zynq-7000) [8, 21].

2. Предложена математическая модель представления задержки распространения сигналов для физически неклонируемой функции типа арбитр, особенностью которой является описание метастабильного состояния арбитра и позволяющая синтезировать аппаратные средства неклонируемой идентификации на программируемых логических интегральных схемах с улучшенной характеристикой стабильности до 1,0 [6, 9].

3. Разработан алгоритм классификации запросов физически неклонируемой функции типа арбитр, позволяющий генерировать уникальные идентификаторы цифровых устройств, реализуемых на программируемых логических интегральных схемах, с улучшением характеристики стабильности с 0,5648 до 1,0 в условиях изменения температуры окружающей среды и без применения дополнительных аппаратурных затрат [6, 9, 18, 19, 20].

4. Предложен метод снижения уязвимости физически неклонируемой функции типа арбитр к криптографическим атакам, основанный на применении нелинейного преобразования значений запросов, который позволяет уменьшить долю предсказанных злоумышленником ответов с 98 до 50 %, а также сократить аппаратурные затраты на 10 % в сравнении с существующими решениями [4, 5, 9, 10, 22, 23].

5. Разработан метод структурного синтеза генераторов случайных числовых последовательностей с равномерным законом распределения на основе физически неклонируемых функций, который в сравнении с существующими решениями позволяет на 40 % сократить аппаратурные затраты, а также улучшить качество вырабатываемых случайных последовательностей по характеристикам приблизительной энтропии и некоррелированности при реализации на программируемых логических интегральных схемах [1–4, 7, 11, 13–17].

6. Разработано аппаратно-программное средство на базе ПЛИС Xilinx Artix-7 и Zynq-7000 XC7Z045 FFG900 для исследования характеристик уникальности, случайности и стабильности ФНФ. Предложенное средство позволяет верифицировать несколько сотен компонент различных классов ФНФ, а также производить анализ полученных данных с использованием стандартных и модифицированных алгоритмов вычисления метрик качества [6, 9, 12, 21].

Рекомендации по практическому использованию результатов

Разработанные методы и алгоритмы использованы отечественными компаниями-проектировщиками и изготовителями цифровых устройств на базе программируемых логических интегральных схем для защиты схемотехнических реализаций от несанкционированного копирования и клонирования. Предложенные в работе методы и алгоритмы неклонируемой идентификации использованы в качестве аппаратных отпечатков пальцев цифровых устройств, реализованных на ПЛИС, с целью доказательства их подлинности. Возможным применением протокола аутентификации на основе физически неклонируемой функции типа арбитр являются цифровые устройства Интернета вещей. Данный протокол позволяет исключить несанкционированный доступ к устройствам, подключенным к сети, с небольшими аппаратурными затратами и уменьшить их уязвимость к криптографическим атакам с помощью методов машинного обучения. Генераторы случайных числовых последовательностей использованы в качестве источника криптографических ключей в протоколах шифрования, а также секретных значений параметров в алгоритмах аппаратного хеширования. Предложенные в диссертационной работе математические модели, методы, алгоритмы и схемотехнические решения разработаны и внедрены на следующих предприятиях Республики Беларусь:

1. Математическая модель представления задержки распространения сигналов для физически неклонируемой функции типа арбитр внедрена в учебный процесс специальности 1-40 01 01 «Программное обеспечение информационных технологий» БГУИР.

2. Алгоритм классификации запросов физически неклонируемой функции типа арбитр внедрен в процесс проектирования контроллеров накопителей информации на основе флеш-памяти в ООО «Софтек Флеш Солюшнс».

3. Метод снижения уязвимости физически неклонируемой функции типа арбитр к криптографическим атакам с помощью методов машинного обучения, основанный на применении нелинейного преобразования значений запросов, внедрен в процесс технического проектирования и производства опытных образцов и прототипов современной цифровой электроники в ООО «Промвад Софт».

