Ain Shams University Information Network
جامعة عين شمس
شبكة المعلومات الجامعية
@ ASUNET

شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

بسم الله الرحمن الرحيم

Ain Shams University Information Network
جامعة عين شمس
شبكة المعلومات الجامعية
@ ASUNET

HANAA ALY

شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

Ain Shams University Information Network
جامعة عين شمس
شبكة المعلومات الجامعية
@ ASUNET

شبكة المعلومات الجامعية
التوثيق الالكتروني والميكروفيلم

HANAA ALY

شبكة المعلومات الجامعية
التوثيق الإلكتروني 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

HANAA ALY

CU-SDAH: A PLATFORM FOR IOT HARDWARE SECURITY, SW/HW PARTITIONING, EXTENDED ALGORITHM HOPPING AND SCA RESISTANCE USING ZYNQ SOC

By

Abdelrhman Mohamed Ibrahim Sayed Abotaleb

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
Computer Engineering

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

CU-SDAH: A PLATFORM FOR IOT HARDWARE SECURITY, SW/HW PARTITIONING, EXTENDED ALGORITHM HOPPING AND SCA RESISTANCE USING ZYNQ SOC

By
Abdelrhman Mohamed Ibrahim Sayed Abotaleb

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
Computer Engineering

Under the Supervision of

Prof. Dr. Amr Galal El-din Wassal

Professor of Computer Engineering
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

CU-SDAH: A PLATFORM FOR IOT HARDWARE SECURITY, SW/HW PARTITIONING, EXTENDED ALGORITHM HOPPING AND SCA RESISTANCE USING ZYNQ SOC

By

Abdelrhman Mohamed Ibrahim Sayed Abotaleb

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
Computer Engineering

Approved by the Examining Committee **Signature**

Prof. Dr. Amr Galal El-din Wassal, Thesis Main Advisor ..………………

Prof. Dr. Samir Ibrahim Shaheen, Internal Examiner ……………….

Prof. Dr. Mohamed W. El-Kharashi, External Examiner ………………..
(Professor at Computer and Systems Engineering, Faculty of Engineering, Ain Shams University)

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

Engineer's Name:	Abdelrhman Mohamed Ibrahim Sayed
Date of Birth:	18/06/1989
Nationality:	Egyptian
E-mail:	aabotaleb@eng.cu.edu.eg
Phone:	01154909591
Address:	4 Ahmed Mostafa St, P 139 , Masr Eladema, Cairo, Egypt.
Registration Date:	01/10/2018
Awarding Date:	…./…./2021
Degree:	Master of Science
Department:	Computer Engineering

Supervisor: **Prof. Dr. Amr Galal El-din Wassal**

Examiners:

Porf. Dr. Amr Galal El-din Wassal (Thesis main advisor)
Prof. Dr. Samir Ibrahim Shaheen (Internal Examiner)
Prof. Dr. Mohamed W. El-Kharashi (External Examiner)
(Professor at Computer and Systems Engineering, Faculty of Engineering, Ain Shams University)

Title of Thesis:

CU-SDAH: A Platform for IoT Hardware Security, SW/HW Partitioning, Extended Algorithm Hopping and SCA Resistance Using ZYNQ SOC

Key Words:

IoT Security, Dynamic Partial Reconfiguration, Genetic Algorithms, Differential Power Analysis, Software/Hardware Partitioning.

Summary:

Internet of things applications are being essential in every life aspects, with the critical risk of breaching the data transmission, In the current thesis, advanced optimization techniques for hardware security implementation is done and evaluated against the proposed framework with three advanced techniques, first technique is the software/hardware partitioning using the SDSoC and being implemented in the ZYNQ SoC and being compared against pure RTL implementation, second technique starts through side channel attack evaluation against AES algorithm by applying differential power analysis using chipWhisperer kit is done and critical vulnerabilities inside the S-Box of the AES algorithm is being enhanced through applying the genetic algorithms to obtain optimized security parameters for the S-Box.. third technique improves algorithm hopping by applying the partial dynamic reconfiguration proposing new security dimension along with saving the chip area.

