УДК 621.382

ОБНАРУЖЕНИЕ АППАРАТНОЙ ЗАКЛАДКИ В ПРОСТЫХ ЦИФРОВЫХ УСТРОЙСТВАХ НА ОСНОВЕ АНАЛИЗА ПО СТОРОННЕМУ КАНАЛУ

Воронов А.Ю., Стемпицкий В.Р.

Белорусский государственный университет информатики и радиоэлектроники,
Минск, Республика Беларусь, voronov.drawtoon@gmail.com

Аннотация: сегодня для уменьшения цикла разработки интегральных схем (далее -ИС) компании прибегают к использованию стороннего программного обеспечения проектирования ИС, внедрению сторонних IP-блоков (Intellectual Property) других фирм и производству микросхем на мощностях коммерческих фабрик, что значительно увеличивает риск внедрения в изделия аппаратных троянов. Аппаратные трояны могут вызвать изменение функциональной работы устройства, утечку информации или вывод из строя [1]. В этой статье представлен процесс внедрения аппаратного трояна в цифровой приемо-передатчик, проведен анализ полученной структуры на функциональном и схемотехническом уровне при помощи программируемых ресурсов программируемой логической интегральной схемы (далее – ПЛИС).

Ключевые слова: цифровая электроника, аппаратная безопасность, аппаратные трояны, ПЛИС, IP-ядра, Serial Peripheral Interface, Side channel analysis, функционально-логическое тестирование.

ВВЕДЕНИЕ

Как и программное обеспечение, аппаратное обеспечение имеет риски, связанные с безопасностью, и долгое время проблемам безопасности аппаратного обеспечения не уделялось должного внимания. Распределенная и многоступенчатая процедура современной цепочки изготовления и поставок микросхем для электронной аппаратуры с использованием многих государств создает высокую опасность включения в микросхемы так называемых аппаратных закладок (аппаратных троянов).

В этой работе рассмотрены неинвазивные способы обнаружения аппаратных закладок как более предпочтительны в связи с низкой стоимостью и возможность обнаружения трояна на этапе разработки, что обеспечивается анализом по стороннему каналу (Side-channel analysis) и логическим тестированием. К анализу по стороннему каналу относится изучение изменений в микросхеме по потребляемой мощности, температуре, временным задержкам и занимаемой площади схемы на кристалле.

Цель проводимого исследования – определение эффективности анализа по стороннему каналу для обнаружения внедренного трояна в ИС. Для этого на базе программного комплекса Xilinx Vivado 2020.1 и ПЛИС семейства Spartan-7 разработан блок SPI (Serial Peripheral Interface) master и SPI slave в который будет введен функциональный аппаратный троян с внутренним механизмом активации и проводится попытка его обнаружения.

МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ

Для внедрения аппаратной закладки выбран цифровой блок, изображенный на рисунке 1. Он представляет собой два SPI приемо-передатчика, которые обмениваются друг с другом информацией, хранящийся в памяти с произвольным доступом (Random Access Memory, RAM). Такая простая структура позволяет более точно оценить незаметность встраиваемой аппаратной закладки и эффективность обнаружения внедренного трояна с помощью анализа по стороннему каналу, а именно потребляемой статической и динамической мощности.

При своей нормальной работе в пакете передаваемых данных младший полубайт больше старшего на единицу, а младшие и старшие полубайты соседних байтов равны. В свою очередь SPI slave сохраняет полученные данных в блочную RAM и по команде SPI master передает их обратно. Аппаратный троян вносит функциональное изменение в работу цифрового устройства, суть которого является подмена данных, идущих из памяти в передатчик. На временной диаграмме симуляции это представлено в виде рисунках 1 и 2. На них видно, что во время передачи данных при активации трояна (сигнал trj_led) на линии send_data_MasterSPI младший полубайт копируется и заменяет своим значением старший полубайт, после чего, полученная SPI slave посылка по команде отправляется обратно с уже испорченными данными.

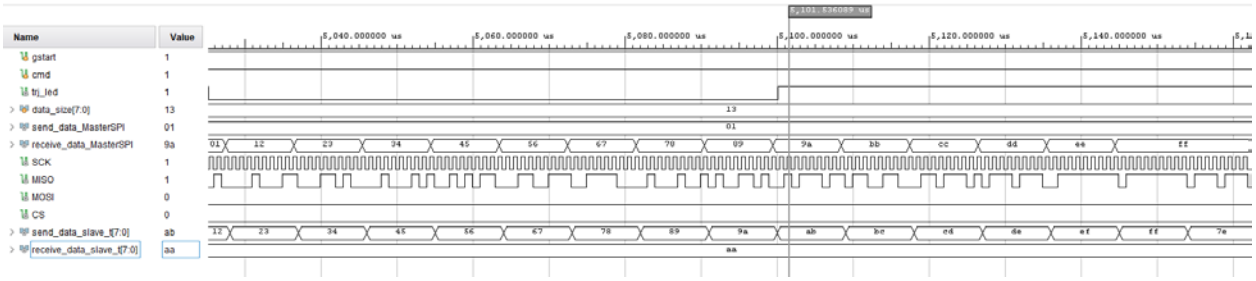

Рисунок 1. Временная диаграмма передачи данных SPI slave с активированным трояном

