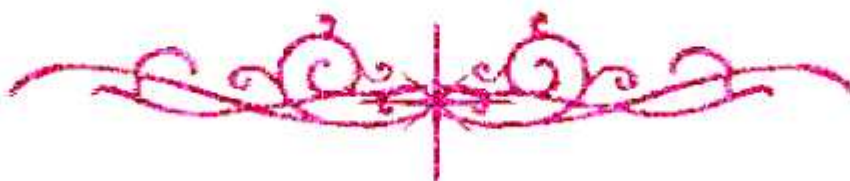


بسم الله الرحمن الرحيم





شبكة المعلومات الجامعية التوثيق الالكتروني والميكرو فيلم



جامعة عين شمس

التوثيق الإلكتروني والميكرو فيلم

قسم

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



يجب أن

تحتفظ هذه الأقراص المدمجة بعيدا عن الغبار





**HARDWARE SECURITY MODULE FOR LOW
POWER INTERNET OF THINGS APPLICATIONS
BASED ON DYNAMIC PARTIAL
RECONFIGURATION**

By

Nagham Samir Abo-Dief Abdel-Raziq

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
2020

**HARDWARE SECURITY MODULE FOR LOW
POWER INTERNET OF THINGS APPLICATIONS
BASED ON DYNAMIC PARTIAL
RECONFIGURATION**

By

Nagham Samir Abo-Dief Abdel-Raziq

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 H. Khalil

Professor

Specialization Department

Faculty of Engineering, Cairo University

Dr. Hassan Mostafa Hassan

Associate Professor

Department of Electronics and Communication Engineering

Faculty of Engineering, Cairo University

**FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT**

2020

**HARDWARE SECURITY MODULE FOR LOW
POWER INTERNET OF THINGS APPLICATIONS
BASED ON DYNAMIC PARTIAL
RECONFIGURATION**

By

Nagham Samir Abo-Dief Abdel-Raziq

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 H. Khalil

Thesis Main Advisor

Dr. Hassan Mostafa Hassan

Advisor

Prof. Dr. Amin Mohamed Nassar

Internal Examiner

Dr. Mohamed Abdelghani Salem
(German University in Cairo)

External Examiner

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

Engineer's Name: Nagham Samir Abo-Dief Abdel-Raziq
Date of Birth: 30/9/1992
Nationality: Egyptian
E-mail: nagham.samir2014@gmail.com
Phone: 01118847199
Address: Kornish-Elnile, Misr ElQadima, Cairo- Egypt
Registration Date: 1/3/2016
Awarding Date: / /2020
Degree: Master of Science
Department: Electronics and Communications Engineering



Supervisors:

Prof. Dr. Ahmed H. Khalil
Dr. Hassan Mostafa Hassan

Examiners:

Prof. Dr. Ahmed H. Khalil	(Thesis main advisor)
Prof. Dr. Amin Mohamed Nassar	(Internal examiner)
Dr. Mohamed Abdelghani Salem	(External examiner)
(German University in Cairo)	

Title of Thesis:

Hardware Security Module for Low Power Internet of Things Applications
Based on Dynamic Partial Reconfiguration

Key Words:

Internet of Things (IoT); Dynamic Partial Reconfiguration (DPR); Advanced Encryption Standard (AES); Field Programmable Gate Array (FPGA);

Summary:

This work implements hardware security module for low power internet of things applications on Zynq-7000 evaluation kit. The new DPR technique is used to switch among the different levels of security depending on the variant energy profile of IoT device. Implementing encryption algorithm using DPR combines the advantage of hardware performance and software flexibility. A test environment is established to measure the effectiveness of the new technique.

