UNIVERSITI PUTRA MALAYSIA

DYNAMIC DETERMINANT MATRIX-BASED BLOCK CIPHER ALGORITHM

JULIA JUREMI

FSKTM 2018 67

DYNAMIC DETERMINANT MATRIX-BASED BLOCK CIPHER ALGORITHM

By

JULIA JUREMI

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

May 2018

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

DYNAMIC DETERMINANT MATRIX-BASED BLOCK CIPHER ALGORITHM

By

JULIA JUREMI

May 2018

Chair : Sharifah Md Yasin, PhD
Faculty : Computer Science and Information Technology

Rijndael (AES) is a well-known block cipher algorithm with proven robustness towards countless cryptographic attacks. Somehow, the substitution box (s-box) in the AES block cipher is fixed or static for all rounds and has become the target of many attacks. The design of the s-box is the most crucial part while designing a new block cipher algorithm since it is the only non-linear element of the cipher. In this research, emphasis is given on increasing the complexity of a block cipher algorithm. We propose a new dynamic determinant block cipher (DDBC) designed based on the determinant matrix properties which shall meet the security requirements of a secure block cipher. This research will first make use of the matrix determinants properties, linear equations and its inverses, identifies the similarity elements and combines them with irreducible polynomials and affine transformation to produce new determinants-boxes to be used in the substitution layer. This research also proposes a new method namely RotateSwapDeterminant function that uses rotation and swapping of the bit based on the 4x4 determinant computations and will act as the permutation layer in the DDBC algorithm. The output from the DDBC algorithm will be tested and validated through NIST Statistical Test Suite. The s-box test will be carried out to verify the security of the new determinant s-boxes constructed. The correlation coefficient and key sensitivity of plaintext and ciphertext produced by DDBC algorithm will be tested through avalanche effect experiments. Analyses on linear, differential and short attack will be performed against the DDBC algorithm to estimate the possible success of all three attacks. The performance analysis is performed on DDBC algorithm to test for the encryption and decryption speed of the block cipher and lastly the complexity analysis is performed on the selected determinant s-boxes to examine the level of complexity contributed by tested and untested determinant s-boxes. Through these extensive experiments, the proposed DDBC algorithm has successfully passed the NIST Statistical Test with all 15 tests show p-value > 0.01.

The results from the s-box test indicate that the determinant s-boxes constructed provides good balanced, sufficient differential uniformity, excellent non-linearity, acceptable algebraic degree and adequate signal to noise ratio (SNR). For the avalanche effect analysis, the DDBC algorithm shows that most of the correlation values tested on the proposed determinant s-boxes and the RotateSwapDeterminant function are near to 0 which indicate a strong positive (or negative) non-linear relationship which means the DDBC algorithm has a high confusion property. The analysis on linear, differential and short attack shows required complexity to be more then 2^{102} attempts for linear cryptanalysis, required complexity to be more then 2^{104} attempts for differential cryptanalysis and $(((2^8)^{10})^{256})^5$ total possibilities of attempts for short attack which provide sufficient evidence that the DDBC algorithm is resistance towards all three attacks. The performance analysis in terms of processing speed of the encryption and decryption process of the DDBC algorithm shows minimal differences in both AES and DDBC algorithm despite of the difference method of transformation used in both algorithms. Lastly, the complexity analysis shows that the determinant s-box that has go through the s-box analysis test show better avalanche criteria proving higher level of complexity compared to non-tested determinant s-box. From the result of the analysis, it has been justified that the proposed DDBC algorithm can be considered as one of the secure symmetric block cipher and can be used as an alternative to other cryptographic algorithm in computer security research area.

