UNIVERSITI PUTRA MALAYSIA

SECURE BLOCK CIPHER INSPIRED BY THE HUMAN IMMUNE SYSTEM

SURIYANI ARIFFIN

FSKTM 2012 33
DEDICATION

To my beloved husband, Syed Helmy Syed Abu Bakar, my daughters, Nurul Syuhada, Syarifah Ainul Mardhiah, Syarifah Balqis and Syarifah Najwatus Sumaiyyah, and my son Syed Muhammad Bilal.
Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

SECURE BLOCK CIPHER INSPIRED BY THE HUMAN IMMUNE SYSTEM

By

SURIYANI ARIFFIN

October 2012

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

In computer security service, cryptographic algorithm is used to ensure adequate security of the systems or of data transfers. Symmetric encryption block cipher is an important cryptographic algorithm and the quest of enhancing data security is crucial due to the heavy usage of internet and mobile devices worldwide. As stated in the Malaysian National Strategy ICT Roadmap, security is one of the pressing needs and critical infrastructure in Malaysia by 2020. As for Malaysia, it is an advantage if we can develop our own symmetric block cipher for our national security interest. Hence, it is necessary to research a secure symmetric block cipher algorithm. This thesis proposes to design a secure symmetric encryption block cipher inspired by human immune system called the Three Dimensional Advanced Encryption Standard (3D-AES). The thesis identifies the similarity elements and highlights the essential computation elements, namely the antigen-antibody inter-
action, somatic hypermutation model, Levinthal’s paradox, and protein structure that can be applied in symmetric block cipher that fulfills Shannon’s confusion and diffusion properties. The empirical findings presented the randomness of the output in the 3D-AES block cipher as compared to the AES block cipher, for the number of iteration rounds reduced by four, from seven to three. The avalanche effect or bit independence analysis has been carried out using correlation coefficient, bit error and key sensitivity in experiments and satisfies the confusion property in non-linearity transformation and sensitivity of the ciphertext generated in the third round of the block cipher. It also measures the diffusion property in linear transformation using branch number in estimating the possible success of differential and linear attacks. There are no three-round linear trails with predictable input-output correlation of above \(2^{-3\times34} = 2^{-102}\), and no three-round differential trails with predictable propagation ratio of above \(2^{-6\times34} = 2^{-204}\), and thus, sufficient to resist differential and linear attacks. It is proven that the 3D-AES block cipher has successfully passed very demanding security analyses and justified that the 3D-AES block cipher is a secure block cipher. Therefore, it will increase the protection of the national information infrastructure and will also contribute as one of a symmetric block cipher in computer security research.
Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

SIFER BLOK YANG SELAMAT DIILHAMKAN DARIPADA SISTEM PERTAHANAN BADAN MANUSIA

Oleh

SURJIANI ARIFFIN

Oktober 2012

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

Dalam perkhidmatan keselamatan komputer, algoritma kriptografi digunakan untuk memastikan keselamatan sistem atau penghantaran maklumat dipenuhi. Penyuli- tan sifer blok simetrik adalah algoritma kriptografi yang penting dan keperluan untuk meningkatkan keselamatan maklumat adalah kritikal disebabkan oleh penggunaan internet dan peranti bergerak yang meluas di seluruh dunia. Seperti yang telah dinyatakan di dalam Rancangan Strategi ICT Kebangsaan, Malaysia, keselamatan adalah salah satu keperluan yang mendesak dan infrastruktur yang kritikal di Malaysia menjelang 2020. Bagi Malaysia, adalah menjadi satu kelebihan jika kita boleh membangunkan sifer blok simetrik kita sendiri untuk kepentingan keselamatan negara. Oleh itu, adalah perlu untuk mengkaji algoritma sifer blok simetri yang selamat. Tesis ini mencadangkan pendekatan yang diilhamkan daripada sistem pertahanan badan manusia dalam reka bentuk fungsi pilihatur yang baharu
dalam pembangunan sifer blok simetri yang dikenali sebagai *Advanced Encryption Standard* Tiga Dimensi (3D-AES). Tesis ini mengenal pasti kaitan dan mengenang gahkan elemen pengkomputeran yang diadapati daripada proses interaksi antara antigen dan antibodi, model somantik hipermutasi, paradoks Levinthal, dan struktur protein yang boleh digunakan dalam sifer blok simetri yang dapat memenuhi sifat-sifat kekeliruan dan pembauran Shannon. Penemuan secara analisa empirikal telah dibentangkan dan dikenal pasti bahawa kerawakan output dalam sifer blok 3D-AES adalah setanding dengan sifer blok AES walaupun bilangan pusingan berlelaran dapat dikurangkan sebanyak empat pusingan iaitu daripada tujuh kepada tiga kitaran sahaja. Keputusan analisa kesan runtuhan pada ujikaji maklumat yang terdiri daripada pecah korelasi, ralat bit dan sensitiviti kekunci telah mendapati bahawa sifer blok ini memenuhi sifat kekeliruan dalam transformasi ketaklelurusan dan sensitiviti penyulitan yang dijana hanya pada pusingan ketiga. Sifer pembauran dari segi transformasi linear juga diukur menggunakan nombor cawangan dalam mengganggarkan kemungkinan kejayaan serangan kebezaan dan serangan linear. Tiada tiga pusingan jejak-jejak linear yang mempunyai ralat korelasi input-output lebih daripada \(2^{-3\times34} = 2^{-102}\) dan tiada tiga pusingan jejak-jejak kebezaan yang mempunyai ralatPROPAGASI lebih daripada \(2^{-6\times34} = 2^{-204}\). Ini menunjukkan bahawa sifer blok 3D-AES berupaya menentang serangan kebezaan dan serangan linear. Ini bermakna bahawa sifer blok 3D-AES telah lulus ujian keselamatan yang amat penting dan wajar dinyatakan bahawa sifer blok 3D-AES adalah sifer blok yang selamat. Oleh itu, ia boleh meningkatkan perlindungan infrastruktur maklumat negara dan boleh dijadikan sebagai salah satu alternatif sifer blok dalam penyelidikan keselamatan komputer.
ACKNOWLEDGEMENT