Table of Contents

List of Tables	v
List of Figures	vi
List of Nomenclature	viii
Nomenclature	xiv
Abstract	xv
1 Introduction	1
1.1 History of Internet of Things (IoT)	1
1.1.1 Internet of Things (IoT) Definition	1
1.2 Internet of Things (IoT) Applications	2
1.3 Internet of Things (IoT) Characteristics	4
1.4 Main Goals of Internet of Things (IoT)	5
1.5 Internet of Things (IoT) Challenges	5
1.6 The Most Challenging Issue for Internet of Things (IoT) Applications . .	5
1.6.1 Software Security	6
1.6.2 Hardware Security	6
1.7 Problem Domain	7
1.8 Organization of the thesis	7
2 ASIC and FPGA Comparative Study for IoT Lightweight Hardware Security Algorithms	9
2.1 Introduction	9
2.2 Purpose of This Comparative Study	9
2.2.1 Internet of Things Security Problems	10
2.2.1.1 Authentication	10
2.2.1.2 Privacy	10
2.2.1.3 Power Consumption	10
2.3 CAESAR Competition	11
2.3.1 Motivation Behind CASEAR Competition	11
2.3.2 Cryptographic Competitions	11
2.3.3 Hardware Application Programming Interface (API) for Authenticated Ciphers	12
2.3.3.1 Pre-Processor	12
2.3.3.2 Cipher Core	13
2.3.3.3 Post-Processor	13
2.3.3.4 Bypass First-In-First-Out (FIFO)	13
2.3.3.5 Auxiliary FIFO	13
2.4 Common Features For CAESAR Candidates	14
2.4.1 Encryption Modes	15
2.4.1.1 Electronics Code Book (ECB)	15

2.4.1.2	Cipher Feed Back (CFB)	15
2.4.1.3	Cipher Block Chaining (CBC)	16
2.4.2	Functional Features	16
2.4.3	Security	17
2.4.4	Features of the Selected Candidates from CAESAR	18
2.5	The Selected Algorithms From CAESAR Competition	18
2.5.1	ACORN Algorithm	18
2.5.2	ASCON Algorithm	20
2.5.3	CLOC Algorithm	20
2.5.4	JOLTIK Algorithm	21
2.5.5	MORUS Algorithm	22
2.5.6	PRIMATEs Algorithm	23
2.5.7	SCREAM Algorithm	25
2.5.8	SILC Algorithm	26
2.6	FPGA/ASIC IMPLEMENTATIONS	27
2.6.1	Implementation on Field Programmable Gate Array (FPGA) . . .	27
2.6.2	Implementation on Application Specific Integrated Circuit (ASIC)	27
2.7	RESULTS AND DISCUSSION	28
2.7.1	FPGA and ASIC Power	28
2.7.2	Area and Slice LUTs	29
2.7.3	Throughput	30
2.7.4	Latency	30
2.8	COMPARISON	31
2.9	Summary	32
3	Dynamic Partial Reconfiguration (DPR): Review and Design Flow	34
3.1	History of FPGA Evolution	34
3.2	ZC702 Evaluation Board	35
3.2.1	CLB Overview	36
3.3	FPGA Configuration Development Process	37
3.3.1	Full Reconfiguration	38
3.3.2	Partial Reconfiguration	39
3.3.2.1	Advantages of Partial Reconfiguration	39
3.3.3	Dynamic Partial Reconfiguration (DPR)	40
3.3.4	Dynamic Partial Reconfiguration Concepts	41
3.3.4.1	Configuration Frames	41
3.3.4.2	Configuration Time	42
3.3.5	PR Configuration Modes	42
3.4	Component of Dynamic Partial Reconfiguration System	43
3.4.1	Overview of Internal Configuration Access Port (ICAP)	43
3.4.2	Dynamic Partial Reconfiguration Controllers	43
3.4.3	Xilinx Dynamic Partial Reconfiguration Controllers	44
3.4.3.1	AXI-HWICAP	44
3.4.3.2	PRC	45
3.4.4	Comparison Among The Partial Reconfiguration Controller	48
3.4.5	Advanced eXtensible Interface (AXI)	48
3.4.6	Integrated Logic Analyzer (ILA)	49

