

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

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

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 أمراً 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 نظراً لأنه أكثر إحكاماً 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 التقليل 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
AUTHOR DECLARATION	II
ACKNOWLEDGEMENTS	III
ABSTRAK	IV
ABSTRACT	V
AL-MULAKHKHAS	VI
TABLE OF CONTENTS	VII
LIST OF TABLES	XII
LIST OF FIGURES	XIV
LIST OF APPENDICES	XVII
LIST OF SYMBOLS	XVIII
LIST OF ABBREVIATION	XX
CHAPTER 1 : INTRODUCTION	1
1.1 Background of the Research	1
1.2 Problem Statement	3
1.3 Research Questions	6
1.4 Research Objectives	7
1.5 Research Contributions	7
1.6 Scope of Study	8
1.7 Thesis Organization	10
CHAPTER 2 : LITERATURE REVIEW	11
2.1 Introduction	11
2.2 Cryptography	11
2.3 Lightweight Block Cipher	15
2.3.1 Lightweight Block Cipher Projects	16
2.3.1.1 NESSIE Project	17
2.3.1.2 NIST Lightweight Cryptography Project	17
2.3.1.3 MySEAL Project	18
2.3.1.4 Security Evaluation Criteria	18
2.3.2 Previous Work on Lightweight Block Cipher	20
2.3.2.1 MISTY	21
2.3.2.2 HIGHT	21
2.3.2.3 PRESENT	22
2.3.2.4 RECTANGLE	23

2.3.2.5	Performance of Lightweight Block Ciphers	24
2.4	Cryptanalysis	25
2.4.1	Avalanche Effect	26
2.4.2	Randomness Tests	27
2.4.3	Cryptanalysis Attacks	31
2.4.3.1	Differential Cryptanalysis	31
2.4.3.2	Linear Cryptanalysis	32
2.5	Chapter Summary	33
CHAPTER 3 : RESEARCH METHODOLOGY		35
3.1	Introduction	35
3.2	Research Method	35
3.2.1	Phase 1 (Analysis)	38
3.2.2	Phase 2 (Development)	39
3.2.3	Phase 3 (Evaluation)	40
3.3	Experimental Setup	41
3.3.1	Avalanche Effect Tests	42
3.3.2	Randomness Tests	43
3.3.3	Cryptanalysis Attacks	44
3.3.4	Software Performance Tests	45
3.4	Chapter Summary	46
CHAPTER 4 : SECURE CRYPTOGRAPHIC COMPONENTS		47
4.1	Introduction	47
4.2	Systematic Literature Review on Lightweight Block Cipher	47
4.3	Comparison of Lightweight Block Cipher Components	64
4.3.1	Comparison of Substitution Component	65
4.3.2	Comparison of Permutation Component	74
4.3.2.1	Permutation Function	80
4.3.2.2	Rotation Function	84
4.4	A Summary of Secure Cryptographic Components	87
4.5	3-Dimensional Cipher	89
4.6	Chapter Summary	91
CHAPTER 5 : RECTANGLE LIGHTWEIGHT BLOCK CIPHER		92
5.1	Introduction	92
5.2	Overview of RECTANGLE	92
5.2.1	Cipher and Subkey States	93
5.2.2	Encryption Algorithm	93
5.2.3	Key Schedule Algorithm	96
5.3	Strengths of RECTANGLE	97

