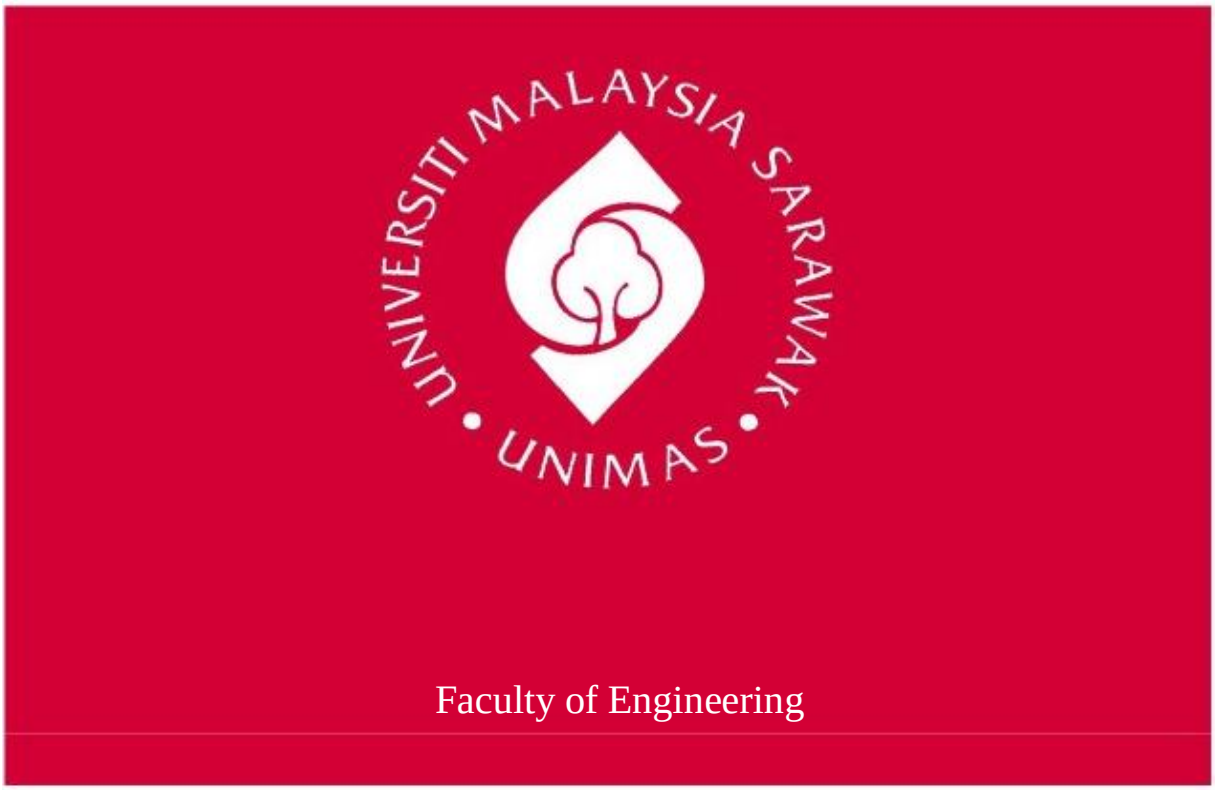

DESIGN AND IMPLEMENTATION OF RIPEMD-160 ALGORITHM ON RECONFIGURABLE HARDWARE

Florisca Aldina Godulus

Bachelor of Engineering (Hons)

In Electronics (Telecommunications)

2019

UNIVERSITI MALAYSIA SARAWAK

Grade: A-

Please tick (√)

Final Year Project Report ☑

Masters ☐

PhD ☐

DECLARATION OF ORIGINAL WORK

This declaration is made on the 12 day of June 2019

Student's Declaration

I Florisca Aldina Goduus, 50517, Faculty Of Engineering

(PLEASE INDICATE STUDENT'S NAME, MATRIC NO. AND FACULTY) hereby declare that the work entitled Design and Implementation of Ripemd-160 on Reconfigurable Hardware is my original work. I have not copied from any other students' work or from any other sources except where due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

12/6/2019
Date submitted

FLORISCA ALDINA GODUUS (50517)
Name of the student (Matric No.)

