

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

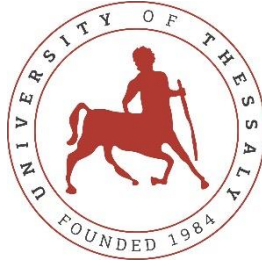
HARDWARE TROJAN DETECTION, USING PATH DELAY FINGERPRINTING.

Diploma Thesis

Paschoudis Athanasios

Supervisor: Stamoulis Georgios

September 2023



UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

HARDWARE TROJAN DETECTION, USING PATH DELAY FINGERPRINTING.

Diploma Thesis

Paschoudis Athanasios

Supervisor: Stamoulis Georgios

September 2023



ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

**ΕΥΡΕΣΗ ΚΑΚΟΒΟΥΛΟΥ ΥΛΙΚΟΥ, ΜΕ ΤΗ ΧΡΗΣΗ
ΑΠΟΤΥΠΩΜΑΤΟΣ ΚΑΘΥΣΤΕΡΗΣΗΣ ΜΟΝΟΠΑΤΙΟΥ.**

Διπλωματική Εργασία

Πασχούδης Αθανάσιος

Επιβλέπων: Σταμούλης Γεώργιος

Σεπτέμβριος 2023

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων

Σταμούλης Γεώργιος

Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών
Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

Μέλος

Σωτηρίου Χρήστος

Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών
Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

Μέλος

Πλέσσας Φώτιος

Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών
Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

Dedicated to Nala

With much love

Acknowledgements

I would like to extend my heartfelt gratitude to a number of people who have been conducive in the completion of this diploma thesis. Foremost, I want to express my deepest appreciation to my family, my father Lazaros, my mother Anna Maria and my sister Evangelia, for their unwavering support, encouragement, and love. I'm deeply grateful to my advisor Professor Stamoulis Georgios, for all the inspiration, his invaluable guidance and expertise in the field of Hardware Security. My gratitude extends to Professors Sotiriou Christos and Plessas Fotios. The supportive academic atmosphere at the Technical University of Thessaly and the provided resources has been essential. I'm thankful for my friends, your moral support have been a tremendous source of encouragement. Last but not least, special thanks to my dog Nala, whose companionship has been a comforting presence throughout this endeavor.

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

Being fully aware of the implications of copyright laws, I expressly state that this diploma thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The Declarant

Paschoudis Athanasios

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελούν αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλουν οποιασδήποτε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχουν έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο Δηλών

Πασχούδης Αθανάσιος

Hardware Trojan Detection, using Path Delay Fingerprinting.

Paschoudis athanasios

Abstract

Both the integration and the increasing complexity of modern integrated circuits (ICs) have brought about new challenges in ensuring the security and reliability of these electronic systems. Hardware Trojans, malicious alterations inserted during fabrication or design phases, pose a significant threat to the functionality and integrity of these ICs. This thesis aims to give an explanatory approach of Path Delay Fingerprinting by leveraging a comparative review to other existing Trojan detection techniques. The proposed methodology harnesses the unique delay signatures of critical paths within ICs to identify the presence of Hardware Trojans, contributing to enhanced system security and trustworthiness.

Keywords:

Integrated circuits, security, reliability, electronic systems, Hardware Trojans, malicious alterations, insert, threat, functional, integrity, detection, approach, path delay fingerprint, analysis, method, paths, IC, trustworthiness

Εύρεση κακόβουλου υλικού, με τη χρήση αποτυπώματος καθυστέρησης μονοπατιού.

Πασχούδης Αθανάσιος

Περίληψη

Η ανάγκη ενσωμάτωσης καθώς και η αυξανόμενη πολυπλοκότητα των σύγχρονων ολοκληρωμένων κυκλωμάτων (ICs), έχουν επιφέρει νέες προκλήσεις στην εξασφάλιση της αξιοπιστίας και της ασφάλειας αυτών των ηλεκτρονικών συστημάτων. Ιδιαίτερη απειλή στην λειτουργικότητα και γενικότερα στην ακεραιότητα των ολοκληρωμένων κυκλωμάτων (ICs) έρχονται να προσδώσουν τα Hardware Trojans. Τμήματα κακόβουλης αλλαγής σε σημεία υλικού, τα οποία εισέρχονται από κάποιον εχθρό στο σύστημα κατά τη διαδικασία της κατασκευής ή της σχεδιαστικής διαδικασίας των κυκλωμάτων. Η διπλωματική αυτή εργασία, αποσκοπεί στην επεξηγηματική προσέγγιση, της μεθοδολογία αποτυπώματος καθυστέρησης μονοπατιού, παρουσιάζοντας μια συγκριτική ανασκόπηση μεταξύ άλλων βασικών τεχνικών ανίχνευσης κακόβουλου υλικού. Η προτεινόμενη αυτή τεχνική αξιοποιεί το μοναδικό αποτύπωμα καθυστέρησης των κρίσιμων μονοπατιών εντός των κυκλωμάτων ICs προκειμένου να εξακριβώσουν πιθανή ύπαρξη κακόβουλου υλικού. Συνεισφέροντας έτσι στην εξασφάλιση ασφαλών και αξιόπιστων συστημάτων.

Λέξεις-κλειδιά:

Ολοκληρωμένα κυκλώματα, αξιοπιστία, ασφάλεια, λειτουργικότητα, ακεραιότητα, εισχώρηση, εχθρός, ανίχνευση, ανάλυση, κακόβουλο υλικό, αποτύπωμα καθυστέρησης μονοπατιού

Table of Contents

Acknowledgements	vi
Abstract	ix
Περίληψη.....	x
Table of Contents	xi
List of Figures	xvi
List of Tables	xvii
List of Abbreviations.....	xviii
CHAPTER 1 INTRODUCTION	1
1.1 Subject of Diploma Thesis	1
1.2 Chapters Organization.....	1
CHAPTER 2 CONCEPTUAL OVERVIEW	3
2.1 Historical Review of Hardware Security, First Attacks and the Need for Prevention	3
2.2 Integrated Circuits (ICs)	4
2.3 Hardware Trojans: Definition, Types, and Impact.....	5
2.3.1 Hardware Trojan Structure	5
2.3.2 Hardware Trojan's Payload	5
2.3.3 Hardware Trojan's Trigger	6
2.3.4 Hardware Trojan Classification	7
CHAPTER 3 HARDWARE TROJAN DETECTION TECHNIQUES.....	9
3.1 Main Attributes and Classification	9
3.2 Side-Channel Detection Techniques.....	10
3.3 Invasive Detection Techniques	10
3.4 Running-Time Detection Techniques	11
3.5 Testing Based Detection Techniques.....	11

3.6 Existing Approaches	12
3.6.1 Utilizing Ring Oscillators for Hardware Trojan Detection	12
3.6.2 Chemical De-layering for Hardware Trojan Detection	13
3.6.3 Visual Inspection for Hardware Trojan Detection	14
3.6.4 Thermal Mapping for Hardware Trojan Detection	15
CHAPTER 4 PATH DELAY FINGERPRINT	20
4.1 Main features	20
4.1.1 Path Delays, Measurements tools and Methodology	20
4.1.2 Applications, Limitations and Future Scope	21
4.2 Case Study 1: Delay Calculation	21
4.3 Case Study 2: Detection of various embedded Trojans	23
4.3.1 Near-input Trojan	24
4.3.2 Near-middle-stage Trojan	24
4.3.3 Near-output Trojan	25
4.3.4 Counter-based Trojan	26
4.3.5 Case Conclusions	26
4.4 Path Delay for IP authentication	27
4.4.1 Clock Glitch Operation	27
4.4.2 Challenges and Limitations	27
CHAPTER 5 COMPARATIVE ANALYSIS	28
5.1 Comparison Set-Up	28
5.1.1 Criteria for Comparison	28
5.1.2 Clarification of Concepts	29
5.2 Path Delay Fingerprint, Key Criteria	31
5.2.1 Detection Accuracy	31
5.2.2 Computational Complexity	31
5.2.3 Scalability	31
5.2.4 Intrusiveness	31
5.2.5 Cost and Time-Efficiency	31
5.2.6 Applicability	31
5.2.7 False Positives Factors	32
5.2.8 False Negatives Factors	32
5.3 Invasive Detection Techniques, Key Criteria	33

5.3.1 Detection Accuracy	33
5.3.2 Computational Complexity	33
5.3.3 Scalability	33
5.3.4 Intrusiveness	33
5.3.5 Cost and Time-Efficiency	33
5.3.6 Applicability	33
5.3.7 False Positives Factors	33
5.3.8 False Negatives Factors	34
5.3.9 Summary and Conclusion	35
5.4 Running Time Detection Techniques, Key Criteria	35
5.4.1 Detection Accuracy	35
5.4.2 Computational Complexity	35
5.4.3 Scalability	35
5.4.4 Intrusiveness	36
5.4.5 Cost and Time-Efficiency	36
5.4.6 Applicability	36
5.4.7 False Positives Factors	36
5.4.8 False Negatives Factors	36
5.4.9 Summary and Conclusion	37
5.5 Testing Based Detection Techniques, Key Criteria	38
5.5.1 Detection Accuracy	38
5.5.2 Computational Complexity	38
5.5.3 Scalability	38
5.5.4 Intrusiveness	38
5.5.5 Cost and Time-Efficiency	38
5.5.6 Applicability	38
5.5.7 False Positives Factors	38
5.5.8 False Negatives Factors	39
5.5.9 Summary and Conclusion	40
5.6 Ring-Oscillator Based Trojan Detection Techniques, Key Criteria	40
5.6.1 Detection Accuracy	40
5.6.2 Computational Complexity	40
5.6.3 Scalability	40
5.6.4 Intrusiveness	41
5.6.5 Cost and Time-Efficiency	41
5.6.6 Applicability	41

5.6.7 False Positives Factors	41
5.6.8 False Negatives Factors.....	41
5.6.9 Summary and Conclusion	42
5.7 Chemical De-layering Methods, Key Criteria	43
5.7.1 Detection Accuracy	43
5.7.2 Computational Complexity	43
5.7.3 Scalability	43
5.7.4 Intrusiveness	43
5.7.5 Cost and Time-Efficiency.....	43
5.7.6 Applicability	43
5.7.7 False Positives Factors	43
5.7.8 False Negatives Factors.....	44
5.7.9 Summary and Conclusion	45
5.8 Visual Inspection Based Detection Techniques, Key Criteria	45
5.8.1 Detection Accuracy	45
5.8.2 Computational Complexity	45
5.8.3 Scalability	45
5.8.4 Intrusiveness	46
5.8.5 Cost and Time-Efficiency.....	46
5.8.6 Applicability	46
5.8.7 False Positives Factors	46
5.8.8 False Negatives Factors.....	46
5.8.9 Summary and Comparison Conclusion	47
5.9 Side-channel Thermal Analysis, Key Criteria.....	48
5.9.1 Detection Accuracy	48
5.9.2 Computational Complexity	48
5.9.3 Scalability	48
5.9.4 Intrusiveness	48
5.9.5 Cost and Time-Efficiency.....	48
5.9.6 Applicability	48
5.9.7 False Positives Factors	48
5.9.8 False Negatives Factors.....	49
5.9.9 Summary and Conclusion	50
5.10 Analysis Observations	50
CHAPTER 6 CONCLUSION	52

6.1 Final Conclusion	52
6.2 Future expansions.....	53
References	54

List of Figures

FIGURE 2.1: Trigger and Payload Hardware Trojan example [7].....	5
FIGURE 2.2: Trojans Impact in a VLSI design flow [10].....	8
FIGURE 3.1: The layout of the Circuit under Test and the GDSII layout of the fabricated chip [7].....	15
FIGURE 3.2: Thermal maps from both a golden circuit and an externalized Trojan infected circuit [19].....	17
FIGURE 3.3: Thermal maps from both a golden circuit and a circuit infected by a well-hidden hardware Trojan [19].....	18
FIGURE 3.4: Obtained Thermal Maps [19]	19
FIGURE 4.1: Example of delay calculation [21].....	22
FIGURE 4.2: A Trojan-free circuit and the same circuit with hardware Trojan inserted in [21].....	23
FIGURE 4.3: Delay Comparison of a near-input Trojan [9].....	24
FIGURE 4.4: Delay Comparison of a middle-stage Trojan [9].....	25
FIGURE 4.5: Delay Comparison of a near-output Trojan [9]	25
FIGURE 4.6: Delay Comparison of 4-bit counter-based Trojan [9].....	26

