

Mona Maghraby



بسم الله الرحمن الرحيم

مركز الشبكات وتكنولوجيا المعلومات

قسم التوثيق الإلكتروني



Mona Maghraby



جامعة عين شمس

التوثيق الإلكتروني والميكرو فيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
على هذه الأقراص المدمجة قد أعدت دون أية تغييرات





Cairo University

INTERNET OF THINGS SECURITY THREATS ANALYSIS

By

Mahmoud Maher El-Sayed Mohammed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Electronics and Communications Engineering

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2019

INTERNET OF THINGS SECURITY THREATS ANALYSIS

By
Mahmoud Maher El-Sayed Mohammed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Electronics and Communications Engineering

Under the Supervision of
Prof. Amin Mohamed Nassar

Professor of Electronics
Electronics and Electrical Communication
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2019

INTERNET OF THINGS SECURITY THREATS ANALYSIS

By
Mahmoud Maher El-Sayed Mohammed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Electronics and Communications Engineering

Approved by the
Examining Committee

Prof. Dr. Amin Mohamed Nassar, (Thesis Main Advisor)
Professor at the faculty of Engineering, Cairo University.

Prof. Dr. El-Sayed Mostafa Saad, (External Examiner)
Professor at the faculty of Engineering, Helwan university.

Dr. Mohamed Mohamed Ali El-Gazzar, (External Examiner)
Assistant professor at the faculty of Engineering, Arab Academy for
Science, Technology & Maritime Transport.

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2019



Engineer's Name: Mahmoud Maher El-Sayed
Date of Birth: 01/01/1990
Nationality: Egyptian
E-mail: Mahmoudmaher2011@gmail.com
Phone: 01128000719
Address: 2 Ahmed Abd El-Nabi st, Hadayek Helwan, Cairo
Registration Date: 01/10/2013
Awarding Date:/....../2019
Degree: Master of Science
Department: Electronics and Communications Engineering

Supervisors:

Prof. Amin Mohamed Nassar

Examiners:

Prof. Amin Mohamed Nassar (Thesis Main Advisor)
Professor at the faculty of Engineering, Cairo University.
Prof. El-Sayed Mostafa Saad (External examiner)
Professor at the faculty of Engineering, Helwan university.
Dr. Mohamed Mohamed Ali El-Gazzar (External examiner) Assistant professor at the faculty of Engineering, Arab Academy for Science, Technology & Maritime Transport.

Title of Thesis:

Internet of Things different Threats attack and Hardware Trojan effect on the Coordinate Rotation Digital Computer core.

Key Words:

Internet-of-Things (IoT), Denial of Service, Side-Channel Analysis, Hardware Attack, Coordinate Rotation Digital Computer.

Summary:

Internet of Things (IoT) devices starts to spread all over the world. IoT revolution makes the devices smarter and it improves the performance of the devices. The devices can now exchange information between each other and distribute data analysis effort between each other or send it to data analysis center. As a prediction from Cisco, the number of IoT devices will be 50 billion IoT device connected together in 2020. This enormous number will make us think about immunity of these IoT devices against the Hardware attacks. We propose in this Thesis the effect of inserting Hardware Threat in Coordinate Rotation Digital Computer (CORDIC). Methods are presented in this Thesis to identify Hardware Trojan and its effect on the CORDIC performance. Two ways to improve the immunity of the hardware design against Hardware Trojan are represented here.

Disclaimer

I hereby declare that this thesis is my own original work and that no part of it has been submitted for a degree qualification at any other university or institute.

I further declare that I have appropriately acknowledged all sources used and have cited them in the references section.

Name: Mahmoud Maher El-Sayed Mohammed.

Date:

Signature:

Acknowledgments

First, I would like to thank my spouse and my family who support me in this thesis travel and they are trying to push me forward. I would also to thank Dr Amin Nassar for his advices and his open office door all the time. Thanks also for Dr Mohamed El-Gazzar who push me forward to resume this thesis and direct me to the right way in my research project.