Supervisor's Declaration:

I SHAMSIAH BINTI SUHAILI (SUPERVISOR'S NAME) hereby certifies that the work entitled DESIGN AND IMPLEMENTATION OF RIPEMD-160 ON RECONFIGURABLE HARDWARE (TITLE) was prepared by the above named student, and was submitted to the "FACULTY" as a * partial/full fulfillment for the conferment of BACHELOR OF ENGINEERING (HONS) in ELECTRONICS (TELECOMUNICATIONS) (PLEASE INDICATE THE DEGREE), and the aforementioned work, to the best of my knowledge, is the said student's work.

Received for examination by: _____ Date: 12/6/2019

(Name of the supervisor)
SHAMSIAH BINTI SUHAILI

I declare that Project/Thesis is classified as (Please tick (√)):

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*
☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*
☑ **OPEN ACCESS**

Validation of Project/Thesis

I therefore duly affirmed with free consent and willingness declare that this said Project/Thesis shall be placed officially in the Centre for Academic Information Services with the abiding interest and rights as follows:

- This Project/Thesis is the sole legal property of Universiti Malaysia Sarawak (UNIMAS).
- The Centre for Academic Information Services has the lawful right to make copies for the purpose of academic and research only and not for other purpose.
- The Centre for Academic Information Services has the lawful right to digitalise the content for the Local Content Database.
- The Centre for Academic Information Services has the lawful right to make copies of the Project/Thesis for academic exchange between Higher Learning Institute.
- No dispute or any claim shall arise from the student itself neither third party on this Project/Thesis once it becomes the sole property of UNIMAS.
- This Project/Thesis or any material, data and information related to it shall not be distributed, published or disclosed to any party by the student except with UNIMAS permission.

Student signature _____ (Date) 12/6/2019

Supervisor signature: _____ (Date) 12/6/2019

Current Address:
Kampung Pangkalan Lama 94257 Tamparuli Sabah

Notes: * If the Project/Thesis is **CONFIDENTIAL** or **RESTRICTED**, please attach together as annexure a letter from the organisation with the period and reasons of confidentiality and restriction.

[The instrument is duly prepared by The Centre for Academic Information Services]

UNIVERSITI MALAYSIA SARAWAK

Grade: _____

Please tick (√)

Final Year Project Report ☑

Masters ☐

PhD ☐

DECLARATION OF ORIGINAL WORK

This declaration is made on the 12 day of June 2019.

Student's Declaration:

I Florisca Aldina Godulus, 50517, Faculty Of Engineering

(PLEASE INDICATE STUDENT'S NAME, MATRIC NO. AND FACULTY) hereby declare that the work entitled Design and Implementation of Ripemd-160 on Reconfigurable Hardware is my original work. I have not copied from any other students' work or from any other sources except where due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

12/6/2019
Date submitted

FLORISCA ALDINA GODULUS (50517)
Name of the student (Matric No.)

Supervisor's Declaration:

I SHAMSIAH BINTI SUHAILI (SUPERVISOR'S NAME) hereby certifies that the work entitled DESIGN AND IMPLEMENTATION OF RIPEMD-160 ON RECONFIGURABLE HARDWARE (TITLE) was prepared by the above named student, and was submitted to the "FACULTY" as a * partial/full fulfillment for the conferment of BACHELOR OF ENGINEERING (HONS) in ELECTRONICS (TELECOMMUNICATIONS) (PLEASE INDICATE THE DEGREE), and the aforementioned work, to the best of my knowledge, is the said student's work.