List of Tables

TABLE 5.1: Sample of Scalable Standards for Measurements	30
TABLE 5.2: Criteria of Comparison for Path Delay Fingerprint.....	32
TABLE 5.3: Criteria of Comparison for Invasive Detection Techniques.....	34
TABLE 5.4: Criteria of Comparison for Running Time Detection Techniques	37
TABLE 5.5: Criteria of Comparison for Testing Based Detection Techniques	39
TABLE 5.6: Criteria of Comparison for Ring-Oscillator Based Detection Techniques	42
TABLE 5.7: Criteria of Comparison for Chemical De-layering Detection Techniques	44
TABLE 5.8: Criteria of Comparison for Visual Inspection Based Detection Techniques	47
TABLE 5.9: Criteria of Comparison for Thermal Analysis	49
TABLE 5.10: Summarized Comparison for Trojan Detection Techniques	51

List of Abbreviations

HT	Hardware Trojan
IC	Integrated Circuit
OS	Operating System
TPM	Trusted Platform Module
HSM	Hardware Security Module
IOT	Internet of Things
CMOS	Complementary Metal Oxide Semiconductor
PMOS	P-channel Metal Oxide Semiconductor
NMOS	N-channel Metal Oxide Semiconductor
GC	Golden Chip
SCA	Side Channel Analysis
PCA	Principal Component Analysis
RTL	Register Transfer Level
IP	Intellectual Property
FSM	Finite State Machine
SEM	Scanning Electron Microscopy
SOM	Scanning Optical Microscopy
PICA	Pico-second Imaging Circuit Analysis
DC	Direct Current
AES	Advanced Encryption Standard
ATPG	Automatic Test Pattern Generation
FPGA	Field Programmable Gate Array
SOC	System on Chips

LIBST	Logic Built-In Self-Test
TDC	Time-to-Digital Converter

CHAPTER 1 INTRODUCTION

The worldwide phenomenon of manufacturing solid and trusted ICs is on top of the topics, since all the factories in order to reduce the cost starts moving worldwide. Constructors, in order to make cheaper and more simplified ICs for substitutability purposes, start increasing unused free space by using more gates. Since then, hackers operation becomes easier, while they can embed hardware Trojans into circuits without affecting the whole chip construction. Therefore, the need for robust and reliable Hardware Trojan detection techniques has never been more imperative.

1.1 Subject of Diploma Thesis

The objective of this thesis is to provide a comprehensive overview of Hardware Trojan detection methods, focusing on their significance in the broader context of hardware security. Special emphasis will be placed on Path Delay Fingerprinting, a technique that offers unique advantages and challenges. The suggested technique, utilizes the distinct delay characteristics found in essential routes within integrated circuits, to pinpoint the existence of Hardware Trojans, thereby elevating the security and reliability of the system. The thesis will also present a theoretical comparison between Path Delay Fingerprinting and other prevalent methods, aiming to provide a nuanced understanding of its relative strengths and weaknesses.

1.2 Chapters Organization

In CHAPTER 1 there is the main introduction to the subject, contextual information about hardware security and the need for Trojans detection. Description of the problem this thesis aims to address, accompanied by the general structure of the Thesis.

CHAPTER 2 provides the background review and the main concepts that are critical for the subject clarification, such ICs fundamentals and basic principles about Hardware Trojans.

CHAPTER 3 examines existing detection methods for Hardware Trojans.

While CHAPTER 4 dives deeper in Path delay fingerprinting, case studies and real world scenarios.

CHAPTER 5 presents a critical examination in a theoretical comparison between Path Delay Fingerprinting and other methods.

Finally CHAPTER 6 gives the conclusion accompanied with observations. Also highlights the need for future work and provides proposals to extend security.

CHAPTER 2 CONCEPTUAL OVERVIEW

2.1 Historical Review of Hardware Security, First Attacks and the Need for Prevention

The evolution of hardware security has been a journey marked by innovation, challenges, and a constant battle against emerging threats. As the complexity of hardware systems has increased, so too has the sophistication of attacks targeting them.

In the early days of computing, hardware security was not a primary concern. Computers were large, expensive, and confined to specialized environments, making physical access to these systems difficult. However, as technology advanced and computers became more accessible, the need for hardware security became evident.

The late 1970s and early 1980s marked a turning point in the history of hardware security. One of the first recorded hardware attacks was the "van Eck phreaking," a form of eavesdropping, where electromagnetic emissions from a device were captured, to reconstruct the data being processed. This attack demonstrated that hardware could be vulnerable to unauthorized data extraction without direct physical access. [1]

Another seminal event was the discovery of hardware Trojans, malicious alterations to hardware components that could compromise the integrity and confidentiality of a system. These early attacks served as a wake-up call for the industry, highlighting the urgent need for robust hardware security measures. [2]

The initial attacks led to a paradigm shift in how hardware security was perceived. No longer could hardware be considered an impenetrable fortress but it was now a potential point of failure that required as much attention as software vulnerabilities.

The late 1990s and early 2000s saw a surge in hardware security research. Academia and industry began to collaborate on developing techniques for hardware encryption, secure boot processes, and hardware-based authentication. The introduction of Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs) marked significant milestones in the journey toward secure hardware systems.

As hardware attacks have evolved, so too has the need for preventive measures. The cost of hardware attacks can be astronomical, not just in terms of financial loss but also in the erosion of consumer trust and brand reputation.

Traditionally, hardware security has been reactive, addressing vulnerabilities as they are discovered. However, this approach is no longer sufficient. Proactive measures, such as hardware attestation and real-time monitoring of hardware behavior, are becoming increasingly important.

The history of hardware security is a testament to the ever-changing landscape of technological threats and the measures taken to counter them. From the first attacks that shook the industry to the current state of constant vigilance, the need for robust hardware security has never been greater. As we move into an era of ubiquitous computing and the Internet of Things (IOT), the lessons learned from history will be invaluable in shaping a secure future for hardware systems.

2.2 Integrated Circuits (ICs)

Integrated Circuits, commonly known as ICs or microchips, are assemblies of electronic components such as transistors, resistors, and capacitors, fabricated on a semiconductor wafer. They serve as the backbone of almost all electronic devices, from simple calculators to complex computer systems. [3]

Complementary Metal-Oxide-Semiconductor (CMOS) is the most widely used technology for designing ICs. It uses both PMOS and NMOS transistors to create digital logic circuits, offering the advantage of low power consumption. [4]

ICs implement digital logic through a series of logic gates like AND, OR, NOT, etc. These gates are the building blocks of more complex functions and algorithms. [5]

ICs are not just functional units but also potential targets for hardware-based attacks, including Hardware Trojans. Understanding their architecture and operation is crucial for developing effective security measures. [2]

Integrated Circuits are the cornerstone of modern electronics and by extension of hardware security. A deep understanding of ICs is essential for anyone venturing into the field of Hardware Trojan detection and other hardware security domains. [6]

2.3 Hardware Trojans: Definition, Types, and Impact

A Hardware Trojan is a malicious circuit which is made by someone who want to harm a system. So the attacker implemented them, in target's hardware in order to benefit with its utilities.

2.3.1 Hardware Trojan Structure

Every Hardware Trojan consists of both the payload and the trigger. In FIGURE 2.1 we provide the main structure of a Trojan depending on those characteristics.

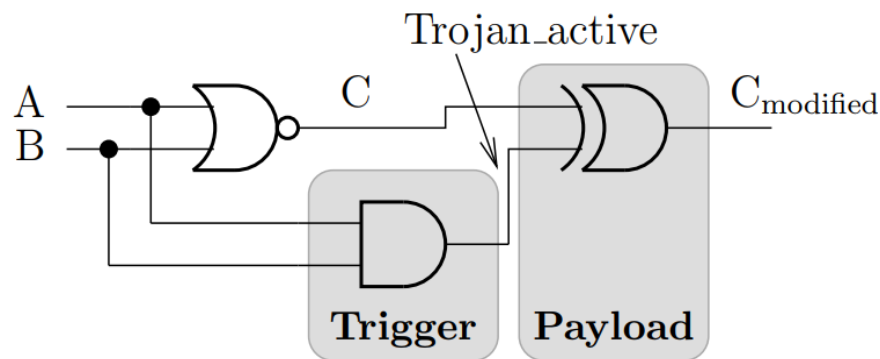


FIGURE 2.1: Trigger and Payload Hardware Trojan example [7]

2.3.2 Hardware Trojan's Payload

Every Hardware Trojan must carry a payload. The payload of a Hardware Trojan refers to the specific malicious function or operation that the Trojan is designed to execute once

activated. The payload is the actual adverse effect that compromises the system's integrity, confidentiality, or availability. [8]

More in depth, a case of Hardware Trojan's payload is to ruin a whole chip. In this case it is very hard for the Trojan to be located during an examination, even more to determine if there is any Trojan at all. That happens while Hardware Trojans aren't active during a testing process, meaning that they don't harm any chip. Actually that wouldn't happen, if the examination process time lasts longer than the Hardware Trojan's sleeping time. [8]

Another payload case is to corrupt the circuit functions. Like replacing some high important information the attacker want to insert, with the plaintext's preset values, while the plaintext will be still shown as the first reasonable one to the victim. This technique is very dangerous especially for military controlling systems, like missile attacking systems, anti-aircraft systems etc. Any attacker of this range, can use for example a location value or a command the victim want to use, as an misleading that will still be shown to the victim in the plaintext, while the attacker's Trojan will have actually change this value with another location or command. So a plaintext: <<activate rockets targeting enemy aircraft>> will actually have changed to <<activate rockets targeting team aircraft>>. [8]

Moreover a Hardware Trojan payload is to relay to the attacker sensitive data with signals form, like an encryption key etc. More specific since the Trojan is triggered, the cipher text along with the encryption key will be transmitted by a transmission channel from which the attacker can get the encryption key and so harm the system. [8]

2.3.3 Hardware Trojan's Trigger

Despite the payload, every Hardware Trojan got a trigger point which activates the Trojan. Thus Trojans also classified according to that. Every Trojan trigger has a special principle relying design, in order to prevent any functional examine to track it. Such as using counter after a long time, undefined input sequences etc. Hardware Trojans can also split into several categories according to their triggers. [8]

The Trojans can be triggered autonomously by a counter, a specific input or other signal alteration. This method is useful when the attacker hasn't any access at the target device. However, the Trojan has got already its own activation rule, as an example some kind of an internal counter. An internal counter like that could counts the times for a function to be executed and while it exceeds the number of times the attacker had set, the Trojans must be trigger. [8]

The Trojans can be triggered by the attacker, while he can access the device and give a specific input. This method is quite hard to be revealed. Either an unused keyboard key or a complex string can be used as inputs in order to trigger the Trojan. Making thus, almost unlikely for a Trojan to be revealed, having in mind that there are vast different input variations. [8]

Finally, Trojans can be always activated, thus no trigger is needed. This method isn't so effective and can easily be revealed due to high power usage demanded, in order to be always activated. Then it requires, well-hidden payload, by using only undetectable ways to transmit the arcanum information. [8]

2.3.4 Hardware Trojan Classification

Dividing Trojans based on their own characteristics, increase the detection accuracy of them and reduce the cost, by choosing the most suitable detection method for each Trojan.

Depending on the payload we can split Hardware Trojans into both implicit payload Trojans and explicit payload Trojans. Implicit Payload Trojans are Hardware Trojans designed to subtly degrade system performance or reliability over time, without executing a specific malicious function. That kind of Trojans is more unlikely to be detected. These Trojans operate in a manner that makes their effects hard to distinguish from natural wear and tear or minor system glitches. Explicit Payload Trojans, on the other hand, are designed to execute a clearly defined malicious function when triggered. These Trojans have a specific, identifiable payload that directly compromises the system's security, such as leaking sensitive information or disabling certain functionalities.

Moreover we can classify Hardware Trojans by their insertion stage. The insertion stage can vary and it's separated into three cases. The Design Stage where Trojans are inserted during the ICs design. Moreover there is the fabrication stage where the Trojans are inserted during the manufacturing process. And last but not least the post fabrication stage where the Hardware Trojans are inserted after the IC has been manufactured but before it is deployed. [9]

In FIGURE 2.2, as it described in [10] we give you the potential impact in the abstraction level of a VLSI design flow, caused by a Hardware Trojan.