5.4	Weaknesses of RECTANGLE	98
5.4.1	S-box	98
5.4.2	Key Schedule Algorithm.....	99
5.5	Preliminary Study on RECTANGLE.....	101
5.5.1	Randomness analysis of RECTANGLE	101
5.5.2	Enhancement of RECTANGLE key schedule algorithm	102
5.5.3	Adoption of 3D cipher in RECTANGLE	102
5.6	Chapter Summary.....	103
CHAPTER 6 : DEVELOPMENT OF LAO-3D LIGHTWEIGHT BLOCK CIPHER....		104
6.1	Introduction	104
6.2	Formulation of 3D Rotation Function.....	104
6.2.1	3D Bit Rotation	105
6.2.2	3D Rotation Function.....	106
6.2.2.1	3D Bit Rotation (X-axis) Function.....	107
6.2.2.2	Add Round Key Function.....	111
6.2.2.3	3D Bit Rotation (Z-axis) Function.....	113
6.3	Development of LAO-3D Lightweight Block Cipher.....	117
6.3.1	Algorithm Specifications	117
6.3.2	Encryption Algorithm	119
6.3.2.1	Add Round Key	120
6.3.2.2	Sub Column	121
6.3.2.3	Double 3D Rotation.....	123
6.3.2.3.1	3D Bit Rotation (X-axis).....	124
6.3.2.3.2	Add Round Key	125
6.3.2.3.3	3D Bit Rotation (Z-axis).....	126
6.3.3	Key Schedule Algorithm.....	128
6.3.3.1	NonceXOR	128
6.3.3.2	Round Key Extraction	130
6.3.3.3	Key Sub Column	131
6.3.3.4	Row Transformation.....	131
6.4	Chapter Summary.....	132
CHAPTER 7 : CRYPTANALYSIS OF LAO-3D LIGHTWEIGHT BLOCK CIPHER		134
7.1	Introduction	134
7.2	Avalanche Effect Tests.....	134
7.2.1	Correlation Coefficient Test	135
7.2.2	Bit Error Rate Test	138
7.2.3	Key Sensitivity Test.....	141
7.3	Randomness Tests	144

7.4	Cryptanalysis Attacks.....	150
7.4.1	Differential Cryptanalysis.....	151
7.4.2	Linear Cryptanalysis	161
7.5	Discussion	172
7.6	Chapter Summary.....	174
CHAPTER 8 : RESULTS AND DISCUSSION.....		176
8.1	Introduction	176
8.2	LAO-3D vs RECTANGLE	177
8.2.1	Correlation Coefficient Test	177
8.2.2	Bit Error Rate Test	178
8.2.3	Key Sensitivity Test.....	179
8.2.4	Randomness Tests.....	179
8.2.5	Differential Cryptanalysis.....	180
8.2.6	Linear Cryptanalysis	181
8.3	LAO-3D vs Other Block Ciphers.....	181
8.3.1	Correlation Coefficient Test	182
8.3.2	Bit Error Rate Test	182
8.3.3	Key Sensitivity Test.....	183
8.3.4	Randomness Tests.....	184
8.3.5	Differential Cryptanalysis.....	184
8.3.6	Linear Cryptanalysis	186
8.4	Software Performance Tests.....	187
8.4.1	LAO-3D vs RECTANGLE.....	188
8.4.2	LAO-3D vs Other Block Ciphers.....	189
8.5	Discussion	190
8.5.1	Encryption Algorithm	191
8.5.2	Key Schedule Algorithm.....	192
8.6	Chapter Summary.....	193
CHAPTER 9 : IMPLEMENTATION OF LAO-3D LIGHTWEIGHT BLOCK CIPHER		194
.....		194
9.1	Introduction	194
9.2	Software Implementation of LAO-3D Lightweight Block Cipher	194
9.2.1	Desktop Application.....	195
9.2.1.1	Encryption	195
9.2.1.2	Decryption	198
9.2.2	Mobile Application.....	201
9.2.2.1	Encryption	203
9.2.2.2	Decryption	206
9.3	Chapter Summary.....	210

CHAPTER 10 : CONCLUSION AND FUTURE WORKS.....	212
10.1 Introduction	212
10.2 Objectives Revisited.....	212
10.2.1 Research Objective 1	213
10.2.1.1 Research Output 1	213
10.2.2 Research Objective 2	214
10.2.2.1 Research Output 2	214
10.2.3 Research Objective 3	215
10.2.3.1 Research Output 3	215
10.2.4 Research Objective 4	216
10.2.4.1 Research Output 4	216
10.3 Recommendation for Future Works.....	218
10.4 Conclusion.....	219
PUBLICATIONS.....	220
REFERENCES	221

UNIVERSITI SAINS ISLAM MALAYSIA
 جامعة العلوم الإسلامية الماليزية
 ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

