AN IMPROVED RECTANGLE LIGHTWEIGHT BLOCK CIPHER BASED ON 3D ROTATION METHOD

Abdul Alif Bin Zakaria

Thesis submitted in partial fulfilment for the degree of
DOCTOR OF PHILOSOPHY IN
SCIENCE AND TECHNOLOGY

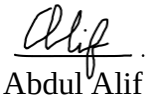
UNIVERSITI SAINS ISLAM MALAYSIA

SEPTEMBER 2022

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 6th SEPTEMBER 2022

Signature : 
Name : Abdul Alif Bin Zakaria
Matric No. : 4192573
Address : ER-05-01, Ehsan Residence,
Jalan Orkid 4/2, Taman Orkid,
43900 Sepang,
Selangor.

ACKNOWLEDGEMENTS

Grateful to Allah SWT for His blessing given to me during my study and in completing this thesis.

First and foremost I am extremely grateful to my supervisors, Assoc. Prof. Dr. Azni Haslizan, Assoc. Prof. Dr. Farida Hazwani, Dr. Nur Hafiza, and Dr. Maslina for their invaluable advice, continuous support, and patience throughout this journey.

Thank you to the most important people in my life, Abah (Zakaria), Mama (Nor Azian), and Nenek (Umi Salmah) who have raised me all this time.

Most importantly, I would like to express my gratitude to my wife (Normasliha) who sacrificed a lot throughout this journey to take care of our three children (Danish, Dania & Dhia).

I would like to express my deepest appreciation to the Ministry of Higher Education (MOHE) who funded my studies and USIM for the support and facilities provided during these three meaningful years.

Additionally, I would like to offer my special thanks to CyberSecurity Malaysia for supporting me in achieving my ambition.

Last but not least, I would like to extend my sincere thanks to everyone in this world who has taught, helped, supported, and encouraged me all this while. May Allah bless all of you.

"We may be ordinary people, but no one can deny our determination to be extraordinary people.

We have the same 24 hours, but the way we take advantage of these 24 hours determines whether we succeed or not."

ABSTRAK

Kesedaran keselamatan siber mempunyai kesan yang besar terhadap peningkatan pembangunan produk keselamatan di pasaran. Memandangkan sifat kritikal pada produk keselamatan, keselamatan maklumat adalah penting kerana pemintasan dan pengubahsuaian data boleh menyebabkan kehilangan kebolehsediaan, integriti, dan kerahsiaan serta kerugian lain seperti kehilangan nyawa, wang, dan aset. Oleh itu, penyulitan diperlukan untuk perlindungan data dan sifer blok ringan dipilih sebagai penyelesaian kepada isu keselamatan kerana ia lebih padat dan memerlukan kuasa pengkomputeran yang kecil. Walau bagaimanapun, keseimbangan antara keselamatan dan kecekapan adalah masalah utama yang perlu diselesaikan dalam mereka bentuk algoritma ringan dengan mengambil kira jenis litar, kelajuan, dan penggunaan memorinya. Melihat kepada situasi yang membimbangkan ini, penyelesaian baharu amat diperlukan untuk mengatasi isu produk keselamatan. Penyelidikan ini bertujuan untuk membangunkan sifer blok ringan yang dinamakan Operasi Algoritma Ringan (LAO-3D) berdasarkan pilih atur 3-dimensi (3D). Kaedah ini terdiri daripada tatasusunan teks biasa yang dilakukan pada tatasusunan bit 3D yang menambah lapisan kekeliruan dan resapan untuk mengukuhkan algoritma sifer blok dari segi keselamatan dan kecekapan prestasi. Untuk mencapai objektif penyelidikan, komponen kriptografi selamat untuk sifer blok ringan dianalisis dalam Fasa 1 (Analisis) yang boleh digunakan untuk pembangunan sifer blok ringan pada masa hadapan oleh pembangun kriptografi. Dalam Fasa 2 (Pembangunan), sifer blok ringan baharu yang boleh dipertimbangkan untuk pelaksanaan bagi menyelesaikan isu produk keselamatan direka bentuk. Sementara itu, analisis kriptografi dan ujian prestasi perisian dijalankan dalam Fasa 3 (Penilaian) yang boleh digunakan untuk membezakan kekuatan sifer blok ringan. Enam ujian kriptanalisis telah dijalankan untuk menilai kekuatan LAO-3D. Penemuan mencadangkan bahawa LAO-3D mencapai keputusan yang lebih baik berbanding dengan sifer blok ringan sedia ada dengan 98.2% keputusan ujian hasil pekali korelasi, menghasilkan keputusan 50% untuk kedua-dua ujian kadar ralat bit dan ujian kepekaan kunci, lulus 100% ujian rawak, dan kebal terhadap serangan kriptanalisis dengan bilangan pusingan maksimum yang boleh diserang menggunakan analisis kriptografi pembezaan dan linear adalah pada pusingan kelima dan keenam. Secara keseluruhannya, penyelidikan ini menyumbang kepada bidang keselamatan siber yang menyokong inisiatif kerajaan Malaysia dalam menjaga kesejahteraan rakyat selaras dengan Dasar Keselamatan Siber Negara.