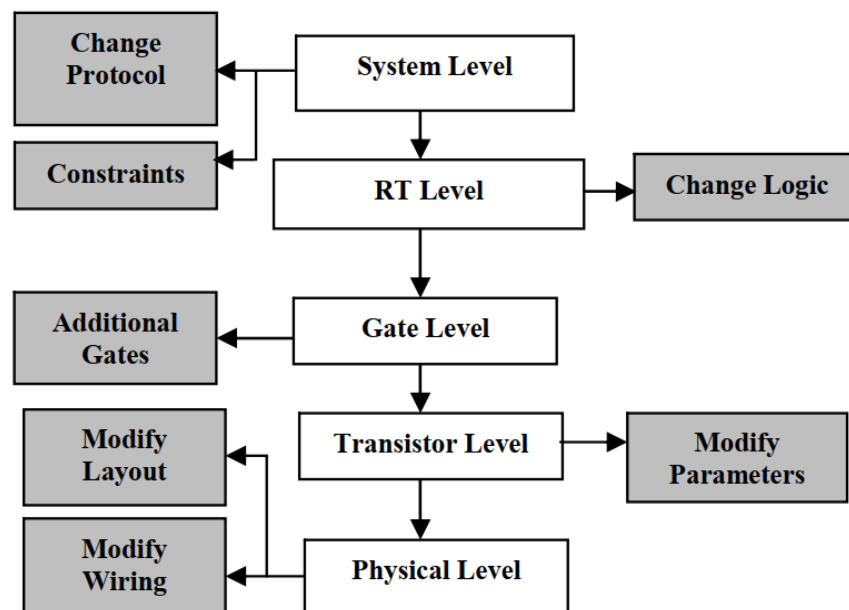


FIGURE 2.2: Trojans Impact in a VLSI design flow [10]

Last, we can classify Trojans by their activation type as we examined in more details at 2.3.3 . Activation type is divided into internal conditions such as a specific sequence of inputs and External conditions like a specific time or date. [9]

Understanding the categorization and classification of Hardware Trojans is crucial for developing effective detection methods, including the use of path delay fingerprinting, which is the focus of this thesis. [11]

CHAPTER 3 HARDWARE TROJAN DETECTION TECHNIQUES

3.1 Main Attributes and Classification

The primary focus of Hardware Trojan detection is to create approaches and instruments for identifying unauthorized changes in circuits. The detection methods can vary, as they are highly influenced by where the Trojan is inserted within the circuit. Various techniques such as logic testing, side channel analysis or reverse engineering may be employed depending on the specific type of Trojan being sought. To prevent Hardware Trojans, certain alterations are made to the circuit to make it challenging for unauthorized modifications to occur. Established methods include the state machine or using logic encoding. [12]

Given that Trojans differ substantially in activation methods, payload, and where they are inserted in the supply chain, a one-size-fits-all detection approach isn't feasible. Different detection methods are suited for different inputs and phases of deployment. Some methods, for example, only need the integrated circuit and its netlist for testing, while others call for a detailed layout description. Some even require a so-called "golden chip," a known Trojan-free version of the circuit under examination, although obtaining a fully reliable golden chip remains an unresolved issue. [12]

Detection methods can also be categorized based on the kind of action needed on the circuit being examined. Such methods can be grouped either into destructive or non-destructive types. For example, functional testing only involves the application of specific test vectors and is therefore non-destructive. In contrast, optical inspection, which involves the removal of chip layers, is considered destructive. [12]

Destructive techniques often involve physical alteration or dissection of the hardware, making them less feasible for real-world applications. Semi-destructive techniques, while less invasive, still involve some level of intrusion into the hardware architecture. Non-destructive methods are the most desirable as they allow for Trojan detection without altering the hardware. While hybrid techniques combine multiple methods, in order to

create more robust detection mechanisms. [13] The rest of the section elaborates on the most frequently used Hardware Trojan detection techniques.

3.2 Side-Channel Detection Techniques

A potent method for spotting unauthorized alterations in integrated circuits is Side-Channel Analysis (SCA). This approach contrasts a physical attribute (such as power usage, electromagnetic emissions, or time delays) of the test device with a benchmark circuit. As is often the case, a "golden circuit" (a verified, Trojan-free version of the circuit) is usually required for comparison. The researchers employed Principal Component Analysis (PCA) as the circuit's side-channel fingerprint to juxtapose it with the golden model. In the past, other physical metrics like leakage current, dynamic current or internal delays have also been used for detecting hardware Trojans. [12]

Side-channel analysis does not require activation of an unknown Trojan, succeeding thus significantly high detection coverage for all types of hardware Trojans.

Two primary constraints exist when using side-channel analysis for detecting Hardware Trojans. First, the physical attributes being measured could change due to factors other than the presence of a Trojan. For example, the power consumption fingerprint of a test circuit might vary from that of the golden circuit because of manufacturing inconsistencies. Second, the chosen physical trait may be difficult to measure accurately. For instance, obtaining the precise timing information needed for a particular circuit pathway can be challenging. [12]

3.3 Invasive Detection Techniques

Invasive approaches involve altering integrated circuit structures at the design phase, such as at the RTL or netlist levels, to prevent the embedding of Hardware Trojans. These methods can also reinforce post-manufacture detection techniques. When it comes to intellectual property (IP) protection, these strategies often involve designers intentionally

modifying the IPs. These deliberate modifications serve as a unique fingerprint to recognize the IP after it's been fabricated. Specifically, this fingerprint often takes the form of an extended Finite State Machine (FSM) that can be activated by particular inputs from the designer. While these invasive techniques can be challenging to implement in complex integrated circuits and may significantly increase costs, they aim to bypass conventional detection methods effectively. [12]

3.4 Running-Time Detection Techniques

Among non-destructive methods, some have been developed to identify hardware Trojans during the circuit's operational phase. These techniques are engineered alongside physical countermeasures. When a Trojan is spotted while the circuit is in use, efforts are made to circumvent the malicious component and maintain safe operation. This approach employs a combination of hardware and software for Trojan detection. [12]

A similar detection strategy named D.E.F.E.N.S.E (Design for Enabling Security), incorporates reconfigurable logic into the functional design to facilitate real-time security monitoring. [14]

Unlike testing time approaches, running time methods offer the advantage of continuous monitoring, making them highly effective in identifying Trojans, that are designed to activate under specific conditions or after a certain period." However, these methods can be costly in terms of the circuit area they occupy and may not be capable of detecting certain kinds of Trojans.

3.5 Testing Based Detection Techniques

Functional testing is commonly performed on a chip before it is shipped and can also serve to identify Hardware Trojans. However, a major challenge is selecting the appropriate test vectors, given that the Trojan to be detected is unknown. Various test patterns can be administered to an integrated circuit to monitor for any unusual

behavior, although only a select few will activate a hidden Trojan. Typically, Trojans have an extremely low likelihood of being activated, making it difficult for standard test patterns to trigger them. Consequently, research has been geared towards developing test methods that can effectively spot hardware Trojans. [12]

One advantage of this testing method is its non-invasive nature. Theoretically, it can also identify Trojans that were inserted at various stages of the design process, even those incorporated into the intellectual property (IP) itself. However, there's no certainty in finding the test vectors that will activate the Trojan, making the reliability of detection through functional testing somewhat uncertain. [12]

3.6 Existing Approaches

3.6.1 Utilizing Ring Oscillators for Hardware Trojan Detection

A ring oscillator is a type of electronic oscillator that consists of a number of NOT gates, or inverters, arranged in a loop. The output of the last inverter feeds back into the first, creating a continuous oscillatory behavior. A fundamental trait of ring oscillators is that they generate a frequency signal, the characteristics of which are highly sensitive to variations in the circuit, such as temperature, voltage, and even the presence of Hardware Trojans. [15]

When a Hardware Trojan is present in an IC, it generally introduces additional load or changes the characteristics of the circuit. These alterations can affect the oscillation frequency of a ring oscillator, thereby serving as an indicator of the Trojan's presence. By monitoring the frequency signals from ring oscillators embedded within or near the suspected circuitry, one can identify abnormal behaviors that signify the existence of a Trojan. [15]

The main procedure for Trojan Detection Using Ring Oscillators as follows. Firstly we have to measure the frequency signals of the embedded ring oscillators under controlled conditions. This serves as the baseline for future comparisons. Then once the IC is deployed, continuously monitor the frequency signals from the ring oscillators. Use real-

time analysis to compare these signals with the baseline measurements. If the frequency signal deviates from the baseline beyond a predefined threshold, flag it as an anomaly. This could be indicative of a Hardware Trojan. [15]

The main advantages of this method is that Ring oscillators are highly sensitive to any modifications in the circuit, making them effective for detecting even subtle changes that could be indicative of a Hardware Trojan. Compared to other Hardware Trojan detection methods, ring oscillators usually require less additional hardware, making them a cost-effective solution. The frequency signals from ring oscillators can be monitored in real-time, allowing for immediate detection and action in case of anomalies. Ring oscillators can be easily incorporated into existing IC designs, making them scalable for various applications and complexities.

Although there are some limitations using this method such the high sensitivity of ring oscillators can sometimes lead to false positives, flagging normal variations as anomalies. Conversely, highly sophisticated Trojans might evade detection. Meanwhile factors such as temperature and voltage fluctuations can also affect the frequency of ring oscillators, potentially complicating the interpretation of results. Moreover the continuous operation of ring oscillators consumes extra power, which could be a concern in low-power applications. While the data from ring oscillators may require sophisticated algorithms for accurate interpretation, adding to the computational overhead.

3.6.2 Chemical De-layering for Hardware Trojan Detection

Chemical De-layering involves the use of chemical solutions to remove the layers of an IC, exposing the underlying circuitry for analysis. This method is particularly useful for detecting Hardware Trojans that are embedded deep within the layers of an IC. [16] This technique involves the systematic removal of individual layers of the chip to expose its internal structure for detailed inspection.

For the Process of Chemical De-layering, the IC is firstly removed from its package, and any protective coatings are stripped away to expose the layers. Then chemical solvents such as hydrofluoric acid (HF) and nitric acid (HNO₃) are used to dissolve the silicon and

metal layers, one at a time, revealing thus the underlying circuitry. The choice of chemical depends on the material that needs to be removed. Once the layers are removed, optical or electron microscopy is used to examine the exposed circuitry for any anomalies indicative of Hardware Trojans. [17] More specific using non-invasive methods like X-ray imaging, the layers to be removed are identified and the chosen chemical solvent is carefully applied to the chip, while the process is closely monitored to ensure only the intended layer is removed. After each layer is removed, the exposed layer is inspected using techniques like Scanning Electron Microscopy (SEM), while the acquired data is analyzed to detect any anomalies that indicative a Hardware Trojan.