LIST OF TABLES

Tables	Page
Table 2.1: Classification of Cryptography	14
Table 2.2: Comparison of Block Cipher Requirements	15
Table 2.3: Comparison of Security Evaluation Criteria of Cryptographic Projects.....	19
Table 2.4: Security Evaluation Criteria	19
Table 2.5: MISTY Algorithm.....	21
Table 2.6: HIGHT Algorithm.....	22
Table 2.7: PRESENT Algorithm.....	22
Table 2.8: RECTANGLE Algorithm	23
Table 2.9: Throughput Comparison	24
Table 2.10: Speed Comparison	25
Table 2.11: Statistical Tests Application Packages.....	28
Table 2.12: Objectives of NIST Statistical Tests	29
Table 2.13: Bits Requirements for NIST Statistical Tests	30
Table 2.14: Statistical Test Results Indication	30
Table 3.1: Research Methodology Mapping	37
Table 3.2: Research Tool.....	41
Table 4.1: Lightweight Block Cipher Components.....	48
Table 4.2: Substitution Function	66
Table 4.3: Comparison of Substitution Function Features.....	73
Table 4.4: Permutation and Rotation Function.....	75
Table 4.5: Comparison of Permutation Function Features.....	83
Table 4.6: Comparison of Rotation Function Features	86
Table 5.1: S-box	95
Table 5.2: Undisturbed bits of RECTANGLE	99
Table 5.3: Comparison of the Least AKI and its Theoretical Value TKI.....	100
Table 6.1: Formulation of 3D Bit Rotation (X-axis)	110
Table 6.2: Formulation of 3D Bit Rotation (Z-axis).....	115
Table 6.3: Input and Output of Add Round Key.....	121
Table 6.4: S-box	122
Table 6.5: Input and Output of Sub Column	123
Table 6.6: Input and Output of Double 3D Rotation.....	123
Table 6.7: 3D Bit Rotation Permutation Table (X-axis).....	124
Table 6.8: Input and Output of 3D Bit Rotation (X-axis).....	125
Table 6.9: Input and Output of Add Round Key	126
Table 6.10: 3D Bit Rotation Permutation Table (Z-axis).....	127
Table 6.11: Input and Output of 3D Bit Rotation (Z-axis).....	127
Table 6.12: Nonce	129
Table 6.13: Input and Output of NonceXOR	129
Table 6.14: Input and Output of Round Key Extraction	130
Table 6.15: Input and Output of Key Sub Column	131

Table 6.16: Input and Output of Row Transformation.....	132
Table 7.1: Correlation Coefficient Test Results Indication.....	135
Table 7.2: Correlation Coefficient Results of LAO-3D	138
Table 7.3: Bit Error Rate Results of LAO-3D.....	141
Table 7.4: Key Sensitivity Results of LAO-3D.....	144
Table 7.5: Data Categories Input.....	146
Table 7.6: Randomness Results for $\alpha = 0.1\%$ (CBC, PCC, RPRK, SKA, and SPA).....	147
Table 7.7: Randomness Results for $\alpha = 0.1\%$ (LDK, HDK, LDP, and HDP).....	147
Table 7.8: Randomness Results for $\alpha = 1\%$ (CBC, PCC, RPRK, SKA, and SPA).....	148
Table 7.9: Randomness Results for $\alpha = 1\%$ (LDK, HDK, LDP, and HDP).....	148
Table 7.10: Comparison of Randomness Results.....	149
Table 7.11: Uniformity Results (CBC, PCC, RPRK, SKA, and SPA)	149
Table 7.12: Uniformity Results (LDK, HDK, LDP, and HDP)	150
Table 7.13: Difference Distribution Table	152
Table 7.14: Probability of Differential Characteristics	153
Table 7.15: 6-round Differential Iterative of LAO-3D	160
Table 7.16: Active S-Boxes and Probabilities of Differential Trails	161
Table 7.17: Linear Approximation Table.....	162
Table 7.18: Correlation Potentials of Linear Characteristics	163
Table 7.19: 7-round Linear Iterative of LAO-3D.....	171
Table 7.20: Active S-Boxes and Correlation Potentials of Linear Trails.....	172
Table 7.21: A Summary of Cryptanalysis Results	172
Table 8.1: Correlation Coefficient Results.....	178
Table 8.2: Bit Error Rate Results	178
Table 8.3: Key Sensitivity Results	179
Table 8.4: Randomness Tests Results.....	180
Table 8.5: Active S-Boxes and Probabilities of Differential Trails	180
Table 8.6: Active S-Boxes and Correlation Potentials of Linear Trails.....	181
Table 8.7: Correlation Coefficient Results.....	182
Table 8.8: Bit Error Rate Results	183
Table 8.9: Key Sensitivity Results	183
Table 8.10: Randomness Tests Results.....	184
Table 8.11: Probabilities of Differential Trails.....	185
Table 8.12: Active S-Boxes of Differential Cryptanalysis.....	185
Table 8.13: Correlation Potentials of Linear Trails.....	186
Table 8.14: Active S-Boxes of Linear Cryptanalysis.....	187
Table 8.15: Performance Tests Results	189
Table 8.16: Performance Tests Results	190
Table 8.17: Modifications of RECTANGLE Encryption Algorithm.....	191
Table 8.18: Modifications of RECTANGLE Key Schedule Algorithm	192

