UNIVERSITI PUTRA MALAYSIA

A BLOCK CIPHER BASED ON GENETIC ALGORITHM

NUR HAFIZA ZAKARIA

FSKTM 2016 42

A BLOCK CIPHER BASED ON GENETIC ALGORITHM

By

NUR HAFIZA ZAKARIA

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

December 2016

DEDICATION

To my beloved husband, Muhamad Zulkhibri Alias, my sons, Muhammad Irfan Farhan and Muhammad Irsyad Fahim. Also to my parents, Zakaria Yusof and Ramlah Ibrahim.

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

A BLOCK CIPHER BASED ON GENETIC ALGORITHM

By

NUR HAFIZA ZAKARIA

December 2016

Chairman : Professor Ramlan Mahmod, PhD
Faculty : Computer Science and Information Technology

The development of block ciphers have resulted in a number of cryptographic algorithms such as, AES, ARIA, BLOWFISH256, DESL, 3D-AES and many more. In many algorithms which are based on the genetic algorithm approach, diffusion properties using crossover and mutation function are being generated to produce a secure data transmission. Permutation functions are components that are commonly used in block cipher to ensure that the ciphers are efficient. However, it would be more effective if we can use the optimum and suitable technique for crossover and mutation function. This research will concentrate on increasing the complexity and the efficiency of block cipher algorithm. This complexity can be done by designing an algorithm that consists of substitution function and permutation function which provides confusion and diffusion properties. Other than that, the evolvement of technology will also contribute towards the development of new block ciphers. To satisfy the information security requirements and to enhance the information security, we need secured communication and data which can be attained by encrypting the data. In this research, we proposed a new block cipher algorithm based on genetic algorithm approach which shall meet the security requirements. The study identifies the similarity elements and highlights the essential computation elements, namely crossover and mutation that generate idea to computational model. It can be applied in designing a new block cipher that fulfils Shanon's confusion and diffusion properties. The structure of the components has a fixed block size which is 128 bits and a key size of 128 bits. There are three functions for each encryption process which are substitution function, crossover and mutation function and add round key function. In this research also, the algorithm has been tested with NIST Statistical Test suite to evaluate the randomness of the output. The avalanche effect or bit independence analysis has been carried out using correlation coefficient and key sensitivity in experiments and satisfies the confusion property in non-linearity transformation and sensitivity of the ciphertext generated in the block cipher. It also measures the diffusion property in cryptanalysis using branch number in estimating the possible success of differential and linear attacks. Based on the results, it is proven that the new proposed block cipher algorithm has successfully passed all the security requirements needed such as NIST Statistical Test, avalanche effect, cryptanalysis and efficiency to justify that it is a secure block

cipher algorithm. Therefore, this new proposed block cipher can be used by countries, organizations, stakeholders or interested parties as one of the secure algorithm to increase the protection of the information and also will contribute as an alternative to other cryptographic algorithms in computer security research.

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

SIFER BLOK BERDASARKAN ALGORITMA GENETIK

Oleh

NUR HAFIZA ZAKARIA

Disember 2016

Pengerusi : Professor Ramlan Mahmod, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Pembangunan sifer blok telah menghasilkan beberapa algoritma kriptografi seperti AES, ARIA, BLOWFISH256, DESL, 3D-AES dan banyak lagi. Dalam banyak algorithma yang berdasarkan pendekatan algoritma genetik, sifat resapan yang menggunakan crossover dan fungsi mutasi telah dihasilkan untuk menghasilkan penghantaran data yang selamat. Fungsi atur adalah komponen yang biasa digunakan dalam sifer blok untuk memastikan bahawa tulisan rahsia adalah cekap. Walau bagaimanapun, ia akan menjadi lebih berkesan jika kita boleh menggunakan teknik yang optimum dan sesuai untuk crossover dan fungsi mutasi. Kajian ini akan menumpukan perhatian kepada meningkatkan kerumitan dan kecekapan algorithm sifer blok. Kerumitan ini boleh dilakukan dengan mereka bentuk algoritma yang terdiri daripada fungsi penggantian dan fungsi atur yang menyediakan ciri-ciri kekeliruan dan penyamaran. Selain itu, kemajuan terkini dalam bidang kriptanalisis memberi motivasi kepada reka bentuk yang baru. Untuk memenuhi keperluan keselamatan maklumat dan untuk meningkatkan keselamatan maklumat, kita memerlukan komunikasi dan data yang selamat yang boleh dicapai dengan menyulitkan data. Dalam kajian ini, kami mencadangkan satu algoritma baru berdasarkan pendekatan algoritma genetik yang memenuhi syarat-syarat keselamatan. Kajian ini mengenal pasti unsur-unsur persamaan dan menonjolkan elemen-elemen penting dalam algoritma genetik iaitu crossover dan mutasi yang menjana idea untuk model pengiraan. Ia boleh digunapakai dalam mereka bentuk sifer blok yang baru yang memenuhi ciri-ciri Shanon iaitu kekeliruan dan penyebaran. Struktur komponen ini mempunyai saiz blok tetap iaitu 128 bit dan saiz kekunci ialah 128 bit. Terdapat tiga fungsi bagi setiap proses penyulitan iaitu fungsi penggantian, fungsi crossover dan mutasi dan fungsi penambahan pusingan kekunci. Dalam kajian ini juga, algoritma telah diuji dengan Ujian Statistik NIST untuk menilai kaedah rawak terhadap hasil algoritma. Kesan runtuhan telah dijalankan dengan menggunakan pekali korelasi dan sensitiviti kekunci dalam eksperimen dan memenuhi ciri-ciri kekeliruan dalam transformasi bukan linear dan sensitiviti tulisan rahsia yang dihasilkan dalam sifer blok. Ia juga mengukur ciri-ciri penyebaran dalam kriptanalisis dengan menggunakan nombor cawangan dalam menganggarkan kemungkinan kejayaan serangan pembezaan dan serangan linear. Berdasarkan keputusan, ianya telah dibuktikan bahawa cadangan algoritma baru ini telah berjaya memenuhi semua keperluan keselamatan yang diperlukan seperti Ujian Statistik NIST, kesan runtuhan, kriptanalisis dan ujian kecekapan untuk menjelaskan bahawa ianya adalah satu algoritma sifer blok yang selamat. Oleh itu, sifer blok baru yang dicadangkan ini boleh digunakan oleh negara, organisasi, badan korporat atau pihak yang berkepentingan untuk meningkatkan perlindungan maklumat dan juga akan menyumbang sebagai satu alternatif algoritma kriptografi lain dalam penyelidikan keselamatan computer.

