

University of Windsor

## Scholarship at UWindor

---

Electronic Theses and Dissertations

Theses, Dissertations, and Major Papers

---

6-18-2021

# A Design for Test and Security Methodology for Integrated Circuits

Tareq Muhammad Supon  
*University of Windsor*

Follow this and additional works at: <https://scholar.uwindsor.ca/etd>

---

### Recommended Citation

Supon, Tareq Muhammad, "A Design for Test and Security Methodology for Integrated Circuits" (2021). *Electronic Theses and Dissertations*. 8616.  
<https://scholar.uwindsor.ca/etd/8616>

This online database contains the full-text of PhD dissertations and Masters' theses of University of Windsor students from 1954 forward. These documents are made available for personal study and research purposes only, in accordance with the Canadian Copyright Act and the Creative Commons license—CC BY-NC-ND (Attribution, Non-Commercial, No Derivative Works). Under this license, works must always be attributed to the copyright holder (original author), cannot be used for any commercial purposes, and may not be altered. Any other use would require the permission of the copyright holder. Students may inquire about withdrawing their dissertation and/or thesis from this database. For additional inquiries, please contact the repository administrator via email ([scholarship@uwindsor.ca](mailto:scholarship@uwindsor.ca)) or by telephone at 519-253-3000ext. 3208.

**A Design for Test and Security Methodology for Integrated Circuits**

By

**Tareq Muhammad Supon**

A Dissertation  
Submitted to the Faculty of Graduate Studies  
through the Department of Electrical and Computer Engineering  
in Partial Fulfillment of the Requirements for  
the Degree of Doctor of Philosophy  
at the University of Windsor

Windsor, Ontario, Canada

2021

© 2021 Tareq Muhammad Supon

**A Design for Test and Security Methodology for Integrated Circuits**

by

**Tareq Muhammad Supon**

APPROVED BY:

---

K. El-Sankary, External Examiner  
Dalhousie University

---

R. Riahi  
Department of Mechanical, Automotive & Materials Engineering

---

E. Abdel-Raheem  
Department of Electrical and Computer Engineering

---

H. Wu  
Department of Electrical and Computer Engineering

---

R. Rashidzadeh, Co-Advisor  
Department of Electrical and Computer Engineering

---

R. Muscedere, Co-Advisor  
Department of Electrical and Computer Engineering

April 01, 2021

---

# DECLARATION OF CO-AUTHORSHIP AND PREVIOUS PUBLICATION

---

## I. Co-Authorship

I hereby declare that this dissertation incorporates material that is the result of joint research, as follows:

Chapters 2 and 3, of the dissertation, were co-authored with Mahasadat Seyedbarhagh under the supervision of Dr. Rashid Rashidzadeh (Chapter 2, 3) and Dr. Roberto Muscedere (Chapter 2). In both cases, the key ideas, primary contributions, experimental designs, data analysis, and interpretation were performed by the author, and Mahasadat Seyedbarhagh contributed to the writing and revisions of the papers. Chapters 4 and 5 were supervised by Dr. Rashid Rashidzadeh.

I am aware of the University of Windsor Senate Policy on Authorship, and I certify that I have properly acknowledged the contribution of other researchers to my dissertation and have obtained written permission from each of the co-author(s) to include the above material(s) in my dissertation.

I certify that, with the above qualification, this dissertation, and the research to which it refers, is the product of my research works.

## II. Previous Publication

This thesis includes four original papers that have been previously published/submitted for publication in peer reviewed journals, and conference proceedings, as follows:

<b>Thesis Chapter</b>	<b>Title of the Publication</b>	<b>Publication Status</b>
<b>Chapter 2</b>	<b>T. M. Supon</b> , M. Seyedbarhagh, R. Rashidzadeh and R. Muscedere, “Hardware Trojan Prevention Through Limiting Access to the Active Region,” <i>2019 14th Int. Conf. on Design &amp; Technology of Integrated Systems In Nanoscale Era (DTIS)</i> , Mykonos, Greece, 2019, pp. 1-6 .	Published
<b>Chapter 3</b>	<b>T. M. Supon</b> , M. Seyedbarhagh and R. Rashidzadeh, “A Method to Prevent Hardware Trojans Limiting Access to Layout Resources,” in <i>Microelectronics Reliability</i> .	2 <sup>nd</sup> Revision Submitted
<b>Chapter 4</b>	<b>T. M. Supon</b> and R. Rashidzadeh, “On-Chip Magnetic Probes for Hardware Trojan Prevention and Detection,” in <i>IEEE Transactions on Electromagnetic Compatibility</i> , doi: 10.1109/TEMC.2020.3003728.	Published
<b>Chapter 5</b>	<b>T. M. Supon</b> and R. Rashidzadeh, “Hardware Trojan Prevention using Memristor Technology,” <i>Microprocessors and Microsystems</i> , Submitted.	Submitted

I certify that I have obtained a written permission from the copyright owner(s) to include the above published material(s) in my thesis. I certify that the above material describes work completed during my registration as a graduate student at the University of Windsor.

### **III. General**

I declare that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained written permission from the copyright owner(s) to include such material(s) in my thesis.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

---

# ABSTRACT

---

The costs of in-house IC fabrication have increased significantly with new technology nodes and nanoscale transistors. Many companies have outsourced their need for IC fabrication to eliminate the overhead costs associated with operating a fabrication facility. While outsourcing has its benefits, it provides opportunities for hardware Trojan (HT) injection at different design levels. Hardware Trojans and IP piracy are the new realities that must be considered for trustworthy IC design. The miniature size of HTs, coupled with their diversity and unpredictable effects, makes them difficult to detect. Even though various solutions and design methods have been proposed to address security concerns posed by HTs, a comprehensive solution is yet far from reach. Moreover, the effects of Process, Voltage, and Temperature (PVT) variations have been largely neglected in the reported solutions which may undermine their effectiveness. This dissertation presents Hardware Trojan prevention techniques that are resilient to PVT variations.

In this dissertation, two new Design-For-Security (DFS) solutions for HT prevention using a layout filling technique and a layout manipulation method are presented. The first DFS technique involves occupying the unused polysilicon layer with minimum feature wires to deprive attackers of the resources needed for Trojan routing. This technique prevents attackers from inserting an active layer on the silicon

substrate. Since the active layer connects to the polysilicon layer directly, if the unused poly layer is covered with minimum size wires, it becomes impossible for an attacker to rout a HT without removing a portion of the polysilicon wires. A readout circuit is used to ensure that the layer is intact and has not been tampered with. This technique can provide a complete utilization of the unused areas of the polysilicon layer.

A novel tamper resilient solution is also presented as the second DFS technique to capture integrated circuits' electromagnetic (EM) signature. In this method, the remaining metal and polysilicon layers are utilized as internal magnetic probes to monitor the device's signature and, in the meantime, deprive attackers of layout resources to route HTs. 3D full-wave EM field simulations using High-Frequency Structural Simulator (HFSS) show that tampering with a chip to insert a Trojan of  $12 \mu\text{m}^2$ , the area required to insert an inverter, can be detected through the magnetic signature. Some unique HTs native to 3D ICs, such as HTs inserted during “Die Stacking” and “TSV Bonding” stages, can also be detected using this technique.

A solution utilizing memristor technology is also presented in this dissertation to implement a configurable layout to obfuscate the design. The main design is divided into sub-circuits and forwarded to a fabrication foundry, but the interconnects between those are not revealed to the foundry. The sub-circuits are connected through configurable memristor switches after fabrication. In the proposed solution, split manufacturing is not needed, and an untrusted foundry can fabricate the circuit without compromising its security. Moreover, the proposed technique provides direct access to the sub-circuits through a network of configurable switches. This will increase the observability and controllability at the test phase and help detect and isolate possible Trojans.



---

## DEDICATION

---

*To my lovely wife, Dr. Mithua Zafrin, who supported me all the way.*

---

## ACKNOWLEDGMENT

---

I would like to extend my acknowledgment to the people without whom this dissertation would never have been accomplished. First and foremost, my wonderful loving wife, Dr. Mithua Zafrin, whose continuous support has provided me with the inspiration, power, and dedication I needed to complete this work. She also put her career to a halt while I finish my studies.

I cannot thank enough my honorable supervisor, Dr. Rashid Rashidzadeh, and co-advisor Dr. Roberto Muscedere, who were my guidance throughout. Dr. Rashidzadeh was monumental in helping me always. The amount of time he spent with me correcting and suggesting my research plan and the effort he put behind me is outstanding.

I appreciate my wonderful committee members, Dr. Reza Riahi from Mechanical, Automotive & Materials Engineering, Dr. Esam Abdel-Raheem, and Dr. Huapeng Wu from Electrical Engineering; their constructive feedback and kind words have made my work even easier and influenced me to go ahead.

Lastly, I would like to thank everyone that I have ever talked to or met during my stay at the University of Windsor.

---

# TABLE OF CONTENTS

---

<b>DECLARATION OF CO-AUTHORSHIP AND PREVIOUS PUBLICATION</b> .....	iii
<b>ABSTRACT</b> .....	vi
<b>DEDICATION</b> .....	viii
<b>ACKNOWLEDGEMENT</b> .....	ix
<b>NOMENCLATURE</b> .....	xiii
<b>LIST OF TABLES</b> .....	xvi
<b>LIST OF FIGURES</b> .....	xvii
<b>LIST OF APPENDICES</b> .....	xxi
<b>Chapter 1 INTRODUCTION</b> .....	1
1.1. HARDWARE TROJAN .....	4
A <i>Hardware Trojan Taxonomy</i> .....	4
B <i>Hardware Trojan Design</i> .....	6
1.2. HARDWARE SECURITY METHODS.....	7
A. <i>Hardware Trojan Detection</i> .....	8
B. <i>Hardware Trojan Prevention</i> .....	11
1.3. HARDWARE TROJAN PREVENTION USING LAYOUT FILLING METHOD .....	15
A. <i>Filling Only Unused Polysilicon Layer with Polysilicon Wires</i> .....	16
B. <i>Filling Entire Unused Space of the Die with Polysilicon and Metal Wires</i> .....	16
C. <i>HT Prevention by Layout Manipulation Using Memristor Devices</i> .....	17
<b>REFERENCE</b> .....	20

<b>CHAPTER 2</b>	<b>HARDWARE TROJAN PREVENTION THROUGH LIMITING ACCESS TO THE ACTIVE REGION</b>	29
2.1	INTRODUCTION	29
2.2	PROPOSED METHOD	33
2.3	READOUT CIRCUIT	36
A	<i>Description of the Readout Circuit</i>	36
B	<i>Working Principle of the Readout Circuit</i>	38
2.4	SIMULATION RESULTS	39
2.5	CONCLUSION	45
	ACKNOWLEDGMENT	46
	REFERENCES	46
<b>Chapter 3</b>	<b>A METHOD TO PREVENT HARDWARE TROJANS LIMITING ACCESS TO LAYOUT RESOURCES</b>	49
3.1	INTRODUCTION	49
3.2	PROPOSED METHOD	56
A	<i>Delay Measurement</i>	56
B	<i>Detecting Signature Variation</i>	60
3.3	READOUT CIRCUIT	62
A	<i>Description of the Readout Circuit</i>	62
B	<i>Working Principle of the Readout Circuit</i>	64
3.4	SIMULATION RESULTS	65
3.5	CONCLUSION	74
	ACKNOWLEDGMENT	75
	REFERENCES	75
<b>Chapter 4</b>	<b>ON-CHIP MAGNETIC PROBES FOR HARDWARE TROJAN PREVENTION AND DETECTION</b>	81
4.1	INTRODUCTION	81
A	<i>HT Detection</i>	83
B	<i>HT prevention</i>	84
4.2	BACKGROUND STUDY	86
4.3	ANALYTICAL DESCRIPTION OF THE PROPOSED METHOD	88
A	<i>Circuit Model for a Magnetic Probe</i>	91

<i>B</i>	<i>Effect of the Geometric Structure on the EM Signature</i> .....	95
<i>C</i>	<i>Circuit Model for a Magnetic Probe</i> .....	96
4.4	SIMULATION RESULTS .....	97
4.5	CONCLUSION .....	110
	REFERENCES .....	110
<b>Chapter 5</b>	<b>HARDWARE TROJAN PREVENTION USING MEMRISTOR TECHNOLOGY</b>	<b>118</b>
5.1	INTRODUCTION.....	118
5.2	PRELIMINARIES .....	124
<i>A</i>	<i>Generic Hardware Trojan</i> .....	124
<i>B</i>	<i>The Basic Idea Behind Design Obfuscation</i> .....	125
<i>C</i>	<i>Memristive Devices</i> .....	126
5.3	PROPOSED TROJAN AND IP PIRACY PREVENTION TECHNIQUE.....	129
<i>A</i>	<i>Proposed Netlist Obfuscation Scheme</i> .....	129
<i>B</i>	<i>Proposed Design Flow Based on the Hardware Trojan Prevention Method</i> .....	136
<i>C</i>	<i>Implementation of Proposed Hardware Trojan Prevention Technique in ISCAS '85 Benchmark Circuit, C432</i> .....	139
<i>D</i>	<i>Security Analysis of the Proposed Technique</i> .....	139
5.4	SIMULATION RESULTS AND COMPARISON.....	141
5.5	CONCLUSION .....	146
	ACKNOWLEDGMENT .....	146
	REFERENCES .....	146
<b>Chapter 6</b>	<b>CONCLUSION AND FUTURE WORK</b> .....	<b>154</b>
<b>APPENDICES</b> .....		<b>157</b>
Appendix A – LIST OF PAPERS DURING PH.D. THAT ARE NOT RELATED TO THE DISSERTATION TOPIC .....		157
Appendix B – PERMISSION TO REUSE CONTENT .....		158
<b>VITA AUCTORIS</b> .....		<b>160</b>

---

# NOMENCLATURE

---

<b>Abbreviation</b>	<b>Full Form</b>	<b>Page</b>
3PIP	Third-party IP	10, 53
ADS	Advanced Design System	97
BISA	Built-In Self Authentication	13, 31, 55, 86, 145
BIST	Built-In-Self Test	51, 86
CAD	Computer-Aided Design	6, 120
CP	Charge Pump	36, 62
CUT	Circuit Under Test	8, 37, 62
DAC	Digital to Analog Converter	97
DARPA	Defense Advanced Research Projects Agency	3, 119
DDM	Delay-Detection-Module	32, 56
DfHT	Design for Hardware Trust	9, 11, 52, 84
DFS	Design-For-Security	55
DLL	Delay Locked Loop	36, 62
DTIS	Design & Technology of Integrated Systems In Nanoscale Era	19

<b>Abbreviation</b>	<b>Full Form</b>	<b>Page</b>
EM	Electromagnetic	82, 83
FF	Flip-Flops	12, 31, 54, 87
HFSS	High-Frequency Structure Simulator	34, 57
HINT	Holistic Approaches for Integrity of ICT Systems	3, 29, 119
HT	Hardware Trojan	1, 29, 50, 81, 118
IC	Integrated Circuit	1, 49, 118
ICT	Information and Communication Technologies	3, 119
IoT	Internet of Things	3, 29, 50
IP	Intellectual Property	6, 120
LFSR	Linear Feed Back Shift Register	86
LPF	Low Pass Filter	36, 62
Memristor	Memory Resistor	17
MEMS	Micro-Electro-Mechanical-Systems	118
MISR	Multiple Input Shift Registers	13, 31, 55, 86
NSERC	Natural Sciences and Engineering Research Council	46, 75, 146
ORA	Output Response Analyzer	13, 31, 55
PFD	Phase Frequency Detector	36, 62
PVT	Process, Voltage, and Temperature	11, 36, 62, 84
RO	Ring Oscillator	82
RTL	Register Transfer Level	6
SNR	Signal-to-Noise-Ratio	9, 30, 50, 52, 83, 96

<b>Abbreviation</b>	<b>Full Form</b>	<b>Page</b>
STG	State Transition Graph	131
TA	Time Amplifier	63
TCA	Trojan-to-circuit Switching Activity	52
TDC	Time-to-Digital Converter	37, 62, 63
TPG	Test Pattern Generator	13, 55, 87
TRNG	True Random Number Generator	82
TSA	Trojan-to-circuit Switching Activity	9
TSV	Through-Silicon-Via	2, 81



---

## LIST OF TABLES

---

TABLE 2.1. TDC OUTPUT SHOWING LINEAR RELATION WITH DELAY .....	44
TABLE 2.2. COMPARISON WITH CURRENT METHODS.....	45
TABLE 3.1. TDC OUTPUT SHOWING LINEAR RELATION WITH DELAY .....	68
TABLE 3.2. COMPARISON WITH CURRENT METHODS .....	73
TABLE 4.1. VARIATION BETWEEN THE $S_{21}$ OF THE ORIGINAL AND THE MANIPULATED DESIGN AT 500 MHZ.....	104
TABLE 4.2. COMPARISON WITH THE STATE-OF-THE-ART METHODS.....	107
TABLE 5.1. CHARACTERISTICS BETWEEN 3 DIFFERENT MEMRISTOR DEVICES FABRICATED AT UNIVERSITY OF MICHIGAN, HP LABS AND ARIZONA STATE UNIVERSITY .....	128
TABLE 5.2. COMPARISON OF THE PROPOSED METHOD WITH SPLIT MANUFACTURING TECHNIQUES OF CIRCUIT432 IN TERMS OF OVERHEAD .....	145
TABLE 5.3. DESIGN OVERHEAD OF THE PROPOSED TECHNIQUE.....	145

---

# LIST OF FIGURES

---

Figure 1.1. Minimum feature size scaling trend for Intel logic technologies [2].	2
Figure 1.2. Generalized concept of a Hardware Trojan [9].	4
Figure 1.3. Detailed taxonomy showing physical, location, activation, and action characteristics of Trojans (Inspired from [16]).	5
Figure 1.4. A typical design flow of IC manufacturing process [9].	6
Figure 1.5. Classification of Hardware Trojan Design [3].	7
Figure 1.6. Taxonomy of measures against hardware Trojans. (inspired by [3]).	13
Figure 1.7. A typical CMOS process indicating layout layers: (a) 3D view (b) Top view [59].	15
Figure 1.8. (a) Routing of a typical digital-to-analog circuit in HFSS environment. (b) Unused layers used as magnetic probes. [61].	17
Figure 1.9. Crossing nanowires are separated by memristor switches at the junctions that can be electrically configured. Nanowire crossbars are connected to a CMOS chip via metallic pins over the CMOS stack [9].	18
Figure 2.1. A typical CMOS process indicating layout layers. (a) Cross section. (b) Top view [21].	32
Figure 2.2. 3D full wave simulation results indicating the electric field difference between (a) the original and (b) the Trojan affected design.	33
Figure 2.3. (a) Conventional Delay Locked Loop, (b) Readout Circuit.	35
Figure 2.4. Circuit-Under-Test.	38
Figure 2.5. The IC with Polysilicon and Readout Circuit added.	39
Figure 2.6. (a) The Locked Signal (b) Control Voltage of the DLL and (c) Delay between the Output and the Input Signals.	40

Figure 2.7. Relationship between VCDL Delay and Control Voltage. ....	41
Figure 2.8. (a) Typical TSMC Inverter (b) Minimum poly needed to be removed to place that inverter (c) Delay caused by that poly. ....	41
Figure 2.9. The IC with polysilicon layer partially removed to insert Trojan. ....	42
Figure 2.10. Time delay and variation. ....	42
Figure 2.11. Delay variation due to change in (a) Temperature, (b) Length and (c) Width. ....	43
Figure 3.1. A typical CMOS process indicating layout layers: (a) 3D view (b) Top view [36]. ....	57
Figure 3.2. 3D full wave simulation indicating the electric field difference between (a) the original and (b) the Trojan affected design. ....	58
Figure 3.3. (a) Conventional Delay Locked Loop, (b) Readout Circuit with Signature detection block. ....	59
Figure 3.4. (a) Block diagram of a typical routing path and the polysilicon wire underneath (b) The equivalent schematic diagram of the same showing the coupling circuit. ....	61
Figure 3.5. Circuit-Under-Test. ....	64
Figure 3.6. The IC with Polysilicon and Readout Circuit added. ....	65
Figure 3.7. (a) Control Voltage of the DLL (b) The Locked Signal and (c) Delay between the Output and the Input Signals. ....	66
Figure 3.8. Relationship between VCDL Delay and Control Voltage. ....	67
Figure 3.9. (a) Typical TSMC Inverter (b) Minimum poly needed to be removed to place that inverter (c) Delay caused by that poly. ....	67
Figure 3.10. (a) Delay of the original routing segment 2; (b) Delay variation due to the removal of a portion of the polysilicon wire. ....	68
Figure 3.11. Output voltage (a) without probe (b) with probe; (c) difference between a and b; and (d) The unique signature. ....	69
Figure 3.12. The IC with polysilicon layer partially removed to insert Trojan. ....	70
Figure 3.13. Graph showing change between the signatures of the original and the manipulated design. ....	71
Figure 3.14. Monte Carlo Simulation for 500 iterations: (a) Output of the main circuit; (b) The signature. ....	72

Figure 3.15. Delay variation due to change in (a) Temperature, (b) Length and (c) Width. .....	72
Figure 4.1. (a) Routing of a typical Digital to Analog circuit in HFSS environment, (b) Unused layers used as magnetic probes.....	89
Figure 4.2. (a) A typical distribution of a signal routing path and a magnetic probe, (b) 3D illustration of a signal trace and a probe branch pair. ....	90
Figure 4.3. (a) Block diagram of the signal trace and a probe branch pair shown in Fig. 4.2. (b) The equivalent schematic diagram of Fig. 4.3 (a) indicating the routing path of the inverter and the coupling circuit together with the signature detection circuit.....	91
Figure 4.4. (a) Equivalent two-port network created by a signal trace and probe branch pair in high frequency (b) Equivalent model of such a pair. ....	93
Figure 4.5. Extracted model of the two-port network shown in Fig. 4.4 (a) at 500 MHz, where trace current plays: (a) a negligible and (b) a dominant role in the induction of the probe. ....	94
Figure 4.6. Types of structures created during an EM coupling with any metal trace or another probe branch in another layer: probe branch crossing the other layer (a) vertically, (b) at an angle, and (c) probe branch run along the other layer. ....	95
Figure 4.7. (a) Magnetic flux density and (b) Electric field distribution of the design shown in Fig. 4.1 (b). ....	98
Figure 4.8. Circuit with the design of the magnetic probe: (a) Original design, and (b) manipulated design with a portion of the probe removed.....	99
Figure 4.9. Lumped models of the coupling between the routing traces and (a) the original magnetic probe, and (b) the manipulated magnetic probe. ....	100
Figure 4.10. Equivalent circuit model of the magnetic probe.....	100
Figure 4.11. Output voltage (a) without probe (b) with probe; (c) difference between a and b; and (d) The unique signature. ....	101
Figure 4.12. Graph showing the signature of the (a) Original design and (b) Manipulated design of Fig. 4.8. (c) Difference between (a) and (b). ....	103
Figure 4.13. S-Parameters of the circuit with (a) original magnetic probe, and (b) manipulated magnetic probe. ....	103
Figure 4.14. Monte Carlo analysis over 500 iterations for $\pm 5\%$ variation of width and length of the probes.....	104
Figure 4.15. Final IC routing including the design of the magnetic probe: (a) the output of the initial design connected to the bottom layer of the final routing using TSV (b) original	

design of the final IC routing, and (c) a portion of metal is removed from, (d) an extra die has been added. ....	105
Figure 4.16. S-Parameters of the routing of the IC of Fig. 4.15 with (a) original magnetic probe, (b) magnetic probe with a portion of metal removed, and (c) magnetic probe with extra die added. ....	106
Figure 4.17. Graph showing the signature of the (a) Original design and (b) Manipulated design of Fig. 4.15 (b, c). and (c) Difference between those two signatures.....	106
Figure 4.18. Graph showing the signature of the (a) Original design and (b) Manipulated design of Fig. 4.15 (b, d). and (c) Difference between those two signatures. ....	108
Figure 4.19. Graph showing change in signatures due to (a) Process, (b) Voltage and (c) Temperature variations. ....	109
Figure 5.1. A typical design flow of IC manufacturing process. ....	119
Figure 5.2. Generic Hardware Trojan. ....	124
Figure 5.3. Crossing nanowires are separated by memristor switches at the junctions that can be electrically configured. Nanowire crossbars are connected to a CMOS chip via metallic pins over the CMOS stack. ....	127
Figure 5.4. Example of original and obfuscated STG. Uncertain interconnections between selected nodes obscure the original STG and hide the rare events. ....	131
Figure 5.5. The grids of crossing nanowires that are configured by memristive switches using ‘Via’ pins. Shift registers are used as boundary scan registers for testing the clusters. ....	135
Figure 5.6. The proposed design flow based on the presented Hardware Trojan and IP piracy prevention technique.....	137
Figure 5.7. (a) Block diagram of ISCAS ’85 C432 Circuit (b) The netlist is divided into five clusters. Connections between clusters are realized with memristor switches through nanocrossbar structure. Memristor switches in the ON state and OFF state are presented by blue and white circles, respectively. ....	138
Figure 5.8. Modified LTspice code for memristor inspired by the model proposed by Chang et al. in [37].....	143
Figure 5.9. Simulation results for the memristor using a Spice model inspired by the model proposed by Chang et al [39]: (a) The variation of current due to the change of voltage (b) The pinched hysteresis loop created by the current as a function of voltage (c) Change of the resistance due to the change in voltage (d) Variation of power consumption due to the variation of voltage. ....	144

---

## LIST OF APPENDICES

---

Appendix A – LIST OF PAPERS DURING PH.D. THAT ARE NOT RELATED TO THE DISSERTATION TOPIC .....	157
Appendix B – PERMISSION TO REUSE CONTENT .....	158

---

# Chapter 1

---

## INTRODUCTION

---

Integrated Circuit (IC) design involves several stages, including simulation, layout generation, fabrication, packaging, and testing. Semiconductor companies could handle all of these steps in-house in the early days. As the semiconductor technology evolved, so did the costs of new fabrication nodes. Meanwhile, as the competition between companies intensified, the design to market time became a significant factor in the success or failure of electronic products. As a result, many companies started outsourcing their IC fabrication to overseas foundries to meet the market challenges [1]. The outsourcing lowered the fabrication costs considerably, allowing companies to devote their resources to research and development. While outsourcing has many benefits, it comes with drawbacks. Aside from the technical knowledge that impairs and fades over time, the security of electronic products can be undermined due to outsourcing. Foundries can modify IC designs by adding extra circuits to reveal sensitive information stored on chips. The hardware circuits added to ICs to alter their functionalities are called Hardware Trojan (HT). In general terms, Hardware Trojan (HT) can be defined as any malicious modification of the original circuit to alter its characteristics that may lead to failure, leakage of confidential information, shortage of the expected lifetime, denial of service under certain conditions or, in general, any undesirable effect on ICs.

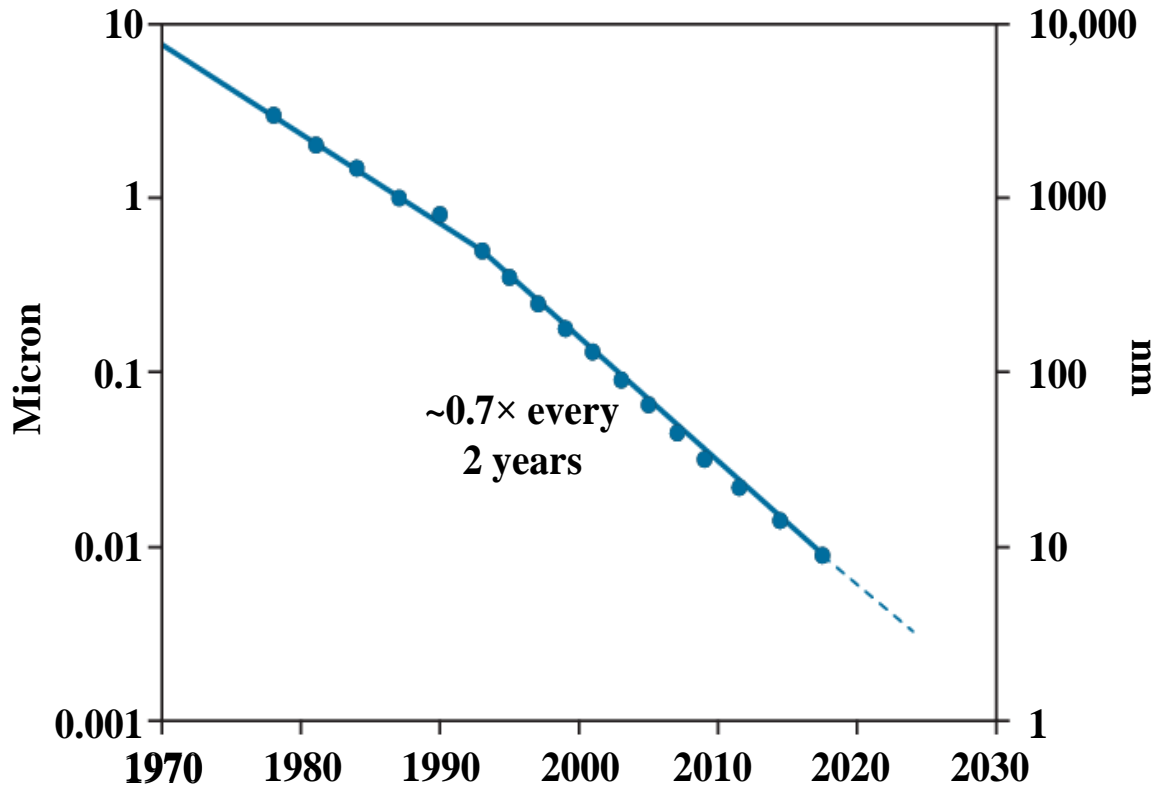


Figure 1.1. Minimum feature size scaling trend for Intel logic technologies [2].

The CMOS technology scaling has slowed down, as shown in Fig. 1.1, due to many technical challenges. 3D IC technologies have emerged as viable solutions to keep up with the demand to add more functionalities to a single chip. The introduction of 3D ICs has reduced the vulnerability against conventional HT attacks and introduced new threats [3], [4]. A 3D IC is usually fabricated by stacking different 2D layers together. The stacked dies are bonded using through-silicon vias (TSVs). 3D ICs have some advantages over 2D chips, such as 1) a 3D IC can be fabricated using split manufacturing by distributing the routing of a single circuit across different dies; 2) modified versions of conventional 2D IC security solutions can be added to different dies to enhance the security of each die [3]. The stacking process of a 3D IC conceals the circuit design details, making reverse engineering challenging [5].



Moreover, the stacked structure of a 3D IC makes it easier to obtain active layers from different foundries. On the other hand, the noise in 3D ICs is commonly higher than the conventional 2D counterparts, which can mask the effects of HTs. Furthermore, the limited access to the internal layers of a 3D IC makes it even harder to detect HTs once the IC is fabricated.

The threat of HTs has drawn more attention after discovering counterfeit chips destined for safety and security-critical systems such as high-speed train breaks, hostile radar tracking in F-16 fighters, and ballistic missile defense control systems and Falcon 5000 nuclear identification tool during recent years [6]. These alarming security concerns about the vulnerability of ICs to HTs have resulted in preventive measures such as the Trust in ICs initiated in US by Defense Advanced Research Projects Agency (DARPA) [7] and the Holistic Approaches for Integrity of ICT (Information and Communication Technologies) – Systems (HINT) project [8] originated in Europe.

Modern electronic devices, such as RFID tags, IoT (Internet of Things) devices, home appliances, or even biomedical equipment, can be vulnerable to security threats [10-12] if Hardware Trojans infect them. If an attacker gets the complete knowledge of a circuit, he/she can design Hardware Trojans with small footprints that can be easily obscured [13]. The insertion of a HT can compromise the reliability and functionality of an IC or a system [14–16]. Trojans not only can leak critical information or secret keys stored in a chip, but they also can jeopardize its functionality.

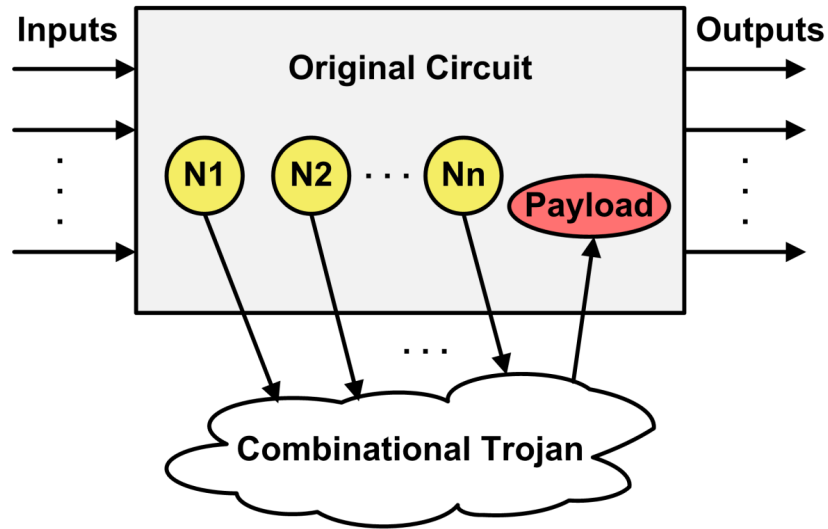


Figure 1.2. Generalized concept of a Hardware Trojan [9].

### 1.1. HARDWARE TROJAN

The operation of a generic hardware Trojan is illustrated in Fig. 1.2. A Trojan observes a group of selected internal nodes known as triggering nodes, indicated by  $N_1$  to  $N_n$  in Fig. 1.2. The status of trigger nodes is used to activate the Trojan under rare circumstances. The trigger is selected from a set of nodes whose combination of desired outputs creates a rare condition. A Trojan can be composed of a combinatorial circuit reacting to particular trigger events. It could also contain several sequential elements forming a finite state machine in which a sequence of transitions has to be traversed before triggering the Trojan. Finally, after the triggering conditions are satisfied, the Trojans payload is delivered to unleash malicious activities that affect one or several nodes depending on the Trojan design.

#### *A Hardware Trojan Taxonomy*

Tehranipoor and Koushanfar in [16] explained a detailed hardware Trojans' taxonomy to classify Trojans depending on their physical, activation, and action

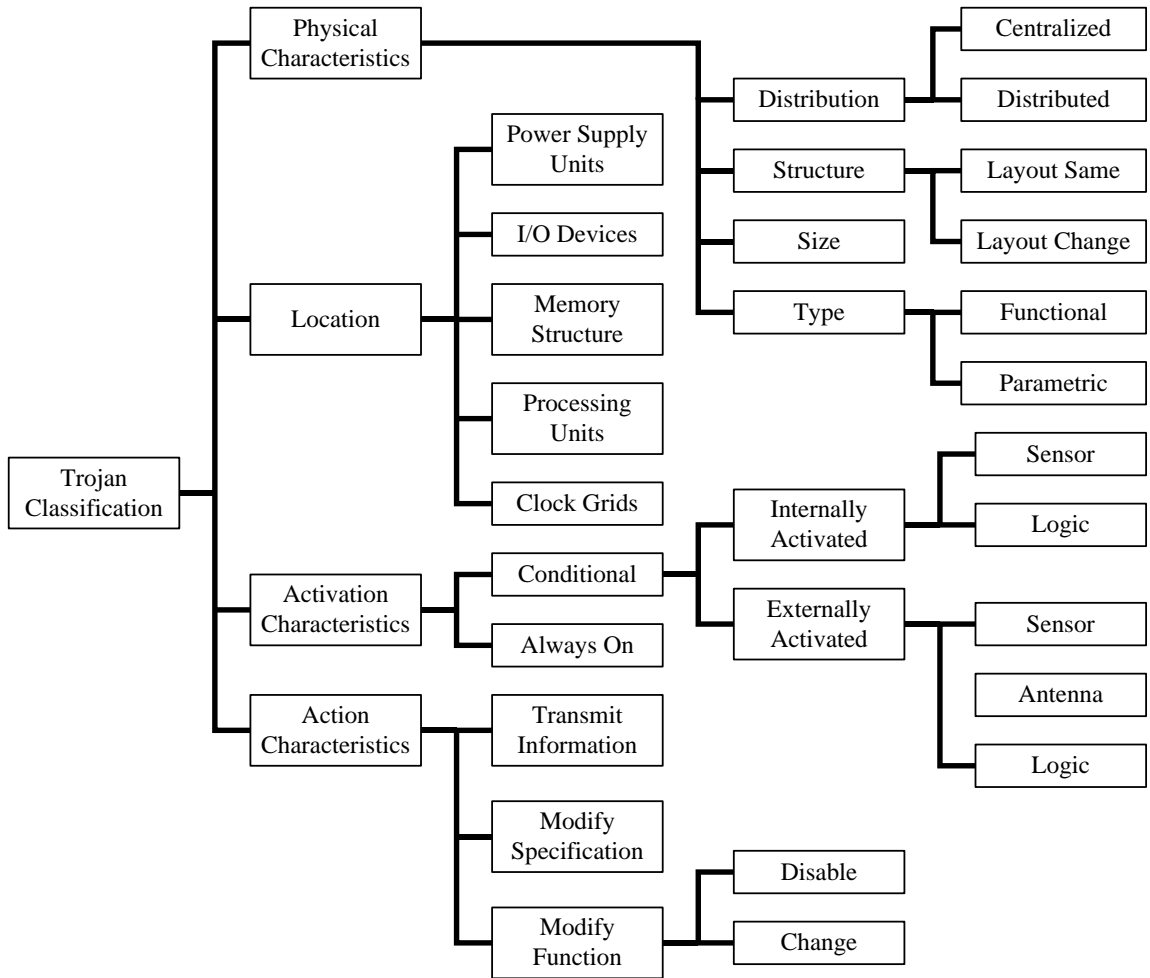


Figure 1.3. Detailed taxonomy showing physical, location, activation, and action characteristics of Trojans (Inspired from [16]).

characteristics. This taxonomy enables researchers to examine their countermeasures against different types of Trojans. The tree diagram shown in Fig. 1.3 has been inspired by the classification presented in [16]. A new classification category is introduced based on Trojans' location characteristics to simplify the Trojan taxonomy further. Also, the branches of Activation characteristics have been rearranged to reflect the classification properties accurately. As stated in [16], Trojans can be hybrids if they can have more than one activation characteristic. Nevertheless, this taxonomy highlights Trojans' main

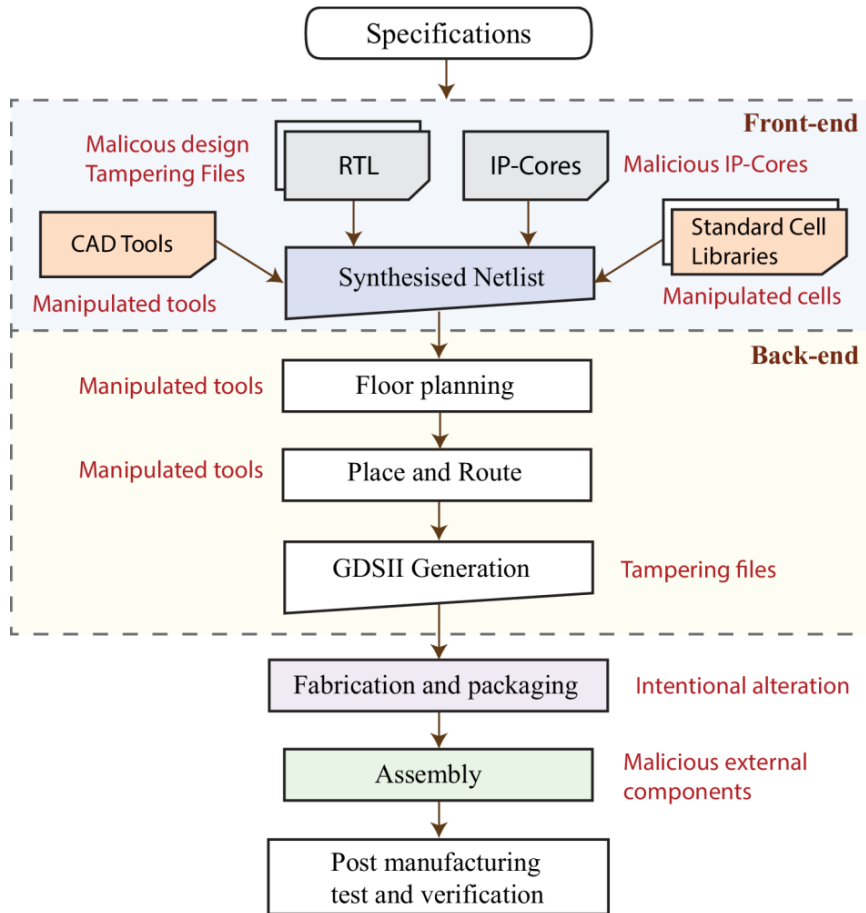


Figure 1.4. A typical design flow of IC manufacturing process [9].

characteristics and is useful for defining and evaluating the capabilities of detection and prevention strategies.

### ***B Hardware Trojan Design***

Figure 1.4 illustrates a typical design flow of IC manufacturing process along with the potential threats in each step. A Trojan can be inserted at any stage of an IC development process from Register Transfer Level (RTL) to fabrication. Assuming trusted Computer-Aided Design (CAD) tools, third-party intellectual property (IP) cores, and untampered design files, our study's primary focus will be on tackling Trojans embedded in the physical design after tape-out and during fabrication.

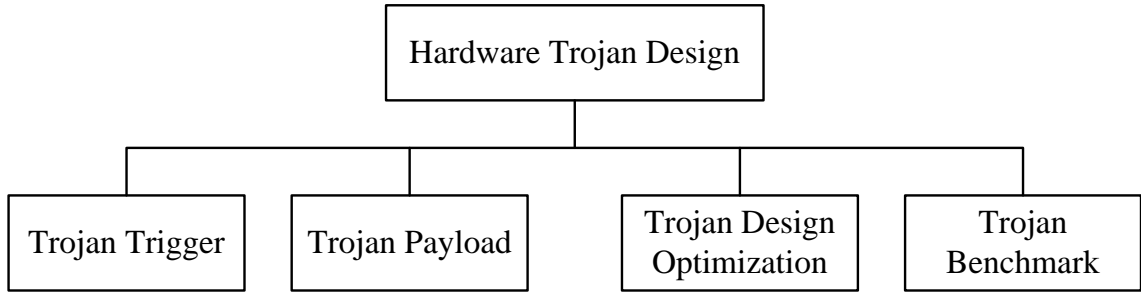


Figure 1.5. Classification of Hardware Trojan Design [3].

The design process of a hardware Trojan can be classified into four categories, as shown in Fig. 1.5 [3]. The trigger and payload mechanisms determine Trojan detection's difficulty, which led researchers to explore and evaluate novel triggers and payloads. On the other hand, the circuitry added by a Trojan can be used to develop a detection mechanism utilizing side channel effects like additional power consumption and variations of radiation, timing, and delay. Design optimization has become a part of a Trojan design to minimize the impact of the Trojan on the main circuit and avoid detection. A benchmark for different types of Trojans and trust test vectors has been developed online at [www.Trust-hub.org](http://www.Trust-hub.org) to facilitate the comparison of different detection and prevention techniques.

## 1.2. HARDWARE SECURITY METHODS

Hardware Trojans can be inserted to perform any or all of the following tasks (a) faulty operation or modification of the main function, (b) electrical modification, and (c) reliability reduction [17]. In addition to the security threats, Trojans added to the main circuit in the fabrication process can also induce economic losses related to IC production. To address the problem of hardware Trojan insertion at various IC design flow stages, researchers have adopted different solutions to target different types of

Trojans. These solutions can be divided into two major groups, namely Hardware Trojan Detection and Hardware Trojan Prevention.

#### ***A. Hardware Trojan Detection***

The design flow of the main circuit is not hampered while detecting Hardware Trojans. In all detection methods, the IC is tested for possible insertion of HTs after fabrication. At a broad level, hardware Trojan detection can be divided into three categories [16] of (a) logic testing, (b) side-channel analysis, and (c) reverse engineering.

In the logic testing method, test vectors are applied during the test phase. The test patterns are generated to perform structural tests and detect stuck-at faults [18, 19]. Test patterns used for HT detection may not excite well-designed hardware Trojans, and they may remain undetected. The restricted observability and controllability limit the potential to detect Trojans in this method. Moreover, a small alteration of the HT trigger can deny the test scheme to pinpoint a HT [20].

Side-channel analysis, such as analyzing round key operations at different cycles of AES encryption, or observing transient current or electromagnetic spectrum, can be used to detect Hardware Trojan [21–27]. This technique is non-invasive, as it does not tamper with the original circuit. This method can be used successfully to extract security-critical information, such as cryptography keys from ICs. Side-channel analysis commonly requires a trusted golden circuit to compare the results with the Circuit Under Test (CUT), which is proven difficult to obtain [3]. Most of the reported approaches [14–27] that require a golden IC, rely on invasive methods that are costly and time-consuming.

Moreover, new fabrication nodes' low supply voltage requirement acts as a detrimental factor for HT detection, as the Signal-to-Noise-Ratio (SNR) is lower compared to previous fabrication nodes. As a result, the background noise and even process variations can mask Trojan activities and prevent detection through side-channel analysis [13]. Another critical point to consider is the delay of logic gates highly affected by the supply voltage variations. The propagation delay of logic gates also increases as the voltage drop increases. Besides, other parameters like channel length ( $L$ ), channel width ( $W$ ) of transistors, the thickness of oxide ( $T_{OX}$ ), the threshold voltage ( $V_{th}$ ), process, temperature, and environmental variations can also affect the propagation delay of fabricated gates and library cells [28]. These variables make HT detection using side-channel analysis very difficult. A Design for Hardware Trust (DfHT) technique has been presented in [29] to increase the percentage variation caused by a HT compared to the original circuit to overcome the conventional limitations of the side-channel analysis. A segment of the circuit is activated, while the other segments are kept inactive to reduce the total circuit switching activity. This solution increases both the Trojan-to-circuit Switching Activity (TSA) and the power consumption ratio between the main circuit and the Trojan circuitry. The authors of [30] have presented another DfHT technique using an optically active protective  $TiO_2$ -Ti- $TiO_2$  layer stack with an angular dependent reflectivity as a chip backside. The light reflected off the chip backside has a strong angle-dependent reflectivity, which alters if the backside is tampered with by an attacker. This method has the potential to determine whether an attack took place or not by creating a pattern of photocurrents during the IC running state.

The reverse engineering method, presented in [31], is a powerful HT detection method compared to other conventional techniques, but it is costly and a destructive approach. Moreover, reverse engineering may fail, as healthy ICs may get selected for reverse engineering in situations where a small portion of fabricated ICs is infected.

With the advancements in big data analysis, researchers have developed newer methods to detect HTs, such as Visual Inspection and Machine Learning. Visual inspection [32, 33] is based on the idea of observing the top-level metal layer and comparing it with the original layout. However, non-destructive visual inspection methods cannot account for HTs designed on low metal layers. Machine learning [34] and isolation-based hardware techniques [35, 36] have also been utilized to detect HTs in IP cores used as building blocks for 3D ICs.

Third-party IP (3PIP) cores add an extra layer of complexity to the problem of Trojan detection. Cores from a third party can be divided into three main categories: (a) soft, (b) firm, and (c) hard [37]. Soft cores are the ones that are designed using hardware description language such as Verilog/VHDL. A firm core is characterized by specific libraries provided by fabrication foundries. Firm cores can be used to optimize the area through placement and routing. Researchers have proposed different ideas in [37–40] as countermeasures for HTs inserted into 3PIP cores. Hardware Trojan detection in 3PIP cores is difficult as codes or libraries or GDSII files provided by third-party designers may include Hardware Trojans. If a core is infected with a Trojan code, all fabricated ICs will be infected.



Most of the available Trojan detection methods are dedicated to detecting a specific HT type and focusing on a particular parameter variation. This shortcoming can lead to undetected Trojans. Moreover, the effect of noise and process, voltage, and temperature (PVT) variations are usually ignored during the detection process, even though these factors can mask the effects of a HT. The numerous possible ways of Trojan insertion combined with their unique triggering systems make it very difficult to detect Hardware Trojans. As a result, a comprehensive solution to detect all types of Trojans is yet far from reach. Moreover, once a Trojan is inserted, the damage is done, and even if it is detected, there is no way other than discarding the infected device. On the other hand, trojan prevention methods have the advantage of protecting ICs in the first place.

### ***B. Hardware Trojan Prevention***

The limitations and complexities of HT detection methods have motivated IC designers to modify design flow to enable HT prevention. Researchers have developed various Design-for-hardware-trust (DfHT) techniques to facilitate HT prevention and support better detection at the same time. These methods are commonly used to detect HTs through differences between the characteristics of a Trojan free IC and an infected one. The methodologies for HT prevention can be classified as (a) logic obfuscation, (b) compact GDS-II layout generation, and (c) layout filling [41].

