UNIVERSITI PUTRA MALAYSIA

A COLLISION RESISTANT CRYPTOGRAPHIC HASH FUNCTION BASED ON CELLULAR AUTOMATA RULES

NORZIANA JAMIL

FSKTM 2013 1

A COLLISION RESISTANT CRYPTOGRAPHIC HASH FUNCTION BASED ON CELLULAR AUTOMATA RULES

By

NORZIANA JAMIL

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

February 2013

DEDICATION

I dedicate this thesis to my beloved late father, Hj Jamil Hj Omar and my beloved mother, Hjh Asmah Sarbini . . .

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A COLLISION RESISTANT CRYPTOGRAPHIC HASH FUNCTION BASED ON CELLULAR AUTOMATA RULES

By

NORZIANA JAMIL

February 2013

Chair: Prof. Dr. Ramlan Mahmod, PhD

Faculty: Computer Science and Information Technology

The subject of this thesis is the study of collision resistant hash function. A cryptographic hash function is one of the cryptographic primitives designed to protect the integrity of data such as that in digital signatures and online business transactions. Popular hash functions are Message Digest 4/5 (MD-4/5), Secure Hashing Algorithm (SHA-0/1) and RIPEMD, which are referred to as MDx-class hash functions due to some commonalities in their design with the MD-family. However, recent advances in cryptanalysis have led to the failure of these hash functions in preserving the strongest property called collision resistance. Factors contributing to the failure are a mathematical weakness found in the Boolean functions used by these cryptographic hash functions, linear message expansion and poor diffusion in the step operation.

This study proposes a design framework for collision resistant hash function. The framework divides requirements for the design of hash function into three classifications namely design requirements, security requirements for Boolean function and

analysis requirements. Following the framework introduced here, a dedicated cryptographic hash function named STITCH-256 was introduced. In STITCH-256 design, an improved formula for message expansion and a step operation that employs a novel permutation technique for better bit propagation, which is called the stitching permutation, are introduced. For the improved formula for message expansion, the study shows that the formula produces higher codewords with minimal weight as compared to the existing formula of message expansion. This leads the effort of attackers to construct differential characteristics with high probability becomes more difficult and challenging. In the step operation that employs a novel stitching permutation, the study shows that the bit propagations are higher and no sufficient condition can be given to construct differential characteristics with high probability. Thus, it is very difficult to find inner collisions in the compression function of STITCH-256. For the second classification in the framework, the study examines the cryptographic properties of 256 one-dimensional Cellular Automata (CA) rules to find cryptographically strong Boolean functions. The study shows that 23 of the rules are cryptographically strong where eight of them are used in our hash function design. Following the third classification of the framework, STITCH-256 is analyzed against all the generic attacks and is measured against its avalanche effect and randomness. The security analysis shows that STITCH-256 is resistant against all the generic attacks and it is very difficult to construct a small list of conditions that gives a successful construction of collision path. The experiments to measure the avalanche effect involved 3000 samples of 512-bit input message and it has been shown that the average avalanche factor for STITCH-256 for these 3000 sequences is 0.5, which is the desired avalanche factor in cryptographic primitives. The 3000 sequences of 256-bit hash values are tested for randomness using NIST Statistical Tests and the results show that the output values from STITCH-256 for these sequences are random. This study also includes a comparison between STITCH-256 and other

MDx-class hash functions. The comparison shows that STITCH-256 employs fewer operations which lead to faster computation.

From the security analysis carried out in this thesis, we believe that STITCH-256 is a strong collision resistant hash function. This is due to its new non-linear recursive function for message expansion that gives higher codewords with minimal weight, its step operation that employs stitching permutation in a target-heavy Balanced Feistel Network that gives no set of conditions for the construction of collision path using established differential attack being constructed, and cryptographically strong Boolean function used in the compression function of STITCH-256 that gives strong non-linearity and diffusion property.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