ACKNOWLEDGEMENT

First of all, I have to express my thanks and gratitude to Allah for his blessings, strength and persistence given on me, enabling me to complete this thesis.

I would like to thank my main supervisor, Professor Dr. Ramlan Mahmod for his guidance and constant support throughout this research. Not forgetten, my appreciation to Associate Professor Dr. Nur Izura Udzir, Associate Professor Dr. Zuriati Ahmad Zukarnain and Dr. Suriyani Ariffin, my supervisory committee members for their continuous support, suggestions and fruitful advice on the dissertation proposal as well as in the completion of the dissertation.

The study was carried out at Universiti Putra Malaysia during my PhD program. It was supported by the Ministry of Higher Education Malaysia, under the IPTA Academic Training Scheme (SLAI) Malaysia. I express gratitude the Faculty of Computer Science and Information Technology, for the laboratory equipments and facilities made accessible to me during the course of my study here. I thank my colleagues at the Universiti Sains Islam Malaysia and Universiti Putra Malaysia with whom I have had the pleasure of sharing all the joyful memories over the last three years.

I would also like offer my deepest thanks to my dad, my mom, my beloved husband and my sons for their encouragement and love in my efforts to successfully complete the journey of my PhD. Last but not least, thanks to all those who have been directly and indirectly involved in helping me complete this research.

I certify that a Thesis Examination Committee has met on 22 December 2016 to conduct the final examination of Nur Hafiza binti Zakaria on her thesis entitled "A Block Cipher Based on Genetic Algorithm" 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 Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Rahmita Wirza binti O. K. Rahmat, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azizol bin Hj Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mohamad Rushdan bin Md Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Edward Dawson, PhD
Professor Emeritus
Queensland University of Technology
Australia
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 22 March 2017

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
(Chairman)

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)

Suriyani Ariffin, PhD
Faculty of Computer Science and Mathematics
Universiti Teknologi MARA
Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date :

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ________________ Date: ________________

Name and Matric No.: Nur Hafiza Zakaria, GS34030

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ___________________
Name of Chairman of Supervisor Committee: Prof. Dr. Ramlan Mahmod

Signature: ___________________
Name of Member of Supervisor Committee: Associate Prof. Dr. Nur Izura Udzir

Signature: ___________________
Name of Member of Supervisor Committee: Associate Prof. Dr. Zuriati Ahmad Zukarnain

Signature: ___________________
Name of Member of Supervisor Committee: Dr. Suriyani Ariffin

TABLE OF CONTENTS

				Page
ABSTRACT				i
ABSTRAK				iii
ACKNOWLEDGEMENT				v
APPROVAL				vi
DECLARATION				viii
LIST OF TABLES				xiv
LIST OF FIGURES				xvii
LIST OF ABBREVIATIONS				xxi
CHAPTER				
1	**INTRODUCTION**			1
	1.1	Introduction		1
	1.2	Problem Statement		2
	1.3	Objective of the Research		3
	1.4	Scope of the Research		3
	1.5	Contributions of the Research		4
	1.6	Organization of the Thesis		4
2	**LITERATURE REVIEW**			6
	2.1	Introduction		6
	2.2	Cryptography		6
	2.3	Symmetric-key Algorithm		6
	2.4	Good Cryptosystem Properties		7
		2.4.1	Confusion	8
		2.4.2	Diffusion	8
	2.5	Design Approach for Block Cipher		8
		2.5.1	Iterative Block Cipher	8
		2.5.2	Key-alternating Block Cipher	9
		2.5.3	Key-iterated Block Cipher	10
		2.5.4	Wide Trail Strategy	11
		2.5.5	Branch Number	15
	2.6	Advanced Encryption Standard		15
		2.6.1	The SubBytes Step	17
		2.6.2	The ShiftRows Step	17
		2.6.3	The MixColumns Step	18
		2.6.4	The AddRoundKey Step	19
	2.7	Security Analysis of Block Cipher		19
		2.7.1	Randomness Test	20
		2.7.2	Avalanche Effect	23
		2.7.3	Security of S-Box	23
		2.7.4	Cryptanalysis	25
	2.8	Modes of Operation		28
		2.8.1	Electronic Codebook (ECB) Mode	28
		2.8.2	Cipher Block Chaining (CBC) Mode	29
		2.8.3	Key-stream Generation Mode	31
	2.9	Block Cipher Models		32

2.9.1 3D-AES 33
2.9.2 Rijndael 35
2.9.3 Summary 36

3 GENETIC ALGORITHM AS INSPIRATION 37
3.1 Introduction 37
3.2 Metaphor Model 37
3.3 Biological Background 37
3.3.1 The Cell 37
3.3.2 Chromosomes 38
3.3.3 Genetics 39
3.3.4 Reproduction 39
3.4 Genetic Algorithm Model 39
3.4.1 Optimization Problem 40
3.5 Crossover 41
3.5.1 Crossover Techniques 41
3.6 Mutation Types 44
3.6.1 Insert Mutation 45
3.6.2 Inversion Mutation 45
3.6.3 Scramble Mutation 45
3.6.4 Swap Mutation 45
3.6.5 Flip Mutation 46
3.6.6 Reversing Mutation 46
3.7 Encoding 46
3.7.1 Binary Encoding 46
3.7.2 Octal Encoding 47
3.7.3 Hexadecimal Encoding 47
3.7.4 Permutation Encoding (Real Number Encoding) 47
3.7.5 Value Encoding 48
3.7.6 Tree Encoding 48
3.8 Implementation in Block Cipher 49
3.8.1 Application in Genetic Algorithm 50
3.8.2 Genetic Algorithm Application in Block Cipher 50
3.9 Summary 50

4 RESEARCH METHODOLOGY 52
4.1 Introduction 55
4.2 Research Methodology 52
4.2.1 Literature Review 52
4.2.2 Research Design 54
4.2.3 Testing and Analysis 54
4.2.4 Result Discussions 57
4.3 Experimental Design 57
4.3.1 Data Preparation 57
4.3.2 Experiment Process 57
4.4 Summary 58

5 DESIGN OF GENETIC ALGORITHM-BASED BLOCK CIPHER 59
5.1 Introduction 59
5.2 Structure and Design 59
5.2.1 Array of Bytes 59
5.2.2 Input and Output 60
5.3 Encryption and Decryption Functions 61
5.3.1 Substitution Function 62
5.3.2 New S-Boxes 64
5.3.3 Crossover and Mutation Function 74
5.3.4 The Key Addition 77
5.4 Encryption and Decryption Operation Flow 77
5.5 The Number of Rounds 78
5.6 Data Encryption and Data Decryption 79
5.7 Summary 80

