АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ИССЛЕДОВАНИЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

С. С. Заливако, А. А. Иванюк, В. П. Клыбик, А. В. Пучков
Факультет электротехники и электроники, Наньянский технологический университет Кафедра программного обеспечения информационных технологий, кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Сингапур, Сингапур; Минск, Республика Беларусь
E-mail: alexander.v.puchkov@gmail.com, vold029@gmail.com, ivaniuk@bsuir.by, zali0001@e.ntu.edu.sg

Рассматривается архитектура разработанного аппаратно-программного комплекса, позволяющего выполнять экспериментальное исследования физически неклонируемых функций. Представления методика проведения экспериментального исследования и полученные результаты, позволяющие судить об эффективности использования физически неклонируемых функций типа арбитр и ее усовершенствованного варианта для решения задачи уникальной неклонируемой идентификации цифровых устройств и систем.

Введение

Одними из наиболее перспективных подходов к защите цифровых устройств и систем от несанкционированного использования являются методы идентификации и аутентификации, основанные на использовании так называемых физически неклонируемых функций (ФНФ). Замечательные свойства ФНФ для решения обозначенной задачи обусловлены тем, что для цифровых устройств функционирование ФНФ основывается на физических вариациях технологического процесса производства интегральных схем. Данные вариации имеют случайный характер и их предсказание, а тем более клонирование, не представляется возможным [1].

Эффективное применение ФНФ требует исследования количественных характеристик их аппаратных реализаций, что может быть осуществлено, например, на программируемых логических интегральных схемах (ПЛИС) типа FPGA. Использование FPGA является быстрым и доступным спобом прототипирования цифровых устройств и систем, позволяющим в рассматриваемом случае реализовать множество экземпляров ФНФ на одном кристалле ПЛИС [2].

Исследованию подлежат такие важные характеристики получаемых ответов ФНФ как стабильность, уникальность и случайность. Их оценки как для нескольких экземпляров ФНФ на одном кристалле, так и на разных кристаллах позволяет сделать выводы о практической применимости ФНФ для решения, например, задачи идентификации цифровых устройств и выработать практические рекомендации для использования ФНФ в этом случае.

I. Постановка задачи

Была поставлена задача разработки аппаратно-программного комплекса исследования ФНФ, позволяющего оценить их основные характеристики с точки зрения уникальной неклонируемой идентификации цифровых устройств и систем, реализованных на основе ПЛИС типа FPGA. Данный комплекс должен позволять в пакетном режиме подавать запросы на ФНФ и отправлять полученные ответы на рабочую станцию, где производится обработка полученных экспериментальных данных с целью получения количественных оценок интересующих характеристик ФНФ.

II. Архитектура

В качестве аппаратной платформы для реализации рассматриваемого комплекса были выбраны платы быстрого прототипирования Nexys-4 производства компании Digilent, используемые в учебном процессе на кафедре программного обеспечения информационных технологий БГУИР. Данные платы построены на базе FPGA Xilinx Artix-7, имеющей 15 850 секций, каждая из которых содержит 4 6-входовых LUT и 8 синхронных триггеров. Кроме того, на плате представлены разнообразные периферийные модули, среди которых следует отметить важные для решения поставленной задачи USB-JTAG порт и USB-UART мост, которые соответственно обеспечивает удобное программирование FPGA и обмен данными между FPGA и рабочей станцией.

Разработка проектного описания аппаратной части комплекса осуществлялась на языке VHDL, итогом чего стали реализации параметризируемой компоненты мультиарбитральной ФНФ и ее усовершенствованного варианта, а также контроллера, реализующего протокол взаимодействия ФНФ с рабочей станцией по интерфейсу UART. Управление ФНФ осуществляется отправлением команд контроллера ФНФ по интерфейсу UART, который также используется для передачи ответов ФНФ на рабочую станцию. Реализация интерфейсного котроллера UART является параметризируемой, в частности можно задать значение скорости передачи дан-

ных. Стоит также отметить, что разработанная система использует дополнительные возможности интерфейсного контроллера UART, представленного на плате, например, аппаратную буферизацию данных.