First and foremost, I am eternally thankful to God for His blessings, strength and perseverance bestowed on me, enabling me to complete this thesis.

Special appreciation goes to Professor Dr. Ramlan Mahmod, my thesis supervisor, for his mentorship and constant support throughout this research. Not forgotten, my appreciation to Associate Professor Dr. Azmi Jaafar and Dr. Muhammad Rezal Kamel Ariffin, my supervisory committee members for their invaluable advice, suggestions and criticisms on the dissertation proposal as well as in the completion of the dissertation. My appreciation to my colleagues Dr. Fakariah Hani Mohd Ali and Associate Professor Dr. Nordin Abu Bakar for the guidance and advice in undertaking the research activities. I thank Dr. Muhammad Reza Za’ba from MIMOS for his valuable insights into the area of block cipher cryptanalysis.

The research project was carried out at Universiti Putra Malaysia during my PhD program. It was supported by the Fundamental Research Grant Scheme (FRGS) project sponsored by the Ministry of Higher Education Malaysia, under the Grant Number FRGS/1/11/SG/UPM/02/4 and the Bumiputera Academic Training Scheme (SLAB) Malaysia. I thank the Faculty of Computer Science and Information Technology, for the laboratory equipments and facilities made available to me during the course of my study here. I thank my colleagues at the Universiti Teknologi MARA and Universiti Putra Malaysia with whom I have had the pleasure of sharing all the happy memories over the last three years.

Above all I am very grateful to my loving and caring husband and my adorable children for their encouragement and love in my efforts to successfully complete the
program. My husband and friends helped me prepare for my presentations and proofread some of the thesis chapters. Without his support and patience, this work would never have come into existence.
I certify that a Thesis Examination Committee has met on October 2012 to conduct the final examination of Suriyani Ariffin on her thesis entitled "Secure Block Cipher Inspired by Human Immune System" 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:

**Hamidah Ibrahim, Ph.D.**
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

**Nur Izura Udzir, Ph.D.**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

**Zuriati Ahmad Zukarnain, Ph.D.**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

**Edward Dawson, Ph.D.**
Professor Emeritus
Information Security Institute
Queensland University of Technology
Level 7, 126 Margaret Street, Qld 4000
Australia
(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 fulfillment 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)

**Azmi Jaafar, PhD**  
Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**Muhammad Rezal Kamel Ariffin, PhD**  
Senior Lecturer  
Faculty of Science  
Universiti Putra Malaysia  
(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.

