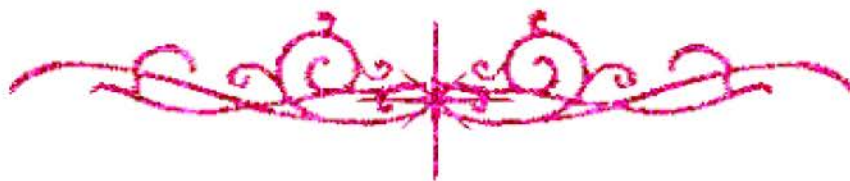


بسم الله الرحمن الرحيم





شبكة المعلومات الجامعية التوثيق الالكتروني والميكروفيلم



جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

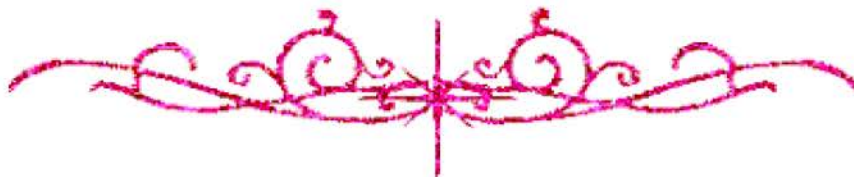
قسم

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



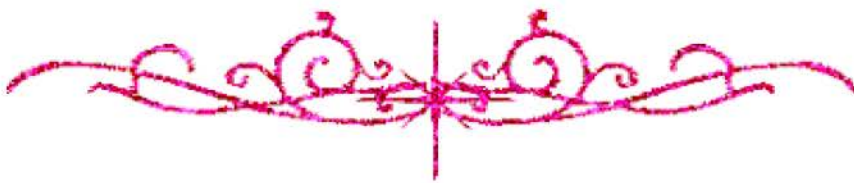
يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار



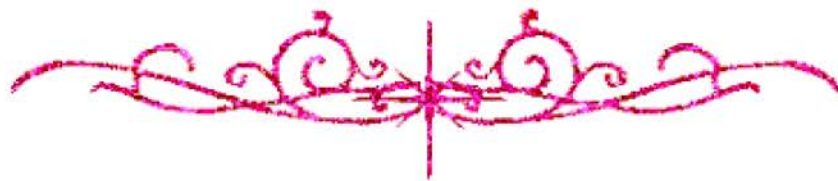


بعض الوثائق الأصلية تالفة





بالرسالة صفحات
لم ترد بالأصل





INTERNET OF THINGS HARDWARE SECURITY

By

Amr Mohamed Abbas Dessouky

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
2021

INTERNET OF THINGS HARDWARE SECURITY

By

Amr Mohamed Abbas Dessouky

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. Dr. Ahmed Nader

**Prof. Dr. Hassan Mostafa
Hassan**

.....

.....

Professor of Electronics and
Communications
Department of Electronics and Electrical
Communications Engineering
Faculty of Engineering, Cairo
University

Assistant Professor of Nano electronics,
Bioelectronics and Optoelectronics
Department of Electronics and
Electrical Communications Engineering
Faculty of Engineering, Cairo
University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

INTERNET OF THINGS HARDWARE SECURITY

By

Amr Mohamed Abbas Dessouky

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. Ahmed Nader Mohieldin

(Thesis Main Advisor)

Prof. Dr. Hassan Mostafa Hassan

(Advisor)

Prof. Dr. Ahmed Hussein Khalil

(Internal Examiner)

Prof. Dr. Amr Talaat Abdel-Hamid
German university in Cairo

(External Examiner)

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

Engineer's Name: Amr Mohamed Abbas Dessouky

Date of Birth: 06/04/1990

Nationality: Egyptian

E-mail: Amr_901@hotmail.com

Phone: 01007415072

Registration Date: 01/10/2013

Awarding Date: -/-/2021

Degree: Master of Science

Department: Electronics and
Communications Engineering



Supervisors:

Prof. Dr. Ahmed Nader Mohie El Dein

Prof. Dr. Hassan Mostafa Hassan

Examiners:

Prof. Dr. Ahmed Nader Mohie El Dein (Thesis Main Advisor)

Prof. Dr. Hassan Mostafa Hassan (Advisor)

Prof. Dr. Ahmed Hussein Khalil (Internal Examiner)

Prof. Dr. Amr Talaat Abdel-Hamid (External Examiner)

German University in Cairo

Title of Thesis:

Internet of things hardware security.