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

ALGORITMA SIFER BLOK DINAMIK BERDASARKAN MATRIX PENENTUAN

Oleh

JULIA JUREMI

Mei 2018

Pengerusi : Sharifah Md Yasin, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Rijndael (AES) adalah algoritma sifer blok yang terkenal serta terbukti ketahanannya terhadap serangan kriptografi yang tidak terkira banyaknya. Walaubagaimanapun, kotak penggantian (s-box) dalam sifer blok AES yang tetap atau statik untuk setiap pusingan telah menjadi sasaran banyak serangan. Reka bentuk s-box adalah bahagian yang paling penting ketika merancang algoritma sifer blok yang baru kerana ia merupakan satu-satunya elemen bukan linear dalam sifer. Dalam kajian ini, penekanan diberikan untuk meningkatkan kerumitan algoritma sifer blok. Kami mencadangkan sifer blok penentu dinamik (DDBC) baru yang direka berdasarkan sifat-sifat matriks penentu yang memenuhi keperluan keselamatan sifer blok. Penyelidikan ini akan menggunakan sifat-sifat penentu matriks, persamaan linear dan penyongsangnya, mengenal pasti unsur-unsur kesamaan dan menggabungkannya dengan polinomial yang tidak dapat dipinda serta transformasi *affine* untuk menghasilkan s-box penentu yang baru dan akan digunakan dalam lapisan penggantian. Penyelidikan ini juga mencadangkan fungsi baru iaitu fungsi RotateSwapDeterminant yang menggunakan putaran dan penggantian bit berdasarkan pengiraan penentu 4x4 dan akan berfungsi sebagai lapisan permutasi dalam algoritma DDBC. Output dari algoritma DDBC akan diuji dan disahkan melalui Ujian Statistik NIST. Ujian s-box akan dijalankan untuk mengesahkan keselamatan kotak-kotak penentu baru yang dihasilkan. Koefisien korelasi dan sensitiviti plainteks dan siferteks yang dihasilkan oleh algoritma DDBC akan diuji melalui eksperimen kesan *avalanche*. Analisis serangan linear, serangan perbezaan dan serangan pendek akan dilakukan terhadap algoritma DDBC untuk menganggarkan kejayaan kemungkinan ketiga-tiga serangan tersebut dan analisis prestasi dilakukan pada algoritma DDBC untuk menguji kelajuan penyulitan dan penyahsulitan blok serpihan. Akhir sekali analisis kerumitan dilaksanakan untuk memeriksa tahap kerumitan yang disumbangkan oleh s-box penentu yang telah diuji dan tidak diuji menerusi ujian s-box. Melalui eksperimen yang menyeluruh, algoritma DDBC yang dicadangkan telah berjaya melepasi Ujian Statistik NIST dengan kesemua 15 ujian menunjukkan p-value> 0.01. Keputusan dari ujian s-box menunjukkan

bahawa s-box penentu yang dibina memberikan keseimbangan yang baik, keseragaman perbezaan yang secukupnya, ketidaklinearan yang sangat baik, tahap algebra yang boleh diterima dan isyarat kepada nisbah hingar (SNR) yang memuaskan. Untuk analisis kesan *avalanche*, algoritma DDBC menunjukkan bahawa kebanyakan nilai korelasi yang diuji pada s-box penentu serta fungsi RotateSwapDeterminant yang dicadangkan menghampiri 0 yang membuktikan hubungan ketidaklinearan positif (atau negatif) yang bermaksud algoritma DDBC mempunyai sifat kekeliruan yang tinggi. Analisis serangan linear, serangan perbezaan dan serangan pendek menunjukkan kerumitan yang diperlukan adalah lebih daripada 2^{102} kali usaha percubaan untuk kriptanalisis linear, kerumitan yang diperlukan adalah lebih daripada 2^{104} kali usaha percubaan untuk kriptanalisis kebezaan dan sebanyak $(((2^8)^{10})^{256})^5$ jumlah kemungkinan percubaan untuk serangan pendek yang memberikan bukti yang mencukupi bahawa algoritma DDBC adalah kalis terhadap ketiga-tiga serangan tersebut. Analisis prestasi dari segi kelajuan pemprosesan proses penyulitan dan penyahsulitan algoritma DDBC menunjukkan perbezaan yang minimum dalam kedua-dua algoritma AES dan DDBC walaupun terdapat perbezaan kaedah transformasi yang digunakan dalam kedua-dua algoritma. Akhir sekali, analisis kerumitan menunjukkan bahawa s-box penentu yang telah melalui ujian analisis x-box mempamerkan kriteria *avalanche* yang lebih baik membuktikan tahap kerumitan yang lebih tinggi berbanding s-box penentu yang tidak diuji. Dari hasil analisis, telah jelas bahawa algoritma DDBC yang dicadangkan boleh dianggap sebagai salah satu sifer blok simetri yang selamat dan boleh digunakan sebagai alternatif kepada algoritma kriptografi lain dalam bidang penyelidikan keselamatan komputer.

ACKNOWLEDGEMENTS

First and foremost, I am eternally thankful to Allah for his blessings, strength and perseverance bestowed upon me, enabling me to complete this thesis. To begin with, I would like to express my sincere gratitude to my supervisors, Dr. Sharifah Md. Yasin, for her continuous support of my PhD study and related research, for her patience, guidance, and motivation, and Prof. Dr. Ramlan Mahmod for his guidance, immense knowledge, inspiration, and constant support throughout this research. Besides my advisors, I would like to thank the rest of my advisory committee, Associate Professor Dr. Nur Izura Udzir and Associate Professor Dr. Zuriati Ahmad Zukarnain, for their insightful comments and encouragement, and also for suggestions and fruitful advice on the dissertation proposal as well as in the completion of the dissertation. My sincere thanks go to the Ministry of Higher Education Malaysia (MOHE), for granted me with the MyBrain15 scholarship under MyPhD program. I express my gratitude to the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia for the laboratory equipment and facilities during the course of my study here. I thank all my precious colleagues who also act as my comrade-in-arms, Husna Saad, Sally Sulaiman, Safuan Raof, Azyyati Zazali, and 'Izzah Ezhar, with whom I have had the pleasure of sharing all the joyful memories over my PhD journey. Above all I am very grateful to have a patience, loving and supporting husband, Jazrin Ramli, and not to forget my families for their encouragement and love. Without them, this work would never have come into existence. Last but not least, thanks to all of those who have been directly and indirectly involved in helping me complete this research.