Внедрение результатов диссертационной работы подтверждает практическое достижение поставленной цели диссертационного исследования – разработку аппаратных средств неклонируемой идентификации и аутентификации, а также генераторов случайных числовых последовательностей на программируемых логических интегральных схемах.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Главы в монографиях

1. Zalivaka, S. S. Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography / S. S. Zalivaka, L. Zhang, V. P. Klybik, A. A. Ivaniuk, C. H. Chang // Secure System Design and Trustable Computing / ed. by C.H. Chang, M. Potkonjak. — New York : Springer, 2016. — P. 39–81. **doi:10.1007/978-3-319-14971-4.**

Статьи в рецензируемых научных журналах

2. Заливако, С. С. Использование физически неклонируемых функций для генерирования действительно случайных числовых последовательностей / С. С. Заливако, А. А. Иванюк // Автоматика и вычислительная техника. — 2013. — № 3. — С. 61–72.

3. Заливако, С. С. Схемная реализация комбинированной физически неклонируемой функции для генерирования действительно случайных числовых последовательностей / С. С. Заливако, А. А. Иванюк // Доклады БГУИР. — 2013. — № 7(77). — С. 37–43.

4. Cao, Y. CMOS Image Sensor Based Physical Unclonable Function for Coherent Sensor-Level Authentication / Y. Cao, L. Zhang, S. S. Zalivaka, C. H. Chang, S. Chen // IEEE Trans. on Circ. and Syst. I: Regular Papers. — 2015. — Vol. 11, № 62. — P. 2629–2640. **doi:10.1109/TCSI.2015.2476318.**

5. Заливако, С. С. Обзор методов активной идентификации цифровых устройств / С. С. Заливако, А. А. Иванюк // Информатика. — 2016. — № 3(51). — С. 38–48.

6. Заливако, С. С. Метод увеличения стабильности физически неклонируемой функции типа «арбитр» / С. С. Заливако, А. А. Иванюк, В. П. Клыбик // Информатика. — 2017. — № 1(53). — С. 31–43.

Статьи в сборниках материалов научных конференций, включенных в системы международного цитирования (Scopus, Web of Science и IEEE Xplore digital library)

7. Cao, Y. CMOS image sensor based physical unclonable function for smart phone security applications / Y. Cao, S. S. Zalivaka, L. Zhang, C. H. Chang, S. Chen // Proc. of 2014 Int. Symp. on Int. Circ. (ISIC'2014), 10–12 Dec. — Singapore, Marina Bay Sands, 2014 — P. 392–395. **doi:10.1109/ISICIR.2014.7029496.**

8. Zalivaka, S. S. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation / S. S. Zalivaka, A. V. Puchkov, V. P. Klybik, A. A. Ivaniuk, C. H. Chang // Proc. of IEEE Asia and South Pacific Design Automation Conf. (ASP-DAC'2016), 26–28 Jan. — Macau, China — P. 533–538. **doi:10.1109/ASPDAC.2016.7428066.**

9. Zalivaka, S. S. FPGA implementation of modeling attack resistant arbiter PUF with enhanced reliability / S. S. Zalivaka, A. A. Ivaniuk, C. H. Chang // Proc. of IEEE Int. Symp. on Quality Electr. Design (ISQED'2017), 13–15 Mar. — Santa Clara, CA, USA — P. 313–318. **doi:10.1109/ISQED.2017.7918334.**

10. Zalivaka, S. S. Low-cost Fortification of Arbiter PUF Against Modeling Attack / S. S. Zalivaka, A. A. Ivaniuk, C. H. Chang // Proc. of IEEE Int. Symp. on Int. Circ. and Syst. (ISCAS'2017), 28–31 May — Baltimore, MD, USA — P. 1600–1603. **doi:10.1109/ISCAS.2017.8050671.**

Статьи в сборниках материалов научных конференций

11. Заливако, С. С. Использование физически неклонируемых функций в качестве источника энтропии для генерирования случайных чисел / С. С. Заливако, А. А. Иванюк // НИРС 2013: сб. научных работ студентов Республики Беларусь / редкол.: А. И. Жук [и др.]. — Минск : Изд. центр БГУ, 2014 — С. 127–131.