As the name suggests, in the logic obfuscation method, the functionality of ICs [17, 42–51] is obscured. A logic obfuscation method has been introduced in [42], where reconfigurable circuits are added to the main design to prevent foundries from determining the circuit's functionality and protect it against reverse engineering. A split manufacturing flow has been introduced to obfuscate the circuit in [43]. This method can

be employed for both 2.5D and 3D IC protection. However, it cannot prevent Hardware Trojan insertion during the die stacking process and TSV bonding in 3D ICs. Chakraborty and Bhunia [44] introduced netlist-level obfuscation, where the gate-level netlist of a pre-synthesized IP core is modified and then resynthesized to support functional and structural obfuscation with a low design overhead. In [45] and [46], different state-obfuscation methods are presented, where the circuit is obfuscated with a security key. An interesting idea is presented in [47] using dummy contact-based IC camouflaging, where the functionality of a circuit is masked using dummy contacts. As a result, the same cell layout can represent different gates, depending on where dummy contacts are placed. A DfHT technique is presented in [17] using new design techniques and new memory technologies to detect various HTs in both testing and in-field operations. This technique can also prevent a wide variety of attacks during the synthesis, place and route, and IC fabrication stages. The idea presented in [48] uses gates with different doping concentrations to vary the threshold voltage and create threshold-dependent camouflaged cells. Attackers can use various approaches to determine camouflaged gates' identities, such as measuring the etch rate to find heavily doped transistors and profiling the difference in power and delay characteristics of camouflaged gates [48]. Logic Locking [49], [50] also have been classified as obfuscation methodologies. Researchers in [51] have summarized all the latest obfuscation methods with their pros and cons.

A compact GDS-II layout has been generated in [52] by adding dummy flip-flops (FFs). Even though this idea was the building block for various new layout filling approaches, it has disadvantages as removing dummy-FFs can not be detected since they

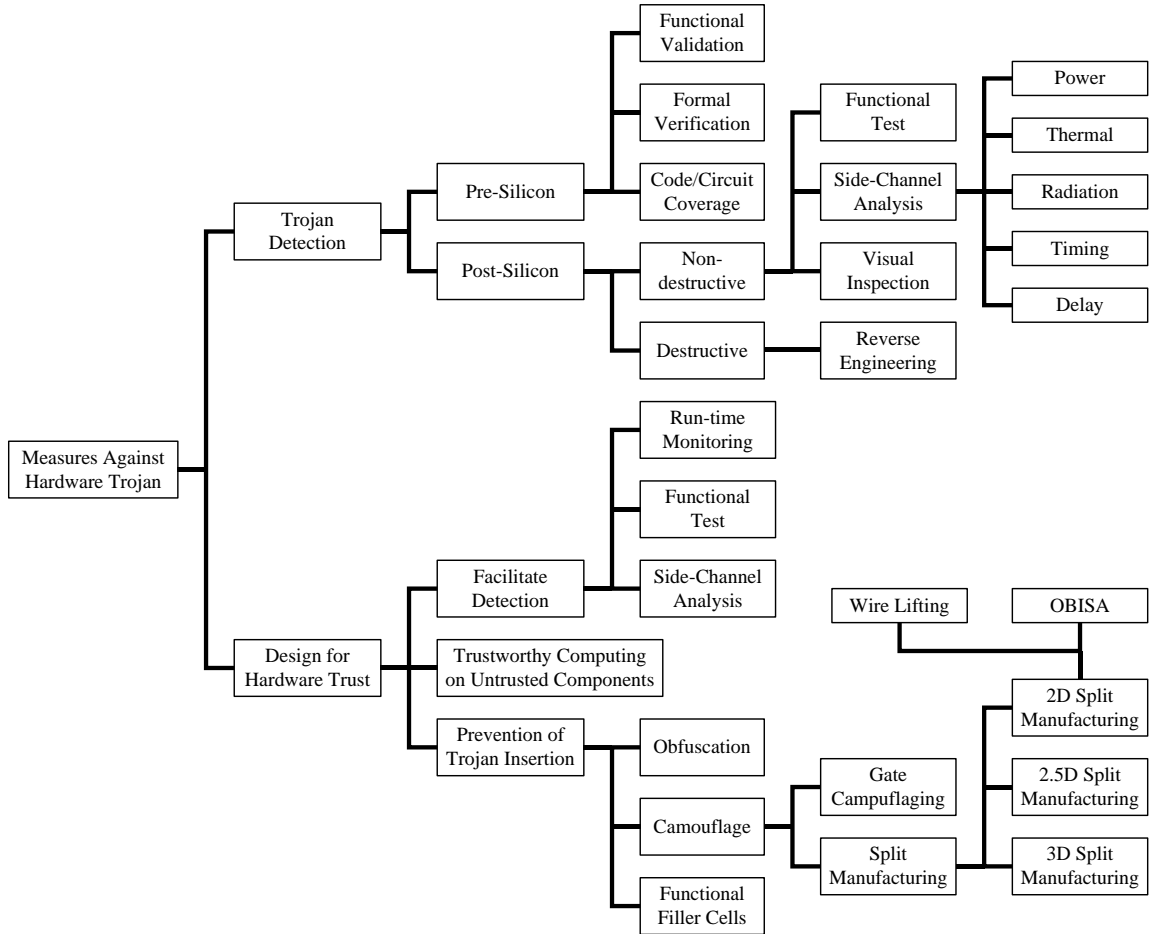


Figure 1.6. Taxonomy of measures against hardware Trojans. (inspired by [3]).

do not perform a function. Thus, dummy FFs can be replaced with HTs by attackers. A more efficient method is the layout filling approach described in [53], where unused spaces in the layout have been filled with functional cells. However, this method only is capable of filling approximately 90% of the existing layout. Another HT prevention method using layout filling approach, called Built-In Self Authentication (BISA), has been proposed in [54]. Standard library cells, along with Test Pattern Generator (TPG) and Output Response Analyzer (ORA), are used in [54] to fill the unused area. Another technique for filling empty spaces using functional cells is introduced in [55], where both shift registers and functional cells are substituted with Multiple Input Shift Registers (MISRs) and Output Response Analyzers (ORAs). These methods are somewhat

vulnerable to Trojan insertion as they cannot fill 100% of the unused die area. The possibility of using functional cells to fill the unused die area also depends on the initial occupation ratio [53]. If the original circuit occupies more than 85% of the die, these methods cannot prevent HT insertion [53]. Moreover, the performance parameters degrade with increasing circuit-complexity.

The classification of measures against hardware Trojans is depicted in Fig. 1.6, inspired by [3]. Another sub-category, delay, has been added as a separate detection method using side-channel analysis as delay-detection methods have gained a lot of interest. The Split Manufacturing for Trust [3] has been more correctly categorized as a sub-level of Camouflage techniques used to prevent HT insertion. Split manufacturing is a technique in which a trusted foundry completes a portion of the circuit fabrication process to camouflage the circuit functionality.

The introduction of 3D ICs has provided attackers with various new methods to insert HTs in ICs [4], [5]. 3D ICs are more vulnerable to HT attack as multiple dies from different foundries are incorporated into a single IC, some of which can come from untrusted foundries. Researchers have proposed some ideas to take advantage of the split manufacturing method [42, 56 – 58] to increase the security of 3D ICs. The idea is to obfuscate the 3D IC design by lifting some key components of the complete design to a single layer and fabricate it in a local trusted foundry. The other layers can be fabricated by any foundries regardless of the trust issue. Even though this method can eliminate most HT insertion threats, it still suffers from HT insertion opportunities unique to 3D manufacturing. The integration of multiple layers requires intermediate levels like die stacking and TSV bonding, where a HT can be inserted. Moreover, TSVs can be

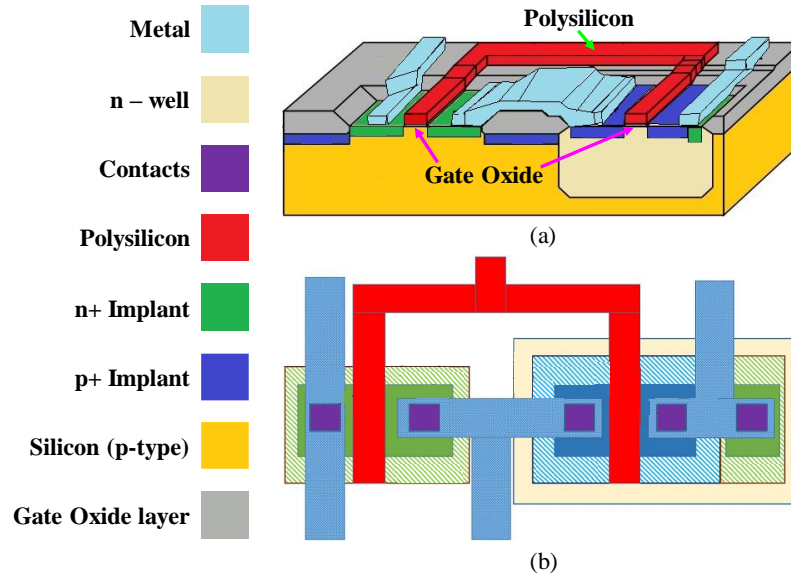


Figure 1.7. A typical CMOS process indicating layout layers: (a) 3D view (b) Top view [59].

exploited during the intermediate steps. One of the main characteristics of a 3D IC that is working against HT detection is its inherent thermal issues and elevated temperature in the middle layers, which can be manipulated as a trigger for a Trojan [60].

### 1.3. HARDWARE TROJAN PREVENTION USING LAYOUT FILLING METHOD

An effective method to prevent hardware Trojan insertion is layout manipulation. It can be done either by filling the unused chip area using components such as gates, routing lines, and various functional circuits and by manipulating the layout of the original design by adding redundancies. As mentioned above, the main drawbacks of layout filling method are the increased power consumption and the fact that the entire unused space cannot be occupied using functional cells. Two separate approaches are presented to overcome these shortcomings in this dissertation. In the first method, the polysilicon space is covered using minimum feature wires, and in the second one, the whole die is concealed using minimum feature polysilicon and metal wires. A third approach is also presented, where the original design is manipulated by rerouting the

critical nodes of the design through an array of Memristor devices. Even though this is a type of obfuscation method, it can also be considered a layout manipulation method.

***A. Filling Only Unused Polysilicon Layer with Polysilicon Wires***

Polysilicon layers connect directly to the active region of an IC, as is shown in Fig. 1.7. Hence, if the entire unused polysilicon layer is covered with minimum feature wires, it will prevent attackers from inserting gates or functional cells to implement a Trojan. To insert a Trojan, in this case, a portion of the polysilicon wire has to be removed. A readout circuit can detect such temper with the polysilicon layer, and hence the Trojan can be detected. It has been shown that this method can detect the insertion of a minimum size library cell. Chapter 2 represents an article depicting this method published in a conference proceeding.

To further improve the prevention method's effectiveness, the polysilicon wires have been placed as probes to capture the original circuit's signature. If a portion of the polysilicon wires is removed or if the wire is replaced by a capacitor, the signature will be different even if the readout circuit does not reflect any change. Chapter 3 presents a journal article published by Elsevier, explaining the complete method as an extension of the method presented in Chapter 3.

***B. Filling Entire Unused Space of the Die with Polysilicon and Metal Wires***

The approach mentioned above can account for a hardware Trojan insertion that requires an active/substrate layer. However, it cannot prevent attackers from using metal wires to modify the original circuit's functionality. The unused area of the die has been covered using both polysilicon and metal wires of minimum feature, as shown in Fig. 1.8.

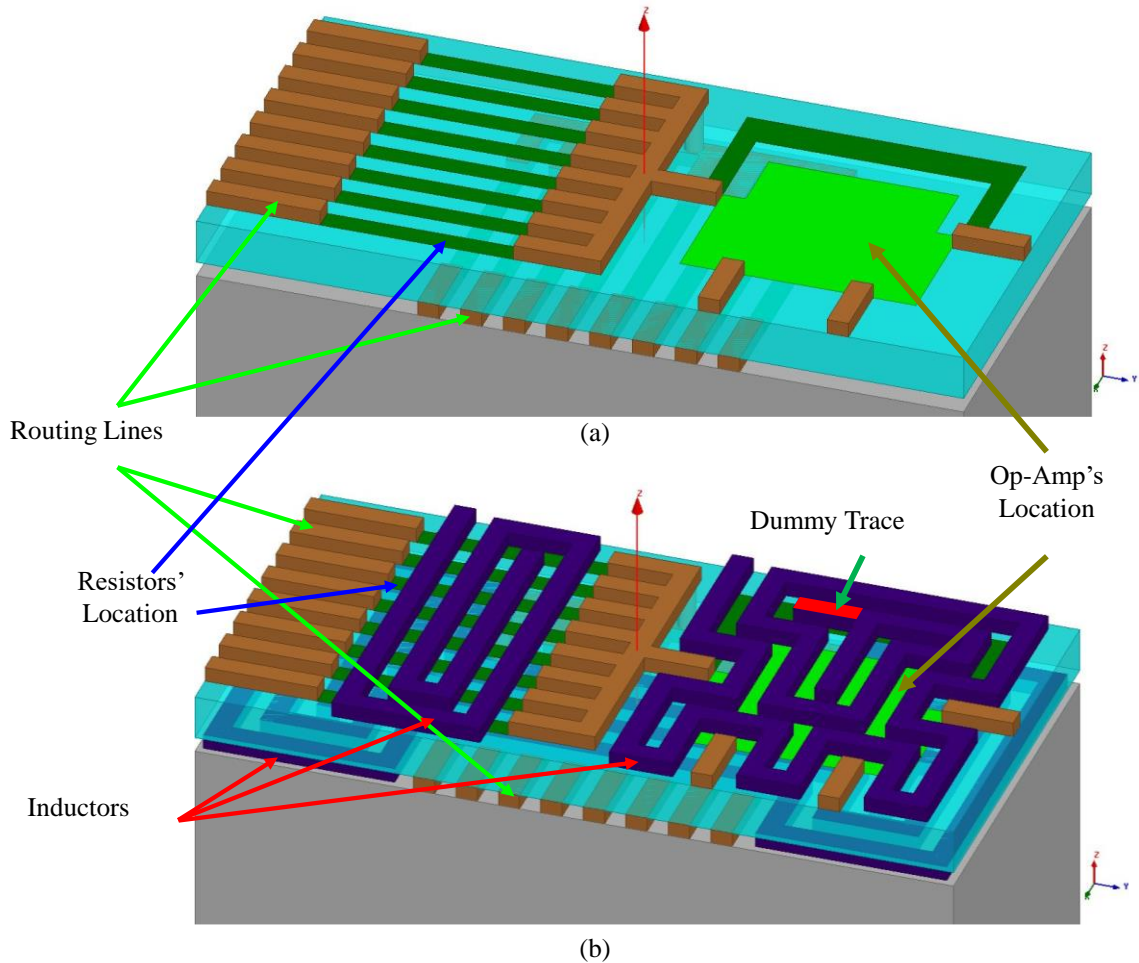
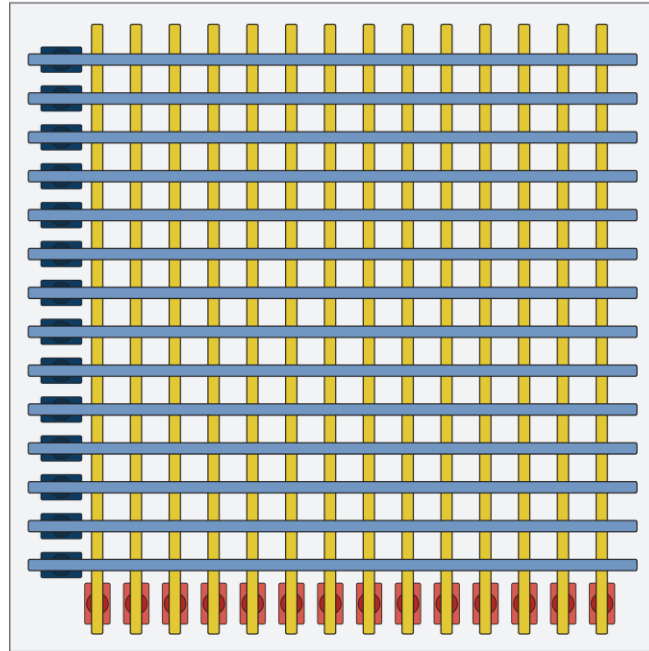


Figure 1.8. (a) Routing of a typical digital-to-analog circuit in HFSS environment. (b) Unused layers used as magnetic probes. [61].

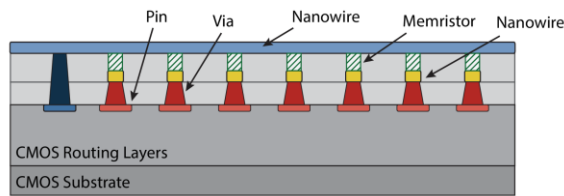
It has also been demonstrated that this technique can also be used effectively for 3D ICs. The main advantage of this method for 3D ICs is that it cannot detect Trojans inserted during Die Stacking and TSV bonding stages of 3D IC fabrication, which are not protected by conventional security methods. A detailed analysis of this method is published in an IEEE transaction, presented in Chapter 4.

### C. HT Prevention by Layout Manipulation Using Memristor Devices

Memristors (a contraction of memory resistors) were first hypothesized by Leon Chua in 1971 [62] as the fourth fundamental circuit element. A memristive device is a two-



(a)



(b)

Figure 1.9. Crossing nanowires are separated by memristor switches at the junctions that can be electrically configured. Nanowire crossbars are connected to a CMOS chip via metallic pins over the CMOS stack [9].

terminal electrical element that acts as a variable resistive switch. Its resistance depends on the magnitude, duration, and polarity of the voltage applied to it. Memristive devices can retain the state of recent internal resistance based on the history of the applied voltage or charge, even without a bias. One of the popular structures implemented using memristors is the crossbar architecture [63], shown in Fig. 1.9 (a). The crossbar structure has two layers, each of which boasts of an array of parallel nanowire electrodes. These two layers together form a grid of orthogonal nanowires. In a memristor-based crossbar structure, a cross-point junction is formed by a memristor switch connecting the top layer to the bottom layer, where two nanowires cross over each other, which is shown in Fig.



1.9 (b). The proposed scheme's basic idea is to obfuscate the circuit's functional behavior by selecting a specific number of connected net pairs from the netlist and rerouting them across a configurable grid of nanowire crossbars. This can be done by connecting one net of each pair to a source contact and the other net to a drain contact along the two metallic pin rails connecting the crossbar to the CMOS stack as shown in Fig. 1.9. The memristors of Fig. 1.9 connect each horizontal line to all vertical lines. In the final design, the vertical line and the horizontal line connections are established based on the voltage applied to the memristors through vias, where memristors act like an open or closed switch depending on the applied voltage.

The rest of the dissertation is organized as follows: Chapter 2 contains a conference publication on Trojan prevention using polysilicon wires, published in *Design & Technology of Integrated Systems In Nanoscale Era (DTIS)*, 2019; Chapter 3 features a journal on Trojan prevention by layout filling method using both polysilicon and metal wires, published in *IEEE Transactions on Electromagnetic Compatibility* in 2020; Chapter 4 shows the content of a journal on Trojan prevention by layout filling method using only polysilicon wires, which is undergoing the second review in *Elsevier Journal of Microelectronics Reliability*; Chapter 5 presents a journal on Trojan prevention inspired by obfuscation technique using the crossbar structure of memristor devices, which has been submitted to a journal. Finally, the layout manipulation method along with the three separate approaches, are discussed with possible future works in the conclusion in Chapter 6.

## REFERENCE

- [1] A. London, “Basic principles for managing foundry programs”, *Microelectronics Reliability*, vol. 45, no. 9-II, pp. 1285-1292, 2005.
- [2] M. T. Bohr and I. A. Young, “CMOS Scaling Trends and Beyond,” in *IEEE Micro*, vol. 37, no. 6, pp. 20-29, November/December 2017.
- [3] K. Xiao et al., “Hardware Trojans: Lessons learned after one decade of research,” *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 1-23, 2016.
- [4] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, “Security and vulnerability implications of 3D ICs,” *IEEE Trans. on Multi-Scale Comp. Sys.*, vol. 2, no. 2, pp. 108 - 122, Apr. 2016.
- [5] J. Dofe, Q. Yu, H. Wang, and E. Salman, “Hardware security threats and potential countermeasures in emerging 3D ICs,” in *2016 Int. Great Lakes Symp. on VLSI (GLSVLSI)*, Boston, MA, USA, 2016, pp. 69-74.
- [6] C. Gorman, “Counterfeit chips on the rise,” in *IEEE Spectrum*, vol. 49, no. 6, pp. 16-17, June 2012, doi: 10.1109/MSPEC.2012.6203952.
- [7] D. Collins, “DARPA Trust in IC's Effort (BRIEFING CHARTS)” DEFENSE ADVANCED RESEARCH PROJECTS AGENCY ARLINGTON VA MICROSYSTEMS TECHNOLOGY OFFICE, 2007. [Online]. Available: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a503809.pdf>. [Accessed 05 November 2020].
- [8] “Holistic Approaches for Integrity of ICT-Systems | HINT Project | FP7 | CORDIS | European Commission” 22 April 2017 (Last Updated). [Online]. Available: <https://cordis.europa.eu/project/id/317930>. [Accessed 05 November 2020].

- [9] T. M. Supon and R. Rashidzadeh, "Hardware Trojan Prevention using Memristor Technology," *Microprocessors and Microsystems*, Submitted.
- [10] R. Karri, J. Rajendran, K. Rosenfeld and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," in *Computer*, vol. 43, no. 10, pp. 39-46, Oct. 2010.
- [11] J. Dofe, J. Frey and Q. Yu, "Hardware security assurance in emerging IoT applications," *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, 2016, pp. 2050-2053.
- [12] L. A. Guimarães, R. P. Bastos, T. F. de Paiva Leite and L. Fesquet, "Simple tri-state logic Trojans able to upset properties of ring oscillators," *2016 International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS)*, Istanbul, 2016, pp. 1-6.
- [13] L. Ni, J. Li, S. Lin and D. Xin, "A method of noise optimization for Hardware Trojans detection based on BP neural network," *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, 2016, pp. 2800-2804.
- [14] Xiaoxiao Wang, M. Tehranipoor and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," *2008 IEEE International Work. on Hardware-Oriented Security and Trust*, Anaheim, CA, 2008, pp. 15-19.
- [15] R. S. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," *2009 IEEE International High Level Design Validation and Test Workshop*, San Francisco, CA, 2009, pp. 166-171.

- [16] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," in *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, Jan.-Feb. 2010.
- [17] T. F. Wu, K. Ganesan, Y. A. Hu, H. - P. Wong, S. Wong and S. Mitra, "TPAD: Hardware Trojan Prevention and Detection for Trusted Integrated Circuits," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 4, pp. 521-534, April 2016.
- [18] S. Dupuis, M. Flottes, G. Di Natale and B. Rouzeyre, "Protection Against Hardware Trojans With Logic Testing: Proposed Solutions and Challenges Ahead," in *IEEE Design & Test*, vol. 35, no. 2, pp. 73-90, April 2018.
- [19] S. Dupuis, P. Ba, M. Flottes, G. Di Natale and B. Rouzeyre, "New testing procedure for finding insertion sites of stealthy Hardware Trojans," *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, 2015, pp. 776-781.
- [20] M. Flottes, S. Dupuis, P. Ba and B. Rouzeyre, "On the limitations of logic testing for detecting Hardware Trojans Horses," *2015 10th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, Naples, 2015, pp. 1-5.
- [21] S. Narasimhan *et al.*, "Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis," in *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2183-2195, Nov. 2013.

- [22] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *2007 IEEE Symp. on Security and Privacy (SP '07)*, Berkeley, CA, USA, 2007, pp. 296-310.
- [23] X. Ngo *et al.*, "Hardware Trojan detection by delay and electromagnetic measurements," *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, 2015, pp. 782-787.
- [24] J. He, Y. Zhao, X. Guo and Y. Jin, "Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 10, pp. 2939-2948, Oct. 2017.
- [25] Yier Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, Anaheim, CA, 2008, pp. 51-57.
- [26] I. Exurville, L. Zussa, J. Rigaud and B. Robisson, "Resilient hardware Trojans detection based on path delay measurements," *2015 IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST)*, Washington, DC, 2015, pp. 151-156.
- [27] M. Lecomte, J. Fournier and P. Maurine, "An On-Chip Technique to Detect Hardware Trojans and Assist Counterfeit Identification," in *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3317-3330, Dec. 2017.
- [28] X. Zhang and M. Tehranipoor, "RON: An on-chip ring oscillator network for hardware Trojan detection," *2011 Design, Automation & Test in Europe*, Grenoble, 2011, pp. 1-6.
- [29] H. Salmani, M. Tehranipoor and J. Plusquellic, "A layout-aware approach for improving localized switching to detect hardware Trojans in integrated

- circuits,” *2010 IEEE International Workshop on Information Forensics and Security*, Seattle, WA, 2010, pp. 1-6.
- [30] E. Amini et al., “IC security and quality improvement by protection of chip backside against hardware attacks,” *Microelectronics Reliability*, vol. 88, pp. 22-25, 2018.
- [31] C. Bao, D. Forte and A. Srivastava, “On Reverse Engineering-Based Hardware Trojan Detection,” in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 1, pp. 49-57, Jan. 2016.
- [32] P. Ghosh and R. S. Chakraborty, “Counterfeit IC Detection By Image Texture Analysis,” *2017 Euromicro Conference on Digital System Design (DSD)*, Vienna, 2017, pp. 283-286.
- [33] S. Bhasin, J. Danger, S. Guilley, X. T. Ngo and L. Sauvage, “Hardware Trojan Horses in Cryptographic IP Cores,” *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Santa Barbara, CA, 2013, pp. 15-29.
- [34] T. Hoque, J. Cruz, P. Chakraborty and S. Bhunia, “Hardware IP Trust Validation: Learn (the Untrustworthy), and Verify,” *2018 IEEE International Test Conference (ITC)*, Phoenix, AZ, USA, 2018, pp. 1-10.
- [35] L. Ramirez Rivera, X. Wang and D. Chasaki, “A separation and protection scheme for on-chip memory blocks in FPGAs,” *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, McLean, VA, 2016, pp. 223-228.
- [36] S. Gundabolu and X. Wang, “On-chip Data Security Against Untrustworthy Software and Hardware IPs in Embedded Systems,” *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Hong Kong, 2018, pp. 644-649.

- [37] M. Tehranipoor, H. Salmani and X. Zhang, "Hardware Trojan Detection: Untrusted Third-Party IP Cores," in *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*, Cham, Springer International Publishing, 2014, pp. 19-30.
- [38] M. M. Farag and M. A. Ewais, "Smart employment of circuit redundancy to effectively counter trojans (SECRET) in third-party IP cores," *2014 Int. Conference on ReConFigurable Computing and FPGAs (ReConFig14)*, Cancun, 2014, pp. 1-6.
- [39] A. Nahiyani, M. Sadi, R. Vittal, G. Contreras, D. Forte and M. Tehranipoor, "Hardware trojan detection through information flow security verification," *2017 IEEE International Test Conference (ITC)*, Fort Worth, TX, 2017, pp. 1-10.
- [40] C. Liu and C. Yang, "Exploiting heterogeneity in MPSoCs to prevent potential Trojan propagation across malicious IPs", *Proceedings of the 24th edition of the great lakes symposium on VLSI (GLSVLSI)*, May 2014, pp. 335-340.
- [41] M. K. Das, "Preventive Techniques for Hardware Trojans," Master Thesis, Masaryk University, Hyderabad, 2016.
- [42] Y. Xie, C. Bao and A. Srivastava, "3D/2.5 D IC-based obfuscation," in *Hardware Protection through Obfuscation*, Cham, Springer Int. Publish., 2017, pp. 291-314.
- [43] M. Li, B. Yu, Y. Lin, X. Xu, W. Li and D. Z. Pan, "A Practical Split Manufacturing Framework for Trojan Prevention via Simultaneous Wire Lifting and Cell Insertion," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 9, pp. 1585-1598, Sept. 2019.
- [44] R. S. Chakraborty and S. Bhunia, "HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection," in *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493-1502, Oct. 2009.

- [45] R. S. Chakraborty and S. Bhunia, "Security against hardware trojan attacks using key-based design obfuscation," *Journal of Electronic Testing*, vol. 27, no. 6, pp. 767–785, Dec. 2011.
- [46] X. T. Ngo, S. Bhasin, J. -L. Danger, S. Guilley and Z. Najm, "Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses," *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC, 2015, pp. 82-87.
- [47] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, Berlin, Germany, 2013, pp. 709-720.
- [48] M. I. Mera Collantes, M. El Massad and S. Garg, "Threshold-Dependent Camouflaged Cells to Secure Circuits Against Reverse Engineering Attacks," *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA, 2016, pp. 443-448.
- [49] J. Rajendran, Y. Pino, O. Sinanoglu and R. Karri, "Security analysis of logic obfuscation," *DAC Design Auto. Conf. 2012*, San Francisco, CA, 2012, pp. 83-89.
- [50] S. Dupuis, P. Ba, G. Di Natale, M. Flottes and B. Rouzeyre, "A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans," *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, Platja d'Aro, Girona, 2014.
- [51] Q. Yu, J. Dofe and Z. Zhang, "Exploiting hardware obfuscation methods to prevent and detect hardware Trojans," *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Boston, MA, 2017, pp. 819-822.



- [52] H. Salmani, M. Tehranipoor and J. Plusquellic, "A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time," in *IEEE Transactions on Very Large Scale Integ. (VLSI) Systems*, vol. 20, no. 1, pp. 112-125, Jan. 2012.
- [53] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware Trojan insertion," *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Austin, TX, 2013, pp. 45-50.
- [54] P. Ba, M. Palanichamy, S. Dupuis, M. Flottes, G. Di Natale and B. Rouzeyre, "Hardware Trojan prevention using layout-level design approach," *2015 European Conference on Circuit Theory and Design (ECCTD)*, Trondheim, 2015, pp. 1-4.
- [55] P. Ba, S. Dupuis, M. Palanichamy, M. Flottes, G. Di Natale and B. Rouzeyre, "Hardware Trust through Layout Filling: A Hardware Trojan Prevention Technique," *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA, 2016, pp. 254-259.
- [56] J. Valamehr *et al.*, "A 3-D Split Manufacturing Approach to Trustworthy System Development," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, no. 4, pp. 611-615, April 2013.
- [57] J. Dofe, Chen Yan, S. Kontak, E. Salman and Q. Yu, "Transistor-level camouflaged logic locking method for monolithic 3D IC security," *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, Yilan, 2016, pp. 1-6.
- [58] F. Imeson, A. Emtenan, S. Garg, and M. Tripunitara, "Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation," in *22nd USENIX Security Symposium (USENIX Security 13)*, 2013, pp. 495–510.

- [59] T. M. Supon and R. Rashidzadeh, "On-Chip Magnetic Probes for Hardware Trojan Prevention and Detection," in *IEEE Trans. on Electromagnetic Compatibility*, doi: 10.1109/TEMPC.2020.3003728.
- [60] S. R. Hasan, S. F. Mossa, O. S. A. Elkeelany and F. Awwad, "Tenacious hardware trojans due to high temperature in middle tiers of 3-D ICs," *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Fort Collins, CO, 2015, pp. 1-4.
- [61] T. M. Supon, M. Seyedbarhagh and R. Rashidzadeh, "A Method to Prevent Hardware Trojans Limiting Access to Layout Resources," in *Microelectronics Reliability*, Revision Requested.
- [62] L. Chua, "Memristor-The missing circuit element," in *IEEE Transactions on Circuit Theory*, vol. 18, no. 5, pp. 507-519, September 1971.
- [63] K.-H. Kim *et al.*, "A functional hybrid memristor crossbar-array/CMOS system for data storage and neuromorphic applications," *Nano Lett.*, vol. 12, no. 1, pp. 389–395, 2012.

---

## Chapter 2

---

# HARDWARE TROJAN PREVENTION THROUGH LIMITING ACCESS TO THE ACTIVE REGION

---

### 2.1 INTRODUCTION

Hardware security is becoming a major concern for IC designers. RFID tags, IoT (Internet of Things) devices, home appliances or even biomedical equipment and any other electronic device can be vulnerable to a security threat [1-3] if it infected with a Hardware Trojan (HT). HT is an intentional circuit modification to alter the functionality of the original design, or to leak valuable information. Trojans can be added to the main circuit during the fabrication process, which in addition to a security threat, can induce an economic loss related to IC production. HTs can be inserted into the original circuit to perform any or all the following three tasks (a) faulty operation or modification of the main function, (b) electrical modification, and (c) reliability reduction [4].

Many solutions have been proposed in the literature [4 – 11] to address the security threats posed by HTs through Hardware Trojan detection. HT detection techniques can be classified into three different categories [5]: (a) logic testing, (b) side-channel analysis and (c) reverse engineering. In the logic testing method, the circuit is inspected using some known IC test methodologies [6, 7]. However, a Trojan can remain undetected in

this method as the test vectors applied to the IC in the test phase may not be able to activate the Trojan. Moreover, the test infrastructures may be denied the possibility to detect an HT insertion via a minute alteration of the HT trigger [8]. The side channel analysis method [9, 10] is a non-invasive method which exploits physical parameters of the circuit such as radiation, current, power, and so on to detect HTs. This method is successfully used to extract critical information such as cryptography keys from integrated circuits systems. It can also be utilized to detect Trojan activities. This method commonly requires a trusted golden circuit for result comparison. As the latest IC technologies work at the lower supply voltages, the Signal-to-Noise-Ratio (SNR) of these ICs is lower compared to previous technologies. Therefore, the background noise and even process variations can mask Trojan activities and prevent them from detection through side channel analysis. The reverse engineering method [11] is a powerful HT detection method compared to the other techniques; however, it is a costly and destructive approach. Moreover, when a small portion of the fabricated ICs is infected, reverse engineering may fail as healthy ICs may get selected for reverse engineering. In a nutshell, Hardware Trojan detection is a difficult task in nature due to the wide range of possible Trojans. Most of the detection methods are developed for certain classes of Trojans and a comprehensive solution to detect all Trojans is yet far from reach. Moreover, once a Trojan is inserted the damage is done and even if it is detected, the infected device needs to be discarded. Trojan prevention methods, on the other hand, have the advantage of protecting the integrated circuit in the first place.

HT prevention approaches are divided into three groups [12]: (a) logic obfuscation, (b) compact GDS-II layout generation and (c) layout filling. In [13], researchers have added

reconfigurable circuits to the main design to protect the circuit against reverse engineering. Another method is proposed in [14] where the authors introduced a secure-by-construction split manufacturing flow to obfuscate the netlist. Although this security measure can be utilized for 2.5D or 3D IC protection, it cannot prevent Trojan insertion during the die stacking and TSV bonding stages. Logic locking and IC camouflaging can also be considered as obfuscation techniques. All the latest obfuscation methods with their pros and cons have been summarized in [15] by some researchers. The researchers have presented a method in [16] to create the layout as dense as possible by filling the empty spaces in a layout by functional cells. This is an effective method but can occupy only around 90% of the total chip. In [17], researchers have added dummy flip-flops (FFs) as a prevention technique of Hardware Trojans. The main concern with this method is that the detection of the removal of those dummy-FFs is not practical, and hence the system will suffer from the possibility of HT insertion, nevertheless. Another HT prevention method named built-in self-authentication (BISA) is presented in [18], in which standard library cells have been added to the main circuit to fill empty areas by using a test pattern generator and output response analyzer. In [19], the authors proposed a solution to solve these issues by adding shift registers and functional cells instead of Multiple Input Shift Registers (MISRs) and Output Response Analyzers (ORAs) to fill empty spaces of the circuit and to create some combinational functions. However, the occupation ratio in this method is around 90%, which gives attackers a chance to insert malicious circuits. All these layout filling methods also depend on the initial occupation ratio. The maximum initial occupation ratio reported in these papers is 85%. If the

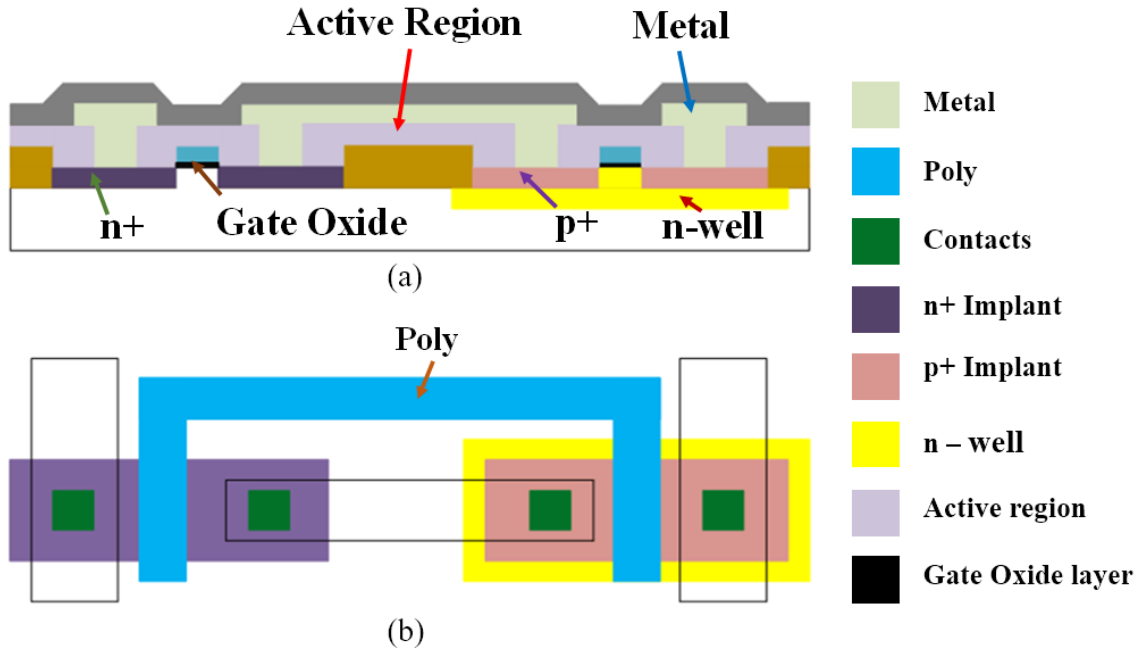


Figure 2.1. A typical CMOS process indicating layout layers. (a) Cross section. (b) Top view [21].

original circuit occupies more than 85% of the die, these methods cannot be used to prevent HT insertion.

This paper presents a new HT prevention technique in which the attackers are deprived of any space to route their malicious circuits. As compared to the prevention methods relying on filling the silicon area, the proposed method in this work is much easier to implement, consumes no power and supports the full occupation regardless of the initial occupation ratio. In the proposed method, after the main circuit design, the path to the active layer is blocked by covering the empty spaces with polysilicon. As polysilicon connects to the active layer directly without the need of any contact, to add an extra component to the circuit, a portion of the poly layer must be removed. Such an alteration can be detected by the implemented readout circuit, inspired by the Delay-Detection-Module (DDM) proposed in [20].

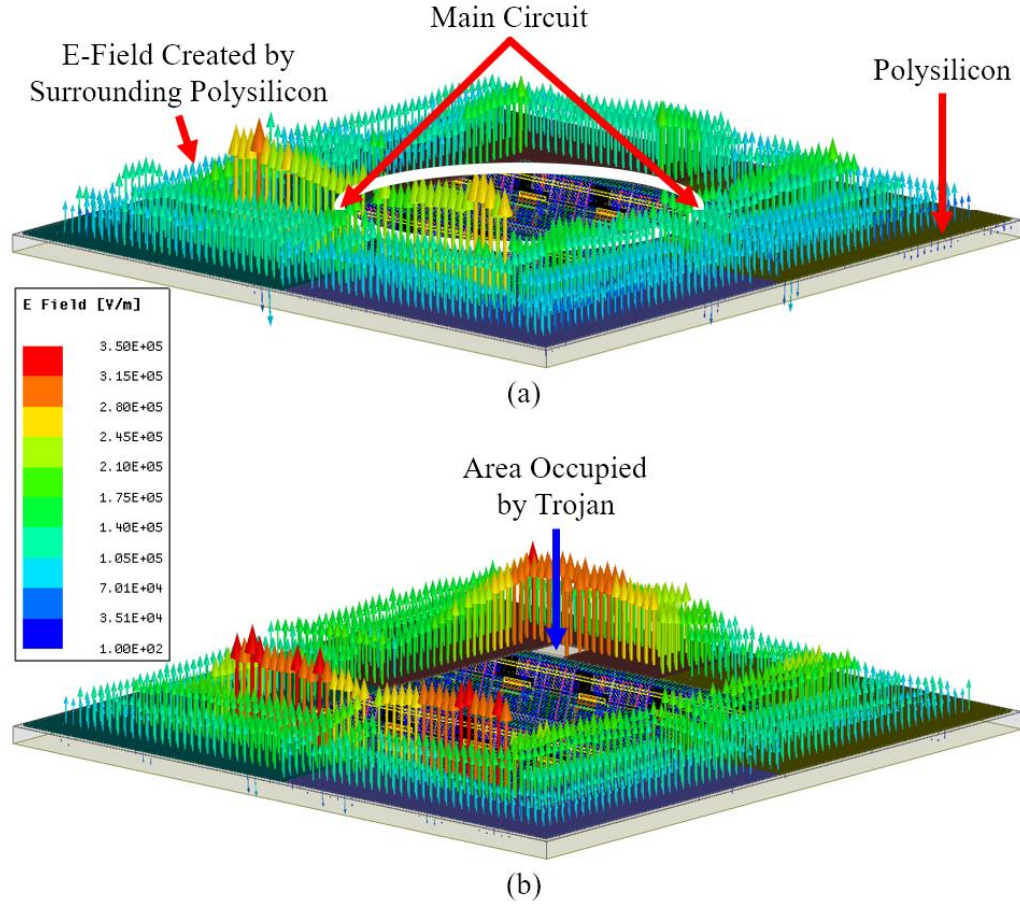


Figure 2.2. 3D full wave simulation results indicating the electric field difference between (a) the original and (b) the Trojan affected design.

The rest of the paper is organized as follows: the proposed method is covered in detail in section II; the readout circuit is discussed in section III; section IV presents the simulation results; and finally, section V summarizes the concluding remarks.

## 2.2 PROPOSED METHOD

As part of the fabrication process for CMOS technologies, the metal layers are connected through contacts to the active silicon layer for the purposes of routing. If unauthorized connections to the active layer are prevented, then the attackers are deprived of the resources to insert functional Trojans. The polysilicon layer, which is separated by a thin oxide layer as shown in Fig. 2.1, can be utilized to cover the silicon

substrate region, where the active regions are formed. Integrated circuits are designed using different active regions routed through polysilicon and metal layers. As shown in Fig. 2.1 (b), the polysilicon connects directly to the active region, whereas the metal layers need contacts to connect them to the active region. Thus, if the empty space of the die is completely covered with a polysilicon layer, attackers will not be able to access the substrate layer to insert malicious circuits or hardware Trojans. The partial removal affects the electric field and alters the path delay and the overall parasitic capacitance of the polysilicon layer which can be detected by an on-chip readout circuit. To evaluate the effect of polysilicon removal on the distribution of the electric field and the path delay, a conceptual IC was designed using HFSS (High-Frequency Structure Simulator). 3D full wave simulation results in Fig. 2.2 shows the distribution of the electric field before and after removal of a small portion of the polysilicon layer accounting for less than 1% of the total polysilicon area. The change in the electric field is due to the variation of the polysilicon layer's parasitic capacitance and path resistance. The relationship between the electric field and the parasitic capacitance of the polysilicon layer can be determined from the stored energy as follows:

$$W_1 = \frac{1}{2} C_{p1} V^2 = \frac{1}{2} \sum_{i=1}^n \epsilon E_i^2 dv \quad (1)$$

where  $W$  is the energy stored,  $C_P$  is the parasitic capacitance,  $V$  is the applied voltage and  $E_i$  is the electric field of discrete points in the device and  $v$  is the volume of between the ground plane and the polysilicon layer. Removal of less than 1% of the total polysilicon area affects the electric field distribution considerably as shown in Fig. 2.2. Consequently, the stored energy after the polysilicon removal changes to:





resistance of the polysilicon layer. Even though  $\Delta C_p$  can be realized using a capacitor, the time constant will not remain the same due to the variation in resistance, and hence, the delay will change. Circuit level simulations indicate that the parasitic capacitance variations can readily be detected by observing the path delay. The readout circuit shown in Fig. 2.3 is used to measure the path delay and detect possible alterations to inset Trojans. The poly area was divided into 8 segments to ensure that the area of each segment is small enough to detect a minor area removal. The number of segments depends on the minimum detectable size of a Trojan. As the number of segments increases, the smaller size Trojans can be detected.

## 2.3 READOUT CIRCUIT

### *A Description of the Readout Circuit*

The readout circuit includes a Delay Locked Loop (DLL) for time measurement. The main advantage of utilizing a DLL for time measurement is its robustness against Process, Voltage, and Temperature (PVT) variations. It is shown in the simulation section that for a  $\pm 5\%$  process variation, the propagation delay changes by less than  $\pm 1\%$ . A conventional DLL includes a Phase Frequency Detector (PFD), Charge Pump (CP), Low Pass Filter (LPF) and delay-line modules, as shown in Fig. 2.3 (a). The DLL adjusts the propagation delay of its delay-line to reduce the time difference between the signals applied to the PFD. In the locked state, the signals applied to the PDF are aligned and ideally, the time difference between them becomes zero.

A DLL based readout circuit is designed to measure propagation delay with a high resolution. The block diagram of the readout circuit is shown in Fig. 2.3 (b). A Circuit-

Under-Test (CUT) is added to the DLL feedback loop to measure the delay difference between its signal paths. The readout circuit also includes two delay-lines used to amplify the time difference captured by the DLL.

When the DLL in the readout circuit captures the lock, the rising edges at the PFD input are aligned as shown in Fig. 2.3 (b). Since the same clock signal is applied to both  $D_1$  and  $D_2$  cells, we can write:

$$T_{D1} + T_{path\_1} = T_{D2} + T_{path\_2} \quad (4)$$

and therefore, we have:

$$T_{D1} - T_{D2} = T_{path\_2} - T_{path\_1} = \Delta T \quad (5)$$

where  $T_{D1}$  and  $T_{D2}$  are the propagation delay of  $D_1$  and  $D_2$  cells respectively and  $T_{path1}$  and  $T_{path2}$  represent the path-1 and path-2 propagation delays in the circuit-under-test.

From equation (5) it can be concluded that the delay difference between the two paths of CUT is replicated by the delay difference between  $D_1$  and  $D_2$  cells. This delay is then amplified using the technique proposed in [22]. The two delay lines of Delay-Line-1 and Delay-Line-2 in the readout circuit are used to amplify the delay difference between the CUT paths. The first delay line is composed of  $D_1$  cells while the second one is built using  $D_2$  cells. Therefore, the delay difference between the outputs of the two delay lines marked as  $Out_1$  and  $Out_2$  in Fig. 2.3 (b), becomes  $N\Delta T$ . This delay amplification relaxes the design requirement for the time-to-digital converter (TDC) and enables the TDC to measure the delay difference between the CUT paths with a high-resolution measurement. The operation detail of the readout circuit is presented in [20].

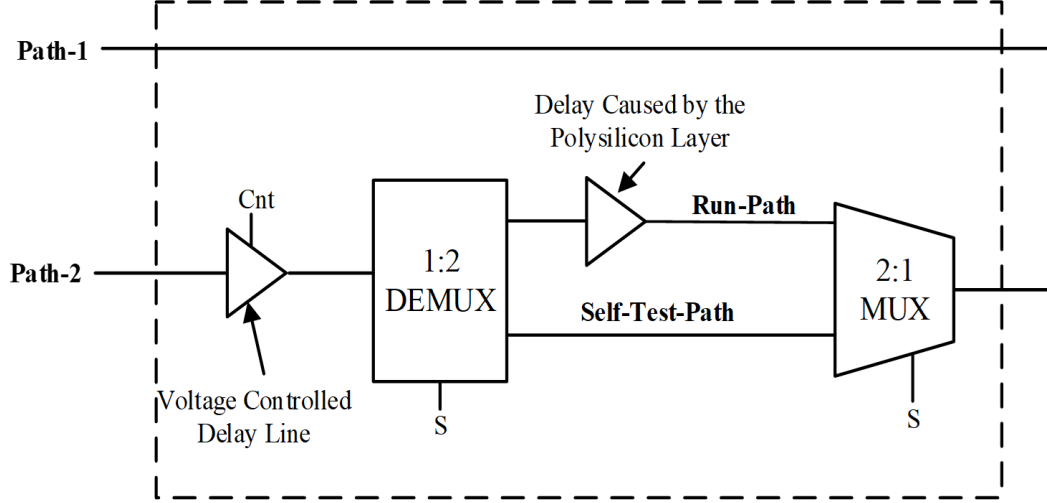


Figure 2.4. Circuit-Under-Test.

To test the propagation delay of the polysilicon layer, the CUT in the readout circuit in Fig. 2.3 (b) is designed as shown in Fig. 2.4. The propagation delay caused by the polysilicon layer is represented by a delay cell in Fig. 2.4. The circuit also incorporates a self-test path to test and ensure that the readout circuit has not been tampered with. The polysilicon layer can be divided into several separate segments to increase the measurement resolution. In this case, each segment is selected separately to measure its nominal propagation delay. There are two modes of operation for the readout circuit, the “Self-Test Mode” and the “Run Mode”.

