AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics Engineering and Electrical Communications

Fragile Watermarking For Hardware IP Blocks

A Thesis submitted in partial fulfilment of the requirements of the degree of

Master of Science in Electrical Engineering

(Electronics Engineering and Electrical Communications)

by

Samar Mohamed Hussein Shukry

Bachelor of Science in Electrical Engineering

(Electronics Engineering and Electrical Communications)

Faculty of Engineering, Ain Shams University, 2013

Supervised By

Prof. Dr. Mohamed Amin Dessouky

Assoc. Prof. Dr. Amr Talaat Abdel-Hamid

Cairo - (2018)

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics and Communications

Fragile Watermarking For Hardware IP Blocks

by

Samar Mohamed Hussein Shukry

Bachelor of Science in Electrical Engineering

(Electronics Engineering and Electrical Communications)

Faculty of Engineering, Ain Shams University, 2013

Examiners' Committee

Name and Affiliation **Signature**

Prof. Dr. Ahmed Hassan Madian ……………….

Electronics and Communications, Nile University

Prof. Dr. Hani Fekri Ragai ……………….

Electronics and Communications, Ain-Shams University

Prof. Dr. Mohamed Amin Dessouky ……………….

Electronics and Communications, Ain-Shams University

Date:10 November 2018

Statement

This thesis is submitted as a partial fulfilment of Master of Science in Electrical Engineering, Faculty of Engineering, Ain shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Student name

Samar Mohamed Hussein Shukry

Signature

Samar Shukry

Date: 10 November 2018

Researcher Data

Name	: Samar Mohamed Hussein Shukry
Date of birth	: 15/07/1990
Place of birth	: Cairo
Last academic degree	: Bachelor of Science
Field of specialization	: Electrical Engineering
University issued the degree	: Ain Shams University
Date of issued degree	: June 2013
Current job	: Teaching Assistant in GUC

Thesis Summary

The increasing cost of IC fabrication and the ever-shrinking transistor size forces IC Industry to move its fabrication facilities to cheaper less reliable foreign sources. SOC designers and IP producers started to adopt the trending technology of IP-Reuse to optimize the design cycle concerning its cost and time-to-market.

Reusing of IP blocks might involve the resources of untrusted third-parties and hence creating the chance of inserting malicious manipulations namely Hardware Trojans at different phases of the design cycle. These Trojans are becoming a real challenge to the IC industry. Hardware Trojans are intended manipulative inclusions that might change the infected design's functionality and specifications, leak sensitive information about its power consumption, delay timing, area constraints, or radiation profile, or degrades its performance. Trojans threaten the authenticity of the design; they jeopardize the interests of clients who invest a lot of money to purchase creditable products.

Fragile watermarking is a process of embedding a signature that is extremely sensitive to any minor design alterations, which makes it an excellent choice to confront the malicious attacks of intentional tampering including the deceitful structures of Hardware Trojans. Yet, fragile watermarks should be robust in the sense that they are resistant to any trial of detecting or removing in order to be dependable in authenticating the IP designs.

In our thesis, we propose a behavioral fragile IP watermarking technique that coincides the signature in hierarchical finite state machines (HFSM) transitions. Our proposed watermarking tool is considered a type of HDL analysis which is a presilicon Trojan detection approach that deals with the design at the RTL abstraction level described in VHDL or Verilog codes; it targets the Trojans embedded in the state machine of the design under test in form of altered input/output functions or manipulated transitions. We propose to insert our fragile watermark in the state machine controller of the design since it visualizes the operational flow of the system and hence any Trojan inserted there, is sufficient to alter the function of the whole design.

Chapter 1

In this chapter, we clearly display the objective of our research and the motivation behind why we chose to study this topic in particular; Our motive is derived by the major threat of Hardware Trojans and their impact on threatening the authenticity and creditability of Hardware IP designs. We demonstrate a full taxonomy of different Trojan classes inserted at any phase of the design cycle and propose a Fragile Dynamic FSM Coinciding Transitions approach as an effective Hardware Trojan detection technique.

Chapter 2

This chapter presents an overview on the state-of-the-art of different FSM watermarking techniques illustrating the advantages and disadvantages of each.

Chapter 3

We will demonstrate our fragile watermarking algorithm in form of a flowchart followed by a detailed explanation of each step within all the watermarking phases of generation, insertion, and extraction. Our tool will be tested on various examples of KISS2 files of traditional FSMs via simulations to clarify its implementation.