It is worth mentioning the main advantages and disadvantages. Since this method enables direct observation of the internal structure of an IC and it's capable of detecting Trojans embedded deep within the layers. While the process can take a considerable amount of time and cost, especially for complex ICs and the IC is rendered unusable after the process. [18]

3.6.3 Visual Inspection for Hardware Trojan Detection

Optical or visual inspection hinges on reverse engineering and uses advanced imaging acquisition and analytical methods, such as Scanning Optical Microscopy (SOM), Scanning Electron Microscopy (SEM), and pico-second imaging circuit analysis (PICA), to create photos of the chip under investigation. These images help reconstruct the chip's layout for comparison reasons against the designer's original layout. More in-depth reverse engineering could even recover the original netlist. Optical inspection is particularly effective for identifying Trojans introduced during fabrication, making it a potent method. FIGURE 3.1 outlines the basic concept of optical inspection, where the layout of the circuit under examination (displayed on the left) is compared against images of the fabricated circuit. These images are obtained by sequentially removing layers from the chip, essentially destroying it in the process. [12]

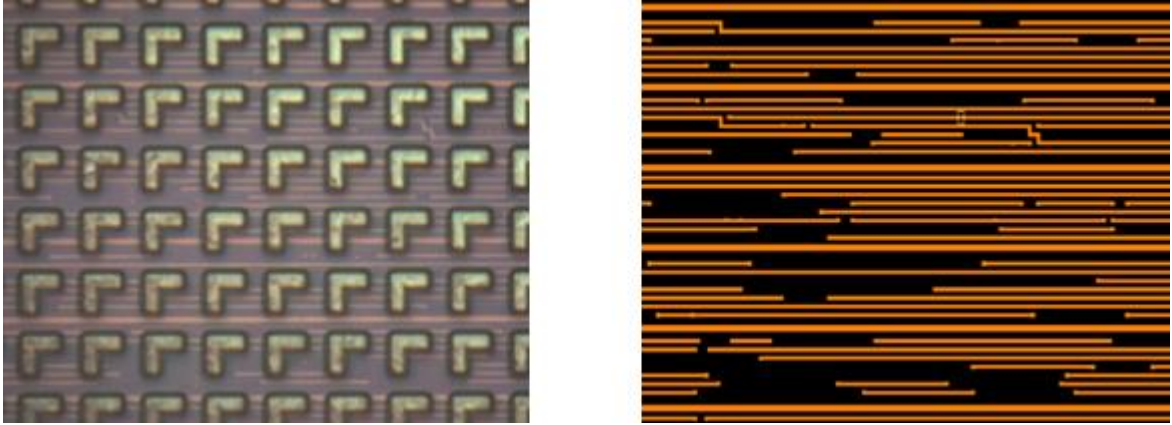


FIGURE 3.1: The layout of the Circuit under Test and the GDSII layout of the fabricated chip [7]

However, the approach has two primary limitations. Its expense and the time it consumes. Despite its precision, optical inspection may be less appealing compared to other quicker, less costly, but also less accurate Trojan detection methods. Moreover, its practicality diminishes when scrutinizing a large batch of integrated circuits, especially since fabrication facilities might use both original and compromised masks for different production runs. [12]

An advancement to offset these limitations was proposed in [7]. The authors introduced a method for detecting Trojans by comparing the images of the last metal layers against the original GDSII layout files. They showed that Trojans with a high core utilization ratio (greater than 80%) would affect the upper metal layers. While the higher the layer used, for routing the Hardware Trojans, the simpler is its detection. Consequently, such Trojans can be identified through cross-correlation between the original GDSII and high-resolution images of the chip's upper layers. [7]

3.6.4 Thermal Mapping for Hardware Trojan Detection

Several methods have been investigated in order to track and record circuit's thermal values. Infra-Red thermography cameras are commonly used in order to measure all chips

thermal emissions. Also DC measurements can be a very helpful tool for dynamic measurements and device's thermal behavior illustration.

Unfortunately DC measurements aren't that helpful for hot spot mapping, and Infra-Red image obtainment is useless. More specific, since both the detector and the thermal emissions are perceptible in room temperature variations, the environmental conditions need to be steady. In addition, chip's static power consumption, generate a DC offset which spreads some extra heat, leading thus to weak spots occultation. As heat diffusion, static thermal emissions and high contrast of material emissivity prevent weak thermal spots to be detected using DC measurements. [19]

Another tool is the lock-in thermography, which is typically useful in order to highlight small hot spots and create thermal maps for the devices. None of the DC offsets affects the final thermal map of each device, since the user can choose a specific area of the chip according to his preferences. In addition, in low power ICs, lock-in thermography is quite effective, for deeply buried in noise, signals detection. [19]

Generally speaking, using thermal analysis in order to detect a malicious circuit, means that we need to extract golden thermal maps from examining a trustful product's IC, like a golden chip. Furthermore we need to compare those maps, with Trojan infected device's thermal maps by a series of measurements and computations of the IC design. Several accuracy levels can achieve the maps comparison, depending on how concealed the Hardware Trojan is. The well concealed Trojans can be examined both by statistical tests like Welch's t-tests and by comparing different positions of the maps. While the same process just demands visual approach for the externalized Hardware Trojans. [19]

So practically for externalized Hardware Trojans the main procedure uses an Infra-Red platform to carry out the measurements, in order to compare visually the thermal map from the Trojan infected IC with a golden thermal map. And compute so, the main difference between the results. Like in the experiment of paper [19], having the mapping results from the Infra-Red platform as it illustrated in FIGURE 3.2 and just by inspecting them visually, more specific by examining the phase maps, we can get a clear view about potential externalized Hardware Trojans existence. [19]

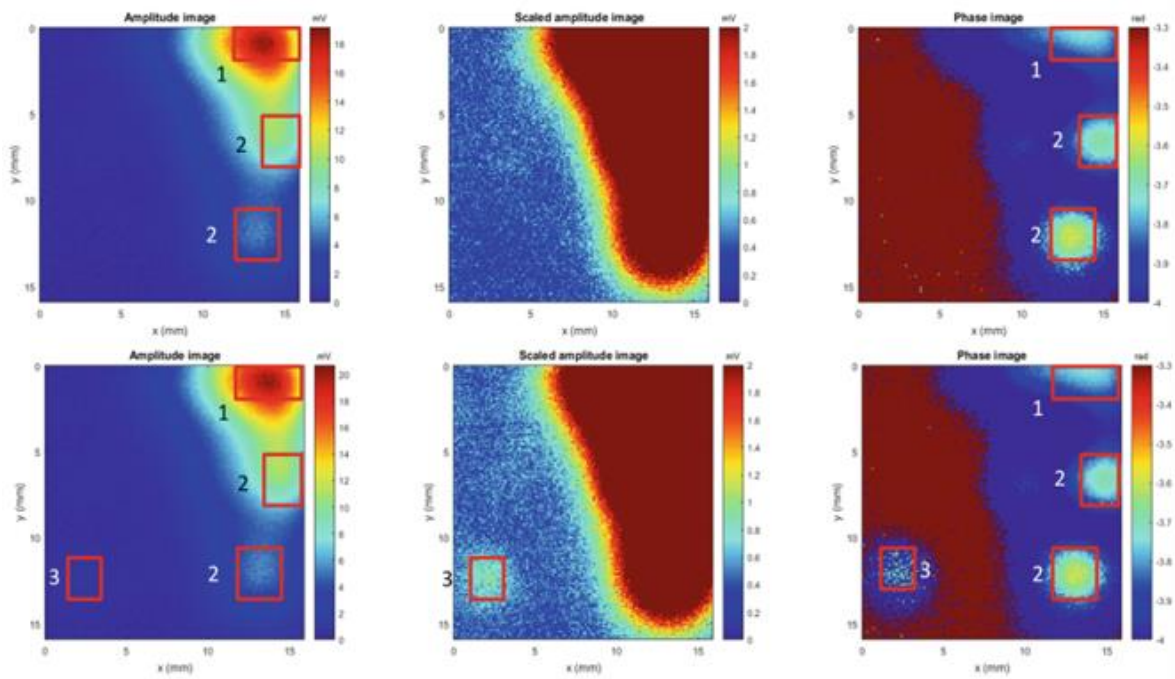


FIGURE 3.2: Thermal maps from both a golden circuit and an externalized Trojan infected circuit [19]

Selections with label 1 represent the AES (Advanced Encryption Standard) positions)

Selections with label 2 represent large output buffers positions

Selections with label 3 represent externalized Hardware Trojan's positions.

The amplitude images give the thermal wave at each coordinate, filled with the proportional color scale. While the scaled amplitude images help us more to track potential Hardware Trojans. Finally the Phase images, give thermal wave's phase with respect to the lock-in signal. [19]

The authors in [19] noticed that for well-hidden Hardware Trojans, more efficacious methods needed compared to the visual approach that used on externalized Trojans. Admittedly this need came up since the AES heat overcome as we noticed in FIGURE 3.3 and shade the heat which is producing due to a Hardware Trojan.

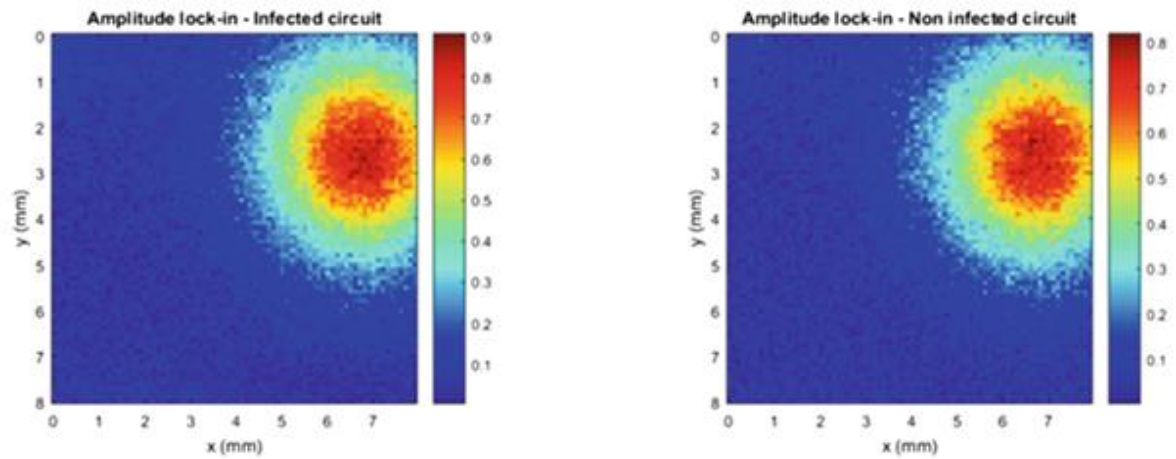


FIGURE 3.3: Thermal maps from both a golden circuit and a circuit infected by a well-hidden hardware Trojan [19]

It's clear that we can't examine these thermal-mapping results by visually comparing them, since the results seem to be quite the same. However, using Welch's t-test comparison is quite an option in order to track tiny heat differences happening due to malicious circuits. Each extra source of heat is concealing the existence of Hardware Trojans. It's quite important so to determine and eliminate any temperature changes happening during this process. Achieving this by minimize the temperature effect on each thermal map in order to extract accurate results. [19]

The extracted maps that arising after practicing Welch t-test method between the chips, are given below in FIGURE 3.4. [19]

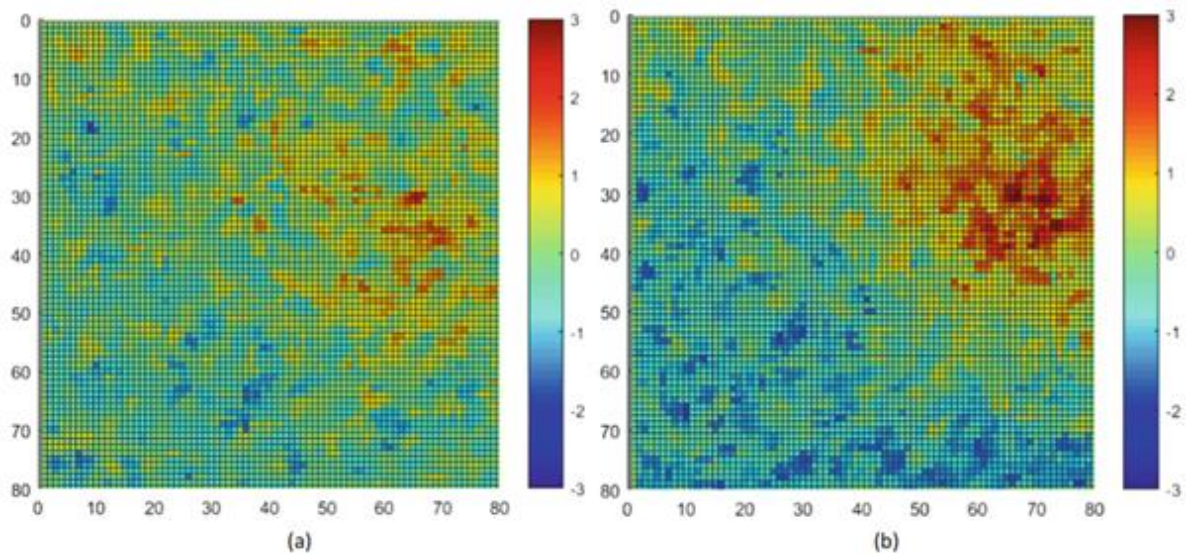


FIGURE 3.4: Obtained Thermal Maps [19]

After using Welch t-tests between a golden chip and:

- Another golden chip in the (a)-map
- A chip infected by a well-hidden hardware Trojan in the (b)-map.

Consequently, while thermal mapping has emerged as a promising technique for Hardware Trojan detection, it is not without its challenges and limitations. As we mentioned before, one of the primary issues is the sensitivity to environmental factors, such as ambient temperature, which can introduce noise into the thermal data. Additionally, the technique often requires specialized equipment that can be costly and may not be readily available. The spatial resolution of thermal maps is another concern, as it may not be sufficient to detect smaller, more stealthily designed Trojans. Furthermore, thermal mapping is generally more time-consuming compared to other detection methods, making it less suitable for real-time or large-scale applications. Lastly, the technique can yield false positives and negatives, particularly when the thermal signatures of benign components are similar to those of Hardware Trojans, complicating thus the interpretation of the results.