Table of Contents

DISCLAIMER	I
ACKNOWLEDGMENTS	II
TABLE OF CONTENTS	III
LIST OF TABLES	VI
LIST OF FIGURES	VII
NOMENCLATURE	VIII
ABSTRACT	IX
CHAPTER 1 : INTRODUCTION	1
1.1. IoT	1
1.1.1. IoT Network.....	1
1.1.2. IoT Methodology	2
1.1.3. Benefits of IoT	2
1.1.4. IoT Devices Statistics.....	3
1.1.5. IoT Concept History.....	3
1.1.6. Inventing on IoT.....	3
1.1.7. IoT Applications	4
1.1.8. Building IoT.....	4
1.1.9. Importance of IoT	4
1.1.10. Management of IoT.....	5
1.1.11. IoT Device Connectivity	5
1.1.12. IoT Challenges	6
1.2. IoT DEVICES	8
1.2.1. Smart Homes.....	10
1.2.2. Smart Elder Care	11
1.2.3. Medical and Healthcare	11
1.2.4. Sport Competitions	12
1.2.5. Transportation	12
1.2.6. Manufacturing.....	12
1.2.7. Agriculture Field	14
1.2.8. Infrastructure Field.....	14
1.2.9. Governmental field	14
1.2.10. Energy Saving	15
1.2.11. Environment Observation	16
1.3. IoT STANDARDS	16
1.3.1. Zigbee Standard	16
1.3.2. Long Range (LoRa) Standard	17
1.3.3. Long-Term Evolution for Machines (LTE-M) Standard	17
1.3.4. WI_FI Standard.....	18
1.3.5. Bluetooth Low Energy Standard.....	19

1.3.6.	Narrow Band.....	20
1.4.	IOT DEVICE SECURITY	20
1.4.1.	Security Concerns	22
1.4.2.	Side-Channel Analysis Attack	24
1.4.3.	Denial of Service.....	25
1.4.4.	Hardware Trojan	26
CHAPTER 2 : HARDWARE THREAT EFFECT ON PARALLEL CORDIC IN IOT DEVICES.....		27
2.1.	INTRODUCTION	27
2.2.	SECURITY ATTACKS.....	28
2.2.1.	Side-Channel Analysis (SCA)	28
2.5.2.1.	Output Delay Comparison	32
2.5.2.2.	Total Area Comparison	34
2.5.2.3.	Power Consumption Comparison.....	34
2.5.2.4.	Critical Path Delay Comparison.....	34
2.5.2.5.	Max Clock Frequency Comparison.....	34
2.5.3.	Pipelined and Parallel CORDIC Architecture Comparison Results	34
2.5.4.	Pipelined and Parallel CORDIC Architecture Comparison conclusion	35
2.6.	HARDWARE TROJAN EFFECT ON PARALLEL CORDIC PROCESSOR	35
2.6.1.	Parallel CORDIC Architecture	36
2.7.	HARDWARE TROJAN ARCHITECTURE.....	37
2.8.	DETECTION METHOD	38
2.9.	RESULTS	39
2.10.	CONCLUSION	39
CHAPTER 3 : DESIGN AND IMPLEMENTATION NEW TECHNIQUES TO PREVENT TROJAN THREAD IN PARALLEL CORDIC.....		40
3.1.	INTRODUCTION	40
3.2.	HARDWARE ATTACKS ELIMINATION	41
3.2.1.	Dynamic permutation.....	41
3.2.2.	Network on chip.....	41
3.2.3.	Voting Algorithm.....	42
3.2.4.	Lockup Table	42
3.3.	TROJAN THREAD ATTACK.....	42
3.4.	TROJAN THREAD EXCLUSION	44
3.4.1.	Voting Algorithm.....	44
3.4.2.	Lockup Table Technique	44
3.5.	RESULTS	47
3.6.	CONCLUSION.....	48
CHAPTER 4 : DISCUSSION AND CONCLUSIONS.....		49
REFERENCES.....		50
LIST OF PUBLICATIONS.....		53
APPENDIX A: VERILOG CODES		54
•	CORDIC CODE	54

•	CORDIC WITH TROJAN ATTACK CODE	58
•	CORDIC TESTBENCH	59
•	CORDIC ATTACKED TESTBENCH.....	64
•	CORDIC REDUNDANT CODE.....	69
•	CORDIC LOCKED UP CODE	70

List of Tables

Table 2. 1: Angle value according to J	30
Table 2. 2: Comparison between Parallel CORDIC and Pipelined CORDIC.....	35
Table 2. 3: DATA path delays due to the Trojan insertion	39