Received for examination by: _____ Date: 12/6/2019

(Name of the supervisor)
SHAMSIAH BINTI SUHAILI

I declare that Project/Thesis is classified as (Please tick (√)):

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*
☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*
☑ **OPEN ACCESS**

Validation of Project/Thesis

I therefore duly affirmed with free consent and willingness declare that this said Project/Thesis shall be placed officially in the Centre for Academic Information Services with the abiding interest and rights as follows:

- This Project/Thesis is the sole legal property of Universiti Malaysia Sarawak (UNIMAS).
- The Centre for Academic Information Services has the lawful right to make copies for the purpose of academic and research only and not for other purpose.
- The Centre for Academic Information Services has the lawful right to digitalise the content for the Local Content Database.
- The Centre for Academic Information Services has the lawful right to make copies of the Project/Thesis for academic exchange between Higher Learning Institute.
- No dispute or any claim shall arise from the student itself neither third party on this Project/Thesis once it becomes the sole property of UNIMAS.
- This Project/Thesis or any material, data and information related to it shall not be distributed, published or disclosed to any party by the student except with UNIMAS permission.

Student signature _____ (Date) 12/6/2019

Supervisor signature: _____ (Date) 12/6/2019

Current Address:
Kampung Rangalau Lama 89257 Tamparuli Sabah

Notes: * If the Project/Thesis is **CONFIDENTIAL** or **RESTRICTED**, please attach together as annexure a letter from the organisation with the period and reasons of confidentiality and restriction.

[The instrument is duly prepared by The Centre for Academic Information Services]

DESIGN AND IMPLEMENTATION OF RIPEMD-160 ALGORITHM ON RECONFIGURABLE HARDWARE

FLORISCA ALDINA GODULUS

A final year project report submitted in partial fulfilment of
the requirement for the degree of
Bachelor of Engineering (Hons) in Electronics (Telecommunications)

Faculty of Engineering
Universiti Malaysia Sarawak

2019

To my beloved family and friends.

ACKNOWLEDGEMENT

I would like to extend my sincere gratitude to everyone who gives me the opportunity to complete this report. A special gratitude I give to my final year project supervisor, Miss Shamsiah Suhaili of University Malaysia Sarawak from Electrical and Electronic department for her contribution in stimulating suggestions and encouragement, help me to coordinate my project especially in writing this project. I would also intend to extend my praise to my family members for their infinite love, support and encouragement to complete my four year undergraduate study. Special thanks to my fellow course mates for their motivations during the whole time of my final year project. I could not express how much gratitude towards those who helped me but sincerely wishes all of them the best in everything now and then.

ABSTRACT

Nowadays information security is the highest priority as it is intended to protect information that has value to people and organizations. It involves more than protecting the information itself. However, computer networks have a lot of vulnerabilities and threats. Previously, many encryption algorithms have been investigated. The Cryptography Algorithm is used to protect data through encryption that allows sensitive information to be passed through the network safely. The data is securely encrypted in a way that no third party can access it except the intended recipient. The cryptography can also verify the authenticity of the sender. It prove that the sender was legitimate and not an impostor. Further, the hash function uses a mathematics conversion to inevitable “encrypt” messages to provide a digital fingerprint. Basically it is used for message digest. One of the algorithms in hash function is RIPEMD-160. The RIPEMD-160 can improve the security in storing information. This project used iterative method to investigate the security algorithm and implemented the algorithm. Besides that, iterative methods also used to improve the frequency, power and are requirements performance of RIPEMD-160 hash function. It is implemented using Verilog HDL software and simulated using the ModelSim software. The efficiency of the result is determined for the maximum of the frequency at 136 MHz and the area is at 692.9 Mbps from the Quartus II software platform.