12. Заливако, С. С. Водяные знаки во встроенных средствах самотестирования с ключами, генерируемыми на основе физически неклонируемой функции / С. С. Заливако, В. В. Сергейчик, А. А. Иванюк // Тенденции и перспективы развития науки и образования в условиях глобализации 2015: материалы междунар. науч.-практ. интернет-конф. / редкол. : В. П. Коцур [и др.]. — Переяславль-Хмельницкий, 2015 — С. 329–332.

Тезисы докладов в сборниках материалов научных конференций

13. Заливако, С. С. Исследование вероятностных характеристик генератора действительно случайных числовых последовательностей на основе физически неклонируемых функций / С. С. Заливако, А. А. Иванюк // Информационные технологии и системы 2012 (ИТС 2012): материалы междунар. науч. конф., Минск, 24 окт. 2012 .г / редкол. : Л. Ю. Шилин [и др.]. — Минск : БГУИР, 2012. — С. 202–203.

14. Заливако, С. С. Применение кольцевых генераторов для получения действительно случайных числовых последовательностей / С. С. Заливако, А. А. Иванюк // Информационные технологии и управление: материалы 49-й научн. конф. аспир., магистр. и студентов, Минск, 6–10 мая 2013 г. — Минск : БГУИР, 2013 — С. 83.

15. Заливако, С. С. Генерирование последовательностей действительно случайных чисел с помощью физически неклонируемой функции типа арбитр / С. С. Заливако, А. А. Иванюк // Информационные технологии и системы 2013 (ИТС 2013): материалы междунар. науч. конф., Минск, 23 окт. 2013 г. / редкол. : Л. Ю. Шилин [и др.]. — Минск : БГУИР, 2013. — С. 204–205.

16. Zalivaka, S. S. Physical Unclonable Functions as Entropy Source to Build True Random Number Generator / S. S. Zalivaka, A. A. Ivaniuk // Proc. of 2-nd Belarus-Korea Forum, 19–20 Nov. — Minsk, Belarus. — P. 87–88.

17. Заливако, С. С. Использование физически неклонируемых функций для решения задачи генерирования действительно случайных чисел и идентификации / С. С. Заливако, А. А. Иванюк // Международная научно-техническая конференция, приуроченная к 50-летию МРТИ–БГУИР: материалы конф., Минск, 18–19 мар. 2014 г. : в 2 ч. / редкол. : А.А. Кураев [и др.]. — Минск : БГУИР, 2014 — С. 436–437.

18. Заливако, С. С. Обзор методов активного измерения цифровых устройств с использованием физически неклонируемых функций / С. С. Заливако, А. А. Иванюк // Компьютерные системы и сети : материалы 50-ой научн. конф. аспир., магистр. и студентов, 24 марта 2014 г. — Минск : БГУИР, 2014. — С. 73–74.

19. Заливако, С. С. Схема удаленного контроля для активного измерения цифровых устройств / С. С. Заливако, А. А. Иванюк // Информационные технологии и системы 2014 (ИТС 2014): материалы междунар. науч. конф., Минск, 29 окт. 2014 г. / редкол. : Л. Ю. Шилин [и др.]. — Минск : БГУИР, 2014. — С. 202–203.

20. Заливако, С. С. Методика замены ключа для схемы активного измерения цифровых устройств / С. С. Заливако, А. А. Иванюк // Компьютерные системы и сети : материалы 51-ой научн. конф. аспир., магистр. и студентов, 13-17 апр. 2015 г. — Минск : БГУИР, 2015. — С. 147–149.

21. Заливако, С. С. Аппаратно-программный комплекс исследования физически неклонируемых функций / С. С. Заливако, А. А. Иванюк, В. П. Клыбик, А. В. Пучков// Информационные технологии и системы 2015 (ИТС 2015): материалы междунар. науч. конф. 28 окт. 2015 г. / редкол. : Л. Ю. Шилин [и др.]. — Минск : БГУИР, 2015. — С. 174–175.