### ***B Working Principle of the Readout Circuit***

A clock signal is fed to the input of the readout circuit in Fig. 2.3 (b). The CUT, in this case, represents the circuit shown in Fig. 2.4. In the run mode, the polysilicon layer in the CUT introduces a delay to the signal path-2. As explained in section 3A, the DLL feedback system compensates for the delay to acquire the lock. Once the lock is captured, we have:

$$T_{D1} - T_{D2} = \Delta T = T_{Poly} + T_{offset} \quad (6)$$



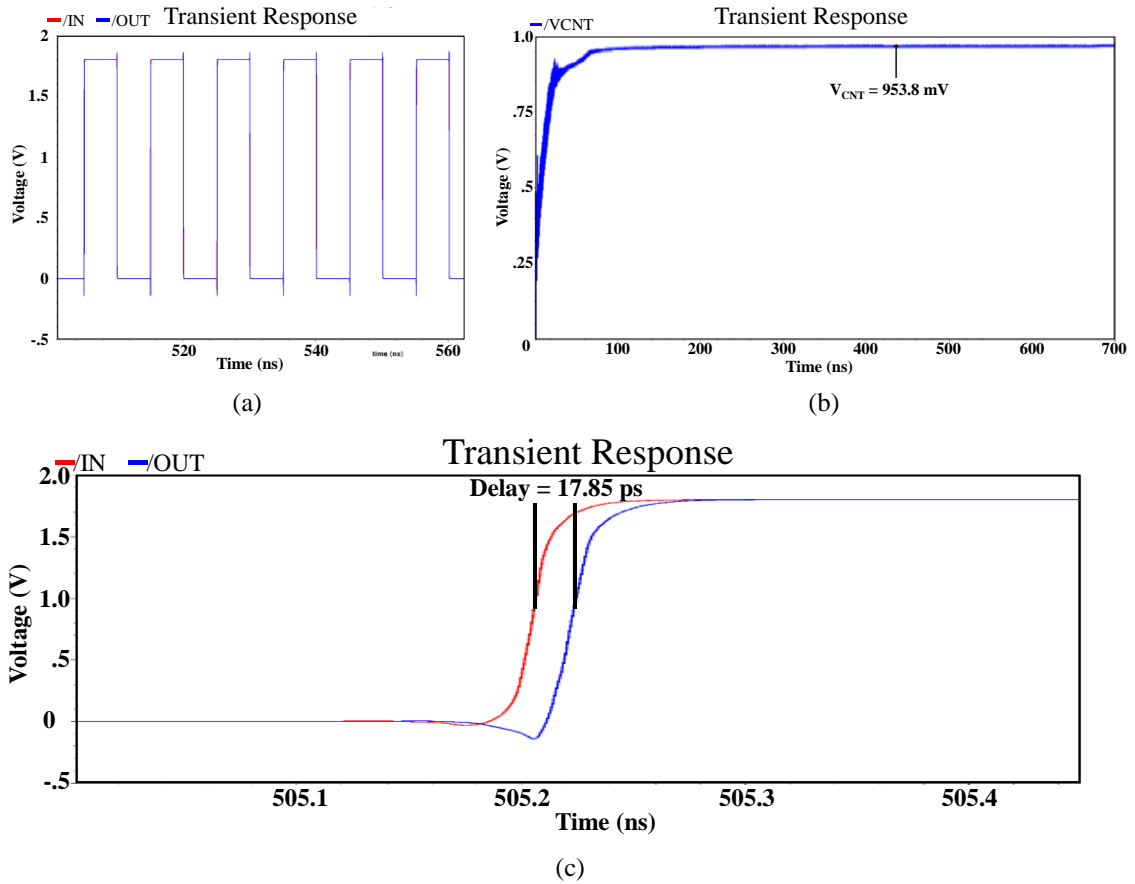


Figure 2.6. (a) The Locked Signal (b) Control Voltage of the DLL and (c) Delay between the Output and the Input Signals.

output signals is 17.85 ps, as indicated in Fig. 2.6 (c). As the control voltage increases from 0 to 1.8 V, the delay rises linearly from 17.85 ps to 66.43 ps, shown in Fig. 2.7. The minimum area required for a Trojan insertion depends on the type of Trojan and the size of the gate. An inverter from the standard cell library of  $0.18\mu\text{m}$  CMOS technology, shown in Fig. 2.8 (a), was added to the circuit to see if the proposed method can detect a small hardware manipulation. The minimum area of the polysilicon layer that must be removed to place this gate is around  $14.85 \mu\text{m}^2$ , as shown in Fig 2.8 (b). Figure 2.8 (c) presents the delay associated with the polysilicon of Fig 2.8 (b) which is about 4.65 ps. The implemented readout circuit can readily detect such a small delay.

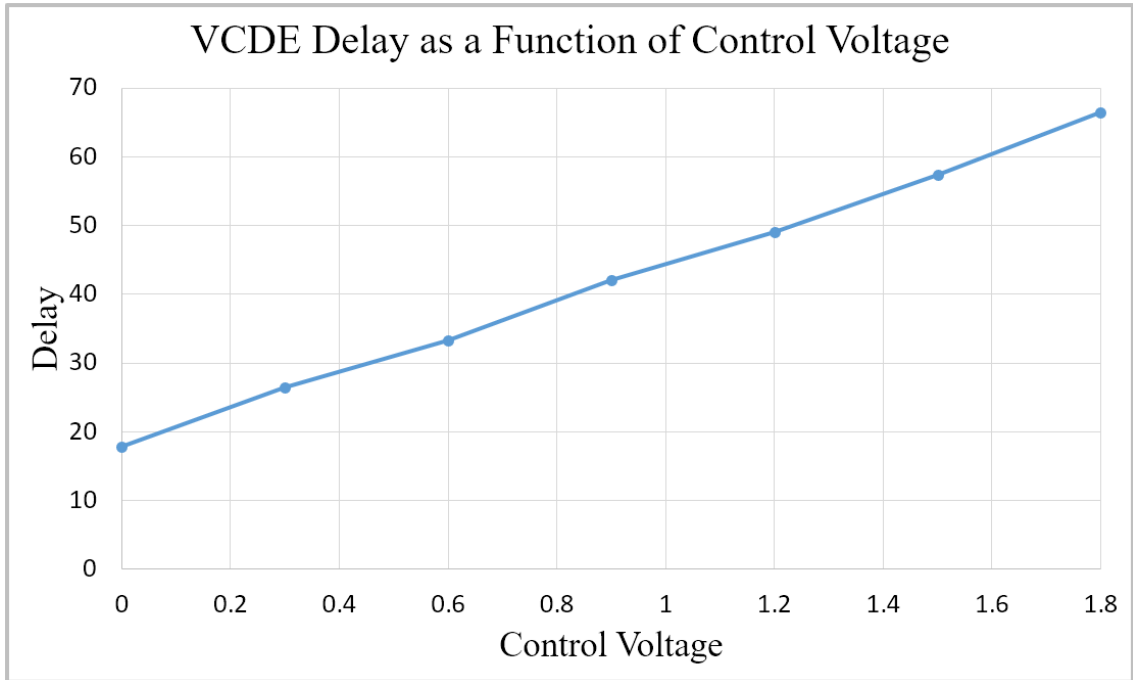


Figure 2.7. Relationship between VCDL Delay and Control Voltage.

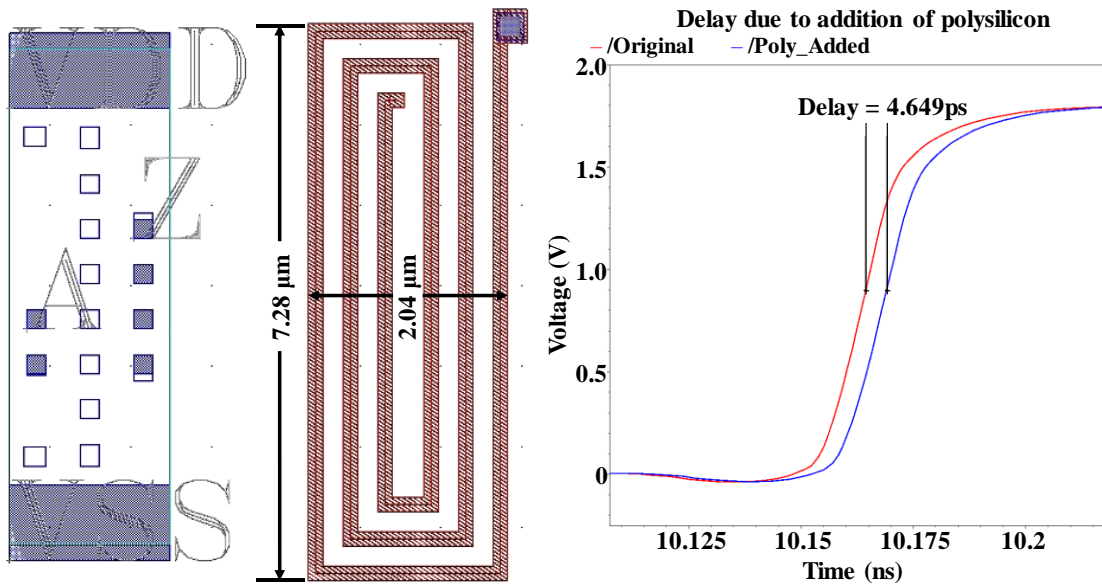


Figure 2.8. (a) Typical TSMC Inverter (b) Minimum poly needed to be removed to place that inverter (c) Delay caused by that poly.

To simulate the effect of Trojan insertion, a portion of the poly routing was removed, which is shown by a small circle in Fig. 2.9. Then transient simulations were performed to find the delay associated with each routing path of the original design of Fig. 2.5. As

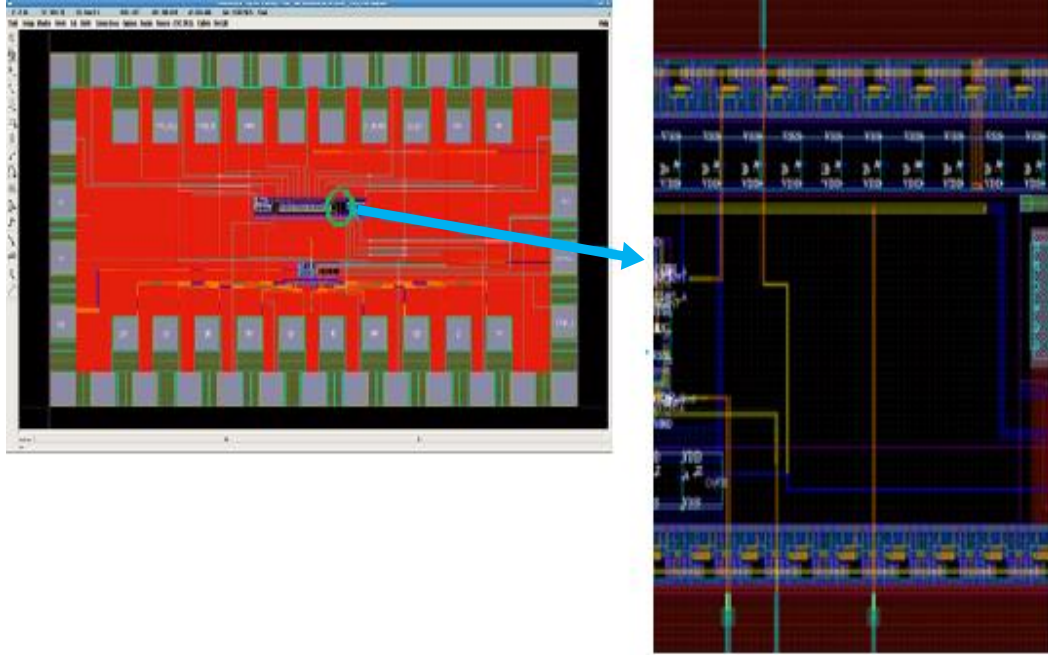


Figure 2.9. The IC with polysilicon layer partially removed to insert Trojan.

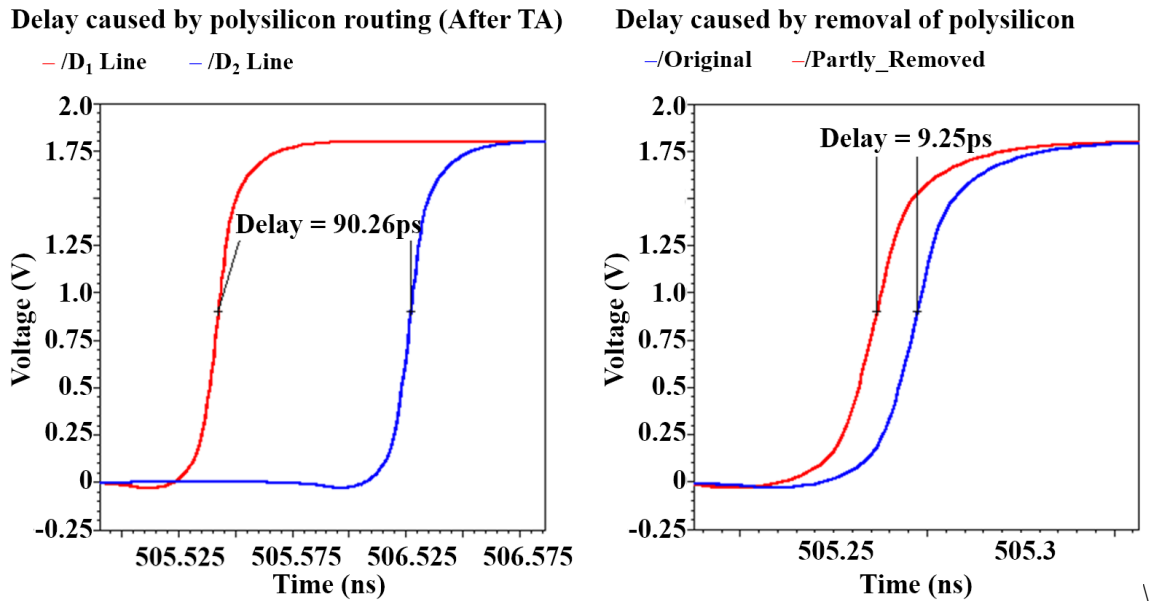
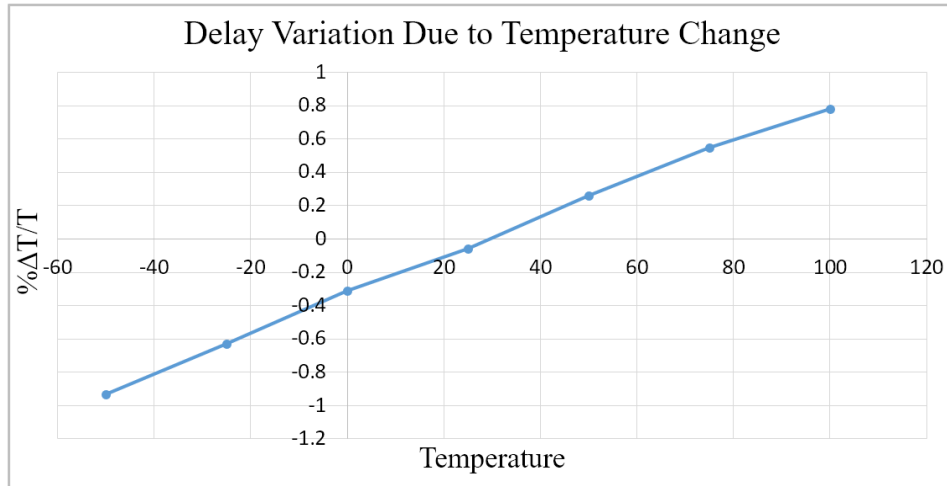


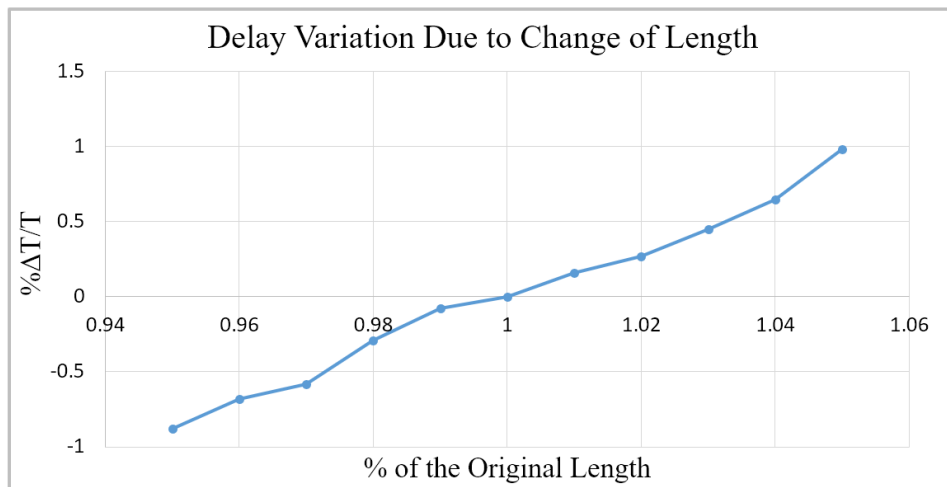
Figure 2.10. Time delay and variation.

shown in Fig. 2.10 (a), the delay of the routing segment 2 is 90.26 ps. Later the same simulation was performed with the layout of Fig. 2.9 to see the effect of poly removal. As can be seen in Fig. 2.10 (b) such a poly layer removal decreases the path delay by 9.25 ps.

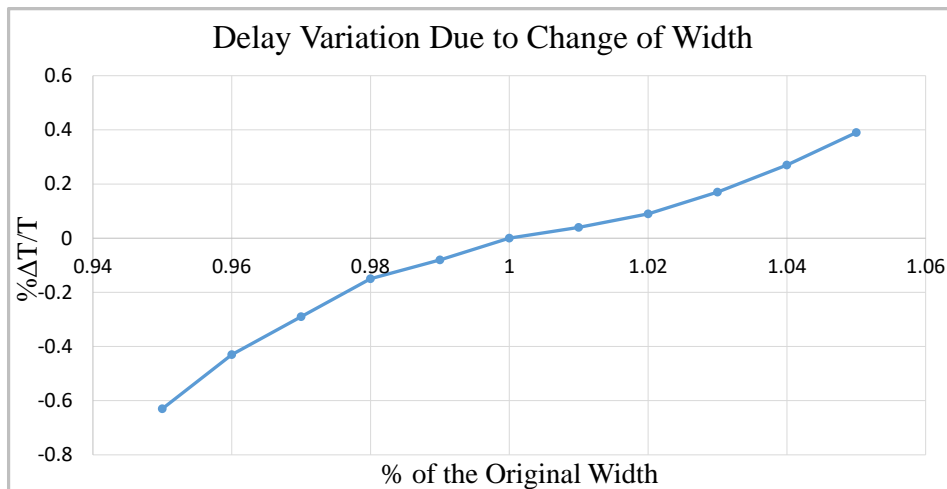




(a)



(b)



(c)

Figure 2.11. Delay variation due to change in (a) Temperature, (b) Length and (c) Width.

TABLE 2.1. TDC OUTPUT SHOWING LINEAR RELATION WITH DELAY

Seg.	Delay (pS)	TDC Output									
		$D_9$	$D_8$	$D_7$	$D_6$	$D_5$	$D_4$	$D_3$	$D_2$	$D_1$	$D_0$
1	86.38	0	0	1	1	1	1	1	1	1	1
2	90.26	0	1	1	1	1	1	1	1	1	1
3	94.15	1	1	1	1	1	1	1	1	1	1
4	90.20	0	1	1	1	1	1	1	1	1	1
5	86.34	0	0	1	1	1	1	1	1	1	1
6	93.98	1	1	1	1	1	1	1	1	1	1
7	90.58	0	1	1	1	1	1	1	1	1	1
8	86.23	0	0	1	1	1	1	1	1	1	1

The output of the TDC is shown in table 2.1 for different routing paths. The result shows that each path has an almost similar delay. As seen from the table, the TDC can detect a delay variation of about 4 ps.

Simulations were also performed to see the effects of temperature and process variations on the path delay. Effects of the temperature variations are shown in Fig. 2.11 (a). The simulation result shows a path delay variation of less than  $\pm 1\%$  when the temperature is varied from  $-50^\circ\text{C}$  to  $100^\circ\text{C}$ . The length and the width of the polysilicon was also varied by  $\pm 5\%$ . The corresponding outputs, shown in Fig. 2.11 (b) and (c), indicate a variation of less than  $\pm 1\%$  in each case. These are expected results due to the internal feedback of the employed DLL. The DLL adjusts its path delays due to its internal feedback to capture the lock regardless of the temperature and process variations. The feedback system in the readout circuit makes the overall measurement module resilient against temperature fluctuations and process variations.

Table 2.2 shows the comparison of the proposed method with the reported techniques in the literature. As seen from the table, only the poly layer needs to be filled using the proposed technique, which can cover 100% of the available empty space, regardless of

TABLE 2.2. COMPARISON WITH CURRENT METHODS.

Method	Maximum Initial Occupation Ratio	Final Occupation	Dependency on the IC Size	HT Detection
Paper [16]	Maximum 85%	>90%	Dependent, but not reported	Hard
Paper [18]	Dependent, but not reported	93%-99%	Does not work well for bigger ICs	Hard
Paper [19]	Maximum 80%	99%-100%	Cannot fill 100% complex circuits	Hard
Proposed	Independent	100% (poly)	Independent of IC size	Relatively Easier

the initial occupation ratio. Other reported methods depend upon the initial occupation ratio to determine what percentage of the empty spaces can be populated. In those techniques, different cells, preferably FFs, are used to cover the empty space which limits the occupation of the empty spaces. With the proposed method, as the poly layer is fully occupied, no cell can be inserted without removing a portion of the poly. Moreover, the removal of even a small portion of the polysilicon layer to insert a Trojan can easily be detected.

## 2.5 CONCLUSION

As the use of outside foundry becomes more popular, the threat of hardware security increases. As a preventative measure against malicious insertion of Trojans a new and easy to implement solution is presented in this paper. The proposed method uses the polysilicon layer to cover the empty spaces of the die to block the use of these spaces by attackers. As a result, attackers will not have access to the resources to implement and route the Trojan circuits. A DLL based readout circuit is presented to measure the propagation delay contributed by the polysilicon layer. Simulation results in cadence environment indicate that unused silicon spaces can be entirely covered to protect the main circuit against possible Trojan insertions. The simulation results also show that a

minor removal of the polysilicon layer to insert even a single inverter can readily be detected by the on-chip readout circuit. Even though CMOS 180nm technology is used in this work as a proof of concept, the same concept will also hold for more recent CMOS technologies. As the TDC resolution depends mainly upon the implemented time amplifier, not the technology.

#### **ACKNOWLEDGMENT**

The authors would like to thank the research and financial support received from the Natural Sciences and Engineering Research Council (NSERC) of Canada and CMC Microsystems.

#### **REFERENCES**

- [1] R. R. Karri, J. Rajandran, K. Rosenfield, and M. Tehranipour, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," in *Computer*, vol. 43, no. 10, pp. 39-46, Oct. 2010.
- [2] J. Dofe, J. Frey, and Q. Yu, "Hardware Security Assurance in Emerging IoT Applications," *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, 2016, pp. 2050-2053.
- [3] L. A. Guimarães et al., "Simple tri-state logic trojans able to upset properties of ring oscillators," *2016 International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS)*, Istanbul, 2016, pp. 1-6.
- [4] T. F. Wu, K. Ganesan, Y. A. Hu, H.-S. P. Wong, S. Wong, and S. Mitra, "TPAD: hardware trojan prevention and detection for trusted integrated circuits," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 4, pp. 521-534, Aug. 2015.
- [5] M. Tehranipour and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," in *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, Jan.-Feb. 2010.

- [6] S. Dupuis, M.-L. Flottes, G. Di Natale and B. Rouzeyre, "Protection against Hardware Trojans with Logic Testing: Proposed Solutions and Challenges Ahead," in *IEEE Design & Test*, vol. 35, no. 2, pp. 73-90, Oct. 2017.
- [7] S. Dupuis, P.-S. Ba, M.-L. Flottes, G. Di Natale and B. Rouzeyre, "New testing procedure for finding insertion sites of stealthy hardware trojans," *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, 2015, pp. 776-781.
- [8] M. L. Flottes, S. Dupuis, P. S. Ba and B. Rouzeyre, "On the limitations of logic testing for detecting Hardware Trojans Horses," *2015 10th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, Naples, 2015.
- [9] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. G. Wolff, C. A. Papachristou, K. Roy and S. Bhunia, "Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis," in *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2183-2195, Nov. 2013.
- [10] J. He, Y. Zhao, X. Guo and Y. Jin, "Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 10, pp. 2939-2948, Jul. 2017.
- [11] C. Bao, D. Forte, and A. Srivastava, "On reverse engineering-based hardware trojan detection," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 1, pp. 49-57, Jan. 2016.
- [12] M. K. Das, "Preventive Techniques for Hardware Trojans," Master Thesis, Masaryk University, Hyderabad, 2016.
- [13] Y. Xie, C. Bao, and A. Srivastava, "3D/2.5D IC-Based Obfuscation," in *Hardware Protection through Obfuscation*, Cham, Switzerland: Springer, 2017, ch. 12, pp. 291-312.
- [14] M. Li et al., "A Practical Split Manufacturing Framework for Trojan Prevention via Simultaneous Wire Lifting and Cell Insertion," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 9, pp. 1585-1598, Jul. 2018, doi: 10.1109/TCAD.2018.2859402.
- [15] Q. Yu, J. Dofe, and Z. Zhang, "Exploiting hardware obfuscation methods to prevent and detect hardware trojans," *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Boston, MA, 2017, pp. 819-822.
- [16] P. -S. Ba et al., "Hardware Trust Through Layout Filling: a Hardware Trojan Prevention Technique," *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA, 2016, pp. 254-259.
- [17] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware trojan detection and reducing trojan activation time," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 1, pp. 112-125, Jan. 2012.

- [18] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware Trojan insertion," *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Austin, TX, 2013, pp. 45-50.
- [19] P.-S. Ba, P. Manikandan, S. Dupuis, M.-L. Flottes, G. Di Natale and B. Rouzeyre, "Hardware trojan prevention using layout-level design approach," *2015 European Conference on Circuit Theory and Design (ECCTD)*, Trondheim, 2015, pp. 1-4.
- [20] T. M. Supon and R. Rashidzadeh, "A phase locking test solution for MEMS devices," *2017 22nd IEEE European Test Symposium (ETS)*, Limassol, 2017, pp. 1-6.
- [21] D. Pradhan and A. Singh, *VLSI Design Short Course Notes*, 1996.
- [22] E. Jedari, R. Rashidzadeh, M. Saif, "A PVT Resilient Short-Time Measurement Solution for On-Chip Testing," in *Microelectronics Journal - Elsevier*, vol. 75, pp. 35-40, 2018.8.

---

## Chapter 3

---

# A METHOD TO PREVENT HARDWARE TROJANS LIMITING ACCESS TO LAYOUT RESOURCES

---

### 3.1 INTRODUCTION

Any Integrated Circuit (IC) fabrication is divided into several stages, such as design, generating schematics or netlist, fabrication, packaging, and testing. In the early days, any semiconductor company could handle all of these steps in house. As technology evolved, new fabrication facilities had to be installed to facilitate that new technology, which meant investing billions of dollars. At the same time, as more industries got involved in IC fabrication, the design to production time, the competition to produce semiconductor design consisting of smaller and smaller transistors and various other factors has also started playing a significant role. To meet all these challenges, in the recent era, companies are more and more adopting “fly-light” model by going fabless, in which the first choice of semiconductor companies is to outsource all the silicon fabrication to foundries [1]. The advantage of outsourcing is that it lowers a big burden for the company to maintain or build a billion-dollar fabrication unit to meet the industry need to produce small and smaller ICs. This move ensured that companies could supply different ICs at a cheaper rate as the manufacturing cost has been reduced, but there are many security concerns associated with outsourcing the manufacturing of ICs in

untrusted foundries. Those foundries can modify the original design by adding extra gates to establish a backdoor to the main circuit and to reveal sensitive information stored on the chip. All these hardware changes which provide backdoor entry to the main functionality of the circuit are called Hardware Trojan (HT). Hardware security is becoming a major concern for IC designers. Any modern electronic device, such as RFID tags, IoT (Internet of Things) devices, home appliances or even biomedical equipment can be vulnerable to a security threat [2-4] if it is infected with a Hardware Trojan. If an attacker has the knowledge of complete functionality of the original circuit, he/she can design Hardware Trojans in such a manner that they can easily be added in the manufacturing flow of an IC with a small footprint as compared to the area occupied by the chip. Also, the knowledge of the original circuit helps the attacker mask the effect of HT insertion. Moreover, as technology evolved, the size of the transistors has been shrinking steadily, reducing the signal-to-noise ratio (SNR) due to their low power requisite. As a result, the effect of any small Trojan insertion can be masked more easily [5]. The insertion of an HT can heavily compromise the reliability and functionality of an IC or the system [6-8]. These Trojans are responsible not only for leaking information or secret keys stored in the chip, but they also can jeopardize the functionality of the circuit. Sometimes, these functionality changes are so severe that it fails or freezes or even makes the system to crash.

Trojans can be added to the main circuit during the fabrication process, which in addition to a security threat, can induce an economic loss related to IC production. HTs can be inserted into the original circuit to perform any or all the following three tasks (a) faulty operation or modification of the main function, (b) electrical modification, and (c)



reliability reduction [9]. To address the problems of hardware Trojans at various stages of IC design flow, many solutions have been discussed regarding Hardware Trojan detection [8-18] and prevention [24-34].

At a broad level, hardware Trojan can be divided into three categories [8]: (a) logic testing, (b) side-channel analysis, and (c) reverse engineering. In the Logic Testing method, test vectors are applied during the testing phase of an IC. It also covers stuck at faults using scan chain-based test technique or analyzing test patterns with good known patterns in Built-In-Self Test technique (BIST) [10, 11]. When used for HT detection, the main drawback of this method is that it is unrealistic to check for all the possible logic combinations in a complex IC, which enables the possibility for advanced hardware Trojans to remain undetected; thus giving the hardware attackers opportunity to use rare logic conditions as Trojan triggers. Another disadvantage of this technique is the limitation posed by the lack of observability and the lack of controllability in manufactured IC due to a large number of IP cores in ASICs and millions of nano-scale building blocks in an IC. Moreover, the test infrastructures may be denied the possibility to detect an HT insertion via a minute alteration of the HT trigger [12]. The physical parameters of the circuit like analyzing the power profile when the IC is performing critical steps, for example analyzing round key operations at different cycles of AES encryption, or analyzing either transient current or electromagnetic spectrum or the delay produced by the gates can also be used to detect Hardware Trojan, which are classified as side-channel analysis [13, 14]. This technique is a non-invasive one as it does not tamper the circuit under attack. This method is successfully used to extract critical information such as cryptography keys from IC systems. It can also be utilized to detect Trojan

activities. This method commonly requires a trusted golden circuit for result comparison. As the latest IC technologies work at the lower supply voltages, the Signal-to-Noise-Ratio (SNR) of these ICs is lower compared to previous technologies. Therefore, the background noise and even process variations can mask Trojan activities and prevent them from detection through side-channel analysis. An important point to consider in this technique is that the delay of logic gates is highly affected by the supply voltage or the voltage drop. As the voltage drop increases, the delay of the gate also increases. In addition, other parameters which can affect gate delay are channel length (L), channel width of transistor (w), the thickness of oxide ( $T_{ox}$ ), threshold voltage of the transistor ( $V_{th}$ ); process and environmental variations also can affect the delay if the ICs are not manufactured at the same temperature [15]. Accounting for all these variables make HT detection using side-channel analysis very difficult. To increase the percentage variation caused by an HT circuit compared to the original circuit, a Design for Hardware Trust (DfHT) technique has been presented in [16], where the design switching of any target region can be localized while keeping others quiet. This reduces total circuit switching activity, which increases the Trojan-to-circuit Switching Activity (TCA) and the power consumption ratio between the original to Trojan circuit. This helps the Trojan detection by magnifying the Trojan's contribution. The authors of [17] have presented another DfHT technique where a protection structure using an optically active protective  $TiO_2$ - $TiO_2$  layer stack with an angular dependent reflectivity has been used for the silicon chip backside. The light reflected off the backside of the chip highlights strong angle-dependent reflectivity, which alters if the backside is affected by any hardware attack. Another contribution of this method is its ability to create a signal to verify whether such

an attack took place or not, by creating a pattern of photocurrents during the IC running state. No additional mask or circuitry is needed for this technique. The reverse engineering method, presented in [18], is a powerful HT detection method compared to the other techniques. However, it is a costly and destructive approach. Moreover, when a small portion of the fabricated ICs is infected, reverse engineering may fail as healthy ICs may get selected for reverse engineering. The third-party IP (3PIP) cores also add an extra layer of challenge while detecting Trojans. Cores from a third party can be divided into three main categories: (a) soft, (b) firm and (c) hard [19]. Soft cores are the ones that are written using hardware description language such as Verilog/VHDL. The firm core is characterized by some specific libraries provided by the design foundries and moving through synthesis without using physical layout. This core can be used to optimize the area through placement and routing and known as a synthesized code. The hard core is described by a hard layout using physical design libraries and recognizable in the form of a GDSII file, which is a collection of mask level blocks. Researchers have proposed different ideas [20-23] as countermeasures for HTs inserted into 3PIP cores. Finding hardware Trojans in these 3PIP cores is very difficult as the codes or the libraries or the GDSII files for those are provided by the third-party designer and they may include Hardware Trojans within them without the knowledge of the user as there is no benchmark Trojan-free core or golden core which can be compared with Trojan infected core. If the core is infected with Trojan code, all the fabricated ICs will be infected with that Trojan circuit. In a nutshell, it is very difficult to detect Hardware Trojan as there are many possible ways to insert a Trojan and there are a lot of varieties depending on various factors such as circuit type, trigger/payload type, desired outcome of the Trojan

circuit and so on. Most of the detection methods work well for certain classes of Trojans while are unable to even detect some other types. A comprehensive solution to detect all types of Trojans is yet far from reach. Moreover, once a Trojan is inserted, the damage is done; and even if it is detected, the infected device needs to be discarded. Trojan prevention methods, on the other hand, have the advantage of protecting the IC in the first place.

The methodologies for HT prevention can be classified into three different groups [24]: (a) logic obfuscation, (b) compact GDS-II layout generation, and (c) layout filling. A logic obfuscation method has been introduced in [25], where the researchers have added some reconfigurable circuits to the main design. This way, the manufacturer is unable to determine the functionality of the main circuit and the circuit is protected against reverse engineering. Another logic obfuscation method is proposed in [26], where a secure-by-construction split manufacturing flow has been introduced to obfuscate the netlist. This method is capable of being used for both 2.5D or 3D IC protection. However, it is not able to prevent Hardware Trojan insertion during the process of the die stacking and TSV bonding. IC camouflaging [27] and Logic Locking [28, 29] also have been classified as obfuscation methodologies. Researchers in [30] have summarized all the latest obfuscation methods with their pros and cons. A compact GDS-II layout has been generated in [31] by adding dummy flip-flops (FFs). Even though this idea was the building block for various new layout filling approach, it has some major concerns as the detection of the removal of any of those dummy-FFs is impractical due to the fact that those cells do not produce any function. Thus, the risk of HT insertion into the layout remains. One of the more efficient methods is a layout filling approach described in [32],

where the unused spaces in the layout have been filled with functional cells. However, this method only is capable of filling approximately 90% of the whole existing layout. Another HT prevention method using layout filling approach, called Built-In Self Authentication (BISA), has been proposed in [33]. The authors of this manuscript added standard library cells along with Test Pattern Generator (TPG) and Output Response Analyzer (ORA) to the main layout in order to fill the unused area. Another technique for filling empty spaces using functional cells is introduced in [34] where both shift registers and functional cells (used in [33]) are substituted with Multiple Input Shift Registers (MISRs) and Output Response Analyzers (ORAs). All these methods are somewhat vulnerable to Trojan insertion as none of these can fill 100% of the unused die area regardless of any condition. The possibility of using functional cells to fill the unused die area also depends on the initial occupation ratio; the maximum being 85%, as reported in [32]. If the original circuit occupies more than the reported percentage of the die, these methods cannot be used to prevent HT insertion. Moreover, their performances degrade with increasing circuit-complexity.

This paper presents a new Design-For-Security (DFS) idea for HT prevention, in which the attackers are deprived of any space to insert the active components of any malicious circuitry. The proposed method in this work is much easier to implement compared to the other prevention methods relying on filling the silicon area with functional cells. It also supports full occupation regardless of the initial occupation ratio and does not consume any power during normal operation mode. In the proposed method, after completion of the main circuit design, the path to the active layer is blocked by covering the unused polysilicon layer using minimum feature wires. As polysilicon

connects to the active layer directly without the need for any contact, no extra component can be added to the circuit without removing a portion of these polysilicon wires. Such an alteration can be detected by both the implemented readout circuit, inspired by the Delay-Detection-Module (DDM) proposed in [35] and the signature detection circuit.

The rest of the paper is organized as follows: the proposed method is explained in section II; section III discusses the readout circuit; section IV presents the simulation results; and finally, section V summarizes the concluding remarks.

### **3.2 PROPOSED METHOD**

The idea proposed in this article is twofold: (a) measure the delay of the added polysilicon wires while keeping the main circuit is in rest mode (which will reduce if a Trojan is inserted, as the polysilicon wires need to be removed to insert a Trojan), and (b) observe and analyze the signature obtained during the normal operation of the main circuit (it will change if a Trojan is inserted, as both the induced magnetic and electric field will change due to structural change of the polysilicon wires).

#### ***A Delay Measurement***

As part of the fabrication process for CMOS technologies, the metal layers are connected through contacts to the active silicon layer for the purposes of routing. The attackers can be deprived of the resources to insert functional Trojans by denying them access to the active layer (n+ or p+ implant) to make any unauthorized connection to that layer. The polysilicon layer, which is separated by a thin oxide layer as shown in Fig. 3.1, can be utilized to cover the silicon substrate region, where the active regions are formed. ICs are designed using different active regions routed through polysilicon and metal

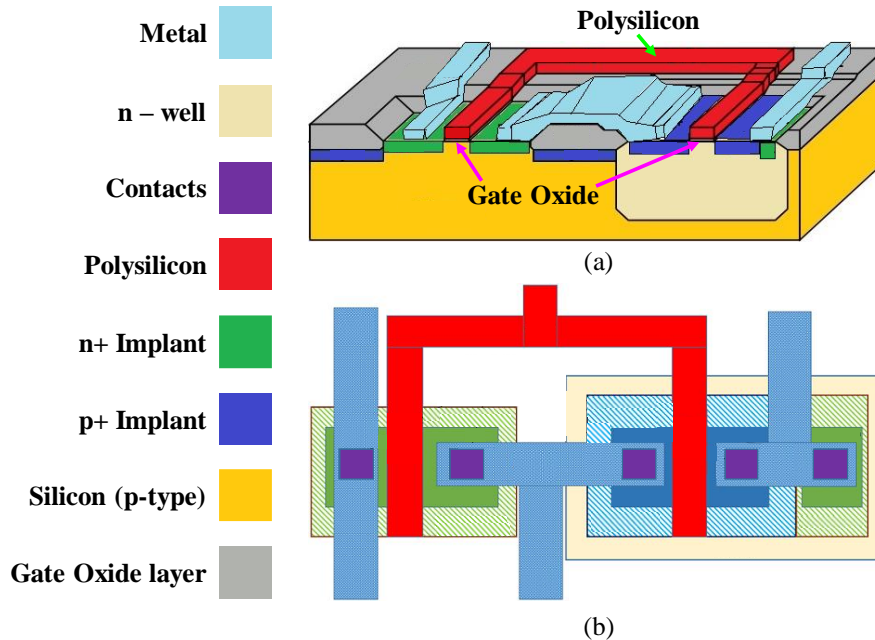


Figure 3.1. A typical CMOS process indicating layout layers: (a) 3D view (b) Top view [36].

layers. As shown in Fig. 3.1, the polysilicon connects directly to the active region through a very thin gate oxide layer. On the other hand, the metal layers are connected to the active region by some contacts. So, if the unused polysilicon layer is covered using minimum feature wires, attackers will not be able to access the substrate layer to insert the active layer necessary for Trojan insertion. Any small removal of the polysilicon wire will alter the path delay and overall parasitic capacitance of the polysilicon layer, which can be detected by an on-chip readout circuit. The electric field induced to the polysilicon wire will also change, which will affect the induced signature. A conceptual design of the routing of a simple circuit was created using HFSS (High-Frequency Structure Simulator) to evaluate the effect of polysilicon removal on the distribution of the electric field and the path delay. 3D full-wave simulation results in Fig. 3.2 show the distribution of the electric field before and after removal of a small portion of the polysilicon layer accounting for less than 1% of the total polysilicon area. The change in the electric field is due to the variation of the polysilicon layer's structure, parasitic capacitance and path

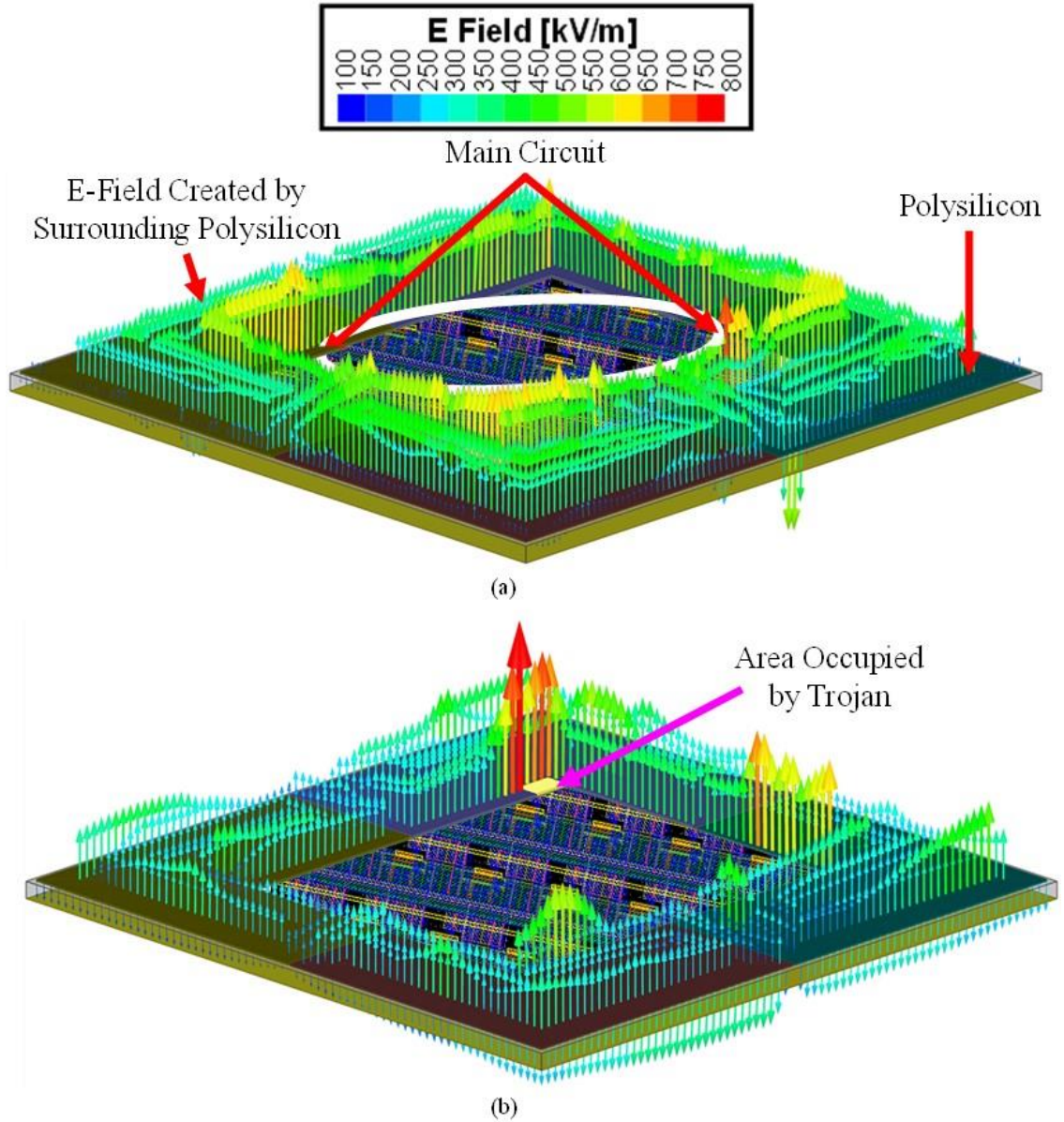


Figure 3.2. 3D full wave simulation indicating the electric field difference between (a) the original and (b) the Trojan affected design.

resistance. The relationship between the electric field and the parasitic capacitance of the polysilicon layer can be determined from the stored energy as:

$$W_1 = \frac{1}{2} C_{p1} V^2 = \frac{1}{2} \sum_{i=1}^n \epsilon E_i^2 dv \quad (1)$$



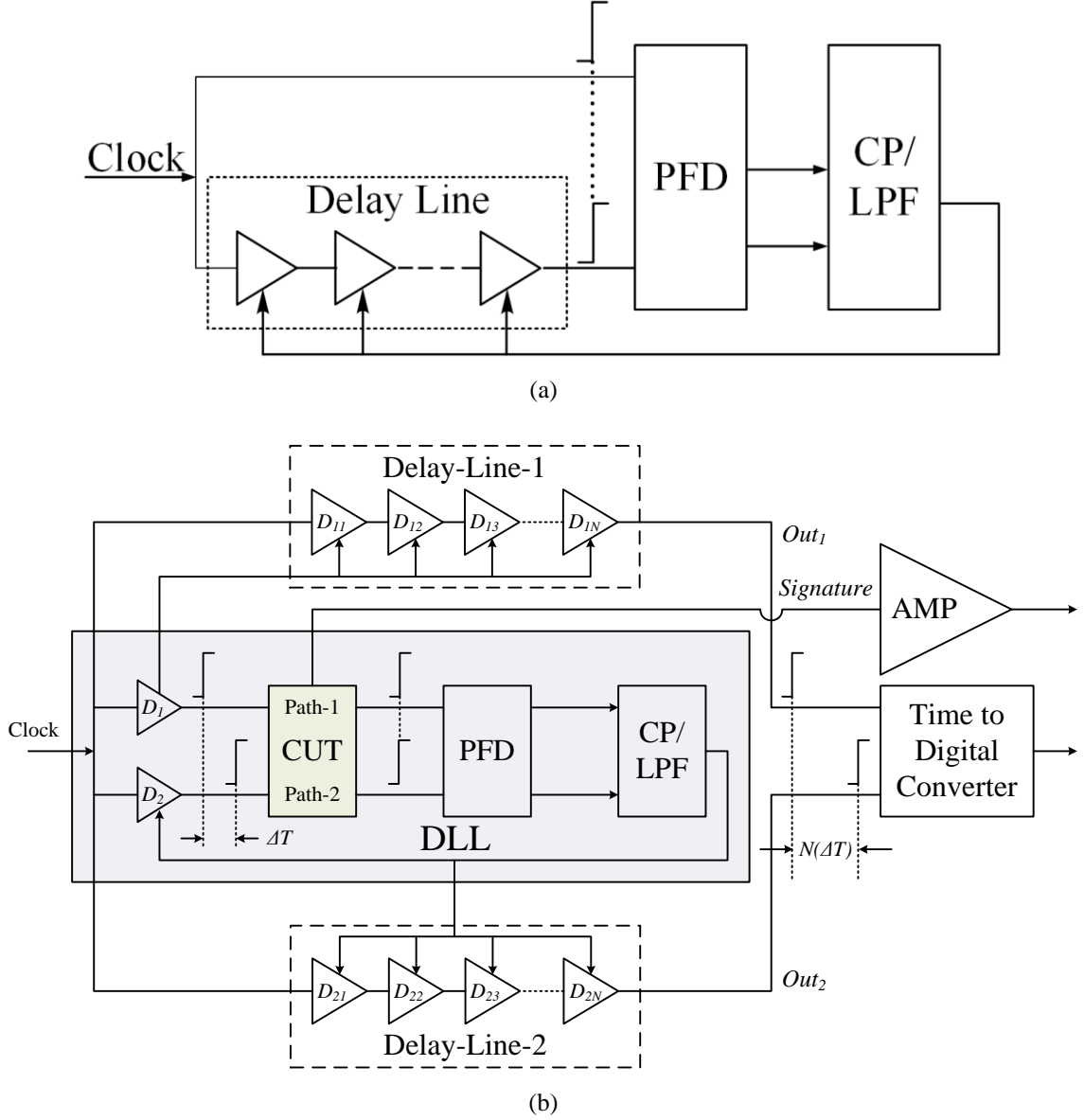


Figure 3.3. (a) Conventional Delay Locked Loop, (b) Readout Circuit with Signature detection block. where  $W$  is the energy stored,  $C_P$  is the parasitic capacitance,  $V$  is the applied voltage and  $E_i$  is the electric field of discrete points in the device and  $v$  is the volume of between the ground plane and the polysilicon layer. The effect of removal of less than 1% of the total polysilicon area is shown in Fig. 3.2 (b). Consequently, the stored energy changes to:

$$W_2 = \frac{1}{2} C_{p_2} V^2 = \frac{1}{2} \sum_{j=1}^n \epsilon E_j^2 dv \quad (2)$$

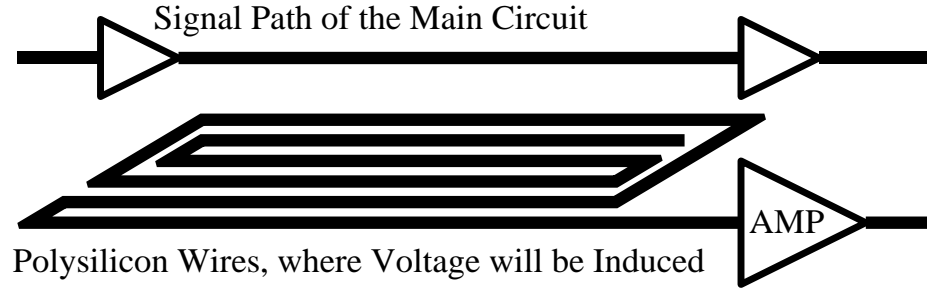
Since  $V$  and  $\varepsilon$  are constants, from (1) and (2) we can write:

$$\Delta C_p \propto \Delta E^2 \quad (3)$$

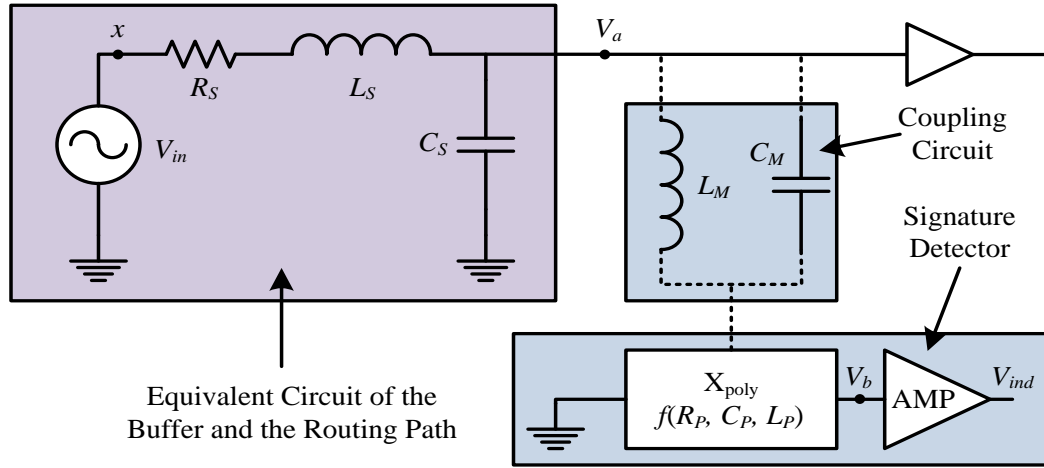
where  $\Delta C_p = C_{p_1} - C_{p_2}$  and  $\Delta E^2 = \sum_{i=1}^n E_i^2 - \sum_{j=1}^n E_j^2$ . The variation in the time constant of the polysilicon layer can be determined from  $\tau = R\Delta C_p$ , where  $R$  is the total resistance of the polysilicon layer. Even though  $\Delta C_p$  can be realized using a capacitor, the time constant will not remain the same due to the variation in resistance, and hence, the delay will change. Simulations conducted in the circuit level indicate that this variation can readily be detected by observing the path delay. The path delay is measured using the readout circuit shown in Fig. 3.3. The poly area was divided into 8 segments to ensure that the area of each segment is small enough to detect a minor area removal. The number of segments depends on the minimum detectable size of a Trojan. As the number of segments increases, the smaller size Trojans can be detected.