ABSTRAK

Keselamatan maklumat pada masa kini adalah keutamaan tertinggi kerana ia bertujuan untuk melindungi maklumat yang mempunyai nilai kepada orang ramai dan organisasi. Ini melibatkan lebih daripada melindungi maklumat itu sendiri. Walau bagaimanapun, rangkaian komputer mempunyai banyak kelemahan dan ancaman. Sebelum ini, banyak algoritma enkripsi telah disiasat. Algoritma kriptografi digunakan untuk melindungi data melalui enkripsi yang membolehkan maklumat sensitif melalui rangkaian dengan selamat. Data tersebut dienkripkan dengan selamat dengan cara yang tidak ada pihak ketiga yang dapat mengaksesnya kecuali penerima yang dimaksudkan. Kriptografi juga boleh mengesahkan kesahihan penghantar. Ia membuktikan bahawa pengirim adalah sah dan bukan seorang penipu. Selanjutnya, fungsi hash menggunakan penukaran matematik kepada mesej "enkripsi" yang tidak dapat dielakkan untuk memberikan cap jari digital. Pada dasarnya, ia digunakan untuk mencerna mesej. Salah satu algoritma dalam fungsi hash adalah RIPEMD-160. RIPEMD-160 boleh meningkatkan keselamatan dalam menyimpan maklumat. Projek ini menggunakan kaedah iteratif untuk menyiasat algoritma keselamatan dan melaksanakan algoritma. Ia dilaksanakan dengan menggunakan perisian Verilog HDL dan disimulasikan menggunakan ModelSim. Hasil projek ditentukan melalui keputusan frekuensi maksimum pada 136 MHz dan keluasan pada 692.9 Mbps dari platform Quartus II.

TABLE OF CONTENT

		Page
ACKNOWLEDGEMENT		i
ABSTRACT		ii
ABSTRAK		iii
TABLE OF CONTENT		iv
LIST OF TABLES		vi
LIST OF FIGURES		vii
LIST OF ABBREVIATIONS		x
Chapter 1	**INTRODUCTION**	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objectives	2
	1.4 Scope of Project	3
	1.5 Expected Outcome	3
	1.6 Project Outline	4
Chapter 2	**LITERATURE REVIEW**	
	2.1 Introduction to Cryptography	6
	2.2 The Cryptography Algorithm	7
	2.3 Hash Function	9
	2.4 Application of Hash Function	11
	2.5 RIPEMD-160	16

2.6 Methods of Researchers 16

2.6.1 Iterative Architecture 16

2.6.2 Pipeline Design Architecture 18

Chapter 3 Methodology

3.1 Software 22

3.1.1 Altera Quartus II 22

3.1.2 Verilog HDL 24

3.1.3 ModelSim 27

3.2 RIPEMD-160 Algorithm 29

3.3 Cryptography Algorithm Coding Assembly 39

3.4 Proposed Method of RIPEMD-160 40

3.4.1 Iterative Design of RIPEMD-160 41

Chapter 4 Results and Discussion

4.1 RIPEMD-160 design 43

4.2 Simulation and Synthesis Analysis 53

4.3 Comparison of Maximum Frequency 70

4.4 Throughput of the design 71

4.5 Comparison of RIPEMD-160 iterative design with other Research 72

Chapter 5 Conclusion

5.1 Conclusion 74

5.2 Recommendation 75

REFERENCES 76

APPENDIX 80

LIST OF TABLES

Table		Page
3.1	Initial Value	30
3.2	Constant	31
3.3	Message Selection	32
3.4	Shift Value	33
4.1	Initial values of RIPEMD-160	45
4.2	The values of K_const and K_const1	48
4.3	Output value of RIPEMD-160 compression function in the left side T[i]	57
4.4	Output value of RIPEMD-160 compression function in the right side T[i]	58
4.5	The comparison of maximum frequency with different device family	71
4.6	The throughput of different device family	72
4.7	The comparison of proposed RIPEMD-160 with other research	73