ABSTRACT

Cyber security awareness has a huge impact on the increasing development of security products in the market. Considering the critical nature of the security products, information security is crucial due to interception and modification of data which can lead to loss of availability, integrity, and confidentiality, and possibly other losses such as loss of life, money, and assets. Thus, encryption is required for data protection and lightweight block cipher is identified as a solution to this security issue since it is more compact and requires small computing power. However, despite being lightweight, the trade-off between security and efficiency are the major problems to be solved in designing a lightweight algorithm. One should consider its type of circuit, speed, and memory consumption. Looking at this alarming situation, new solutions are needed to overcome security product issues. The research aims to develop a lightweight block cipher named Light Algorithm Operation (LAO-3D) based on 3-dimensional (3D) permutation. This method is composed of an array of plaintext that is performed on a 3D bits array that adds confusion and diffusion layer to strengthen the block cipher algorithm in terms of security and performance efficiency. In order to achieve the research objectives, the secure cryptographic components for lightweight block cipher are analysed in Phase 1 (Analysis) that can be used for future development of lightweight block cipher by cryptographic developers. In Phase 2 (Development), a new lightweight block cipher is designed that can be considered for implementation to solve security product issues. Meanwhile, cryptanalysis and software performance tests are carried out in Phase 3 (Evaluation) which can be used to distinguish the strength of lightweight block ciphers. Six cryptanalysis tests were conducted to assess the strength of LAO-3D. The findings suggested that LAO-3D achieved better results compared to other existing lightweight block ciphers with 98.2% correlation coefficient result, produced 50% results for both bit error rate and key sensitivity tests, passed 100% of the randomness test, and resistant to cryptanalysis attacks with the maximum number of rounds that can be attacked using differential and linear cryptanalysis are five and six rounds correspondingly. On top of that, LAO-3D obtained competitive performance results with 10.85% faster execution speed and produced 12.18% more throughput than the closest competitor. Overall, this research contributes to the field of cybersecurity supporting the Malaysian government's initiatives in safeguarding the well-being of the people in line with the National Cyber Security Policy.