### ***B Detecting Signature Variation***

During the normal mode of the main circuit, the routing lines create both electric and magnetic fields; a portion of which is induced in the added polysilicon wires. These filler routing lines will induce voltage following the principle of coupled transmission lines [37]. The response can be characterized by their resistances ( $R_R, R_P$ ) and self and mutual inductances ( $L_R, L_P, L_M$ ) and capacitances ( $C_R, C_P, C_M$ ) per unit length, where subscripts R, P, and M represent Routing line, Polysilicon and Mutual respectively. The equivalent model of a single routing line and the polysilicon wires is shown in Fig. 3.4 (a) and the equivalent circuit model is shown in Fig. 3.4 (b). The voltage at point “a” can be found by:



(a)



(b)

Figure 3.4. (a) Block diagram of a typical routing path and the polysilicon wire underneath (b) The equivalent schematic diagram of the same showing the coupling circuit.

$$V_a = V_{in} \frac{X_{C_R}}{R_R + X_{L_R} + X_{C_R}} \quad (4)$$

where  $V_{in}$  represents the input signal at point “x”,  $R_R$ ,  $L_R$ , and  $C_R$  are the resistance, inductance, and capacitance of the routing line. So, the voltage at point “b”, induced by the polysilicon wire, can be represented as:

$$V_b = V_a \left( \frac{X_{Poly}}{X_{Poly} + X_{Coupling} + X_{Routing}} \right) \quad (5)$$

where  $X_{Poly} = (R_P + X_{L_P}) \parallel X_{C_P}$ ,  $X_{Coupling} = X_{L_M} \parallel X_{C_M}$  and  $X_{Routing} = (R_R + X_{L_R}) \parallel X_{C_R}$ . The voltage found by equation 5 is for a single routing line whereas a circuit

has many such lines. If  $n$  represents the total number of routing lines, the total induced voltage after amplification,  $V_{ind}$  can be written as:

$$V_{Ind} = A \sum_{i=1}^n V_{b_i} = \sum_{i=1}^n \frac{AV_{a_i}(X_{Poly_i})}{X_{Poly_i} + X_{Coupling_i} + X_{Routing_i}} \quad (6)$$

where  $A$  is the gain of the amplifier. This induced voltage will act as a unique signature for the IC as the waveform will depend on the position of the polysilicon wires relative to the routing paths, as it will affect the amount of induction.

### 3.3 READOUT CIRCUIT

#### *A Description of the Readout Circuit*

The readout circuit includes a Circuit-Under-Test (CUT) module, a modified Delay Locked Loop (DLL) for time measurement and a Time-to-Digital Converter (TDC), as shown in Fig. 3.3 (b). The main advantage of utilizing a DLL for time measurement is its robustness against Process, Voltage, and Temperature (PVT) variations. It is shown in the simulation section that for a  $\pm 5\%$  process variation, the propagation delay changes by less than  $\pm 1\%$ . A conventional DLL includes a Phase Frequency Detector (PFD), Charge Pump (CP), Low Pass Filter (LPF) and delay-line modules, as shown in Fig. 3.3 (a). The DLL adjusts the propagation delay of its delay-line to reduce the time difference between the signals applied to the PFD. In the locked state, the signals applied to the PDF are aligned and ideally, the time difference between them becomes zero. The block diagram of the readout circuit is shown in Fig. 3.3 (b). A CUT is added to the DLL feedback loop to measure the delay difference between its signal paths. The readout circuit also includes two delay-lines used to amplify the time difference captured by the DLL.

When the DLL in the readout circuit captures the lock, the rising edges at the PFD input are aligned as shown in Fig. 3.3 (b). Since the same clock signal is applied to both  $D_1$  and  $D_2$  cells, we can write:

$$T_{D1} + T_{path\_1} = T_{D2} + T_{path\_2} \quad (7)$$

and therefore, we have:

$$T_{D1} - T_{D2} = T_{path\_2} - T_{path\_1} = \Delta T \quad (8)$$

where  $T_{D1}$  and  $T_{D2}$  are the propagation delay of  $D_1$  and  $D_2$  cells respectively and  $T_{path1}$  and  $T_{path2}$  represent the path-1 and path-2 propagation delays in the circuit-under-test. From equation 8 it is evident that the delay difference between cells  $D_1$  and  $D_2$  makes up the delay difference between the two paths of CUT. A Time Amplifier (TA), proposed in [38], is then used to amplify this delay. Delay-Line-1 and Delay-Line-2 in the readout circuit are used to amplify the delay difference between the CUT paths. The first delay line is composed of  $D_1$  cells while the second one is built using  $D_2$  cells. Therefore, the delay difference between the outputs of the two delay lines marked as  $Out_1$  and  $Out_2$  in Fig. 3.3 (b), becomes  $N\Delta T$ . This amplification of the delay relaxes the design requirement for the time-to-digital converter (TDC) and enables the TDC to measure the delay difference between the CUT paths a with a high-resolution measurement. The operation detail of the readout circuit is presented in [35].

To test the propagation delay of the polysilicon layer, the CUT in the readout circuit in Fig. 3.3 (b) is designed as shown in Fig. 3.5. The propagation delay caused by the polysilicon layer is represented by a delay cell in Fig. 3.5. The circuit also incorporates a self-test path to test and ensure that the readout circuit has not been tampered with. The

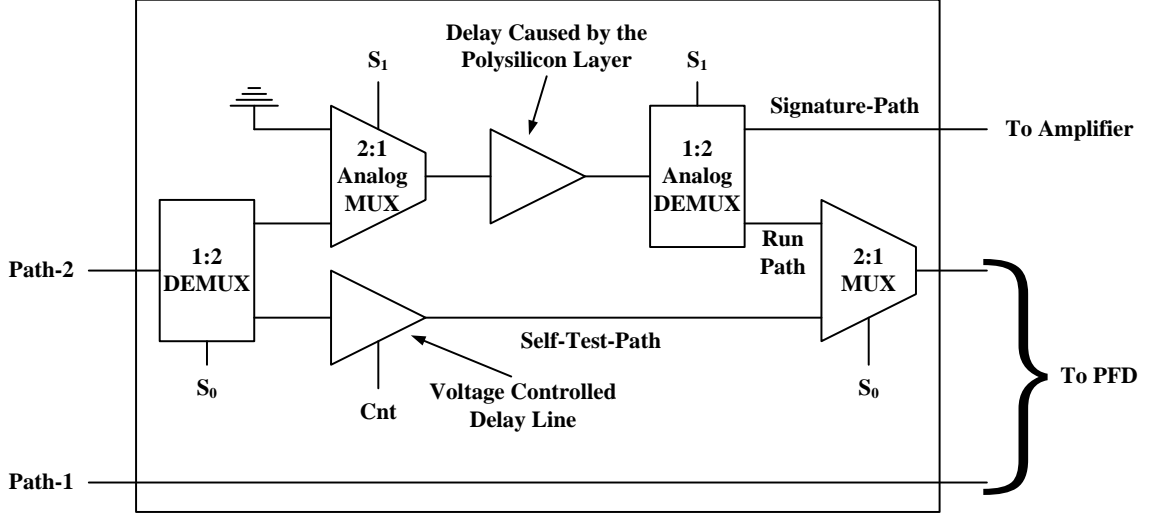


Figure 3.5. Circuit-Under-Test.

polysilicon layer can be divided into several separate segments to increase the measurement resolution. In this case, each segment is selected separately to measure its nominal propagation delay. There are two modes of operation for the readout circuit, the “Self-Test Mode” and the “Run Mode”.

### ***B Working Principle of the Readout Circuit***

A clock signal is fed to the input of the readout circuit in Fig. 3.3 (b). Initially, the readout circuit is run in the “Self-Test” mode to confirm the proper functioning of the readout circuit and to calibrate the device. Then the run mode is selected. The polysilicon layer in the CUT introduces a delay to the signal path-2. As explained in section 3A, the DLL feedback system compensates for the delay to acquire lock. Once the lock is captured, we have:

$$T_{D1} - T_{D2} = \Delta T = T_{Poly} + T_{offset} \quad (9)$$

where  $T_{Poly}$  is the propagation delay contributed by the polysilicon layer. Since the offset delay of the readout circuit is determined during calibration in the self-test mode, the

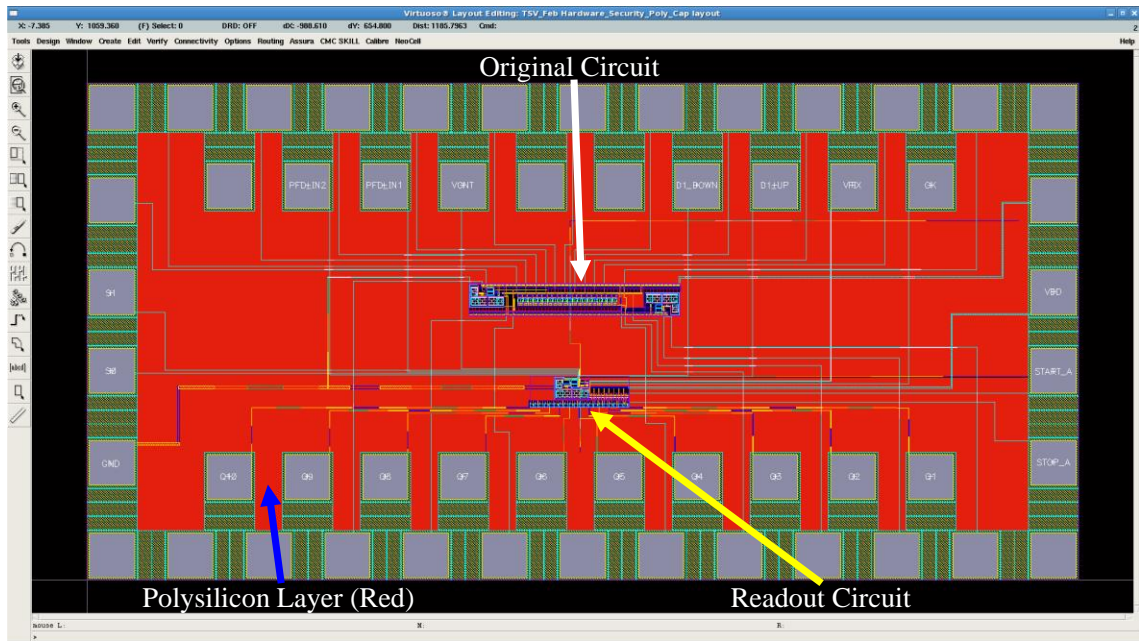


Figure 3.6. The IC with Polysilicon and Readout Circuit added.

propagation delay due to the polysilicon layer can readily be calculated and delay variations from the nominal values can be identified.

### 3.4 SIMULATION RESULTS

To validate the proposed method, the readout circuit was implemented in the Cadence environment where the polysilicon layer was used to cover the unused silicon area to ensure that it will not be utilized for Trojan insertion. The red area in Fig. 3.6 shows the polysilicon layer which is divided into 8 segments. After filling out the empty spaces with polysilicon, the readout circuit was tested in the self-test-mode to determine the offset delay. To perform the self-test, initially, the control voltage,  $V_{CNT}$ , of the VCDL was kept at 0 V. The input and output signals of the readout circuit at the locked state, with the control voltage set to zero, are shown in Fig. 3.7 (a). Fig. 3.7 (b) shows the locked condition with  $V_{CNT}$  settling at 953.8 mV. The initial delay between the input and output signals is 17.85 ps, as indicated in Fig. 3.7 (c). As the control voltage increases

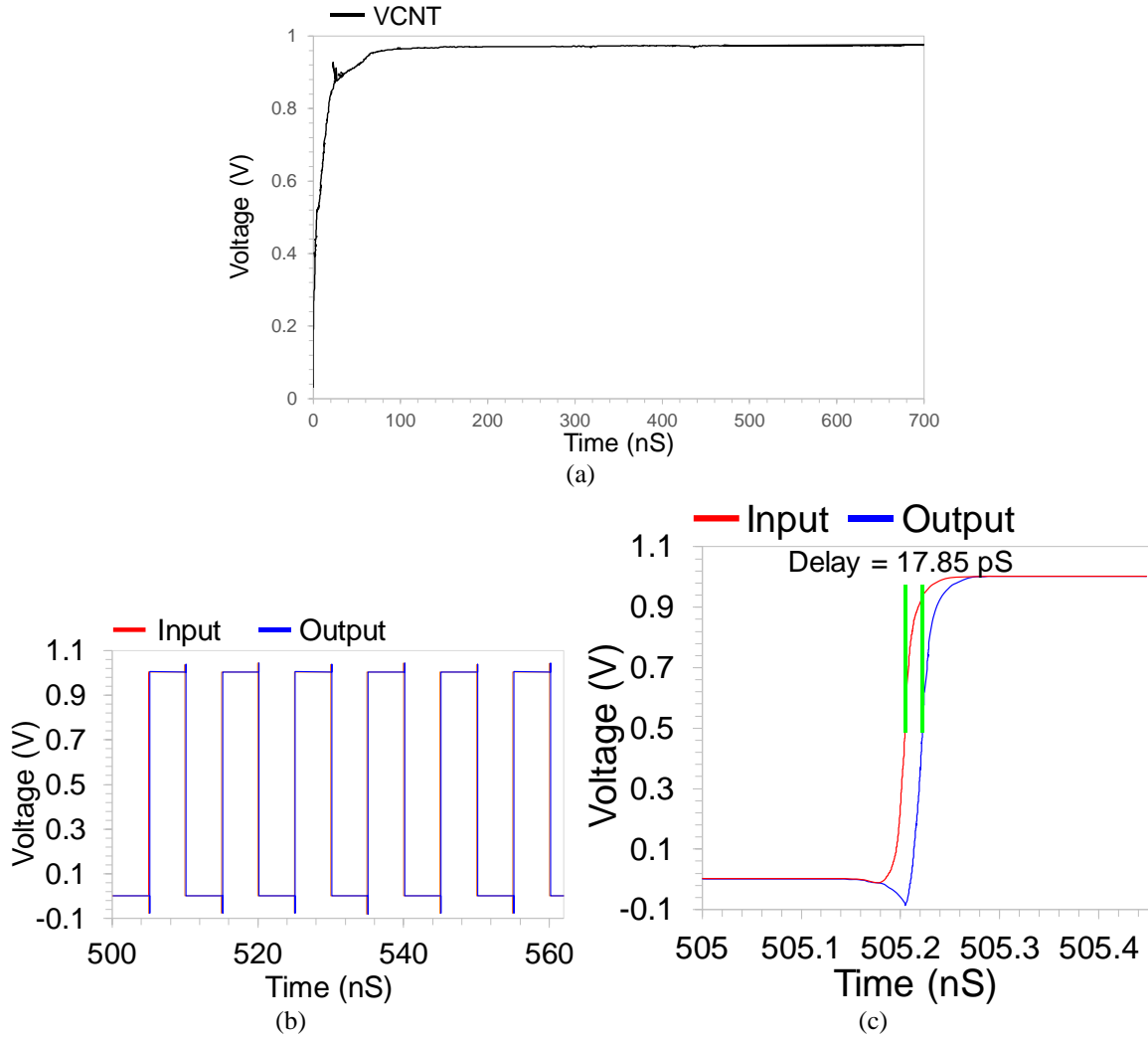


Figure 3.7. (a) Control Voltage of the DLL (b) The Locked Signal and (c) Delay between the Output and the Input Signals.

from 0 to 1.8 V, the delay rises linearly from 17.85 ps to 66.43 ps, shown in Fig. 3.8. The minimum area required for a Trojan insertion depends on the type of Trojan and the size of the gate. An inverter from the standard cell library of 0.18 $\mu\text{m}$  CMOS technology, shown in Fig. 3.9 (a), was added to the circuit to see if the proposed method can detect a small hardware manipulation. The minimum area of the polysilicon layer that must be removed to place this gate is around 14.85  $\mu\text{m}^2$ , as shown in Fig 3.9 (b). Figure 3.9 (c) presents the delay associated with the polysilicon of Fig. 3.9 (b) which is about 4.65 ps. The implemented readout circuit can readily detect such a small delay.



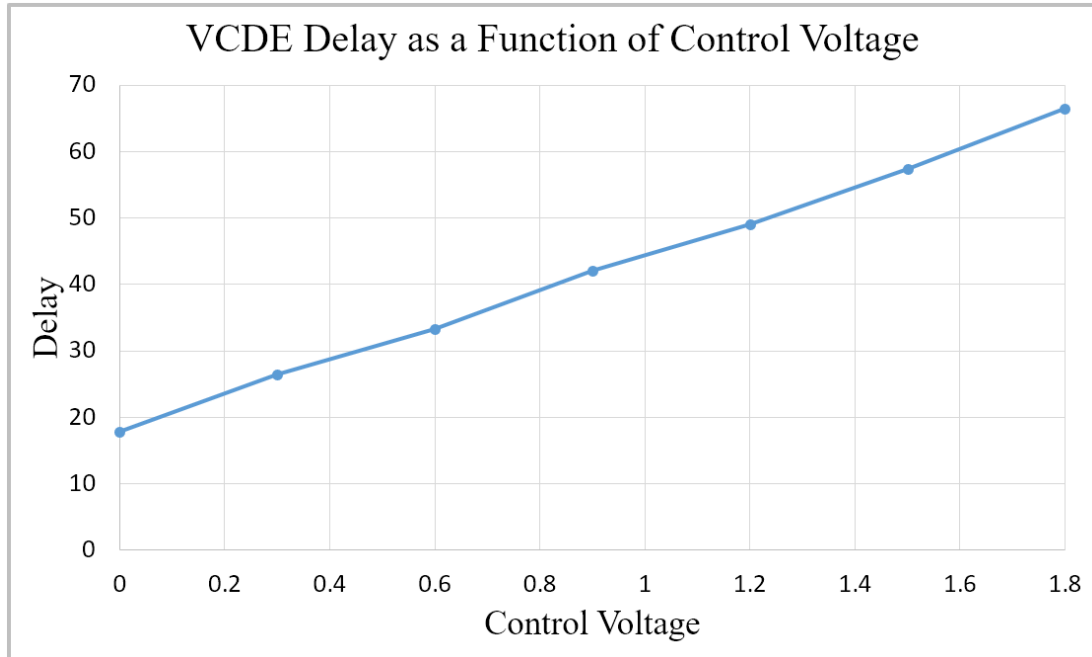


Figure 3.8. Relationship between VCDL Delay and Control Voltage.

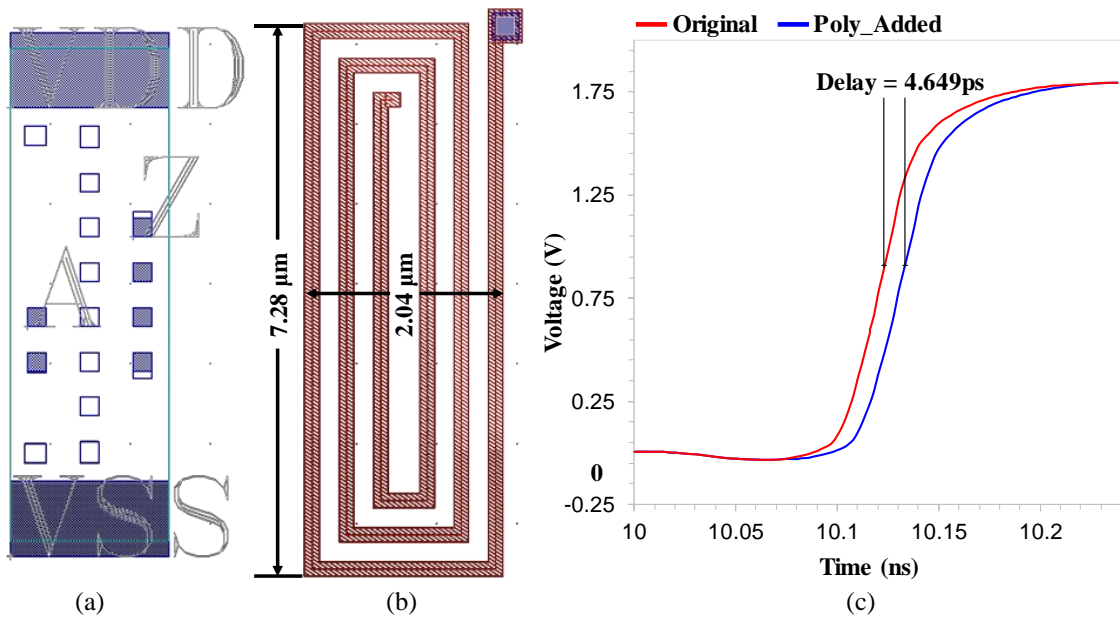


Figure 3.9. (a) Typical TSMC Inverter (b) Minimum poly needed to be removed to place that inverter (c) Delay caused by that poly.

The change in the delay associated with such removal was also observed. As shown in Fig. 3.10 (a), the delay of the routing segment 2 is 90.26 ps. Later the same simulation was performed with the layout of Fig. 3.9 to see the effect of the removal of a portion of

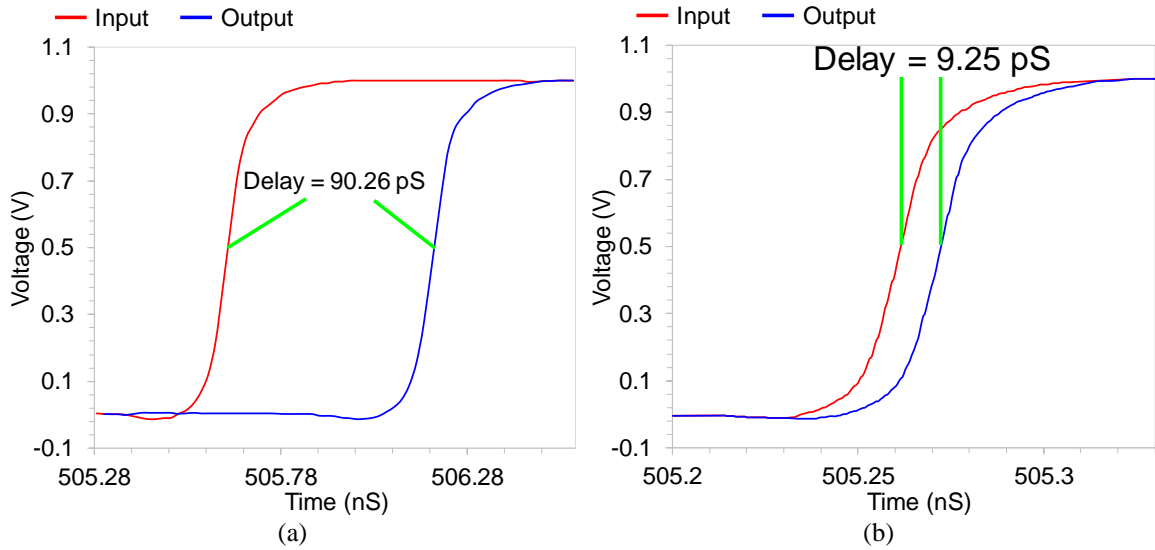


Figure 3.10. (a) Delay of the original routing segment 2; (b) Delay variation due to the removal of a portion of the polysilicon wire.

TABLE 3.1. TDC OUTPUT SHOWING LINEAR RELATION WITH DELAY

Seg.	Delay (pS)	TDC Output									
		$D_9$	$D_8$	$D_7$	$D_6$	$D_5$	$D_4$	$D_3$	$D_2$	$D_1$	$D_0$
1	86.38	0	0	1	1	1	1	1	1	1	1
2	90.26	0	1	1	1	1	1	1	1	1	1
3	94.15	1	1	1	1	1	1	1	1	1	1
4	90.20	0	1	1	1	1	1	1	1	1	1
5	86.34	0	0	1	1	1	1	1	1	1	1
6	93.98	1	1	1	1	1	1	1	1	1	1
7	90.58	0	1	1	1	1	1	1	1	1	1
8	86.23	0	0	1	1	1	1	1	1	1	1

the polysilicon wires. As can be seen in Fig. 3.10 (b) such a removal decreases the path delay by 9.25 ps. The output of the TDC is shown in Table 3.1 for different routing paths. The result shows that each path has an almost similar delay. As seen from the table, the TDC can detect a delay variation of about 4 ps.

The signature was also obtained for the whole circuit, which is shown in Fig. 3.11 along with the effect of adding extra polysilicon wires. Fig. 3.11 (a) shows the output of the original circuit without the polysilicon wires, whereas Fig. 3.11 (b) shows the same output with the wires added to the circuit. The difference between the first and second waveforms is shown in Fig 3.11 (c), with a maximum error range of 500  $\mu$ V, while the

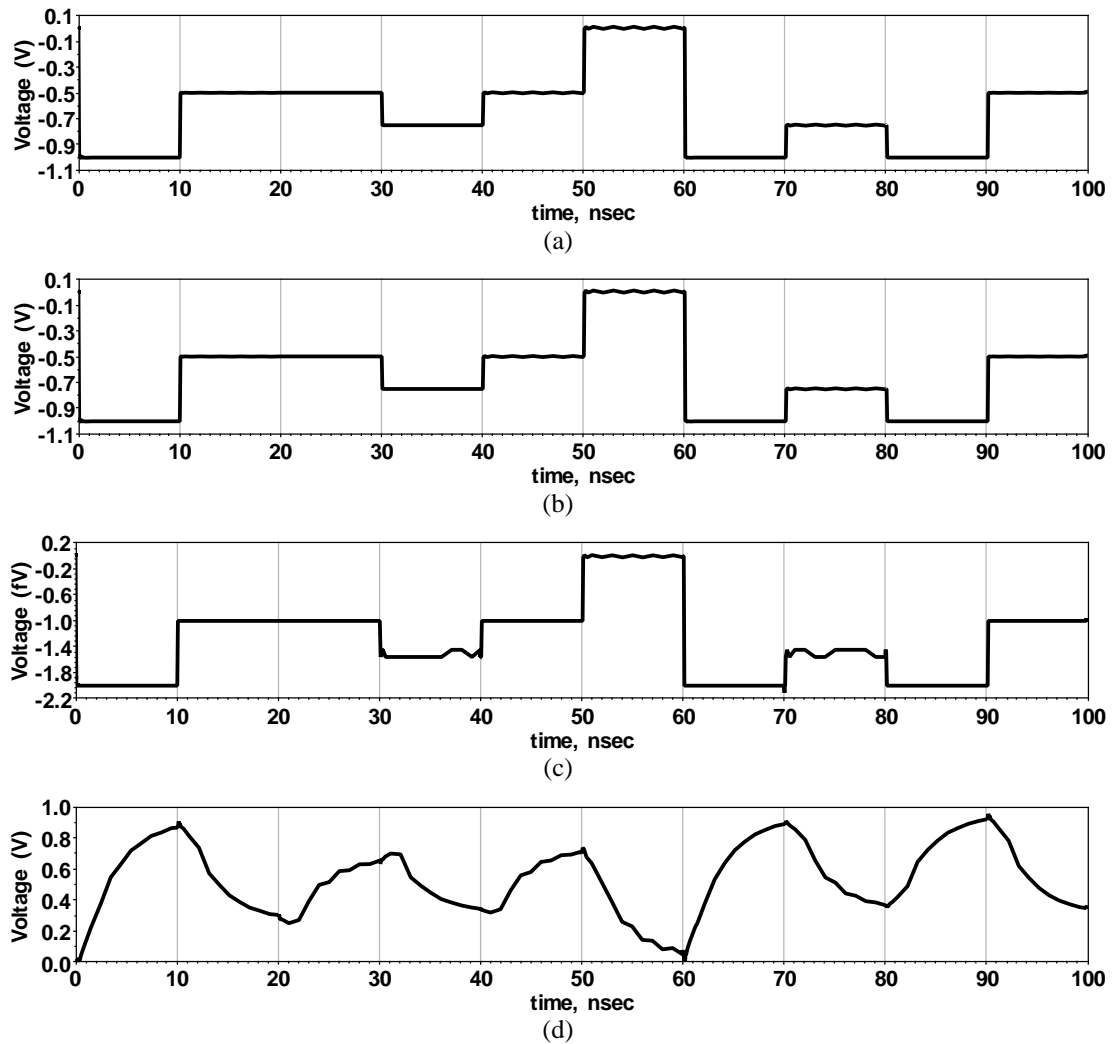


Figure 3.11. Output voltage (a) without probe (b) with probe; (c) difference between a and b; and (d) The unique signature.

shape of the output remains the same. This indicates that the addition of those extra polysilicon lines barely affects the performance of the circuit. The unique signature obtained from the circuit is shown in Fig. 3.11 (d), which is reproducible as the same signature will be generated for the same input. This signature will change if either the placement of the probe is altered, or a portion of it is removed.

To verify that statement, a portion of the polysilicon routing was removed to simulate the effect of Trojan insertion, which is shown by a small circle in Fig. 3.12. Then

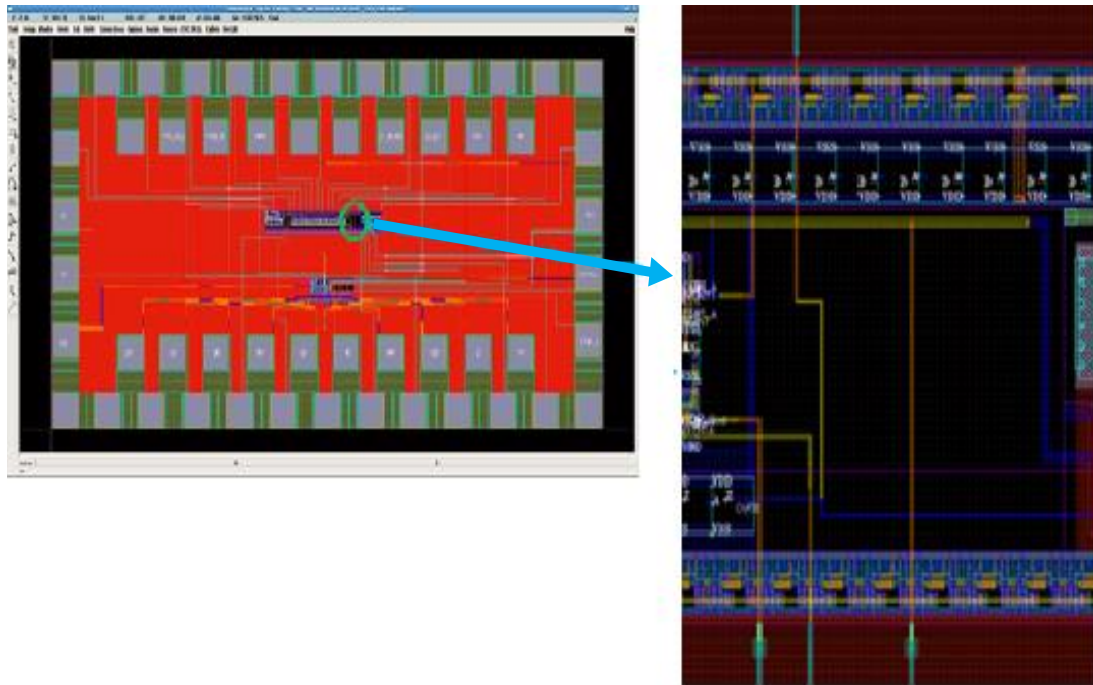


Figure 3.12. The IC with polysilicon layer partially removed to insert Trojan.

transient simulations were performed to find the delay associated with each routing path of the original design of Fig. 3.6. The effect of the polysilicon removal on the signature is shown in Fig. 3.13. The signature obtained by the original design of the polysilicon wires is shown in Fig. 3.13 (a), whereas the signature after removing part of that said polysilicon wire is shown in Fig. 3.13 (b). The difference between these two waveforms is shown in Fig. 3.13 (c), which varies between  $-0.6$  mV and  $+0.9$  mV. The change in the voltage level is high enough to easily detect. Moreover, as the shape of the signature also changes, the detection becomes much easier.

The Monte-Carlo simulations performed to check the effect of process variation show that even though the voltage level of the signature varies considerably; the shape of the signature remains unchanged. The parameters of the polysilicon wires were varied by  $\pm 10\%$  over a simulation of 500 iterations. The output of the simulation is shown in Fig.

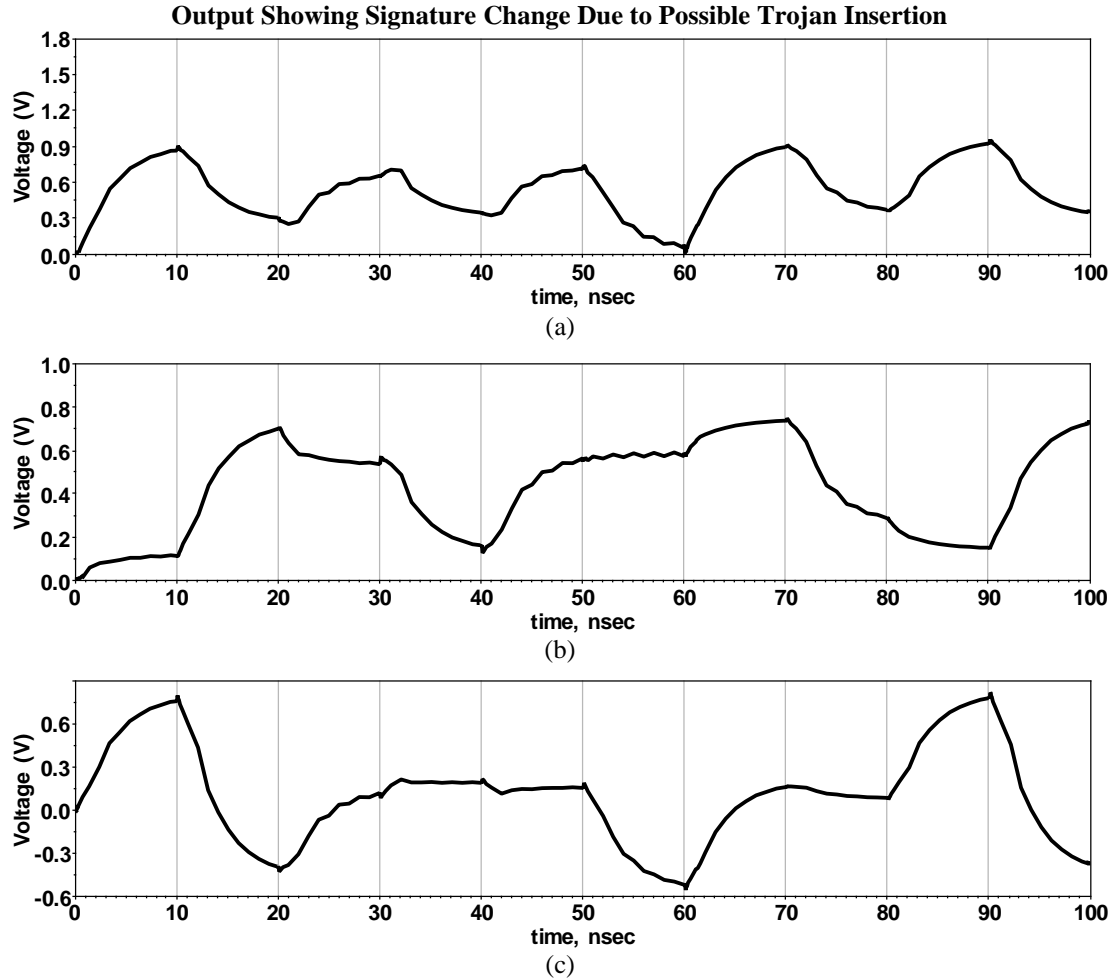


Figure 3.13. Graph showing change between the signatures of the original and the manipulated design.

3.14. Fig. 3.14 (a) shows the output of the original circuit, which indicates that it remains unchanged regardless of any variation of the probe. As shown in Fig. 3.14 (b), the DC offset of the signature varies considerably by as much as 135 mV. The frequency content of the signature and accordingly the shape of the signature remains unchanged, whereas any change in the model of the probe varies the shape of the signature.

Simulations were also performed to see the effects of temperature and process variations on the path delay. The effects of the temperature variations are shown in Fig. 3.15 (a). The simulation result shows a path delay variation of less than  $\pm 1\%$  when the temperature is varied from  $-50^{\circ}\text{C}$  to  $100^{\circ}\text{C}$ . The length and the width of the polysilicon

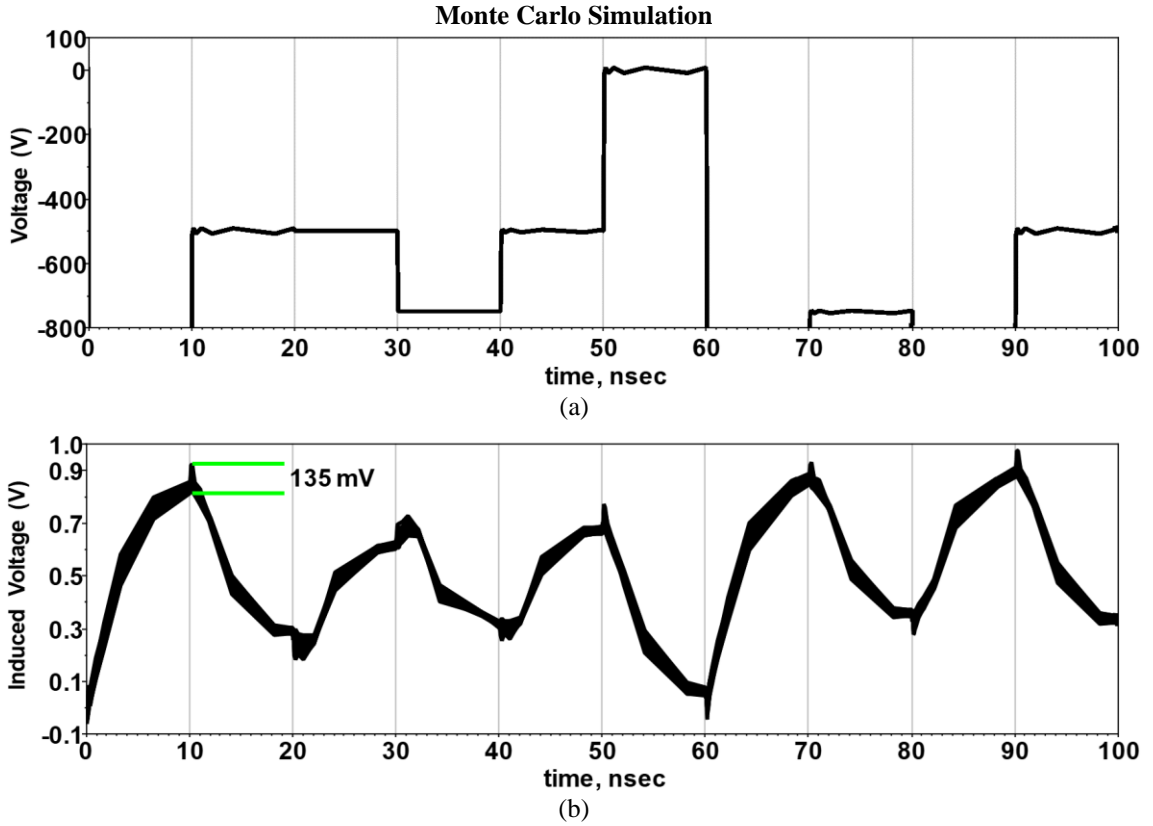


Figure 3.14. Monte Carlo Simulation for 500 iterations: (a) Output of the main circuit; (b) The signature.

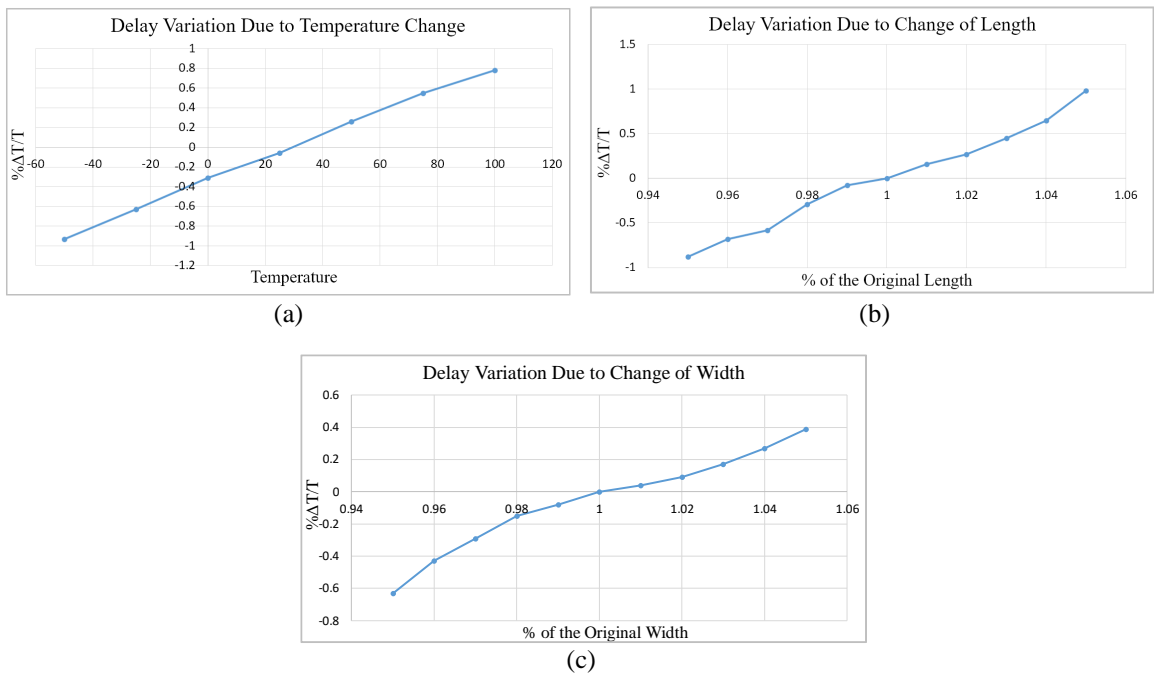


Figure 3.15. Delay variation due to change in (a) Temperature, (b) Length and (c) Width.

TABLE 3.2. COMPARISON WITH CURRENT METHODS

Method	Maximum Initial Occupation Ratio	Final Occupation	Dependency on the IC Size	HT Detection
Paper [32]	Maximum 85%	>90%	Dependent, but not reported	Hard
Paper [33]	Dependent, but not reported	93%-99%	Does not work well for bigger ICs	Hard
Paper [34]	Maximum 80%	99%-100%	Cannot fill 100% complex circuits	Hard
Proposed	Independent	100% (poly)	Independent of IC size	Relatively Easier

was also varied by  $\pm 5\%$ . The corresponding outputs, shown in Fig. 3.15 (b) and (c), indicate a variation of less than  $\pm 1\%$  in each case. These are expected results due to the internal feedback of the employed DLL. The DLL adjusts its path delays due to its internal feedback to capture the lock regardless of the temperature and process variations. The feedback system in the readout circuit makes the overall measurement module resilient against temperature fluctuations and process variations.

Table 3.2 shows the comparison of the proposed method with the reported techniques in the literature. Using the proposed method, 100% of the unused polysilicon layer can be covered regardless of the initial occupation ratio, whereas other methods depend upon the initial occupation ratio to determine what percentage of the unused spaces can be populated. In all those techniques, different cells, preferably FFs, are used to cover the empty space which limits the occupation of the empty spaces. With the proposed method, as the poly layer is fully occupied, no cell can be inserted without removing a portion of the poly. Moreover, the removal of even a small portion of the polysilicon layer to insert a Trojan can easily be detected both by the readout and the signature detection modules.

### 3.5 CONCLUSION

As the use of outside foundry becomes more popular, the threat of hardware security increases. As a preventative measure against any malicious insertion of Trojans, a new and easy-to-implement solution is presented in this paper. The proposed method uses minimum feature wires to cover unused spaces of the polysilicon layer of the die. As a result, attackers will not have access to the resources to implement and route the Trojan circuits, as no active layer can be accessed without removing a portion of the polysilicon wire, which will affect the characteristics of the polysilicon wires. The proposed method of this article prevents Trojan insertion by denying access to the active layer and at the same time detects any possible Trojan insertion in two separate methods: (a) using a DLL based readout circuit to measure the propagation delay contributed by the polysilicon layer (b) a signature detection block to verify the signature obtained by the polysilicon wires. Simulation results in cadence environment indicate that unused silicon spaces can be entirely covered to protect the main circuit against possible Trojan insertions. The simulation results also show that a minor removal of the polysilicon layer to insert even a single inverter can readily be detected by the on-chip readout circuit. The signature verification block also supports the results obtained by the readout circuit, by changing the signature for the same polysilicon wire removal. Both Monte Carlo and PVT variation simulations show a robust response. Even though CMOS 180nm technology is used in this work as a proof of concept, the same concept will also hold for more recent CMOS technologies. As the TDC resolution depends mainly upon the implemented time amplifier, not the technology.



## ACKNOWLEDGMENT

The authors would like to thank the research and financial support received from the Natural Sciences and Engineering Research Council (NSERC) of Canada and CMC Microsystems.

