شبكة المعلومات الجامعية

بسم الله الرحمن الرحيم

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

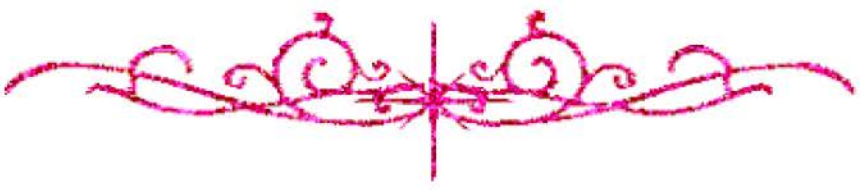
نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

شبكة المعلومات الجامعية

بعض الوثائق الأصلية تالفة



بالرسالة صفحات لم ترد بالأصل

HARDWARE ACCELERATION OF STREAM CIPHER SECURITY ALGORITHMS USING DYNAMIC PARTIAL RECONFIGURATION DPR AND SDSoC TOOLS

By

Sara Taha Mostafa Kamal Taha

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

HARDWARE ACCELERATION OF STREAM CIPHER SECURITY ALGORITHMS USING DYNAMIC PARTIAL RECONFIGURATION DPR AND SDSoC TOOLS

By

Sara Taha Mostafa Kamal Taha

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 Hussein Mohamed

……..

Professor of Electronics
Department of Electronics
Faculty of Engineering, Cairo University

Assoc. Prof. Hassan Mostafa Hassan

……..

Associate Professor of Electronics
Department of Electronics
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

HARDWARE ACCELERATION OF STREAM CIPHER SECURITY ALGORITHMS USING DYNAMIC PARTIAL RECONFIGURATION DPR AND SDSoC TOOLS

By

Sara Taha Mostafa Kamal Taha

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 Hussien Mohamed	**Thesis Main Advisor**
Assoc. Prof. Hassan Mostafa Hassan	**Advisor**
Prof. Dr. Mohamed Riad El-Gonemy	**Internal Examiner**
Prof. Dr. Amr Talaat Abd El-Hamid	**External Examiner**

- Professor, Electronics and Networks department, German University in Cairo

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2021

Engineer's Name:	Sara Taha Mostafa Kamal Taha
Date of Birth:	03/03/1993
Nationality:	Egyptian
E-mail:	sarahtahamostafa@gmail.com
Phone:	01113329637
Address:	15th May City
Registration Date:	01/03/2015
Awarding Date:	…./…./2021
Degree:	Master of Science
Department:	Electronics and Communications Engeneering

Supervisors:	Prof. Dr. Ahmed Hussien Mohamed Khalil Assoc. Prof. Hassan Mostafa Hassan Mostafa
Examiners:	Prof. Dr. Ahmed H. M. Khalil (Thesis main advisor) Assoc. Prof. Hassan M. H. Mostafa (Advisor) Prof. Dr. Mohamed R. El-Gonemy (Internal examiner) Prof. Dr. Amr T. Abd El-Hamid (External examiner) German University in Cairo

Title of Thesis:

Hardware Acceleration of Stream Cipher Security Algorithms using Dynamic Partial Reconfiguration DPR and SDSoC

Key Words:
SDSoC; DPR; Stream Cipher; Security; Hardware Acceleration.

Summary:

With the spread of the fourth industry revolution applications which includes many smart devices like Robots, cloud systems, IoT, cyber security...etc, data security has become one of the most important topics that the world are focuses on it due to the huge amount of data that needs to be transferred from point to point on these applications. Data security means protecting data from corruption or from being disclosed from unauthorized users. This thesis presents different implementations techniques to accelerate stream cipher security algorithms which provide both confidentiality and integrity for a variable length of data. The implementation techniques provided in this thesis are implementation using SDSoC tool, implementation using DPR technique and implementation using both SDSoC and DPR at the same time.

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: Sara Taha Date: ../../2021

Signature:

.

Acknowledgments

All praise to Allah, the sole creator with no partners, the most bestower, the All-Provider, the most merciful, the lord of the lords.

This thesis's journey would have never been completed without the support of certain people whom words will never be fulfilling to how it really feels towards them.