LIST OF FIGURES

Figures	Page
Figure 1.1: Research Scope.....	9
Figure 2.1: Overview of Cryptology.....	12
Figure 2.2: Symmetric Cryptography.....	13
Figure 2.3: Asymmetric Cryptography.....	13
Figure 2.4: Lightweight Block Cipher Evaluation Criteria.....	25
Figure 3.1: Flow of Research Process.....	36
Figure 3.2: Analysis Process.....	38
Figure 3.3: Development Process.....	39
Figure 3.4: Evaluation Process.....	40
Figure 3.5: Avalanche Effect Tests Process.....	42
Figure 3.6: Randomness Tests Process.....	43
Figure 3.7: Cryptanalysis Process.....	44
Figure 3.8: Software Performance Tests Process.....	45
Figure 4.1: Functions of Lightweight Block Cipher.....	60
Figure 4.2: Secure Cryptographic Components.....	88
Figure 4.3: Cube.....	90
Figure 5.1: Cipher State.....	93
Figure 5.2: Add Round key.....	94
Figure 5.3: Sub Column.....	95
Figure 5.4: Shift Row.....	95
Figure 5.5: Key State.....	96
Figure 5.6: Subkey.....	96
Figure 6.1: 3-Dimensional Cipher State.....	105
Figure 6.2: 3D Bit Rotation Formation.....	106
Figure 6.3: 3D Rotation Process.....	107
Figure 6.4: 2D Plaintext.....	107
Figure 6.5: 3D Cipher State.....	108
Figure 6.6: X-axis Rotation.....	108
Figure 6.7: 3D Bit Rotation (X-axis) Cipher State.....	109
Figure 6.8: 3D Bit Rotation (X-axis) Output.....	111
Figure 6.9: Add Round Key.....	112
Figure 6.10: Add Round Key ($Slice_0$ to $Slice_3$).....	113
Figure 6.11: Z-axis Rotation.....	113
Figure 6.12: 3D Bit Rotation (Z-axis) Cipher State.....	114
Figure 6.13: 3D Bit Rotation (Z-axis) Output.....	116
Figure 6.14: Cipher State and Key State.....	118
Figure 6.15: LAO-3D Encryption and Decryption Process.....	119
Figure 6.16: Add Round Key.....	120
Figure 6.17: Output Distribution of S-box.....	122
Figure 6.18: Sub Column.....	123