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 as I have cited them in the references section.

Name: Abdelrhman Mohamed Ibrahim Sayed Abotaleb

Date: 5/5/2021

Signature:

Dedication

To my mother Inas Hassan Abdallah, for endless support during my whole life, she is my instructor and educator, Thank you my mother for all of your support and help.

To my father's soul Eng/Mohamed Ibrahim Sayed Abotaleb, who brought me up and helped me tackling every life problem, he devoted himself for the service of his nation and country when working as a telecommunication engineer then as a manager at different Telecom Egypt company's centrals, he passed away few days after defending the current thesis, May Allah bless him.

To my family

To my colleagues Hesham Yamany, Mohamed Youssef Hassan, Gamal Zayed, Usama Tuson, and Mustafa Abdallah

To my professors

Acknowledgments

All praise is to Allah, the current master thesis work is done successfully.

Special thanks to Prof. Amr Wassal for teaching me professional digital design, VHDL, AMS-VHDL and related techniques in my under-graduate courses and advanced techniques for computer aided design and acceleration techniques of developing convolutional neural networks in FPGA in the post-graduate courses, these techniques contribute thoroughly for my thesis work development.

Special thanks also to Prof.Dr.Samir Shaheen for teaching me thoroughly the computer security algorithms and techniques in my fourth year undergraduate course, this course helped me a lot to easily understand and implement the different security mathematical functions discussed in the current work.

I would like to thank also Dr. Hassan Mostafa for supervising me through a wide range of research projects during 2018 and 2019.

I am also acknowledging Prof. Ashraf Badwi the dean of the Zewail City of Engineering, Dr. Tamer Ashour and Prof. Hossam Fahmy, the head of Communications and Information Theory Department at Zewail City for their continuous support and encouraging my academic progress during my second bachelor degree studying at the computer engineering department.

I would like to thank my colleagues Eng. Mohamed Tharwat and Eng. Mohamed Hamed for providing me with some needed hardware kits like ZYBO and the chip-whisperer kit, without their cooperation, the current thesis work would not be completed.

Great thanks, for my great mother Inas Hassan Abdallah and my father Eng. Mohamed Abotaleb for their endless love and support during my whole life.

Contents

DISCLAIMER I

DEDICATION II

ACKNOWLEDGMENTS III

CONTENTS IV

LIST OF TABLES VI

LIST OF FIGURES VIII

NOMENCLATURE XI

ABSTRACT XIV

CHAPTER 1: INTERNET OF THINGS: TOOLS AND CHALLENGES 1

1.1. INTERNET OF THINGS DEFINITION 1
1.2. INTERNET OF THINGS APPLICATIONS AND MARKET SIZE 3
1.2.1. Vehicle to Vehicle IoT System 3
1.2.2. Smart Meters IoT System 5
1.2.3. Radioactivity IoT Measurement System 7
1.2.4. Market Analysis 9
1.3. INTERNET OF THINGS COMMUNICATIONS PROTOCOLS 11
1.4. INTERNET OF THINGS SECURITY CONCERNS 15
1.5. THESIS ORGANIZATION 16

CHAPTER 2: OVERVIEW OF IOT HARDWARE AND SOFTWARE SECURITY ALGORITHMS 18

2.1. INTRODUCTION 18
2.2. RELATED WORK 18
2.3. SELECTED IOT SECURITY ALGORITHMS 22
2.3.1. AES 24
2.3.2. AEGIS 31
2.3.3. ASCON 33
2.3.4. COLM 35
2.3.5. MORUS 36
2.3.6. Deoxys 38
2.3.7. JAMBU 39
2.3.8. NORX 40
2.3.9. SILC 41
2.3.10. OCB 44
2.3.11. TIAOXIN 46