6 SECURITY ANALYSIS : RANDOMNESS TEST 81
6.1 Introduction 81
6.2 Sequence of Testing 81
6.3 Preliminary Test 82
6.4 Random Plaintext with Random Key 82
6.5 Low-density Plaintext with Low-density Key 85
6.6 High-density Plaintext with High-density Key 86
6.7 Randomness Test Compared with AES Block Cipher 88
6.8 Summary 90

7 SECURITY ANALYSIS : AVALANCHE EFFECT 92
7.1 Introduction 92
7.2 Correlation Coefficient 92
7.2.1 Correlation Coefficient on Permutation Function 92
7.2.2 Correlation Coefficient on All Functions 107
7.3 Key Sensitivity Test 111
7.4 Summary 125

8 SECURITY ANALYSIS : CRYPTANALYSIS AND S-BOX ANALYSIS 126
8.1 Introduction 126
8.2 Security on Branch Number 126
8.3 Differential Cryptanalysis 127
8.4 Linear Cryptanalysis 127
8.5 Measure of Diffusion based on Branch Number 127
8.6 Truncated Differential 128
8.6.1 Transformation with maximum branch number 128
8.6.2 Correlation 129
8.7 Cryptographic Properties of S-Boxes 131
8.8 Efficiency Analysis of the Algorithm 134
8.9 Summary 135

9 CONCLUSIONS AND FUTURE WORKS 136
9.1 Introduction 136
9.2 Conclusions 136

9.3 Recommendation for Future Works 137

REFERENCES 138
APPENDICES 147
BIODATA OF STUDENT 186
LIST OF PUBLICATIONS 187

LIST OF TABLES

Table		Page
2.1	Minimum requirement parameters for each statistical test	22
2.2	CipherFOUR S-Box transformation (Knudsen, 2011)	28
3.1	Translated circumstances of corresponding elements between natural evolution and genetic algorithm	49
5.1	Hexadecimal notation of bit	60
5.2	S-Box for the polynomial 01_h	65
5.3	S-Box for the polynomial 07_h	66
5.4	S-Box for the polynomial $0b_h$	66
5.5	S-Box for the polynomial $0d_h$	67
5.6	S-Box for the polynomial 13_h	68
5.7	S-Box for the polynomial 15_h	68
5.8	S-Box for the polynomial 19_h	69
5.9	S-Box for the polynomial $1f_h$	70
5.10	S-Box for the polynomial 25_h	70
5.11	S-Box for the polynomial $2f_h$	71
5.12	S-Box for the polynomial 37_h	72
5.13	S-Box for the polynomial $3d_h$	72
5.14	S-Box for the polynomial 57_h	73
5.15	S-Box for the polynomial $7f_h$	74
6.1	Frequency test result over a low-density input	82
6.2	Statistical Test for S-Box 01_h	83
6.3	The p-value of Frequency Test with low-density plaintext and key for sequence number 1 – 128	86
6.4	The p-value of Frequency Test with high-density plaintext and key for sequence number 1-64	87

6.5	The p-value of Frequency Test with high-density plaintext and key for sequence number 65-128	87
6.6	NIST statistical test results for AES block cipher	89
6.7	NIST statistical test results for new block cipher	89
7.1	Correlation coefficient on permutation function (shift rows and crossover) for AES & S-Box 1-4	94
7.2	Correlation coefficient on permutation function (shift rows and crossover) for S-Box 5-9	95
7.3	Correlation coefficient on permutation function (shift rows and crossover) for S-Box 10-14	96
7.4	Correlation coefficient on all function for AES & S-Box 1-4	107
7.5	Correlation coefficient on all function for S-Box 5-9	109
7.6	Correlation coefficient on all function for S-Box 10-14	110
7.7	Number of bit error and bit error rate of key (S-Box 1)	111
7.8	Number of bit error and bit error rate of key (S-Box 2)	112
7.9	Number of bit error and bit error rate of key (S-Box 3)	113
7.10	Number of bit error and bit error rate of key (S-Box 4)	114
7.11	Number of bit error and bit error rate of key (S-Box 5)	115
7.12	Number of bit error and bit error rate of key (S-Box 6)	116
7.13	Number of bit error and bit error rate of key (S-Box 7)	117
7.14	Number of bit error and bit error rate of key (S-Box 8)	118
7.15	Number of bit error and bit error rate of key (S-Box 9)	119
7.16	Number of bit error and bit error rate of key (S-Box 10)	120
7.17	Number of bit error and bit error rate of key (S-Box 11)	121
7.18	Number of bit error and bit error rate of key (S-Box 12)	122
7.19	Number of bit error and bit error rate of key (S-Box 13)	123
7.20	Number of bit error and bit error rate of key (S-Box 14)	124

8.1 Comparisons of cryptographic properties of S-boxes 132

8.2 Comparison of time efficiency between AES and the new proposed block cipher 135

LIST OF FIGURES

Figure		Page
2.1	Encryption with a Symmetric Key	7
2.2	Iterative block cipher with three rounds	9
2.3	Block Ciphers based on Feistel Networks	9
2.4	Key-alternating block cipher with two rounds	10
2.5	Block cipher taxonomy	11
2.6	Design structure of block cipher from Wide Trail Strategy	12
2.7	The SubBytes Step	17
2.8	The ShiftRows Step	17
2.9	The MixColumns Step	18
2.10	The AddRoundKey Step	19
2.11	CipherFOUR encryption (Knudsen, 2011)	27
2.12	Electronic Codebook (ECB) mode encryption	29
2.13	Electronic Codebook (ECB) mode decryption	29
2.14	Cipher Block Chaining (CBC) mode encryption	31
2.15	Cipher Block Chaining (CBC) mode decryption	31
2.16	Structure of 3D-AES Block Cipher	34
2.17	Rijndael Encryption Algorithm	36
3.1	Anatomy of animal cell, cell nucleus	38
3.2	A model of chromosome	39
3.3	One-point crossover	41
3.4	Two-point crossover	42
3.5	“Cut and splice”	42
3.6	Uniform crossover and half uniform crossover	43