Key Words:

Internet Of things, Partial Dynamic Reconfiguration, Authenticated Encryption with Associated Data, Field-programmable Gate Array, Application-Specific Integrated Circuit

Summary:

The objective of this thesis is to provide a low area low power optimized implementation for cryptography algorithms to match the power constraints imposed by the low power IoT applications. In this thesis low area and low power implementations of selected ciphers from the CAESAR candidates namely NORX, Tiaoxin, SILC, COLM, and JAMBU are provided. Moreover, Partial dynamic reconfiguration is used to achieve resource-efficient and energy-efficient hardware security.

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: Amr Mohamed Abbas

Date: --/--/2021

Signature:

Acknowledgments

Alhamdulillah, all praises and gratitude to Allah, for all his blessings and support me with the strength and health to complete this thesis.

I would like to thank my academic supervisors Dr. Hassan Mustafa and Dr. Ahmed Nader for their guidance and help during the thesis work.

I would like as well to thank my managers and colleagues in Mentor Graphics for their support (Eman El-Mandouh, Haytham Shoukry, Nahla Mohamed, Khaled Nouh and Islam Osama).

Last but absolutely not least, I want to extend my deepest and most sincere gratitude and thanks to my family for their support throughout my study.

Table of Contents

DISCLAIMER	I
ACKNOWLEDGMENTS	II
TABLE OF CONTENTS.....	III
LIST OF TABLES.....	V
LIST OF FIGURES	VI
NOMENCLATURE.....	VII
ABSTRACT	VIII
CHAPTER 1 : INTRODUCTION.....	1
1.2. Thesis Objectives	4
1.3. Organization of the Thesis	4
CHAPTER 2 : INTRODUCTION TO AUTHENTICATED ENCRYPTION.....	5
2.1. Cryptography	5
2.2. Encryption scheme	6
2.3. Authenticated Encryption	8
2.4. Authentication Techniques	9
2.4.1. Cryptographic Hash Functions	9
2.4.2. Message authentication code (MAC).....	10
2.5. Authentication Ciphers Types	11
2.5.1. Block ciphers	11
2.5.2. Stream Cipher	12
2.5.3. Tweakable Block ciphers.....	12
2.6. Authenticated Encryption approaches.....	13
2.6.1. Encrypt-then-MAC (EtM)	13
2.6.2. MAC-then-Encrypt (MtE)	13
2.6.3. Encrypt-and-MAC (E&M).....	13
2.7. Attacks on ciphers	15
2.8. Attack analysis: differential and linear cryptanalysis	16
2.9. Competition for Authenticated Encryption: Security, Applicability, and Robustness	16
CHAPTER 3 : LOW AREA AND LOW POWER IMPLEMENTATION OF CAESAR ENTICATED CIPHERS	21
3.1. Power Measurements	21
3.2. IOT Power Profile	22
3.3. Literature Survey	22
3.4. Low Power low Area Optimization	24
3.4.1. The General Approach.....	24
3.4.2. Implementations Evaluation.....	24
3.4.2.1.Implementation on field programmable gate array (FPGA).....	24
3.4.2.2.Implementation on application specific integrated circuit (ASIC).....	25
3.4.3. The GMU Hardware API for Authenticated Ciphers	25
3.4.4. Common Features for CASEAR Candidates	25
3.5. NORX	28
3.5.1. Operation.....	28
3.5.2. Low Area Low Power Optimization	29
3.5.3. Results.....	30

