ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ БЫСТРОГО ПРОТОТИПИРОВАНИЯ И ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ НА БАЗЕ ПЛИС

Шамына А. Ю., Кайкы М. Н., Иванюк А. А.
Кафедра программного обеспечения информационных технологий, кафедра информатики,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: shamyna@bsuir.by, kaikymykhailo@gmail.com, ivaniuk@bsuir.by

В настоящей работе описываются построение, инструментарий и конфигурация аппаратно-программного комплекса, предназначенного для проведения исследований криптографических примитивов, реализованных на FPGA в составе плат быстрого прототипирования. Рассмотрены нюансы построения сетевой, аппаратной и программной части исследовательского комплекса.

Введение

В настоящее время использование средств физической криптографии приобретает все более широкий характер [1]. Одновременно с этим растет интерес к исследованиям в данной области. Зачастую разработчики и исследователи в качестве платформы для реализации различных схем физической криптографии выбирают FPGA. Однако, наиболее трудоемким этапом подготовки эксперимента является конфигурация инфраструктуры для сбора и анализа данных. Кроме этого, существует проблема проведения экспериментов при стационарных внешних условиях (например, температура, напряжение питания и т.п.). Немаловажной является проблема представления и анализа данных экспериментов в максимально унифицированном виде. Одной из главных целью разработки аппаратно-программного комплекса является стремление решить эти проблемы и предоставить возможность исследователям максимально сократить время развертывания эксперимента.

I. Описание установки

Центральным узлом комплекса является хост – ПЭВМ на базе CPU Intel Xeon Bronze 3104 с 32 ГБ ОЗУ под управлением ОС Ubuntu 22.04. В состав ПЭВМ входят также несколько сетевых карт, где одна из них подключена к сети лаборатории, а вторая - к сетевому коммутатору с подключенными к нему платами быстрого прототипирования Digilent Zybo Z7-10 [2] (см. рис. 1). Для обеспечения стационарности температуры используется температурная камера TestEquity 155 Benchtop [3] с диапазоном температур от -20 °C до +130 °C и возможностью удаленного управления с использованием протокола SCPI (Standard Commands for Programmable Instruments). В качестве управляемого лабораторного блока питания выбран ELEMENT 305DB. В состав выбранной модели платы быстрого прототипирования входит СНК Xilinx Zynq 7000 [4] с двуядерным процессором Cortex-A9 с частотой 667 МГц и 1 ГБ DDR3 RAM, что делает возможным работу ОС Linux на данной платформе. В качестве дистрибутива Linux был выбран PetaLinux 2022.1 [5] с интегрированным клиентом синхронизации времени по протоколу NTP (Network Time Protocol) и драйвером, необходимым для загрузки конфигурации FPGA. Также был внедрен сервер TCF (Target Communications Framework) для сохранения возможности отладки программ из Vitis при работе PetaLinux. Образ ОС на плате загружается с карты памяти MicroSD. Для автоматического назначения IP-адресов сетевым интерфейсам плат на хосте был развернут DHCP-сервер с резервированием адресов из пула адресов по MAC-адресу сетевой карты. Для удобства управления платами на локальном DNS-серевере хоста были созданы DNS записи типа A, где имя для платы генерируется с использованием MAC-адреса. Сценарии работы и управления были написаны с использованием Bash. Управление платами осуществляется по протоколу SSH.

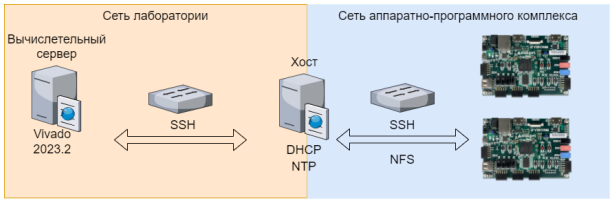

Рис. 1 – Схема аппаратно-программного комплекса

На хосте создана сетевая директория, в которой для каждой платы существует собственная поддиректория и которая включает в себя папки данных и скриптов. Эти папки являются сетевыми и монтируются в файловую систему отладочных плат в качестве NFS (Network File System) директорий.