3.7 Three parent crossover 43

3.8 Ordered crossover 43

3.9 Three point crossover 44

3.10 Insert Mutation 45

3.11 Inversion Mutation 45

3.12 Scramble Mutation 45

3.13 Swap Mutation 46

3.14 Flip Mutation 46

3.15 Reversing Mutation 46

3.16 Binary encoding 47

3.17 Octal encoding 47

3.18 Hexadecimal encoding 47

3.19 Permutation encoding 48

3.20 Value encoding 48

4.1 Research methodology 53

4.2 NetBeans software 54

4.3 NIST Statistical Test Suite 55

5.1 State and cipher key layout 61

5.2 Encryption and decryption of new block cipher 62

5.3 Sequence of Steps of New Proposed Block Cipher Algorithm 63

5.4 Substitution function 63

5.5 Crossover and Mutation Function 75

5.6 Crossover Function Algorithm 76

5.7 Mutation Function Algorithm 76

5.8 AddRoundKey function 77

5.9 Encryption function algorithm 78

5.10 Decryption function algorithm 78

5.11 Data encryption 79

5.12 Data decryption 80

6.1 Statistical Test for S-Box 01_h 85

6.2 The chart for the p-values between 128,000 bits generated from AES and new block cipher algorithm 90

7.1 Laboratory experiment process of correlation coefficient on permutation only 93

7.2 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 1) 98

7.3 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 2) 99

7.4 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 3) 99

7.5 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 4) 100

7.6 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 5) 101

7.7 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 6) 101

7.8 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 7) 102

7.9 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 8) 103

7.10 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 9) 103

7.11 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 10) 104

7.12 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 11) 105

7.13 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 12) 105

7.14 Scatter chart of the correlation coefficient on permutation 106 function (shiftRows AES and crossover in S-Box 13)

7.15 Scatter chart of the correlation coefficient on permutation function (shiftRows AES and crossover in S-Box 14) 107

8.1 Boolean transformation ∅ operating on 16-bundle vectors 128

8.2 Two-round trail of proposed block cipher 131

8.3 SET – S-box Evaluation Tool 134

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
BBS	Blum Blum Shub
DES	Data encryption standard
ECB	Electronic Codebook Mode
GF	Galois Field
IDEA	International Data Encryption Algorithm
NIST	National Institute of Standards and Technology
P-box	Permutation box
P-value	Probability value
RSA	Rivest Shamir Adleman
SAC	Strict Avalanche Criterion
SPN	Substitution-permutation network
S-box	Substitution box
XOR	Exclusive OR

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cryptography is the study of mathematical techniques related to aspects of information security for example confidentiality, data integrity, authentication and non-repudiation. Cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without doubts of cheating and deception. In our daily routine, we always interact with others electronically, whether it is using e-mail, e-commerce, ATM machines or cellular phones. The continuous increase of information transmitted electronically has lead to an increased dependence on cryptography. With cryptography, we can make sure the websites and electronic transmissions are secured and trusted. All the data transmitted between two computers where the data is kept and received must be encrypted. This will allows people to do online banking, online trading and make online purchases with their credit card without worrying that any of their account information is being compromised. Cryptography is very important to the continued development of the Internet and electronic commerce.

In January 1997, the US National Institute of Standards and Technology (NIST) announced the start of a proposal to develop a new encryption standard: the Advanced Encryption Standard (AES). The new encryption standard was to become a Federal Information Processing Standard (FIPS), replacing the old Data Encryption Standard (DES) and triple-DES (Daemen and Rijmen, 2002). Unlike the selection process for the DES, the Secure Hash Algorithm (SHA-1) and the Digital Signature Algorithm (DSA), NIST had declared that the AES selection process would be open. Anyone could submit a candidate cipher. Each submission, provided it met the requirements, would be considered on its merits. NIST would not perform any security or efficiency evaluation itself, but instead invited the cryptology community to mount attacks and try to cryptanalyze the different candidates and anyone who was interested to evaluate implementation cost. All results could be sent to NIST as public comments for publication on the NIST AES website or be submitted for presentation at AES conferences. Finally, on 2 October 2000, NIST officially announced that Rijndael without modifications would become the AES (Daemen and Rijmen, 2002).

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is based on Rijndael cipher which is developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. AES is a block cipher with block size of 128 bits or 16 bytes. Keys for the cipher come in one of three lengths: 128, 192 or 256 bits, which is 16, 24, or 32 bytes. The main mathematical difficulty with the algorithm is that it uses arithmetic over the field $GF(2^8)$. Aim for this research is to propose a new design of AES block cipher algorithm based on genetic algorithm approach. Genetic algorithm is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in genetic algorithms contain selection, crossover and mutation. The genetic algorithm also goes through the following cycle: evaluate, select, mate and mutate until some stopping criteria are reached. This research also will define the genetic algorithm approaches that will be used in cryptographic algorithm. This element can be associated with the confusion and diffusion properties in cryptography.

1.2 Problem statement

The rapid evolvements of technology have resulted in a number of new proposals on block ciphers. Bogdanov et.al. (2013) proposed a new Autheticated Lightweight Encryption algorithm coined ALE. The basic operation of ALE is the AES round transformation and the AES-128 key schedule. ALE is an online single-pass authenticated encryption algorithm that supports optional associated data. Gong et. al. (2012) came up with new family of lightweight block ciphers named KLEIN, which is designed for resource-constrained devices such as wireless sensors and RFID tags. This cipher has the advantage in the software performance on legacy sensor platforms while its hardware implementation can be compact as well. Guo et.al. (2011) proposed a new block cipher, LED that is dedicated to compact hardware implementation and offering the smallest silicon footprint among comparable block ciphers. The cipher has been designed to simultaneously tackle three additional goals. First, the authors explore the role of an ultra-light key schedule. Second, they consider the resistance of ciphers and LED in particular to related-key attacks, they are able to derive simple yet interesting AES-like security proofs for LED regarding related –or single-key attacks. And third, while they provide a block cipher that is very compact in hardware, they aim to maintain a reasonable profile for software implementation. Murphy et.al. (2002) proposed a new block cipher, BES that uses only simple algebraic operation in GF(2^8). The properties of this new cipher are related to the properties of the AES, as the AES is essentially the BES with a restricted message and key space.

In many algorithms, (Sliman et al., 2013; Suvajit D. et al., 2014; Somalina C., 2015; Sindhuja K. et al., 2014; Sania J. et al., 2014; Poornima G.N. et al., 2014; Lavkush S. et al., 2012; Ranajay K. S. et al., 2015; Vivina G.M. et al., 2016; Prempratap Singh et al., 2014;) which are based on the genetic algorithm approach, diffusion properties using crossover and mutation function are being generated to produce a secure data transmission. Permutation functions are components that are commonly used in block cipher to ensure that the ciphers are efficient. However, it would be more effective if we can use the optimum and suitable technique for crossover and mutation function. This research will concentrate on increasing the complexity and the efficiency of block cipher algorithm. This complexity can be done by designing an algorithm that consists of substitution function and permutation function which provides confusion and diffusion properties.