Figure 6.19: Distribution of Bit Rotation (X-axis) Output	124
Figure 6.20: 3D Bit Rotation (X-axis).....	125
Figure 6.21: Add Round Key	126
Figure 6.22: Distribution of Bit Rotation (Z-axis) Output	127
Figure 6.23: 3D Bit Rotation (Z-axis).....	127
Figure 6.24: LAO-3D Key Schedule Process	128
Figure 6.25: Key State	129
Figure 6.26: Row Key	130
Figure 6.27: Round Key.....	130
Figure 6.28: Key Sub Column	131
Figure 6.29: Row Transformation.....	132
Figure 7.1: Scatter Charts of Correlation Coefficient Results.....	137
Figure 7.2: Scatter Charts of Bit Error Rate Results	140
Figure 7.3: Scatter Charts of Key Sensitivity Results.....	143
Figure 7.4: 1-Round Differential Characteristic for Round 1 of LAO-3D	154
Figure 7.5: 1-Round Differential Characteristic for Round 2 of LAO-3D	155
Figure 7.6: 1-Round Differential Characteristic for Round 3 of LAO-3D	156
Figure 7.7: 1-Round Differential Characteristic for Round 4 of LAO-3D	157
Figure 7.8: 1-Round Differential Characteristic for Round 5 of LAO-3D	158
Figure 7.9: 1-Round Differential Characteristic for Round 6 of LAO-3D	159
Figure 7.10: 1-Round Linear Characteristic for Round 1 of LAO-3D.....	164
Figure 7.11: 1-Round Linear Characteristic for Round 2 of LAO-3D.....	165
Figure 7.12: 1-Round Linear Characteristic for Round 3 of LAO-3D.....	166
Figure 7.13: 1-Round Linear Characteristic for Round 4 of LAO-3D.....	167
Figure 7.14: 1-Round Linear Characteristic for Round 5 of LAO-3D.....	168
Figure 7.15: 1-Round Linear Characteristic for Round 6 of LAO-3D.....	169
Figure 7.16: 1-Round Linear Characteristic for Round 7 of LAO-3D.....	170
Figure 9.1: Encryption	196
Figure 9.2: Input Encryption Key	196
Figure 9.3: Input Message.....	197
Figure 9.4: Output Ciphertext	198
Figure 9.5: Decryption	199
Figure 9.6: Input Decryption Key.....	199
Figure 9.7: Input Ciphertext.....	200
Figure 9.8: Output Plaintext.....	200
Figure 9.9: Mobile Encryption Application.....	201
Figure 9.10: Encryption and Decryption Process.....	202
Figure 9.11: Encryption	203
Figure 9.12: Input Message.....	204
Figure 9.13: Input Encryption Key	205
Figure 9.14: Output Ciphertext	206
Figure 9.15: Decryption	207
Figure 9.16: Input Ciphertext.....	208

Figure 9.17: Input Decryption Key 209
Figure 9.18: Output Plaintext 210



LIST OF APPENDICES

Appendices	Page
APPENDIX A: Key Schedule Algorithm Components.....	237
APPENDIX B: Encryption Algorithm Components.....	245
APPENDIX C: Decryption Algorithm Components	252
APPENDIX D: Source Code of LAO-3D Lightweight Block Cipher (Encryption).....	259
APPENDIX E: Source Code of LAO-3D Lightweight Block Cipher (Decryption).....	264
APPENDIX F: Source Code of LAO-3D Lightweight Block Cipher Sample Generation for Randomness Tests Using Nine Data Categories.....	270
APPENDIX G: Source Code of Differential Cryptanalysis for LAO-3D Lightweight Block Cipher.....	284
APPENDIX H: Source Code of Linear Cryptanalysis for LAO-3D Lightweight Block Cipher	291
APPENDIX I: Source code of Avalanche Effect (Correlation Coefficient, Bit Error Rate, and Key Sensitivity Tests) for LAO-3D Lightweight Block Cipher	298
APPENDIX J: Samples of Data Set	300

LIST OF SYMBOLS

$a_{i,j}$	Cipher State (at i^{th} Slice and j^{th} bit)
<i>AddRoundKey</i>	Add Round Key Function
<i>AND</i>	AND Operation
<i>BER</i>	Bit Error Rate
<i>C</i>	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)
<i>E</i>	Avalanche Effect
E_K	Encryption
E_K^{-1}	Decryption
<i>K</i>	Key
<i>KeySubColumn</i>	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
<i>NonceXOR</i>	Nonce XOR Function
<i>OR</i>	OR Operation
<i>P</i>	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
<i>Prob</i>	Probability
<i>R</i>	Round
$RowKey_i$	Key State (at i^{th} row)
<i>RowTransformation</i>	Row Transformation Function
r_{pc}	Correlation Coefficient
s	Sample Size
<i>Slice</i>	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)
<i>XOR</i>	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
ΔX	Input Difference
ΔY	Output Difference
<i>3DBitRotation</i>	3D Bit Rotation Function
<i>3DBitRotation_X-axis</i>	3D Bit Rotation at X-axis Function
<i>3DBitRotation_Z-axis</i>	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

UNIVERSITI SAINS ISLAM MALAYSIA
 جامعة العلوم الإسلامية
 ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA