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

УДК 004.3’1:004.4

Витенко
Алексей Александрович

Методы и алгоритмы обнаружения несанкционированных изменений аппаратуры цифровых 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 А.А.
доктор т.н., доцент

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

В наше время из-за глобализации сферы производства цифровых устройств, разработчик не может полностью контролировать все этапы производства [1]. На некоторых этапах злоумышленник может внести какие-то изменения в устройство, которые могут привести к нарушению функциональности, краже данных. В некоторых областях деятельности человека, таких как: медицина, военное дело, различные системы мониторинга окружающей среды, системы предупреждения о землетрясениях и цунами, различные охранные системы и др., такие ошибки могут иметь очень большую цену. Коммерческое же устройство может быть просто скопировано, и уже дальше распространяться в качестве нелегальной копии. Что будет означать убытки разработчику цифрового устройства и, также, подвергать различным рискам пользователей данного устройства. Кроме того, в различных системах аналитики очень важно точно и надёжно идентифицировать устройство.

Исходя из этого, большое значение приобретает вопрос поиска эффективных способов обнаружения и предотвращения несанкционированной модификации или копирования устройства, методов идентификации цифровых устройств и отдельных его компонент. Одним из таких способов является использование физически неклонируемых функций. Физически неклонируемая функция — это функция, воплощенная в физической структуре, которую просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести. Физически неклонируемые функции используют неупорядоченности, вносимую внутренними или внешними факторами. Наиболее интересными для моей задачи являются физически неклонируемые функции, использующие внутреннюю неупорядоченности, а конкретнее — кремниевые PUF. Интересны они тем, что кремний является основным полупроводником, используемым в современной промышленности. Поэтому, можно с уверенностью сказать, что на каждом цифровом устройстве реально реализовать и использовать физически неклонируемую функцию.

Некоторые PUF, основанные на различных задержках при смене состояний компонентов, такие как кольцевой осциллятор, или PUF типа «арбитр» должны быть заложены на этапе проектирования компонента цифрового устройства. Другие же, такие как PUF, основанные на использовании статической или динамической памяти, не требуют специальной подготовки проекта.

В своей работе я искал способ использования физические неклонируемых функций на цифровых устройствах без модификации аппаратной составляющей, ограничиваясь только изменениями в программном обеспечении цифрового устройства и используя только те компоненты, которые могут быть включены в устройство по дизайну. Это позволит разработать метод, который может быть применён на широком перечне устройств, в том числе уже на готовых компонентах.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является разработка метода для защиты цифровых устройств от несанкционированной модификации или копирования. Разработанный метод должен обеспечивать возможность реализации защиты от модификации на широком спектре персональных вычислительных машин.

Для достижения поставленной цели необходимо решить следующие задачи:

1.Изучить существующие методы защиты цифровых устройств от несанкционированной модификации.

2.Изучить известные физически неклонируемые функции.

3.Экспериментально исследовать выбранные физически неклонируемые функции.

4.Разработать метод воздействия на выбранную физически неклонируемую функцию и считывания выходных значений, без модификации аппаратного обеспечения цифрового устройства.

5.Реализовать программный комплекс для идентификации цифровых устройств или их компонент на основе разработанного метода взаимодействия с физически неклонируемой функцией.

Объектом исследования являются физически неклонируемые функции.

Предметом исследования являются физически неклонируемые функции, применение их для идентификации цифровых устройств или их компонентов.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность использования физически неклонируемуй функции основанной на динамической памяти для идентификации цифрового устройства или некоторых его компонентов.

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

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие 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 51-й научно-технической конференции аспирантов, магистрантов и студентов БГУИР (Минск, Республика Беларусь, 2015).

