AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Department of Computer and Systems Engineering

Obfuscation of Digital Systems using Isomorphic Cells and Split Fabrication

A Thesis submitted in partial fulfillment of the requirements of
the Master of Science Degree in Computer and Systems Engineering
Department of Computer and Systems Engineering

by

Mohamad Ahmad AbdelAziz Ibrahim Masoud
Bachelor of Science in Computer and Systems Engineering
Department of Computer and Systems Engineering
Faculty of Engineering, Ain Shams University, 2014

Supervised By

Prof. Dr. Mohamed Watheq Ali Kamel El-Kharashi
Dr. Yousra Mohsen Alkabani

Cairo, 2019

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Department of Computer and Systems Engineering

Obfuscation of Digital Systems Using Isomorphic Cells and Split Fabrication

by

Mohamad Ahmad AbdelAziz Ibrahim Masoud
Bachelor of Science in Computer and Systems Engineering
Department of Computer and Systems Engineering
Faculty of Engineering, Ain Shams University, 2014

Examiners' Committee

Name and affiliation	**Signature**
Prof. Dr. Khaled Ali Hefnawy Shehata Professor at Electronics and Communications Engineering College of Engineering and Technology Arab Academy for Science and Technology and Maritime Transport – Heliopolis, Cairo Branch	.....
Prof. Dr. Mohamed Amin Dessouky Professor at Electronics and Communications Engineering Faculty of Engineering, Ain Shams University	.....
Prof. Dr. Mohamed Watheq Ali Kamel El-Kharashi Professor at Computer and Systems Engineering Faculty of Engineering, Ain Shams University	.....

Date:dd Month yyyy

Statement

This thesis is submitted as a partial fulfillment of the Master of Science degree 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.

Mohamad Ahmad AbdelAziz Ibrahim Masoud
Mohamad AbdelAziz

.....

Date: 15 March 2019

Researcher Data

Name: Mohamad Ahmad AbdelAziz Ibrahim Masoud
Date of Birth: 11/01/1993
Place of Birth: Cairo, Egypt
Last academic degree: Bachelor of Science
Field of specialization: Computer and Systems Engineering
University issued the degree : Ain Shams University
Date of issued degree : 2014
Current job : Senior Embedded Software Engineer at eJad

Abstract

Due to the difficulty for design houses to have their own foundries due to costs and complexity, most design houses tend to outsource the production of their chips to third-party foundries. This could lead to piracy, the insertion of hardware trojans, unauthorized production and usage of chips, as well as other undesired side effects in case the foundries are untrustworthy. It is, therefore, necessary to protect designs against such malicious attempts, while maintaining the design secrets of third-party foundries.

In this study, we reuse the concepts of split fabrication and isomorphic cells to introduce an algorithm for protecting hardware designs against malicious attacks at foundries. Split fabrication aims at splitting designs into two or more different parts that could be designed separately. One of the parts is relatively simple, and could be implemented by a relatively less advanced foundry, which needs to be trusted, and the other part contains the main functionality and usually needs to be implemented by an advanced foundry that is not necessarily trusted.

We combine split fabrication with isomorphic cells, which are generic logic cells that could implement any functionality based on their connections. Split fabrication is applied by disconnecting some vital wires that define the functionality of isomorphic cells, and these connections could be connected later by a trusted foundry.

Experimental results show improvements in security based on several concepts and metrics we introduce in this thesis, and based on other concepts we reuse from recent related work.

Summary

This thesis tackles the problem of hardware security, which has gained increasing attention recently. Due to the difficulty of having their own foundries, most design houses tend to outsource the production of their chips to third-party foundries, which could be untrusted. This could lead to undesired side effects like reverse engineering, piracy, and hardware trojans. Therefore, it is necessary to find ways of protecting IPs (Intellectual Properties) against such malicious attacks.

In this thesis, we contributed to this field by proposing an algorithm for replacing critical gates in designs with generic isomorphic cells that could be configured by a trusted foundry to implement a specific functionality in order to obfuscate designs at advanced foundries which could be untrusted. By combining isomorphic cells and split fabrication, it is more difficult for third parties to achieve any potential malicious goals.

The thesis is split down into six chapters as follows:

Chapter 1 Introduces the problem being studied. Also, we discuss the motivation of this work, and the intended objectives. This chapter also serves as a detailed introduction to the thesis, including a roadmap to the remaining parts.

Chapter 2 summarizes lots of research that has been done into the field of hardware security. The main focus of the mentioned related research is Hardware Trojans, split fabrication, malicious attacks on integrated circuits, protection techniques, and other relevant topics.

Chapter 3 provides a detailed theoretical background. We discuss several concepts reused from recent related work, such an Entropy, Isomorphic Cells, Optimized Isomorphic Cells, and Split Fabrication. We also introduce several new concepts and metrics such as Isomorphic Entropy, Cluster Normalization, Gate Normalization, Cluster Forms, and Truth Table Inclination. All of these concepts serve as a basis for the algorithm we introduce in this work.

Chapter 4 discusses the algorithm at the core of this thesis. The algorithm aims at analysing the effect of each gate on the signal probability of a certain connected cluster of gates. Afterwards, the gates with the highest impact on a design based on several configurable parameters are replaced with isomorphic cells. In this chapter, we discuss our proposed algorithm in detail, including a pseudo code for making things easier.

Chapter 5 provides some information on the designs used as test cases for our algorithm as well as detailed experimental results for each of them. For the scope of this work, we chose several Verilog-based designs as test cases, some of which were implemented by us, and others were reused from other sources. The experimental results include several different metrics for measuring the effect of replacing gates with isomorphic cells based on several configuration parameters. By tuning the configuration parameters, it is possible to get different results, and we provide some examples on this. We also provide some details on the environment setup and the tools used to implement our algorithm.

Chapter 6 summarizes the thesis, including the most important points, and provides hints for potential future work.

Keywords: Hardware Security, Split Fabricaton, Obfuscation, Digital Systems, Foundries, Isomorphic Gates, Reverse Engineering, Piracy.

Acknowledgment

I thank Allah for granting me the will and knowledge to get this work done, for without His blessings, I doubt I could have completed this study.

To my supervisors, Prof. Dr. Mohamed Watheq Ali Kamel El-Kharashi and Dr. Yousra Mohsen Alkabani, I thank you for your continuous support and patience, and for your guidance throughout my journey towards my master's degree.

I would like to thank my parents and sisters for their constant support, and for waiting patiently for this moment.

Finally, I would like to thank my wife for being there for me, and for pushing me forward and giving me enough support to get through this.

Mohamad Ahmad AbdelAziz Ibrahim Masoud
Department of Computers and Systems Engineering
Faculty of Engineering
Ain Shams University
Cairo, Egypt
March 2019

Contents