Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 681.324

КАРБОВСКИЙ
Дмитрий Викторович

РЕАЛИЗАЦИЯ НЕКЛОНИРУЕМОЙ АППАРАТНОЙ ИДЕНТИФИКАЦИИ СОФТ-ПРОЦЕССОРОВ ДЛЯ FPGA

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 1-40 80 01 – Компьютерная инженерия

Научный
руководитель
Иванюк А.А.
д.т.н., профессор
кафедры информатики

Минск 2023

Работа выполнена на кафедре электронных вычислительных средств учреждения образования “Белорусский государственный университет информатики и радиоэлектроники”

Научный руководитель: **ИВАНЮК Александр Александрович**, доктор технических наук, профессор кафедры информатики учреждения образования “Белорусский государственный университет информатики и радиоэлектроники”

Рецензент: **СТРОГОВА Александра Сергеевна**, заместитель начальника главного управления науки-начальник отдела организации и сопровождения инновационной деятельности Белорусского государственного университета.

Защита диссертации состоится 27 апреля 2023 года в 12:00 часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования “Белорусский государственный университет информатики и радиоэлектроники” по адресу 220013, Минск, ул. П. Бровки, 6, корп. 1, ауд 311б, тел. 293-89-46, E-mail: kafevs@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования “Белорусский государственный университет информатики и радиоэлектроники”.

ВВЕДЕНИЕ

В современном мире цифровые устройства проникли во все области жизни человека. Невозможно представить область быта, которая бы не изменилась по причине распространения компьютеров и цифровых технологий.

Каждое цифровое устройство имеет микропроцессор, который занимается обработкой данных. Современные микропроцессоры имеют полупроводниковых кристалл с электронными компонентами на нём. Множество моделей и архитектур были разработаны для различных задач. Данная отрасль является крайне востребованной и прибыльной, однако, многие задачи в ней по-прежнему остаются сложными. К примеру, проектирование структуры микропроцессора занимает длительное время на разработку и верификацию, а тестирование физического образца подразумевает изменения в процессе производства полупроводниковых кристаллов.

Большинство процессоров относится к категории ASIC − Application-Specific Integrated Circuit (микросхема специального назначения). Это означает, что архитектура вычислительного устройства была разработана для решения конкретной задачи. Создание другой архитектуры или исправление ошибок в существующей требует затратов ресурсов (человеческих, временных, физических).

Многие современные процессоры содержат внутреннюю конфигурацию, также называемую микрокодом. Эта конфигурация является управляющим кодом, влияющим на логику работы устройства. Этот подход позволяет исправлять некоторые ошибки проектирования, заменяя конфигурацию микропроцессора. Такое решение не всегда является тривиальным, но позволяет решать многие серьёзные проблемы в архитектуре.

В то время, как процессоры специального назначения имеют некоторые возможности для реконфигурации, но фиксированную архитектуру, параллельно с этим появился новый класс устройств, называемый FPGA − Field-Programmable Gate Array (программируемая матрица). Кристалл такого устройства содержит набор базовых элементов логики, памяти и элементы соединения. Выбор путей, соединяющих элементы, а также поведение компонентов настраиваются конфигурацией FPGA. Поток конфигурации − ключевой элемент в работе кристалла, поступает из внешнего источника при включении устройства.

FPGA играет важную роль в прототипировании, тестировании и верификации цифровых устройств. Вычислительные способности кристаллов FPGA уступают кристаллам ASIC, но на стадии прототипирования это не главный критерий. Кроме того, использование FPGA позволяет менять поведение устройства во время его работы. Это бесценное свойство для удалённой коррекции работы устройств и систем, устранения неисправности и создания систем с высоким показателем надёжности. Процессорная система, реализованная на кристалле FPGA, также называется софт-процессор. Она представляет собой виртуальный процессор, отличающийся топологически, но логически реализующий описание процессора.

Производство полупроводников и выпуск вычислительных устройств связаны с определёнными рисками. Одна из возможных причин убытков − копирование дизайна конкурентами. Анализ современных микропроцессоров типа ASIC является сложной задачей; к тому же, были разработаны техники обфускации (запутывания) и скрытия структуры кристалла. FPGA, напротив, анализировать не нужно: для копирования устройства достаточно получить аналогичный кристалл и подать на него конфигурацию с оригинального. В случае, если используемый кристалл доступен для приобретения на рынке, конфигурация кристалла нуждается в защите.

Защита от нелегального копирования может быть реализована множеством способов. Файл конфигурации может быть зашифрован, описание логики может реализовывать верификацию достоверности устройства. Эти направления требуют дополнительного исследования и представляют актуальные задачи для современных исследований в защите устройств и применении физической криптографии. В рамках данной работы рассматриваются возможности цифровых устройств для уникальной самоидентификации.

ОБЩАЯ ХАРАКТЕРИСТИКА

Цели и задачи исследования

Цель данной работы − провести анализ существующих проблем в области проектирования полупроводниковых устройств, в частности − устройств на базе FPGA, а также возможностей их нелегального копирования. На основе этого рассмотреть специфику использования FPGA-кристаллов для реализации софт-процессоров и разработать методы защиты от клонирования устройств.