При проведении эксперимента имеющиеся в наличии 10 плат Digilent Nexys-4 подключаются к внешнему источнику питания, а выходы USB всех плат объединяются концентратором, который подключается к рабочей станции. Подобная организация позволяет удобно параллельно работать со всеми платами. Так, был разработан скрипт, который выполняет программирование всех FPGA заданым образом конфигурации. Что же касается обмена данными по интерфейсу UART, то автоматически устанавливаемый драйвер обеспечивает, чтобы каждое устройство в этой системе было представлено виртуальным COM-портом, работа с которым является достаточно простой с точки зрения интерфейса программирования.

Программная часть описываемого комплекса была разработана на языках программирования C# и Python. Развитая инфраструктура платформы .NET и появившиеся в .NET 4.5 удобные конструкции для асинхронного программирования позволили создать надежное программное средство взаимодействие с реализованным на FPGA контроллером ФНФ. В свою очередь на Python были разработаны скрипты, выполняющие обработку полученных экспериментальных данных.

III. Экспериментальное исследование

Объектом проводимого исследования является физически неклонируемая функция типа арбитр, хорошо описанная в литературе, а также её усовершенствованная модификация. Основная идея построения и функционирования ФНФ типа арбитр заключается в изготовлении двух функционально и топологически идентичных путей, которые будут иметь близкие, но все же принципиально различные значения времени распространения сигнала по ним. Данное различие можно определить, подавая на вход обоих путей фронта сигнала и определении, какой из них появится на выходе быстрее. Последнее может быть осуществлено в простейшем случае при помощи синхронного D-триггера. В этом случае выход с одного пути соединяется со входом данных триггера, а выход со второго пути - с его входом синхронизации. В результате на выходе такого арбитра будет формироваться значение 0 либо 1 в зависимости от того, какой из путей имеет меньшую задержку распространения сигнала. При этом сами пути строятся на основании двухвходовых мультиплексоров, что делает их конфигурируемыми. Селективные входы мультиплексоров объединяются в шину запроса ФНФ, что даёт 2^N различных возможных конфигураций путей, где N - длина путей (количество двухвходовых мультиплексоров) [1]. Стоить отметить, что арбитр на основе синхронного D-триггера принципиально может оказаться в метастабильном состоянии [2]. Данный факт лежит в основе предложенного более совершенного варианта ФНФ, в котором используется RS-защёлка и счётчик. Это позволяет определить кроме устойчивых состояний 0 и 1 также нестабильное состояние HFO (high frequency oscillation).

При проведении эксперимента на ФНФ подавались запросы от генератора, представляющего собой сдвиговый регистр с линейной обратной связью (LFSR), причем каждый следующий запрос генерировался спустя количество тактов, равное разрядности LFSR, что позволило добиться слабой корреляции запросов. Количество подаваемых запросов управляется программным обеспечением, выполняющим на рабочей станции, а сам же генератор запросов был реализован аппаратно в FPGA. Получение ответов ФНФ на большой набор запросов производилось неоднократно, что позволяет оценить стабильность получаемых ответов. В среднем, получение ответов ФНФ на 10000 запросов в 30 экспериментах на рассматриваемом аппаратно-программном комплексе занимает порядка 25 минут, что можно считать неплохим результатом.

Важнейшими характеристиками с точки зрения уникальной неклонируемой идентификации, оценка которых производилась для ФНФ, являются стабильность и уникальность. Результаты, полученные на эксперименте с арбитром на основе синхронного D-триггера показали стабильность в среднем 0.998, что говорит о крайне низкой вероятности получения неверного ответа при многократной подаче фиксированного запроса. Стабильность для усовершенствованного арбитра остается примерно такой же. Уникальность же оценивается как 0,495.

Заключение

Разработка рассмотренного аппаратно-программного комплекса позволяет исследовать важнейшие характеристики физически неклонируемых функций, на основании чего можно сделать выводы о эффективности их использования в решении задачи уникальной неклонируемой идентификации цифровых устройств и систем. Работа над комплексом продолжается, и дальнейшие его усовершенствования касаются автоматизации процессов и обеспечения удаленного доступа к аппаратно-программному комплексу.

1. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – № 2. – С. 90–100.
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.