CHAPTER 3: PROPOSED IOT HARDWARE SECURITY PLATFORM 47

3.1. INTRODUCTION 47
3.2. PROPOSED IOT HARDWARE SECURITY PLATFORM OUTLINE 48
3.2.1. Hardware/Software Partitioning 48
3.2.2. Combating Differential Power Analysis Attacks 48

3.2.3. Dynamic Cryptographic Algorithms Hopping....48
PROPOSED IOT HARDWARE SECURITY PLATFORM PURPOSE 49
3.3. PROPOSED IOT HARDWARE SECURITY PLATFORM SOFTWARE TOOLS....51

CHAPTER 4: SW / HW PARTITIONING, IDEA AND RESULTS. 52

4.1. SOFTWARE/HARDWARE PARTITIONING METHODOLOGIES:....52
4.1.1. Softcore Processor Implementation....52
4.1.2. Hardcore Processor along with the FPGA.....54
4.2. SOFTWARE/HARDWARE PARTITIONING SECURITY ENGINE DEVELOPMENT:....59
4.2.1. AEGIS IoT HW/SW Partitioning Engine Development 59
4.3. SOFTWARE/HARDWARE PARTITIONING RESULTS 61
4.3.1. Experiment Setup....61
4.3.2. AEGIS Software/Hardware Partitioning Results....62

CHAPTER 5: SIDE CHANNEL ATTACK RESULTS ON CHOSEN IOT CRYPTOGRAPHIC ALGORITHMS 67

5.1. CHIPWHISPERER HARDWARE ENVIRONMENT....68
5.2. CHIPWHISPERER SOFTWARE ENVIRONMENT 70
5.3. DEVELOPING POWER CONSUMPTION PATTERNS 75
5.4. POWER BASED SIDE CHANNEL ATTACK 82
5.5. DIFFERENTIAL POWER ATTACK ON AES RESULTS 83
5.6. SIDE CHANNEL ATTACKS MATHEMATICAL BACKGROUND....86
5.6.1. Linear Cryptanalysis....87
5.6.2. Linear Approximation Table 88
5.6.3. Differential Cryptanalysis....89
5.6.4. Differential Distribution Table 91
5.7. GENETIC ALGORITHMS BASED SIDE CHANNEL ATTACKS RESISTANCE 93
5.7.1. The Need for Heuristic Search....93
5.7.2. Genetic Algorithms Introduction....93
5.7.3. Side Channel Attacks Resistance Based on Genetic Algorithms Strategy 94
5.7.4. Accelerating the genetic algorithms optimization using cloud-based GPUs on Microsoft Azure.....122

CHAPTER 6 EXTENDED ALGORITHM HOPPING BASED ON PARTIAL DYNAMIC RECONFIGURATION 1244

6.1. DYNAMIC PARTIAL RECONFIGURATION....125
6.2. EXTENDED ALGORITHM HOPPING BASED USING HWICAP DESIGN STEPS....128
6.3. EXTENDED ALGORITHM HOPPING BASED ON PDR RESULTS 141

CONCLUSIONS AND FUTURE WORK 143

REFERENCES 145

APPENDIX A: AES AND TINY-AES CRYPTOGRAPHIC ALGORITHM S-BOX ANALYSIS 151

A.1 AES SUBSTITUTION BOX 151
A.2 AES S-BOX LINEAR APPROXIMATION TABLE....152
A.3 AES S-BOX DIFFERENCE DISTRIBUTION TABLE 158

