ИССЛЕДОВАНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ С ИСПОЛЬЗОВАНИЕМ СОФТ-ПРОЦЕССОРА MICROBLAZE

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

Пучков А. В.

Иванюк А. А. – доктор технических наук, профессор

Одним из перспективных решений в области защиты цифровых устройств и систем от несанкционированного использования является применение решений, основанных на так называемых физически неклонируемых функциях. В основе их функционирования лежит структурная сложность физических систем. В силу своей природы физически неклонируемые функции наиболее полно исследуются в своих физических реализациях. Рассмотренное в работе программно-аппаратное решение использует программируемые логические интегральные схемы типа FPGA с работающим на базе них софт-процессором и высокопроизводительным сетевым интерфейсом для эффективной постановки экспериментов на реализациях физически неклонируемых функций.

В условиях, когда несанкционированное использование цифровых устройств, систем и их проектных описаний становится все большей проблемой, широкое распространение получают методы физической криптографии, в частности использование физически неклонируемых функций (ФНФ) [1]. При создании любых цифровых систем принципиально невозможно управлять величинами многих физических параметров, вследствие чего последние вследствие вариации техпроцесса принимают случайные, но уникальные для каждой цифровой системы значения. Идея извлечения подобных уникальных параметров из цифровых систем и является основой аппаратных реализаций ФНФ [1].

Эффективное использование ФНФ не представляется возможным без предварительного исследования их свойств на целевой аппаратной платформе. В настоящее время широко распространены программируемые логические интегральные схемы (ПЛИС) типа FPGA, которые предлагают чрезвычайную гибкость, и используются не только для прототипирования цифровых систем, но и для их конечной реализации [1].Исследование различных аспектов реализаций физически неклонируемых функций на FPGA неоднократно становилось предметом исследований [2].

Однако процесс исследования сопряжен с рядом трудностей, в числе которых можно выделить необходимость передавать с платы прототипирования на основе FPGA на рабочую станцию большой объем данных (в простейшем случае, запросов и ответов ФНФ), а также надежность используемого решения, напрямую влияющая на достоверность получаемых данных.В рамках разработанного решения были предприняты шаги к эффективному решению данных проблем, состоящие в использовании высокопроизводительного сетевого интерфейса, а также реализации значительной части логики системы программным способом, при этом выполнение программного кода осуществляет софт-процессор MicroBlaze, разработанный корпорацией Xilinx.

При помощи имеющихся плат быстрого прототипирования Xilinx Artix-7 и программного обеспечения Xilinx Vivado была спроектирована цифровая система, осуществляющая управление реализациями ФНФ и передачу данных от них к рабочей станции или иному устройству. Ядром системы стал софт-процессор MicroBlaze, соединенный с периферийными устройствами посредством шины AXI. К важнейшим из периферийных устройств относятся контроллер Ethernet (канальный уровень), внешняя память ОЗУ и сами реализации ФНФ. Использование Ethernet позволило улучшить производительность и надежность интерфейсного взаимодействия с рабочей станцией по сравнению с [2].При этом физический уровень модели ISO/OSI присутствовал в виде аппаратного модуля на плате прототипирования, канальный реализован вышеупомянутым контроллером, а все вышележащие – программным способом (с использованием протокола TCP в качестве транспортного), что делает данное решение еще более гибким.

Из-за того, что логика управления ФНФ реализована в виде программного обеспечения для реализованного средствами FPGA софт-процессора MicroBlaze, она легко отлаживается и, что немаловажно, любые ее изменения не приводят к очень затратной по времени процедуре синтеза проектного описания цифровой системы. Вместо этого происходит лишь перекомпиляция исполняемых модулей встраиваемого ПО и их загрузка. Кроме того, сам софт-процессор, будучи конфигурируемой IP-компонентой, может быть легко настроен для наиболее эффективного решения поставленных задач.

Для выполнения на стороне рабочей станций было разработано клиентское программного средство с использованием технологии .NET на языке C#.

Использование новых решений позволило существенно улучшить эффективность исследования в части используемого времени, а также возможностей верификации, гибкости в использовании, что было отмечено уже в первых экспериментах.

Список использованных источников:

1. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем: монография / А. А. Иванюк. – Минск: Бестпринт, 2012. – 337 с.
2. Заливако, С. С. Аппаратно-программный комплекс исследования физически неклонируемых функций / С. С. Заливако, А. А. Иванюк, В. П. Клыбик, А. В. Пучков // Материалы международной научной конференции ITS 2015. – Минск: БГУИР, 2015. – С. 174–175.