Besides, as time goes by, the evolvement of technology will also contribute towards the development of new block ciphers. Every country has different requirements when requesting block cipher so there is no limit in developing them. According to the National IT Council (NITC) report on “Securing Malaysia Sovereignty in the

CyberWorld" provided by Ministry of Science, Technology and Innovation, Malaysia (MOSTI, 2008), they have outlined critical areas in which new and additional research and development is needed to increase the protection of the national information data. One of the critical areas is, secured communication which helps to protect the confidentiality and integrity of information during transmission and storage. Secured communication can be achieved by encrypting and hiding data transmission and also when it is stored on a system. One of the area which has been identified as priority with respect to secured communications is conventional cryptography which provides the fundamental security and privacy in the information society. As stated in the National Strategy ICT Roadmap, security is one of the pressing needs and critical infrastructure in Malaysia by 2020. It is an advantage if we can develop our own symmetric block cipher for our national security interest. Therefore, it is necessary to research a secure symmetric block cipher algorithm. Towards that and after reviewing related research, we proposed a new design of block cipher algorithm which shall meet the security requirements. This new block cipher algorithm will increase the protection of the data information. The design of this new block cipher also will consider all the security requirements in all the other block ciphers mentioned in the literature review.

1.3 Objective of the research

The objective of this study is to design and implement a secure symmetric encryption block cipher inspired by genetic algorithm which shall fulfill the security requirements.

a) To design new block cipher based on the properties and elements of the genetic algorithm.
b) To design new 14 S-Boxes using affine transformation which produce good cryptographic S-boxes properties which are nonlinearity, balanced Boolean function, confusion coefficient variance and the differential uniformity.
c) To produce a set of function based on the genetic algorithm model which is crossover and mutation function that have the characteristics or properties of the proposed block cipher.

1.4 Scope of the research

The scope of this study is to develop a secure symmetric block cipher. For this proposed block cipher, the features which have been identified to be taken into consideration are:

a) Block size
The length of the block size is 128 bits.

b) Key length
The length of the key is 128 bits.

c) Security analysis

Several security analyses such as randomness tests, avalanche effect, linear and differential cryptanalysis has been carried out for the proposed block cipher in order to fulfil the security requirements.

d) Efficiency analysis
An investigation into efficiency of the proposed algorithm was also included in this research because it is necessary to ensure that the proposed block cipher is secure and efficient. Furthermore, the efficiency is the second important category of evaluation.

1.5 Contributions of the research

The contribution of this work as follows:

a) This research focuses on the genetic algorithm approaches to design symmetric encryption block cipher algorithm. It classifies the similarities and dissimilarities of elements and highlights the crucial elements that can be applied in symmetric encryption block cipher algorithms. The essential elements of genetic algorithm can be related with the Shannon's confusion and diffusion properties in cryptography.

b) This study uses affine transformation to produce 14 new S-Boxes. The S-boxes have 8 x 8 *A* matrix and a constant *C* of one byte, a column matrix.

c) This research uses genetic algorithm approach to develop the design of new block cipher consists of a new transformation function. The structure of the components has a fixed block size which is 128 bits and a key size of 128 bits.

1.6 Organization of the thesis

This thesis is organized into nine related chapters. It begins with Chapter 1, providing the introduction of the thesis that includes the research problems, research objectives, scope of the research and contributions of the research.

Chapter 2 describes literature surveys and background study on some related works. It covers the information about cryptography, symmetric key algorithm, AES block cipher, security analysis, previous work of block ciphers, model applied based on genetic algorithm, terms and terminologies concepts used in this thesis.

Chapter 3 discusses about genetic algorithm as inspiration in designing a secure block cipher algorithm. This chapter also describes the model applied based on genetic algorithm. This chapter presents the essential models in genetic algorithm to apply in designing the new block cipher.

Chapter 4 describes the research methodology. This chapter describes how the researcher conducts this research. This chapter also explains all the process of measuring confusion and diffusion or randomness of the block cipher output.

Chapter 5 presents the proposed design of the block cipher based on genetic algorithm approach. The details on the structure and design of new functions which are crossover and mutation function and also new S-Boxes are stressed out in this chapter.

Chapter 6 discusses the first security analysis, which is the randomness test. The experiments were carried out using the NIST Test Suite application, which consists of fifteen tests which are frequency (monobits) test, frequency within a block test, runs test, longest run of ones in a block test, random binary matrix rank test, discrete fourier transform (spectral) test, non-overlapping (aperiodic) template matching test, overlapping (periodic) template matching test, maurer's universal statistical test, linear complexity test, serial test, approximate entropy test, cumulative sum (cusum) test, random excursions test and random excursions variant test.

Chapter 7 presents the second security analysis which is avalanche effect. The confusion property of the new block cipher including the correlation coefficient, bit error and key sensitivity are discussed in this chapter.

Chapter 8 presents the third security analysis which is cryptanalysis. It discussed the results of the analysis of the diffusion property of new block cipher. The branch number is calculated in order to measure the diffusion property and it is important to resist differential, linear attacks and truncated attacks. New S-boxes also will be analysed using S-box Evaluation Tool (SET). SET is a tool for the analysis of cryptographic properties of Boolean functions and S-boxes. Lastly, the proposed block cipher has been tested for the efficiency in terms of speed.

Finally, Chapter 9 provides the conclusions of the whole research study. Besides, some recommendations for future works are proposed in this chapter to explore the study.

REFERENCES

Al-Janabi, S. (2011). Nahrainfish: A grren cryptographic block cipher. In *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International,* pages 1-5.

Ali, F. H. M., Mahmod, R., Rushdan, M., and Abdullah, I. (2009). A faster version of Rijndael cryptographic algorithm using cyclic shift and bit wise operations. In *International Journal of Cryptology Research,* 1(2):215–223.

Amador, J. J. and Green, R. W. (2005). Symmetric-key block cipher for image and text cryptography. In *International Journal of Imaging Systems and Technology,* 15(3):178–188.

Andrews, P. and Timmis, J. (2005). Inspiration for the next generation of artificial immune systems. In Jacob, C., Pilat, M., Bentley, P., and Timmis, J., editors, in *Artificial Immune Systems,* volume 3627 of Lecture Notes in Computer Science, pages 126–138. Springer Berlin / Heidelberg.