FUNGSI CINCANG KRIPTOGRAFI YANG TAHAN PERTEMBUNGAN BERASASKAN PERATURAN-PERATURAN SEL AUTOMATA

Oleh

NORZIANA JAMIL

Februari 2013

Pengerusi: Profesor Ramlan Mahmod, PhD

Fakulti: Sains Komputer dan Teknologi Maklumat

Penyelidikan ini mengkaji fungsi cincang kriptografi yang tahan pertembungan. Fungsi cincang kriptografi adalah salah satu daripada primitif kriptografi, yang direka untuk melindungi integriti data sebagaimana yang digunakan dalam tandatangan digital dan transaksi bisnes atas talian. Fungsi cincang yang digunakan secara meluas dalam aplikasi ini adalah Fungsi Cincang 5 (MD-5), Algoritma Cincang Selamat (SHA-0/1) dan RIPEMD, juga dikenali sebagai fungsi cincang khusus kerana reka bentuknya yang sesuai untuk implementasi yang pantas. Walaubagaimanapun, aktiviti memecahkan fungsi cincang ini sangat terkedepan sehingga menyebabkan fungsi cincang ini gagal untuk mengekalkan kriterianya yang paling penting, yang dikenali sebagai ketahanan pertembungan. Faktor yang menyebabkan kegagalan ini adalah disebabkan kelemahan yang dikenalpasti dalam fungsi matematik yang digunakan dalam fungsi cincang ini, formula pemgembangan mesej yang sekata dan penyerapan yang lemah di dalam langkah operasi.

Penyelidikan ini mencadangkan satu kerangka reka bentuk untuk fungsi cincang yang tahan pertembungan. Ia dibahagikan kepada beberapa klasifikasi iaitu keperluan reka bentuk, keperluan keselamatan fungsi Boolean dan keperluan analisa keselamatan. Rentetan dari kerangka ini, fungsi cincang kriptografi yang tahan pertembungan, yang dinamakan sebagai STITCH-256 diperkenalkan. Dalam reka bentuk STITCH-256, formula untuk mengembangkan mesej yang diperbaiki dan langkah operasi yang mengaplikasikan teknik baru untuk permutasi yang dikenali sebagai permutasi jahitan, diperkenalkan. Untuk formula pengembangan mesej yang diperbaiki, kajian kami menunjukkan ia telah menghasilkan jumlah yang tinggi untuk kod mesej berpemberat rendah. Ini adalah penemuan yang sangat baik kerana ia mengakibatkan usaha dari penyerang kod untuk membina jalan pertembungan adalah sangat sukar. Untuk langkah operasi yang mengaplikasikan teknik jahitan, kajian kami menunjukkan bahawa pembiakan bit adalah lebih tinggi dan adalah sangat sukar untuk penyerang kod untuk membila jalan pertembungan pada kadar yang tinggi. Seterusnya untuk klasifikasi keperluan keselamatan fungsi Boolean, tesis ini mengkaji tentang kriteria kriptografi yang dipunyai oleh 256 peraturan sel automata berdimensi satu. Kajian menunjukkan bahawa 23 daripada peraturan sel ini mempunyai kriteria kriptografi yang kuat dan kami menggunakan 8 peraturan daripada mereka di dalam reka bentuk fungsi cincang STITCH-256. Bagi klasifikasi ketiga, STITCH-256 telah dianalisis ke atas semua serangan umum dan dikirakan faktor runtuhan dan kerawakannya. Analisis keselamatan yang telah dijalankan menunjukkan bahawa STITCH-256 mempunyai ketahanan ke atas kesemua jenis serangan umum dan sangat sukar untuk membina jalan pertembungan yang boleh menggagalkan fungsi cincang STITCH-256 ini. Eksperimen untuk mengukur kesan runtuhan melibatkan 3000 sampel mesej yang bernilai 512 bit setiap satu, di mana keputusan eksperimen menunjukkan faktor runtuhan secara keseluruhan untuk STITCH-256 adalah 0.5. Ini adalah nilai yang sangat dikehendaki dalam semua algoritma kriptografi. Kemudian, sebanyak 3000 sampel yang mengandungi nilai cincang sebanyak 256 bit setiap satu diuji kerawakannya menggunakan ujian statistik yang diperkenalkan oleh NIST dan keputusan menunjukkan nilai hasil dari STITCH-256 untuk kesemua sampel ini adalah rawak. Penyelidikan ini juga membuat perbandingan antara STITCH-256 dengan fungsi cincang yang digunakan secara meluas, dari segi jumlah operasi yang digunakan secara keseluruhan. Perbandingan yang telah dibuat menunjukkan bahawa STITCH-256 mempunyai bilangan operasi yang kurang berbanding fungsi cincang yang lain, sekaligus menjadikan STITCH-256 lebih laju dari segi pengiraan dan implementasinya.

Daripada analisis keselamatan yang telah dilakukan di dalam penyelidikan ini, kami percaya bahawa STITCH-256 adalah satu fungsi cincang kriptografi yang kuat. Ini adalah disebabkan oleh komponennya yang baharu iaitu formula pengembangan mesej yang tidak sekata yang memberikan lebih banyak mesej kod berpemberat rendah, langkah operasi yang mempunyai permutasi jahitan yang menjadikan pembinaan kondisi untuk pertembungan sebagai sangat sukar dan fungsi Boolean yang kuat secara kriptografinya yang memberikan nilai ketidak-sekataan dan kekeliruan yang tinggi.