SURINYANI ARIFFIN

Date: 11 October 2012
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEDICATION</td>
<td>i</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>iv</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>vi</td>
</tr>
<tr>
<td>APPROVAL</td>
<td>viii</td>
</tr>
<tr>
<td>DECLARATION</td>
<td>x</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xv</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xviii</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xxi</td>
</tr>
</tbody>
</table>

## CHAPTER

1 INTRODUCTION
   1.1 Introduction                           1
   1.2 Problem statement                      1
   1.3 Objective of the research              3
   1.4 Scope of the research                  5
   1.5 Contributions of the research          6
   1.6 Organization of the thesis             7

2 BLOCK CIPHER
   2.1 Introduction                           9
   2.2 Computer security                       9
   2.3 Classification of cryptography         11
   2.4 Symmetric block cipher                  12
      2.4.1 Confusion                          13
      2.4.2 Diffusion                          14
   2.5 Block cipher design structure          14
      2.5.1 Iterative block cipher             15
      2.5.2 Key-alternating block cipher       16
      2.5.3 Key-iterated block cipher          17
      2.5.4 Wide Trail Strategy                17
      2.5.5 Branch number                      19
      2.5.6 Mode of operation                   20
   2.6 Security analysis of block cipher       20
      2.6.1 Randomness test                    22
      2.6.2 Avalanche effect                    25
      2.6.3 Cryptanalysis                      26
2.7 Block cipher models
   2.7.1 Shark 32
   2.7.2 Square 33
   2.7.3 Crypton 33
   2.7.4 Khazad and Anubis 35
   2.7.5 AES or Rijndael 35
   2.7.6 Pyramid 38
   2.7.7 Curupira 39
   2.7.8 3D block cipher 40
   2.7.9 2D Rotation 41
2.8 Concepts and terminologies from AES block cipher
   2.8.1 Boolean permutation 42
   2.8.2 Finite field 42
   2.8.3 MDS codes 43
   2.8.4 Operation on bytes 43
   2.8.5 4-byte columns 43
2.9 Summary 44

3 IMMUNOLOGY AS INSPIRATION 45
   3.1 Introduction 45
   3.2 Metaphor model 45
   3.3 Immune system model 46
   3.4 Artificial Immune System 47
   3.5 Deciding the immune system models 49
      3.5.1 Antigen-antibody interaction 51
      3.5.2 Somatic Hypermutation Model 53
      3.5.3 Protein structure 54
      3.5.4 Levinthal’s paradox 55
   3.6 Implementation in block cipher 56
   3.7 Summary 60

4 RESEARCH METHODOLOGY 61
   4.1 Introduction 61
   4.2 Research methodology 61
      4.2.1 Literature review 61
      4.2.2 Research design 63
      4.2.3 Research analysis and discussion result 63
      4.2.4 Documentation 64
   4.3 Experimental design 65
      4.3.1 Data preparation 65
      4.3.2 Experiment process 66
      4.3.3 Result and analysis 68
   4.4 Summary 73
5 DESIGN OF 3D-AES BLOCK CIPHER

5.1 Introduction
5.2 Generalization function description
  5.2.1 Antigen-antibody interaction
  5.2.2 Somatic Hypermutation
  5.2.3 Protein structure
5.3 Structure and design
  5.3.1 Notation
  5.3.2 Array of bytes
  5.3.3 Input and output
  5.3.4 Key rotation function
  5.3.5 Key mixing function
  5.3.6 Substitution function
  5.3.7 Permutation function
  5.3.8 Transposition function
5.4 Round structure
5.5 Encryption and decryption functions
5.6 Encryption and decryption operation flow
5.7 Summary

6 RANDOMNESS TEST

6.1 Introduction
6.2 Preliminary test
6.3 Random plaintext with random key
6.4 Low-density plaintext with low-density key
6.5 High-density plaintext with high-density key
6.6 Randomness test compared with AES block cipher
6.7 Summary

7 AVALANCHE EFFECT

7.1 Introduction
7.2 Correlation coefficient
  7.2.1 Correlation coefficient on permutation function
  7.2.2 Correlation coefficient on all functions
7.3 Bit error analysis
7.4 Key sensitivity analysis
7.5 Summary

8 CRYPTANALYSIS

8.1 Introduction
8.2 Security on branch number
8.3 Definitions
8.4 Branch number
8.5 Differential cryptanalysis
8.6 Measure of diffusion based on branch number 131
8.7 Resistance to differential and linear cryptanalysis 133
8.8 Summary 133

9 CONCLUSIONS AND FUTURE WORKS 134
9.1 Introduction 134
9.2 Conclusions 134
9.3 Recommendation of future works 136

REFERENCES 138

APPENDIX

A CODE OF BLUM BLUB SHUB 147
A.1 Source code 147

B EXAMPLE VECTORS 152
B.1 Cipher (encrypt) 152
B.2 Inverse cipher (decrypt) 156

C LABORATORY EXPERIMENT RESULTS 160
C.1 The results of randomness tests at round 1 160
C.2 The results of randomness tests at round 2 175
C.3 The results of randomness tests at round 3 190

BIODATA OF STUDENT 206
LIST OF PUBLICATIONS 207