Andrews, P. and Timmis, J. (2006). On diversity and artificial immune systems: Incorporating a diversity operator into ainet. In Apolloni, B., Marinaro, M., Nicosia, G., and Tagliaferri, R., editors, Neural Nets, volume 3931 of *Lecture Notes in Computer Science*, pages 293–306. Springer Berlin Heidelberg.

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T. (2001). Camellia : A 128-bit block cipher suitable for multiple platforms and design andanalysis. In Stinson, D. and Tavares, S., editors, Selected Areas in Cryptography, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer Berlin / Heidelberg.

Ariffin, S. (2012). *A Human Immune System Inspired Byte Permutation of Block Cipher.* Universiti Putra Malaysia.

Ariffin, S., Mahmod, R. A. Jaafar, and Ariffin, M.R.K. (2011). Byte permutation in block cipher based on immune syetems, in *2011 International Conference on Computer Design and Engineering (ICCDE 2011),* 2011.

Ariffin, S., Mahmod, R. A. Jaafar, and Ariffin, M.R.K. (2011). Immune systems approaches for cryptographic algorithm, in 2011 *Sixth International Conference on Bio-Inspired Computing: Theories and Applications.*

Auday, H. S. (2015). *A DNA-Based Dynamic Key-Dependent Block Cipher.* Universiti Putra Malaysia.

B. Schneier and D. Whiting, “A Performance Comparison of the Five AES Finalists”, 15 March 2000.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, "The Twofish Team's Final Comments on AES Selection", 2000.

Barreto, P. S. and Rijmen, V. (2000a). The Khazad legacy-level block cipher. Available from http://www.cryptonessie.org/workshop/submissions.html.

Barreto, P. S. and Rijmen, V. (2000b). the anubis block cipher. Available from http://www.cryptonessie.org/workshop/submissions.html.

Barreto, P. S. L. M. and Simplicio, M. (2007). CURUPIRA, a block cipher for constrained platforms.

Biham, E., Anderson, R., and Knudsen, L. (1998). Serpent: A new block cipher proposal. In Vaudenay, S., editor, *Fast Software Encryption: 5th International Workshop, FSE98,* volume 1372 of Lecture Notes in Computer Science, pages 222–238. Springer Berlin / Heidelberg.

Biham, E. and Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4:3–72.

Biham, E. and Shamir, A. (1993). Differential cryptanalysis of the full 16-round DES. In Brickell, E., editor, *Advances in Cryptology CRYPTO 92*, volume 740 of Lecture Notes in Computer Science, pages 487–496. Springer Berlin / Heidelberg.

Biryukov, A. (2003). Analysis of involutional ciphers: Khazad and Anubis. In Johansson, T., editor, *Fast Software Encryption*, volume 2887 of Lecture Notes in Computer Science, pages 45–53. Springer Berlin / Heidelberg.

Bogdanov, A., Knudsen, L. R., Le, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., and Vikkelsoe, C. (2007). Present: An ultra-lightweight block cipher. In the proceedings of CHES 2007. Springer.

Brownlee, J. (2007). *Antigen-antibody interaction*. Complex Intelligent Systems Laboratory, Centre for Information Technology Research, Faculty of Information and Communication Technologies, Swinburne University of Technology Melbourne, Australia.

Casakin, H. P. (2007). Metaphors in design problem solving: Implications for creativity. *International Journal of Design.*

Castro, J., Sierra, J., Seznec, A., Izquierdo, A., and Ribagorda, A. (2005). The strict avalanche criterion randomness test. In *Mathematics and Computers in Simulation*, 68(1):1–7.

Chakraborty, D. and Sarkar, P. (2006). A general construction of Tweakable block ciphers and different modes of operations. In Lipmaa, H., Yung, M., and Lin, D., editors, *Information Security and Cryptology*, volume 4318 of Lecture Notes in Computer Science, pages 88–102. Springer Berlin / Heidelberg.

Chen, H., Feng, D., and Fan, L. (2009). New statistical test on block ciphers. *Jisuanji Xuebao/Chinese Journal of Computers*, 32(4):595–601.

Cheng, H., Heys, H., and Wang, C. (2008). Puffin: A novel compact block cipher targeted to embedded digital systems. In *Digital System Design Architectures, Methods and Tools, 2008. DSD '08. 11th EUROMICRO Conference* on, pages 383 –390.

Clark, A. and Dawson, E. (1998). Optimization heuristics for the automated cryptanalysis of classical ciphers.In *Journal of combinatorial mathematics and combinatorial computing.*

Cook, D., Yung, M., and Keromytis, A. (2009). Elastic block ciphers: method, security and instantiations. In *International Journal of Information Security,* 8:211–231.

Daemen, J., Knudsen, L., and Rijmen, V. (1997). The block cipher square. In Biham, E., editor, *Fast Software Encryption,* volume 1267 of Lecture Notes in Computer Science, pages 149–165. Springer Berlin / Heidelberg. 10.1007/BFb0052343.

Daemen, J. and Rijmen, V. (1999). *AES proposal: Rijndael*. Technical report. available at http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

Daemen, J. and Rijmen, V. (2002a). AES and the Wide Trail Design strategy. In Knudsen, L., editor, *Advances in Cryptology EUROCRYPT 2002,* volume 2332 of Lecture Notes in Computer Science, pages 108–109. Springer Berlin Heidelberg.

Daemen, J. and Rijmen, V. (2002b). *The Design of Rijndael, AES - The Advanced Encryption Standard.* Springer-Verlag.

Daemen, J. and Rijmen, V. (2002c). Security of a Wide Trail Design. In A. Menezes, P. S., editor, *INDOCRYPT 2002,* volume 2551 of Lecture Notes in Computer Science, pages 1–11. Springer Berlin Heidelberg.

Dasgupta, D. and Forrest, S. (1999). Artificial Immune Systems in industrial applications. In *Intelligent Processing and Manufacturing of Materials, 1999. IPMM '99.* Proceedings of the Second International Conference on, volume 1, pages 257 –267 vol.1.

de Castro, L. N. and Timmis, J. (2002). *Artificial Immune Systems: A New Computational Intelligence Approach.* Springer.

Denny, R. M. and Sunderland, P. L. (2005). Researching cultural metaphors in action: metaphors of computing technology in contemporary u.s. life. *Journal of Business Research, 58(10):1456 – 1463. La Londe Seminar 2003 - communications and consumer behavior.*

Dobson, C. M. and Karplus, M. (1999). The fundamentals of protein folding: bringing together theory and experiment. Current Opinion in *Structural Biology,* 9(1):92 – 101.

Dorigo, M. and Gambardella, L. (1997). Ant colony system: a cooperative learning approach to the traveling salesman problem. *Evolutionary Computation, IEEE Transactions* on, 1(1):53 –66.