LIST OF FIGURES

Figure		Page
2.1	The Illustrated Cryptography of Symmetry	7
2.2	The Illustrated CryptographyAsymmetric	8
2.3	The Three types of Cryptography Algorithms	8
2.4	Classification of Techniques of Cryptography	9
2.5	Illustrated Function of Hash	10
2.6	Illustration of Collision-resistance	10
2.7	Illustration of Second Pre-image Resistance	11
2.8	Illustration of Pre-image Resistance	11
2.9	Model of Digital Signatures	12
2.10	Process of Message Authentication Code	13
2.11	Storing hash instead of password	14
2.12	Verification of the password using the hash function	15
2.13	Checking data integrity process	15
2.14	Iterative Architecture of RIPEMD-160	17
2.15	RIPEMD-160 core 5-stage pipeline architecture	18
2.16	A single RIPEMD-160 operation block	19
2.17	RIPEMD-160 Core	20
3.1	Quartus II Design Flow	23
3.2	The three levels of Verilog HDL	25

3.3	Top down ASIC Design Flow	26
3.4	Top down ASIC Design Flow (cont.)	26
3.5	The Simulation Flow	27
3.6	ModelSim in Altera Quartus II	28
3.7	Create a file with a waveform	29
3.8	Waveform Simulation Editor	29
3.9	The Top Level of RIPEMD-160	34
3.10	Compression Function of RIPEMD-160 Hash Function	35
3.11	Gate of Function logic 1 (F1)	36
3.12	Gate of Function logic 2 (F2)	36
3.13	Gate of Function logic 3 (F3)	36
3.14	Gate of Function logic 4 (F4)	37
3.15	Gate of Function logic 5 (F5)	37
3.16	Gate of Function logic 1 (F’1)	37
3.17	Gate of Function logic 2 (F’2)	38
3.18	Gate of Function logic 3 (F’3)	38
3.19	Gate of Function logic 4 (F’4)	38
3.20	Gate of Function logic 5 (F’5)	39
3.21	Flow Chart of Cryptography Algorithm Process	40
3.22	RIPEMD-160 Iterative Architecture Design	42
4.1	RTL netlist viewer of RIPEMD160c design	44
4.2	Counter block module	47
4.3	Coder block module	47
4.4	Kconst_ripemd block module	48

4.5	Message_ripemd block module	49
4.6	Multiplexer block module	50
4.7	Function_ripemd_parallel block module	51
4.8	Hash block module	52
4.9	Hash_rmd block module	52
4.10	Synthesis and Analysis Report in Quartus II	53
4.11	Full simulation of RIPEMDc design	55
4.12	Hash output for input string “abc”	56
4.13	RIPEMD-160 hash output from HashCalc	57
4.14	Maximum frequency with device of the Arria II GX family	71

LIST OF ABBREVIATION

ASIC	-	Application Specific Integrated Circuit
CAD	-	Computer Aided Design
CPLD	-	Complex Programmable Logic Device
FPGA	-	Field Programmable Gate Array
HDL	-	Hardware Description Language

CHAPTER 1

INTRODUCTION

1.1 Project Background

Presently various applications incorporate authenticating services. Digital signature algorithm applications, which is used to authenticate services such as mobile services, electronic mail, peer-to-peer file sharing networks, electronic funds transfer and so on is based on the use of critical cryptography primitive of hash functions [1]. Therefore, security issues are important in this high-tech internet. Sensitive information is kept in a networked computer and transmitted through a various types of unprotected networks.

Cryptography is the scientific field that offered security over internet. It is an important weapon to protect and secured the sensitive data. All applications were previously considered as validation modules that include nested hash functions in application execution[2]. The hash function labeled as message digest algorithm is an input message transformation and returns a fixed-size string called the hash value. To identify message from the initial messages, the hash is simple but complicated. Finding the other hash value that has the same hash as the initial message is also difficult.

This project aims to determine some of the terms and concepts behind the algorithm of cryptography and observe how it is being used today. The second purpose is to give the real example of cryptography applications and discuss the performance of implementation.

1.2 Problem Statement

Information security is very important as it aims to protect sensitive and important information. This is because once the information is saved on the computer system it will be processed by the software and delivered via communication. Each of these areas must be protected as well. The main goal of information security is to prevent data theft from hackers. Nowadays there are many security issues involving hacking and stealing information form internet. This makes users worry and scared to use and store their data in any online applications.