II. Порядок выполнения эксперимента

Для проведения экспериментов необходимо подготовить IP-компонент исследуемого криптографического примитива, интерфейс которого должен быть выполнен по шаблону. HDL-описание аппаратуры содержит достаточное количество конфигурационных регистров и данных

для обеспечения работы исследуемых криптографических примитивов, которые спроецированы в адресное пространство PS (Processing System). Подключение компонентов, управляемых из адресного пространства PS осуществляется через интерфейс AXI4-LITE.

Затем подготовленный компонент подключается к проекту с HDL-описанием аппаратуры и уже вновь сгенерированный проект помещается по заданному пути.

На следующем этапе выполняется настройка скрипта Bash выполнения эксперимента, которая заключается в указании набора плат, на котором будет запускаться эксперимент, а также исходного кода программы на языке C, запускаемой на платах для опроса примитива. Затем выполняется запуск скрипта анализа данных экспериментов на Python. Есть также возможность указания количества экспериментов и реконфигураций блока программируемой логики (англ. Programmable Logic, PL), температурного режима и уровня напряжения питания плат. Алгоритм проведения эксперимента можно представить в виде последовательности действий (см. рис. 2).

Рис. 2 – Алгоритм выполнения эксперимента

После выполнения анализа, выполняется перемещение данных эксперимента на сетевой накопитель с указанием идентификатора эксперимента и временной отметки. Генерирование .bit файла конфигурации PL и синтез проекта осуществляется с использованием мощностей вычислительного сервера. Загрузка конфигурации FPGA производится из PS Zynq 7000 с использованием fpga_util без перезагрузки PetaLinux. Использование такого подхода для конфигурации PL требует геннерирование из файла конфигурации .bit файла .bin, которое производится утилитой BitGen, доступной в пакете PetaLinux. Кроме полной реконфигурации PL доступно также ее частичная реконфигурация (англ. Partitial Reconfiguration, PR) [6].

III. Заключение

В результате выполнения описанной работы был создан аппаратно-программный комплекс, который существенно снижает временные и трудовые затраты при выполнении исследований криптографических примитивов. Параметризация сценариев работы экспериментальной установки позволяет гибко ее настраивать под конкретный эксперимент. Использование высокоскоростной сетевой инфраструктуры 1 Гбит/с в сочетании с сетевыми хранилищами общим объемом 24 ТБ, построенных на RAID-массивах, позволяет работать с большим объемом экспериментальных данных. Потенциально данная схема экспериментов может быть расширена для исследования любых других схем физической криптографии.

Список литературы

1. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – №2. – С. 90-100.
2. Zybo Z7 Refence / Digilent inc [Electronic resource]. – Mode of access: `https://digilent.com/reference/programmable-logic/zybo-z7/start`. – Date of access: 10.10.2023.
3. TestEquity Chambers TE-155 Benchtop Temperature Chamber / TestEquity LLC [Electronic resource]. – Mode of access: `https://www.testequity.com/product/20200-1-TE-155`. – Date of access: 10.10.2023.
4. Zynq 7000 SoC / Advanced Micro Devices, Inc. [Electronic resource]. – Mode of access: `https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html`. – Date of access: 10.10.2023.
5. PetaLinux Tools Documentation: Reference Guide / Advanced Micro Devices, Inc. [Electronic resource]. – Mode of access: `https://docs.xilinx.com/r/2022.1-English/ug1144-petalinux-tools-reference-guide`. – Date of access: 10.10.2023.
6. Vivado Design Suite User Guide Dynamic Function eXchange / Advanced Micro Devices, Inc.[Electronic resource]. – Mode of access: `https://docs.xilinx.com/v/u/2020.1-English/ug909-vivado-partial-reconfiguration`. – Date of access: 10.10.2023.