CHAPTER 4 PATH DELAY FINGERPRINT

4.1 Main features

Many issues arising by existing Trojan detection methods have made imperative the need of developing more efficient models, in the name of Hardware Security. Path delay fingerprint came to fill the gap of previous destructive, non-scalable and high cost-time Trojan detection models that also tend to have low applicability. A non-destructive technique aimed at identifying unique characteristics in ICs. [20]

4.1.1 Path Delays, Measurements tools and Methodology

Every IC has a set of inherent variations, introduced during the manufacturing process, such as doping concentration and oxide thickness. These variations manifest themselves as distinct path delays when signals traverse through the IC. By measuring these delays, we can generate a unique "fingerprint" for each IC, making it easier to distinguish genuine components from counterfeit or recovered ones. [20]

The original work employed a systematic methodology to capture the path delay fingerprint of ICs. They started with a pre-characterization phase where certified ICs were tested to generate a "golden" fingerprint. Subsequently, the fingerprints of suspect ICs were compared against this golden standard. If significant deviations were found, that means the existence of a Hardware Trojan and the IC was flagged as recovered or counterfeit. [20]

The path delay variations are primarily the result of manufacturing process variations and can be captured using advanced testing methods like Automatic Test Pattern Generation (ATPG). These tests apply a set of test vectors to the IC's input pins and measure the corresponding output responses. By analyzing the time it takes for signals to traverse from input to output, we can calculate the path delays. [20]

Those calculations are achieved using tools like TDCs which are hardware components that can measure time intervals with high precision. They are often used in conjunction with other hardware or software tools to calculate path delays in ICs. [11]

Also High-speed oscilloscopes are commonly used for measuring path delays. They capture the waveforms of signals traversing the paths and calculate the time difference between specific points on the waveforms. [9]

4.1.2 Applications, Limitations and Future Scope

The immediate application of this technique is in the supply chain, where it can serve as a reliable method for screening components. It could also be applied in quality control, providing an additional layer of security to ensure the reliability of electronic systems. Moreover, this method is not limited to ICs but could be extended to other electronic components like Field Programmable Gate Arrays (FPGAs) and System on Chips (SOCs). [20]

While path-delay fingerprinting presents a promising avenue, it is not without limitations. For instance, it requires specialized equipment and expertise to carry out the testing procedures. Also, the method may not be effective against sophisticated counterfeiting techniques that can artificially manipulate path delays. [20]

4.2 Case Study 1: Delay Calculation

In order to examine an IC design we need to select many chips. So in a sample of chips, a wide range of different input patterns are both selected and run in order to collect high dimension path delay information. And then according to those path delays, a series of delay fingerprints are generating and mapped into low dimension spaces. [21]

Talking about path delay computing there is a classical model that combines both gate delay and wire delay. At the FIGURE 4.1 there is an example model with two AND gate

inputs and a single output. In this model arise three different types of delay. Gate delay, path delay and output delay. [21]

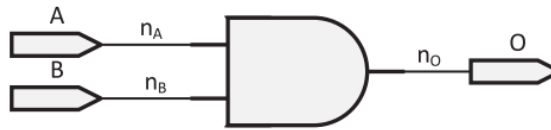


FIGURE 4.1: Example of delay calculation [21]

There is delay in each component. Talking about gate delay there is an ensemble of the standard parasitic delay and the effort delay. The effort delay depends on the load at the output. More specifically the value of the effort delay defined from the multiplication of two proportional parameters. The logical effort which is the result of the gate's input capacitance dividing with an inverter's input capacitance, delivering the same current at the output and the electrical effort which is the result of the capacitance that is loading in the output, dividing with the capacitance that is presenting in the input. [21]

Furthermore we can talk about output delay, which is the delay between input ports and output ports, including clock signals in sequential circuits. The time from the moment a second vector is applied, to the moment the output takes the updated value, constitutes the output delay. So typically all that needs is just a pair of input vectors in order to have some output delay. [21]

Also there is the path delay. For example in FIGURE 4.1 the delay of a path is decided by its control bit, the change of which updates the value of the output. [21]

Finally there can also be an extra path delay, which can be caused by a Hardware Trojan like in the right side of the FIGURE 4.2. Usually in that case, an extra path delay incurred by a Hardware Trojan, is added on paths where the Trojan is inserted in, or connected to. The inserted payload of a Hardware Trojan is responsible for increasing the path delay, unlike the example in the left side of the FIGURE 4.2 where there isn't any extra delay gushes from a potential Trojan. [21]

All these cases combined, form the path delay fingerprint.

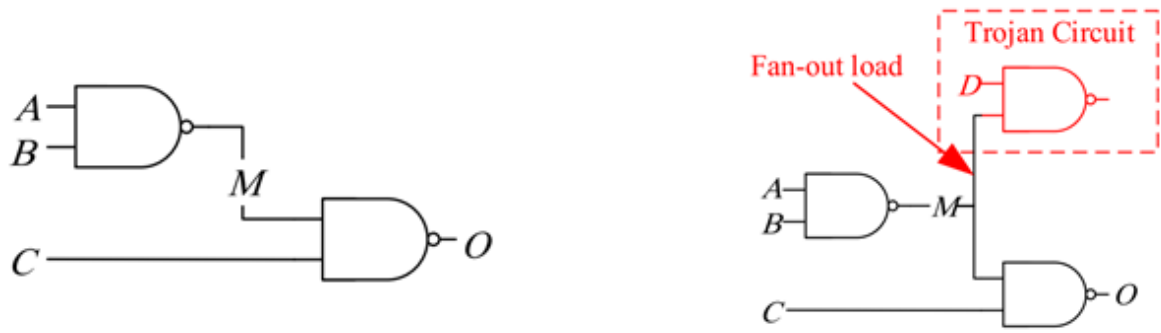


FIGURE 4.2: A Trojan-free circuit and the same circuit with hardware Trojan inserted in [21]

4.3 Case Study 2: Detection of various embedded Trojans

First of all we need to get the gate level netlist, of a Trojan free circuit. By collecting detailed delay information of every single gate in the design, we can create a standard delay format file, for each chip under test. So we have a reliable data structure with the fingerprints of each nominal chip. [9]

Examining how effective are those information in order to detect a Hardware Trojan, we need to modify this circuit's netlist, by embedding a Trojan circuits. Then we have to use plenty of patterns in order to collect path delay information for the Trojan circuit as well, by covering as many parts of the whole chip as possible. So we can prevent any chance the chip stay undetectable under any change. [9]

For the experiment in [9] the author inserts a 2-bit comparator-based Trojan near the input pin of the circuit core, in the middle-stage of the chip and near the output of the circuit core. Then conducts delay simulations with several test points for each of the cases and extracts some results.

Considering that a 2-bit comparator occupies a tiny area of the whole chip, if the test points are in or near the convex hull, it is valid to say that the chip might be genuine. Unlike the cases where the sample points are far from the convex hull and in which cases we can identify the circuits as Trojan circuits. [9]

4.3.1 Near-input Trojan

In FIGURE 4.3 the author gives the results of inserting a 2-bit comparator Trojan near the input. The Trojan detection is easy, as in every near-input Trojan case, the sample points seems to be far from the convex hull. So the path delay fingerprint examination is very effective. [9]

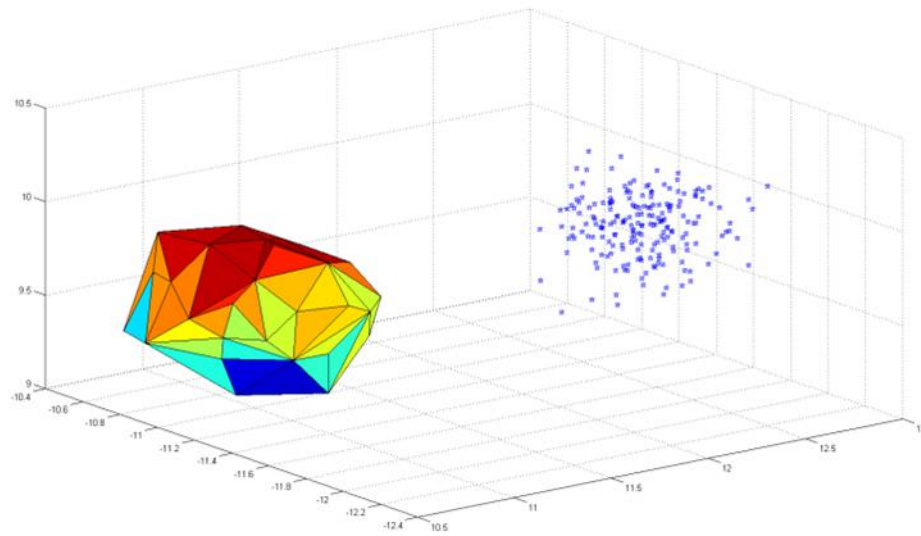


FIGURE 4.3: Delay Comparison of a near-input Trojan [9]

4.3.2 Near-middle-stage Trojan

Same results arise by the insertion of a 2-bit comparator-based Trojan in the middle-stage of the chip as it displayed in the FIGURE 4.4. The testing points are clearly separated from the convex hull, so every Trojan is easily detectable. [9]

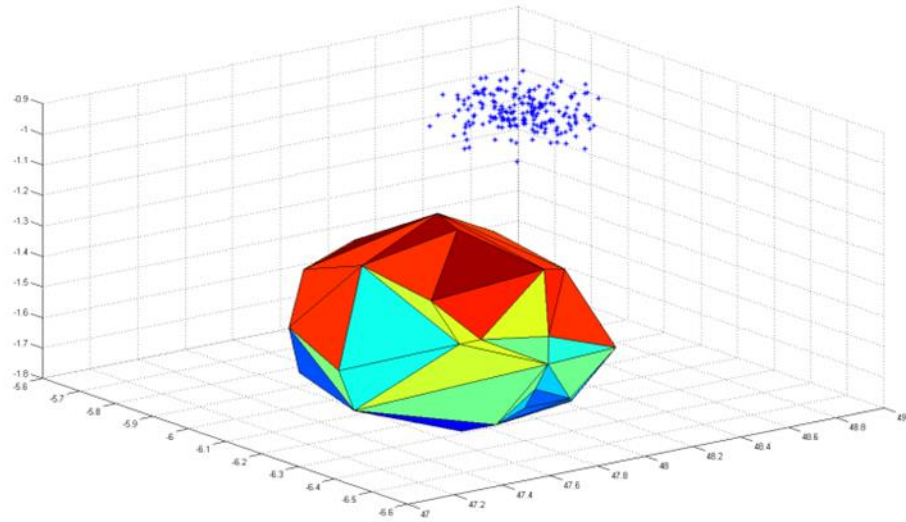


FIGURE 4.4: Delay Comparison of a middle-stage Trojan [9]

4.3.3 Near-output Trojan

In FIGURE 4.5 a lot more separated, the sample points seems to be from the convex hull, while a 2-bit comparator-based Trojan is inserted near the output. Thus a hardware Trojan circuit is 100% detectable in this case. [9]

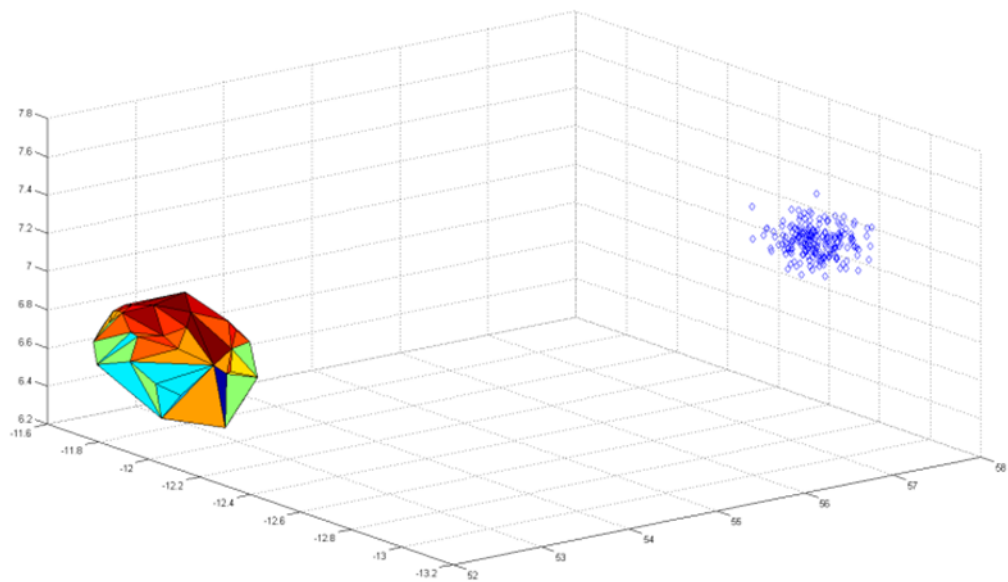


FIGURE 4.5: Delay Comparison of a near-output Trojan [9]