## REFERENCES

- [1] A. London, “Basic principles for managing foundry programs”, *Microelectronics Reliability*, vol. 45, no. 9-II, pp. 1285-1292, 2005.
- [2] R. Karri, J. Rajendran, K. Rosenfeld and M. Tehranipoor, “Trustworthy Hardware: Identifying and Classifying Hardware Trojans,” in *Computer*, vol. 43, no. 10, pp. 39-46, Oct. 2010.
- [3] J. Dofe, J. Frey and Q. Yu, “Hardware security assurance in emerging IoT applications,” *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, 2016, pp. 2050-2053.
- [4] L. A. Guimarães, R. P. Bastos, T. F. de Paiva Leite and L. Fesquet, “Simple tri-state logic Trojans able to upset properties of ring oscillators,” *2016 International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS)*, Istanbul, 2016, pp. 1-6.
- [5] L. Ni, J. Li, S. Lin and D. Xin, “A method of noise optimization for Hardware Trojans detection based on BP neural network,” *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, 2016, pp. 2800-2804.

- [6] Xiaoxiao Wang, M. Tehranipoor and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," *2008 IEEE International Work. on Hardware-Oriented Security and Trust*, Anaheim, CA, 2008, pp. 15-19.
- [7] R. S. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," *2009 IEEE International High Level Design Validation and Test Workshop*, San Francisco, CA, 2009, pp. 166-171.
- [8] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," in *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, Jan.-Feb. 2010.
- [9] T. F. Wu, K. Ganesan, Y. A. Hu, H. -. P. Wong, S. Wong and S. Mitra, "TPAD: Hardware Trojan Prevention and Detection for Trusted Integrated Circuits," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 4, pp. 521-534, April 2016.
- [10] S. Dupuis, M. Flottes, G. Di Natale and B. Rouzeyre, "Protection Against Hardware Trojans With Logic Testing: Proposed Solutions and Challenges Ahead," in *IEEE Design & Test*, vol. 35, no. 2, pp. 73-90, April 2018.
- [11] S. Dupuis, P. Ba, M. Flottes, G. Di Natale and B. Rouzeyre, "New testing procedure for finding insertion sites of stealthy Hardware Trojans," *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, 2015, pp. 776-781.
- [12] M. Flottes, S. Dupuis, P. Ba and B. Rouzeyre, "On the limitations of logic testing for detecting Hardware Trojans Horses," *2015 10th International Conference on*

*Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, Naples, 2015, pp. 1-5.

- [13] S. Narasimhan *et al.*, “Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis,” in *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2183-2195, Nov. 2013.
- [14] J. He, Y. Zhao, X. Guo and Y. Jin, “Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis,” in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 10, pp. 2939-2948, Oct. 2017.
- [15] X. Zhang and M. Tehranipoor, “RON: An on-chip ring oscillator network for hardware Trojan detection,” *2011 Design, Automation & Test in Europe*, Grenoble, 2011, pp. 1-6.
- [16] H. Salmani, M. Tehranipoor and J. Plusquellic, “A layout-aware approach for improving localized switching to detect hardware Trojans in integrated circuits,” *2010 IEEE International Workshop on Information Forensics and Security*, Seattle, WA, 2010, pp. 1-6.
- [17] E. Amini *et al.*, “IC security and quality improvement by protection of chip backside against hardware attacks,” *Microelectronics Reliability*, vol. 88, pp. 22-25, 2018.
- [18] C. Bao, D. Forte and A. Srivastava, “On Reverse Engineering-Based Hardware Trojan Detection,” in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 1, pp. 49-57, Jan. 2016.

- [19] M. Tehranipoor, H. Salmani and X. Zhang, "Hardware Trojan Detection: Untrusted Third-Party IP Cores," in *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*, Cham, Springer International Publishing, 2014, pp. 19-30.
- [20] M. M. Farag and M. A. Ewais, "Smart employment of circuit redundancy to effectively counter trojans (SECRET) in third-party IP cores," *2014 International Conference on ReConFigurable Computing and FPGAs (ReConFig14)*, Cancun, 2014, pp. 1-6.
- [21] A. Nahiyani, M. Sadi, R. Vittal, G. Contreras, D. Forte and M. Tehranipoor, "Hardware trojan detection through information flow security verification," *2017 IEEE International Test Conference (ITC)*, Fort Worth, TX, 2017, pp. 1-10.
- [22] C. Liu and C. Yang, "Exploiting heterogeneity in MPSoCs to prevent potential Trojan propagation across malicious IPs", *Proceedings of the 24th edition of the great lakes symposium on VLSI (GLSVLSI)*, May 2014, pp. 335-340.
- [23] M. Tehranipoor, H. Salmani and X. Zhang, "Hardware Trojan Detection: Untrusted Third-Party IP Cores," in *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*, Cham, Springer International Publishing, 2014, pp. 19-30.
- [24] M. K. Das, "Preventive Techniques for Hardware Trojans," Master Thesis, Masaryk University, Hyderabad, 2016.
- [25] Y. Xie, C. Bao and A. Srivastava, "3D/2.5 D IC-based obfuscation," in *Hardware Protection through Obfuscation*, Cham, Springer International Publishing, 2017, pp. 291-314.
- [26] M. Li, B. Yu, Y. Lin, X. Xu, W. Li and D. Z. Pan, "A Practical Split Manufacturing Framework for Trojan Prevention via Simultaneous Wire Lifting and Cell

- Insertion,” in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 9, pp. 1585-1598, Sept. 2019.
- [27] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, “Security Analysis of Integrated Circuit Camouflaging,” *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 709-720.
- [28] J. Rajendran, Y. Pino, O. Sinanoglu and R. Karri, “Security analysis of logic obfuscation,” *DAC Design Automation Conference 2012*, San Francisco, CA, 2012, pp. 83-89.
- [29] S. Dupuis, P. Ba, G. Di Natale, M. Flottes and B. Rouzeyre, “A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans,” *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, Platja d'Aro, Girona, 2014, pp. 49-54.
- [30] Q. Yu, J. Dofe and Z. Zhang, “Exploiting hardware obfuscation methods to prevent and detect hardware Trojans,” *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Boston, MA, 2017, pp. 819-822.
- [31] H. Salmani, M. Tehranipoor and J. Plusquellic, “A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time,” in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 1, pp. 112-125, Jan. 2012.
- [32] P. Ba, S. Dupuis, M. Palanichamy, M. Flottes, G. Di Natale and B. Rouzeyre, “Hardware Trust through Layout Filling: A Hardware Trojan Prevention Technique,” *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA, 2016, pp. 254-259.

- [33] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware Trojan insertion," *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Austin, TX, 2013, pp. 45-50.
- [34] P. Ba, M. Palanichamy, S. Dupuis, M. Flottes, G. Di Natale and B. Rouzeyre, "Hardware Trojan prevention using layout-level design approach," *2015 European Conference on Circuit Theory and Design (ECCTD)*, Trondheim, 2015, pp. 1-4.
- [35] T. M. Supon and R. Rashidzadeh, "A phase locking test solution for MEMS devices," *2017 22nd IEEE European Test Sympo. (ETS)*, Limassol, 2017, pp. 1-6.
- [36] "VLSI Concepts," VLSI Expert Group, 14 November 2014. [Online]. Available: <http://www.vlsi-expert.com/2014/11/>. [Accessed 03 November 2020].
- [37] V. K. Tripathi, "Equivalent Circuits and Characteristics of Inhomogeneous Nonsymmetrical Coupled-line Two-Port Circuits (Short Papers)," in *IEEE Trans. on Microwave Theory and Techniques*, vol. 25, no. 2, pp. 140-142, Feb. 1977.
- [38] E. Jedari, R. Rashidzadeh and M. Saif, "A PVT resilient short-time measurement solution for on-chip testing", in *Microelectronics Journal*, vol. 75, pp. 35-40, May 2018.
- [39] Y. Gong, F. Qian and L. Wang, "Design for Test and Hardware Security Utilizing Retention Loss of Memristors," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 11, pp. 2536-2547, Nov. 2019.
- [40] T. M. Supon, M. Seyedbarhagh, R. Rashidzadeh and R. Muscedere, "Hardware Trojan Prevention Through Limiting Access to the Active Region," *2019 14th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS)*, Mykonos, Greece, 2019, pp. 1-6.

---

## Chapter 4

---

# ON-CHIP MAGNETIC PROBES FOR HARDWARE TROJAN PREVENTION AND DETECTION

---

### 4.1 INTRODUCTION

With the shrinking transistor sizes near to the limits, 3D IC technologies have emerged as viable solutions to keep up with the demand to add more functionalities to a single chip. The costs of fabrication facilities for these new technologies left many companies with no choice other than outsourcing their IC fabrication needs. A 3D IC is usually fabricated by stacking different 2D layers together. The stacked dies are bonded using Through Silicon Vias (TSV). 3D ICs have some advantages over 2D chips, such as (a) a 3D IC can be fabricated using split manufacturing by distributing the routing of a single circuit across different dies, which masks the functionality of the circuit, (b) modified versions of conventional 2D IC security solutions can be added to different dies to enhance the security of each die [1]. It also conceals the details of the circuit design once the dies are stacked together, making reverse engineering challenging [2]. Moreover, the stacked structure of a 3D IC also makes it easier to obtain active layers from different foundries. The major concern with this approach is the possibility of insertion of malicious circuitry, called Hardware Trojan (HT), from untrusted facilities [3, 4]. HTs are

commonly inserted to alter the behavior of an IC, to access a crypto key or to deny the user the intended service [5]. HTs are also utilized to weaken the immunity of integrated circuits to inject false data using electromagnetic waves [6]. There is a direct correlation between the intensity of electromagnetic (EM) radiation and the information leakage. According to [7], it is possible to generate both the EM radiation map and the information leakage map of a cryptographic device simultaneously by scanning the device. Moreover, it is reported that the randomness of a ring oscillator (RO) based True Random Number Generator (TRNG) can be undermined by inducing sinusoidal electromagnetic waves [8]. Hardware Trojans are different in the sense that each of them is designed to serve a specific purpose, sometimes under certain predetermined conditions. As a result, each HT has unique physical characteristics with a specific functionality and activation mechanism [9]. This makes the detection of an HT very difficult. It is quite challenging to account for all possible hardware malicious modifications in any stage of IC fabrication or post-fabrication. The minute size of HTs also compounds to that challenge, as HTs usually occupy a small area of the main circuit [10]. The introduction of 3D IC reduces the vulnerability against reverse engineering attacks but introduces some new and more dangerous threats [2, 11]. The noise in 3D ICs is commonly higher compared to its conventional 2D counterparts, which can mask the effects of HT on the main circuit. Moreover, the limited access to the internal layers makes it even harder to detect HTs once the IC is fabricated. The solutions developed to ensure hardware security can be divided into two major groups of (a) HT detection and (b) HT prevention.



## ***A HT Detection***

In this technique, the design flow of the original circuit is not hampered, and the IC is tested for possible insertion of HT once the fabrication process is completed. Researchers have used different techniques, such as logic testing, side-channel analysis, and visual inspection to detect possible HT insertion.

In the logic testing methods [12-14], a set of predefined test stimuli is applied to the ICs under evaluation. The responses are then compared with the expected ones; any deviation from which indicates a trojan insertion. In this method, it is assumed that the HT changes the functionality of the IC and therefore it cannot protect circuits against information leaking or denial of service attacks.

The side-channel analysis-based methods monitor the variations of different physical characteristics such as power, temperature [15], and electromagnetic (EM) profiles [15-17], path delay measurement [18, 19], static distribution of the supply voltage [20] or relationship between dynamic current and maximum operating frequency [21, 22] to detect HT insertion. It is assumed that inserting a malicious circuit affects these parameters in such a way that the infected ICs can be detected. This method relies on comparison with a golden reference IC, which is proven difficult to obtain [1]. Most of the approaches using this technique [15-20] rely on invasive methods to obtain an HT-free golden IC, which is costly and time-consuming. Moreover, the introduction of nanoscale technologies threatens to make these detection methods obsolete by masking the effect of a small HT due to their poor signal-to-noise-ratio (SNR) [23].

Visual inspection [24, 25] is based on the idea of observing the top-level metal layer and comparing it with the original layout. However, non-destructive visual inspection methods cannot account for HTs designed on low metal layers.

Machine learning [26] and isolation-based hardware techniques [27, 28] have been utilized to detect HTs in IP cores used as building blocks for 3D ICs. The main objective of this work is to detect Trojans on 2D and 3D ICs and the detection of HTs in third party IP cores is beyond the scope of this paper. Most of the Trojan detection methods are designed to detect a specific type of HT or focus on a specific performance parameter variation and therefore a well-designed Trojan can remain undetected. Moreover, the effect of noise and Process, Voltage and Temperature (PVT) variations are usually ignored during the detection process, which can mask the effect of an HT.

## ***B HT prevention***

The limitations and complexities of HT detection methods have motivated IC designers to modify design flow to enable HT prevention. Design-for-Hardware-Trust (DfHT) techniques are being developed to facilitate HT prevention and support better detection at the same time. These methods are commonly used to detect HTs through differences between the characteristics of a Trojan free IC and an infected one. To that extent, researchers have developed solutions to obscure the functionality of ICs [29-34], as the creation of an HT demands a good understanding of the original circuit functionality. The authors of [29] introduced netlist-level obfuscation, where the gate-level netlist of a pre-synthesized IP core is modified and then resynthesized to obtain maximum functional and structural obfuscation at low design overhead. In [30, 31], different methods of state-obfuscation are presented, where the states of different

components of the circuit are obfuscated using security keys. An interesting idea is presented in [32] using dummy contact-based IC camouflaging techniques, where the functionality of a circuit is masked using dummy contacts. As a result, the same layout of a cell can represent different gates depending on where dummy contacts are placed. A DfHT technique is presented in [33] using new design techniques and new memory technologies to detect a wide variety of HTs during both IC testing in-field operation. At the same time, this technique can also prevent a wide variety of attacks during synthesis, place-and-route, and fabrication of ICs. The idea presented in [34] uses gates of different doping concentrations to vary their threshold voltages and thus create threshold dependent camouflaged cells. Attackers can use various approaches to determine the identities of camouflaged gates, such as: measuring the etch rate to find the heavily doped transistors and profiling the difference in power and delay characteristics of camouflaged gates to determine their identities [34].

Another idea is to create the design as dense as possible by “layout filling” technique to prevent an attacker from exploiting the available spaces, after the place and route [35-39]. As this method deprives the attacker of the space required for inserting malicious circuitry, it has the potential to be used as an effective method for HT prevention. This technique can also be used in 3D IC design. The proposed methods using this technique are discussed in detail in the next section. The existing literature regarding the hardware security of 3D IC is also discussed in the same section.

In this work, a new method is presented to prevent HT insertion by depriving malicious parties of routing resources. In the proposed solution, after the main circuit implementation, the unused metal and polysilicon layers are fully utilized to design on-

chip magnetic probes. As a result, there is no room left for the routing of the Trojan circuitries. Moreover, on-chip probes are used to get the magnetic signature of the chip to detect performance variations caused by possible HT insertion.

The rest of the paper is organized as follows: Section II discusses the background studies and the related works in 3D IC. Section III elaborates on the proposed Hardware Trojan prevention method in detail, which is then supported by simulation results in Section IV. Lastly, Section V includes the concluding remarks.

## **4.2 BACKGROUND STUDY**

An efficient method of HT prevention is to make the final design of the IC as dense as possible. To that extent, researchers have proposed different techniques to fill the unused silicon once the original circuit is designed. The authors of [35] have used filler cells to improve the density uniformity of the circuit. The idea is to fill the unused silicon area using different arbitrary cells after the original circuit is designed. The main drawback of this method is that these cells create an opportunity for the insertion of malicious circuits. Moreover, it is difficult to identify whether any malicious circuit is inserted due to the high circuit density. To negate that possibility, a technique called Built-In Self-Authentication (BISA) is proposed in [36], where the unused spaces are filled using a separate network of combinational cells. This network can be tested to identify potential alterations and Trojan insertions into the original circuitry. A separate Built-In Self-Test (BIST) circuit is designed using Linear Feed Back Shift Registers (LFSRs) and Multiple-Input Shift-Registers (MISRs) and placed in the unused spaces to test the network. This is an effective method for smaller ICs; but loses its effectiveness, as the size of the IC

grows bigger. In addition, it cannot completely occupy unused spaces. A similar method is proposed in [37], but the unused silicon layer is prioritized to improve the layout filling efficiency. In typical circuits, some nodes are more vulnerable to be used as the trigger for an HT. These locations, termed as “critical empty spaces” in [37], are identified using an algorithm and filled first. The researchers used shift registers instead of a Test Pattern Generator (TPG) and a MISR to test the functions generated by filler cells placed in the unused spaces to reduce the area overhead. The main drawback of this method is its dependency on the unused space left after the design of the original circuit. For a medium-sized IC, if the unused space is less than 20%, this method is not effective. Moreover, it does not work well for complex circuits. In [38], the authors proposed an enhanced algorithm to derive the highest number of combinatorial functions using the number of flip-flops (FFs) that can be inserted. They also introduced some logical gates to the dense designs where FFs cannot be inserted. The final occupation ratio is reported to be higher than 90%. One of the main concerns with this technique is a counterfeit filler circuit. If the original filler circuit is replaced by a smaller design with the same output, the saved space can be used to insert HT cells. Also, if the area of the main circuit covers 85% of a medium-size ASIC, the remaining empty spaces are not large enough to accommodate the components required to implement this method. A different approach of layout filling is proposed in [39], where the researchers focused on the unused polysilicon layer instead of the silicon layer. In this method, the unused polysilicon layer is filled using the minimum feature wires. The wires are connected to a readout circuit to measure the delay created by that wire. Here, it is assumed that any HT needs to be placed in the active layer. As an active layer is placed in the silicon layer and connects to

the polysilicon placed on top of that layer directly, any HT is bound to connect to some of those polysilicon wires as they cover the unused polysilicon layer. This will change the delay caused by the wire; removal of a portion of the polysilicon will also do the same. The approach thus can easily detect the insertion of any new gate.

The introduction of 3D ICs has provided attackers with various new methods to insert HTs in ICs [2, 11]. As multiple dies from different foundries are incorporated into a single 3D IC, some of them can be from untrusted foundries. Researchers have proposed some ideas to take advantage of the split manufacturing method [40-43] to increase security of 3D ICs. In this method, some of the layers are obfuscated and fabricated by trusted foundries, whereas the other layers are fabricated in untrusted foundries. Even though this method can eliminate most of the threats of HT insertion, it still suffers from HT insertion opportunities unique to 3D manufacturing. The integration of multiple layers of dies requires other intermediate levels like die stacking and TSV bonding, during which stages a HT can be inserted. Some additional malicious circuits or dies can be implemented, or TSVs can be exploited during these intermediate steps. 3D ICs also suffer from thermal issues, which can form high temperature in the middle layers as an inherent characteristic of the design type. This can result in a larger delay violation in those layers, which can be manipulated as a trigger for the Trojan [44].

### **4.3 ANALYTICAL DESCRIPTION OF THE PROPOSED METHOD**

In the proposed method, after routing of the main circuit, the unused metal and polysilicon layers are filled using minimum feature wires. There are various ways to place those wires: it can be filled arbitrarily, or the metals can be designed as inductive

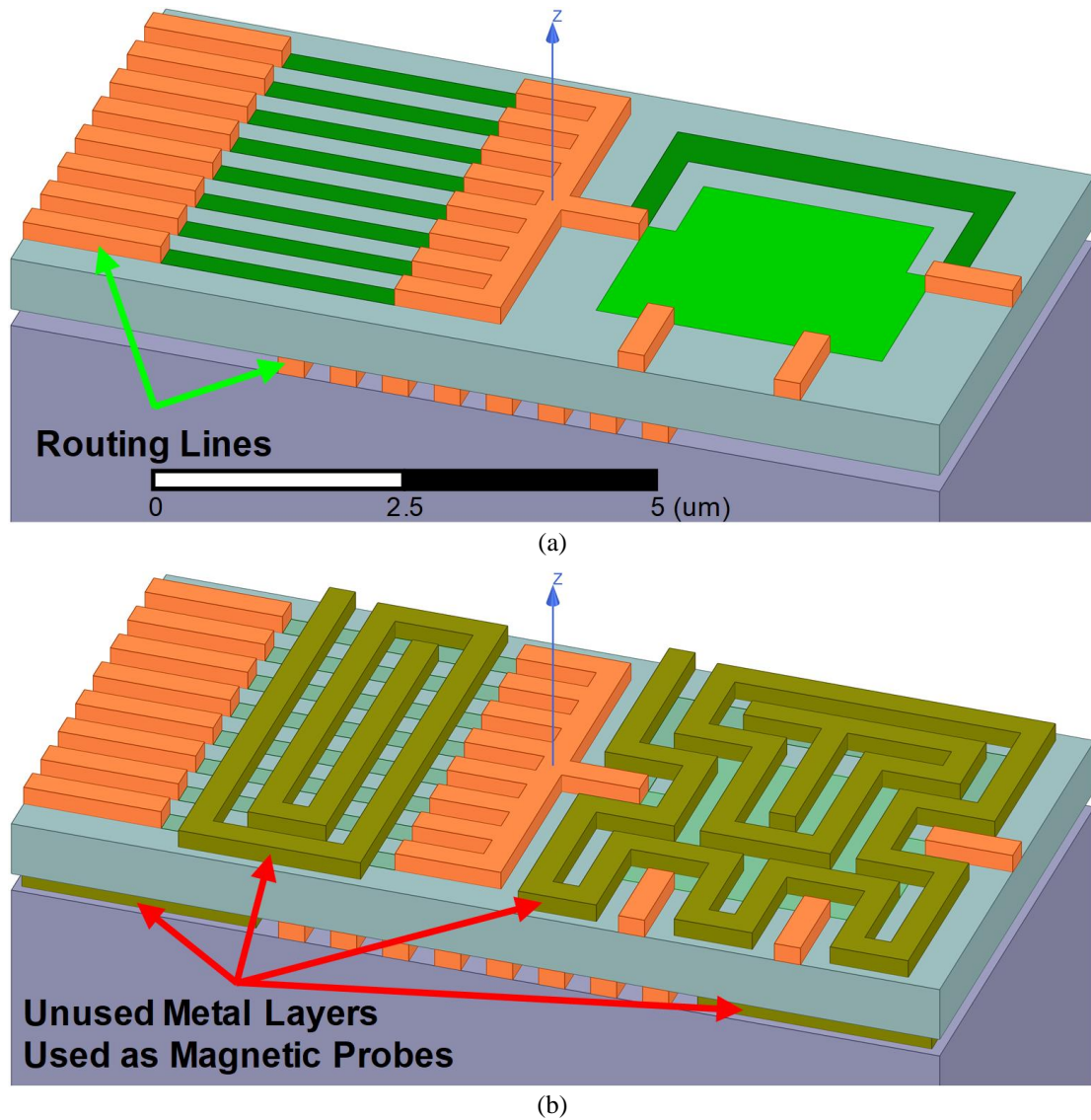


Figure 4.1. (a) Routing of a typical Digital to Analog circuit in HFSS environment, (b) Unused layers used as magnetic probes.

sensors. Designing inductive sensors has some distinct advantages compared to a random distribution. Inductive sensors can be used as internal magnetic probes to capture the induced signature of the chip when a certain portion of the main circuit is activated. At the end of this process, there will be no resources left to connect Trojan circuits. If an attacker tries to redesign the magnetic probes or change the main circuit placement to access the resources to insert and rout a Trojan, it will change the signature of the IC. Moreover, the probes are tested separately to determine any change in their properties.

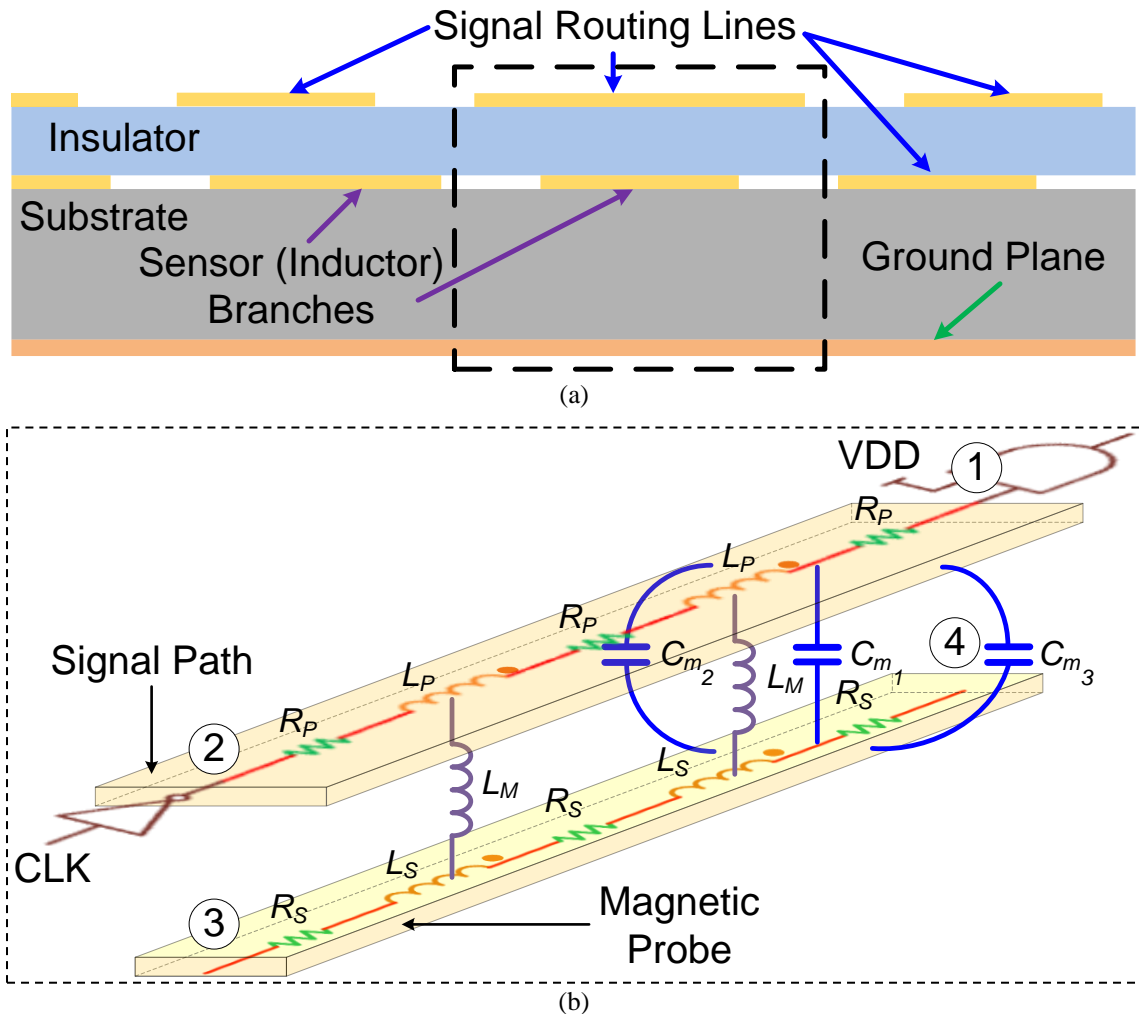
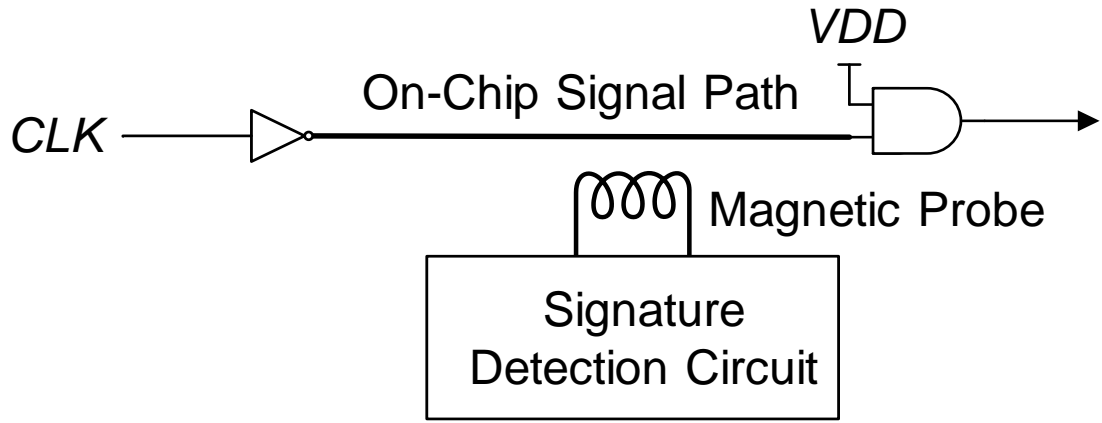


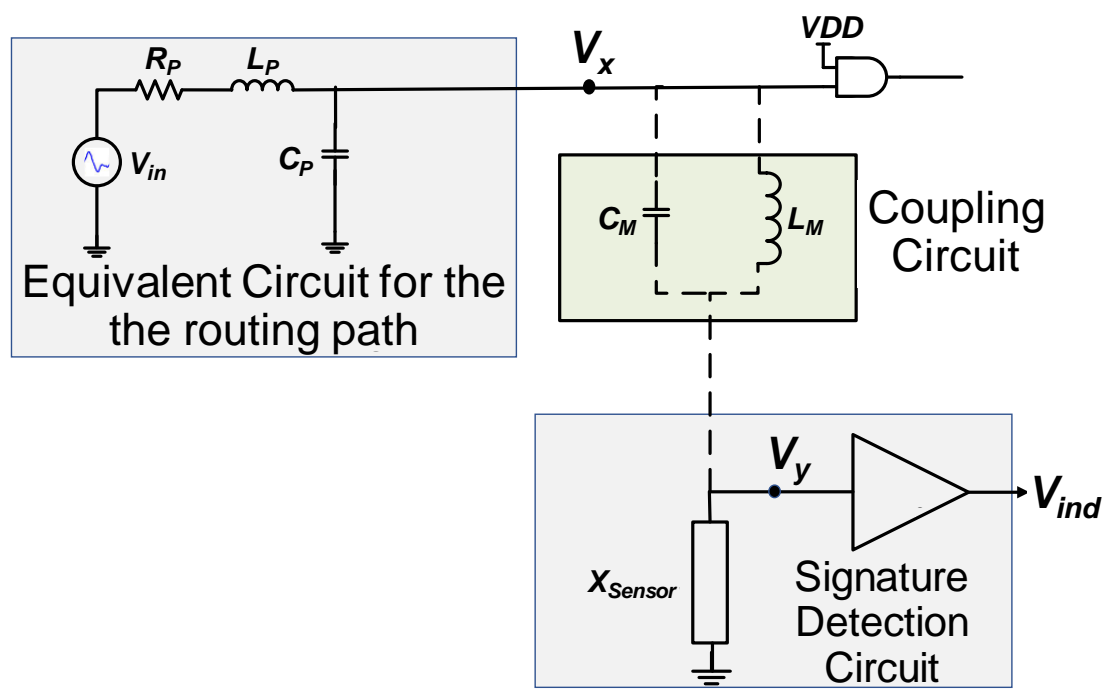
Figure 4.2. (a) A typical distribution of a signal routing path and a magnetic probe, (b) 3D illustration of a signal trace and a probe branch pair.

A sample structure of an inductive sensor in a circuit is shown in Fig. 4.1, where the unused spaces of a two-layer device are filled with traces of minimum width metal and polysilicon. The filler routing lines will induce voltage to the magnetic probe following the principle of coupled transmission lines. The response can be characterized by their resistances ( $R_P$ ,  $R_S$ ) and self and mutual inductances ( $L_P$ ,  $L_S$ ,  $L_M$ ) and capacitances ( $C_P$ ,  $C_S$ ,  $C_M$ ) per unit length, where subscripts P, S, and M represent Signal-Path, Sensor and Mutual respectively. In a typical circuit, a probe branch is surrounded by different routing lines as shown in Fig. 4.2 (a). Each probe branch and routing line pair forms a model





(a)



(b)

Figure 4.3. (a) Block diagram of the signal trace and a probe branch pair shown in Fig. 4.2. (b) The equivalent schematic diagram of Fig. 4.3 (a) indicating the routing path of the inverter and the coupling circuit together with the signature detection circuit.

equivalent to the coupled transmission line, which is shown in Fig. 4.2 (b). The parasitic capacitances to the ground plane are not shown in the figure for simplicity.

### A Circuit Model for a Magnetic Probe

Fig. 4.3 (a) shows the equivalent model for the case shown in Fig. 4.2 (b). The equivalent lumped circuit model is shown in Fig. 4.3 (b), in which the signal picked up

by the magnetic probe is amplified.  $V_{in}$  represents the equivalent input signal and  $R_P$ ,  $C_P$  and  $L_P$  are the resistance, capacitance, and inductance of the equivalent circuit. The voltage  $V_x$  can be calculated from:

$$V_x = V_{in} \frac{X_{C_P}}{X_{C_P} + R_P + X_{L_P}} \quad (1)$$

where  $X_{C_P}$  and  $R_P$  are the lumped parameters of the equivalent circuit. The impedance of the equivalent circuit,  $X_{eq}$ , the sensor,  $X_{Sensor}$ , and the coupling circuit,  $X_{Coupling}$ , can be calculated from:

$$X_{eq} = (R_P + X_{L_P}) \parallel X_{C_P} \quad (2)$$

$$X_{Sensor} = (R_S + X_{L_S}) \parallel X_{C_S} \quad (3)$$

$$X_{Coupling} = X_{L_M} \parallel X_{C_M} \quad (4)$$

The probe induced voltage,  $V_y$ , can then be readily found from:

$$V_y = V_x \left( \frac{X_{Sensor}}{X_{Sensor} + X_{Coupling} + X_{eq}} \right) \quad (5)$$

Here,  $V_y$  is the voltage induced at terminal 3 of Fig. 4.2 (b) due to a signal between the terminals 1 and 2. As the total system has multiple “trace – probe branch” combinations, the total induced voltage from  $m$  branches can be found by:

$$V_{Ind} = \sum_{i=1}^m V_{y_i} = \sum_{i=1}^m \frac{V_{x_i}(X_{i_{Sensor}})}{X_{i_{Sensor}} + X_{i_{Coupling}} + X_{i_{eq}}} \quad (6)$$

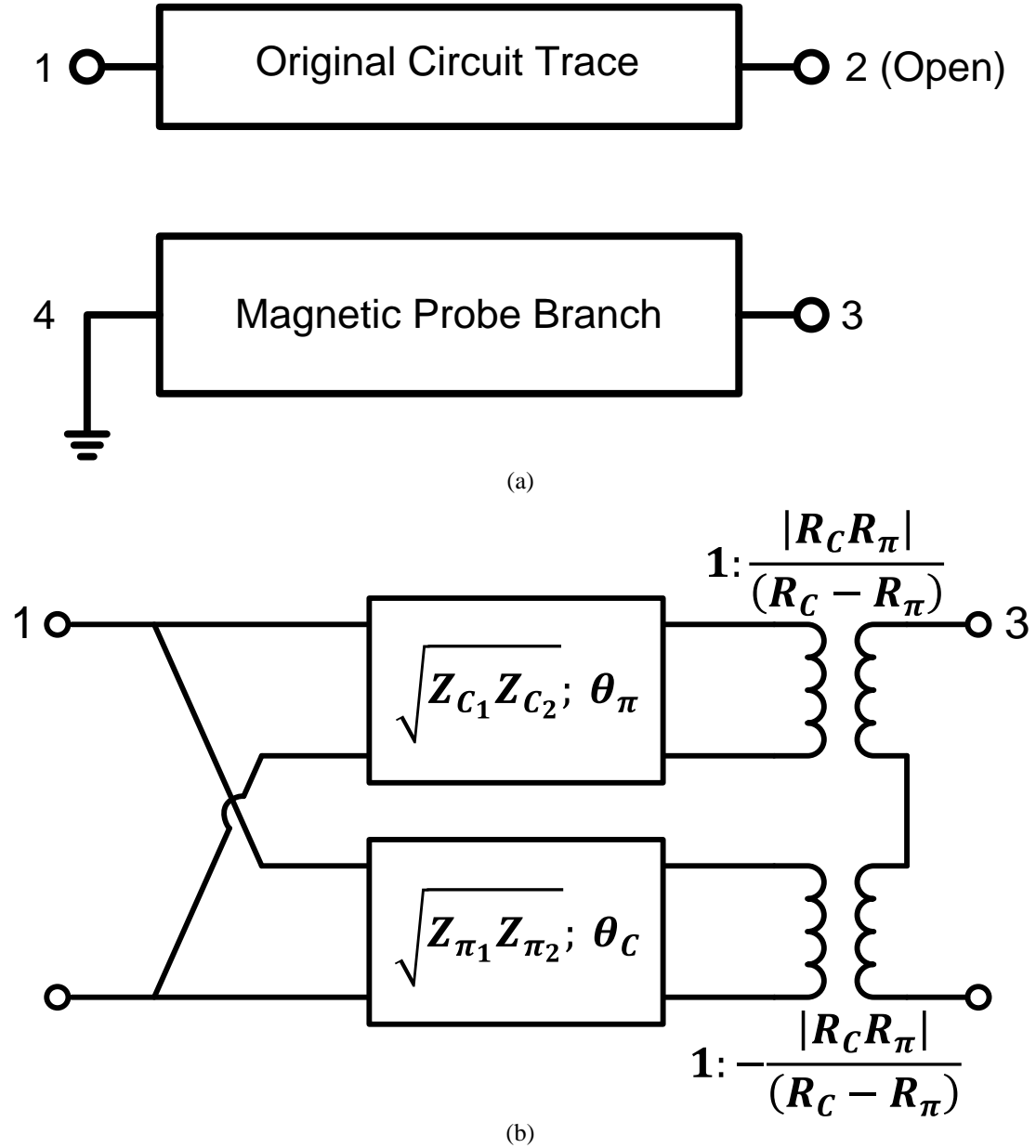


Figure 4.4. (a) Equivalent two-port network created by a signal trace and probe branch pair in high frequency (b) Equivalent model of such a pair.

The lumped model can be used to approximate the circuit response at low frequencies. At high frequencies, for response analysis, the circuit can be represented by a two-port network as shown in Fig. 4.4 (a). The equivalent high-frequency circuit model is shown in Fig. 4.4 (b). The induced voltage at terminal 3 of Fig. 4.2 (b) becomes:

$$V_3 = Z_{31}I_1 + Z_{32}I_2 + Z_{33}I_3 \quad (7)$$

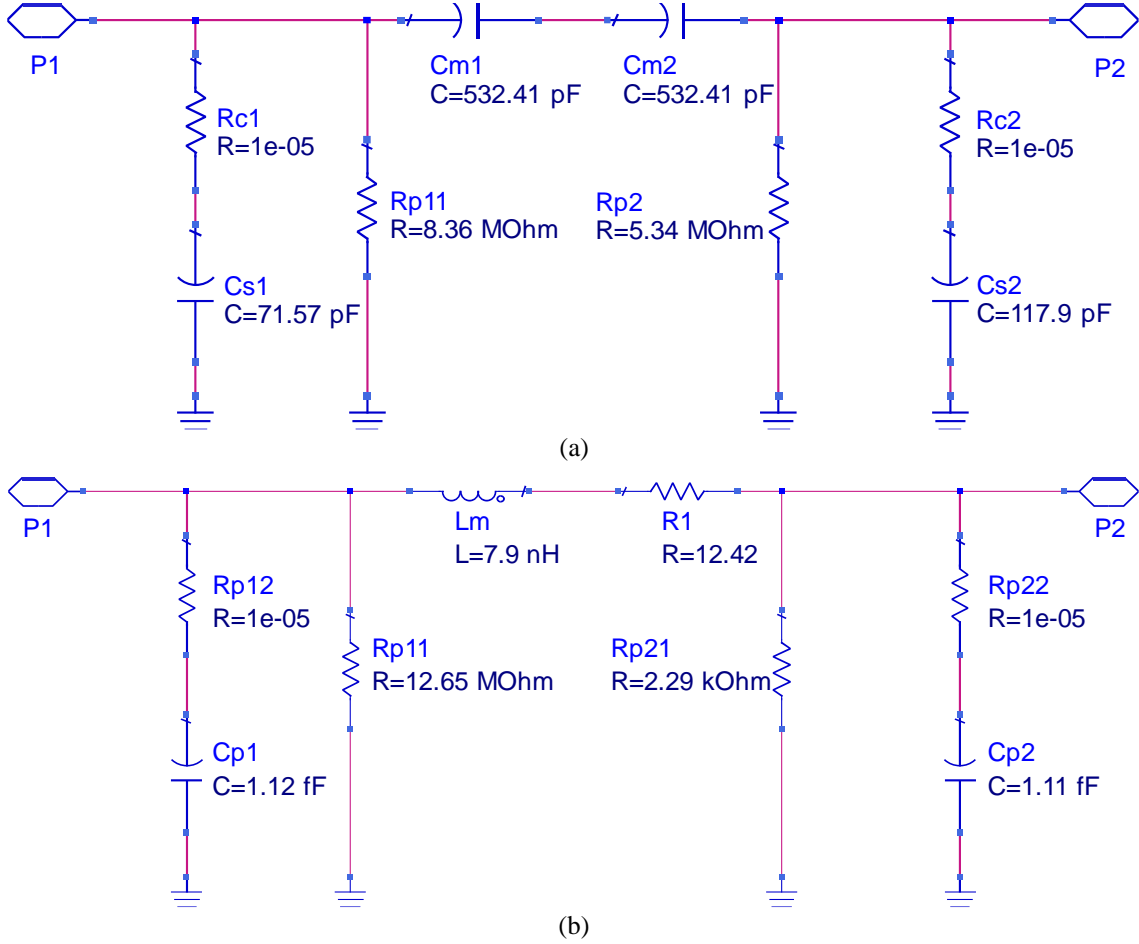


Figure 4.5. Extracted model of the two-port network shown in Fig. 4.4 (a) at 500 MHz, where trace current plays: (a) a negligible and (b) a dominant role in the induction of the probe.

where,

$$Z_{31} = \frac{R_c Z_{c_1}}{(1 - R_c/R_\pi) \sinh \gamma_c l} + \frac{R_\pi Z_{\pi_1}}{(1 - R_\pi/R_c) \sinh \gamma_\pi l} \quad (8)$$

$$Z_{32} = \frac{R_c^2 Z_{c_1}}{(1 - R_c/R_\pi) \sinh \gamma_c l} + \frac{R_\pi^2 Z_{\pi_1}}{(1 - R_\pi/R_c) \sinh \gamma_\pi l} \quad (9)$$

$$Z_{33} = \frac{R_c^2 Z_{c_1} \coth \gamma_c l}{(1 - R_c/R_\pi)} + \frac{R_\pi^2 Z_{\pi_1} \coth \gamma_\pi l}{(1 - R_\pi/R_c)} \quad (10)$$

A detailed mathematical analysis along with the explanations of the parameters used in equations (7 – 10) can be found in [45]. The equivalent extracted spice model, shown

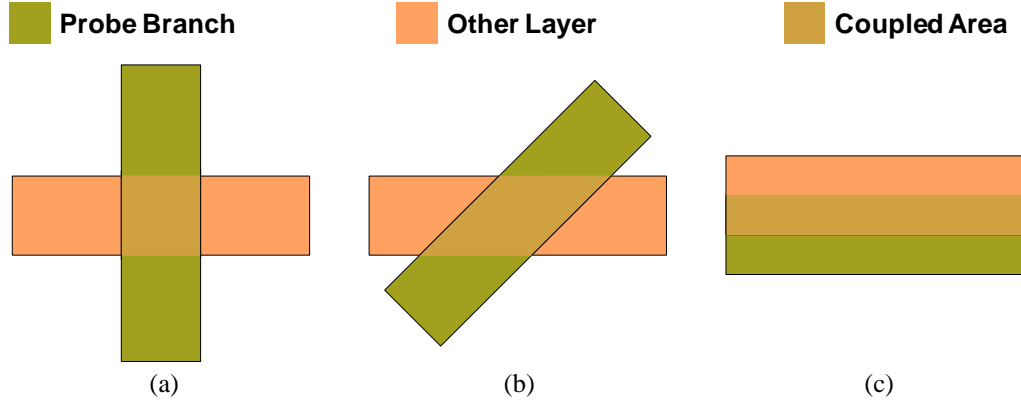


Figure 4.6. Types of structures created during an EM coupling with any metal trace or another probe branch in another layer: probe branch crossing the other layer (a) vertically, (b) at an angle, and (c) probe branch run along the other layer.

in Fig. 4.5, displays the induction process for different circuit compositions. When the signal routing path is driven by a source with a negligible current, the electric coupling becomes the dominant factor and the signal is induced on the probe through the capacitors. Whereas when a considerable current flow through the signal routing path, the magnetic field becomes the dominant coupling mechanism and the sensor probe is fed through the series resistor – inductor combination. The extracted model was obtained at 500 MHz clock frequency; the extract parameters are frequency dependent.

### ***B Effect of the Geometric Structure on the EM Signature***

A branch of the probe can form three types of structures while creating an EM coupling with any metal trace or another probe branch in another layer. The probe branch can simply cross the other layer at an angle, which are shown in Fig. 4.6 (a) and (b), or it can run along the other layer, as shown in Fig. 4.6 (c). In any case, both electric and magnetic fields will contribute towards the signature, but depending on the structure, the mutual inductance ( $X_{LM}$ ) and capacitance ( $X_{CM}$ ) will change. This will result in a change to coupling impedance ( $X_{Coupling}$ ) of equation (4), and hence the induced voltage ( $V_{ind}$ ) of equation (6).

### *C Circuit Model for a Magnetic Probe*

To make sure that a circuit modification by adversaries can be detected, the variation of the signature must be higher than the noise level, preferably by 10 dB for reliable detection. The noise power,  $P_n$ , in a circuit [46] can be represented by:

$$P_n = 4k_B T \Delta f \quad (11)$$

where  $k_B$  is the Boltzmann constant,  $T$  is the absolute temperature, and  $\Delta f$  is the equivalent noise bandwidth. Accounting for the noise in the circuit, the induced voltage on the magnetic probe from equation (6) is modified to:

$$\sum_{i=1}^m V_{y_i} - V_n \leq V_{Ind} \leq \sum_{i=1}^m V_{y_i} + V_n \quad (12)$$

where,  $V_n$  is the noise RMS voltage of resistance  $R$ , given by:

$$V_n = \sqrt{4k_B TR \Delta f} \quad (13)$$

As can be seen from equation (12), the induced voltage varies between the minimum and maximum values. This is due to the random nature of noise which can be added or subtracted from the induced voltage. To reliably detect the induced voltage in the presence of noise, a Signal-to-Noise Ratio (SNR) of a minimum of 10 dB is required. For a probe made of a metal layer with 1 GHz bandwidth and an aspect ratio of 100 in CMOS 180 nm technology that has a typical sheet resistance of  $0.08 \Omega/\mu\text{m}^2$ , the RMS noise voltage,  $V_n$  is equal to  $1.15 \mu\text{V}$ . Such a probe can detect a circuit modification resulting in more than  $11.5\mu\text{V}$ .

The die stacking in a 3D IC introduces additional thermal noise due to the lack of possibility of heat dissipation in the internal layers. The total noise can be found by adding this noise with the root of the sum of squares of the noise of the different dies of that IC. For a 3D IC of  $i$  layers, the total noise is:

$$V_{n_{eq}} = V_{n_{internal}} + \sqrt{V_{n_1}^2 + V_{n_2}^2 + \dots + V_{n_i}^2} \quad (14)$$

#### 4.4 SIMULATION RESULTS

To validate the proposed method, the routing of a simple DAC (Digital to Analog Converter) was designed in the HFSS environment, as shown in Fig. 4.1 (a). Tempering with the routing of the DAC affects the EM signature which can be detected by the detection circuitry. The unused metal and polysilicon layers between the routing lines were filled using magnetic probes of different shapes, which is shown in Fig. 4.1 (b). Any change in the structure of the probe will also affect the EM signature and will be readily detected. The extracted Spice model of the routing was later exported to the Advanced Design System (ADS) environment, where the orange colored traces act as the routing lines and the citron colored ones as the probe. Minimum feature traces are preferred to prevent the insertion of malicious circuitry by playing with the width of the traces.