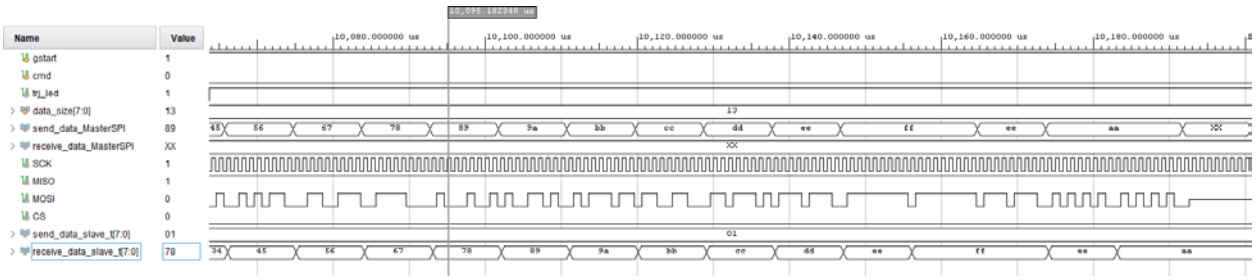

Рисунок 2. Временная диаграмма передачи данных на SPI master с активированным трояном

Статическая потребляемая мощность – это мощность, потребляемая устройством в простое, когда на него не подаются сигналы, в том числе тактовый сигнал. В основном, эта мощность определяется токами утечки паразитных диодов КМОП-схем. Рост статической мощности по сравнению с “золотым образцом” часто свидетельствует о внесении автомата конечных состояний в проект. Статическая потребляемая мощность рассчитывается по формуле 1 [2]:

$$P_{stat} = VDD \times I_{leak}, \quad (1)$$

где VDD – напряжение питания, I_{leak} – ток утечки.

Динамическая потребляемая мощность обусловлена переключением транзисторов из одного состояния в другое. При работе устройства транзисторы меняют свое состояние с открытого на закрытое и наоборот, из-за чего также происходит зарядка и разрядка емкостей КМОП-схем. Когда конструкция функционирует в результате передачи данных или вычислений, транзисторы меняют свое состояние с включенного на выключенное и с выключенного на включенное. Рост динамической мощности по сравнению с “золотым образцом” может свидетельствовать о внедрении в устройство трояна на основе комбинационной логики, так и о трояне-счетчике. Для расчета динамической потребляемой мощности применяется формула 2 [2]:

$$P_{dyn} = \frac{1}{2} C_L \times VDD^2 \times f, \quad (2)$$

где C_L – общая емкость нагрузки, VDD – напряжение питания, f – тактовая частота.

Для “золотого образца”, т.е. цифрового устройства без аппаратных закладок, P_{stat} = 0,068 Вт и P_{dyn} = 5,180 Вт, что было рассчитано при помощи Xilinx Power Estimator (далее – XPE) [3], входящего в состав Xilinx Vivado.

Аппаратная закладка имеет внутренний механизм активации и представляет собой обычный 32-битный счетчик, который тактируется не от основного тактового сигнала, а от простой комбинационной схемы, которая может представлять собой несколько управляющих или передающих сигналов, подключенные через логический элемент, как представлено на рисунке 3. Такой прием при сохранении размеров троянов и их энергопотребления позволяет значительно увеличить срок работы устройства перед запланированным отказом. Среди функциональных аппаратных закладок, такие представляют большой интерес с точки зрения незаметности потому, что они могут представлять собой обычную комбинационную схему, которая будет вызывать периодические, кратковременные сбои в работе, что при диагностировании проблемы будет выглядеть как обычный дефект микросхемы. Полученные в XPE значение статической мощности P_{stat} = 0,068 Вт, а динамической – P_{dyn} = 5,383 Вт.