ACKNOWLEDGEMENTS

All praise to the Almighty ALLAH SWT for it is through His Grace and Mercy that I am able to complete this thesis on time and to the satisfaction of the university.

I would like to express my gratitude to my supervisor, Prof. Dr. Ramlan Mahmod for his assistance and guidance. I am also deeply grateful to my co-supervisors, Assoc. Prof. Dr Nur Izura Udzir, Assoc. Prof. Dr. Zuriati Ahmad Zukarnain and Dr. Muhammad Reza Z'aba, and my thesis examiners, Assoc. Prof. Dr. Azmi Jaafar, Assoc. Prof. Dr. Mohd. Rushdan Md. Said and Prof. Dr. Ir. Bart Preneel, for their support, constructive comments, valuable suggestions, guidance and interest in my research.

I am happy to acknowledge here the role of my parents, Hjh Asmah Sarbini and my late father Hj Jamil Omar. Their love, care, courage, confidence, wisdom and integrity provided me the solid foundation upon which I have built.

I cannot express enough gratitude and appreciation to my husband and all my lovely children who supported me wholeheartedly the entire length of my studies in every possible way. Words are just not enough to express my gratefulness having all of you in my life.

I would also like to express my heartfelt appreciation to all my study mates and colleagues, for their invaluable help, many discussions and an inspiring example of a passionate PhD candidate. Finally but not least, my gratitude to the Ministry of Higher Education Malaysia for supporting this research work through research grants.

I certify that a Thesis Examination Committee has met on **26 February 2013** to conduct the final examination of **NORZIANA JAMIL** on her thesis entitled "**A DESIGN OF COLLISION RESISTANT CRYPTOGRAPHIC HASH FUNCTION BASED ON CELLULAR AUTOMATA RULES**" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the degree of **Doctor of Philosophy**.

Members of the Thesis Examination Committee were as follows:

Abdul Azim Abd Ghani, Ph.D.
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Azmi Jaafar, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mohd Rushdan Md. Said, Ph.D.
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Internal Examiner)

Bart Preneel, Ph.D.
Professor
Department of Elektrotechniek-ESAT/COSIC
Katholieke Universiteit Leuven
Belgium
(External Examiner)

SEOW HENG FONG, Ph.D.
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Ramlan Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Nur Izura Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Muhammad Reza Z'aba, PhD
Cryptography Lab
MIMOS Berhad
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

NORZIANA JAMIL

Date: 26 February 2013

TABLE OF CONTENTS

	Page
DEDICATION	i
ABSTRACT	ii
ABSTRAK	v
ACKNOWLEDGEMENTS	viii
APPROVAL	ix
DECLARATION	xi
LIST OF TABLES	xvi
LIST OF FIGURES	xviii
LIST OF ABBREVIATIONS	xx

CHAPTER

1	**INTRODUCTION**		1
	1.1	Problem Statement	5
	1.2	Objectives	7
	1.3	Scope of Research	7
	1.4	Contribution of the thesis	8
	1.5	Thesis Organisation	11
2	**BASIC CONCEPTS AND SECURITY REQUIREMENTS**		13
	2.1	Hash Functions in Cryptography	14
	2.2	Cryptographic Hash Functions	16
	2.3	Security Requirements of Cryptographic Hash Functions	16
		2.3.1 Pre-image Resistance	17
		2.3.2 Second Pre-image Resistance	18
		2.3.3 Collision Resistance	18
	2.4	Applications of Hash Functions	19
		2.4.1 Data Authentication	19
		2.4.2 Challenge Response Protocols	20
		2.4.3 Digital Signatures	21
		2.4.4 Password Obfuscation	22
		2.4.5 Random Number Generator	22
	2.5	Designs of Cryptographic Hash Functions	23
		2.5.1 Iterative Structure	24
		2.5.2 Mode of Operation	27
	2.6	Generic Attacks on Cryptographic Hash Functions	29
		2.6.1 Brute Force Attacks	30

2.6.2 Meet in the Middle Attack 31
2.6.3 Fixed Point Attack 31
2.6.4 Length Extension Attack 32
2.6.5 Joux Generic Attacks 33
2.6.6 Long Message 2^{nd} Pre-image Attack 35
2.6.7 Herding Attack 37
2.6.8 Multi-block Collision Attack 38
2.7 Specific Attacks on Cryptographic Hash Functions 40
2.8 Collision Finding Techniques 41
2.8.1 Brute Force Collision Finding Algorithm 41
2.8.2 Differential Cryptanalysis 41
2.9 Summary 42