The magnetic and electric fields' distributions of the routing lines and probes of Fig. 4.1 (b) are shown in Fig. 4.7. The routing lines were excited by a voltage source of one-volt amplitude with a source impedance of 50 ohms. As shown in Fig. 4.7, the main portion of both magnetic and electric fields find their way into the designed probes. The maximum magnetic field intensity is about 0.24 A/ $\mu\text{m}$  while most of the fields vary

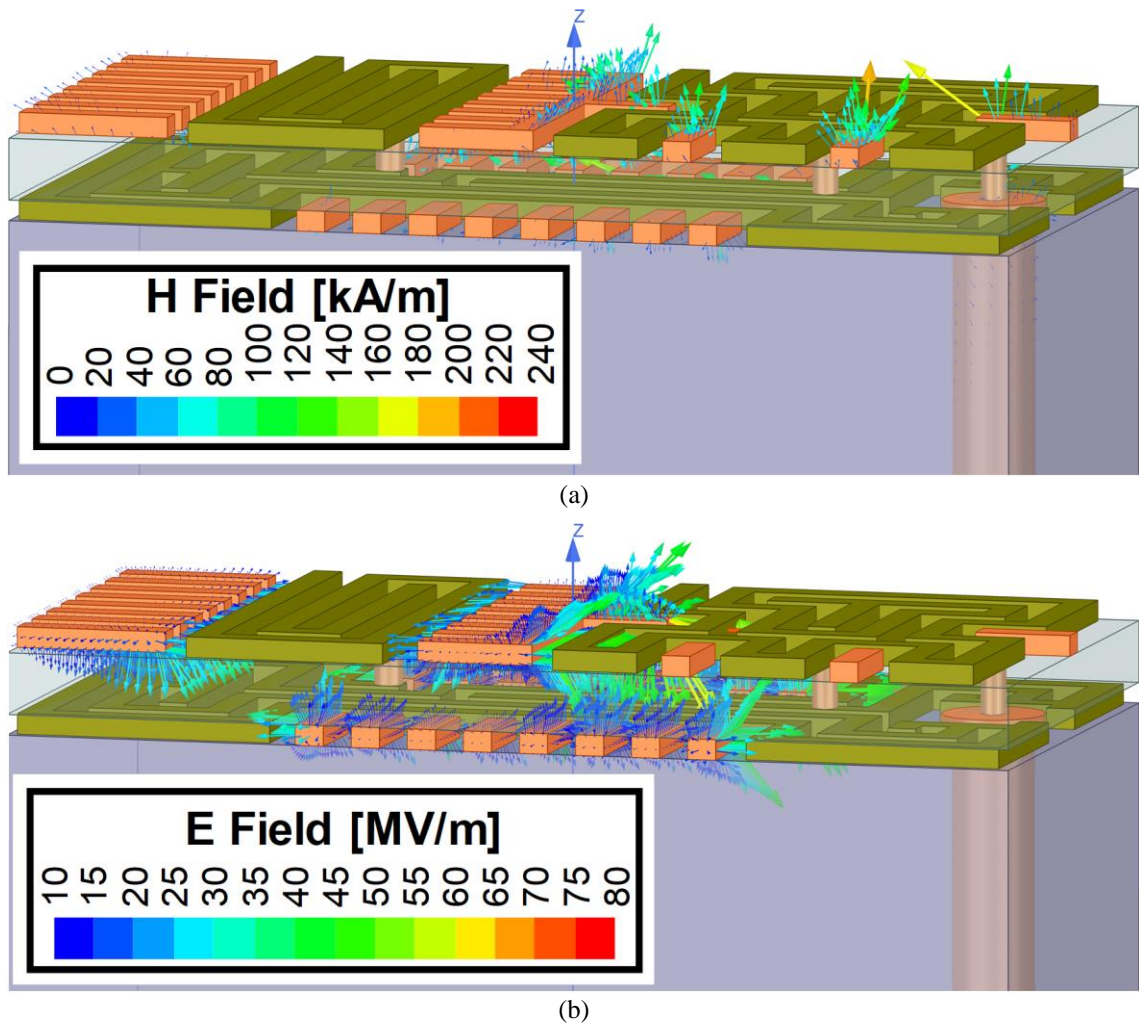


Figure 4.7. (a) Magnetic flux density and (b) Electric field distribution of the design shown in Fig. 4.1 (b).

between 0.08 and 0.16 A/ $\mu\text{m}$ . The maximum electric field exceeds 80 V/ $\mu\text{m}$ , but most of the field lines stay within 20 to 65 V/ $\mu\text{m}$ . Such electric and magnetic fields can readily be detected by an on-chip probe to get the signature of the device.

The spice models of both the original and manipulated magnetic probe structures along with the routing lines were extracted to ADS from the designs created in HFSS, which are shown in Fig. 4.8 (a) and (b). The extracted lumped models are shown in Fig. 4.9, from where it is evident that both the original and the manipulated design have similar extracted circuit model, with a slight change in the parameters. The models are



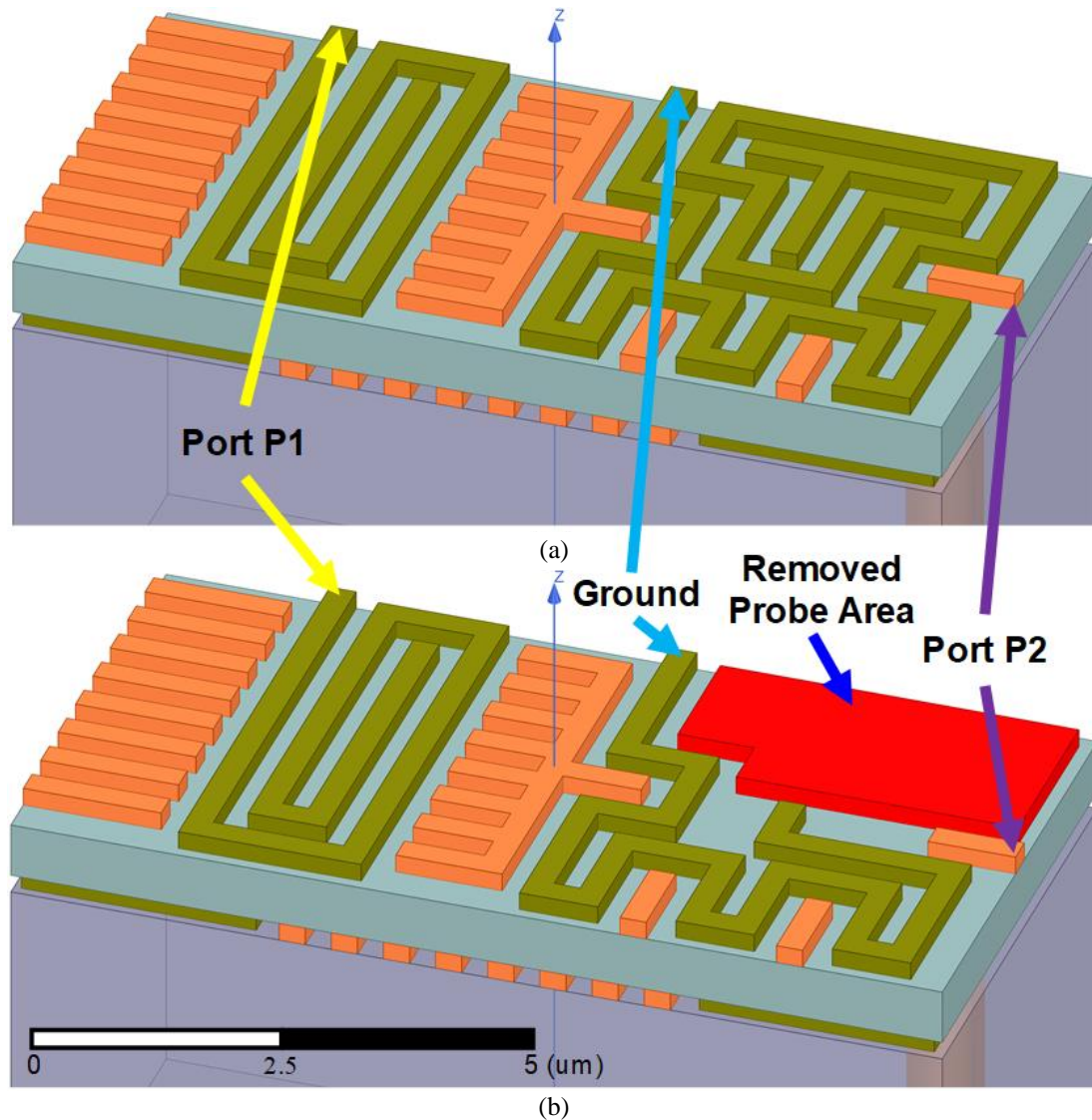


Figure 4.8. Circuit with the design of the magnetic probe: (a) Original design, and (b) manipulated design with a portion of the probe removed.

then exported to the ADS environment to identify the effect of manipulation. Initially, the simulations were performed using the model of the original design of the probe. An input was applied to the circuit to capture the signature. The magnetic fields created by the routing wires are picked up by the probe. The output of the probe is then fed to the inverted input of an OPAMP with the following specification:

Single Supply: 1 V

Power: 10 mW

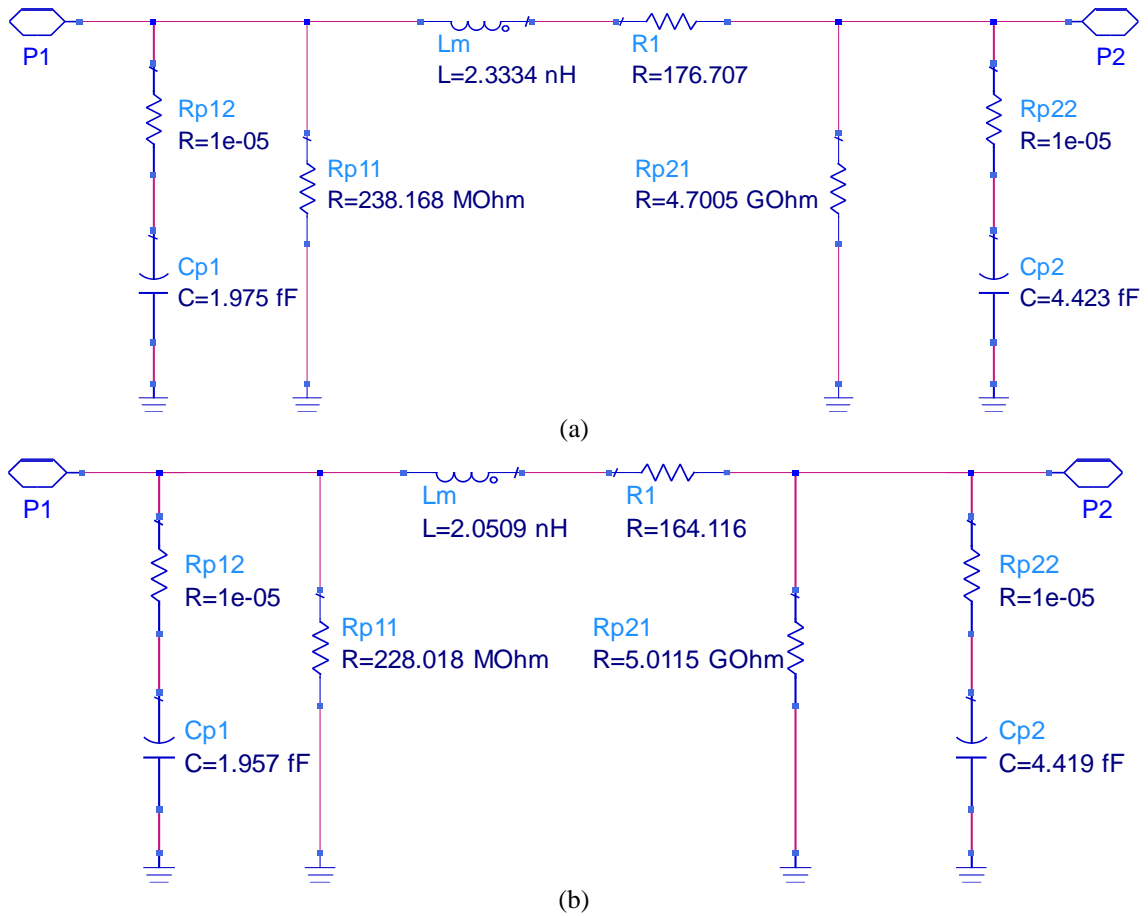


Figure 4.9. Lumped models of the coupling between the routing traces and (a) the original magnetic probe, and (b) the manipulated magnetic probe.

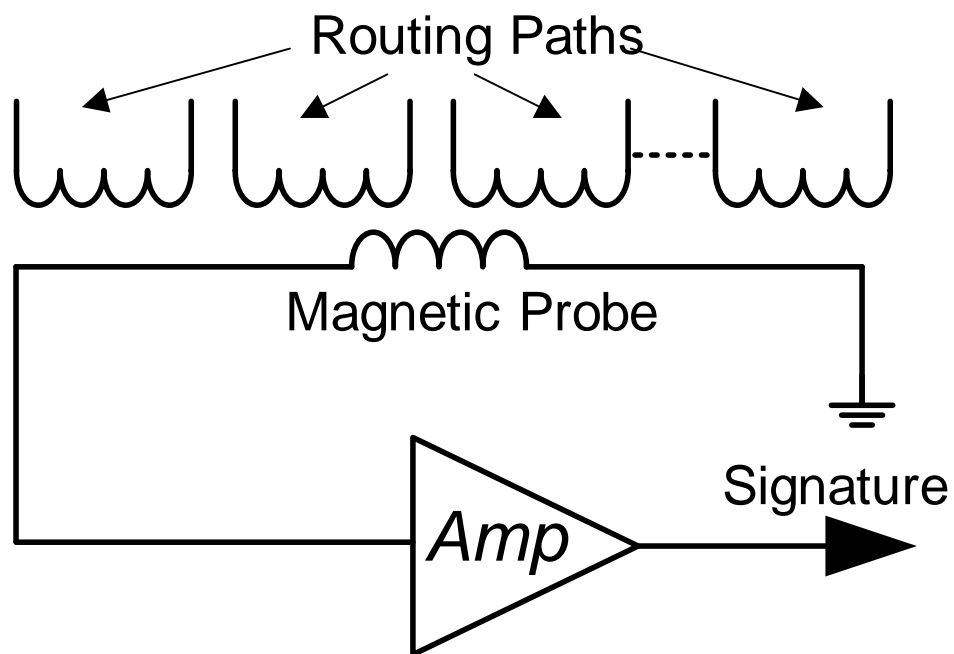


Figure 4.10. Equivalent circuit model of the magnetic probe.

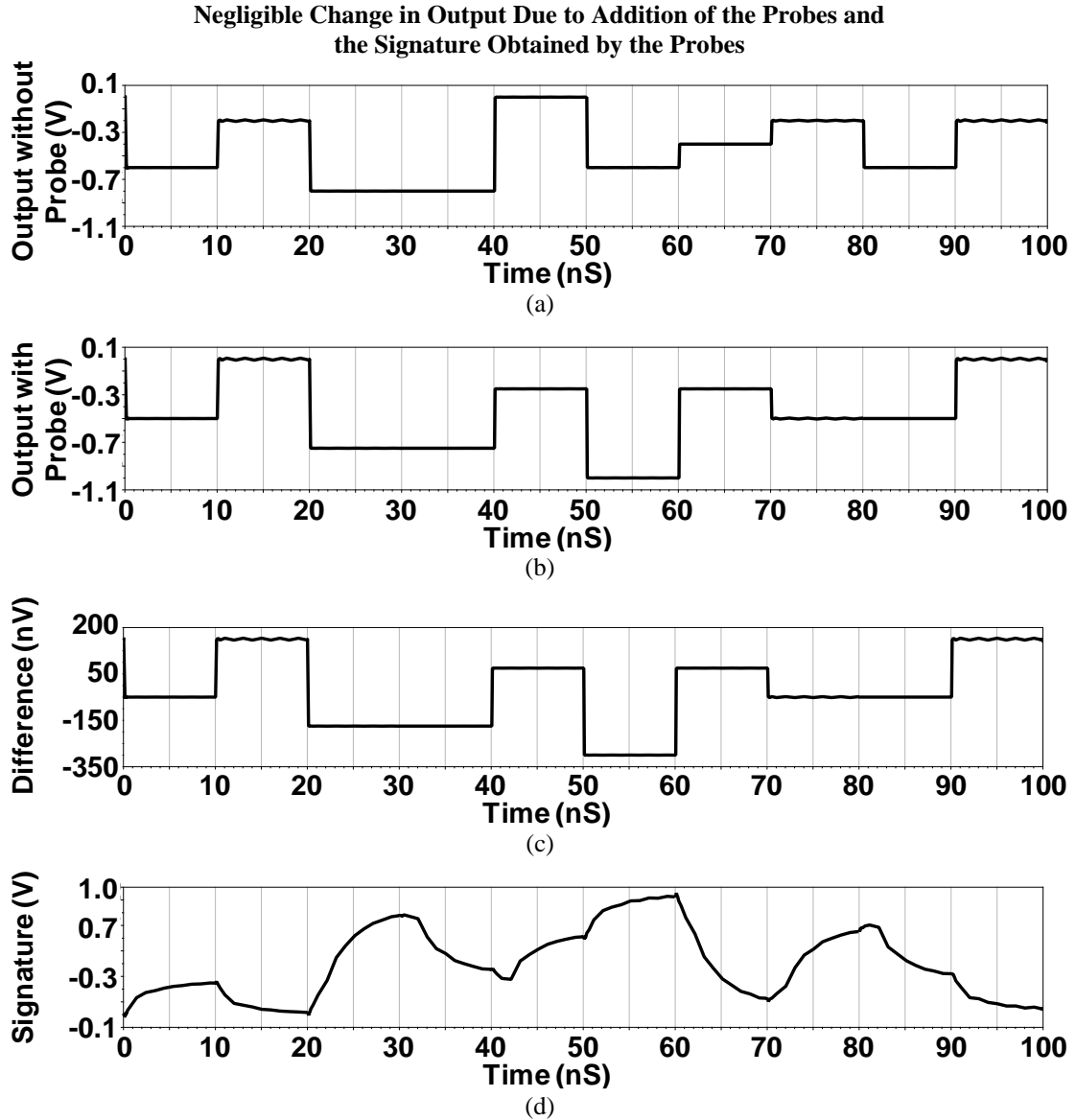


Figure 4.11. Output voltage (a) without probe (b) with probe; (c) difference between a and b; and (d) The unique signature.

Gain: 60 dB at 100MHz

Noise Figure: 1.2 dB at 100 MHz

As different routing lines are at different voltage levels, the fields captured by the probe are also different at different locations. The induced signature varies depending on the placement and orientation of the probe. To observe this effect, one terminal of the magnetic probe from the extracted model was grounded while the other was connected to

the amplifier, as shown in Fig. 4.10. After the probes and routing lines designed in HFSS are exported to ADS, transient simulation of the complete DAC circuit is performed for both designs without probe and with probe. The effect of adding the probe to the original design is shown in Fig. 4.11 along with the obtained signature. Fig. 4.11 (a) shows the digital output of the original circuit without the probe, whereas Fig. 4.11 (b) shows the same output with the probe added to the circuit. The difference between the first and second waveforms is shown in Fig 4.11 (c), with a maximum error range of 550 nV, while the shape of the digital output remains unchanged. This indicates that the effect of the insertion of the magnetic probes on the performance of the circuit is very negligible. The unique signature obtained from the circuit is shown in Fig. 4.11 (d). Even though it is obtained by using a random input to the main circuit, the signature is reproducible as the same signature will be generated for that exact input. This signature will change if either the placement of the probe is altered, or a portion of it is removed. To verify this statement, a portion of the probe design with an area of  $12 \mu\text{m}^2$ , shown in Fig. 4.8 (b), was removed. The effect of the manipulation is observed in ADS environment by passing the same input signal through the DAC using the extracted spice model of both the original and the manipulated design. The results are shown in Fig. 4.12, where Fig. 4.12 (a) indicates the signature of the original circuit and 4.12 (b) shows the signature of the manipulated design. The difference between the two waveforms is shown in Fig. 4.12 (c), which varies within the range of  $\pm 0.6 \text{ V}$ . The change in the voltage level is much higher than the noise voltage, which ensures a proper detection of any malicious activity. This manipulation also displays a detectable change in the S-Parameters of the probe, which

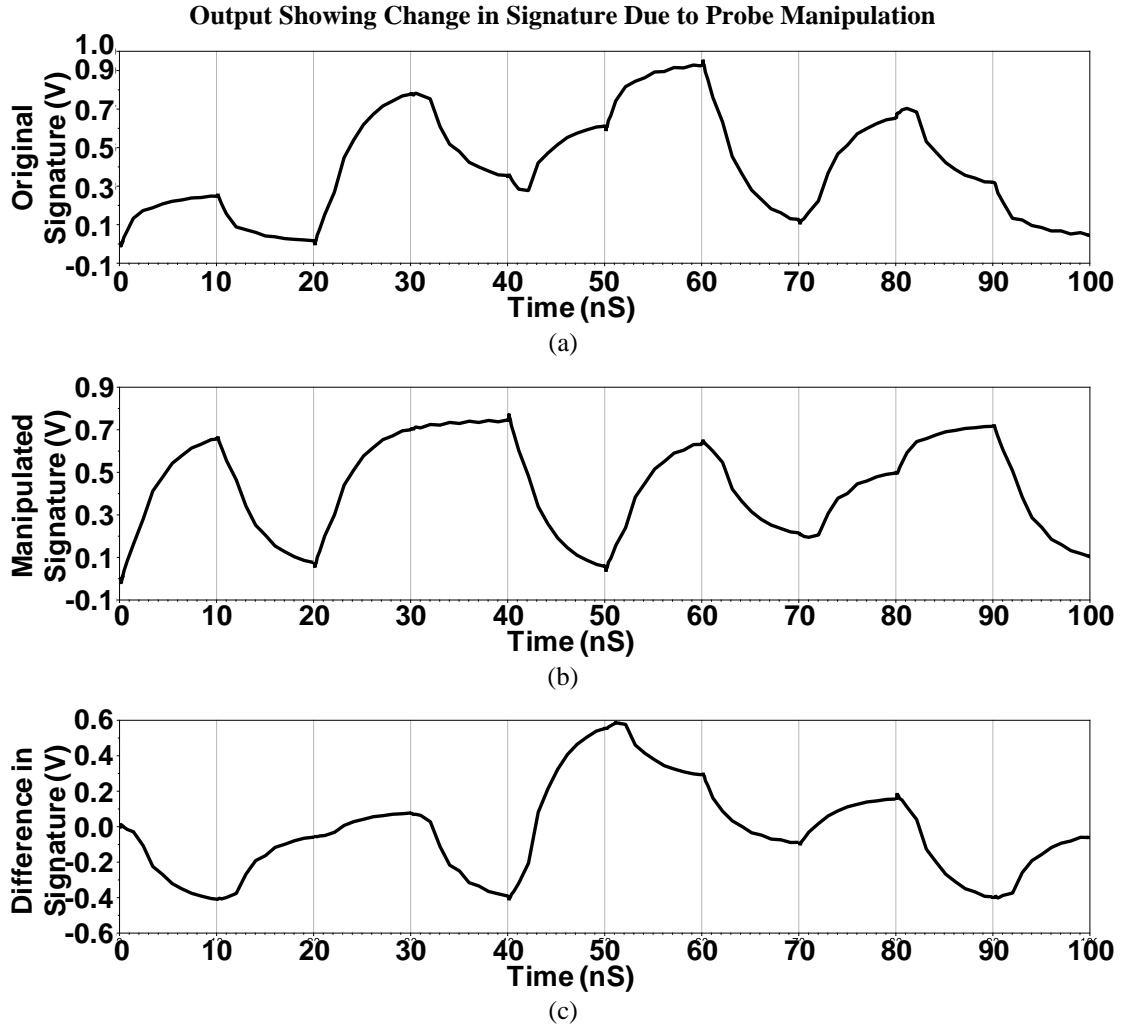


Figure 4.12. Graph showing the signature of the (a) Original design and (b) Manipulated design of Fig. 4.8. (c) Difference between (a) and (b).

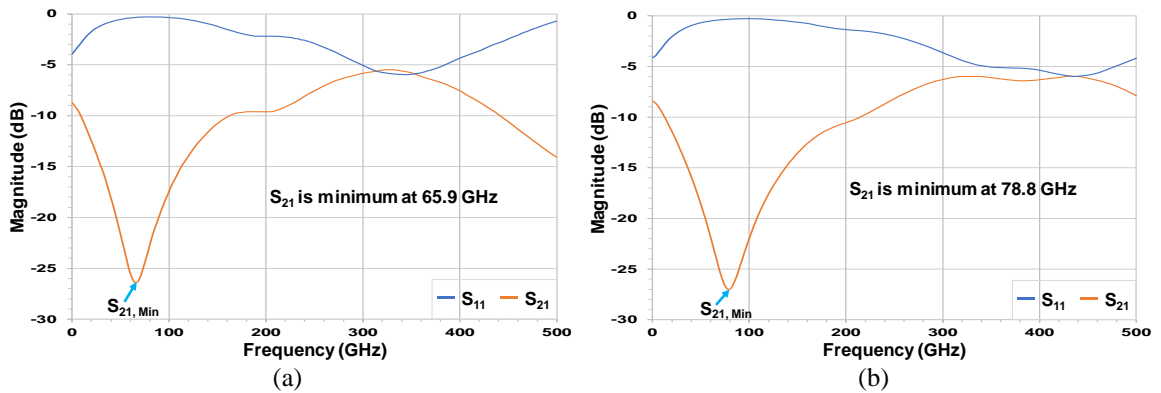


Figure 4.13. S-Parameters of the circuit with (a) original magnetic probe, and (b) manipulated magnetic probe.

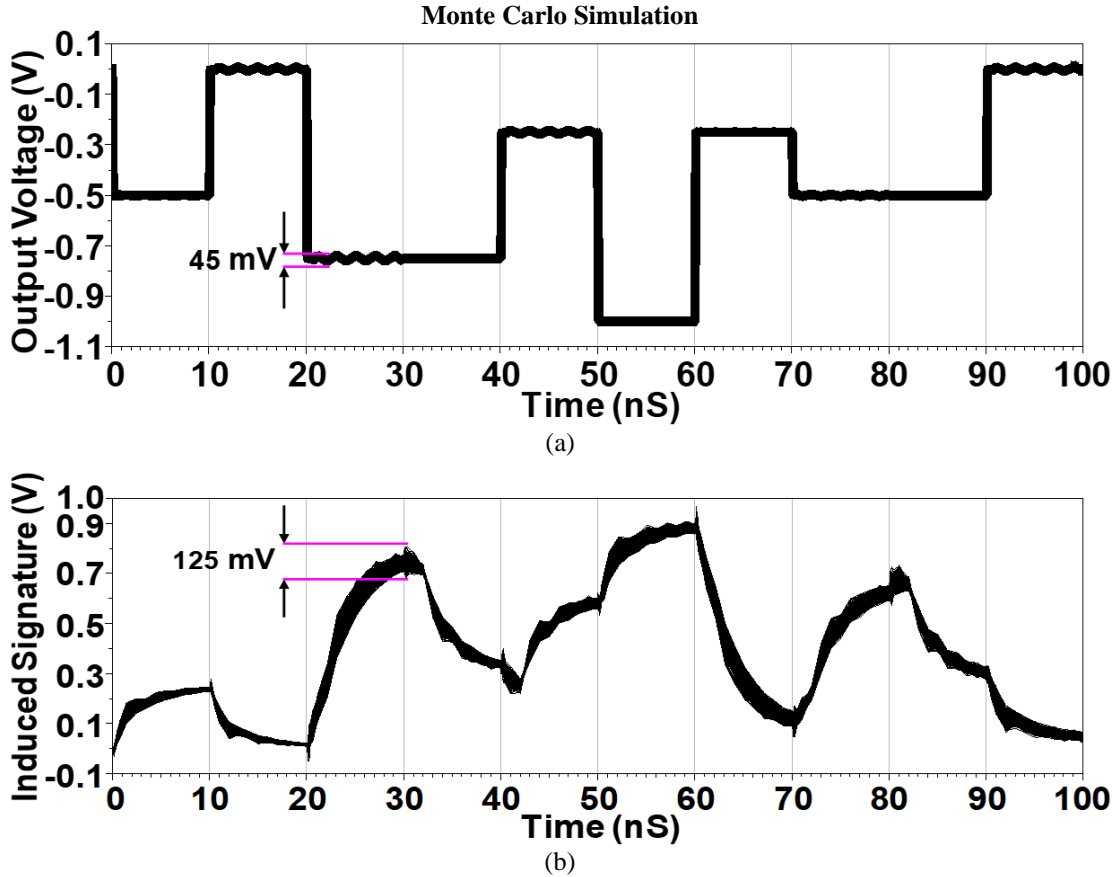


Figure 4.14. Monte Carlo analysis over 500 iterations for  $\pm 5\%$  variation of width and length of the probes.

TABLE 4.1. VARIATION BETWEEN THE  $S_{21}$  OF THE ORIGINAL AND THE MANIPULATED DESIGN AT 500 MHZ

Freq (MHz)	$S_{21}$ (dB) of the Original Design	$S_{21}$ (dB) of the Manipulated Design
125.0	-8.417	-8.825
250.0	-8.423	-8.831
375.0	-8.428	-8.836
<b>500.0</b>	<b>-8.432</b>	<b>-8.84</b>
625.0	-8.437	-8.846
750.0	-8.442	-8.852
875.0	-8.447	-8.858
1000	-8.453	-8.865

are shown in Fig. 4.13. Resonant frequency of the original probe was 65.9 GHz and changed to 78.8 GHz for the manipulated probe.

The frequency domain Simulations were also conducted at 500 MHz to show the correlation between the results in the time domain and the frequency domain. The results in Table 4.1 indicates that  $S_{21}$ , which corresponds with the gain in time domain, decreases

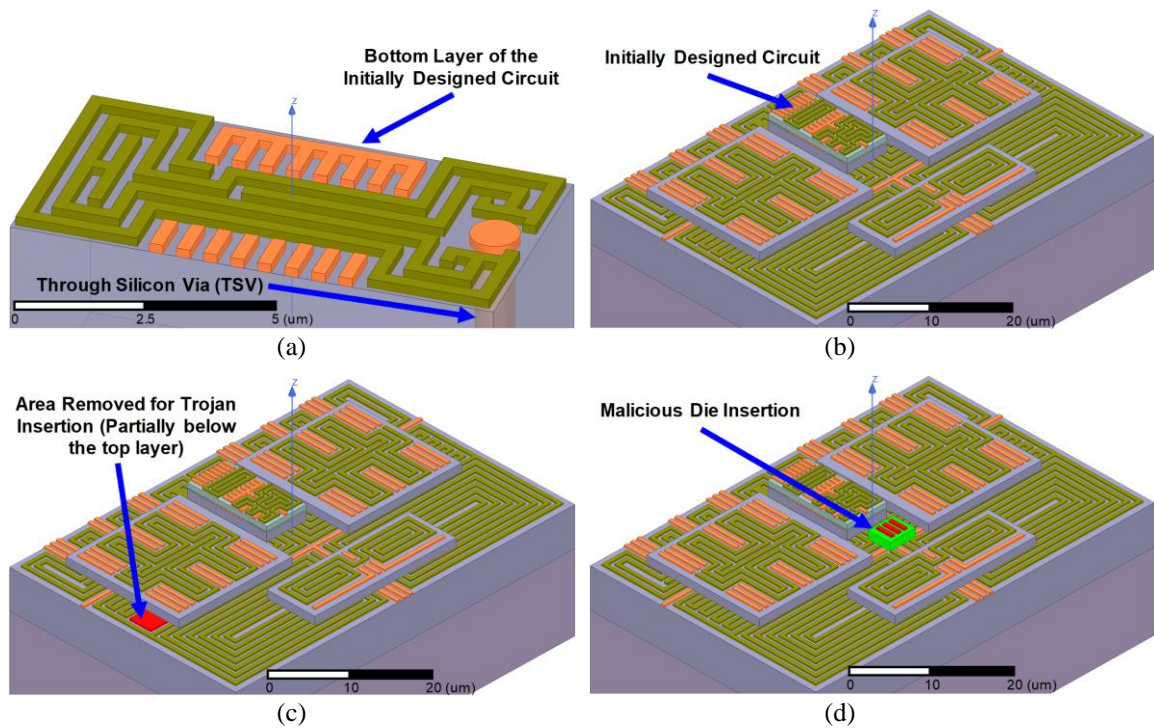


Figure 4.15. Final IC routing including the design of the magnetic probe: (a) the output of the initial design connected to the bottom layer of the final routing using TSV (b) original design of the final IC routing, and (c) a portion of metal is removed from, (d) an extra die has been added.

by about  $-0.4$  dB when the circuit is manipulated. The simulation results in the time domain in Fig. 4.12 (a) and Fig. 4.12 (b) also indicate that the gain drops slightly for the manipulated circuit.

Monte Carlo simulation of the DAC circuit was also performed to check the effect of process variation. The parameters of the magnetic probe were varied by  $\pm 5\%$  over a simulation of 500 iterations. The output of the simulation is shown in Fig. 4.14. Fig. 4.14 (a) shows the output of the original circuit, which indicates that it remains unchanged regardless of any variation of the probe. As shown in Fig. 4.14 (b), the DC offset of the signature varies by as much as 125 mV, but the frequency content and hence the shape of the signature remains unchanged; whereas any change in the model of the probe varies both of those.

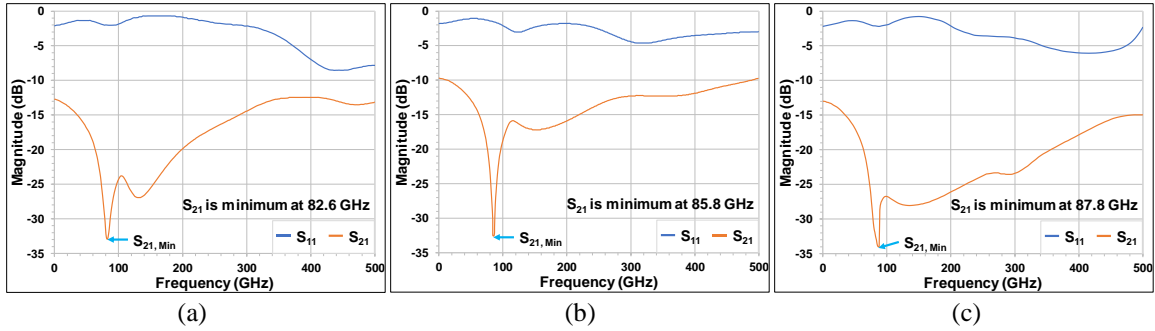


Figure 4.16. S-Parameters of the routing of the IC of Fig. 4.15 with (a) original magnetic probe, (b) magnetic probe with a portion of metal removed, and (c) magnetic probe with extra die added.

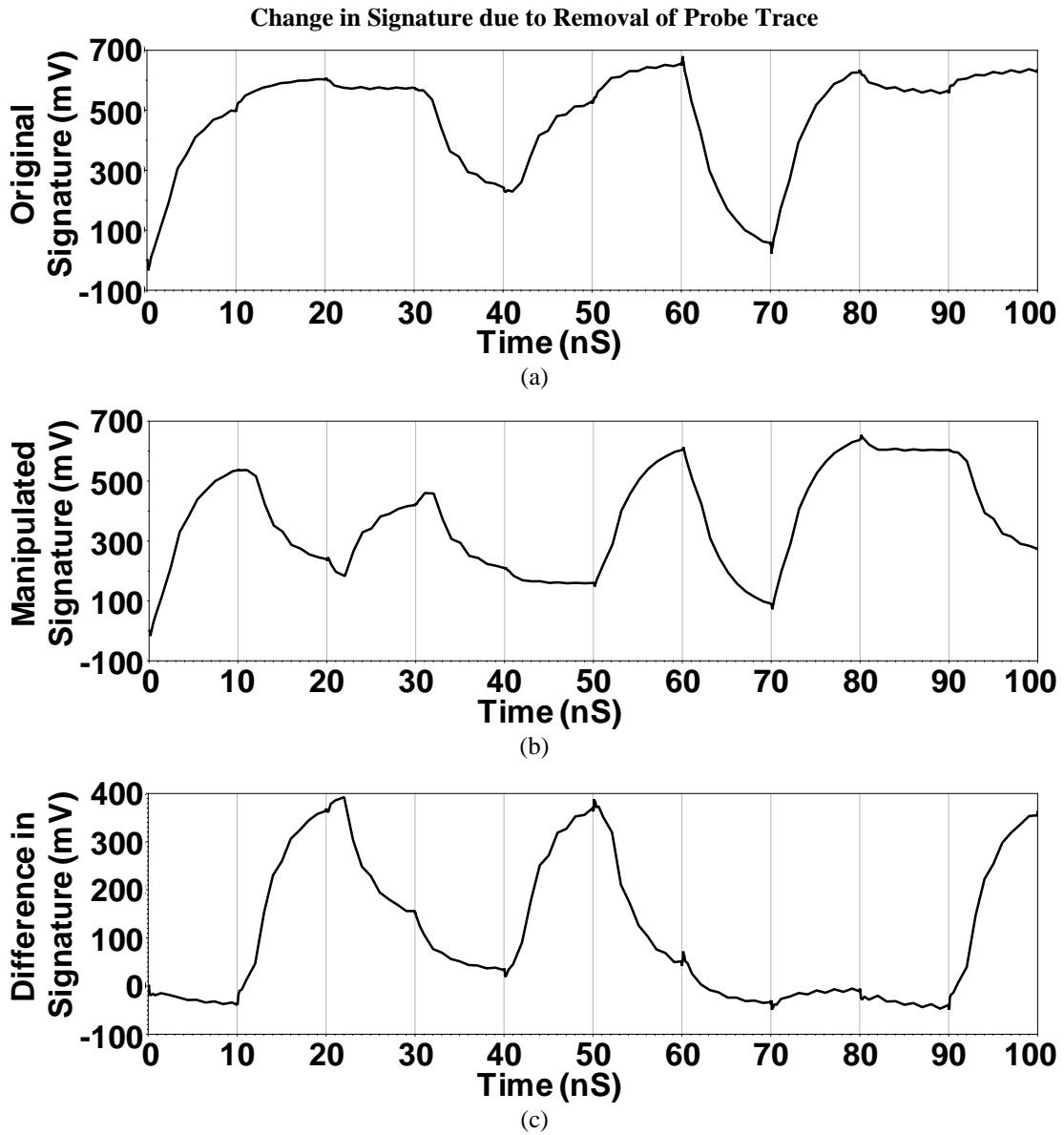


Figure 4.17. Graph showing the signature of the (a) Original design and (b) Manipulated design of Fig. 4.15 (b, c), and (c) Difference between those two signatures.



TABLE 4.2. COMPARISON WITH THE STATE-OF-THE-ART METHODS

Method	% Filled	Dependency on the IC Size	Maximum Size of Main Circuit	Hardware Trojan Distinguishability	Signature Obtained by Using
Paper [36]	93%-99%	Does not work well for bigger ICs	Not reported	Hard	Bit-Sequence
Paper [37]	99%-100%	Cannot fill 100% in complex circuits	80% of the die	Hard	Bit-Sequence
Paper [38]	>90%	Dependent, but not reported	85% of the die	Hard	Bit-Sequence
Paper [39]	100% Poly	Independent of IC size	Independent	Comparatively Easier	Delay Measurement
Proposed	100%	Independent of IC size	Independent	Comparatively Easier	Analog Voltage Profile

The circuit simulated previously is connected via a TSV to another design. The location of the TSV is shown in Fig. 4.15 (a). The final IC routing is shown in Fig. 4.15 (b). To mimic the manipulation by an attacker,  $12 \mu\text{m}^2$  area was removed from the probe metals as indicated in Fig. 4.15 (c). Part of the removed metal is under the top layer, which is expected with both 2.5D and 3D ICs. During the die stacking and TSV bonding process of 3D IC, a separate die with the Trojan circuit can also be added to the original design, which is shown in Fig. 4.15 (d). The resulting S-parameters, shown in Fig. 4.16, exhibit a considerable shift in  $S_{21}$ : from 82.6 GHz for the original circuit of Fig. 4.15 (b) to 85.8 GHz for the IC of Fig. 4.15 (c) and to 87.8 GHz for the IC of Fig. 4.15 (d). The spice models were then extracted from the HFSS model and the transient simulations of the complete circuit were performed in the ADS environment to see the variation of the signature. Figure 4.17 shows the signatures obtained from the circuits in Fig. 4.15 (b) and (c), and difference between their signatures. The difference between the two signatures varies between -100 mV and 400 mV as shown in Fig. 4.17 (c). Similarly, Fig. 4.18 (a) and (b) shows the signature obtained from original probe and probe with a Trojan added by placing an extra die during the bonding stage, and Fig. 4.18 (c) shows the

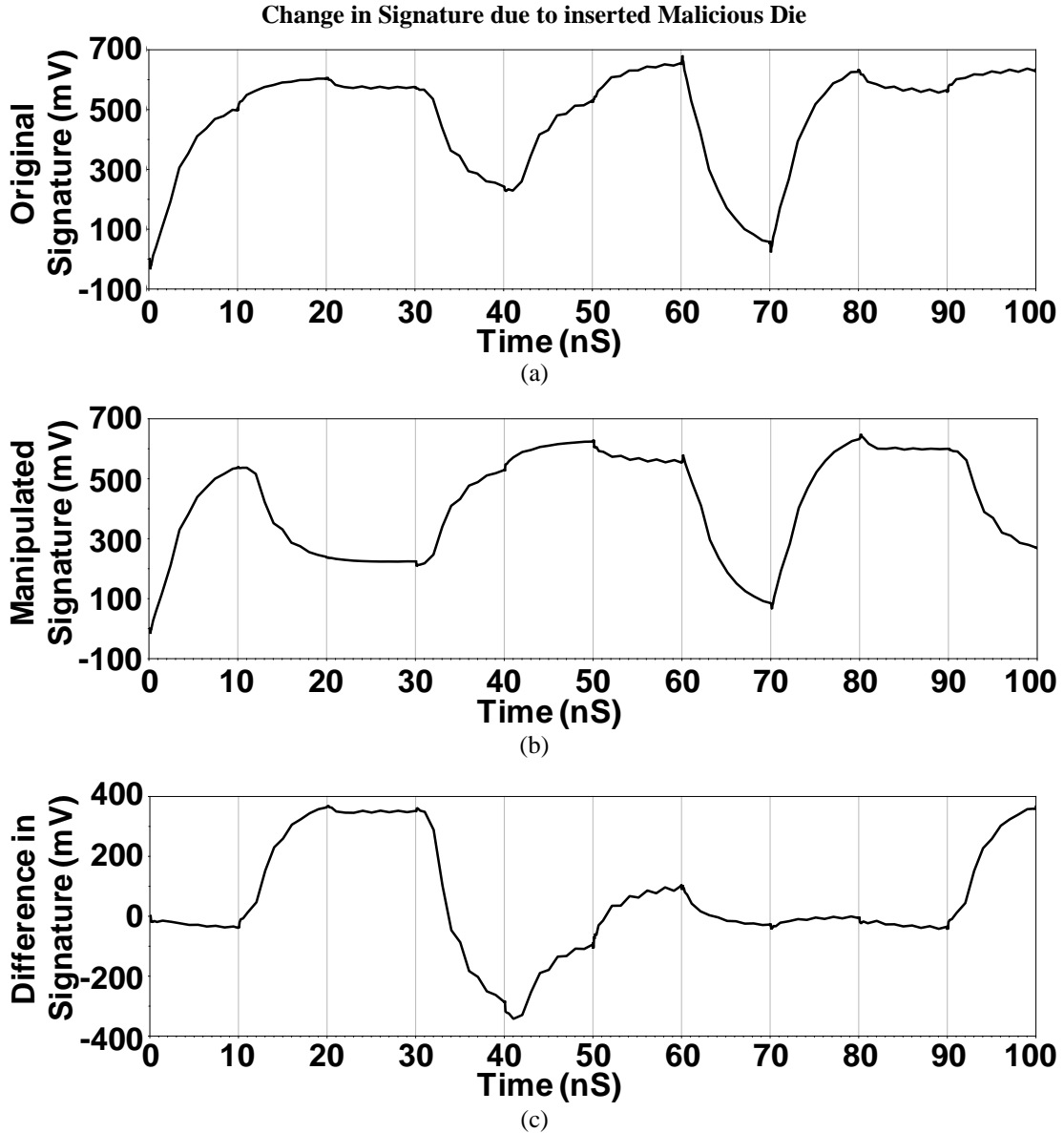


Figure 4.18. Graph showing the signature of the (a) Original design and (b) Manipulated design of Fig. 4.15 (b, d). and (c) Difference between those two signatures.

difference between their signatures, which has a range of  $\pm 400$  mV. The variation in both cases is large enough to be readily detected by the implemented magnetic probe.

Table 4.2 show the comparison between the performance parameters of the existing methods and those of the proposed solution. As shown in the table, [36] cannot reach 100% filled space, but both [37] and [38] can do so, given the original circuit occupies a maximum of 80% (for [37]) or 85% (for [38]) of the whole die. The technique of

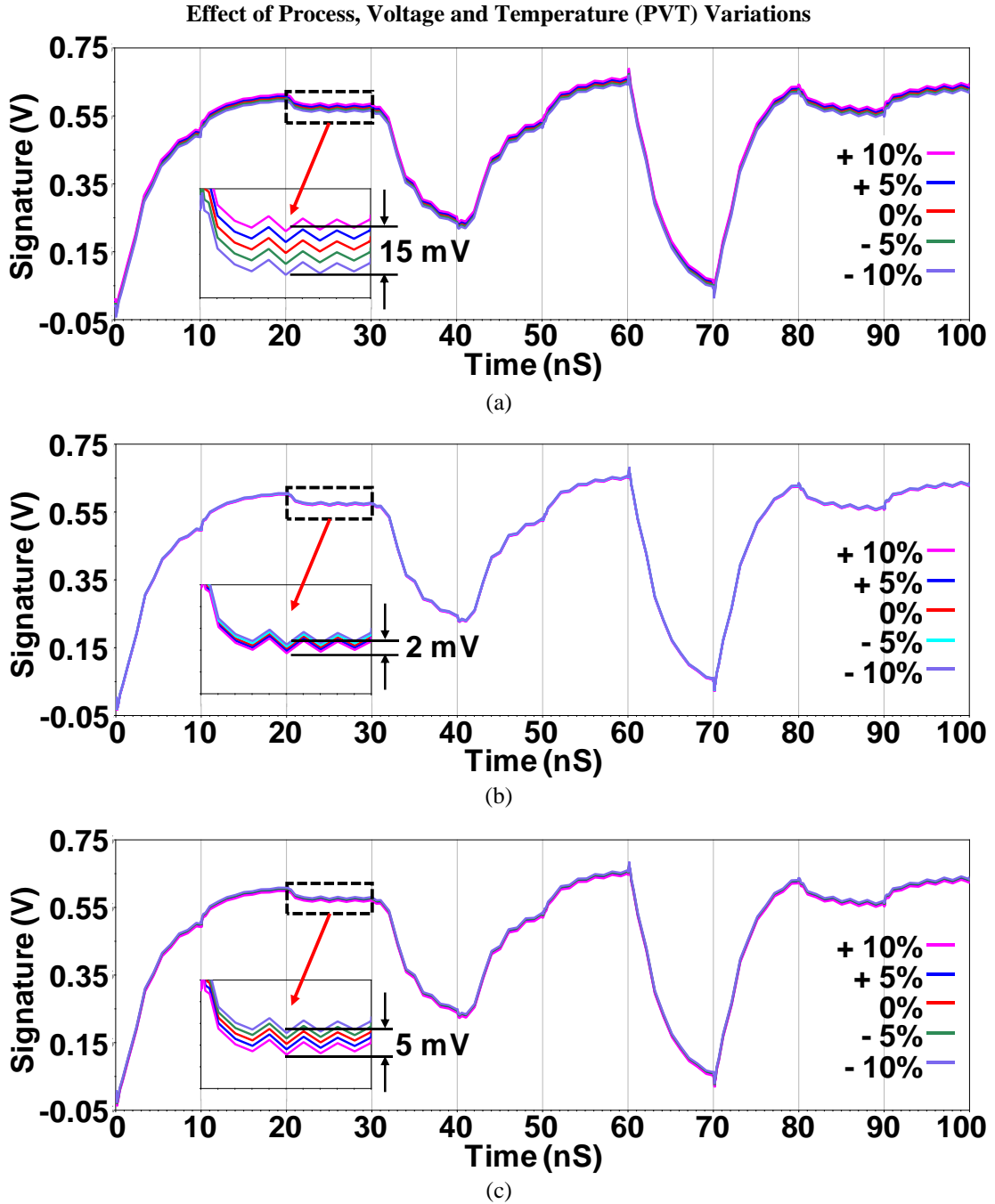


Figure 4.19. Graph showing change in signatures due to (a) Process, (b) Voltage and (c) Temperature variations.

manuscript [39] is independent of the size of both the design and the IC and creates a unique signature, which is sensitive to the PVT variations. Thus, a relatively complex readout circuit traces with minimum width and gap are used in this method. Moreover,

the signatures in the reported works are digital while in the proposed method, the signature is an analog one, which is more difficult to duplicate.

The effect of PVT variations on the obtained signature was also observed to verify the robustness of the proposed method. For each simulation, the parameter was varied by a maximum of  $\pm 10\%$  from the nominal value. As seen in Fig. 4.19, amplitude of the signature varies marginally due to PVT variations: the amplitude varies linearly with the process and voltage variations, whereas it varies inversely with temperature. Each variation is large enough to be detected. The change in the amplitude caused by PVT variations affect the DC offset.