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 печатные работы, из них 1 статья в рецензируемом издании, 1 работа в сборнике трудов и материалов конференции аспирантов, магистрантов и студентов БГУИР.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, шести глав, заключения, списка использованных источников, списка публикаций автора и приложений. В первой главе проведён краткий обзор литературы по теме работы. Вторая глава посвящена исследованию предметной области и поиску существующих методов и алгоритмов защиты устройств от несанкционированной модификации. В третьей главе представлены и обоснованы показатели эффективности физически неклонируемых функций. В четвертой главе экспериментально исследована физически неклонируемая функция типа «кольцевой осциллятор». В пятой главе предложена практическая реализация метода взаимодействия реализацией физически неклонируемой функции, основанной на DRAM, на реальном устройстве. В шестой главе представлены результаты экспериментов.

Общий объем работы составляет 63 страницы, из которых основного текста – 50 страниц, 31 рисунок на 10 страницах, 10 таблиц на 5 страницах, список использованных источников из 20 наименований на 2 страницах и 3 приложения на 9 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** проведен обзор использовавшейся литературы и дан подробный анализ некоторых методов для защиты цифровых устройств от несанкционированной модификации или копирования. Особое внимание уделено физически неклонируемым функциям (ФНФ). Рассматриваются два вида ФНФ:

в которых беспорядочность вносятся внешними факторами, внутренними факторами. Особый упор сделан на ФНФ, использующими внутреннюю неупорядоченность. Рассмотрены ФНФ на базе кольцевого генератора импульсов, SRAM-PUF и DRAM-PUF.

Во **второй главе** определены и обоснованы количественные и статистические критерии оценки физически неклонируемых функций. Это случайность, устойчивость, размытость и уникальность.

В **третьей главе** описан эксперимент по идентификации ПЛИС с использованием физически неклонируемой функции, базирующейся на кольцевом генераторе импульсов, и метода опорных векторов. Приведены результаты, которые подтверждают возможность использования этого типа ФНФ для идентификации устройств.

В **четвертой главе** разрабатывается метод для использования DRAM-PUF на компьютерах общего назначения. Производится обоснованный выбор операционной системы. Описывается процесс загрузки ядра ОС Linux. Приводится применимый на практике механизм использования DRAM-PUF.

В **пятой главе** проводится оценка экспериментальных данных, полученных с применением метода, описанного в четвёртой главе. В эксперименте были использованы два идентичных планшетных ПК. Основываясь на характеристиках, введённых в главе 2, сделан вывод, о возможность использования DRAM-PUF для построения идентификатора устройства.

ЗАКЛЮЧЕНИЕ

1. Предложен метод для идентификации ПЛИС с применением алгоритма классификации по методу опорных векторов. Лучшие результаты этот метод даст при использовании Non-Parallel SVM, оптимизированного для работы тремя и более классами. Классификация проводится для значений, получаемых от реализации физически неклонируемой функции, базирующейся на кольцевом генераторе импульсов. Предложенный метод позволяет реализовать систему идентификации и защиты от несанкционированной модификации цифровых устройств, выполненных на базе ПЛИС.

2. Предложен метод построения идентификатора, основанный на использовании в качестве средства реализации ФНФ динамическую память с произвольным доступом. Дано теоретическое обоснование и приведены примеры исследований по данной теме. Предложенный метод позволит проводить идентификацию компьютеров общего назначения без модификации аппаратной составляющей. Также этот метод может быть применён на всех цифровых устройствах, использующих DRAM.

3. Предложенный выше метод был успешно применён на практике в качестве расширения ядра операционной системы CyanogenMod. Это позволило провести исследования на реальных устройствах. Результаты были оценены с помощью различных характеристик физически неклонируемых функций. Основываясь на этих характеристиках, а в особенности, на характеристике устойчи-

вости, был сделан вывод, что используя реализацию ФНФ на основе DRAM можно строить идентификатор устройства.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Витенко, А.А. Применение методов линейной классификации для идентификации ПЛИС / А.А. Витенко // Компьютерные системы и сети: материалы 51-ой научной конференции аспирантов, магистрантов и студентов. – Минск: БГУИР, 2015. – с. 81–82.

2-А. Витенко, А.А. Использование DRAM-PUF для идентификации мобильных устройств под управлением ОС Android / А.А. Витенко // Апробация. №1(40) - 2016.