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

УДК 004.942

Пучков
Александр Владимирович

Методы и алгоритмы неклонируемой идентификации программируемых логических устройств

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-40 80 05 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Научный руководитель
Иванюк Александр Александрович
доктор технических наук, доцент

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

Расширяющийся мировой рынок сложных цифровых устройств и систем ставит перед их разработчиками множество новых задач, среди которых важное место занимает защита проектов цифровых устройств на языках описания аппаратуры и уже реализованных устройств от несанкционированных действий человека. К таким действиям можно отнести обратное проектирование, модификацию, передачу либо использование проектных описаний, повлекшие за собой нарушение авторских прав производителя, а также многократное клонирование цифровой системы в обход соглашений с производителем.

В этой связи необходимым является обеспечение надежной идентификации каждого экземпляра устройства. При этом каждое устройство после производства имеет доступный только для чтения идентификатор, наличие которого позволяет эффективно решать целый ряд задач. Помимо реализации методов и алгоритмов защиты от несанкционированного использования идентификатор может быть применен, например, для адресации устройств, подключенных к единой информационной магистрали, или в качестве открытого ключа при реализации алгоритмов шифрования.

Перспективным в данном случае является использование методов физической криптографии, которая основана на структурной сложности электронных систем. Цифровые системы, как правило, состоят из множества компонент, физические параметры которых на стадии производства принимают случайные значения. В процессе создания таких систем принципиально невозможно управлять величинами физических параметров их компонент. Таким образом, наличие подобных случайных параметров делает каждую цифровую систему уникальной и физически неклонируемой. Идея извлечения уникальных параметров из цифровых систем лежит в основе так называемых физически неклонируемых функций (ФНФ) – ключевого понятия физической криптографии.

Диссертационная работа посвящена исследованию существующих решений на основе ФНФ, методике оценки их качества, в частности, их основных характеристик, таких как уникальность, случайность и стабильность, имеющих существенное значение для приложений уникальной неклонируемой идентификации цифровых устройств и систем. Предлагаются новые схемотехнические и алгоритмические решения, позволяющие повысить качество уникальной неклонируемой идентификации, что отражается в результатах проведенного экспериментального исследования на разработанном специализированном программно-аппаратном комплексе. Полученные результаты могут быть внедрены в процесс разработки цифровых устройств и систем, а также в специализированные системы автоматизированного проектирования.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью диссертационной работы является реализация методов стабильной неклонируемой идентификации цифровых устройств и систем, реализованных на программируемых логических интегральных схемах (ПЛИС), с использованием различных вариантов физически неклонируемых функций (ФНФ) типа арбитр.

Для достижения поставленной цели необходимо решить следующие задачи:

1) анализ существующих схемотехнических решений реализации физически неклонируемых функций для программируемых логических интегральных схем (ПЛИС);

2) анализ существующих и разработка новых количественных характеристик для оценки ФНФ;

3) разработка новых схемотехнических и алгоритмических решений для реализации ФНФ с улучшенными характеристиками.

Объектом исследования являются программируемые логические интегральные схемы.

Предметом исследования являются методы и средства программно-аппаратной идентификации цифровых устройств, реализованных на ПЛИС.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность реализации алгоритмических и схемотехнических средств, позволяющих ресурсами самого устройства детектировать метастабильные состояния элементов памяти, входящих в состав различных вариантов реализации ФНФ типа арбитр. Детектирование метастабильных состояний позволит разработать методы стабилизации ответов ФНФ, что повысит их качество для приложений уникальной неклонируемой идентификации.

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

Работа выполнялась в соответствии с научно-техническими заданиями и планами работ кафедры «Программное обеспечение информационных технологий» БГУИР:

«Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обу-

чающие комплексы» (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя А. А. Иванюка, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на международной научной конференции «Информационные технологии и системы» (Минск, Беларусь, 2015); международной научной конференции «21st Asia and South Pacific Design Automation Conference» (Macao, China, 2016); 52-й научно-технической конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2015).

