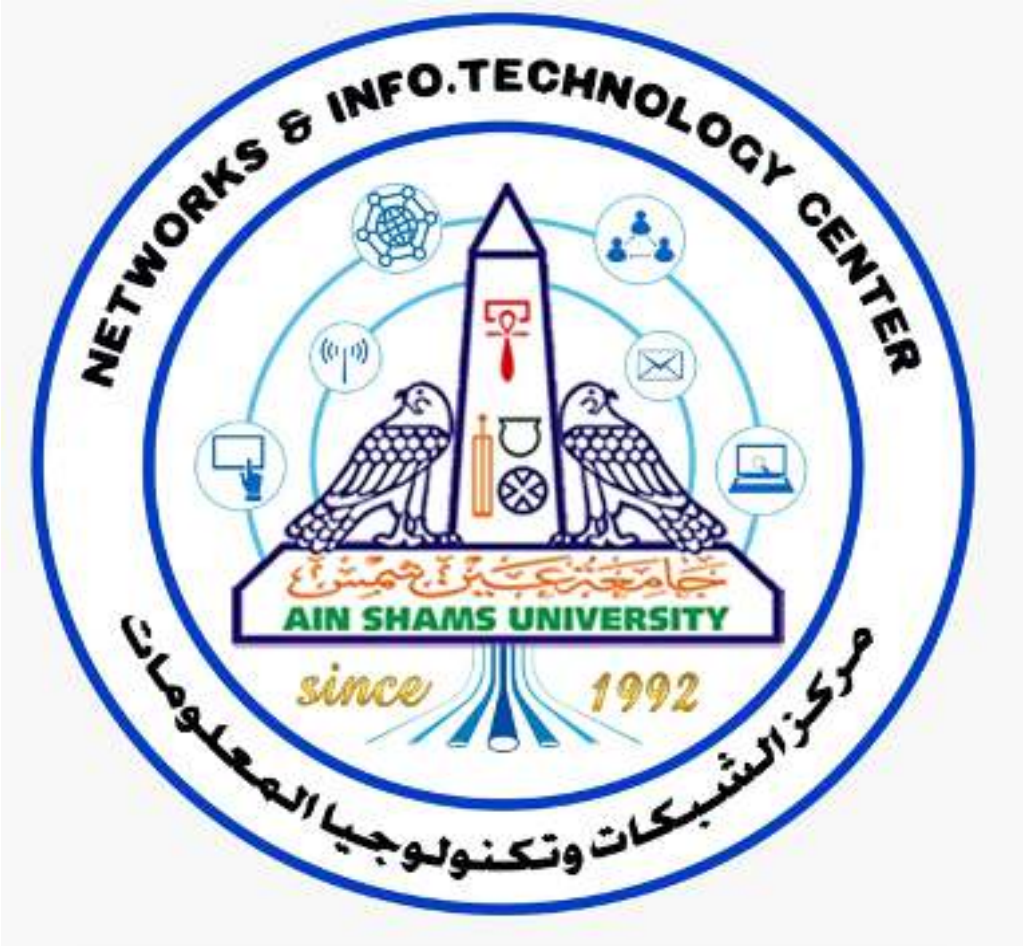
Mona Maghraby

# بسم اللّه الرحمن الرحيم

## مركز الشبكات وتكنولوجيا المعلومات

## قسم التوثيق الإلكتروني



Mona Maghraby

# جامعة عين شمس

## التوثيق الإلكتروني والميكروفيلم

## قسم

نقسم باللّه العظيم أن المادة التي تم توثيقها وتسجيلها

علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات


# 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:**

Porf. 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

# List of Tables

# List of Figures

# 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.