3 **MDX-CLASS HASH FUNCTIONS** 44
3.1 Parameters and Notations 45
3.2 Design Principles of the MDx-Class Hash Functions 47
3.2.1 Description of MD4 and MD5 Algorithms 51
3.2.2 Description of RIPEMD Algorithm 57
3.2.3 Description of RIPEMD-128/160 Algorithms 59
3.2.4 Description of RIPEMD-256 and RIPEMD-320 Algorithms 61
3.2.5 Description of SHA-0/1 Algorithms 62
3.2.6 Description of SHA-2 Family Algorithms 63
3.3 Cryptanalysis of MDx-class Hash Functions 67
3.3.1 Cryptanalysis for MD4, MD5 and RIPEMD 68
3.3.2 Cryptanalysis for SHA Family Hash Functions 71
3.4 Collision-Finding Techniques for Cryptanalysis of MDx-class Hash Functions 74
3.4.1 Chabaud and Joux, 1998 74
3.4.2 Biham and Chen, 2004 78
3.4.3 Wang et al., 2005 80
3.4.4 Rechberger and De Canniẽre, 2006 82
3.5 Analysis of the Weaknesses in MDx-class Hash Functions 83
3.6 Status of MDx-class Hash Functions 84
3.7 SHA-3 Competition 85
3.8 Summary 86

4 **RESEARCH METHODOLOGY** 87
4.1 Introduction 87
4.2 Phase I: Data Collection and Literature Reviews 87
4.3 Phase II: Development of Design Framework 89
4.4 Phase III: Design and Analysis 90
4.4.1 Formulation of Message Expansion 91
4.4.2 Identification of Cryptographically Strong Boolean Functions 91
4.4.3 Design of Step Operations and Permutation Technique 93

4.5 Phase IV: Finalization 94
4.6 Summary 94

5 **A PROPOSED DESIGN FRAMEWORK FOR COLLISION RESISTANT HASH FUNCTION** 95
5.1 Design Requirements for Collision Resistant Hash Function 96
5.1.1 Iterative Construction 96
5.1.2 Mode of Operations 99
5.1.3 Pre-processing 101
5.1.4 Compression Function 104
5.2 Security Requirements for Cryptographic Boolean Functions 116
5.2.1 Balancedness 117
5.2.2 Non-linearity 118
5.2.3 Propagation Criterion 118
5.2.4 Algebraic Degree 119
5.3 Analysis Requirements for Collision Resistant Hash Function 120
5.3.1 Analysis Against Known Generic Attacks 120
5.3.2 Analysis of Diffusion Property 121
5.3.3 Analysis Against Differential Attack 121
5.3.4 Analysis Against Linear Attack 122
5.3.5 Analysis of Avalanche Effects 123
5.3.6 Analysis of Algorithm's Randomness 125
5.4 Summary 128

6 **A NEW DESIGN OF COLLISION RESISTANT HASH FUNCTION** 129
6.1 A Design of STITCH-256 129
6.1.1 Notation and Definition 130
6.1.2 STITCH-256 Design Principles and Components 130
6.1.3 Iterative Construction and Mode of Operation 130
6.1.4 Pre-Processing 133
6.1.5 Compression Function 134
6.1.6 Comparison 144
6.2 Cryptographic Properties of STITCH-256 Boolean Functions 146
6.2.1 Motivation to Find Cryptographically Strong Boolean Functions 147
6.2.2 Cellular Automata (CA) 148
6.2.3 Measurement of Cryptographic Properties of CA Rules 150
6.3 Security Analysis of STITCH-256 151
6.3.1 Security Analysis Against Long Message 2^{nd} Pre-image Attacks 152
6.3.2 Security Analysis Against Multi-block Collision Attacks 154
6.3.3 Security Analysis Against Collision Attack 155
6.3.4 Analysis of Diffusion Property of STITCH-256 Message Expansion 156

6.3.5 Analysis of STITCH-256 Step Operation Against Differential Attack 166
6.3.6 Analysis of the Avalanche Effect of STITCH-256 169
6.3.7 Analysis of the Randomness of STITCH-256 174
6.4 Summary 179

7 CONCLUSION 181
7.1 Work Done 181
7.2 Recommendations for Future Works 183

REFERENCES 185
APPENDICES 197
BIODATA OF STUDENT 216
LIST OF PUBLICATIONS 218