Опубликованность результатов диссертации

По теме диссертации опубликовано 5 печатных работ, из них 5 работ в сборниках трудов и материалов конференций, в том числе международных.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, списка публикаций автора и приложений. В первой главе представлен анализ предметной области, рассмотрены существующие решения в рамках тематики исследования и выявлены их основные проблемы. Вторая глава посвящена разработке новых методов стабилизации ответов ФНФ, а также новой методике оценки качества ФНФ. В третьей главе рассмотрены этапы проектирования и реализации программно-аппаратного комплекса экспериментального исследования физически неклонируемых функций. В четвертой главе предложена методика использования разработанного комплекса, а также представлены результаты экспериментальных исследований, подтверждающие выдвинутую гипотезу.

Общий объем работы составляет 84 страницы, из которых основного текста – 55 страниц, 22 рисунка на 20 страницах, 4 таблицы на 4 страницах, список

использованных источников из 33 наименований на 3 страницах и 2 приложения на 19 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **первой главе** представлен анализ проблемы уникальной неклонируемой идентификации и аутентификации применительно к цифровым устройствам и системам. Рассмотрены существующие решения и отмечены их недостатки.

Проведен обзор основных положений физической криптографии и физически неклонируемых функций, даны соответствующие определения и введен понятийный аппарат. Рассмотрены классические архитектуры ФНФ, являвшиеся объектом исследования первых работ по данной тематике, а также комбинированные ФНФ, представляющие попытку их усовершенствования.

Проанализированы основные существующие подходы к оценке качества ФНФ.

Вторая глава посвящена разработке новых решений, призванных улучшить качество ответов ФНФ. К ним относятся новые реализации ФНФ, являющиеся усовершенствованием классической ФНФ типа арбитр. Улучшение заключается в замене арбитра, представленного в исходном варианте синхронным D-триггером на другие схемы, позволяющие детектировать метастабильные ответы.

Представлена новая методика оценки качества ответов ФНФ, а именно таких ее важнейших характеристик как уникальность, случайность, стабильность. Предложено использование метрики Сокала-Михенера в качестве меры различия между двумя двоичными векторами, а также, в обобщенном виде, для меры различия между тернарными векторами, отображающими также нестабильные ответы (формула (1), таблица 1). Показаны преимущества статистических тестов, в частности, тестов NIST, для оценки случайности генерируемой последовательности ответов.

$$D_{Sokal-Michener}(v_1, v_2) = \frac{2 \cdot (b + c) + f + g + h + i}{2m}. \qquad (1)$$

Таблица 1 – Различные комбинации тернарных значений для вычисления расстояния Сокала-Михенера

Переменная	$v_1(i)v_2(i)$
a	11
b	01
c	10
d	00
e	XX
f	$0X$
g	$X0$
h	$1X$
i	$X1$

В **третьей главе** рассмотрены этапы проектирования программно-аппаратного комплекса экспериментального исследования ФНФ. Аппаратной платформой комплекса являются ПЛИС типа FPGA Xilinx Artix-7, на которых реализуются проектные HDL-описания соответствующих ФНФ, а также софт-процессор MicroBlaze и интерфейсные контроллеры Fast Ethernet и UART, предназначенные для управления ФНФ и обмена данными между ПЛИС и рабочей станцией. Обмен данными происходит по высокопроизводительному сетевому интерфейсу Fast Ethernet (100 Мбит/с).

Рассмотрены преимущества используемых решений на основе ПЛИС, IP-компонент софт-процессора MicroBlaze и интерфейсных контроллеров, обозначено текущее состояние разработки и перспективы ее усовершенствования.

В **четвертой главе** предложена методика использования разработанного комплекса, а также представлены результаты экспериментальных исследований, полученные с его помощью. Экспериментальные данные были обработаны, получены значения метрик, характеризующих качество новых реализаций ФНФ. Были применены тесты NIST, позволившие оценить случайность получаемых от ФНФ ответов. Оценены аппаратурные затраты на реализацию новых видов ФНФ и проведен их сравнительный анализ. Полученные результаты свидетельствуют об улучшении качества предложенных решений в сравнении с известными аналогами.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложены метрики и подходы, позволяющие оценивать качество ответов ФНФ с точки зрения уникальность, случайности и стабильности. Подобный математический аппарат важен, поскольку позволяет оценить качественное улучшение новых реализаций ФНФ в сравнении с существующими, а также может применяться для сравнения различных типов ФНФ.