List of Figures

Figure 1. 1: Internet of Things Benefits	2
Figure 1. 2: IoT Communication standards	6
Figure 1. 3: IoT network in Factory	7
Figure 1. 4: Internet of Things Applications	8
Figure 1. 5: Internet of Things List	10
Figure 1. 6: Fourth revolution of the industry	13
Figure 1. 7: Different Attack Types to IoT.....	21
Figure 1. 8: Design Architecture of Cyber-Physical Systems.....	23
Figure 2. 1: Vector rotation between two vectors	30
Figure 2. 2: Parallel CORDIC Output Delay.....	33
Figure 2. 3: Pipelined CORDIC Output Delay.....	33
Figure 2. 4: Parallel Architecture of CORDIC	36
Figure 2. 5: Hardware Trojan Architecture	37
Figure 2. 6: Parallel CORDIC output not affected by Hardware Trojan.....	38
Figure 3. 1: Dynamic Permutation Technique	42
Figure 3. 2: Trojan thread Architecture	43
Figure 3. 3: Trojan thread Architecture	44
Figure 3. 4: Voting Algorithm Architecture.....	45
Figure 3. 5: Voting Algorithm outputs with defected CORDIC	45
Figure 3. 6: Lockup Table Algorithm Architecture.....	46
Figure 3. 7: Lockup Table Algorithm outputs with defected CORDIC	47

Nomenclature

AP	Access Point
AMI	Advanced metering infrastructure
BCD	Binary-coded decimal
BLE	Bluetooth Low Energy
CORDIC	Coordinate Rotation Digital Computer
CPA	Correlation power analysis
DPA	Differential power analysis
COAP	Constrained Application Protocol
DOS	Denial of service
DSP	Digital signal processing
DTLS	Datagram Transport Layer Security
HT	Hardware Trojan
IC	Integrated circuit
IMS	Intelligent Maintenance Systems
IoT	Internet of Things
IP	Intellectual Property
LTE-M	Long-Term Evolution for Machines
LoRa	Long-Range Wireless Communication
LPWA	Low power wide area
LPWAN	Low power wide-area network
MQTT	Message Queuing Telemetry Transport
M2M	Machine-to-machine
NB	Narrow Band
NFC	Near-field communication
NoC	Network on Chip
RFID	Radio Frequency Identification
RTL	Register-transfer level
SCA	Side-Channel Analysis
SIM	Subscriber identify module
SPA	Simple power analysis
TIM	Traffic Indication Map
TWT	Target Wake Time

Abstract

Internet of Things (IoT) devices starts to spread all over the world. IoT revolution makes the devices smarter and it improves the performance of the devices. The devices can now exchange information between each other and distribute data analysis effort between each other or send it to data analysis center. As a prediction from Cisco, the number of IoT devices will be 50 billion IoT device connected together in 2020. This enormous number will make us think about immunity of these IoT devices against the Hardware attacks. There are security attacks that can affect IoT device. The Side-Channel Analysis (SCA) aims to get information from the IoT device like power consumption, delays, and electro- magnetic radiated from the device while it performs any cryptographic algorithm. Denial of service (DOS) attack is cyber-attack. This attack affects the connection between the IoT device and the network by flooding the IoT device with excess requests. Hardware Trojan can affect the IC performance in different manners other than the functionality like changing the power cycle time if the chip has sleep and wakeup modes, changing the clock frequency that adjusted internally, Make the processor busy by sending false interrupts to it etc. We will see the effect of inserting Hardware Threat in Coordinate Rotation Digital Computer (CORDIC). Methods like simulations comparison and synthesizing difference are presented in this thesis to identify Hardware Trojan and its effect on the CORDIC performance. If we want to make our design immune against the hardware trojan, there are two methods represented here in the thesis. First method is redundant cores method. This method is done by inserting two redundant similar cores beside the main core and make voting between these cores. If one core is infected by hardware trojan, then the voting controller will see that its output is different from the two other cores output and isolate its output. The second method is lockup table method. This method depends on inserting lockup table beside the main core and another redundant core. We will store some of our expected outputs and compare these outputs to the output from the cores, if one core is different to the expected output, then we will isolate its output and the other core which match expected output will connected to the global output.