I certify that a Thesis Examination Committee has met on 18 May 2018 to conduct the final examination of Julia binti Juremi on her thesis entitled "Dynamic Determinant Matrix-Based Block Cipher 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:

Nor Fazlida binti Mohd Sani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

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

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

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

RUSLI HAJI ABDULLAH, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 30 July 2018

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:

Sharifah Md Yasin, PhD
Senior Lecturer
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
Professor
Faculty of Computer Science and Information Technology
Universiti Putra 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.: ____

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 Supervisory Committee: ______________________________

Signature: ______________________________
Name of Member of Supervisory Committee: ______________________________

Signature: ______________________________
Name of Member of Supervisory Committee: ______________________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
BBS	Blum Blum Shub
DES	Data encryption standard
GF	Galois Field
NIST	National Institute of Standards and Technology
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 Overview

As society has evolved and communications are expanding widely, the world becomes more connected to each other. People from all around the world are creating new ways of securing communications and cryptologist continues to develop secure algorithms to protect non-secure channels. Protection from the unauthorized access and cyber-attacks includes detection of any flaws and alterations in a network or system, and response towards the consequences of alteration and destruction are highly in demands. Cryptography is undoubtedly the most efficient means that is used to protect the confidentiality, integrity, authentication and non-repudiation of information. The underlying fundamental beneath cryptographic algorithms are mainly mathematical properties. Cryptographic algorithms protect not only data and privacy but it also protects people from someone who have ill-intentioned especially with the rapid growth of social medias and mobile applications. Once people get connected to the network, registered or posted anything online, it will never become private anymore. That information will always stays in the web, personal details can always be tracked down, information will be gathered, harvested and analysed by third parties. Cryptography protects not only data in computers, it is used to protect the data during the transmission, it protects any source of communications, and it also protects people's privacy, anonymity and sometimes it protects people's lives (Schneier, 2015).

In Malaysia, cryptography is a very active discipline and widely reinforced in information security area due to the numerous growths and developments in technology and industry. The Research Division of Cyber Security Malaysia (CSM), a national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI) team up with other government ministries and agencies are developing, coordinating and stimulating a continuous research activities and one of their successful initiative is developing the National Cryptography Policy. One of the current and future development are to design new, provable-secure cryptographic primitives and protocols, improving the security and efficiency of cryptographic applications, formalising and analysing common cryptographic practices and cryptanalysis. It is correspond with the main vision and mission of CSM which is to be a universally recognised National Cyber Security Reference and Specialist Centre by 2020 and to create and sustain a safer cyberspace to promote national sustainability, social well-being and wealth creation (Cyber Security Malaysia, 2017).

Symmetric block cipher algorithm is one of the significant cryptographic algorithms due to its simplicity, speed and robustness. The use of suitable symmetric block cipher to encrypt and decrypt data is unsurpassed and standard modus operandi to achieve privacy for storage systems especially in cloud storage (Kamara and Papamanthou, 2013). Changing a single bit in a string of key or doubling the key length may add a slight amount of work to a cryptologist, but it will also increases the attempts and difficulties of breaking the cipher. Attackers will have difficulties in accessing information since they have to bypass the mathematical properties embedded in the algorithm. The main purpose of every encryption algorithm is always to make it secure and make it as difficult as possible for attackers to break the ciphertext.

The Advanced Encryption Standard (AES), established by the U.S. National Institute of Standards and Technology (NIST) in 2001 is treated as the specification for data encryption. AES block cipher is developed by Joan Daemen and Vincent Rijmen. It is a block cipher with 128 bits block size and the keys come in one of three lengths: 128, 192 or 256 bits. The main objective of this research is to propose a new design of AES block cipher algorithm based on the properties of determinants, linear equations and its inverses. This research will also define the determinant matrix properties and approaches that will be used in cryptographic algorithm. This element can be associated with the encryption and decryption of the block cipher algorithm as well as providing the confusion and diffusion properties in cryptography.

