UNIVERSITI PUTRA MALAYSIA

SECURE BLOCK CIPHER INSPIRED BY THE HUMAN IMMUNE SYSTEM

SURIYANI ARIFFIN

FSKTM 2012 33

SECURE BLOCK CIPHER INSPIRED BY THE HUMAN IMMUNE SYSTEM

By

SURIYANI ARIFFIN

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

October 2012

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 interaction, somantic 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 $2^{-3\times 34} = 2^{-102}$, and no three-round differential trails with predictable propagation ratio of above $2^{-6\times 34} = 2^{-204}$, 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

SURIYANI 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. Penyulitan 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 simetrik yang dikenali sebagai *Advanced Encryption Standard* Tiga Demensi (3D-AES). Tesis ini mengenal pasti kaitan dan mengenengahkan elemen pengkomputeran yang diadaptasi daripada proses interaksi antara antigen dan antibodi, model somantik hipermutasi, paradoks Levinthal, dan struktur protin yang boleh digunapakai dalam sifer blok simetrik 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 makmal yang terdiri daripada pekali 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. Sifat pembauran dari segi transformasi linear juga diukur menggunakan nombor cawangan dalam menganggarkan kemungkinan kejayaan serangan kebezaan dan serangan linear. Tiada tiga pusingan jejak-jejak linear yang mempunyai ramalan korelasi input-output lebih daripada $2^{-3\times34} = 2^{-102}$ dan tiada tiga pusingan jejak-jejak kebezaan yang mempunyai ramalan nisbah propagasi 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.

SURIYANI ARIFFIN

Date: 11 October 2012

TABLE OF CONTENTS

APPENDIX