However, the cryptography algorithms such as the hash functions are very useful in order to prevent information from leaking. The hash algorithm will help users to securely encrypt the information so that no third party, except the intended recipient, can read it. The cryptography algorithm have been widely used and developed to improve the security system from time to time.

In this project, the RIPEMD-160 hash algorithm was investigated to find the error detection during transmission of information. There are some research that have been done to improve the security of RIPEMD-160 which produces hashes that are difficult to decrypt. A lot of method has been proposed to improve RIPEMD-160 performance. In this project, the design of reconfigurable architecture RIPEMD-160 hash function is iterative to increase the throughput so that the unauthorized person cannot hack or attack the information.

1.3 Objective

This project's goals are:

- To design and implement the RIPEMD-160 hash function algorithm by using Verilog HDL.
- To analyze the algorithm for cryptography.

- To improve the frequency, power and area requirements performance of RIPEMD-160 hash function.

1.4 Scope of Project

This project is to create design of RIPEMD-160 hash function by using CAD Tool (Altera Quartus II) to improve the maximum frequency, power and area. The algorithm is designed using Altera Quartus II and simulated using ModelSim. The coding is entered and executed in Verilog HDL to confirm it is synthesized and functionally simulated. A design of iterative RIPEMD-160 hash function architecture will be proposed to improve the performance of the throughput and study the effects of iterative on speed and area requirements. A further study and analysis will be made to previous research of iterative to make sure that RIPEMD-160 architecture can give the fastest and best performance after implementation process has been done.

1.5 Expected Outcome

Expected outcome for this project is the student will be able to design and implement program that is related to RIPEMD-160 hash function for satisfying the different trims of complement security and to prevent the challenged hash attacks by increasing the complication level of the proposed algorithm. Altera Quartus II and ModelSim will be used to design and simulate the result of RIPEMD-160 hash function algorithm respectively.

1.6 Project Outline

Chapter 1 Introduction

Chapter 1 will discuss the project background, problem statement, goals, project scope and project outline.

Chapter 2 Literature Review

Chapter 2 will focus on the previous research study. In order to increase the performance and give a highly acceptable result, as shown in results and discussions, there will be a comparison between previous project and current project.

Chapter 3 Methodology

Chapter 3 will discuss the methodology on how the project is implemented using software, design, development and method. The project implementation will be discussed in this chapter 4. The flow chart of this project is as follow:

- Altera Quartus II Flow Chart
- ModelSim Flow Chart
- Overall Process of RIPEMD-160 Hash Function Flow Chart
- Cryptographic Process Flow Chart
- RIPEMD-160 Algorithm Flow Chart

Chapter 4 Results and Discussion

The input and output of ModelSim simulation will be discussed in Chapter 4. The maximum frequency of the iterative design of RIPEMD-160 will be compared with different device family. The design performance will be calculated. Comparison was made between the proposed iterative design of RIPEMD-160 and other research.

Chapter 5 Conclusion

Chapter 5 discusses the overall project and concludes it by referring to the outcome in Chapter 4. Recommendations for future improvements have been made. Compare the maximum frequency of RIPEMD-160 iterative design with different device family.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction to Cryptography

In Greek words, the meaning of cryptography is “hidden” kryptós, and “to write” gráphein, or in other words “hidden writing”[3]. Cryptography is the science and art of transforming messages into an unintelligible form while being transmitted or stored so that unauthorized users cannot access it. Some professionals state thatafter writing has been developed, the applications start from a political memorandum to a war plans [4]. Cryptography enables people to store or transmit information across unsafe networks to block others from access it. The cryptography has a unique way to represent the information by encryption and decryption using mathematics[5]. The cryptography provides the basic protections, such as

1. Privacy or Confidentiality: To ensure just the permitted user can read the information.
2. Integrity: To satisfy the receiver can receive message that has not been developed in any policy from the first message.
3. Availability: To ensure that the information can be access to authorized users.
4. Authenticity: To verify the identity of the user.
5. Non-repudiation: To confirm that a user performed an action.