4.3.4 Counter-based Trojan

This method only seems to be invalid, when we are dealing with a 4-bit counter-based Trojan. A counter-based trojan, only uses an inner signal in order to trigger the counter, without inserting any explicit delay. Some additional delay is observed on the path, due to the extra capacity load of the inner signal. Although in every experiment, the test points seems to be close enough to the convex hull as we can see in the FIGURE 4.6. So the Trojans are more unlikely to be detected in those cases, decreasing significantly the Trojan detection rate. [9]

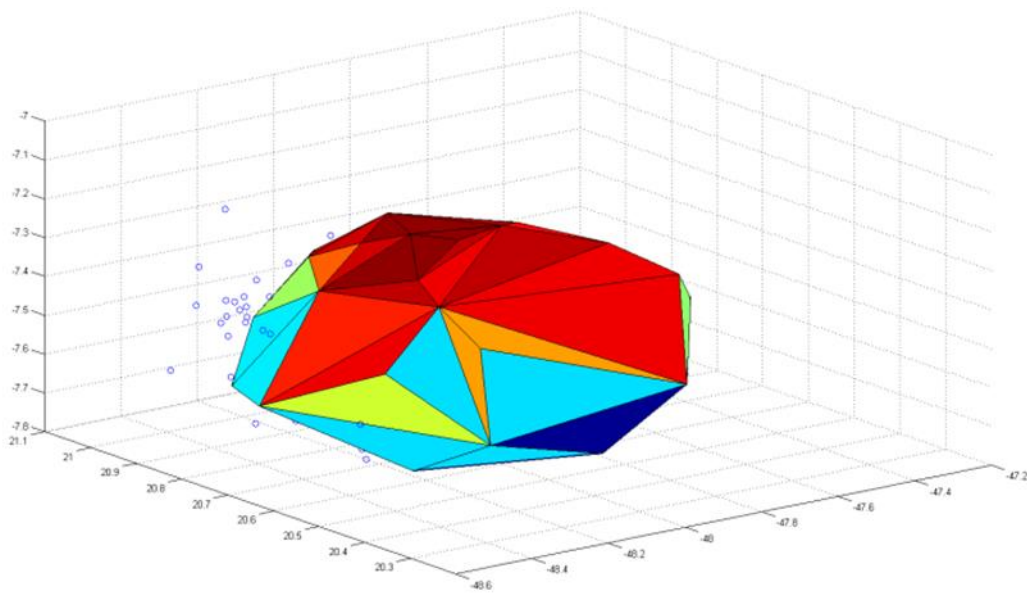


FIGURE 4.6: Delay Comparison of 4-bit counter-based Trojan [9]

4.3.5 Case Conclusions

Practicing path delay fingerprinting, in order to detect Hardware Trojans, is quite an effective way in most of the cases. Despite the implicit-payload Trojan cases, where the Trojans are much difficult to be detected through this method. Although path delay fingerprinting is 100% effective in explicit-payload Trojans, even in those who are considerably smaller to the whole circuit.

4.4 Path Delay for IP authentication

Intellectual Property (IP) authentication is a critical aspect of hardware security, ensuring that only authorized ICs are utilized in a given system. The study in [22] aims to delve into the methods and results concerning the measurement of path delays for IP authentication and integrity verification. Traditional methods often relied on static characteristics, which are not sufficient in today's complex hardware landscape. The paper underlines the use of advanced techniques that focus on measuring the actual path delays associated with each bit of a hardware AES-FPGA implementation. By employing a clock glitch technique, the paper demonstrates how path delays can be accurately captured.

4.4.1 Clock Glitch Operation

The Clock Glitch Technique involves intentionally embed glitch into the clock signal of an IC. The glitch's parameters, such as duration and amplitude, are carefully chosen to ensure that they do not cause functional failures. This glitch affects the timing behavior of the IC, particularly the path delays between different components. By measuring these path delays, unique fingerprints can be generated for authentication purposes. The generated fingerprint is compared against a database of authorized fingerprints. If matching, the IC is authenticated while otherwise, it is flagged as unauthorized. These measurements contribute to a more robust methodology for ensuring hardware IP integrity and authentication. [22]

4.4.2 Challenges and Limitations

While the paper outlines the significance of path delay measurements, like low computational overhead and minimal impact on system performance, it also sheds light on the challenges and limitations. For instance, the process can be time-consuming and may require specialized equipment. Moreover, the glitch could inadvertently affect other timing-sensitive operations within the IC, leading thus to potential false positives or negatives during the authentication process. Lastly, the technique may not be universally applicable across all types of ICs, limiting its scalability and widespread adoption. [22]

CHAPTER 5 COMPARATIVE ANALYSIS

While numerous Trojan detection techniques have been developed, each comes with its own set of advantages, limitations, and applicability scenarios. Therefore, a comprehensive comparison between these techniques is not just beneficial but essential as well. Such a comparison provides invaluable insights into the effectiveness, efficiency, and reliability of each method, enabling better-informed decisions in both academic research and practical applications. Moreover, it lays the groundwork for the development of hybrid or new techniques that can leverage the strengths and mitigate the weaknesses of existing methods, thereby enhancing the overall robustness of hardware security. By comparing those techniques on multiple fronts, you can make a well-informed decision on which technique is more suitable for specific scenarios or types of hardware.

5.1 Comparison Set-Up

5.1.1 Criteria for Comparison

This chapter aims to conduct a comparison between Path Delay Fingerprinting and a range of other Hardware Trojan detection techniques, specifically Invasive Detection Techniques, Running Time Detection Techniques, Testing-Based Detection Techniques, Ring-Oscillator-Based Detection Techniques, Chemical De-layering Methods, Visual Inspection-Based Detection Techniques and Side-channel Thermal Analysis. The comparison will be structured around the following key criteria of Detection Accuracy, Computational Complexity, Scalability, Intrusiveness, Cost and Time-Efficiency, Applicability and False Positive/Negative Rates. Considering CHAPTER 3 and CHAPTER 4 , each technique will be individually examined against those criteria and a summarized conclusion will be drawn in relation to Path Delay Fingerprinting. The findings will be presented in a table summarizing the results for each technique. Finally, a comprehensive table will be created to encapsulate all the summarized results, serving as the basis for the observations of this analysis.

5.1.2 Clarification of Concepts

The efficacy of any Hardware Trojan detection technique is often evaluated based on its ability to minimize false positives and false negatives. False positives occur when the detection system incorrectly identifies a benign circuit as infected by a Hardware Trojan. On the other hand, false negatives are arguably more dangerous, as they signify the failure to detect an actual Hardware Trojan. A common factor, that affect those rates are the environmental noise. Factors like temperature and voltage fluctuations can affect measurements in most detection techniques, leading to false positives. Moreover the inherent complexity of modern ICs can sometimes obscure the signals or characteristics being measured, contributing to both false positives and false negatives. Also Trojans that activated under specific conditions may evade detection during standard testing procedures, leading thus to false negatives. The clarification of those concepts will be key point on understanding the following comparative analysis.

TABLE 5.1: Sample of Scalable Standards for Measurements

EFFECT \ CRITERIA	BAD ➡ GOOD						
Detection Accuracy	VL	L	L-M	M	M-H	H	VH
Computation Complexity	VH	H	M-H	M	L-M	L	VL
Scalability	NS	LS	MS	HS			
Intrusiveness	HI	MI	NI				
Cost Efficiency	VL	L	L-M	M	M-H	H	VH
Time Efficiency	VL	L	L-M	M	M-H	H	VH
Applicability	VL	L	L-M	M	M-H	H	VH
False Positives Factors	VH	H	M-H	M	L-M	L	VL
False Negatives Factors	VH	H	M-H	M	L-M	L	VL

TABLE ABBREVIATIONS

VL	Very Low
L	Low
M	Moderate
H	High
VH	Very High
NS	Non-Scalable
LS	Low Scalable
MS	Moderate Scalable
HS	High Scalable
HI	High Intrusive
MI	Moderate Intrusive
NI	Non-Intrusive

5.2 Path Delay Fingerprint, Key Criteria

5.2.1 Detection Accuracy

Path Delay Fingerprint boasts high detection accuracy by capturing the unique timing characteristics of each chip. This method is particularly effective in identifying subtle timing anomalies that could be indicative of a Hardware Trojan.

5.2.2 Computational Complexity

The computational complexity is moderate, mainly involving timing measurements and statistical analysis. Specialized equipment is often required to capture precise timing data.

5.2.3 Scalability

This technique is moderately scalable and can be applied to various chip architectures. However, it does require baseline measurements for comparison, which can be a limiting factor.

5.2.4 Intrusiveness

One of the major advantages is its non-destructive nature. The technique only measures timing delays, thereby not affecting the functionality of the chip.

5.2.5 Cost and Time-Efficiency

The cost is moderate, given the need for specialized timing measurement equipment. Time-efficiency is also moderate, as the measurements and subsequent analysis can be time-consuming.

5.2.6 Applicability

Path Delay Fingerprint has a broad applicability and is suitable for both digital and analog circuits.

5.2.7 False Positives Factors

Environmental Noise: Fluctuations in temperature or voltage can affect the path delay measurements, leading to false positives.

Manufacturing Variability: Inconsistencies during the manufacturing process can introduce variations in path delays, which may be mistaken for a Trojan.

Complex Circuitry: Highly complex circuits may have inherent delays that are difficult to distinguish from those introduced by a Trojan.

5.2.8 False Negatives Factors

Subtle Trojans: Some Hardware Trojans are designed to have minimal impact on path delays, making them difficult to detect.

Insufficient Sampling: Inadequate or improper sampling of paths can miss the Trojan-affected paths.

Dynamic Behavior: Trojans that activated under specific conditions may not be detected during regular testing.

TABLE 5.2: Criteria of Comparison for Path Delay Fingerprint

CRITERIA	TROJAN DETECTION METHOD	Path Delay Fingerprint
Detection Accuracy		H
Computation Complexity		M
Scalability		MS
Intrusiveness		NI
Cost Efficiency		M
Time Efficiency		M
Applicability		VH
False Positives Factors		M
False Negatives Factors		M

5.3 Invasive Detection Techniques, Key Criteria

5.3.1 Detection Accuracy

Invasive Detection Techniques, such as micro-probing, offer very high detection accuracy but are destructive in nature.

5.3.2 Computational Complexity

The computational complexity is generally low, as these techniques often involve physical inspection rather than computational analysis.

5.3.3 Scalability

These techniques are not scalable, as each chip must be individually inspected, making it less suitable for large-scale operations.

5.3.4 Intrusiveness

Invasive Detection Techniques are highly intrusive, often requiring the destruction of the chip for thorough inspection.

5.3.5 Cost and Time-Efficiency

The cost is high due to the need for specialized equipment and skilled personnel. The process is also labor-intensive and time-consuming, making it less time-efficient.

5.3.6 Applicability

These techniques are mainly applicable to digital circuits and are less effective for analog or mixed-signal circuits.

5.3.7 False Positives Factors

Human Error: The manual nature of some invasive techniques can lead to human errors, resulting in false positives.

Tool Limitations: The precision and capabilities of the invasive tools can also contribute to false positives.

Physical Damage: The invasive nature of these techniques can sometimes cause physical alterations that are mistaken for Trojans.

5.3.8 False Negatives Factors

Stealthy Design: Some Hardware Trojans are engineered to be physically unobtrusive, making them difficult to be detected through invasive methods.

Depth of Inspection: The level of invasiveness may not be sufficient to detect deeply embedded Trojans.

Resource Limitations: Invasive techniques can be time-consuming and expensive, which may lead to incomplete analyses and thus false negatives.