2. Предложены новые схемотехнические реализации ФНФ с расширенной шиной ответа, позволяющие прямо или косвенно детектировать некоторые переходные процессы, свойственные многим реализациям ФНФ, что положительно сказывается на их характеристиках, поскольку в алфавит выходных ответов включаются заведомо нестабильные ответы.

3. Разработан программно-аппаратный комплекс экспериментального исследования ФНФ на базе ПЛИС типа FPGA Xilinx Artix-7, позволяющий осуществлять взаимодействие реализованных на ПЛИС экземпляров ФНФ и рабочей станции по высокоскоростному сетевому протоколу Fast Ethernet (100 Мбит/с). Для разработанного комплекса были реализованы HDL-описания новых видов ФНФ с целью их исследования.

4. На основании обработки полученных экспериментально данных с применением разработанных метрик, а также пакета статистических тестов NIST, было показано качественное превосходство новых видов ФНФ над существующими решениями, показав близкие к идеальным значения стабильности (0,9985) и уникальности (0,4959). При этом были пройдены тесты NIST, что позволяет говорить о последовательности ответов ФНФ как об истинно случайной.

5. Выработаны алгоритмические рекомендации по типу и последовательности подаваемых на ФНФ запросов, позволяющие повысить качество идентификации и устойчивость ФНФ к атакам машинного обучения.

6. Результаты исследования были представлены на научных конференциях в РБ, а также на международной конференции «21st Asia and South Pacific Design Automation Conference». Работа по теме исследования приняла участие в XXII Республиканском конкурсе научных работ студентов, где получила 2 категорию.

7. Результаты исследования были внедрены в учебный процесс в 2015-2016 учебном году на кафедре ПОИТ в качестве материалов лекционного курса «Программное обеспечение цифрового проектирования» для студентов 5-го

курса специальности 40 01 01 «Программное обеспечение информационных технологий».

Рекомендации по практическому использованию результатов

1. Предложенные метрики качества ФНФ могут быть использованы для сравнительной оценки различных типов и реализаций ФНФ, в частности, для приложений уникальной неклонируемой идентификации.

2. Новые типы ФНФ могут быть использованы разработчиками цифровых устройств и систем для решения задачи уникальной неклонируемой идентификации либо более сложной задачи аутентификации. В том числе возможно автоматизированное внедрение рассматриваемых компонент ФНФ в проектные описания цифровых устройств и систем.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Пучков, А.В. Программно-аппаратное средство исследования свойств физически неклонируемых функций / А.В. Пучков // Компьютерные системы и сети: материалы 51-ой научной конференции аспирантов, магистрантов и студентов, Минск, 13-17 апреля 2015 г. / Белорус. гос. ун-т информатики и радиоэлектроники. ; редкол.: В.А. Прытков (гл. ред.) [и др.]. – Минск, 2015. – С. 89-91.

2. Пучков, А.В. Экспериментальное исследование основных характеристик мультиарбитральной физически неклонируемой функции / А.В. Пучков // Компьютерные системы и сети: материалы 51-ой научной конференции аспирантов, магистрантов и студентов, Минск, 13-17 апреля 2015 г. / Белорус. гос. ун-т информатики и радиоэлектроники. ; редкол.: В.А. Прытков (гл. ред.) [и др.]. – Минск, 2015. – С. 127-128.

3. 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., БГУИР, Минск, Беларусь, 26 октября 2015 г. / редкол. : Л.Ю. Шилин [и др]. – Минск : БГУИР, 2015. – С. 172-173.

4. 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 // Special Session on Cyber-Physical Systems and Security, in Proc. 21st IEEE Asia and South Pacific Design Automation Conf. (ASP-DAC 2016), Macao, China, 26-28 Jan. 2016. – P. 533-538.

5. Пучков, А.В. Исследование физически неклонируемых функций с использованием софт-процессора MicroBlaze / А.В. Пучков // Компьютерные системы и сети: материалы 52-ой научной конференции аспирантов, магистрантов и студентов, Минск, 25-30 апреля 2015 г. / Белорус. гос. ун-т информатики и радиоэлектроники. ; редкол.: В.А. Прытков (гл. ред.) [и др.]. – Минск, 2016. – С. 89-91.