3.6.	SILC	31
3.6.1.	Operation.....	31
3.6.2.	Low Area Low Power Optimization	33
3.6.3.	Results.....	34
3.7.	Tiaoxin-346	35
3.7.1.	Operation.....	35
3.7.2.	Low Area Low Power Optimization	36
3.7.3.	Results.....	37
3.8.	COLM.....	37
3.8.1.	Operation.....	38
3.8.2.	Low Area Low Power Optimization	40
3.8.3.	Results.....	40
3.9.	JAMBU	40
3.9.1.	Operation.....	41
3.9.2.	Low Area Low Power Optimization	42
3.9.3.	Results.....	44
3.10.	Conclusion.....	44
CHAPTER 4 DYNAMIC PARTIAL RECONFIGURATION HARDWARE IMPLEMENTATION		47
4.1.	Configuration Definition.....	47
4.2.	Dynamic Partial Reconfiguration	47
4.3.	Configuration Modes.....	48
4.3.1.	External Modes	48
4.3.2.	Internal Modes	48
4.4.	Advantage and Disadvantage of DPR.....	49
4.5.	Dynamic Partial Reconfiguration Controller	50
4.5.1.	Xilinx ICAP Controller (AXI-HWICAP).....	51
4.5.2.	Xilinx Partial Reconfiguration Manager	51
4.5.3.	Custom DMA Based ICAP Controller	51
4.5.4.	Software-Controlled Partial Reconfiguration	51
4.6.	Literature Survey	55
4.7.	Resource Efficient Hardware Implementation for AEAD Ciphers Using PDR	55
4.7.1.	Proposed System Overview	58
4.7.1.1.	COLM Reconfigurable Crypto processor.....	58
4.7.1.2.	OCB Reconfigurable Crypto processor.....	58
4.7.2.	Reconfiguration Time.....	59
4.7.3.	Resource Utilization	59
4.7.4.	Power Consumption and Energy Efficiency	59
4.8.	Energy Efficient Hardware Implementation for AEAD Ciphers Using PDR	60
4.9.	Conclusion.....	61
CHAPTER 5 CONCLUSION AND FUTURE WORK		62
5.1.	Conclusion.....	62
5.2.	Future Work	63
REFERENCES.....		64
APPENDIX A: LIST OF PUBLICATIONS		69

LIST OF Tables

Table 1 Comparison of Results to Work in [16]	45
Table 2 Results of Implementation in virtex 7 FPGA	46
Table 3 Results of Implementation in ASIC	46
Table 4 Zynq FPGA Configuration Modes	49
Table 5 OCB Resource Utilization.....	59
Table 6 COLM Resource Utilization	59
Table 7 OCB Energy Utilization	60
Table 8 COLM Energy Utilization.....	60

LIST OF Figures

Figure 1: IoT Devices	1
Figure 2: Symmetric Encryption [5].....	6
Figure 3: Asymmetric Encryption [5]	7
Figure 4: Input and Output of an Authenticated Cipher [6]	8
Figure 5: Cryptographic Hash Functions [7].....	9
Figure 6 Message authentication code	10
Figure 7: Authenticated Encryption approaches [15].....	14
Figure 8: the inputs and output of authenticated ciphers participating in the CAESAR competition [15]	18
Figure 9: FPGA Benchmarking Results of Round 3 Candidates [15].....	18
Figure 10: Top-level block diagram of a lightweight architecture of a single-pass authenticated cipher core, AEAD [16]	20
Figure 11 Typical power profile of an IoT node [59]	22
Figure 12 AES encryption algorithm	27
Figure 13 Duplex construction based Authenticated encryption scheme [24].....	28
Figure 14 NORX Algorithm [24]	29
Figure 15: NORX High speed Block diagram	30
Figure 16: SILC Algorithm [27].....	32
Figure 17: SILC high speed block diagram.....	34
Figure 18: Tiaoxin-346 Algorithm [25]	35
Figure 19: Tiaoxin-346 high speed state update block diagram.....	37
Figure 20: COLM Algorithm [26].....	38
Figure 21: Associated data processing in COLM.....	39
Figure 22: Processing of the plaintext	42
Figure 23: MixColumns multiplier.....	43
Figure 24: Processing of the plaintext	43
Figure 25 : Dynamic Partial Reconfiguration in SRAM-FPGAS	48
Figure 26: Partial Reconfiguration Controller in DPR System [45]	50
Figure 27: Types of Internal Partial Reconfiguration Controllers [45].....	52
Figure 28: Reconfiguration Time for Different PR Controllers [45]	53
Figure 29: (a) Resource Utilization, (b) Avg. Reconfiguration Throughput and (c) Power Consumption Comparisons between different PR controllers [45]	54
Figure 30: COLM, OCB Round Function.....	56
Figure 31: OCB cipher [56].....	57
Figure 32: COLM Reconfigurable Crypto processor	58
Figure 33: OCB Reconfigurable Crypto processor	58
Figure 34: Energy Consumption [58].....	60