22. Заливако, С. С. Исследование уязвимости ФНФ типа арбитр к криптографическим атакам с использованием машинного обучения / С. С. Заливако, А. А. Иванюк // Информационные технологии и системы 2016 (ИТС 2016): материалы междунар. науч. конф. 26 окт. 2016 г. / редкол. : Л. Ю. Шилин [и др.]. — Минск : БГУИР, 2016. — С. 208–209.

23. Заливако, С. С. Методика обеспечения стойкости ФНФ типа арбитр к атакам с помощью машинного обучения / С. С. Заливако, А. А. Иванюк // Информационные технологии в промышленности, логистике и социальной сфере сфере (ITI’2017): тез. докл. IX междунар. науч.-техн. конф. 23-24 мая 2017 г. — Минск : ОИПИ НАН Беларуси, 2017. — С. 58–60.

РЕЗЮМЕ

Заливако Сергей Сергеевич

СИНТЕЗ АППАРАТНЫХ СРЕДСТВ НЕКЛОНИРУЕМОЙ ИДЕНТИФИКАЦИИ И ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМАХ

Ключевые слова: физически неклонируемые функции, идентификация, аутентификация, генераторы случайных числовых последовательностей, методы обнаружения метастабильности.

Цель работы: разработка аппаратных средств неклонируемой идентификации и аутентификации, а также генераторов случайных числовых последовательностей на программируемых логических интегральных схемах.

Полученные результаты и их новизна: разработана методика обнаружения метастабильного состояния арбитра физически неклонируемой функции, основанная на эффекте затухающего колебания асинхронного RS-триггера; предложено оригинальное решение задачи генерирования неклонируемых идентификаторов цифровых устройств, реализуемых на ПЛИС, с учетом особенностей задержки распространения сигналов для физически неклонируемой функции типа арбитр; предложен новый алгоритм классификации запросов физически неклонируемой функции типа арбитр; разработан новый метод снижения уязвимости физически неклонируемой функции типа арбитр к криптографическим атакам с помощью машинного обучения, основанный на применении нелинейного преобразования значений запросов; предложен новый метод структурного синтеза генераторов случайных числовых последовательностей с равномерным законом распределения на основе физически неклонируемых функций, ориентированный на реализацию на программируемых логических интегральных схемах.

Рекомендации по использованию и область применения: разработанные схемотехнические решения, методы и алгоритмы использованы отечественными компаниями-проектировщиками и изготовителями цифровых устройств на базе программируемых логических интегральных схем для защиты схемотехнических реализаций от несанкционированного копирования и клонирования. Результаты внедрены в учебный процесс специальности 1-40 01 01 «Программное обеспечение информационных технологий» БГУИР, в процесс проектирования контроллеров накопителей информации на основе флеш-памяти в ООО «Софтек Флеш Солюшнс», а также в процесс проектирования и производства опытных образцов и прототипов современной цифровой электроники в ООО «Промвад Софт».

РЭЗЮМЭ

Залівака Сяргей Сяргеевіч

СІНТЭЗ АПАРАТНЫХ СРОДКАЎ НЕКЛАНІРУЕМАЙ ІДЭНТЫФІКАЦЫІ І ГЕНЕРАТАРАЎ ВЫПАДКОВЫХ ЛІКАВЫХ ПАСЛЯДОЎНАСЦЕЙ НА ПРАГРАМУЕМЫХ ЛАГІЧНЫХ ІНТЭГРАЛЬНЫХ СХЕМАХ

Ключавыя словы: фізічна некланіруемыя функцыі, ідэнтыфікацыя, аўтэнтыфікацыя, генератары выпадковых лікавых паслядоўнасцей, метады выяўлення метастабільнасці.

Мэта работы: распрацоўка апаратных сродкаў некланіруемай ідэнтыфікацыі і аўтэнтыфікацыі, а таксама генератараў выпадковых лікавых паслядоўнасцей на праграмуемых інтэгральных схемах.

