УДК 621.382

ОСНОВНЫЕ МЕТОДИКИ ОБНАРУЖЕНИЯ АППАРАТНЫХ ТРОЯНОВ НА ЭТАПЕ ПРОЕКТИРОВАНИЯ

Воронов А.Ю., Стемпицкий В.Р.

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

Аннотация: увеличение разнообразия и спектров применения интегральных микросхем (далее – ИС) приводит к росту числа участников их производства и проектирования. Стороннее программное обеспечение для проектирования ИС, использование IP-блоков (Intellectual Property) других компаний значительно увеличивает риск внедрения в устройства вредоносных схем, называемых аппаратными троянами, уже на этапе проектирования. Аппаратные трояны могут вызвать изменение функциональной работы устройства, утечку информации или вывод из строя [1]. В этом тезисе рассмотрены современные и малостоящие методы обнаружения аппаратной закладки без разрушения микросхемы.

Ключевые слова: цифровая электроника, аппаратная безопасность, аппаратные трояны, ПЛИС, IP-ядра, анализ по стороннему каналу, функционально-логическое тестирование.

ВВЕДЕНИЕ

Сегодня, наравне с программным обеспечением, аппаратная часть устройств также подвержена внедрению вредоносных схем, называемых аппаратными троянами, которые могут быть использованы для нарушения безопасности пользователя устройства. Связано это с большим распределением этапов разработки электронных устройств не только между компаниями, но и между странами и даже континентами. В таких условиях невозможно соблюсти те же требования по безопасности к аппаратной части, какими они были еще 30 – 40 лет назад, когда разработка и производство микросхемы велось в рамках одной фирмы и никогда за пределами страны-производителя. Сейчас же даже отдельные цифровые блоки принято отдавать на стороннее проектирование или вовсе использовать по лицензии IP-блоки (Intellectual Property) для уменьшения издержек, связанных с разработкой электронных устройств.

Для обнаружения аппаратных закладок применяются 2 большие группы методов: с последующим разрушением микросхемы и без. Метод с разрушением чипа основывается на изучении топологии готовой микросхемы после снятия каждого слоя металлизации с помощью оптической или электронно-лучевой микроскопии. Данный метод обладает высокой точностью, однако долог, дорогостоящ и требует специализированную лабораторию с обученным персоналам, не говоря уже о затратах на производство тестовой партии микросхем. Неинвазивные способы обнаружения более предпочтительны в связи с низкой стоимостью и возможностью обнаружения аппаратного трояна еще на этапе разработки. К данному направлению относится группа методов анализа по стороннему каналу (Side-channel analysis), с помощью которых изучаются изменения в микросхеме по потребляемой мощности, выделяемой температуре, временным задержкам и так далее.

Целью данного исследования является нахождение методики, которая при комбинации группы анализов по стороннему каналу и логического тестирования, помогала бы с достаточной и необходимой точностью определить наличие трояна в проекте на ПЛИС на этапе разработки цифровой микросхемы малого объема (до 3 тысяч элементов). Для этого в этой статье будут рассмотрены современные методы, относящиеся к анализу по стороннему каналу и логическому тестированию, и будет дана им оценка по соотношению денежных и временных издержек к получаемому результату.

ОСНОВНАЯ ЧАСТЬ

Логическое тестирование заключается в создании нескольких тестовых шаблонов данных, которые должны представлять собой как стандартный поток данных, так и редкие их комбинации с целью нахождения условий активации аппаратной закладки. Если же ответы между образцом и эталоном различны, то логическое тестирование обнаружило аппаратный троян. Главная проблема такого подхода заключается в том, что для ИС большого объема (VLSI, Very Large Scale Integration) невозможно перебрать все возможные комбинации битов вместе со всеми возможными комбинациями этих тестовых посылок потому, что симуляция работы с исчерпывающим набором тестовых шаблонов данных для обнаружения всех возможных аппаратных закладок трудно выполнимо на текущих вычислительных мощностях. Связано это с тем, что при получении каждой новой посылки, изменяются состояния отдельных конечных автоматов или процессорных подсистем, регистров, защелок и т.д.,

комбинация данных на выходе которых и может вызвать отказ устройства. Для тестирования ИС с большой степенью интеграции (от 100 тысяч элементов на кристалле) можно выделить два основных подхода: разбиение схемы на малые функциональные узлы и логическое тестирование с анализом данных по стороннему каналу.

В работе [2] представлен способ, где тестируемая схема разбивалась на подсхемы. В каждой такой схеме выбирались конкретные узлы, в которых будет происходить сравнение получаемых данных с таким же узлом соседней подсхемы. Отличие ответа хоть одной такой ячейки может свидетельствовать о наличии трояна в массиве однотипных подмодулей. Данное тестирование может масштабироваться, избегая проблем, связанных с типом ИС и процессом разработки.