Doroshenko, S., Fionov, A., Lubkin, A., Monarev, V., Ryabko, B., and Shokin, Y. I. (2008). Experimental statistical attacks on block and stream ciphers, volume 101 of Notes on Numerical Fluid Mechanics.

Elkamchouchi, H. and Makar, M.A. (2005). Measuring encryption quality of bitmap images encrypted with Rijndael and KAMKAR block ciphers. In *Twenty Second National Radio Science Conference (NRSC).*

Elumalai, R. and Reddy, A. R. (2011). Improving diffusion power of AES Rijndael with 8x8 MDS matrix. In *International Journal on Computer Science and Engineering,* 3(1):246–253. Fan, L., Feng, D., and Zhou, Y. (2008). A fuzzy-based randomness evaluation model for block cipher. Jisuanji Yanjiu yu Fazhan/Computer Research and Development, 45(12):2095–2101.

U.S. Department of Commerce. (2001). *"Fips197 : Advanced encryption standard (AES),* fips pub 197 federal information processing standard publication 197."

Griffiths, A. J., Gelbart, W. M., Miller, J. H., and Lewontin, R. C. (1999). *Modern Genetic Analysis*. W. H. Freeman and Company.

Guangzhao, C., Cuiling, L., Haobin, L. and Xiaoguang, L. (2009)"DNA Computing and Its Application to Information Security Field", in *2009 Fifth International Conference on Natural Computation.*

Ha, M., Pedrycz, W., Zhang, A., and Fan, Y. (2008). A development of inclusion degree-based rough fuzzy random sets. *Fundamental Informatic*, 86(4):481–502.

Heys, H. M. (2001). A tutorial on linear and differential cryptanalysis. Available from http://citeseerx.ist.psu.edu/.

Izadi, M., Sadeghiyan, B., Sadeghian, S., and Khanooki, H. (2009). Mibs: A new lightweight block cipher. In Garay, J., Miyaji, A., and Otsuka, A., editors, *Cryptology and Network Security*, volume 5888 of Lecture Notes in Computer Science, pages 334–348. Springer Berlin / Heidelberg.

Jamel, S., Deris, M. M., Yanto, I. T. R., and Herawan, T. (2011). The hybrid cubes encryption algorithm (HiSea). In Al-Majeed, S. S., Hu, C.-L., and Nagamalai, D., editors, *Advances in Wireless, Mobile Networks and Applications,* volume 154 of Communications in Computer and Information Science, pages 191–200. Springer Berlin Heidelberg.

Junod, P. and Vaudenay, S. (2005). Fox : A new family of block ciphers. In Handschuh, H. and Hasan, M., editors, *Selected Areas in Cryptography*, volume 3357 of Lecture Notes in Computer Science, pages 114–129. Springer Berlin / Heidelberg.

Karplus, M. (1997). The Levinthal paradox: yesterday and today. Folding and Design, 2(Supplement 1):69–75.

Katos, V. (2005). A randomness test for block ciphers. In *Applied Mathematics and Computation*, 162(1):29–35.

Knudsen, L., Leander, G., Poschmann, A., and Robshaw, M. (2010). Printcipher: A block cipher for ic-printing. In Mangard, S. and Standaert, F.-X., editors, *Cryptographic Hardware and Embedded Systems, CHES 2010*, volume 6225 of Lecture Notes in Computer Science, pages 16–32. Springer Berlin / Heidelberg.

Knudsen, L. R. and Robshaw, M. J. (2011). Introduction. In The Block Cipher Companion, *Information Security and Cryptography*, pages 35–64. Springer Berlin Heidelberg.

Kruppa, H. and Shahy, S. U. A. (1998). *Differential and linear cryptanalysis in evaluating AES candidate algorithms.* Technical report, National Institute of Standards and Technology.

Levinthal, C. (1969). How to fold graciously. Mssbaun Spectroscopy in *Biological Systems Proceedings*, Univ. of Illinois Bulletin, 67(41):22–24.

Li, C. K. and Wong, D. S. (2010). Signcryption from randomness recoverable public key encryption. *Information Sciences*, 180(4):549–559. Cited By (since 1996): 2.

Li, T. and Wang, G. (2007). Security analysis of two ultra-lightweight rfid authentication protocols. In the proceedings of *IFIP SEC 2007*.

Li, W., Gu, D., and Li, J. (2008). Differential fault analysis on the ARIA algorithm. *Information Sciences*, 178(19):3727–3737.

Li, Z., Woo, C. J., Iglesias-Ussel, M. D., Ronai, D., and Scharff, M. D. (2004). The generation of antibody diversity through somatic hypermutation and class switch recombination. *Gene and Development*, 18:1–11.

Lian, S. (2009). A block cipher based on chaotic neural networks. *Neurocomputing,* 72(4-6):1296–1301.

Lim, C. H. (1998). *Crypton: A new 128-bit block cipher - specification and analysis.*

Liu, F., Ji, W., Hu, L., Ding, J., Lv, S., Pyshkin, A., and Weinmann, R.-P. (2007). Analysis of the sms4 block cipher. In Pieprzyk, J., Ghodosi, H., and Dawson, E., editors, *Information Security and Privacy*, volume 4586 of Lecture Notes in Computer Science, pages 158–170. Springer Berlin / Heidelberg.

MacWilliams, F. J. and Sloane, N. (1978). The Theory of Error-Correting Codes. North-Holland Publishing Company.

Mahmod, R., Ali, S. A., and Ghani, A. A. A. (2009). A shift column with different offset for better Rijndael security. *International Journal of Cryptology Research,* 1(2):245–255.

Marhusin, M., Cornforth, D., and Larkin, H. (2008). Malicious code detection architecture inspired by human immune system. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08.* Ninth ACIS International Conference on, pages 312 –317.

Mathur, C., Narayan, K., and Subbalakshmi, K. (2006). High diffusion cipher: Encryption and error correction in a single cryptographic primitive. In Zhou, J., Yung, M., and Bao, F., editors, *Applied Cryptography and Network Security,* volume 3989 of Lecture Notes in Computer Science, pages 309–324. Springer Berlin / Heidelberg.

Matsui, M. (1994). Linear cryptanalysis method for DES cipher. In Helleseth, T., editor, *Advances in Cryptology EUROCRYPT 93*, volume 765 of Lecture Notes in Computer Science, pages 386–397. Springer Berlin / Heidelberg.

Menezes, A. J., Oorschot, P. C. V., and Vanstone, S. A. (1997). Handbook of Applied Cryptography. CRC Press.

