ПРОГРАММНОЕ СРЕДСТВО АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кирвель Е.А.

Иванюк А.А. – д-р. техн. наук, профессор

В докладе рассмотрены проблемы и особенности реализации физически неклонируемых функций, а также описаны методы оценки качества физически неклонируемых функций. Рассматриваются технические проблемы, связанные с реализацией статических тестов NIST, и методы их решения.

В современном мире информационных технологиях все большее внимание стоит уделять защите информации. Криптографические методы применяются практически во всех информационных технологиях и охватывают полный стек промышленной разработки: начиная от цифровых устройств и заканчивая протоколами передачи данных в веб-технологиях. Физическая криптография является одним из наиболее современных достижений в области криптографии и защиты информации. Доминирующей категорией физической криптографии являются физически неклонируемые функции (ФНФ). Существуют множества вариантов реализации физически неклонируемых функций. В данном докладе рассмотрен вариант реализации физически неклонируемой функции типа арбитр, для анализа которой и было применено описываемое программное средство. Для определения качества ФНФ обычно используют следующие параметры: уникальность, стабильность, случайность. Для расчета каждой из них имеются свои подходы и особенности. К примеру для расчета случайности часто прибегают к статическим тестам Д. Кнута, тестам Дж Марсальи, Национального института стандартов США (NIST). Описываемое программное средство реализует статические тесты NIST для расчета случайности. На данный момент имеются реализации тестов NIST на языке C, однако эти пакеты имеют ряд недостатков: имеют ошибки в реализации алгоритмов, алгоритмы не оптимизированы, нечитабельный код. При использовании потоков и элементарных оптимизаций, можно значительно улучшить производительность данных тестов. Для расчета уникальности и стабильности описываемое программное средство предоставляет возможность выбора метода расчета разницы между двумя векторами ответов от одной и той же ФНФ. В настоящее время не существует такого программного средства, которое агрегировало бы в себе тесты для ФНФ, позволяло бы в удобной форме получать результаты и проводить анализ.

Основными целями создания программного средства являются:

1) Обеспечить возможность расчёта основных характеристик ФНФ таких как уникальность, стабильность, случайность.

2) Реализовать статические тесты NIST используя .NET Framework.

3) Добиться улучшения производительности тестов NIST за счет распараллеливания операций.

4) Обеспечить анализ результатов исследования ФНФ типа арбитр на программируемых логических интегральных схемах (ПЛИС) типа FPGA.

5) Реализовать возможность получения результатов в виде графиков для удобства анализа результатов.

В качестве языка программирования для реализации программного средства был использован язык C#. Развитая инфраструктура платформы .NET и появившиеся в .NET 4.5 удобные конструкции асинхронного и параллельного программирования позволили создать надежное и высокопроизводительное программное средство.

В ходе реализации все поставленные цели были достигнуты. Были использованы различные средства параллельного программирования .Net Framework. При помощи PLINQ удалось добиться увеличения производительности тестов более чем в 2 раза. Программное средство было протестировано при подаче 100 блоков, состоящих из 100 000 бит каждый.

Таким образом, разработанное программное средство автоматизации тестирования физически неклонируемых функций позволяет осуществлять расчет основных характеристик ФНФ, а также упрощает анализ полученных результатов. Предлагаемое программное средство было использовано на практике для исследования ФНФ типа арбитр на программируемых логических интегральных схемах (ПЛИС) типа FPGA. При помощи данного программного средства исследовались характеристики как для нескольких экземпляров ФНФ на одном кристалле, так и на разных кристаллах.

Список использованных источников:

1. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонируемые функции / Информатика, №2, 2011 г. 12с..
2. Клыбик В.П. Применение физически неклонируемой функции типа арбитр для решения задачи идентификации цифровых устройств / В.П Клыбик, А.А. Иванюк // Информатика. – 2015., - №3 – С 24-34
3. Zalivaka S.S, Puchkov A.V., Klubik V.P., Ivaniuk A.A., Chang C.H. Multi-valued arbiters for Quality Enhancement of PUF Resp
4. onses on FPGA Implementation.