On top of my life's list comes family. My mother, my greatest supporter and fan. The one who would have been the happiest with my achievement today but did not get the chance to witness this moment. I deliver this message to you through the skies to where you are and tell you "Thank you! I miss you and I love you! You're always here, this is your moment as much as it's mine." I cannot thank my father and my sister enough for their huge support. I also want to express the infinite love and joy to my nephew Youssef. It would have never been as fun and joyful to write down the thesis if he was not by my side filling me with laughter and joy. Those people are the backbone, without whom dreams, and achievements would have no meaning. Their continuous support has always pushed me into being a better person for myself and others. Without them, those sleepless nights would have been painful. Again, this will never spare anyone of them their rights towards the support they have always provided and will always continue providing.

I would like to thank Dr. Hassan Mostafa and One Lab team for their enlightening guidance, wise advice, useful suggestions, encouragement, perceptive and continuous feedback throughout the whole thesis.

Last, but not least, special thanks to my best friends for always being supportive.

Table of Contents

Chapter 1 Introduction 1
1.1. MOTIVATION 1
1.2. OVERVIEW OF AUTHENTICATED ENCRYPTION ALGORITHMS 2
1.3. OVERVIEW OF AUTHENTICATED ENCRYPTION APPROACHES 3
1.4. OVERVIEW OF CAESAR COMPETITION 5
1.5. SCOPE OF THESIS 6
1.6. THESIS ORGANIZATION 6

Chapter 2 Literature Review 7
2.1. OVERVIEW OF THE IOT SECURITY 7
2.2. MEANING OF CRYPTOGRAPHY AND THE DIFFERENT SECURITY'S ASPECTS DEFINITIONS. 7
2.3. OVERVIEW OF CAESAR COMPETITION STREAM CIPHERS. 9
2.3.1. ACORN DESCRIPTION 9
2.3.2. AEGIS DESCRIPTION 11
2.3.3. MORUS DESCRIPTION 16
2.3.4. TIAOXIN DESCRIPTION 19
2.4. OVERVIEW OF IMPLEMENTATION TECHNIQUES. 24
2.4.1. SOFTWARE IMPLEMENTATION 24
2.4.2. HARDWARE IMPLEMENTATION 24
2.4.3. IMPLEMENTATION USING SDSOC 25
2.4.3.1. SDSOC PROJECT CREATION 26
2.4.3.2. IMPLEMENTATION OF THE FUNCTION USING PROGRAMMABLE LOGIC 27
2.4.3.3. DEFINE HARDWARE FUNCTION INTERFACES 27
2.4.3.4. EVALUATION BOARD SETUP 28
2.4.4. IMPLEMENTATION USING DPR 29

Chapter 3 Implementation using SDSoC 32
3.1. SDSOC PLATFORM AND SETTINGS. 32
3.2. ACORN IMPLEMENTATION USING SDSOC. 34
3.3. AEGIS IMPLEMENTATION USING SDSOC. 38
3.4. MORUS IMPLEMENTATION USING SDSOC. 42
3.5. TIAOXIN IMPLEMENTATION USING SDSOC. 45
3.6. RESULTS OF SDSOC IMPLEMENTATIONS. 48

Chapter 4 Implementation using DPR 51
4.1. ABOUT DPR (THE NEED FOR AND USAGE). 51
4.2. PERFORMANCE OF HARDWARE IMPLEMENTATION FOR AUTHENTICATED ENCRYPTION STREAM CIPHERS. 53