الملخص

الوعي بالأمن السيبراني له تأثير كبير على التطوير المتزايد لمنتجات الأمن في السوق. بالنظر إلى الطبيعة الحرجة للمنتجات الأمنية ، يعد أمن المعلومات أمرًا بالغ الأهمية بسبب اعتراض البيانات وتعديلها مما قد يؤدي إلى فقدان التوافر والنزاهة والسرية ، وربما خسائر أخرى مثل الخسائر في الأرواح والمال والأصول. وبالتالي ، فإن التشفير مطلوب لحماية البيانات ويتم تحديد تشفير الكتلة الخفيف كحل لمشكلة الأمان هذه نظرًا لأنه أكثر إحكاما ويتطلب قوة حوسبة صغيرة. ومع ذلك ، على الرغم من كونها خفيفة الوزن ، فإن المفاضلة بين الأمان والكفاءة هي المشاكل الرئيسية التي يجب حلها في تصميم خوارزمية خفيفة الوزن. ينبغي للمرء أن ينظر في نوع الدائرة والسرعة واستهلاك الذاكرة. بالنظر إلى هذا الموقف المقلق ، هناك حاجة إلى حلول جديدة للتغلب على مشكلات المنتجات الأمنية. يهدف البحث إلى تطوير شفرة كتلة خفيفة الوزن تسمى Light Algorithm Operation (LAO-3D) على أساس التقليب ثلاثي الأبعاد (3D). تتكون هذه الطريقة من مصفوفة من النص العادي التي يتم إجراؤها على مصفوفة بتات ثلاثية الأبعاد تضيف طبقة الارتباك والانتشار لتقوية خوارزمية تشفير الكتلة من حيث الأمان وكفاءة الأداء. من أجل تحقيق أهداف البحث ، يتم تحليل مكونات التشفير الآمنة للتشفير الكتلي الخفيف الوزن في المرحلة الأولى (التحليل) التي يمكن استخدامها للتطوير المستقبلي لتشفير الكتلة الخفيف بواسطة مطوري التشفير. في المرحلة 2 (التطوير) ، تم تصميم تشفير كتلة خفيف الوزن جديد يمكن اعتباره للتنفيذ لحل مشكلات منتج الأمان. وفي الوقت نفسه ، يتم إجراء اختبارات تحليل التشفير واختبارات أداء البرامج في المرحلة 3 (التقييم) والتي يمكن استخدامها لتمييز قوة الأصفار الكتل خفيفة الوزن. تم إجراء ستة اختبارات لتحليل الشفرات لتقييم قوة LAO-3D. أشارت النتائج إلى أن LAO-3D حققت نتائج أفضل مقارنة بأصفار الكتلة خفيفة الوزن الأخرى الحالية بنتيجة معامل الارتباط ٪98.2 ، وأنتجت نتائج ٪50 لكل من معدل خطأ البتات واختبارات الحساسية الرئيسية ، واجتازت ٪100 من اختبار العشوائية ، ومقاومة لتحليل التشفير. الهجمات مع الحد الأقصى لعدد الجولات التي يمكن مهاجمتها باستخدام تحليل التشفير التفاضلي والخطي هي خمس وست جولات في المقابل. علاوة على ذلك ، حصلت LAO-3D على نتائج أداء تنافسية مع سرعة تنفيذ أسرع بنسبة ٪10.85 وأنتجت إنتاجية أكثر بنسبة ٪12.18 من أقرب منافس. بشكل عام ، يساهم هذا البحث في مجال الأمن السيبراني الذي يدعم مبادرات الحكومة الماليزية في حماية رفاهية الناس بما يتماشى مع السياسة الوطنية للأمن السيبراني.