List of Tables

Table 2-1 Initial state of salsa 20/12 security algorithm 20
Table 2-2 QR function sequence of application in Salsa20/12 cryptographic algorithm 21
Table 2-3 Comparison of the selected cryptographic IoT algorithms. 23
Table 2-4 Rotation amount for both ROL_128_32 and ROL operations.......................36
Table 4-1 List of common softcore processors 53
Table 4-2 Comparison of selected Xilinx ZYNQ SoC chips 55
Table 4-3 Data motion network for sub-bytes RTL and PS..62
Table 4-4 Utilization of Subbytes RTL IP only 63
Table 4-5 Utilization of all generated RTL for the first SW/HW Partitioning scenario (The HW part) 63
Table 4-6 Utilization of all generated RTL for the second SW/HW Partitioning scenario (The HW part) 64
Table 4-7 Utilization of all generated RTL for the third SW/HW Partitioning scenario (The HW part) 66
Table 5-1 CWLITE Top level Verilog Module Ports 69
Table 5-2 Sample of simple serial protocol commands and responses..........................75
Table 5-3 Single run of DPA attack on Tiny-AES inside AT-XMEGA results 83
Table 5-4 Ten runs of the DPA attack on Tiny-AES inside AT-XMEGA results.........84
Table 5-5 Statistics about the 10 DPA attacking trials..85
Table 5-6 Single run of DPA attack on Tiny-AES inside AT-XMEGA with 8000 power traces results 85
Table 5-7 Sample 4 by 4 S-Box 86
Table 5-8 Linear transformation between input bits A_2, and A_3 checking against output bits B_1, B_3 and B_4 combination example..87
Table 5-9 LAT generated for the 4*4 s-box sample given in table 5-7 89
Table 5-10 Output differential computed for an input differential equals 8 applied for the sample s-box...90
Table 5-11 All Differential pair with input differential equals 8 computed for the sample s-box..90
Table 5-12 DDT generated for the 4*4 s-box sample given in table 5-6 92
Table 5-13 SAC mark, balanced mark, non-linearity mark, maximum bias, and maximum propagation ratio for the original tiny-AES s-box 103
Table 5-14 Illustration of the row and column numbers linear relations representations 103
Table 5-15 Proposed mark combinations for the ten genetic algorithms runs.............104
Table 5-16 Security measures profiling values for 10 genetic algorithms runs' generated s-boxes with 300 generations and mark combination 1 105
Table 5-17 Security measures profiling values for 10 genetic algorithms runs' generated s-boxes with 300 generations and mark combination 2 105
Table 5-18 Security measures profiling values for 10 genetic algorithms runs' generated s-boxes with 300 generations and mark combination 3 106

Table 5-19 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 4 106
Table 5-20 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 5 (Multi-threaded)...................107
Table 5-21 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 6 (Multi-threaded)...................107
Table 5-22 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 7 (Multi-threaded)...................108
Table 5-23 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 8 (Multi-threaded)...................108
Table 5-24 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 9 (Multi-threaded)...................109
Table 5-25 Security measures profiling values for 10 genetic algorithms runs’ generated s-boxes with 300 generations and mark combination 10 (Multi-threaded).................109
Table 5-26 Security measures values for 10 genetic algorithms runs’ generated s-boxes with 1000 generations and all 10-mark combinations (Multi-threaded). 110
Table 5-27 Security measures values for 30 genetic algorithms runs’ generated s-boxes with 1000 generations and M6 mark combination (Multi-threaded) 110
Table 5-28 Security measures values for 10 genetic algorithms runs’ generated s-boxes with 2500 generations and mark combination M6 (Multi-threaded) 111
Table 5-29 Security measures values for 10 genetic algorithms runs’ generated s-boxes with 1000 generations, mark combination M6, Pm=10% (Multi-threaded) 112
Table 5-30 Security measures values for 11 genetic algorithms runs’ generated s-boxes with 1000 generations, mark combination M9, Pm=10% (M9-01 to M9-10 are Multi-threaded) 113
Table 5-31 Results for the S-Box based improved genetic algorithms II with the 300 iterations case and marking scheme C1...120
Table 5-32 Results for the S-Box based improved genetic algorithms II with the 1000 iterations case and marking scheme C1...120
Table 5-33 Results for the S-Box based improved genetic algorithms II with the 3000 iterations case and marking scheme C1...121
Table 5-34 Results for the S-Box based improved genetic algorithms II with the 10,000 iterations case and marking scheme C1...121
Table 5-35 Results for the S-Box based improved genetic algorithms II with the 10,000 iterations case , mutation promotion strategy 0 and marking scheme GPU1Elite0. 123
Table 5-36 Results for the S-Box based improved genetic algorithms II with the 10,000 iterations case , mutation promotion strategy 1 and marking scheme GPU1Elite0. 123
Table 6-1 Whole static part: HWICAP IP and AXI Interconnect FPGA utilization....141
Table 6-2 Pure RTL utilizations for the 10 IoT Security Algorithms 141
Table 6-3 Partial reconfiguration block utilization saving the area running the 10 IoT algorithms dynamically 142
Table 6-4 Summary of the area reduction results of algorithm hopping using dynamic partial reconfiguration versus the combined design. 142
Table A.1: AES Algorithm S-Box……………………………………………………151
Table A-2 AES S-Box linear approximation table…………………………………...152