#### **4.5 CONCLUSION**

In this paper, a method to prevent untrusted foundry from inserting malicious circuits or Hardware Trojans is presented. In the proposed solution, the excess layout resources, which include metal and polysilicon layers, are used to design on-chip magnetic probes. As a result, the attacker will not have routing resources to implement a Hardware Trojan and connect it to the main circuit. Moreover, the magnetic probes are used to capture the unique signature of the IC, which can be used to verify Trojan-free chips. A layout-filling ratio of 100% can be obtained using the proposed technique. The proposed method can also be used to detect Trojans in 3D ICs during die stacking or TSV bonding stages.

#### **REFERENCES**

- [1] K. Xiao et al., "Hardware Trojans: Lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 1-23, 2016.

- [2] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware security threats and potential countermeasures in emerging 3D ICs," in *2016 Int. Great Lakes Symp. on VLSI (GLSVLSI)*, Boston, MA, USA, 2016, pp. 69-74.
- [3] K. Huang, J. M. Carulli, and Y. Makris, "Counterfeit electronics: A rising threat in the semiconductor manufacturing industry," in *2013 IEEE Int. Test Conf. (ITC)*, Anaheim, CA, USA, 2013, pp. 1-4.
- [4] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. of the IEEE*, vol. 102, no. 8, pp. 1207 - 1228, Jul. 2014.
- [5] M. Beaumont, B. Hopkins, and T. Newby, "Hardware trojans - prevention, detection, countermeasures (A Literature Review)," Edinburgh, SA, Australia. Tech. Note DSTO-TN-1012, Jul. 2011. [Online]. Available: <https://apps.dtic.mil/docs/citations/ADA547668>
- [6] S. Kaji, M. Kinugawa, D. Fujimoto and Y. Hayashi, "Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan," in *IEEE Trans. on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1115-1121, Aug. 2019.
- [7] Y. Hayashi, N. Homma, T. Mizuki, H. Shimada, T. Aoki, H. Sone, L. Sauvage, and J. L. Danger, "Efficient Evaluation of EM Radiation Associated With Information Leakage From Cryptographic Devices," in *IEEE Trans. on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 555-563, June 2013.

- [8] S. Osuka et al., "EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage," in *IEEE Trans. on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1122-1128, Aug. 2019.
- [9] M. Tehranipoor, and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10 - 25, Feb. 2010.
- [10] F. S. Hossain, T. Yoneda, M. Inoue, and A. Orailoglu, "Detecting hardware trojans without a Golden IC through clock-tree defined circuit partitions," in *2017 22nd IEEE European Test Symp. (ETS)*, Limassol, Cyprus, 2017, pp. 1-6.
- [11] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, "Security and vulnerability implications of 3D ICs," *IEEE Trans. on Multi-Scale Comp. Sys.*, vol. 2, no. 2, pp. 108 - 122, Apr. 2016.
- [12] S. Dupuis, P.-S. Ba, M.-L. Flottes, G. D. Natale, and B. Rouzeyre, "New testing procedure for finding insertion sites of stealthy hardware trojans," in *2015 Design, Auto. & Test in Europe Conf. & Exhi. (DATE)*, Grenoble, France, 2015, pp. 776-781.
- [13] R. S. Chakraborty, S. Pagliarini, J. Mathew, S. R. Rajendran, and M. N. Devi, "A flexible online checking technique to enhance hardware trojan horse detectability by reliability analysis," *IEEE Trans. on Emerg. Topics in Comp.*, vol. 5, no. 2, pp. 260 - 270, Jan. 2017.
- [14] S. Dupuis, M.-L. Flottes, G. D. Natale, and B. Rouzeyre, "Protection against hardware trojans with logic testing: Proposed solutions and challenges ahead," *IEEE Design & Test*, vol. 35, no. 2, pp. 73 - 90, Apr. 2018.

- [15] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *2007 IEEE Symp. on Security and Privacy (SP '07)*, Berkeley, CA, USA, 2007, pp. 296-310.
- [16] X.-T. Ngo, I. Exurville, S. Bhasin, J.-L. Danger, S. Guilley, Z. Najm, J.-B. Rigaud, and B. Robisson, "Hardware trojan detection by delay and electromagnetic measurements," in *2015 Design, Auto. & Test in Europe Conf. & Exhi. (DATE)*, Grenoble, France, 2015, pp. 782-787.
- [17] J. He, Y. Zhao, X. Guo, and Y. Jin, "Hardware trojan detection through chip-free electromagnetic side-channel statistical analysis," *IEEE Trans. on Very Large Scale Integration (VLSI) Sys.*, vol. 25, no. 10, pp. 2939-2948, Jul. 2017.
- [18] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," in *2008 IEEE Int. Work. on Hard. Ori. Security and Trust*, Anaheim, CA, USA, 2008, pp. 51-57.
- [19] I. Exurville, L. Zussa, J.-B. Rigaud, and B. Robisson, "Resilient hardware trojans detection based on path delay measurements," in *2015 IEEE Int. Symp. on Hard. Ori. Security and Trust (HOST)*, Washington, DC, USA, 2015, pp. 151-156.
- [20] M. Lecomte, J. Fournier, and P. Maurine, "An on-chip technique to detect hardware trojans and assist counterfeit identification," *IEEE Trans. on Very Large Scale Integration (VLSI) Sys.*, vol. 25, no. 12, pp. 3317 - 3330, Dec. 2017.
- [21] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff, C. Papachristou, K. Roy, and S. Bhunia, "Multiple-parameter side-channel analysis: A non-invasive hardware trojan detection approach," in *2010 IEEE Int. Symp. on Hard. Ori. Security and Trust (HOST)*, Anaheim, CA, USA, 2010, pp. 13-18.

- [22] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. G. Wolff, C. A. Papachristou, K. Roy, and S. Bhunia, "Hardware trojan detection by multiple-parameter side-channel analysis," *IEEE Trans. on Computers*, vol. 62, no. 11, pp. 2183 - 2195, Nov. 2013.
- [23] L. Ni, J. Li, S. Lin, D. Xin, "A method of noise optimization for Hardware Trojans detection based on BP neural network", *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, pp. 2800-2804, Oct. 2016.
- [24] P. Ghosh and R. S. Chakraborty, "Counterfeit IC detection by image texture analysis," in *2017 Euromicro Conf. on Digital System Design (DSD)*, Vienna, Austria, 2017, pp. 283-286.
- [25] S. Bhasin, J.-L. Danger, S. Guilley, X. T. Ngo, and L. Sauvage, "Hardware trojan horses in cryptographic IP cores," in *2013 Work. on Fault Diag. and Tolerance in Crypto.*, Santa Barbara, CA, USA, 2013, pp. 15-29.
- [26] T. Hoque, J. Cruz, P. Chakraborty, and S. Bhunia, "Hardware IP Trust Validation: Learn (the Untrustworthy), and Verify," in *2018 IEEE International Test Conference (ITC)*. IEEE, 2018, pp. 1–10.
- [27] L. R. Rivera, X. Wang, and D. Chasaki, "A Separation and Protection Scheme for On-Chip Memory Blocks in FPGAs," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2016, pp. 223–228.
- [28] S. Gundabolu, and X. Wang, "On-chip Data Security Against Untrustworthy Software and Hardware IPs in Embedded Systems," in *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, July 2018, pp. 644–649.



- [29] R. S. Chakraborty and S. Bhunia, "HARPOON: An obfuscation-based SoC design methodology for hardware protection," *IEEE Trans. on Comp.-Aided Design of Integ. Circuits and Sys.*, vol. 28, no. 10, pp. 1493 - 1502, Oct. 2009.
- [30] R. S. Chakraborty and S. Bhunia, "Security against hardware trojan attacks using key-based design obfuscation," *J. of Elec. Testing*, vol. 27, no. 6, p. 767–785, Dec. 2011.
- [31] X. T. Ngo, S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "Linear complementary dual code improvement to strengthen encoded circuit against hardware trojan horses," in *2015 IEEE Int. Symp. on Hard. Ori. Security and Trust (HOST)*, Washington, DC, USA, 2015, pp. 82-87.
- [32] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. of the 2013 ACM SIGSAC conf. on Comp. & comm. security*, Berlin, Germany, 2013, pp. 709-720.
- [33] T. F. Wu, K. Ganesan, Y. A. Hu, H.-S. P. Wong, S. Wong, and S. Mitra, "TPAD: Hardware trojan prevention and detection for trusted integrated circuits," *IEEE Trans. on Comp.-Aided Design of Integ. Circuits and Sys.*, vol. 35, no. 4, pp. 521 - 534, Apr. 2016.
- [34] M. I. M. Collantes, M. E. Massad, and S. Garg, "Threshold-dependent camouflaged cells to secure circuits against reverse engineering attacks," in *2016 IEEE Comp. Society Annual Symp. on VLSI (ISVLSI)*, Pittsburgh, PA, USA, 2016, pp. 443-448.
- [35] J. Ichimiya, "Layout design method of semiconductor integrated circuit, and semiconductor integrated circuit, with high integration level of multiple level metalization," U.S. Patent 7 076 756 B2, Jul. 11, 2006.

- [36] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware trojan insertion," in *2013 IEEE Int. Symp. on Hard. Ori. Security and Trust (HOST)*, Austin, TX, USA, 2013, pp. 45-50.
- [37] P.-S. Ba, M. Palanichamy, S. Dupuis, M.-L. Flottes, G. D. Natale, and B. Rouzeyre, "Hardware trojan prevention using layout-level design approach," in *2015 European Conf. on Circuit Theory and Design (ECCTD)*, Trondheim, Norway, 2015, pp. 1-4.
- [38] P.-S. Ba, S. Dupuis, M. Palanichamy, M.-L.-. Flottes, G. D. Natale, and B. Rouzeyre, "Hardware trust through layout filling: A hardware trojan prevention technique," in *2016 IEEE Comp. Society Annual Symp. on VLSI (ISVLSI)*, Pittsburgh, PA, USA, 2016, pp. 254-259.
- [39] T. M. Supon, M. Seyedbarhagh, R. Rashidzadeh, and R. Muscedere, "Hardware trojan prevention through limiting access to the active region," in *2019 Int. Conf. Design and Test of Integ. Sys. in Nano. Era (DTIS)*, Greece, 2019, in press.
- [40] Y. Xie, C. Bao, and A. Srivastava, "3D/2.5D IC-based obfuscation," in *Hardware Protection through Obfuscation*, Cham, Switzerland: Springer, 2017, ch. 12, pp. 291-312.
- [41] J. Valamehr, T. Sherwood, R. Kastner, D. Marangoni-Simonsen, T. Huffmire, C. Irvine, and T. Levin, "A 3-D split manufacturing approach to trustworthy system development," *IEEE Trans. on Comp.-Aided Design of Integ. Circuits and Sys.*, vol. 32, no. 4, pp. 611-615, Apr. 2013.

- [42] J. Dofe, C. Yan, S. Kontak, E. Salman, and Q. Yu, "Transistor-level camouflaged logic locking method for monolithic 3D IC security," in *2016 IEEE Asian Hard.-Ori. Security and Trust (AsianHOST)*, Yilan, Taiwan, 2016, pp. 1-6.
- [43] F. Imeson, A. Emtenan, S. Garg, and M. V. Tripunitara, "Securing computer hardware using 3D integrated circuit (IC) technology and split manufacturing for obfuscation," in *Proc. of the 22nd USENIX conf. on Security*, Washington, D.C., USA, 2013, pp. 495-510.
- [44] S. R. Hasan, S. F. Mossa, O. S. A. Elkeelany, and F. Awwad, "Tenacious hardware trojans due to high temperature in middle tiers of 3-D ICs," in *2015 IEEE 58th Int. Midwest Symp. on Circuits and Systems (MWSCAS)*, Fort Collins, CO, USA, 2015, pp. 1-4.
- [45] V. K. Tripathi, "Equivalent circuits and characteristics of inhomogeneous nonsymmetrical coupled-line two-port circuits," *IEEE Trans. Microw. Theory Tech.*, vol. MTT-25, no. 2, pp. 140-142, Feb. 1977.
- [46] B. Razavi, "Noise," in *Design of Analog CMOS Integrated Circuits*, 2nd ed. New York, NY, USA: McGraw-Hill, 2016, ch. 7, pp. 201–239.
- [47] I. I. Basith and R. Rashidzadeh, "Contactless test access mechanism for TSV-based 3-D ICs utilizing capacitive coupling," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 1, pp. 88–95, Jan. 2016

---

## Chapter 5

---

# HARDWARE TROJAN PREVENTION USING MEMRISTOR TECHNOLOGY

---

### 5.1 INTRODUCTION

Advances in deep submicron semiconductor technologies have enabled an unprecedented level of integration of complex and high-performance analog and digital circuits, processing units, Micro-Electro-Mechanical-Systems (MEMS), input/output interfaces, memories, and sensors into a single Integrated Circuit (IC). A state-of-the-art fabrication node would cost design companies billions of dollars [1]. To decrease the capital costs and mitigate the final cost escalation, outsourcing strategies have been long adopted by design houses as a practical alternative. However, from a security point of view, the trend toward outsourcing is not flawless. The migration of in-house fabrication to overseas foundries could provide opportunities for malicious activities and pave the way for potential security threats such as Hardware Trojans and IP theft [2].

In its broad sense, Hardware Trojan (HT) can be defined as any malicious modification of a circuit to alter its characteristics that may lead to failure in normal functionality, leakage of confidential information, shortage of the expected lifetime, denial of service under certain conditions or, in general, any undesirable effect on ICs [3].

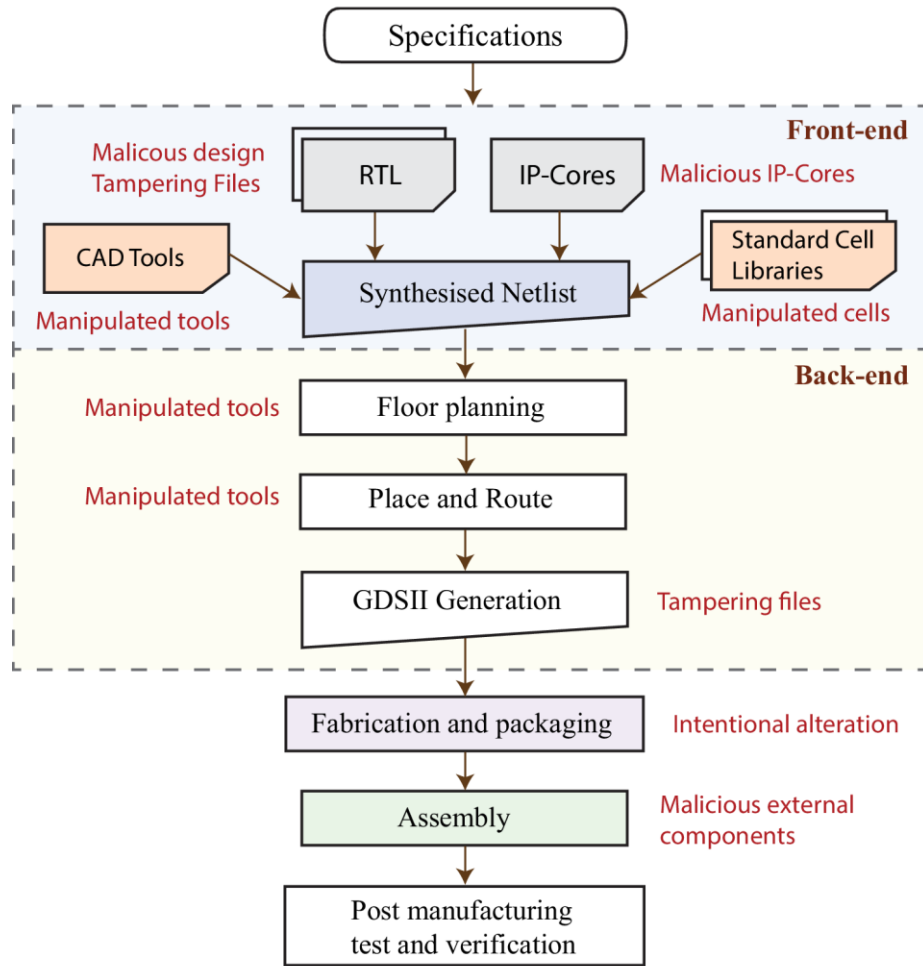


Figure 5.1. A typical design flow of IC manufacturing process.

The threat of HTs has drawn more attention after the discovery of counterfeit chips destined for safety and security-critical systems such as high-speed train breaks, hostile radar tracking in F-16 fighters, ballistic missile defense control systems, and Falcon 5000 nuclear identification tool during recent years [4]. These alarming security concerns about the vulnerability of ICs to HTs have brought about preventive measures such as the Trust in ICs program initiated by the Defense Advanced Research Projects Agency (DARPA) [5] or the European funded Holistic Approaches for Integrity of ICT (Information and Communication Technologies)-Systems (HINT) project [6] to address these new challenges. Researchers have also started treating hardware security as an

integral part of chip design [7]. They proposed to design the security measures in such a way that their performance can be evaluated and be optimized if necessary.

Trojan insertion can be done in any stage of an IC development process from RTL design to fabrication. Figure 5.1 illustrates a typical design flow of IC manufacturing process. The potential threat in each step is also shown in the figure. Assuming trusted Computer-Aided Design (CAD) tools, third party intellectual property (IP) cores, and untampered design files, in what follows our main focus will be on tackling Trojans embedded in the physical design after tapeout and during fabrication, which is a direct consequence of outsourcing.

A set of security measures against HTs, known as Trojan prevention techniques, has recently gained great attention. Trojan prevention relies mainly on the fact that Trojan insertion without having prior knowledge about the functional behavior of the original design is very challenging as Trojans either will not be triggered or be easily detected.

Based on this idea, Chakraborty et al. presented a novel technique to obfuscate the original behavior of the design by expanding the reachable state space of the original design. In this method, an extremely rare condition must happen for a transition from the obfuscated mode to the normal mode [8], [9]. The basic idea is to confine the circuit to an isolated (obfuscated) state-space unless a unique input sequence is applied that allows the transition from obfuscated to normal mode. Since the starting state of the circuit operation is located inside the isolated state space, the signal probabilities computed by the adversary through applying random inputs would highly differ from the true quantities resulting from an operation of the circuit in the normal mode.

Malik et al. have developed an obfuscated standard cell library in which all the cells have identical masking layers and only differ in dopant polarity of the active area [10]. Although this technique provides a high level of obscurity against visual inspection for reverse engineering, the functionality of the original design remains unchanged, and low probability nodes are still exposed. Moreover, a similar structure for all the standard gates would cause negative effects on delay, area, and power consumption.

Split manufacturing is another way to provide a high level of obfuscation in the functional behavior of the chip. In this method, the bottommost layers of a chip including the substrate and transistor layers together with a few layers of metal wiring would be made in the first foundry (with the possibility of malicious activities). This stage must be done at a state-of-the-art fabrication foundry as these layers contain the most finely detailed features of the chip. Then the wafer would be shipped to one or two trusted foundries so that the higher less detailed layers of the chip can be fabricated. Note that the latter stage could be done in a less advanced foundry as fabricating the higher layers requires less advanced technology and can be carried out in-house.

Based on the idea of split manufacturing, Mitra et al. have devised a randomized parity checker circuitry integrated into the original chip that constantly monitors ongoing processes [11]. The transistor and first metal layers were built in the Global Foundries fab in Singapore. The next four metal layers were added at an IBM-built plant in Burlington, VT, and finally to obfuscate the function of the checker circuitry some of its connections were made later by adding a layer of resistive RAM-based switches. This method presents a promising solution however, the cost overhead of several sub-manufacturing and shipping would not be justifiable for all applications.

Another method is presented by Fournaris et al. where they used reconfigurable-logic barriers as a prevention technique against Hardware Trojans and IP Piracy [12]. Here, they divided the whole circuit into different subcircuits, the flow of signal among which depends upon a security key. The desired flow of information is possible only by providing the correct key. This is a very efficient method; the main drawbacks being the added area and power overhead associated with the logic gates used for the security key.

In all the above-mentioned methods, robustness against Trojans insertion is achieved at the cost of additional logic cells embedded into the original design. This hardware overhead could have a negative effect on the performance of the original circuit in terms of power consumption, critical path delay, or required die area. They can also mask the effect of the insertion of a Trojan [13]. Recent studies [14]–[16] have shown the vulnerability of typical split-manufacturing and obfuscation techniques against Boolean satisfiability (SAT) solver attacks, which eliminates incorrect connection combinations while recovering missing back-end-of-line signals. As a countermeasure, researchers have come up with different techniques in [17]–[21] to increase the difficulty of executing a SAT attack. The primary assumption of a SAT attack is that the attacker has access to an activated IC, where the IC performs its normal operation and correct input-output pairs are generated. Moreover, the attacker must know the gate level logical representation of the circuit. If both the assumptions are satisfied, the attacker can use the SAT attack to obtain the applied key bits.

Inspired by the idea of obfuscation and recent advances in memristive devices, in this paper, we present a novel Trojan and IP piracy prevention technique using a hybrid architecture of nanowire crossbars and CMOS technology to conceal the functional



behavior of the circuit. We show that the proposed technique can be applied to any type of design with a low area and power overhead. Broadly speaking, the idea presented here runs in the same vein as the one presented in [12]; the main idea being obfuscating the actual netlist of the design. The one presented here has some added advantages compared to the one in [12]. The implementation of the obscuring method presented here is much simpler than the one presented in [12]; the new method being as simple as rerouting a net through 2 conductors, and just a memristor. Moreover, the use of memristor devices as opposed to the CMOS gates used in [12] ensures lower power and area overhead [22]. A new design flow and test method based on the proposed hybrid architecture has also been presented in this article. The proposed method is resilient against SAT-based attacks since even if the attacker gets a pre-activated IC, it is very unlikely to have the netlist of the original design. The crossbar structure ensures that a single net can be connected to an array of other nets, based on the biasing values. The most feasible way to know the actual netlist is to know the biasing values beforehand, which in this case is the applied key bits. Hence, the proposed method can thwart a SAT attack efficiently.

The organization of this paper is as follows. Section II provides a brief introduction of a generic Hardware Trojan, explains the concept of design obfuscation, and briefly introduces Memristor devices. The proposed architecture, that prevents both Hardware Trojan insertion and IP piracy, the proposed design flow, and the test method are presented in Section III. The simulation results and comparisons are provided in Section IV. Finally, in Section V concluding remarks are drawn.

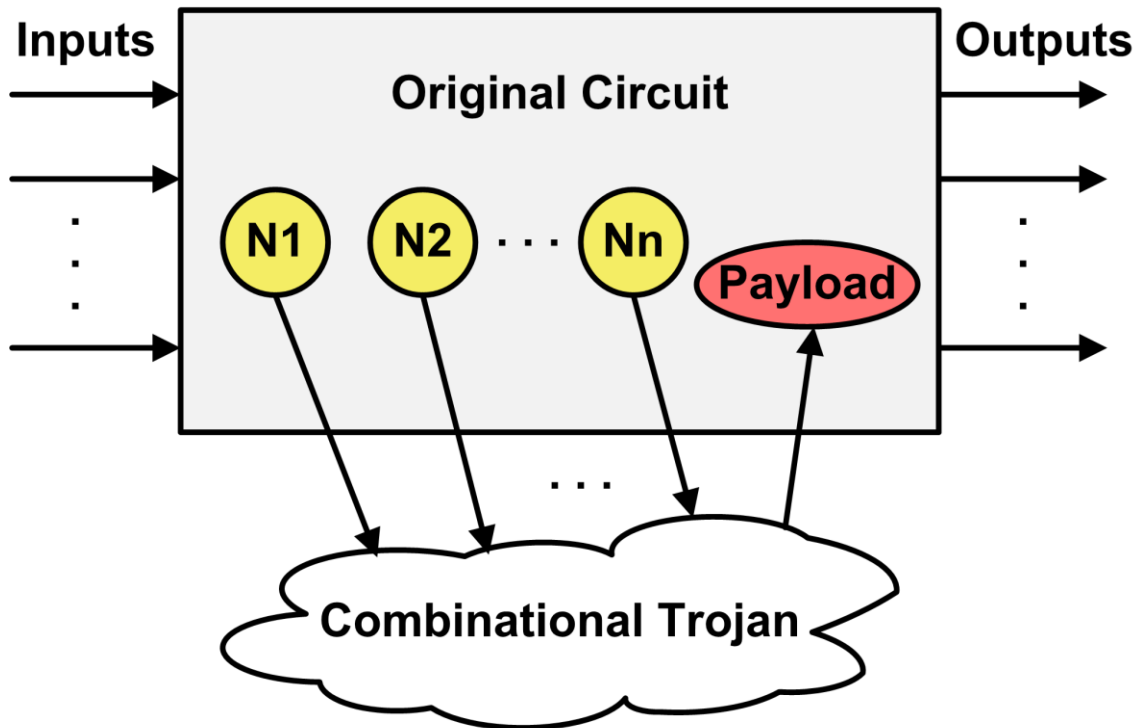


Figure 5.2. Generic Hardware Trojan.

## 5.2 PRELIMINARIES

### A *Generic Hardware Trojan*

The operation of a generic hardware Trojan is illustrated in Fig. 5.2. A Trojan constantly listens to the variations in the values of a group of carefully selected internal nodes known as triggering nodes (indicated by N1 to Nn in Fig. 5.2). To camouflage a Trojan as much as possible, despite the nature of the Trojan's functional behavior, the triggering nodes should be essentially selected from a set of nodes whose combination of desired values creates a rare condition known as triggering event.

The structure of a Trojan can be composed of a combinatorial circuit reacting to specific triggering events. It could also contain several sequential elements forming a

finite state machine, in which a sequence of transitions must be traversed before triggering a malfunction. Finally, after the triggering conditions are satisfied, Trojans would affect one or several nodes referred to as the payload. Having an overall picture of how a hardware Trojan operates, in what follows the concept of design obfuscation is explained first and then the proposed scheme is presented in Section III.

### ***B The Basic Idea Behind Design Obfuscation***

Trojan activation is a very popular detection technique due to two reasons: First, it is highly reliable against process variations and measurement noises. Second, the process can be integrated into the Logic Test stage of the post-manufacturing and verification phase (Fig. 5.1).

From the standpoint of a well-designed Trojan detector, an appropriate set of input test vectors would be the one that can trigger the low probability events i.e. the set of nodes whose values rarely change during the normal operation of the IC, which makes them a potential choice for generating triggering conditions. However, it is extremely hard to scan the whole state space and cover all the inter-state transitions of the design through randomly generated test vectors.

On the other hand, from an adversary point of view, any tampering in the functional behavior of the original design should be concealed in a way that is very difficult to detect with conventional logic test methods. In other words, the adversary would make certain that the Trojan is only triggered under very rare conditions at the internal nodes, which are unlikely to arise during the test phase but can occur during long hours of field operation.

To find the set of low probability events, a good approach for an adversary would be to simulate the conditions under which the IC would be used in normal operation mode. This can be done by randomly bringing the circuit to one of the states, available in the reachable state space, and then feeding the circuit with random input vectors. This way, a good approximation of node signal probabilities can be acquired. Then, nodes with the smallest signal probabilities would be selected from the pool of internal nodes as potential candidates.

One effective approach to prevent an intelligent adversary from discovering rare conditions is to obfuscate the true functionality of the circuit. In general, design obfuscation is a technique whose main objective is to hide the functionality and structure of the original design by transforming it into a secondary functionally equivalent design that is significantly more difficult to comprehend compared to the original one.

### *C Memristive Devices*

The current trend towards downscaling transistor dimensions in semiconductor technology is reaching its limits. Over the past few years, it has become more and more evident that other strategies should be employed to enable us to keep pace with performance improvement. Postulated first by Leon Chua in 1971 [23] as the fourth fundamental circuit element, memristors (contraction of memory resistors) introduce further integration capacity to conventional IC technology.

In general, a memristive device is a two-terminal electrical element that acts like a resistive switch whose resistance is dependent on the magnitude, duration, and polarity of the voltage applied to it. Memristive devices are known for the non-volatile alteration of

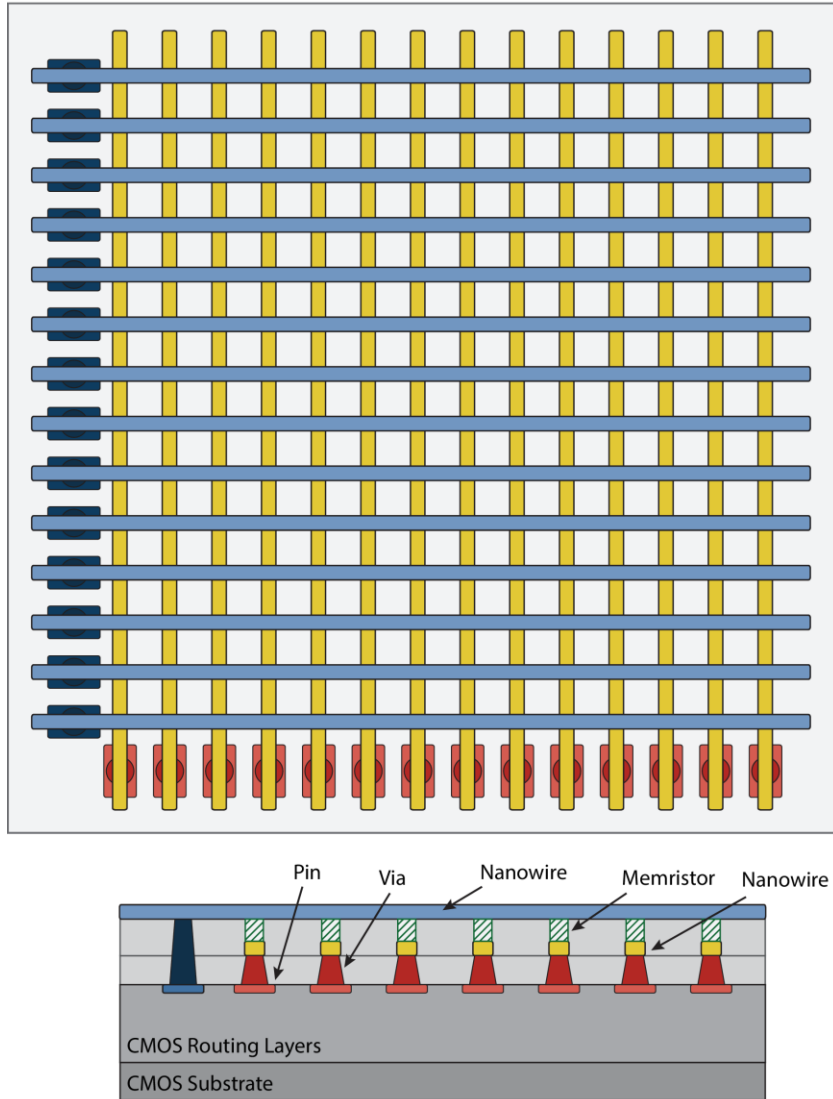


Figure 5.3. Crossing nanowires are separated by memristor switches at the junctions that can be electrically configured. Nanowire crossbars are connected to a CMOS chip via metallic pins over the CMOS stack.

their resistance, in the sense that they are capable of retaining a state of the most recent internal resistance based on the history of the applied voltage or the amount of charge that passed through them. The most notable feature of memristors is their current-voltage hysteresis curve, originally called pinched-hysteresis loops, that demonstrates their nonlinear behavior. This hysteretic current-voltage characteristic is caused by the inherent dependency of their resistance (or conductance) on the history of the voltage applied to them.

TABLE 5.1. CHARACTERISTICS BETWEEN 3 DIFFERENT MEMRISTOR DEVICES FABRICATED AT UNIVERSITY OF MICHIGAN, HP LABS AND ARIZONA STATE UNIVERSITY

Memristor	$R_{on}$ ( $\Omega$ )	$R_{off}$ ( $\Omega$ )	$V_t$ (V)	Switching time (ns)	Advantage
[31]	125K	125G	4.0	10	low energy intake
[32]	100	10K	0.7	2	low switching time
[33]	500K	1G	0.6	50	low write voltage

Apart from non-volatile random access memories which would be the most obvious application of memristors stemming from their hysteretic switching behavior, the high scalability, low power dissipation, short dynamic response, and more importantly nonlinear behavior of memristive devices make them appealing for a wide range of applications such as reconfigurable switches in FPGA-like ICs, material implication logic gates and synaptic connections for a neuromorphic network just to name a few [24]–[26].

One of the popular structures used for the fabrication of memristors is the crossbar architecture [27]. The crossbar structure is composed of two layers each consisting of an array of parallel nanowire electrodes as shown in Fig. 5.3. These two layers together form a grid of orthogonal nanowires. In a memristor-based crossbar structure, a cross-point junction is formed by a memristor switch connecting the top layer to the bottom layer where two nanowires cross over each other. Fabrication of hybrid CMOS/memristor-based crossbar architectures reported in [27]–[29] proves the feasibility of the memristor technology combined with the existing CMOS technology. Table 1 presents the characteristics of three memristor switches [30] fabricated in different labs at the University of Michigan [31], HP labs [32], and Arizona State University [33].

### 5.3 PROPOSED TROJAN AND IP PIRACY PREVENTION TECHNIQUE

The proposed scheme that is explained in the rest of this section differs from the previously proposed schemes in that:

1. No limitation is imposed on the type of standard cell libraries used to synthesize the RTL description and no modification is made on the set of standard cells.
2. Obfuscation is achieved by hiding the functionality of the circuit using a layer of configurable switches that blurs the actual netlist of the circuit at the time of outsourcing.
3. Netlist obfuscation is carried out without adding extra logic elements and as a result the delay and power overheads are kept minimal.
4. A configurable routing layer can be fabricated in the same foundry as the rest of the IC is fabricated, which in turn averts the cost overhead of split manufacturing.

The secure netlist clustering combined with obfuscation improves the testability, fault coverage and Trojan detection if any Trojan could be inserted.

#### *A Proposed Netlist Obfuscation Scheme*

The proposed scheme takes advantage of memristor switches to add a level of configurability to the signal routing in Nano/CMOS hybrid architectures. New advances in the fabrication of memristors have enabled an additional level of configurability in routing layers stemming from integrating a layer of nanowire crossbar over the CMOS stack using nanoimprint lithography technology [27], [28], and [34]. The basic idea

behind the proposed scheme is to obfuscate the functional behavior of the circuit by selecting a specific number of connected net pairs from the netlist and rerouting them across a configurable grid of nanowire crossbars. This can be done by connecting one of the nets of each pair to a source contact and the other net to a drain contact along the two metallic pin rails connecting the crossbar to the CMOS stack as shown in Fig. 5.3. The memristors of Fig. 5.3 connect each horizontal line to all the vertical lines. In the final design, which vertical line will connect to the horizontal line depends on the voltage applied to the memristors through the vias, as the resistance of all the memristors depend on the applied voltage. This resistance can be expressed as:

$$M(x) = [R_{ON}x + R_{OFF}(1 - x)] \quad (1)$$

where,  $R_{ON}$  and  $R_{OFF}$  are the resistances of the memristor during the ON and OFF states respectively, and  $x$  is the state variable, which is represented by the ratio between the thickness of the doped region,  $w$  and the width of the thin film,  $D$  as:

$$x = \frac{w}{D} \quad (2)$$

If  $w = D$ , the doped region covers the full width of the thin film, and the memristor is in ON state and vice versa.

Other types of switches such as Flash, e-fuse, and anti-fuse can also be used to form a programmable routing layer. However, the configuration of these switches requires higher voltage compared to memristor switches which result in higher power consumption during configuration. Also, configuration time is larger than the one for memristor switches. Moreover, these switches are larger than memristor switches.



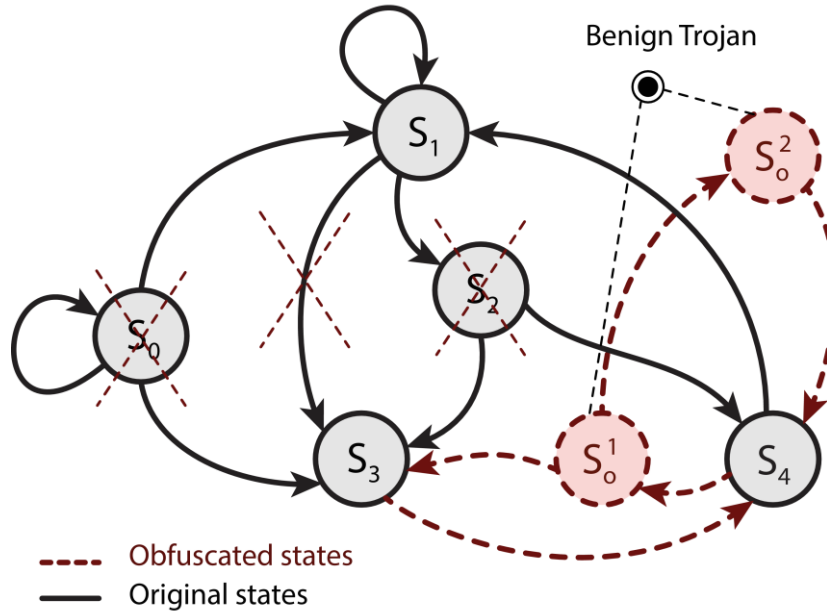


Figure 5.4. Example of original and obfuscated STG. Uncertain interconnections between selected nodes obscure the original STG and hide the rare events.

The effect of replacing several routing tracks with a layer of nanowires and configurable switches can be further explained by an example shown in Fig. 5.4. The figure symbolically illustrates the State Transition Graph (STG) of a circuit before and after netlist obfuscation. The part of the graph depicted in black belongs to the original circuit with completely routed interconnections. Assume that a set of connected nets are carefully selected from the netlist and for each pair of connected nets the permanent routing interconnecting wires are replaced with a pair of crossing nanowires and a reconfigurable memristor switch at the intersection of the nanowires. The crossbar structure of the nanowires allows the possibility of forming arbitrary connection between any source and drain net pairs.

The switches are programmed later at the design house to form the remaining required connections of the routing interconnect. As a result, the full routing map of the IC is not exposed to the foundry with the possibility of malicious activities at the time of

fabrication. Without having prior knowledge about the final ON/OFF state of the memristor switches it is extremely hard to extract either the correct netlist or the original STG of the circuit. Furthermore, any random guess about the correct configuration of the switches by an adversary may result in a different STG which is partially different from that of the correctly routed circuit. This may include removing several correct states, adding several states not reachable in the original STG, and adding/removing some of the transitions between states that can be detected in the test phase.

Figure 5.4 also shows an example of possible STG changes caused by an incorrect configuration setting of the switches. As shown in Fig. 5.4, two states along with their respective state transitions which originally belonged to the unreachable state space are now added to the set of reachable states. Moreover, states  $S_0$  and  $S_2$  are removed from the set of reachable states. Also, any changes in the netlist of the circuit may result in never satisfying one or several transition conditions as in the case with the state transition from  $S_1$  to  $S_3$ .

As discussed earlier, an intelligent adversary would typically be interested in finding rare triggering events. One of the most important outcomes of the circuit's functional obscurity is the ability to hide rare events. Getting confined in the modified STG would result in node probability estimations that significantly deviate from that of the original circuit. Similarly, changes in the functional behavior of the circuit caused by netlist obfuscation would mislead the adversary in finding fewer observable nodes in an attempt to use as payloads. Another direct result stemming from an alteration of the reachable state set is that those potential Trojans whose malicious functionality depends on the

temporarily reachable states will not be activated after a correct configuration of the switches as those states are not reachable in the correct operating mode of the circuit.

To increase the probability of hiding rare conditions, candidate nets should be selected in a way that strongly affects the signal probability of poorly controllable/ accessible nodes in the circuit. Intuitively, the more pairs of candidate nets are selected from the synthesized netlist the higher level of obfuscation can be achieved. While the task of replacing all routing tracks with a single grid of crossing nanowires might be formidable due to density limitations, a more realistic opportunity lies in selecting those interconnections that have the most radical effects on the rare conditions, namely less controllable/accessible nodes. Those nodes can be connected using network clustering to deprive the attackers of the knowledge of the most vulnerable nets. Another key factor that needs to be considered during selecting these nets is testability. The sub-circuits have to be designed in such a way that they can later be tested separately.

#### ***a) Netlist Clustering***

The most vulnerable nets can be connected using this method to ensure that an attacker does not know the key netlists to execute an attack. Furthermore, the circuit can be divided into different blocks or clusters as in [35] where each block can then be secured separately. The objective of clustering the circuit's netlist into sub-circuits is threefold. First, only the routing tracks between clusters are selected to be configurable because it is not feasible to make all the routing tracks programmable as mentioned earlier. Second, instead of testing the whole circuit, each cluster is tested separately which improves the test quality. Third, detection of hardware Trojans inserted in sub-circuits requires much less effort compared with detection of those inserted in the original

circuit with billions of gates. It is true that even after netlist clustering, the number of gates in a single sub-circuit may be numerous but the sub-circuit becomes easier to test due to the ease of access to its circuitry.

Conventional circuit partitioning techniques in VLSI design only optimize the design constraints including area, delay, and power consumption which can reveal information and undermine the security of the circuit. Partitioning methods have been proposed in the literature [36], [37] that consider security metrics while incurring cost overheads. Secure partitioning methods choose nets to hide them from an untrusted foundry. The goal of these methods is to provide the required level of security with minimal performance degradation and cost overhead. Partitioning techniques have also been proposed to facilitate hardware Trojan detection [38]–[40] or obfuscate the circuit to complicate hardware Trojan insertion [41].

**a) *Proposed Clustering Method:*** To apply the proposed hardware Trojan prevention technique on a circuit, first the circuit netlist at the gate level is clustered into groups of smaller netlists. Then, the layout of each cluster is designed. Finally, clusters are connected through the reconfigurable memristive switches. The designers/test engineers are the only people that know the correct configurations of the switches.

Since the objective is to hide the rare events, the proposed clustering technique at first finds the nets with low switching probabilities or low observability/controllability. In the second step, the circuit netlist is clustered so that the connections between the clusters are composed of the nets found at the first step.

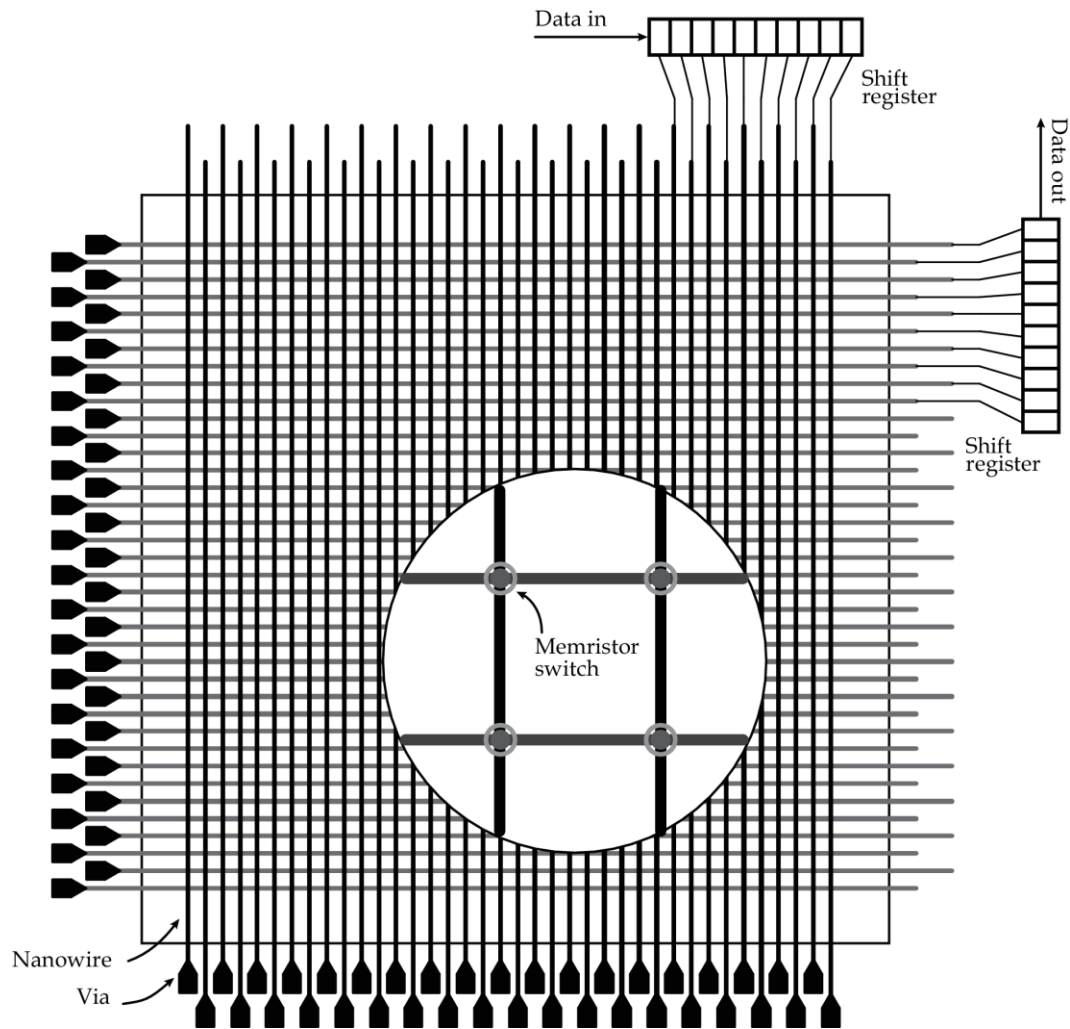


Figure 5.5. The grids of crossing nanowires that are configured by memristive switches using ‘Via’ pins. Shift registers are used as boundary scan registers for testing the clusters.

The proposed clustering method prioritizes security over hardware optimization. The clustering method finds the minimum speed, area, and power consumption requirements and does not optimize these constraints further since security constraints are more important. Therefore, the secure clustering technique prevents proximity attacks. Two more constraints listed below are also considered by the proposed clustering technique:

1. The cut-size is bounded by the number of reconfigurable routing switches.

2. The number of input and output signals for each cluster is bounded by the maximum number of boundary scan cells defined for testing clusters. The boundary scan cells are routed by reconfigurable memristor switches to the cluster under test.

### ***b) Testability***

The proposed architecture is tested cluster by cluster. The test mechanism for a cluster (sub-circuit) is provided by boundary scan registers as shown in Fig. 5.5, which illustrates the grids of crossing nanowires that are configured by memristive switches using ‘Via’ pins. One cluster at a time can be tested through boundary scan registers. Inputs and outputs of the cluster under test are connected to the input and output boundary registers by proper configuration of the memristor switches.

Testing the circuit through its sub-circuits facilitates the testing process. Intermediate signals of the whole circuit become the primary inputs/outputs of a sub-circuit which are accessible by boundary registers during the test phase. This improves the controllability/observability of the signals inside the circuit. Higher fault coverage can be achieved with a smaller number of test vectors for each sub-circuit. As sub-circuits are connected by the nanowire crossbar structure, testing the connection between them can be performed by testing the memristor crossbar architecture.

### ***B Proposed Design Flow Based on the Hardware Trojan Prevention Method***

For utilizing the proposed Hardware Trojan prevention technique in the digital design process, the standard design flow requires some modifications. Figure 5.6 illustrates the proposed design flow. Blocks with red dashed line border present changes applied to the

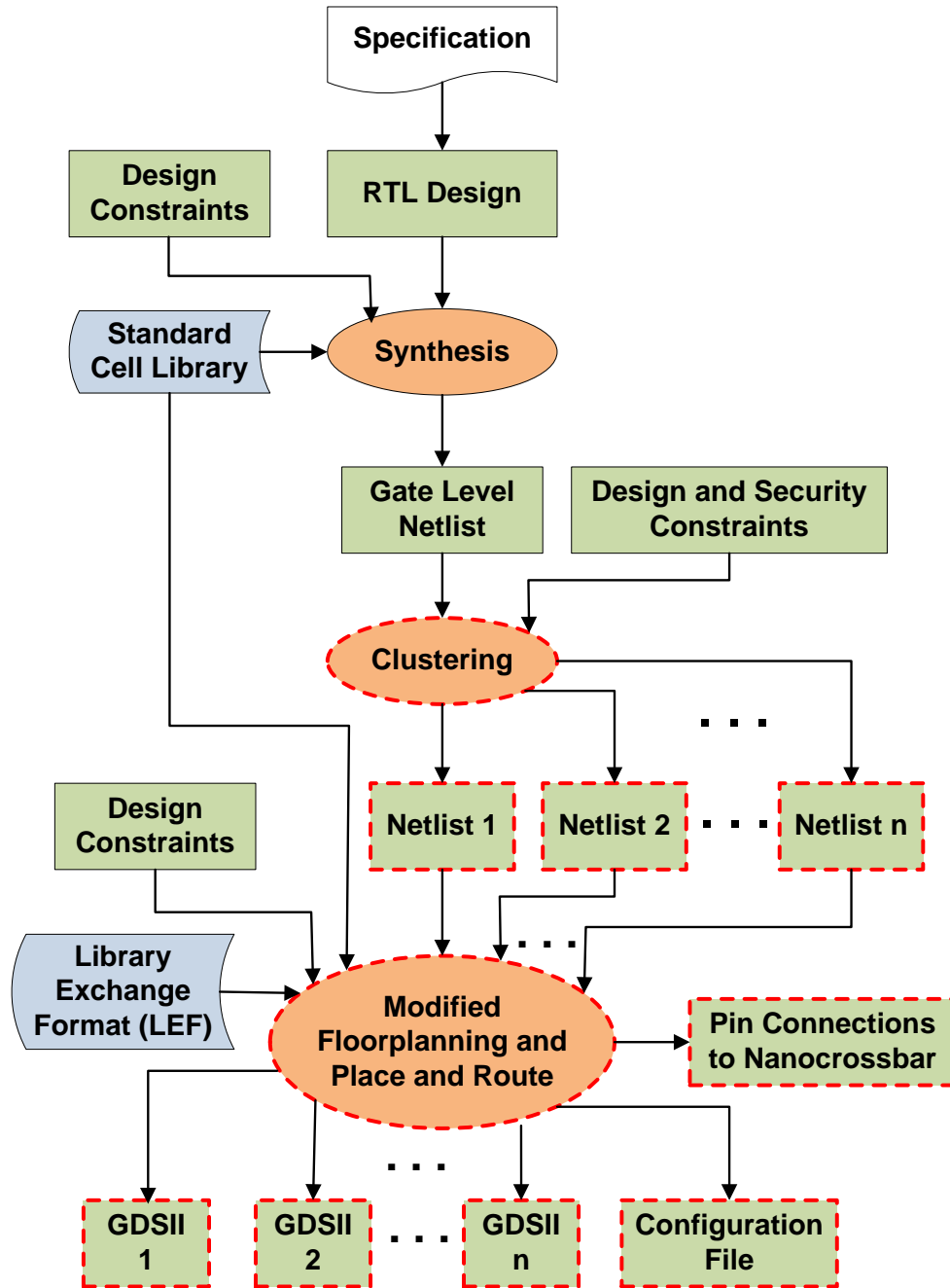


Figure 5.6. The proposed design flow based on the presented Hardware Trojan and IP piracy prevention technique.

standard design flow. The clustering operation accepts the circuit's netlist, and design and security constraints defined by the designer and generates  $n$  clusters of gate-level netlists. The number of clusters ( $n$ ) is determined based on the security level and design constraints.