Millan, W., Clark, A., and Dawson, E. (2005). An effective genetic algorithm for finding highly nonlinear Boolean functions. *Information and Communication Seccurity,* volume 1334, pages 149-158. Springer Link.

Murphy, S. (2000). *The power of NIST's statistical testing of AES candidates.*

Murphy, S. and Robshaw M.J.B (2002). Essential Algebraic Structure Within the AES. *Advances in Cryptology – Crypto '02, LNCS,* volume 2442, pages 1-16. Springer-Verlag.

Nechvatal, J., Bassham, E. B. L., Dworkin, M., Foti, J., and Roback, E. (2000). Report on *The development of the Advanced Encryption Standard (AES).* Technical report.

NHGRI (2006). Primary structure of a protein. Technical report, National Human Genome Research Institute. Available from http://en.wikipedia.org/wiki/Amino acid.

NIST (2001). Fips197: *Advanced Encryption Standard (AES),* FIPS PUB 197 Federal Information Processing Standard Publication 197. Technical report, National Institute of Standards and Technology.

NITC (2007). *National strategic ICT road map.* Technical report, Minister of Science, Technology and Innovation (MOSTI) Malaysia, MSC Technology Centre Sdn. Bhd (MSCTC) and IBM Corporation.

Nyberg, K. (1994). Differentially uniform mappings for cryptography. In Helleseth, T., editor, *Advances in Cryptology EUROCRYPT 93*, volume 765 of Lecture Notes in Computer Science, pages 55–64. Springer Berlin / Heidelberg.

Ojha, S., Kumar, N., Jain, K., and Sangeeta (2009). TWIS - a lightweight block cipher. In Prakash, A. and Sen Gupta, I., editors, *Information Systems Security*, volume 5905 of Lecture Notes in Computer Science, pages 280–291. Springer Berlin / Heidelberg.

Patidar, V., Sud, K. K., and Pareek, N. K. (2009). A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Informatica (Ljubljana)*, 33(4):441–452.

Pedrycz, W. (2008). Collaborative architectures of fuzzy modeling, volume 5050 LNCS of Lecture Notes in Computer Science (including subseries Lecture Notes in *Artificial Intelligence and Lecture Notes in Bioinformatics).*

Rashed, A. A. (2004). Intelligent Encryption Decryption System Using Partial Genetic Algorithm and Rijndael Algorithm. *Arab Academy for Banking and Financial Sciences.*

Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., and De Win, E. (1996). The cipher shark. In Gollmann, D., editor, *Fast Software Encryption*, volume 1039 of Lecture Notes in Computer Science, pages 99–111. Springer Berlin / Heidelberg.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S. (2008). *Sp80022: A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Technical report, National Institute of Standards and Technology.

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code* in C. John Wiley & Sons, Inc., New York, NY, USA, 2nd edition.

Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656 – 715.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. (2007). The 128bit block cipher clefia (extended abstract). In Biryukov, A., editor, *Fast Software Encryption*, volume 4593 of Lecture Notes in Computer Science, pages 181–195. Springer Berlin / Heidelberg.

Simplicio, M., Jr., Barreto, P. S. L. M., Carvalho, T. C. M. B., Margi, C. B., and Nslund, M. (2007). The CURUPIRA-2 block cipher for constrained platforms: Specification and benchmarking.

Somayaji, A., Hofmeyr, S., and Forrest, S. (1997). Principles of a computer immune system. In Proceedings of the *1997 workshop on New security paradigms, NSPW '97*, pages 75–82, New York, NY, USA. ACM.

Soto, J. and Bassham, L. (2000). *Randomness testing of the advanced encryption standard finalist candidates.* Technical report, National Institute of Standards and Technology.

Soto, J. J. (2000). *Randomness testing of the AES candidate algorithms.* Technical report, National Institute of Standards and Technology.

Spillman, R. (1993). *Cryptanalysis of knapsack ciphers using genetic algorithm.* Cryptologia.

Stallings, W. (2011). *Cryptography and network security: principles and practice.* Prentice Hall.

Sulak, F., Doganaksoy, A., Ege, B., and Koak, O. (2010). Evaluation of randomness test results for short sequences, volume 6338 LNCS of Lecture Notes in *Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

Timmis, J. (2010). Artificial Immune Systems. In Sammut, C. and Webb, G. I., editors, *Encyclopedia of Machine Learning*, pages 40–44. Springer US.

Wang, Y., Liao, X., Xiao, D., and Wong, K. (2008). One-way hash function construction based on 2d coupled map lattices. *Information Sciences,* 178(5):1391– 1406. Cited By (since 1996): 19.

Watada, J. and Bakar, R. A. (2008). “DNA Computing and Its Applications”, in *Eighth International Conference on Intelligent Systems Design and Applications.*

Webster, A. and Tavares, S. (1986). On the design of S-Boxes. In Williams, H., editor, Advances in *Cryptology CRYPTO 85 Proceedings,* volume 218 of Lecture Notes in Computer Science, pages 523–534. Springer Berlin / Heidelberg.

Wu, Y., Noonan, J., and Agaian, S. (2010). Binary data encryption using the Sudoku block cipher. In *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference* on, pages 3915 –3921.

Yaseen, I.F.T and Sahasrabuddhe, H.V. (1998). A genetic algorithm for the cryptanalysis of Chor-rivest knapsack public key cryptosystem (PKC). In proceeding of the *Third International Conference on Computational Intelligence and Multimedia Applications.*

Z’aba, M.R., Wong, K. and Dawson, Ed. (2010). Algebraic analysis of small scale LEX-BES. In the *2nd International Cryptology Conference 2010 (Cryptology 2010).*

Z’aba, M.R., Raddum, H., Simpson, L., Dawson, Ed., Henricksen, M and Wong, K. (2009). Algebraic Analysis of LEX. In *Australasian Information Security Conference (AISC 2009), volume 91 of Conferences in Research and Practice in Information Technology (CRPIT),* pages 33-45. Australian Computer Society.

Z’aba, M.R., Raddum, H., Henricksen, M. and Dawson, Ed. (2008). Bit-pattern based integral attack. In *Fast Software Encryption: 15th International Workshop, FSE 2008,* volume 5086 of Lecture Notes in Computer Science, pages 363-381. Springer-Verlag.

Zhou, Q., Liao, X., Wong, K., Hu, Y., and Xiao, D. (2009). True random number generator based on mouse movement and chaotic hash function. *Information Sciences*, 179(19):3442–3450.

Zhu, Z., Zhang, W., Wong, K., and Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences,* 181(6):1171–1186.