List of Figures

Figure 1-1 Internet of Everything example for a smart city [1] 2
Figure 1-2 The hardware setup done in Cairo University project that I was co-supervised of Vehicle to Vehicle communications IoT application [2] 4
Figure 1-3 The hardware manufactured at Cairo University for the smart electricity meter. 6
Figure 1-4 The hardware manufactured at Cairo University for the smart water meter, this is the board with MSP430FR4133 with the pin headers for the LCD but LCD itself is not mounted 7
Figure 1-5 FHT 6020 and Gamma radiation probes 9
Figure 1-6 IoT market size in billion U.S. dollars..10
Figure 2-1 AES Visualization project in CrypTool...24
Figure 2-2 AES Structure demonstrated by the CrypTool 25
Figure 2-3 Substitution operation applied to the last four bytes of the old key demonstrated by the CrypTool 26
Figure 2-4 Addition of the round constant to the S-Box(K') demonstrated by CrypTool. 26
Figure 2-5 XORing of the first column of the old key with the result from Round constant addition to S-Box(K') demonstrated by the CrypTool 27
Figure 2-6 Last step in each round of the key expansion is the XOR of old key column ith with the generated key column i-1th demonstrated by the CrypTool 27
Figure 2-7 XORing previous round state with the round key to obtain the new round state..28
Figure 2-8 Sub-Bytes operation done in AES core encryption demonstrated by CrypTool...29
Figure 2-9 Shift-rows operation done in AES core encryption demonstrated by CrypTool...29
Figure 2-10 Mix-columns operation, before multiplying the first column of the shift-rows matrix result by the multiplication constants matrix demonstrated by CrypTool .30
Figure 2-11 Mix-columns operation, after multiplying the first column of the shift-rows matrix result by the multiplication constants matrix demonstrated by CrypTool..........30
Figure 2-12 AEAD encryption process 31
Figure 2-13 AEAD decryption process 31
Figure 2-14 ASCON encryption algorithm as per ASCON standard............................34
Figure 2-15 ASCON encryption block diagram as per ASCON standard 34
Figure 2-16 COLM Encryption as per the COLM standard...35
Figure 2-17 Deoxys algorithm as per the original standard 38
Figure 2-18 NORX Encryption structure with parallelism degree =1 as per the NORX standrad...40
Figure 2-19 Folded iteration function used inside the NORX encryption algorithm.....40
Figure 2-20 HASH function block diagram 41
Figure 2-21 ENC function block diagram, used in teh SILC encryption only..............41
Figure 2-22 DEC function block diagram, used in the SILC decryption only..............42
Figure 2-23 PRF function block diagram..42
Figure 2-24 SILC Encryption block diagram...43
Figure 2-25SILC Decryption block diagram..43