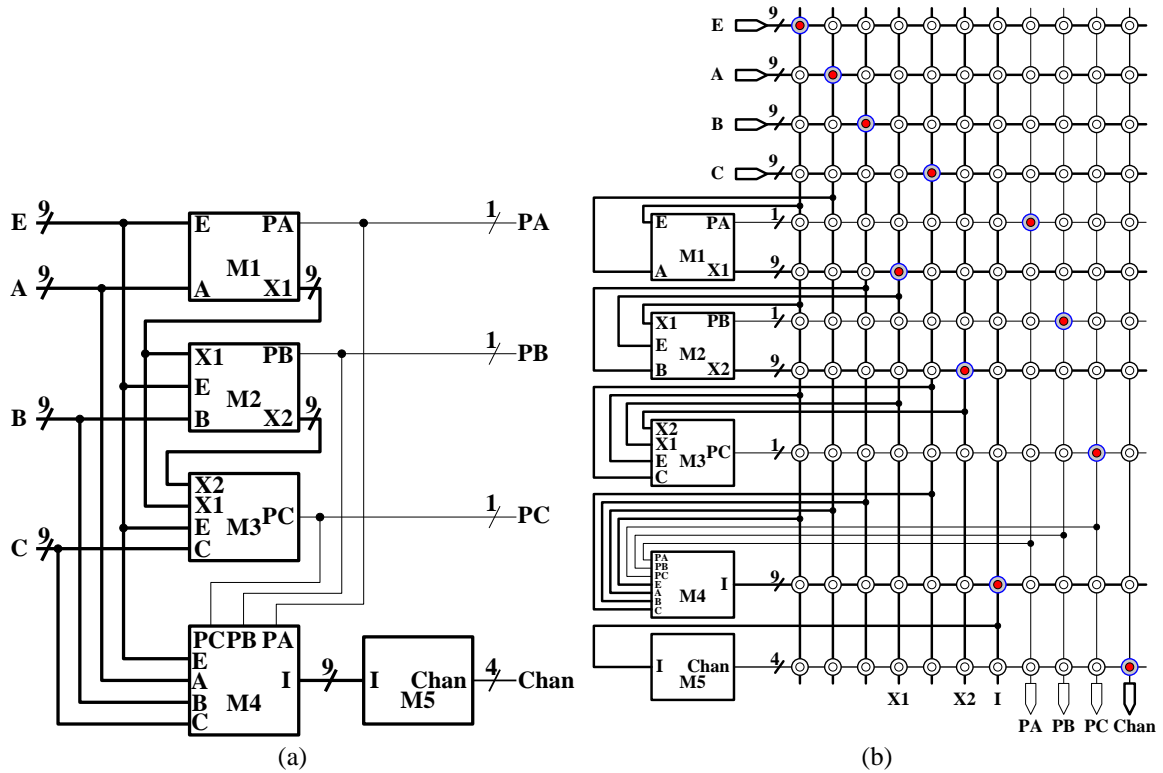


Figure 5.7. (a) Block diagram of ISCAS '85 C432 Circuit (b) The netlist is divided into five clusters. Connections between clusters are realized with memristor switches through nanocrossbar structure. Memristor switches in the ON state and OFF state are presented by blue and white circles, respectively.

The netlists are placed and routed separately, and their layouts are generated which are presented as GSDII files in Fig. 5.6. The “Placement and Routing” tool also creates the routing tracks from the input/output pins of the generated layouts to the nano-crossbar structure and a configuration file. GSDII files and the file containing routing track layers between layouts and the nano-crossbar switches are shipped to the factory for chip fabrication. The configuration file is only accessible by in-house designers and it is used to configure the programmable routing layers before the final deployment of the chip.



### ***C Implementation of Proposed Hardware Trojan Prevention Technique in ISCAS '85 Benchmark Circuit, C432***

The proposed hardware Trojan prevention method was implemented in ISCAS '85 Benchmark Circuit, C432, a 27-channel interrupt controller. The interrupt controller's block diagram is shown in Fig. 5.7 (a). The netlist is divided into 5 clusters (M1-M5). The complete structure of the interrupt controller, after rerouting using the memristive crossbar structure, is shown in Fig. 5.7 (b). The connections among clusters are realized by a nano-crossbar architecture with memristor switches. The switches are presented with circles and blue circles show that the vertical and the horizontal wires are connected. As shown in Fig. 5.7, outputs of clusters and primary inputs are connected to horizontal nanowires while inputs of clusters and primary outputs are connected to the vertical ones.

### ***D Security Analysis of the Proposed Technique***

To analyse the security of the proposed technique, let us assume that the attacker is in an untrusted foundry that fabricates the circuit, and they do not know the function of the circuit. The attacker's goal is to find the correct configuration of the reprogrammable routing layer to connect the sub-circuits correctly and thus gain the knowledge needed to insert a stealthy trojan. Following are some clues that can help the attacker to achieve the goal:

1. Memristor switches and the crossbar structure of the switches guide the attacker to the possibility of programmable routing.
2. Using the crossbar structure, the attacker can apply high or low voltages to the "Vias" as shown in Fig. 5.5 to configure the switches. For a crossbar of  $n$

switches, there exist a total of  $2^n$  possible configurations. The number of switches should be large enough to ensure the required level of security.

The use of a memristor switch can add some extra layer of obfuscation to the circuit. The extent of the doped region and hence the resistance of the memristor depends on the voltage applied to the via. So, some of the resistors needed in the original circuit can be replaced by memristors of the crossbar and those vias can be biased to a certain voltage to reflect that resistance. That way, unmasking the original purpose of the device becomes more challenging as the vias can have any number of voltage levels between 0 and 1 resulting in much more than  $2^n$  possible configurations. It also reduces the power requirement of the original circuit as memristors consume much less area and power compared to its CMOS counterpart [42]. The concept can be supported mathematically. The change of the state variable can be depicted as:

$$\frac{dx}{dt} = \frac{\mu_v R_{ON}}{D^2} i(t) \quad (3)$$

where  $\mu_v$  is the electron mobility. Thus, the state variable,  $x(t)$  can be rewritten as:

$$x(t) = \mu_v \frac{R_{ON}}{D^2} q(t) \quad (4)$$

and equation (1) becomes:

$$M(x) = \left[ \mu_v \frac{R_{ON}^2}{D^2} q(t) + R_{OFF} \left( 1 - \mu_v \frac{R_{ON}}{D^2} q(t) \right) \right] \quad (5)$$

For the memristors used as switches,  $R_{ON} \ll R_{OFF}$  and the resistance of the memristor can be calculated from:

$$M(x) = R_{OFF} \left( 1 - \mu_v \frac{R_{ON}}{D^2} q(t) \right) \quad (6)$$

As evident from equation 6, the resistance of the memristor varies based on the charge, and hence, the voltage supplied to the via, which can be considered for replacing the resistors of the original circuit.

#### 5.4 SIMULATION RESULTS AND COMPARISON

The effect of clustering on the cost overhead and security is emphasized by the netlist of the 27-channel interrupt controller with five clusters in Fig. 5.7 (b). The 9-bit data streams are shown as a bus bar in the figure. Clustering can improve security since it conceals the correct connections among sub-circuits. The fact that the wrong combinations generate some form of output makes it very difficult to obtain the actual functionality of the circuit without having any idea about the proper netlist. In the worst case, an adversary should try all possible routes among clusters to find the correct configuration. The phenomenon can be described by estimating the total number of possible connections among sub-circuits for a less complicated scenario, where each output of one cluster can only be connected to one input of another cluster or itself. Let  $n$  be the number of sub-circuits and  $m_i$  and  $o_i$  denote the number of inputs and outputs of each cluster, respectively. The total number of possible configurations is  $(\sum_{i=1}^n m_i)! = (\sum_{i=1}^n o_i)!$ . For example, for a circuit divided into ten sub-circuits with five inputs and five outputs each, the total number of configurations is  $50!$ . The larger the possible configurations, the more difficult it is for the adversary to find the correct configuration. The circuit of Fig. 5.7 (b) contains 4900 ( $70 \times 70$ ) reconfigurable switches. The security of the circuit can be further enhanced by increasing the number of programmable switches

or by increasing the number of clusters, which can be realized by dividing the circuit of each cluster into multiple smaller clusters. Besides, clustering the circuit into smaller sub-circuits improves the detection of inserted hardware Trojans and facilitates the test process. On the other hand, each switch increases the power and delay overhead. So, a balance needs to be maintained between the security and the overhead. To observe the effect of a memristor switch on the routing path of a circuit, a spice model was developed following the model proposed by Chang et al [43]. The memristor equations are defined as [43]:

$$I(t) = (1 - x(t))\alpha[1 - e^{-\beta V(t)}] + x(t)\gamma \sinh(\delta V(t)) \quad (7)$$

$$\frac{dx}{dt} = \gamma[e^{\eta_1 V(t)} - e^{-\eta_2 V(t)}] \quad (8)$$

where equation 7 is the  $I$ - $V$  relation representing the Schottky barrier between the oxide layer and the bottom electrode by the first term, and the tunnelling through the MIM junction by the second term. The ion migration and hence the conductivity of the device is determined by the state variable  $x(t)$ , which has a value within the range of 0 and 1. The parameters  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$ ,  $\eta_1$ , and  $\eta_2$  are all determined by material properties such as the barrier height for Schottky barrier and tunnelling, the depletion width in the Schottky barrier region, the effective tunnelling distance in the conducting region, and interface effects.

The parameters were considered carefully to obtain a low resistance in the ON mode and relatively high resistance in the OFF mode so that the device can be used as a switch.

```

**** LTspice code for metal oxide memristors ****
* Connections:
* TE: Top electrode
* BE: Bottom electrode

*****

.SUBCKT memristor TE BE

*****
* Parameters:
* alpha:      Prefactor for Schottky barrier
* beta:       Exponent for Schottky barrier
* gamma:      Prefactor for tunneling
* delta:      Exponent for tunneling
* xmax:       Maximum value of state variable
* xmin:       Minimum value of state variable
* lambda:     State variable multiplier
* eta1, eta2: State variable exponential rates
* tau:        Diffusion coefficient
*****

.param alpha=0.5e-6 beta=0.5 gamma=5e-6 delta=2
+ xmax=1 xmin=0 lambda=5 eta1=0.062 eta2=4 tau=10

.param cp={1}
Cpvar 1 0 {cp}

*Rate equation considering the diffusion effect
Gx 0 1 value={trunc(V(TE,BE),cp*V(1))*lambda*(
+etal*sinh(eta2*V(TE,BE))-cp*V(1)/tau)}

*rate equation without the diffusion effect
Gx 0 1 value={trunc(V(1,2),cp*V(1))*lambda*(
+etal*sinh(eta2*V(1,2)))}
.ic V(1) = 0.0

*****
*auxiliary functions to limit the range of w
.func sign2(var) {(sgn(var)+1)/2}
.func trunc(var1,var2) {sign2(var1)*sign2(xmax-
+var2)+sign2(-var1)*sign2(var2-xmin)}
*****
*Output:
Gw TE BE value={(1-cp*V(1))*alpha*(1-exp(-beta*
+V(TE,BE)))+(cp*V(1))*gamma*sinh(delta*V(TE,BE))}
.ENDS memristor

```

Figure 5.8. Modified LTspice code for memristor inspired by the model proposed by Chang et al. in [37].

The resulting spice model is shown in Fig. 5.8. The constants in the equations were defined as follows:  $\alpha = 5 \times 10^{-7}$ ,  $\beta = 0.5$ ,  $\gamma = 5 \times 10^{-6}$ ,  $\delta = 2$ ,  $\lambda = 5$ ,  $\eta_1 = 0.062$ ,  $\eta_2 = 4$ , and  $\tau = 10$ . The simulation results are shown in Fig. 5.9. Figure 5.9 (a) shows the  $I$ - $V$  curve with respect to time, where the prominent curvature in the current waveform is due to the hyperbolic sinusoidal term in the  $I$ - $V$  relationship of equation 7. As a result of this

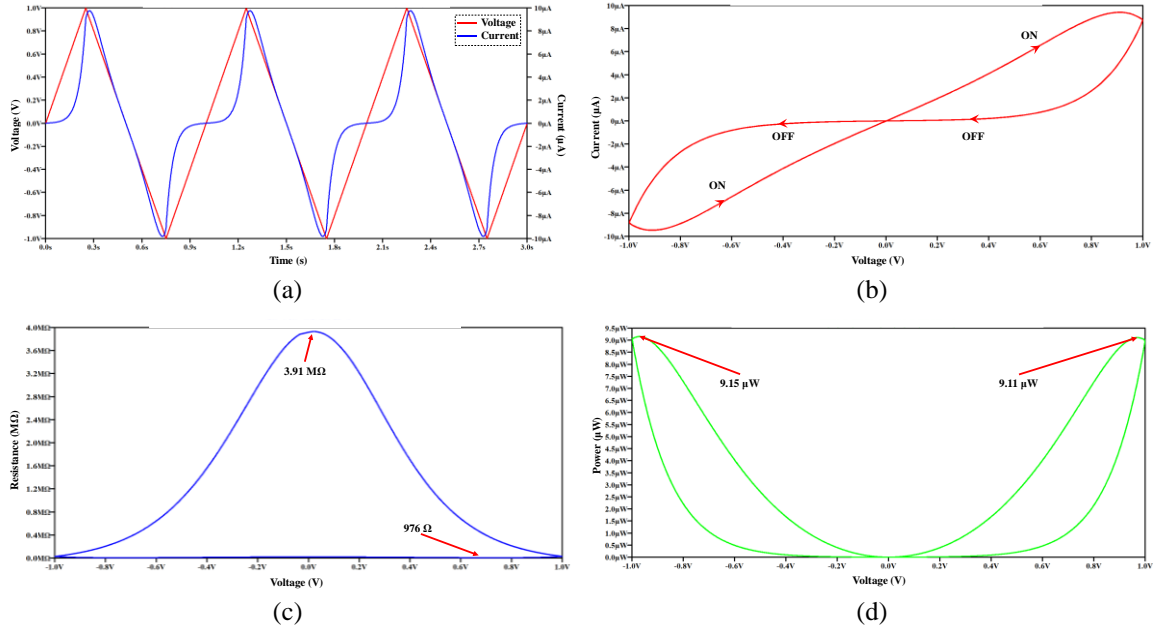


Figure 5.9. Simulation results for the memristor using a Spice model inspired by the model proposed by Chang et al [39]: (a) The variation of current due to the change of voltage (b) The pinched hysteresis loop created by the current as a function of voltage (c) Change of the resistance due to the change in voltage (d) Variation of power consumption due to the variation of voltage.

curvature, the resistance during the OFF state becomes very large, somewhere in the megaohm range. The pinched hysteresis loop of Fig. 5.9 (b) shows almost zero current in the OFF state due to the high resistance in that state as shown in Fig. 5.9 (c). The resistance of the ON state is considerably low. The resistance versus voltage waveform of Fig. 5.9 (c) signifies that the value of the resistance is a function of both the applied voltage and the previous state. These unique characteristics of a memristor can be manipulated to replace different resistances of the original design as was discussed before with the help of equation 6. The maximum power consumed by a memristor is around  $9 \mu\text{W}$ , which is shown in Fig. 5.9 (d). Clustering not only improves the circuit security but can also be used as an effective test-access-mechanism to the internal nodes of the circuit-under-test. With direct access to the clusters through the memristor crossbar, the observability and controllability of the circuit under test increases significantly. As a result, it is much easier to detect a HT at the test phase if it is inserted in a cluster, as less

TABLE 5.2. COMPARISON OF THE PROPOSED METHOD WITH SPLIT MANUFACTURING TECHNIQUES OF CIRCUIT432 IN TERMS OF OVERHEAD

Techniques	Delay Ratio	Power Ratio
[33]	2.14	1.92
[42]	1.48	1.97
Proposed	1.13	1.89

TABLE 5.3. DESIGN OVERHEAD OF THE PROPOSED TECHNIQUE

Circuit432	Delay	Power Consumption
Without Memristor Switches	1.7	1.77E-04
With Memristor Switches	1.915	3.36E-04

effort is required to activate Trojans in smaller sub-circuits than in the main circuit. Moreover, the proposed technique is resistant to proximity attack [44] as the gates and their connections are clustered randomly without considering spatial proximity.

Many split manufacturing techniques have been proposed in the literature to prevent hardware Trojan insertion. Authors in [36] proposed a split manufacturing technique that utilizes 3D IC technology. Some wires are lifted to a top layer and fabricated on a trusted foundry. In [45], an obfuscated Built-in self-authentication (BISA) method, which is a combination of split-manufacturing and BISA techniques, has been proposed that protects ICs from both IP theft and hardware Trojan insertion. Both techniques used the C432 circuit to find the overhead required by the corresponding method. Using the same benchmark, the method proposed here yields less power and delay compared to the other two techniques. The comparison is shown in Table 2. The effect of adding the memristor crossbar architecture to the design overhead is also observed and is shown in Table 3, both delay and power consumption increase negligibly due to the insertion of this architecture.

## 5.5 CONCLUSION

Untrusted design tools and fabrication facilities expose ICs to different types of attacks. Hardware Trojans are among the most important threats to the security of integrated circuits. In this paper, a new approach is proposed that prevents Hardware Trojan insertion and IP piracy during the IC fabrication process. This technique can be applied to any circuit without affecting the area or power consumption significantly. In the proposed method, the circuit is divided into sub-circuits which are connected to a network of memristor switches. As a result, the routing between the sub-circuits is obfuscated. The proposed method does not require split manufacturing and the entire circuit can be fabricated by one foundry, provided that it is capable of incorporating memristor devices into the CMOS IC, which can reduce the overall costs. The proposed clustering scheme can also be used as a test-access-mechanism to apply test vectors to the sub-circuits and observe their responses. Such direct access to the internal sub-circuit increases the testability considerably and assists the detection of possible Trojans inserted in the sub-circuits.

## ACKNOWLEDGMENT

The authors would like to thank the Natural Sciences and Engineering Research Council of Canada (NSERC) and CMC Microsystems for their support.

## REFERENCES

- [1] D. Byrne, B. Kovak, and R. Michaels, "Offshoring and price measurement in the semiconductor industry," in *Measurement Issues Arising from the Growth of Globalization*, Nov. 2009.



- [2] H. Li, Q. Liu, and J. Zhang, "A survey of hardware Trojan threat and defense," *Integr. VLSI J.*, vol. 55, pp. 426–437, Sep. 2016, doi: 10.1016/j.vlsi.2016.01.004.
- [3] K.G. Liakos, G.K. Georgakilas, S. Moustakidis, N. Sklavos, and F.C. Plessas, "Conventional and machine learning approaches as countermeasures against hardware trojan attacks," *Microprocess. Microsyst.*, vol. 79, pp. 103295, 2020, doi: 10.1016/j.micpro.2020.103295.
- [4] C. Gorman, "Counterfeit chips on the rise," in *IEEE Spectrum*, vol. 49, no. 6, pp. 16-17, June 2012, doi: 10.1109/MSPEC.2012.6203952.
- [5] D. Collins, "DARPA Trust in IC's Effort (BRIEFING CHARTS)" DEFENSE ADVANCED RESEARCH PROJECTS AGENCY ARLINGTON VA MICROSYSTEMS TECHNOLOGY OFFICE, 2007. [Online]. Available: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a503809.pdf>. [Accessed 05 April 2021].
- [6] "Holistic Approaches for Integrity of ICT-Systems | HINT Project | FP7 | CORDIS | European Commission" 22 April 2017 (Last Updated). [Online]. Available: <https://cordis.europa.eu/project/id/317930>. [Accessed 05 April 2021].
- [7] B. Halak, "Course on secure hardware design of silicon chips," in *IET Circuits, Devices & Systems*, vol. 11, no. 4, pp. 304-309, 7 2017, doi: 10.1049/iet-cds.2017.0028.
- [8] R. S. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," *2008 IEEE/ACM International Conference on Computer-Aided Design*, San Jose, CA, 2008, pp. 674-677, doi: 10.1109/ICCAD.2008.4681649.

- [9] R. S. Chakraborty and S. Bhunia, "Security against hardware Trojan through a novel application of design obfuscation," *2009 IEEE/ACM International Conference on Computer-Aided Design - Digest of Technical Papers*, San Jose, CA, 2009, pp. 113-116, doi: 10.1145/1687399.1687424.
- [10] S. Malik, G. T. Becker, C. Paar and W. P. Burleson, "Development of a Layout-Level Hardware Obfuscation Tool," *2015 IEEE Computer Society Annual Symposium on VLSI*, Montpellier, 2015, pp. 204-209, doi: 10.1109/ISVLSI.2015.118.
- [11] S. Mitra, H. - P. Wong and S. Wong, "The Trojan-proof chip," in *IEEE Spectrum*, vol. 52, no. 2, pp. 46-51, February 2015, doi: 10.1109/MSPEC.2015.7024511.
- [12] A. Baumgarten, A. Tyagi and J. Zambreno, "Preventing IC Piracy Using Reconfigurable Logic Barriers," in *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 66-75, Jan.-Feb. 2010, doi: 10.1109/MDT.2010.24.
- [13] A. Nejat, S.M.H. Shekarian, and M.S. Zamani, "A study on the efficiency of hardware Trojan detection based on path-delay fingerprinting," in *Microprocess. Microsyst.*, vol. 38, pp. 246–252., 2014, doi: 10.1016/j.micpro.2014.01.003.
- [14] P. Subramanyan, S. Ray and S. Malik, "Evaluating the security of logic encryption algorithms," *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC, 2015, pp. 137-143, doi: 10.1109/HST.2015.7140252.
- [15] K. Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan and Y. Jin, "AppSAT: Approximately deobfuscating integrated circuits," *2017 IEEE International*

- Symposium on Hardware Oriented Security and Trust (HOST)*, McLean, VA, 2017, pp. 95-100, doi: 10.1109/HST.2017.7951805.
- [16] K. Z. Azar et al., “SMT Attack: Next Generation Attack on Obfuscated Circuits with Capabilities and Performance Beyond the SAT Attacks”, *IACR Trans. on Cryptographic Hardware and Embedded Systems*, no. 1, pp. 97-122, 2019, doi: 10.13154/tches.v2019.i1.97-122.
- [17] S. Koteswara, C. H. Kim and K. K. Parhi, “Key-Based Dynamic Functional Obfuscation of Integrated Circuits Using Sequentially Triggered Mode-Based Design,” in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 79-93, Jan. 2018, doi: 10.1109/TIFS.2017.2738600.
- [18] K. Juretus and I. Savidis, “Importance of Multi-parameter SAT Attack Exploration for Integrated Circuit Security,” *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Chengdu, 2018, pp. 366-369, doi: 10.1109/APCCAS.2018.8605696.
- [19] S. Chen and R. Vemuri, “Exploiting Proximity Information in a Satisfiability Based Attack Against Split Manufactured Circuits,” *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, McLean, VA, USA, 2019, pp. 171-180, doi: 10.1109/HST.2019.8740833.
- [20] A. Shabani and B. Alizadeh, “PMTP: A MAX-SAT-Based Approach to Detect Hardware Trojan Using Propagation of Maximum Transition Probability,” in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 1, pp. 25-33, Jan. 2020, doi: 10.1109/TCAD.2018.2889663.

- [21] Q. -L. Nguyen, E. Valea, M. -L. Flottes, S. Dupuis and B. Rouzeyre, "A Secure Scan Controller for Protecting Logic Locking," *2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, Napoli, Italy, 2020, pp. 1-6, doi: 10.1109/IOLTS50870.2020.9159730.
- [22] S. Hamdioui et al., "Memristor for computing: Myth or reality?," *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, Lausanne, Switzerland, 2017, pp. 722-731, doi: 10.23919/DATE.2017.7927083.
- [23] L. Chua, "Memristor-The missing circuit element," in *IEEE Transactions on Circuit Theory*, vol. 18, no. 5, pp. 507-519, September 1971, doi: 10.1109/TCT.1971.1083337.
- [24] J. Borghetti, G. S. Snider, P. J. Kuekes, J. J. Yang, D. R. Stewart, and R. S. Williams, "Memristive switches enable stateful logic operations via material implication," *Nature*, vol. 464, no. 7290, pp. 873–876, 2010, doi: 10.1038/nature08940.
- [25] S. H. Jo, T. Chang, I. Ebong, B. B. Bhadviya, P. Mazumder, and W. Lu, "Nanoscale memristor device as synapse in neuromorphic systems," *Nano Lett.*, vol. 10, no. 4, pp. 1297–1301, 2010, doi: 10.1021/nl904092h.
- [26] S. Tanachutiwat, M. Liu and W. Wang, "FPGA Based on Integration of CMOS and RRAM," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 11, pp. 2023-2032, Nov. 2011, doi: 10.1109/TVLSI.2010.2063444.
- [27] K.-H. Kim *et al.*, "A functional hybrid memristor crossbar-array/CMOS system for data storage and neuromorphic applications," *Nano Lett.*, vol. 12, no. 1, pp. 389–395, 2012.

- [28] P. Lin, S. Pi, and Q. Xia, “3D integration of planar crossbar memristive devices with CMOS substrate,” *Nanotechnology*, vol. 25, no. 40, p. 405202, 2014.
- [29] Q. Xia *et al.*, “Memristor- CMOS hybrid integrated circuits for reconfigurable logic,” *Nano Lett.*, vol. 9, no. 10, pp. 3640–3645, 2009.
- [30] C. Yakopcic, R. Hasan, and T. M. Taha, “Hybrid crossbar architecture for a memristor based cache,” *Microelectronics J.*, vol. 46, no. 11, pp. 1020–1032, 2015, doi: 10.1016/j.mejo.2015.08.015.
- [31] W. Lu, K. Kim, T. Chang and S. Gaba, “Two-terminal resistive switches (memristors) for memory and logic applications,” *16th Asia and South Pacific Design Automation Conference (ASP-DAC 2011)*, Yokohama, 2011, pp. 217-223, doi: 10.1109/ASPDAC.2011.5722187.
- [32] F. Miao *et al.*, “Anatomy of a nanoscale conduction channel reveals the mechanism of a high-performance memristor,” *Adv. Mater.*, vol. 23, no. 47, pp. 5633–5640, 2011.
- [33] M. N. Kozicki, M. Balakrishnan, C. Gopalan, C. Ratnakumar and M. Mitkova, “Programmable metallization cell memory based on Ag-Ge-S and Cu-Ge-S solid electrolytes,” *Symposium Non-Volatile Memory Technology 2005.*, Dallas, TX, 2005, pp. 7 pp.-89, doi: 10.1109/NVMT.2005.1541405.
- [34] S. Pi, P. Lin, and Q. Xia, “Cross point arrays of 8 nm × 8 nm memristive devices fabricated with nanoimprint lithography,” *J. Vac. Sci. Technol. B, Nanotechnol. Microelectron. Mater. Process. Meas. Phenom.*, vol. 31, no. 6, p. 06FA02, 2013.
- [35] A. Sengupta, M. Ashraf, M. Nabeel and O. Sinanoglu, “Customized Locking of IP Blocks on a Multi-Million-Gate SoC,” *2018 IEEE/ACM International Conference*

- on Computer-Aided Design (ICCAD)*, San Diego, CA, 2018, pp. 1-7, doi: 10.1145/3240765.3243467.
- [36] F. Imeson, A. Emtenan, S. Garg, and M. Tripunitara, “Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation,” in *22nd USENIX Security Symposium (USENIX Security 13)*, 2013, pp. 495–510.
- [37] Y. Xie, C. Bao, and A. Srivastava, “Security-aware design flow for 2.5 D IC technology,” in *Proceedings of the 5th International Workshop on Trustworthy Embedded Devices*, 2015, pp. 31–38.
- [38] B. Lippmann *et al.*, “Verification of physical designs using an integrated reverse engineering flow for nanoscale technologies,” *Integration*, vol. 71, pp. 11–29, 2020.
- [39] K. M. Abdellatif, C. Cornesse, J. Fournier, and B. Robisson, “New partitioning approach for hardware Trojan detection using side-channel measurements,” in *International Symposium on Applied Reconfigurable Computing*, 2016, pp. 171–182.
- [40] Y. Cao, C. Chang and S. Chen, “A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection,” in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2220-2231, Dec. 2014, doi: 10.1109/TIFS.2014.2360432.
- [41] Y. Cheng, Y. Wang, H. Li and X. Li, “A Similarity Based Circuit Partitioning and Trimming Method to Defend against Hardware Trojans,” *2015 IEEE Computer*

- Society Annual Symposium on VLSI*, Montpellier, 2015, pp. 368-373, doi: 10.1109/ISVLSI.2015.93.
- [42] S. S. Sarwar, S. A. N. Saqueeb, F. Quaiyum and A. B. M. H. Rashid, “Memristor-Based Nonvolatile Random Access Memory: Hybrid Architecture for Low Power Compact Memory Design,” in *IEEE Access*, vol. 1, pp. 29-34, 2013, doi: 10.1109/ACCESS.2013.2259891.
- [43] T. Chang, S. H. Jo, K. H. Kim, P. Sheridan, S. Gaba, and W. Lu, “Synaptic behaviors and modeling of a metal oxide memristive device,” *Appl. Phys. A Mater. Sci. Process.*, vol. 102, no. 4, pp. 857–863, 2011, doi: 10.1007/s00339-011-6296-1.
- [44] Y. Wang, P. Chen, J. Hu, G. Li and J. Rajendran, “The Cat and Mouse in Split Manufacturing,” in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 5, pp. 805-817, May 2018, doi: 10.1109/TVLSI.2017.2787754.
- [45] Q. Shi, K. Xiao, D. Forte, and M. M. Tehranipoor, “Securing split manufactured ICs with wire lifting obfuscated built-in self-authentication,” *Proc. ACM Gt. Lakes Symp. VLSI, GLSVLSI*, vol. Part F1277, pp. 339–344, 2017, doi: 10.1145/3060403.3060588.

---

## Chapter 6

---

### CONCLUSION AND FUTURE WORK

---

Hardware Trojan analysis and countermeasures have gained considerable interest in recent years due to the increased vulnerability of hardware security. Many companies are adopting the fabless fly-light model. A hardware Trojan is commonly designed to serve a specific purpose under a particular condition that makes its detection a difficult task. A comprehensive solution to detect all types of hardware Trojan is far from reach. A more practical approach is a design for hardware tests and security methods to prevent Trojan insertion in the first place. Among the many solutions in the literature, layout filling and layout manipulation are considered promising techniques to prevent Trojan insertion. In this work, two different layout filling methods together with a layout manipulation solution are presented.

In the first layout filling approach, the unused polysilicon layer is filled with microstrip inductive probes of minimum feature size to deny attackers accessing the active layer to insert a Trojan. As the polysilicon layer connects directly to the active layer, the only way to insert a Trojan is by removing a portion of the polysilicon layer. This removal will change the original circuit's signature and can be detected by an embedded readout circuit. Simulation results show that removing the polysilicon layer to



insert even a single library can affect the device signature. The results of Monte Carlo simulations indicate the solution robustness against deviations of circuit parameters.

In the second approach, a layout filling method is presented in which the unused die area is covered by on-chip magnetic probes using minimum feature polysilicon and metal wires. The advantage of this method is the ability to detect routing manipulations. This method can occupy the entire unused layers and can provide a 100% occupation ratio. The proposed method shows a strong performance even for 3D ICs and can be used to detect Trojans in 3D ICs during die stacking or TSV bonding stages.

For future work, the probes' design in the presented layout filling methods can be optimized for power, area, and speed to improve the performance. Manual filling of the unused chip areas will be time-consuming for large circuits. An auto-routing software tool can be developed to automatically modify the original routing to ensure protection against Trojan injection while optimizing the routing for power consumption and speed.

The third approach is a type of layout manipulation where the original circuit is divided into sub-circuits connected through a network of memristor switches. In this method, the routings between sub-circuits are obfuscated. As such, the fabrication foundry will not have access to the complete netlist and functionality of the final circuit. Another advantage of this method over conventional obfuscation methods is the support for fabrication in one foundry regardless of the trust level and without the need to split manufacturing, which can reduce the fabrication costs. This method can facilitate the testing process as direct access to sub-circuits is provided. Such direct access to the

internal circuits increases the testability considerably and helps detect Trojans in sub-circuits.








The unique properties of memristors can be used to replace some resistors in the main circuit to mask its functionality. For future work, a combination of crossbars and resistors swapped with memristors can be utilized to obfuscate circuits and protect them against unauthorized alteration. An attacker has to find a voltage between the on and off state biasing voltages to successfully wage an attack. The search for correct biasing becomes quite challenging if several resistors in the main circuit are replaced with memristors.

# APPENDICES

## Appendix A – LIST OF PAPERS DURING PH.D. THAT ARE NOT RELATED TO THE DISSERTATION TOPIC


Title of the Publication	Publication Type
<p><b>T. M. Supon</b>, I. I. Basith, E. Abdel-Raheem and R. Rashidzadeh, “Efficient integrated bus coding scheme for low-power I/O,” <i>AEU - International Journal of Electronics and Communications</i>, vol. 82, pp. 30-36, December, 2017.</p>	<p>Journal Article</p>
<p><b>T. M. Supon</b> and R. Rashidzadeh, “A phase locking test solution for MEMS devices,” <i>2017 22nd IEEE European Test Symposium (ETS)</i>, Limassol, 2017, pp. 1-6.</p>	<p>Conference Paper</p>
<p>R. Rashidzadeh, E. Jedari, <b>T. M. Supon</b> and V. Mashkovtsev, “A DLL-based test solution for through silicon via (TSV) in 3D-stacked ICs,” <i>2015 IEEE International Test Conference (ITC)</i>, Anaheim, CA, 2015, pp. 1-9.</p>	<p>Conference Paper</p>
<p>I. I. Basith, <b>T. M. Supon</b>, E. Abdel-Raheem and R. Rashidzadeh, “Comparative study on bus-coding schemes and improvement on SINV coding,” <i>2016 28th International Conference on Microelectronics (ICM)</i>, Giza, 2016, pp. 17-20.</p>	<p>Conference Paper</p>
<p>H. Rashidzadeh, P. S. Kasargod, <b>T. M. Supon</b>, R. Rashidzadeh and M. Ahmadi, “Energy harvesting for IoT sensors utilizing MEMS technology,” <i>2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)</i>, Vancouver, BC, 2016, pp. 1-4.</p>	<p>Conference Paper</p>
<p>M. Alamgir, I. I. Basith, <b>T. Supon</b> and R. Rashidzadeh, “Improved bus-shift coding for low-power I/O,” <i>2015 IEEE Int. Symposium on Circuits and Systems (ISCAS)</i>, Lisbon, 2015, pp. 2940-2943.</p>	<p>Conference Paper</p>

## Appendix B – PERMISSION TO REUSE CONTENT



Home    Help    Email Support    Sign in    Create Account

### Hardware Trojan Prevention Through Limiting Access to the Active Region



**Requesting permission to reuse content from an IEEE publication**

**Conference Proceedings:**  
2019 14th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS)

**Author:** Tareq Muhammad Supon

**Publisher:** IEEE

**Date:** April 2019

*Copyright © 2019, IEEE*

### Thesis / Dissertation Reuse

**The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:**

*Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:*

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

*Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:*

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to [http://www.ieee.org/publications\\_standards/publications/rights/rights\\_link.html](http://www.ieee.org/publications_standards/publications/rights/rights_link.html) to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#) [CLOSE WINDOW](#)

©2020 Copyright - All Rights Reserved | [Copyright Clearance Center, Inc.](#) | [Privacy statement](#) | [Terms and Conditions](#)  
Comments? We would like to hear from you. E-mail us at [customer@copyright.com](mailto:customer@copyright.com)



### On-Chip Magnetic Probes for Hardware Trojan Prevention and Detection

**Author:** Tareq Muhammad Supon

**Publication:** Electromagnetic Compatibility, IEEE Transactions on

**Publisher:** IEEE

**Date:** Dec 31, 1969

*Copyright © 1969, IEEE*

#### Thesis / Dissertation Reuse

**The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:**

*Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:*

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

*Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:*

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to [http://www.ieee.org/publications\\_standards/publications/rights/rights\\_link.html](http://www.ieee.org/publications_standards/publications/rights/rights_link.html) to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#)

[CLOSE WINDOW](#)

---

## VITA AUCTORIS

---

NAME: Tareq Muhammad Supon

PLACE OF  
BIRTH: Barisal, Bangladesh

YEAR OF BIRTH: 1984

EDUCATION: B.Sc. in Electrical and Electronic Engineering  
Ahsanullah University of Science and Technology, Dhaka,  
Bangladesh, 2007

M.Eng. in Electrical and Computer Engineering  
University of Windsor, Windsor, ON, Canada, 2010

MASc in Electrical and Computer Engineering  
University of Windsor, Windsor, ON, Canada, 2012

Ph.D. in Electrical and Computer Engineering  
University of Windsor, Windsor, ON, Canada, 2021

## WORK EXPERIENCE

---

<b>Research Assistant</b> University of Windsor Windsor, ON, Canada Jan 2014 – Current	<ul style="list-style-type: none"><li>• Conducting research on different types of hardware security concerns and solutions</li><li>• Developing new techniques for hardware testing and authentication</li></ul>
<b>Graduate Assistant</b> University of Windsor Windsor, ON, Canada Jan 2014 – Current	<ul style="list-style-type: none"><li>• Attend scheduled labs and assist the corresponding instructor with in-class activities</li><li>• Evaluate assignments, lab reports, and exams</li><li>• Assist with different queries of the students during the weekly office hours</li></ul>
<b>Apprenticeship</b> LandauGage Windsor, ON, Canada Nov 2015 – Feb 2016	<ul style="list-style-type: none"><li>• Design a laser assembly system to extract various features of a V-Groove pulley</li><li>• Compare the measurement results with the existing data to confirm the validity of the results obtained from the laser system</li></ul>
<b>Research Associate</b> University of Windsor Windsor, ON, Canada Sep 2012 – Dec 2013	<ul style="list-style-type: none"><li>• Designing a 77 GHz radar module using LTCC (Low Temperature Co-fired Ceramic) for automotive collision avoidance system.</li><li>• Collaborating with CMC (Canadian Microelectronics Corporation) and IMST (Institute of Mobile and Satellite Communication Techniques) to fabricate the device.</li><li>• Designing a test setup to test the fabricated device and carry out the testing at ARFSL (Advanced RF Systems Lab) at the University of Manitoba.</li><li>• Performing literature reviews, organizing reference materials and preparing a test report.</li></ul>
<b>Research Assistant</b> University of Windsor Windsor, ON, Canada Sep 2010 – Apr 2012	<ul style="list-style-type: none"><li>• Doing research on different types of analog/digital testing devices</li></ul>
<b>Graduate Assistant</b> University of Windsor Windsor, ON, Canada Sep 2010 – Apr 2012	<ul style="list-style-type: none"><li>• Attend scheduled labs and assist the corresponding instructor with in-class activities</li><li>• Evaluate assignments, lab reports, and exams</li><li>• Assist with different queries of the students during the weekly office hours</li></ul>

---

<b>Executive Engineer</b> Powermann Bangladesh Limited Dhaka, Bangladesh Jan 2009 – Jun 2009	<ul style="list-style-type: none"> <li>• Selling and installing transformers, generators, MDB/SDB box, ATS, etc.</li> <li>• Helping the customer with decommissioning of the transformer.</li> </ul>
<b>Lecturer</b> Ahsanullah University of Science and Technology Dhaka, Bangladesh Nov 2007 – Dec 2008	<ul style="list-style-type: none"> <li>• Delivering lectures on different courses including Electrical Circuits-I, Electronics-I, etc.</li> <li>• Conduct the lab sessions of corresponding courses and evaluate the students</li> <li>• Hold examinations and evaluate the students based on their performance</li> </ul>

## EDUCATION

<b>Ph.D. in Electrical Engineering</b> (Dec 2020)	University of Windsor, Windsor, ON, Canada Electrical and Computer Engineering
<b>MASc in Electrical Engineering</b> (Apr 2012)	University of Windsor, Windsor, ON, Canada Electrical and Computer Engineering Thesis: A PLL based built-in self-test for MEMS sensors
<b>M.Eng. in Electrical Engineering</b> (Sep 2010)	University of Windsor, Windsor, ON, Canada Electrical and Computer Engineering
<b>B.Sc. in Electrical Engineering</b> (Nov 2007)	Ahsanullah University of Science and Technology (AUST), Dhaka, Bangladesh Electrical and Electronic Engineering

## ACCOMPLISHMENTS

<b>MEMS Readout and Testing</b>	I have designed a readout and test circuitry using PLL technology for MEMS devices which reduces the effects of PVT variations. The paper was shortlisted as one of the top eight articles among more than two hundred papers for the best paper award.
<b>Fabrication and testing of two ICs</b>	During my Ph.D. and master's programs, I have successfully fabricated two different ICs using two different technologies (TSMC 180nm and 65nm). I have also tested both of those to make sure of their proper functioning.
<b>Long-Range Radar Package Design using LTCC</b>	I have designed the packaging of long-range millimeter-wave radar using LTCC (Low Temperature Co-fired Ceramic) process using ADS. This allowed the whole device to be housed within a 30×30×0.8 package while reducing the power loss.



---

## TECHNICAL SKILLS

---

- Design microelectronic circuits to perform IC security, authentication, and testing
  - Design RF / Analog circuits and VLSI / Mixed-Signal systems
  - MEMS DIB design using LTCC (Low Temperature Co-fired Ceramics)
  - Nano-electronic circuit design
  - Ability to understand and interpret any schematic diagram and reconstruct those in a circuit board with skillful soldering
  - Nano-electronic circuit design
  - Ability to understand and interpret any schematic diagram and reconstruct those in a circuit board with skillful soldering
- 

## INDUSTRY CAD TOOLS & PROGRAMMING LANGUAGES

---

- Cadence – Microelectronic circuit design and fabrication
  - Advanced Design System (ADS) – Microelectronic circuit design
  - COMSOL Multiphysics – 3D design of new transistor technologies
  - High Frequency Structure Simulator (HFSS) – Design of any 3D structure
  - IntelliSuite software – Total MEMS solutions
  - SIMON – Nano-electronic circuit design
  - LT-Spice – Simulation of any circuit netlist
  - AutoCAD – Mechanical design
  - MATLAB & Simulink – Mathematical modeling of any design
  - LabView – Systems engineering software for test, measurement, and control
  - Machine Vision Software by National Instruments – Analyzing and interpreting images captured in a computer
  - Assembly and C languages
- 

## AWARDS AND SCHOLARSHIPS

---

- Entrance Scholarship – *University of Windsor (2010 – 2012)*
  - Dean’s List of Honor – *Ahsanullah University of Science and Technology (2007)*
  - Merit Scholarship – *Ahsanullah University of Science and Technology (2003 – 2007)*
- 

## LEADERSHIP & PROFESSIONAL ACTIVITIES

---

- Secretary and Treasurer, Joint chapter of Circuits and Systems (CAS) & Computer Society (CS), IEEE University of Windsor, Canada (April 2015 – March 2018)
- Vice President (University Affairs), Graduate Student Society, University of Windsor, Canada (April 2014 – March 2015)

- Vice President (Academic Affairs), Graduate Student Society, University of Windsor, Canada (April 2011 – March 2012)
- Cofounder of IEEE AUST Student Branch
- IEEE active Member since 2005
- Reviewer of papers at the following conferences:
- ISCAS 2020, MWSCAS 2017
- Member, Quantum Foundation, Bangladesh, (September 2003 – June 2009)
- Student Representative in Senate, Academic Appeals Committee, University of Windsor, 2014-2015.
- Student Representative in Senate, APC committee, PDC committee, University of Windsor, 2011-2012.

## EXTRA-CURRICULAR ACTIVITIES

- A lifetime donor at the Quantum Foundation (Blood Donor Club), Bangladesh.
- A player of both the cricket and the football team of Ahsanullah University of Science and Technology, Bangladesh from January 2004 – November 2007.
- Cofounder of Ahsanullah University of Science and Technology (AUST) Science Club.

## PUBLICATIONS

### Journal Papers

- **T. M. Supon** and R. Rashidzadeh, “On-Chip Magnetic Probes for Hardware Trojan Prevention and Detection,” in *IEEE Trans. on Electromagnetic Compatibility*, doi: 10.1109/TEMPC.2020.3003728.
- **T. M. Supon**, M. Seyedbarhagh and R. Rashidzadeh, “A Method to Prevent Hardware Trojans Limiting Access to Layout Resources,” in *Microelectronics Reliability*. Review Requested.
- **T. M. Supon** and R. Rashidzadeh, “Hardware Trojan Prevention using Memristor Technology,” *Microprocessors and Microsystems*, Submitted.
- **T. M. Supon**, I. I. Basith, E. Abdel-Raheem and R. Rashidzadeh, “Efficient integrated bus coding scheme for low-power I/O,” *AEU - International Journal of Electronics and Communications*,
- **T. M. Supon**, K. Thangarajah, R. Rashidzadeh and M. Ahmadi, “A READOUT SOLUTION FOR MEMS SENSORS,” *Journal of Circuits, Systems, and Computers*, vol. 21, no. 6, pp. 1240014, 2012.

### Conference Proceedings

- **T. M. Supon**, M. Seyedbarhagh, R. Rashidzadeh and R. Muscedere, “Hardware Trojan Prevention Through Limiting Access to the Active Region,” *2019 14th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS)*, Mykonos, Greece, 2019, pp. 1-6.

- **T. M. Supon** and R. Rashidzadeh, “A phase locking test solution for MEMS devices,” *2017 22nd IEEE Euro. Test Symposium (ETS)*, Limassol, 2017, pp. 1-6.
  - I. I. Basith, **T. M. Supon**, E. Abdel-Raheem and R. Rashidzadeh, “Comparative study on bus-coding schemes and improvement on SINV coding,” *2016 28th International Conference on Microelectronics (ICM)*, Giza, 2016, pp. 17-20.
  - H. Rashidzadeh, P. S. Kasargod, **T. M. Supon**, R. Rashidzadeh and M. Ahmadi, “Energy harvesting for IoT sensors utilizing MEMS technology,” *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Vancouver, BC, 2016, pp. 1-4.
  - M. Alamgir, I. I. Basith, **T. Supon** and R. Rashidzadeh, “Improved bus-shift coding for low-power I/O,” *2015 IEEE Int. Symposium on Circuits and Systems (ISCAS)*, Lisbon, 2015, pp. 2940-2943.
  - R. Rashidzadeh, E. Jedari, **T. M. Supon** and V. Mashkovtsev, “A DLL-based test solution for through silicon via (TSV) in 3D-stacked ICs,” *2015 IEEE International Test Conference (ITC)*, Anaheim, CA, 2015, pp. 1-9.
  - **T. M. Supon**, K. Thangarajah, R. Rashidzadeh and M. Ahmadi, “A PLL based readout and built-in self-test for MEMS sensors,” *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Seoul, 2011, pp. 1-4.
  - I. I. Basith, **T. M. Supon**, A. Muhury, R. Rashidzadeh and M. Ahmadi, “Performance enhancement of single electron junction 1-bit full adder,” *2011 18th IEEE International Conference on Electronics, Circuits, and Systems*, Beirut, 2011, pp. 157-160.
-