TABLE 5.3: Criteria of Comparison for Invasive Detection Techniques

CRITERIA TROJAN DETECTION METHODS	Path Delay Fingerprint	Invasive Detection Techniques
Detection Accuracy	H	VH
Computation Complexity	M	L
Scalability	MS	NS
Intrusiveness	NI	HI
Cost Efficiency	M	L
Time Efficiency	M	L
Applicability	VH	M
False Positives Factors	M	L
False Negatives Factors	M	H

5.3.9 Summary and Conclusion

In TABLE 5.3 both Path Delay Fingerprint and Invasive Detection Techniques offer unique advantages and limitations. While Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy, Invasive Detection Techniques offer the highest level of scrutiny but are destructive, costly, and not scalable.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Path Delay Fingerprint may be more suitable due to its non-intrusive nature and moderate scalability. On the other hand, for critical applications where the highest level of scrutiny is required, Invasive Detection Techniques may be the preferred choice, despite their limitations.

5.4 Running Time Detection Techniques, Key Criteria

5.4.1 Detection Accuracy

Running Time Detection Techniques, such as performance counters and runtime monitoring, offer moderate to high detection accuracy but may miss Trojans that are triggered under specific conditions.

5.4.2 Computational Complexity

The computational complexity is generally low, as these techniques often leverage existing hardware features for monitoring.

5.4.3 Scalability

These techniques are highly scalable, as they can be easily integrated into existing systems without requiring additional hardware.

5.4.4 Intrusiveness

Running Time Techniques are generally non-intrusive, as they monitor the system during its normal operation.

5.4.5 Cost and Time-Efficiency

The cost is generally low, as no specialized equipment is usually required. These techniques are also time-efficient, as they can be run in parallel with normal system operation.

5.4.6 Applicability

These techniques are mainly applicable to digital circuits and systems where runtime monitoring is feasible.

5.4.7 False Positives Factors

Environmental Factors: Variations in temperature, voltage, or other environmental conditions can affect the running time, leading to false positives.

Software Overheads: Sometimes, the software running on the hardware can introduce delays that are mistaken for Hardware Trojans.

Tool Sensitivity: The granularity and precision of the measurement tools can also contribute to false positives.

5.4.8 False Negatives Factors

Stealthy Design: Some Hardware Trojans are engineered to have minimal impact on running time, making them difficult to be detected.

Task-Specific Activation: Trojans that activated only during specific tasks may not be detected during general running time analysis.

Resource Limitations: Inadequate computational resources can sometimes lead to incomplete or rushed analyses, resulting in false negatives.

TABLE 5.4: Criteria of Comparison for Running Time Detection Techniques

CRITERIA \ TROJAN DETECTION METHODS	Path Delay Fingerprint	Running Time Detection Techniques
Detection Accuracy	H	M-H
Computation Complexity	M	L
Scalability	MS	HS
Intrusiveness	NI	NI
Cost Efficiency	M	H
Time Efficiency	M	H
Applicability	VH	M
False Positives Factors	M	H
False Negatives Factors	M	M

5.4.9 Summary and Conclusion

In TABLE 5.4 both Path Delay Fingerprint and Running Time Detection Techniques offer unique advantages and limitations. While Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy, Running Time Detection Techniques are more scalable and cost-time-effective but may offer slightly lower detection accuracy.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Running Time Detection Techniques may be more suitable due to their scalability and cost-effectiveness. On the other hand, for critical applications where high scrutiny is required, Path Delay Fingerprint may be the preferred choice, despite its limitations.

5.5 Testing Based Detection Techniques, Key Criteria

5.5.1 Detection Accuracy

Testing Based Detection Techniques, such as Automatic Test Pattern Generation (ATPG) and Logic Built-In Self-Test (LBIST), offer high detection accuracy for functional Trojans but may miss Trojans that are triggered under specific conditions.

5.5.2 Computational Complexity

The computational complexity is high, involving the generation and application of test patterns, as well as the analysis of test responses.

5.5.3 Scalability

These techniques are less scalable, often requiring new test patterns for different chip architectures, making them less suitable for large-scale operations.

5.5.4 Intrusiveness

Testing Based Techniques are generally non-intrusive, requiring the insertion of test patterns into the chip, which mainly don't affect its functionality.

5.5.5 Cost and Time-Efficiency

The cost is high due to the need for test pattern generation and analysis tools. The process is also time-consuming, making it less time-efficient.

5.5.6 Applicability

These techniques are mainly applicable to digital circuits and are less effective for analog or mixed-signal circuits.

5.5.7 False Positives Factors

Test Vector Limitations: Sometimes, the test vectors used can produce behavior that mimics that of a Hardware Trojan, leading to false positives.

Environmental Noise: Factors like temperature and voltage fluctuations can affect the test results, leading to false positives.

Tool Sensitivity: The granularity and precision of the measurement tools can also contribute to false positives.

5.5.8 False Negatives Factors

Stealthy Design: Some Hardware Trojans are engineered to activate only under specific conditions that may not be covered by the test vectors, leading to false negatives.

Complex IC Designs: The inherent complexity of modern ICs can sometimes obscure the Trojan-affected paths or components, contributing to false negatives.

Resource Limitations: Testing-based techniques can be time-consuming and computationally expensive, which may lead to incomplete analyses and thus false negatives.

TABLE 5.5: Criteria of Comparison for Testing Based Detection Techniques

CRITERIA \ TROJAN DETECTION METHODS	Path Delay Fingerprint	Testing Based Detection Techniques
Detection Accuracy	H	H
Computation Complexity	M	H
Scalability	MS	LS
Intrusiveness	NI	NI
Cost Efficiency	M	L
Time Efficiency	M	L
Applicability	VH	M
False Positives Factors	M	M
False Negatives Factors	M	L

5.5.9 Summary and Conclusion

In TABLE 5.5 both Path Delay Fingerprint and Testing Based Detection Techniques offer unique advantages and limitations. Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy. In contrast, Testing Based Detection Techniques excel in detection accuracy but are computationally intensive, costly, and intrusive.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Path Delay Fingerprint may be more suitable due to its non-intrusive nature and moderate scalability. On the other hand, for critical applications where high scrutiny is required, Testing Based Detection Techniques may be the preferred choice, despite their limitations.

5.6 Ring-Oscillator Based Trojan Detection Techniques, Key Criteria

5.6.1 Detection Accuracy

Ring-Oscillator Based Techniques offer moderate to high detection accuracy, depending on the design and placement of the ring-oscillators.

5.6.2 Computational Complexity

The computational complexity is generally low, mainly involving the measurement and analysis of oscillation frequencies.

5.6.3 Scalability

This technique is highly scalable, as ring-oscillators can be easily integrated into existing chip designs.

5.6.4 Intrusiveness

Ring-Oscillator Based Techniques are generally non-intrusive but do require the integration of additional hardware components, which could potentially affect the chip's functionality.

5.6.5 Cost and Time-Efficiency

The cost is generally low, as no specialized equipment is usually required. These techniques are also time-efficient, as they can be run in parallel with normal system operation.

5.6.6 Applicability

This technique is mainly applicable to digital circuits and may be less effective for analog or mixed-signal circuits.

5.6.7 False Positives Factors

Environmental Factors: Variations in temperature, voltage, or other environmental conditions can affect the oscillation frequencies, leading to false positives.

Manufacturing Variability: Inconsistencies during the manufacturing process can introduce variations in frequencies, which may be mistaken for a Trojan.

Tool Sensitivity: The granularity and precision of the measurement tools can also contribute to false positives.

5.6.8 False Negatives Factors

Stealthy Design: Some Hardware Trojans are engineered to have minimal impact on oscillation frequencies, making them difficult to detect.

Task-Specific Activation: Trojans that activate only during specific tasks may not be detected during general frequency analysis.

Resource Limitations: Inadequate computational resources can sometimes lead to incomplete or rushed analyses, resulting in false negatives.

TABLE 5.6: Criteria of Comparison for Ring-Oscillator Based Detection Techniques

CRITERIA \ TROJAN DETECTION METHODS	Path Delay Fingerprint	Ring-Oscillator Based
Detection Accuracy	H	M-H
Computation Complexity	M	L
Scalability	MS	HS
Intrusiveness	NI	MI
Cost Efficiency	M	H
Time Efficiency	M	H
Applicability	VH	M
False Positives Factors	M	H
False Negatives Factors	M	M

5.6.9 Summary and Conclusion

In TABLE 5.6 both Path Delay Fingerprint and Ring-Oscillator Based Trojan Detection Techniques offer unique advantages and limitations. While Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy, Ring-Oscillator Based Techniques are more scalable and cost-effective but may offer slightly lower detection accuracy depending on the design.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Ring-Oscillator Based Techniques may be more suitable due to their scalability and cost-effectiveness. On the other hand, for critical applications where high scrutiny is required, Path Delay Fingerprint may be the preferred choice, despite its limitations.

5.7 Chemical De-layering Methods, Key Criteria

5.7.1 Detection Accuracy

Chemical De-layering Methods offer very high detection accuracy but they are destructive in nature, making them unsuitable for functional ICs.

5.7.2 Computational Complexity

The computational complexity is generally low, as these techniques often involve physical inspection rather than computational analysis.

5.7.3 Scalability

These techniques are not scalable, as each chip must be individually inspected, making it less suitable for large-scale operations.

5.7.4 Intrusiveness

Chemical De-layering Methods are highly intrusive, often requiring the destruction of the chip for thorough inspection.

5.7.5 Cost and Time-Efficiency

The cost is high due to the need for specialized equipment and skilled personnel. The process is also labor-intensive and time-consuming, making it less time-efficient.

5.7.6 Applicability

These techniques are mainly applicable to digital circuits and are less effective for analog or mixed-signal circuits.

5.7.7 False Positives Factors

Human Error: The manual nature of some chemical de-layering techniques can lead to human errors, resulting in false positives.

Chemical Residue: Sometimes, the chemicals used can leave residues that are mistaken for Hardware Trojans.

Tool Limitations: The precision and capabilities of the microscopic tools used for inspection can also contribute to false positives.

5.7.8 False Negatives Factors

Depth of Inspection: The level of de-layering may not be sufficient to reveal deeply embedded Trojans.

Chemical Limitations: Some chemicals may not be effective in removing all types of materials, leaving some Trojans undetected.

Resource Limitations: Chemical de-layering can be time-consuming and expensive, which may lead to incomplete analyses and thus to false negatives.

TABLE 5.7: Criteria of Comparison for Chemical De-layering Detection Techniques

CRITERIA TROJAN DETECTION METHODS	Path Delay Fingerprint	Chemical De-layering
Detection Accuracy	H	VH
Computation Complexity	M	L
Scalability	MS	NS
Intrusiveness	NI	HI
Cost Efficiency	M	L
Time Efficiency	M	L
Applicability	VH	M
False Positives Factors	M	M
False Negatives Factors	M	H

5.7.9 Summary and Conclusion

In TABLE 5.7 both Path Delay Fingerprint and Chemical De-layering Methods offer unique advantages and limitations. While Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy, Chemical De-layering Methods offer the highest level of scrutiny but are destructive, costly, and not scalable.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Path Delay Fingerprint may be more suitable due to its non-intrusive nature and moderate scalability. On the other hand, for critical applications where the highest level of scrutiny is required, Chemical De-layering Methods may be the preferred choice, despite their limitations.

5.8 Visual Inspection Based Detection Techniques, Key Criteria

5.8.1 Detection Accuracy

Visual Inspection offers very high detection accuracy through direct visual examination of the hardware, often augmented by advanced imaging techniques like SEM.

5.8.2 Computational Complexity

The computational complexity is generally low, although automated systems may involve some level of image processing.

5.8.3 Scalability

The technique is not scalable, as each chip must be individually inspected, making it less suitable for large-scale operations.

5.8.4 Intrusiveness

Visual Inspection is highly intrusive, often requiring de-layering or de-capsulation of the chip, which can potentially damage the hardware.

5.8.5 Cost and Time-Efficiency

The cost is high due to the need for specialized imaging equipment. The process is also labor-intensive and time-consuming, making it less time-efficient.

5.8.6 Applicability

The technique is mainly applicable to digital circuits and is less effective for analog or mixed-signal circuits.

5.8.7 False Positives Factors

Human Error: The manual nature of visual inspection can lead to human errors, resulting in false positives.

Manufacturing Anomalies: Sometimes, benign manufacturing anomalies can be mistaken for Hardware Trojans.

Tool Limitations: The resolution and capabilities of the microscopic tools used for inspection can also contribute to false positives.