4.2.1. HARDWARE IMPLEMENTATION PERFORMANCE..... 54
4.2.2. ACORN PERFORMANCE AFTER MODIFICATIONS. 55
4.3. IMPLEMENTATION FLOW 57
4.3.1. CUSTOM IP CREATION 57
4.3.2. DPR FLOW 59
4.3.2.1 CREATE NEW PROJECT AND ADD THE REQUIRED IP. 59
4.3.2.2 CREATE SYSTEM WRAPPER AND GENERATE SYNTHESIS DESIGN 60
4.3.2.3 READ THE FIRST CONFIGURATION VHDL FILES AND GENERATE SYNTHESIS DESIGN 61
4.3.2.4 READ THE SECOND CONFIGURATION VHDL FILES AND GENERATE SYNTHESIS DESIGN 62
4.3.2.5 READ THE THIRD CONFIGURATION VHDL FILES AND GENERATE SYNTHESIS DESIGN 62
4.3.2.6 SET THE FLOOR PLAN TO DEFINE THE RECONFIGURABLE AND THE STATIC PARTS 63
4.3.2.7 SET THE EXTERNAL PINS CONFIGURATION 64
4.3.2.8 RUN DRC 65
4.3.2.9 IMPLEMENT THE FIRST CONFIGURATION 65
4.3.2.10 REPORT POWER CONSUMPTION AND AREA UTILIZATION OF THE FIRST CONFIGURATION 65
4.3.2.11 LOCK DESIGN CONFIGURATION AND REPLACE THE RECONFIGURABLE MODULE WITH BLACK BOX 66
4.3.2.12 REPEAT THE PREVIOUS THREE STEPS FOR THE SECOND AND THE THIRD CONFIGURATION 66
4.3.2.13 CREATE BLANKING CONFIGURATION 66
4.3.2.14 VERIFY ALL CONFIGURATIONS 67
4.3.2.15 GENERATE FULL AND PARTIAL BITSTREAM FILES 67
4.3.2.16 WRITE THE SOFTWARE TESTCODE 68
4.4. DPR RESULTS 70

Chapter 5 Implementation using SDSoC and DPR 73
5.1. SDSOC PERFORMANCE OPTIMIZATION 75
5.2. DPR FLOW WITH THE SDSOC TOOL 78
5.3. C++ CODE MODIFICATION TO INCLUDE THE DPR ON THE SDSOC TOOL 81
5.4. RESULTS 82

Discussion and Conclusion 86
REFERENCES 88
الملخص ..... أ

List of Tables

Table 1: comparison between stream, block and dedicated ciphers 3
Table 2: corresponding mode of operation for Ca & Cb variables 11
Table 3: SDSoC performance for all algorithms' hardware functions 48
Table 4: SDSoC performance in terms of speed for all stream ciphers' algorithms 49
Table 5: SDSoC performance for all algorithms in terms of slice utilization and Figure of Merit 50
Table 6: performance of all algorithms in terms of speed, power consumption and area utilization 54
Table 7: ACORN-v3-32bit performance 56
Table 8: DPR Area Utilization 71
Table 9: DPR Power Consumption 71
Table 10: the performance of hardware function using ZCU104 and real time processor 82
Table 11: the performance of all algorithms using SDSoC only after modification 82
Table 12: DPR and SDSoC performance in terms of speed 83
Table 13: DPR and SDSoC hardware functions' performance in terms of area and power 85

List of Figures

Figure 1: Authenticated Encryption Stream Cipher....4
Figure 2: ACORN state update registers [9]....9
Figure 3: AES block diagram [32]....14
Figure 4: state update registers of AEGIS_128L algorithm [33]....15
Figure 5: state update registers of MORUS-V2 [11]....18
Figure 6: state update registers for Tiaoxin-346v2 [33] 21
Figure 7: SDSoC design flow [19]....26
Figure 8: FPGA dynamic partial reconfiguration [27] 29
Figure 9: DPR using PCAP....30
Figure 10: ACORN implementation using SDSoC 35
Figure 11: ACORN platform on ZC702 Evaluation Kit....37
Figure 12: AEGIS implementation using SDSoC 39
Figure 13: MORUS implementation using SDSoC....42
Figure 14: Tiaoxin implementation using SDSoC....45
Figure 15: Area utilization of the FPGA resources 49
Figure 16: block diagram of ACORN....53
Figure 17: AEGIS and MORUS block diagrams....53
Figure 18: AEGIS and MORUS cipher-core interfaces 55
Figure 19: ACORN Cipher Core interfaces....56
Figure 20: Custom IP block Diagram 58
Figure 21: Custom IP Components....58
Figure 22: AEAD interfaces on DPR project 59
Figure 23: DPR floorplan for ZYNQ ZC702 implementation....64
Figure 24: ACORN implementation....70
Figure 25: AEGIS implementation 70
Figure 26: MORUS implementation....71
Figure 27: platform of stream cipher algorithms using DPR and SDSoC....79
Figure 28: ACORN floor plan for DPR with SDSoC implementation....83
Figure 29: AEGIS floor plan for DPR with SDSoC implementation....84
Figure 30: MORUS floor plan for DPR with SDSoC implementation 84