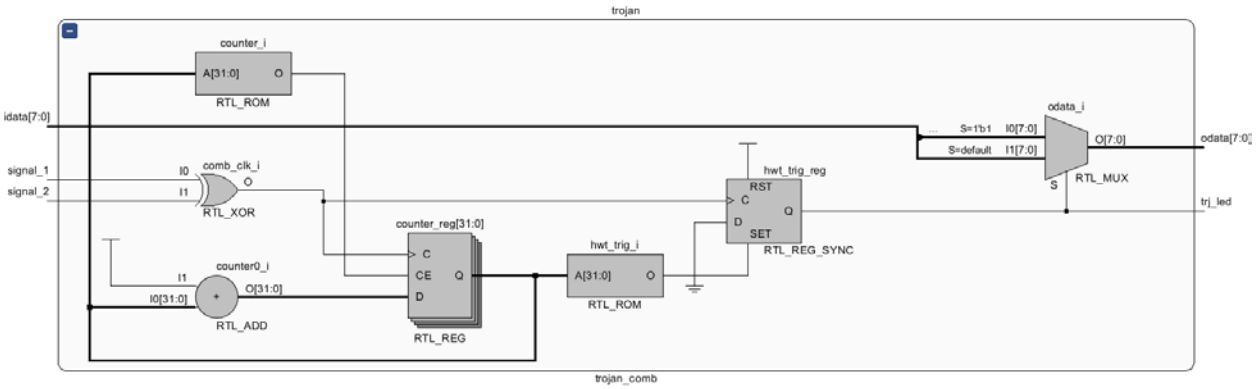

Рисунок 3. Схематичное изображение комбинационного трояна-счетчика

Для удобства сравнения полученных результатов, значения статических и динамических потребляемых мощностей, а также задействованных ресурсов ПЛИС продублированы в таблице 1. Из них видно, что во всех случаях внедрения аппаратной закладки росла потребляемая динамическая мощность устройства и самое большое значение у комбинационного трояна-счетчика. Неизменность статической мощности объясняется как малыми размерами трояна и самого цифрового устройства, так и самой архитектурой ПЛИС, где незадействованная программируемая логика сама по себе является основным потребителем мощности в простое устройства. Так же видно, что “золотой образец” занимает больше места, чем комбинация “золотой образец” и аппаратная закладка. Учитывая, что и исследуемое устройство, и его комбинация с аппаратной закладкой работают согласно ожиданиям, а стратегии оптимизации одинаковы для их обоих проектов, следует предположить, что компилятор программного обеспечения Xilinx Vivado 2020.1 просто переиспользует занятые элементы для сохранения ресурсов ПЛИС [4].

Таблица 1. Потребляемая мощность исследуемых устройств

Исследуемый проект	P_{stat}, Вт	P_{dyn}, Вт	$P_{общ}$, Вт	LUT, шт.	FF, шт.
“Золотой образец”	0,068	5,180	5,248	567	356
“Золотой образец” + комбинационный троян	0,068	5,488	5,556	209	353

Дополнительно к анализу по стороннему каналу, для детектирования трояна использовалось обычное функционально-логическое тестирование в симуляции, где данные, полученные с тестируемого проекта, сравнивались с данными из “золотого образца”. Тестовая последовательность включала в себя посылки по 256 байт в 10 случайных комбинациях. С помощью такого подхода не удалось обнаружить активацию аппаратной закладки с помощью встроенных средств Xilinx Vivado 2020.1.

ЗАКЛЮЧЕНИЕ

Проведено исследование методики обнаружения, основанной на анализе по стороннему каналу, аппаратной закладки в цифровой блок внутренним механизмом активации. Показана эффективность данного метода при использовании инструментария программного обеспечения Xilinx Vivado 2020.1. Данная методика может быть использована для исследования эффективности обнаружения аппаратных троянов с другими механизмами активации и последующей ее доработки.

ЛИТЕРАТУРА

[1] Белоус А. И., Солодуха В. А., Шведов С. В. Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия. Москва, Техносфера, 2019. 688 с

[2] Prashanth Reddy G. Design and detection of hardware trojans. Hyderabad, Masaryk University, 2017. 64 p.

[3] Xilinx Power Estimator User Guide (UG440). Santa Clara, AMD, 2023. 129 p.

[4] Vivado Design Suite User Guide (UG901). Santa Clara, AMD, 2020. 295 p.

[5] 7 Series FPGAs Clocking Resources (UG472). Santa Clara, AMD, 2018. 114 p.

[6] 7 Series DSP48E1 Slice (UG479). Santa Clara, AMD, 2018. 58 p.

HARDWARE TROJAN DETECTION BASED ON SIDE-CHANNEL ANALYSIS IN SIMPLE DIGITAL DEVICES

A. Voronov, V. Stempitsky

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus,
voronov.drawtoon@gmail.com

Abstract: today, in order to reduce the development cycle of integrated circuits (ICs), companies resort to using third-party ICs design software, implementing third-party IP blocks (Intellectual Property) of other companies, and manufacturing microcircuits at the facilities of commercial factories, which significantly increases the risk of introducing hardware trojans into products. Hardware trojans can cause a change in the functional operation of the device, leak information, or disable it [1]. This article presents the process of imserting a hardware trojan into a digital transceiver, and analyzes the result structure at the functional and circuit levels using programmable resources of a programmable logic integrated circuit (FPGA).

Keywords: digital electronics, hardware security, hardware trojans, FPGA, IP-cores, Serial Peripheral Interface, Side channel analysis, functional testing.