TABLE OF CONTENTS

CONTENT **PAGE**

LIST OF TABLES

Tables **Page**

LIST OF FIGURES

Figures **Page**

LIST OF APPENDICES

Appendices **Page**

LIST OF SYMBOLS

$a_{i,j}$	Cipher State (at i^{th} *Slice* and j^{th} bit)
AddRoundKey	Add Round Key Function
AND	AND Operation
BER	Bit Error Rate
C	Ciphertext
c_i	Ciphertext (at i^{th} bit)
Col_j	Column (at j^{th} position)
$DDT[\Delta_\alpha][\ \Delta_\beta]$	Difference Distribution Table Output (at Δ_α and Δ_β inputs)
E	Avalanche Effect
E_K	Encryption
E_K^{-1}	Decryption
K	Key
KeySubColumn	Key Sub Column Function
k_i	Round Key (at i^{th} bit)
$k_{i,j}$	Key State (at i^{th} row and j^{th} column)
$LAT[\lambda_\alpha][\ \lambda_\beta]$	Linear Approximation Table Output (at λ_α and λ_β inputs)
m	Number of Bit
m_d	Differential Active S-boxes
m_l	Linear Active S-boxes
n	Block Size
NonceXOR	Nonce XOR Function
OR	OR Operation
P	Plaintext
p_α	Portion of Sequence (at α)
p_i	Plaintext (at i^{th} bit)
p-value	Probability of Obtaining Test Results
$\hat{p}$	Probability of Occurrence
q	Total Bias
$\hat{q}$	Bias
$Prob$	Probability
R	Round
$RowKey_i$	Key State (at i^{th} row)
RowTransformation	Row Transformation Function
r_{pc}	Correlation Coefficient
s	Sample Size
Slice	Plaintext Slice
$S(i)$	S-box Output (at i^{th} input)
v_i	Key State (at i^{th} bit)
w_i	Plaintext (at i^{th} bit)
X_i	Input (at i^{th} bit)
XOR	Exclusive OR Operation
Y_j	Output (at j^{th} bit)

α	Significance Level
λ_α	Input Masks
λ_β	Output Masks
Δ_α	Input Difference of S-box
Δ_β	Output Difference of S-box
$\triangle X$	Input Difference
$\triangle Y$	Output Difference
3DBitRotation	3D Bit Rotation Function
3DBitRotation_X-axis	3D Bit Rotation at *X*-axis Function
3DBitRotation_Z-axis	3D Bit Rotation at *Z*-axis Function

LIST OF ABBREVIATION

AES	Advanced Encryption Standard
AKBA	New Cryptographic Algorithm
AKI	Actual Key Information
AKSA	Existing Cryptographic Algorithm
AND	AND Operation
ARX	Addition, Rotation, and XOR
ATM	Automated Teller Machine
AX-box	Addition and XOR Box
CBCM	Cipher Block Chaining Mode
Char.	Characteristic
CNII	Critical National Information Infrastructure
Corr.	Correlation Potential
CRYPTREC	Cryptography Research and Evaluation Committees
DC	Differential Cryptanalysis
DDT	Difference Distribution Table
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
e.g.	Example
eSTREAM	ECRYPT Stream Cipher Project
FIPS	Federal Information Processing Standards
FN	Feistel Network
GFN	Generalized Feistel Network
HDK	High Density Key
HDP	High Density Plaintext
HW	Hardware
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standards
IV	Initialization Vector
Kb	Kilobit
LAO	Light Algorithm Operation
LAT	Linear Approximation Table
LC	Linear Cryptanalysis
LDK	Low Density Key
LDP	Low Density Plaintext
LFSR	Linear Feedback Shift Register
MA-box	Multiplication and Addition Box
Mb	Megabit
MDS	Maximum Distance Separable
ms	Millisecond
MySEAL	National Trusted Cryptographic Algorithm List
NCP	National Cryptography Policy
NCSP	National Cyber Security Policy

NESSIE	New European Schemes for Signatures, Integrity, and Encryption
NIST	National Institute of Standards and Technology
NLFSR	Nonlinear Feedback Shift Register
PCC	Plaintext/Ciphertext Correlation
PKI	Public-Key Infrastructure
Prob	Probability
RAM	Random Access Memory
RFID	Radio-Frequency Identification
RPRK	Random Plaintext/Random Key
SAC	Strict Avalanche Criterion
S-box	Substitution Box
SKA	Strict Key Avalanche
SPA	Strict Plaintext Avalanche
SPN	Substitution-Permutation Network
SW	Software
TKI	Theoretical Key Information
XNOR	Exclusive-NOR Operation
XOR	Exclusive OR Operation
3D	3-Dimensional