Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

УДК

Сечко
Павел Анатольевич

МЕТОДЫ И СРЕДСТВА ИДЕНТИФИКАЦИИ ЦИФРОВЫХ УСТРОЙСТВ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-59 81 01
«Управление безопасностью производственных процессов»

Магистрант П.А. Сечко

Научный руководитель
А.А. Иванюк, профессор, доктор технических наук, доцент

Заведующий кафедрой ИПиЭ
К.Д. Яшин, кандидат технических наук, доцент

Нормоконтролер
О.В. Павловская,
ассистент, магистр психологических наук

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Идентификация цифровых устройств решает вопросы защиты программно-аппаратных решений, разработанных на базе этих цифровых устройств, от клонирования (несанкционированного повторения и использования) или внедрения аппаратных троянов, изменяющих функционирование, нарушающих или снижающих работоспособность или передающих секретную информацию из устройства. Также возможно определение легальности компонент сложной системы для защиты от несанкционированной замены компонент на аналогичные с точки зрения интерфейсов и логики взаимодействия с внешним миром, но нарушающих структуру и функционирование устройства.

Для решения задачи идентификации в проектное описание часто внедряют идентификаторы, наличие которых позволяет использовать их для адресации *FPGA* в сложных системах, в качестве ключей в системах шифрования и в реализации алгоритмов защиты от несанкционированного использования. Также для усложнения нелегального копирования может использоваться лексическая обфускация описания устройства. Однако популярным вектором атаки является клонирование *bit*-образа и обратное проектирование описания устройства с целью модификации и изучения его функционирования. Таким образом, необходимо решение, идентифицирующее устройство, но не привязанное к значениям, задаваемым при производстве.

Таким решением могут являться физически неклонируемые функции (*PUFs*, *physically unclonable functions*).

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование существующих методов защиты интеллектуальной собственности, коей являются в том числе и цифровые устройства, а также методов их идентификации.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- Проанализировать существующие методы защиты и идентификации цифровых устройств;
- Рассмотреть возможность идентификации цифровых устройств при помощи физически неклонируемых функций;
- Получить и описать статистические данные с модели цифрового устройства и с реального цифрового устройства.

Объектом исследования являются методы идентификации цифровых устройств.

Предметом исследования является использование конфигурируемого кольцевого генератора (*RO*, *ring oscillator*) в качестве схемной реализации физически неклонируемой функции (*PUF*, *physically unclonable function*).

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

В связи с быстрым развитием отрасли информационных технологий, популярностью интернета вещей и ростом количества выпускаемых электронных устройств, появляется необходимость в защите и идентификации данных устройств от нелегального клонирования и модификации.

Методика идентификации может быть основана на непредсказуемых и невоспроизводимых отклонениях в физической структуре кристалла, на котором реализовано цифровое устройство. В результате появляется возможность как однозначной идентификации цифрового устройства и защиты его от клонирования и модификации, так и использования данных аспектов в

качестве основы для реализации систем шифрования. Важным пунктом является неуправляемость перечисленных выше отклонений относительно действий разработчика.

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя А. А. Иванюка заключается в формулировке целей и задач исследования, помощи в выборе направления и методологии исследования, советах по выбору научных источников для изучения.

Опубликованность результатов диссертации

Результаты работы были представлены на Международной научной конференции «Информационные технологии и системы» в виде публикации «Использование конфигурируемых кольцевых генераторов для идентификации цифровых устройств программируемой логики» в секции «Проектирование встраиваемых систем».

Научные исследования были проведены в рамках научно-исследовательской работы кафедры информатики БГУИР "Разработка принципов построения интеллектуальных систем автоматизации моделирования структурно сложных объектов".

Структура и объем диссертации

Диссертация состоит из общей характеристики работы, введения, двух глав, заключения и библиографического списка.

В первой главе представлен анализ предметной области – методов и средств идентификации цифровых устройств. Рассмотрена краткая история развития и роста рынка устройств программируемой логики, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения.

Вторая глава посвящена использованию конфигурируемого кольцевого генератора импульсов в качестве схемной реализации физически

неклонируемой функции для идентификации устройств программируемой логики. Подробно рассмотрены аспекты выбора метода идентификации и сложности, связанные с разработкой компоненты-объекта интеллектуальной собственности и применения её на железе.

Общий объем работы составляет 64 страницы, из которых основного текста – 46 страниц, 41 рисунок на 14 страницах, девяти таблиц на четырёх страницах и списка использованных источников из 30 наименований на трёх страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В диссертации исследуются методы и средства идентификации цифровых устройств. Рассматриваются практические варианты идентификации, а также исследуются существующие методы и проблемы внедрения идентификаторов в описание устройства.

Автор начинает диссертацию с рассмотрения краткой истории развития цифровых устройств с упором на развитие устройств на базе программируемой логики, рассматривает основные векторы атак на цифровую технику и методы защиты от этих атак. Приводятся доводы в пользу использования решений на базе физически неклонируемых функций.

Во второй главе автор рассматривает практический пример идентификации устройств при помощи конфигурируемого кольцевого генератора импульсов как схемной реализации физически неклонируемой функции. Подробно описываются основные этапы проектирования генератора, а также подсчёта его выходных импульсов. Рассматриваются отличия генерируемых импульсов в зависимости от геометрической расположенности генератора на кристалле.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Были рассмотрены и проанализированы основные способы атак на цифровые устройства и способы защиты от них. Способ идентификации при помощи конфигурируемых кольцевых генераторов как схемной реализации физически неклонируемой функции был выбран для подробного исследования как оптимальный благодаря малому количеству недостатков (реализованный компонент занимает мало места на кристалле) и благодаря возможности однозначно идентифицировать устройство с его помощью. Данный способ идентификации также может применяться в системах шифрования и в реализации алгоритмов защиты от несанкционированного использования

2. Был получен опыт использования компонент интегрированной среды разработки *Xilinx ISE*, а также получен практический навык работы с моделью *FPGA Artix*-7.

3. Результаты диссертации были опубликованы на Международной научной конференции «Информационные технологии и системы» в виде публикации «Использование конфигурируемых кольцевых генераторов для идентификации цифровых устройств программируемой логики» в секции «Проектирование встраиваемых систем», а также на 51 и 52 СНТК студентов, магистрантов, аспирантов БГУИР в 2015 и 2016 годах соответственно.

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют теоретическую и практическую базу для разработки *IP*-компонент для идентификации цифровых устройств. Они могут быть использованы при разработке новых и совершенствовании существующих решений в данной области.

2. Результаты работы могут использоваться в университете при подготовке специалистов в области защиты интеллектуальной собственности.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Сечко П.А., Иванюк А.А. Использование конфигурируемых кольцевых генераторов для идентификации цифровых устройств программируемой логики // Информационные технологии и системы ИТС-2016: материалы международной научной конференции / редкол.: Л.Ю. Шилин [и др.]. - Минск: БГУИР, 2016. - 340 с. ISBN 978-985-543-271-6. - С. 212-213.