В работе [3] предлагается использовать масштабируемый метод генерации статистических тестов, который может генерировать высококачественный набор тестовых шаблонов для создания команд с высокой вероятностью активации встроенного произвольного трояна. Этот метод генерирует команды с учетом анализа сигналов по сторонним каналам. Такой анализ позволяет установить отклик в виде дополнительного переключения транзисторов в аппаратной закладке и определить не только наличие встроенного трояна, но и механизм его активации, включая и сам шаблон активации.

Анализ сигнала по стороннему каналу сравнивает ИС в роли “золотого образца” с тестируемой ИС по всем видам сторонних параметров, таких как напряжение, температура, задержка распространения сигнала (path delay) и т. д. По изменениям этих параметров в ходе тестирования исследуемой схемы можно предположить, что расхождение исследуемых параметров при анализе по стороннему каналу свидетельствует о наличии незаявленного дополнительного логического узла в ИС с неизвестным функционалом, который может привести к неисправности устройства, содержащего аппаратную закладку. Тем не менее, не только шум мешает обнаружению аппаратного трояна, но и малые величины изменения напряжений и тока потребления.

В работе [4] предложен метод обнаружения аппаратных закладок в ИС на основе матрицы разницы температур. Эта матрица представляет собой попиксельный анализ теплового изображения схемы за некоторое время. В эксперименте, приведенном в данной работе, добавлены также дополнительные модули для создания теплового шума для маскировки аппаратного трояна. Однако сравнение температурной матрицы исследуемого образца со встроенной аппаратной закладкой и “золотого образца” показало значительное повышение дифференциальной температуры.

В работе [5] представлен новый метод обнаружения встроенных аппаратных закладок на основе анализа задержки распространения сигнала. В этой работе предложение объединить исследуемую схему со структурой защелки, и эта структура защелки способна показать задержку, вызванную аппаратной закладкой. Этот метод позволяет решить проблему влияния изменения технологического процесса ИС и в то же время уменьшить влияние шума на эффективность анализа по стороннему каналу.

В связи с тем, что целью данной работы является нахождение методики, включающей в себя методы, требующие минимальных финансовых вложений, а также проверка этой методики на микросхеме малого объема, в качестве анализа по стороннему каналу предлагается использовать анализ изменения расчетной статической мощности и динамической мощности потребления устройства. Таким образом, используя в качестве анализа по стороннему каналу статическую потребляемую мощность и динамическую потребляемою мощность, теоретически можно определить наличие вредоносной аппаратной закладки с внутренним или внешним механизмами активации.

ЗАКЛЮЧЕНИЕ

Рассмотрены методы функционально-логического тестирования и анализа по стороннему каналу. На основе анализа временных и финансовых затрат решено для обнаружения аппаратной закладки в ИС малого объема использовать комбинацию стандартного функционально-логического тестирования всей схемы, анализа статической и динамической мощностей и используемых ресурсов ПЛИС и сравнение полученных результатов с “золотым образцом”. Данная методика будет использоваться для обнаружения аппаратных закладок с внутренним и внешним механизмом активации, а тестируемое устройство будет представлять собой обычный SPI master и SPI slave, реализованные на одном кристалле ПЛИС Spartan-7 кампании Xilinx.

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] Bazzazi, A.; Shalmani, M.T.M.; Hemmatyar, A.M.A. Hardware Trojan Detection Based on Logical Testing. J. Electron. Test. 2017, 33, 381–395.

[3] Huang, Y.W.; Bhunia, S.; Mishra, P. Scalable Test Generation for Trojan Detection Using Side Channel Analysis. IEEE Trans. Inf. Forensics Secur. 2018, 13, 2746–2760.

[4] Zhong, J.X.; Wang, J.Y. Thermal images based Hardware Trojan detection through differential temperature matrix. Opt. Int. J. Light Electron Opt. 2018, 158, 855–860.

[5] Zarrinchian, G.; Zamani, M.S. Latch-Based Structure: A High Resolution and Self-Reference Technique for Hardware Trojan Detection. IEEE Trans. Comput. 2017, 66, 100–113.

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

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

MAIN METHODS FOR DETECTING HARDWARE TROJANS AT THE DESIGN STAGE

A. Voronov, V. Stempitsky

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

Abstract: the increasing diversity and range of application of integrated circuits (ICs) leads to an increase in the number of participants in their production and design. Third-party software for ICs design, the use of IP-blocks (Intellectual Property) of other companies significantly increases the risk of introducing malicious circuits, called hardware trojans, into devices already at the design stage. Hardware trojans can cause a change in the functional operation of the device, leak information, or disable it [1]. This thesis examines modern and low-cost methods for detecting a hardware bug without destroying the chip.

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