Chapter 4

We introduce the concept of hierarchical state machines (HSM) and clarify the modifications that were implemented on our watermarking approach presented in Chapter 3 to be applicable on more complex hierarchical designs with different concurrent and communicating modules. The flow chart of our new hierarchical watermarking design will be presented and the changed framework will be thoroughly interpreted.

Chapter 5

Different Trojan detection techniques are displayed through countermeasure taxonomy and a comparison is set up to evaluate our approach based on some important design's constraints including delay, area, and power consumption. The sensitivity of our proposed watermarking algorithm is tested against different attack scenarios to check its robustness confronting the minimal Trojan manipulations.

Chapter 6

We will conclude our thesis and present our future work.

Key words: SOC, Tampering Protection, Hardware Trojan Detection, Fragile Watermarking, HSM.

Acknowledgment

First and foremost, my deep gratefulness and indebtedness is to *Allah*, the Most Gracious and the Most Merciful.

I would like to express my deepest appreciation and respect to *Prof, Dr. Mohamed Dessouky*, Professor of Electronics, Faculty of Engineering-Ain Shams University, for his priceless effort, generous guidance, and patience.

I am grateful to *Assoc. Prof, Dr. Amr Talaat Abdel-Hamid*, Associate Professor of Electronics, Faculty of Information Engineering and Technology-German University in Cairo, for being a great mentor who never spared an effort in guiding me, and for his valuable encouragement, endless patience, and continuous support.

Lastly and not least, I send my deepest love and appreciation to my beloved parents who are always there for me, my precious sister who stood by my side all the time, and my dearest friends who surrounded me with their sincere care and support.

Abstract

The productivity growth rate in IC Industry is the number of transistors produced per person per month, cannot keep up with the rate the SOC design complexity level increases. Thus, the gap between them becomes wider as time passes. The re-use of pre-validated IP designs helps to reduce this gap and thus provides a solution to shorten the time-to-market and optimize its manufacturing cost. SOC developers use products provided by different facilities that may involve unreliable resources, thereby compromising the security of the product and exposing it to Trojans.

Hardware Trojans (HT) are intentional modifications that are included in the original design to manipulate the intended function of its circuitry. In addition, Trojans can control, disable, monitor, or modify the whole design operational flow. Trojan may leak sensitive information about the original design, reduce its performance, block it, or even worse shut it down completely. Trojans are a real challenge for the IC industry as they threaten the interests of SOC manufacturers as well as customers who invest a lot of money to buy genuine products. Many defensive techniques have been applied to combat the severe impact of Trojans through detection, protection, and prevention.

In our thesis, we propose using a Fragile HFSM Watermarking technique, which is very sensitive to any minor change that may occur in the HFSM design of the original system for Trojan detection and hardware design authentication. We have chosen to add the watermark in the design’s hierarchical state machines because they are usually responsible for controlling the functional operation of the whole system and any Trojan alters them, can easily take control over vital design units. Our work illustrates the three phases of the proposed technique, including the processes of generating, inserting, and extracting the watermark. We also evaluated the performance of our proposed technique concerning its impact on the original design's power consumption, delay time, area constraints. In addition, we tested the sensitivity of our approach towards minor Trojan attacks in form of random manipulative insertions in the original HFSM design. Finally, a review of the various Trojan detection techniques is performed to show the pros and cons of our proposed framework.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3PIP	Third Party Intellectual Property
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
CAD	Computer-Aided Design
COTS	Commercial Off-The-Shelf
CRC	Cyclic Redundancy Check
CSFSM	Completely Specified Finite State Machine
CUT	Circuit Under Test
DFT	Design For Testability
DSP	Digital Signal Processing
DUT	Design Under Test
EDA	Electronic Design Automation
EPIC	Ending Piracy of Integrated Circuit
FIR	Finite Impulse Response
FSM	Finite State Machine
GDSII	Geometrical Data Base Standard for Information Interchange
HDL	Hardware Description Language
HSM	Hierarchal State Machine
HT	Hardware Trojan
IC	Integrated Circuit
IoT	Internet of Things
IP	Intellectual Property
IPP	Intellectual Property Protection
ISFSM	Incomplete Specified Finite State Machine
KISS	Keep It Stupid Simple
MD5	Message Digest

NP	Nondeterministic Polynomial
PCB	Printed Circuit Board
RE	Reverse Engineering
RFID	Radio Frequency Identification Device
RTL	Register Transfer Level
SOC	System On Chip
STG	State Transition Graph
VHDL	Very High Speed Integrated Circuit Hardware Description Language
VSI	Virtual Socket Interface
WCG	Watermark Circuit Generator