3.4.6.1	Supported Features of ILA	49
3.5	Summary	49
4	Energy-Adaptive Lightweight Hardware Security Module using Dynamic Partial Reconfiguration for Energy Limited Internet of Things Applications	50
4.1	Motivation	50
4.2	System Architecture	51
4.3	AEAD ARCHITECTURE	52
4.4	RTL Description of the Selected Algorithms	52
4.4.1	Pi-Cipher Encryption Mode	53
4.4.2	JAMBU Encryption Mode	55
4.5	EXPERIMENTAL RESULTS	57
4.6	Summary	59
5	Multi-Level Security of Generic-AES Using Dynamic Partial Reconfiguration Targeting Lightweight Internet of Things Applications on Xilinx Zynq FPGA	60
5.1	Motivation	60
5.2	The Proposed Generic-AES Algorithm	62
5.2.1	Traditional Advanced Encryption Standard (AES) Algorithm	62
5.2.2	Hardware Implementation of The Proposed Generic Advanced Encryption Standard (Generic-AES) Algorithm	63
5.2.3	RTL Experimental Results Of The Generic-AES Algorithm	65
5.2.3.1	Latency	65
5.2.3.2	Hardware Utilization	67
5.2.3.3	Energy Consumption	68
5.3	Dynamic Partial Reconfiguration (DPR)	69
5.3.1	History of Programmable Logic	69
5.3.2	Dynamic Partial Reconfiguration (DPR)	72
5.3.3	The Suggested DPR System	73
5.4	The Experimental Results Of The Suggested DPR System	76
5.4.1	Hardware Utilization	76
5.4.2	Power Consumption	77
5.4.3	Reconfiguration Time	78
5.5	Summary	78
6	Conclusion and Future Work	79
6.1	Suggestions for Future Work	79
	References	80
	Appendix A VHDL Code of Key Expansion Module For Generic-AES Algorithm	89
	Appendix B VHDL Code of Encryption Module For Generic-AES Algorithm	112
	Appendix C VHDL Code of Decryption Module For Generic-AES Algorithm	135

Appendix D	Software Application Code For FPGA Prototyping	152
Appendix E	FPGA Prototyping and DPR Steps	192

List of Tables

2.1	COMPARISON BETWEEN OUR DESIGNS AND PREVIOUS DESIGNS IN ASIC FLOW	32
2.2	COMPARISON BETWEEN OUR DESIGNS AND PREVIOUS DESIGNS IN FPGA FLOW	33
3.1	CONFIGURATION MODES OF ZYNQ-7000 XC7Z020 SoC EVALUATION BOARD	38
3.2	CONSTRAINTS OF DIFFERENT CONFIGURATION PORTS	42
4.1	PI-CIPHER FEATURES	53
4.2	EXPERIMENTAL RESULTS PRIOR DPR TECHNIQUE	57
4.3	COMPARISON AMONG IMPLEMENTED DESIGNS	58
4.4	ENCRYPTION MODES RESULTS USING DPR TECHNIQUE	58
5.1	LATENCY OF THE KEY EXPANSION MODULE	66
5.2	LATENCY OF THE GENERIC-AES ENCRYPTION MODULE	66
5.3	LATENCY OF THE GENERIC-AES DECRYPTION MODULE	67
5.4	TOTAL LATENCY OF THE GENERIC-AES ENCRYPTION MODULE AND THE KEY EXPANSION MODULE	67
5.5	LATENCY OF THE GENERIC-AES DECRYPTION MODULE AND THE KEY EXPANSION MODULE	68
5.6	FPGA UTILIZATION OF GENERIC-AES ENCRYPTION MODULES	69
5.7	FPGA UTILIZATION OF GENERIC-AES DECRYPTION MODULES	69
5.8	POWER CONSUMPTION OF ENCRYPTION MODULE	70
5.9	POWER CONSUMPTION OF DECRYPTION MODULE	70
5.10	ENERGY CONSUMPTION OF THE GENERIC-AES ENCRYPTION MODULE AND KEY CALCULATION IS EXCLUDED	70
5.11	ENERGY CONSUMPTION OF THE GENERIC-AES DECRYPTION MODULE AND KEY CALCULATION IS EXCLUDED	71
5.12	ENERGY CONSUMPTION OF THE GENERIC-AES ENCRYPTION MODULE AND KEY CALCULATION IS INCLUDED	71
5.13	ENERGY CONSUMPTION OF THE GENERIC-AES DECRYPTION MODULE AND KEY CALCULATION IS INCLUDED	72
5.14	RESULTS OF THE STATIC DESIGN FOR THE SUGGESTED ENCRYPTION MODULES	76
5.15	RESULTS OF THE DYNAMIC DESIGN FOR THE SUGGESTED ENCRYPTION MODULES	77
5.16	RESULTS OF THE STATIC DESIGN FOR THE SUGGESTED DECRYPTION MODULES	77
5.17	RESULTS OF THE DYNAMIC DESIGN FOR THE SUGGESTED DECRYPTION MODULES	77
5.18	POWER CONSUMPTION OF THE SUGGESTED ENCRYPTION MODULES	77
5.19	POWER CONSUMPTION OF THE SUGGESTED DECRYPTION MODULES	78
5.20	RECONFIGURATION TIME FOR THE SUGGESTED SECURITY SYSTEM	78