Атрыманыя вынікі і іх навізна: распрацавана методыка выяўлення метастабільнага стану арбітра фізічна некланіруемай функцыі, заснаваная на эфекце загасальнага вагання асінхроннага RS-трыгера; прапанавана арыгінальнае рашэнне задачы генерыравання некланіруемых ідэнтыфікатараў лічбавых прылад, рэалізуемых на ПЛІС, з улікам асаблівасцей затрымкі распаўсюджання сігналаў фізічна некланіруемай функцыі тыпу арбітр; прапанаваны новы алгарытм класіфікацыі запытаў фізічна некланіруемай функцыі тыпу арбітр; распрацаваны новы метад зніжэння ўразлівасці фізічна некланіруемай функцыі тыпу арбітр да крыптаграфічных атак з дапамогай машыннага навучання, заснаваны на выкарыстанні нелінейных пераўтварэнняў значэнняў запытаў; прапанаваны новы метад структурнага сінтэзу генератараў выпадковых лікавых паслядоўнасцей з раўнамерным законам размеркавання на аснове фізічна некланіруемых функцый, арыентаваны на рэалізацыю на праграмуемых лагічных інтэгральных схемах.

Рэкамендацыі па выкарыстанні і галіна прымянення: распрацаваныя метады і алгарытмы выкарыстаны айчыннымі кампаніямі-праекціроўшчыкамі і вытворцамі лічбавых прылад на базе праграмуемых лагічных інтэгральных схем для абароны схематэхнічных рэалізацый ад несанкцыянаванага капіравання і кланіравання. Вынікі былі ўкаранёны ў вучэбны працэс спецыяльнасці 1-40 01 01 «Праграмнае забеспячэнне інфармацыйных тэхналогій» БДУІР, у працэс праектавання кантролераў назапашвальнікаў інфармацыі на аснове флэш-памяці ў ТАА «Сафтэк Флэш Салюшнс», а таксама ў працэс праектавання і вытворчасці вопытных узораў і прататыпаў сучаснай лічбавай электронікі ў ТАА «Прамвад Софт».

SUMMARY

Zalivaka Siarhei Siarheevich

SYNTHESIS OF HARDWARE FOR UNCLONABLE IDENTIFICATION AND RANDOM NUMBER SEQUENCE GENERATORS ON COMPLEX PROGRAMMABLE LOGIC DEVICES

Key words: physical unclonable functions, authentication, true random number generators, metastability detection methods.

Purpose of this work: development of unclonable identification and authentication hardware and random number sequence generators based on complex programmable logic devices.

Obtained results and their novelty: a metastability state detection technique for arbiter physical unclonable function based on dumped oscillation effect of RS-latch is developed; an original solution of unclonable identifiers generation task for digital devices implemented in CPLD is proposed, the solution is based on signals propagation delay specifics; a new challenge classification algorithm for arbiter physical unclonable function is proposed; a method of decreasing vulnerability of arbiter physical unclonable function to cryptographic machine learning attacks is developed, the method is based on nonlinear challenge value transformation; a new method for structural synthesis of uniform distribution random number sequences generators based on arbiter physical unclonable function CPLD implementation.

Recommendations for utilization and area of application: developed methods and algorithms have been used by domestic companies, which are specializing in field-programmable gate array based digital devices to prevent unauthorized copying and cloning of their circuit implementation. The results of this work have been implemented into a lecture course for 1-40 01 01 specialization entitled “Software for information technologies”, to design process of flash memory based storage devices at “Softeq Flash Solutions” LLC and to design and manufacturing process of modern digital electronics prototypes at “Promwad Soft” LLC.

Научное издание

Заливако Сергей Сергеевич

СИНТЕЗ АППАРАТНЫХ СРЕДСТВ НЕКЛОНИРУЕМОЙ ИДЕНТИФИКАЦИИ И ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМАХ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.05 – Элементы и устройства вычислительной техники и систем управления

Подписано в печать 30.08.2018. Формат 60×84 1/16 Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 1,63. Учетн. изд. л. 1,4. Тираж 60 экз. Заказ 282.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/238 от 24.03.2014,
№ 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
ЛП № 02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6