Для этого необходимо выполнить следующие задачи:

– проанализировать причины угрозы нелегального копирования конфигурации устройств;
– углубиться в методы физической криптографии;
– ознакомиться с существующими методами защиты устройств;
– реализовать механизм защиты от копирования;
– провести эксперименты:
  a) с различными реализациями физически неклонируемых функций;
  b) с устройствами с разными параметрами;
– повторить эксперименты на различных устройствах;
– собрать тестовые данные;
– рассчитать значения метрик;
– сделать выводы;
– предложить направления дальнейших исследований, улучшений и применений.

Объектом исследования являются физически неклонируемые функций, реализованные на кристалле FPGA.

Предметом исследования выступают методы их реализации и значения их метрик.

Гипотеза данного исследования − использование физически неклонируемых функций в устройстве на базе FPGA позволяет надёжно защищать его от нелегального распространения благодаря уникальной идентификации кристалла и его конфигурации.

Опубликованность результатов диссертации

Результаты некоторых экспериментов, выполненных в рамках данного исследования, были опубликованы на 59-ой научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники». В рамках защиты представленных тезисов был обобщён полученный опыт и сделаны выводы о результатах исследования.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и приложения. В первой главе представлен анализ предметной области, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения.

В первой главе данной пояснительной записки описываются методы и задачи физической криптографии, даётся определение физически неклонируемой функции и также перечисляются их роли в области полупроводниковых устройств. Во второй главе описываются выбранные инструменты и структура экспериментальной установки, перечисляются использованные аппаратное и программное обеспечение. Третья глава приводит результаты экспериментов и описывают их условия. В четвёртой главе описывается анализ полученных экспериментальных данных, приводятся рассчитанные значения метрик, строятся выводы относительно первоначальной теории и предлагаются дальнейшие направления исследований и улучшений результатов.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении описаны категории микропроцессоров, описаны причины использования FPGA-кристаллов в качестве базы для устройств, рассмотрена роль FPGA, приведены причины потребности в защите от нелегального копирования.

В общей характеристике определяются цели данной работы, поставленные задачи, выбираются объект и субъект исследования, предлагается гипотеза исследования.

В первой главе приводится определение физической криптографии, перечисляются её особенности, а также свойства физически неклонируемых

функций и их применения, даются определения физическим функциям типа арбитр, типа кольцевой осциллятор и ФНФ на базе бистабильного элемента.

Во второй главе описывается процесс разработки устройств на базе FPGA, а также выбираются аппаратное и программное обеспечения, описывается процесс разработки проекта и выбор и выбор используемых физически неклонируемых функций и предпочтительных свойств, приведена схема компонентов в проекте.

В третьей главе описываются проводимые эксперименты, делаются предварительные выводы и описывается дальнейшее направление исследования с учётом первых результатов, приводятся результаты экспериментов, значения метрик полученных ФНФ и дополнительные свойства реализованных функций.

В четвёртой главе подведены итоги исследования, сделаны выводы из полученных результатов, а также предложены методы улучшения значений метрик и векторы для новых исследований.

ЗАКЛЮЧЕНИЕ

В ходе работы над магистерской диссертацией была изучена предметная область, составлена гипотеза и выбраны используемые инструменты и оборудование. Был получен опыт работы с FPGA-устройствами и с САПР Vivado. Была изучена литература в исследуемой области, велось обсуждение со специалистами, занимающихся физической криптографией и проектированием аппаратуры.

В процессе исследования возникали и решались технические проблемы. Было решено отказаться от исследования свойств ненадёжных физически неклонируемых функций, таких как кольцевой осциллятор. В процессе исследования ФНФ на базе бистабильного элемента также была определена ненадёжной и неприменимой в чистом виде в устройствах на базе FPGA.

При работе над диссертацией производились сбор информации и обсуждение со специалистами в данной области, что приводило к корректировке направления исследования.

При проведении экспериментов уделялось внимание качеству и точности получаемых данных, сомнительные результаты перепроверялись, а неточности исправлялись. Уделялось внимание возможности повторения эксперимента, а также дальнейшему развитию теории и возможности применения данных на практике.

Результаты исследования могут быть применены при проектировании уникальной идентификации, а также самоидентификации цифровых устройств на базе FPGA. Кроме того, значения полученных метрик могут быть улучшены различными способами.

Данная работа имеет потенциал в дальнейших исследований, а результаты данного исследования могут послужить основной для последующих экспериментов в данной области. Полученный опыт может быть перенесён в другие условия и в другие области применения физической криптографии.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1] Карбовский, Д. В. Применение физической криптографии в устройствах на базе FPGA / Д. В. Карбовский, А. А. Иванюк // Информатика : материалы 59-й научной конференции аспирантов, магистрантов и студентов, Минск, 17 – 21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023.

РЕЗЮМЕ

Карбовский Дмитрий Викторович

Реализация неклонируемой аппаратной идентификации софт-процессоров для FPGA

Ключевые слова: физически неклонируемые функции, уникальная идентификация, FPGA.

Цель работы: исследование способов реализации уникальной идентификации устройств на базе FPGA для предотвращения нелегального копирования.

Полученные результаты и их новизна: проведён анализ существующих методов идентификации, проанализированы подходящие физически неклонируемые функции, предложена структура экспериментальной установки, проведены эксперименты и приведены результаты исследования; сделаны выводы об использовании физически неклонируемых методов для уникальной идентификации устройств на базе FPGA.

Область применения: физическая криптография, защита от копирования.