List of Figures

1.1	The Internet of Things (IoT) [4]	1
1.2	The connection to the Internet extends by means of Internet of Things (IoT) [5]	2
1.3	Communication Protocol of the IoT [7]	2
1.4	The IoT application and its marketplace [1]	3
1.5	The connection among the IoT network for smart home [13]	3
1.6	Wearable IoT devices within Human Body [12]	4
2.1	CAESAR hardware Application Programming Interface (API)	12
2.2	AES algorithm [40]	14
2.3	Supported feature for the selected candidate	18
2.4	ACORN_v2 cipher core data path	19
2.5	ASCON's mode of operations [57]	20
2.6	Block diagram of CLOC	21
2.7	JOLTIK block diagram of processing the message [52]	22
2.8	Block diagram of MORUS implementation	23
2.9	Mix Columns transformation for PRIMATES-80. The state matrix is multiplied column by column with the 5x5 matrix [63]	24
2.10	SCREAM algorithm cipher core [67]	25
2.11	SILC encryption and decryption block diagrams	27
2.12	SoC encounter chip layouts of the Eight cryptographic algorithms	28
2.13	FPGA and ASIC power estimation results	29
2.14	FPGA utilization and ASIC area results	29
2.15	Throughput results	30
2.16	Latency results	31
3.1	Generic PAL architecture [78]	34
3.2	Generic array FPGA architecture [78]	35
3.3	Zynq-7000 SoC Block Diagram [80]	36
3.4	Arrangement of Slices within the CLB [82]	37
3.5	Row and Column Relationship between CLBs and Slices [82]	37
3.6	FPGA Architecture [83]	39
3.7	Typical Partial Reconfiguration Process [86]	40
3.8	The hardware of ICAP primitive [89]	43
3.9	Block diagram of XPS_HWICAP [90]	44
3.10	Block diagram of AXI_HWICAP [94]	45
3.11	Internal structure of virtual socket manager [95]	45
3.12	PRC virtual socket manager [95]	46
3.13	PRC in DPR system [95]	46
3.14	Fetch path of the PRC [95]	47
3.15	Comparison among different PRCs [96]	48
3.16	ILA Core Symbol [99]	49
4.1	Block diagram of the proposed DPR system	51

4.2	Internal state concatenation [117]	53
4.3	Triplex block [117]	54
4.4	Pi-function [117]	54
4.5	Pi-Cipher controller chart [117]	55
4.6	Block diagram of plaintext processing for JAMBU [114]	56
4.7	SIMON block diagram [114]	56
5.1	The expected market share of IoT applications [27]	61
5.2	Energy utilization of common IoT device [27]	62
5.3	Flow Chart of AES Algorithm For Encryption	63
5.4	Data Chain Implementation of Generic-AES Encryption Module	64
5.5	The Suggested DPR System	74
5.6	Generic-AES Reconfigurable Partition Variants	75
E.1	Step 1 of DPR flow Steps	193
E.2	Step 2 of DPR flow Steps	193
E.3	Step 3 of DPR flow Steps	194
E.4	Step 4 of DPR flow Steps	195
E.5	Step 5 of DPR flow Steps	195

List of Nomenclature

<i>AD</i>	associated data
<i>AE</i>	Authenticated Encryption
<i>AEAD</i>	Authenticated Encryption with Associated Data
<i>AES</i>	Advanced Encryption Standard
<i>API</i>	Application Programming Interface
<i>APR</i>	Auto Place and Route
<i>ASIC</i>	Application Specific Integrated Circuits
<i>AXI</i>	Advanced eXtensible Interface
<i>BFA</i>	Brute Force Attack
<i>BRAM</i>	Block RAM
<i>CA</i>	Constant Addition
<i>CAESAR</i>	Competition for Authenticated Encryption: Security, Applicability, and Robustness
<i>CBC</i>	Cipher Block Chaining
<i>CCM</i>	Counter with Cipher Block Chaining Message Authentication Code
<i>CFB</i>	Cipher Feed Back
<i>CFB</i>	Cipher FeedBack
<i>CLB</i>	configurable logic block
<i>CPLD</i>	Complex Programmable Logic Device
<i>DEC</i>	Decryption engine
<i>DPA</i>	differential power analysis
<i>DPR</i>	Dynamic partial reconfiguration
<i>EAX</i>	Encryption-then-Authentication-then-Translate
<i>EAX – prime</i>	Encryption-then-Authentication-then-Translate-prime
<i>ECB</i>	Electronics Code Book
<i>ENC</i>	Encryption engine