5.8.8 False Negatives Factors

Stealthy Design: Some Hardware Trojans are engineered to be physically unobtrusive, making them difficult to be detected through visual inspection.

Depth of Inspection: The level of visual inspection may not be sufficient to detect deeply embedded Trojans.

Resource Limitations: Visual inspection can be time-consuming and expensive, which may lead to incomplete analyses and thus to false negatives.

TABLE 5.8: Criteria of Comparison for Visual Inspection Based Detection Techniques

CRITERIA \ TROJAN DETECTION METHODS	Path Delay Fingerprint	Visual Inspection Based
Detection Accuracy	H	VH
Computation Complexity	M	L
Scalability	MS	NS
Intrusiveness	NI	HI
Cost Efficiency	M	L
Time Efficiency	M	L
Applicability	VH	M
False Positives Factors	M	L
False Negatives Factors	M	M

5.8.9 Summary and Comparison Conclusion

In TABLE 5.8 both Path Delay Fingerprint and Visual Inspection Based Techniques offer unique advantages and limitations. While Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy, Visual Inspection excels in detection accuracy but falls short in scalability and intrusiveness.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Path Delay Fingerprint may be more suitable due to its non-intrusive nature and moderate scalability. On the other hand, for critical applications where the highest level of scrutiny is required, Visual Inspection may be the preferred choice despite its limitations.

5.9 Side-channel Thermal Analysis, Key Criteria

5.9.1 Detection Accuracy

Side-channel Thermal Analysis offers moderate to high detection accuracy, depending on the resolution of thermal imaging and the nature of the Trojan.

5.9.2 Computational Complexity

The computational complexity is generally low to moderate, mainly involving the capture and analysis of thermal images.

5.9.3 Scalability

This technique is moderately scalable, as thermal imaging can be applied to various chip architectures but may require calibration for different types of ICs.

5.9.4 Intrusiveness

Side-channel Thermal Analysis is generally non-intrusive, as it involves capturing thermal images without affecting the chip's operation.

5.9.5 Cost and Time-Efficiency

The cost is moderate to high, depending on the sophistication of the thermal imaging equipment. Time-efficiency is moderate, as capturing and analyzing thermal images can be time-consuming.

5.9.6 Applicability

This technique is mainly applicable to digital circuits and may be less effective for analog or mixed-signal circuits.

5.9.7 False Positives Factors

Environmental Noise: External factors like temperature and voltage fluctuations can affect the side-channel measurements, leading to false positives.

Data Dependencies: The data being processed can sometimes produce side-channel signals that mimic those of a Hardware Trojan, causing false alarms.

Tool Limitations: The granularity and sensitivity of the measurement tools can also contribute to false positives.

5.9.8 False Negatives Factors

Stealthy Trojans: Some Hardware Trojans are designed to minimize their side-channel signals, making them difficult to be detected.

Complex IC Designs: The inherent complexity of modern ICs can sometimes obscure the side-channel signals of a Trojan.

Adaptive Behavior: Trojans that activate under specific conditions may evade detection during standard testing procedures.

TABLE 5.9: Criteria of Comparison for Thermal Analysis

CRITERIA \ TROJAN DETECTION METHODS	Path Delay Fingerprint	Thermal Analysis
Detection Accuracy	H	M-H
Computation Complexity	M	L
Scalability	MS	MS
Intrusiveness	NI	NI
Cost Efficiency	M	M-H
Time Efficiency	M	M
Applicability	VH	M
False Positives Factors	M	H
False Negatives Factors	M	H

5.9.9 Summary and Conclusion

In TABLE 5.9 both Path Delay Fingerprint and Side-channel Thermal Analysis offer unique advantages and limitations. While Path Delay Fingerprint provides a non-intrusive, moderately scalable approach with high detection accuracy, Side-channel Thermal Analysis also offers the advantage of being non-intrusive but may have varying levels of detection accuracy depending on several factors.

The choice between these two techniques depends on various factors such as the scale of operation, available resources, and the specific requirements of the hardware being examined. For large-scale, diverse hardware environments, Path Delay Fingerprint may be more suitable due to its non-intrusive nature and moderate scalability. On the other hand, for applications where thermal behavior is a critical factor, Side-channel Thermal Analysis may be the preferred choice.

5.10 Analysis Observations

By observing the approximate results of the TABLE 5.10, we agree that Path Delay Fingerprint domain over other techniques on the field of applicability while also keeps its non-destructive nature. Moreover maintain cost and time levels to moderate while most techniques, unlike Running Time and Ring Oscillator which seems to be the most cost and time efficient, are quite costly and time consuming. Also provides less computation complexity than testing-based methods and keeps detection accuracy satisfactory. While it comes to scalability it's preferred over none scalable-ones as invasive, visual or chemical de-layering. Although needs to go a step further at false positives/negatives, while thermal analysis seems to be a step back. By understanding the strengths and weaknesses of each technique, practitioners can make well-informed decisions tailored to their specific Hardware Trojan detection needs.

TABLE 5.10: Summarized Comparison for Trojan Detection Techniques

TROJAN DETECTION TECHNIQUES \ CRITERIA	Path Delay Fingerprint	Invasive	Running Time	Testing	Ring- Oscillator	Chemical De-layering	Visual Inspection	Thermal Analysis
Detection Accuracy	H	VH	M-H	H	M-H	VH	VH	M-H
Computation Complexity	M	L	L	H	L	L	L	L
Scalability	MS	NS	HS	LS	HS	NS	NS	MS
Intrusiveness	NI	HI	NI	NI	MI	HI	HI	NI
Cost Efficiency	M	L	H	L	H	L	L	M-H
Time Efficiency	M	L	H	L	H	L	L	M
Applicability	VH	M	M	M	M	M	M	M
False Positives Factors	M	L	H	M	H	M	L	H
False Negatives Factors	M	H	M	L	M	H	M	H

CHAPTER 6 CONCLUSION

6.1 Final Conclusion

In an era of increasing digitalization, the security and authenticity of hardware components have never been more pivotal. This study delved into the intricate domain of Hardware Trojan detection, specifically focusing on the utilization of path delay fingerprints as a primary mechanism for detection, highlighting their importance in the realm of hardware security. Various methods and techniques were explored, including Invasive detection techniques, Running-time detection techniques, Testing-based detection techniques, Ring-Oscillator techniques, Chemical De-layering techniques, Visual Inspection techniques, and Side-Channel Detection techniques. Special attention was given to the Path Delay Fingerprinting technique, examining its unique advantages and limitations in comparison to the previous methods. Compared to other detection techniques, Path Delay Fingerprinting offers a unique blend of non-intrusiveness, scalability, and accuracy. However, it doesn't negate the value of complementary detection methods, but rather emphasizes that a multi-faceted approach for hardware security is both prudent and effective. Meanwhile, several challenges were encountered during this study. The vast diversity in potential Trojan designs and their possible placements can make them incredibly elusive. Furthermore, the natural variations in manufacturing, environmental influences, and aging effects often introduce noise into the delay measurements, requiring sophisticated algorithms and calibration techniques to extract meaningful results.

The increasing complexity of integrated circuits and the proliferation of the IOT devices present a vast landscape for potential Trojan attacks. As we look to the future, the need for advancements in Hardware Trojan detection will only grow. While path delay fingerprinting has proven to be an invaluable tool, it is incumbent upon the research community to continue innovating, refining existing methods, and developing new techniques to safeguard our digital world and giving an unyielding commitment to stay one step ahead of potential threats.

6.2 Future expansions

In light of the findings presented in this thesis, several avenues for future exploration emerge. One promising direction is the development of advanced algorithms tailored to minimize false detection rates across various Trojan detection techniques. Additionally, the integration of machine learning models could offer a transformative approach to Hardware Trojan identification, warranting further investigation. Research in this area could focus on how machine learning algorithms can be tailored to each specific detection technique. In addition, environmental calibration techniques also present an opportunity for enhancing detection accuracy, particularly in mitigating false positives and negatives. Moreover, the theoretical comparisons made in this study underscore the need for empirical, real-world testing to validate the effectiveness of those methods. Lastly, given the focus on path delay fingerprinting, future research could benefit from empirical studies or prototype development, to ascertain its practical applicability in real-world scenarios.

References

- [1] VAN ECK, Wim. Electromagnetic radiation from video display units: An eavesdropping risk?. Computers & Security, 1985, 4.4: 269-286.
- [2] TEHRANIPOOR, Mohammad; KOUSHANFAR, Farinaz. A survey of hardware trojan taxonomy and detection. IEEE Design & Test of Computers, 2016, 01: 1-1.
- [3] MEAD, Carver; CONWAY, Lynn. Introduction to VLSI systems. 1980.
- [4] WESTE, Neil HE; HARRIS, David. CMOS VLSI design: a circuits and systems perspective. Pearson Education India, 2015.
- [5] M MORRIS, Mano, et al. Digital Design With an Introduction to the Verilog HDL FIFTH EDITION. 2013.
- [6] WOLF, Wayne. Modern VLSI Design: IP-Based Design (paperback). Pearson Education, 2008.
- [7] BHASIN, Shivam, et al. Hardware Trojan horses in cryptographic IP cores. In: 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography. IEEE, 2013. p. 15-29.
- [8] JIN, Yier; KUPP, Nathan; MAKRIS, Yiorgos. Experiences in hardware Trojan design and implementation. In: 2009 IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE, 2009. p. 50-57.
- [9] JIN, Yier; MAKRIS, Yiorgos. Hardware Trojan detection using path delay fingerprint. In: 2008 IEEE International workshop on hardware-oriented security and trust. IEEE, 2008. p. 51-57.
- [10] FRANCO, Julien; FRICK, Florian. Introduction to hardware Trojan detection methods. In: 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2015. p. 770-775.
- [11] TEHRANIPOOR, Mohammad; KOUSHANFAR, Farinaz. A survey of hardware trojan taxonomy and detection. IEEE design & test of computers, 2010, 27.1: 10-25.

- [12] BHASIN, Shivam; REGAZZONI, Francesco. A survey on hardware trojan detection techniques. In: 2015 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2015. p. 2021-2024.
- [13] MOEIN, Samer, et al. Classification of hardware trojan detection techniques. In: 2015 Tenth International Conference on Computer Engineering & Systems (ICCES). IEEE, 2015. p. 357-362.
- [14] ABRAMOVICI, Miron; BRADLEY, Paul. Integrated circuit security: new threats and solutions. In: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. 2009. p. 1-3.
- [15] ZHANG, Xuehui; TEHRANIPOOR, Mohammad. RON: An on-chip ring oscillator network for hardware Trojan detection. In: 2011 Design, Automation & Test in Europe. IEEE, 2011. p. 1-6.
- [16] TORRANCE, Randy; JAMES, Dick. The state-of-the-art in IC reverse engineering. In: International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. p. 363-381.
- [17] SKOROBOGATOV, Sergei P.; ANDERSON, Ross J. Optical fault induction attacks. In: Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4. Springer Berlin Heidelberg, 2003. p. 2-12.
- [18] AGRAWAL, Dakshi, et al. Trojan detection using IC fingerprinting. In: 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007. p. 296-310.
- [19] COZZI, Maxime; GALLIERE, Jean-Marc; MAURINE, Philippe. Thermal scans for detecting hardware Trojans. In: Constructive Side-Channel Analysis and Secure Design: 9th International Workshop, COSADE 2018, Singapore, April 23–24, 2018, Proceedings 9. Springer International Publishing, 2018. p. 117-132.
- [20] ZHANG, Xuehui; XIAO, Kan; TEHRANIPOOR, Mohammad. Path-delay fingerprinting for identification of recovered ICs. In: 2012 IEEE International symposium on

defect and fault tolerance in VLSI and nanotechnology systems (DFT). IEEE, 2012. p. 13-18.

- [21] CUI, Xiaotong, et al. Hardware Trojan detection using the order of path delay. ACM Journal on Emerging Technologies in Computing Systems (JETC), 2018, 14.3: 1-23.
- [22] EXURVILLE, Ingrid, et al. Practical measurements of data path delays for IP authentication & integrity verification. In: 2013 8th International Workshop on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC). IEEE, 2013. p. 1-6.
- [23] HASEGAWA, Kento; SHI, Youhua; TOGAWA, Nozomu. Hardware trojan detection utilizing machine learning approaches. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018. p. 1891-1896.
- [24] KUMAR, Prasanna; SRINIVASAN, Ramasamy. Detection of hardware Trojan in SEA using path delay. In: 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science. IEEE, 2014. p. 1-6.