1.2 Problem Statement

Since the nonlinearity of the block cipher depends heavily on the substitution box or known as s-box, which is normally fixed or static on each round, it has become the target of countless attacks. Fixed s-box permits attackers to study the s-box and find weak points (Janadi and Anas, 2008; Das et. al., 2012). The implementation of different s-boxes or dynamic s-boxes in preliminary research shows good cryptography strength as well as resistant to cryptanalysis attacks. Nevertheless, construction of dynamic s-boxes in previous researches does not focus on the importance of testing each particular s-box for its cryptographic properties before placing them in the substitution layer of the block cipher algorithm. The s-boxes that were constructed during the round transformation of a block cipher were not tested separately and independently hence lead to insufficient security. With regards to the literature, it is necessary to think of more on developing a proven satisfying s-boxes before implements them into a particular block cipher. A cryptographically secured s-box relies on several boolean properties and these properties need to be tested so that the usage of different secured s-boxes for different round contributes to higher complexity and leads to higher effort in cryptanalyzing the whole cipher. Therefore, this research will focus on increasing the complexity of the whole block cipher algorithm by proposing a new dynamic determinant block cipher (DDBC). New determinant s-boxes are proposed for the substitution layer, tested with several boolean properties and will be chosen randomly for each round of transformation making it unknown to the attackers. New RotateSwapDeterminant function is proposed for the permutation layer where the rotation and swapping of bits is based on the determinant computation to provide diffusion to the whole cipher. Both newly proposed substitution and permutation layer shall offer both confusion and diffusion properties needed so that the DDBC can be declared as a secure block cipher.

In linear algebra, the determinant matrix computation is performed on a square matrix and it shares the resemblance of the cipher state in a block cipher algorithm where the plaintext and ciphertext state is being organized in the form of square matrix to go through the round transformations. The determinant of a square matrix permits its inversion or is said to be reversible only if the properties of determinants are followed whereas in the block cipher algorithm, it is said that the encryption process is counted as successful only if the decryption process is reversible and returns the original plaintext. The similarities between the determinant matrix properties and the encryption decryption functions of a block cipher lead to few studies involving determinant matrix properties and its application in block ciphers algorithm (Obimbo and Salami, 2007; Ali, 2009). Nevertheless, to the best knowledge of the researcher, there has been no any work done to take the advantage of these properties in designing a whole new SPN symmetric block cipher algorithm. The simplicity of the matrix multiplication and inversion used in determinants generates not only fast output but also high throughput for enciphering and deciphering functions (Ismail et al., 2006; Toorani and Falahati, 2009; Valizadeh, 2016).

Although there are already various attempts and efforts emerged in new block ciphers enhancement, development of a new block cipher is always required by the industry as long as the security features are met (Junod and Verdenay, 2004). Since every country has different requirements when demanding for encryption algorithm, so there is no limit in developing a new one. Designing and improving a provable secure cryptographic primitives, protocols and applications are listed as one of the current and future research under Cyber Security Malaysia Research Division. This proves that there is always a necessity to study, to enhance or to develop a new cryptographic algorithm. Developing our own block cipher algorithm gives major benefit towards our own national security purposes. Therefore, the requirement to carry out researches on developing a secure block cipher algorithm to provide such security and privacy is always needed and should be performed continuously.

1.3 Objective of the Research

The objective of this research is to design and implement a secure dynamic symmetric encryption block cipher constructed based on the determinant matrix elements and properties. In order to achieve the objective, the following tasks will be carried out.

a) To design a new dynamic determinant block cipher algorithm (DDBC) based on the properties and elements of matrix and determinants of square matrices.

b) To propose new determinant s-boxes using combination of determinant computation, irreducible polynomials and affine transformation which satisfy all test criteria of good cryptographic s-boxes properties and proven to increase the complexity of whole DDBC algorithm.

c) To design a new RotateSwapDeterminant function based on the 4x4 determinant matrix computations which generates not only fast output and high throughput, but also to be used as the permutation layer and provides diffusion properties to the whole DDBC algorithm.

1.4 Scope of the Research

The scope of this research is to develop a secure dynamic block cipher which consists of the following features that will be taken into considerations:

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
The DDBC algorithm is required to pass all 15 standard randomness tests, succeed several s-box test criteria, avalanche effect and proven to be resisted against linear, differential and short attacks in order to fulfil the security requirements.

d) Performance and complexity analysis
An investigation to evaluate the performance of the DDBC algorithm in terms of the algorithm's encryption and decryption speed is included to ensure that the proposed algorithm is not only proven secure, but also considered as an efficient algorithm. The complexity analysis is to prove that the tested determinant s-boxes show better avalanche criteria compare to non-tested or randomly generated s-boxes.

1.5 Contributions of the Research

The research will contribute on the following:

a) This research identifies and uses determinant matrices properties to produce and design the new DDBC algorithm. The main elements and properties of determinant matrices can be applied within the symmetric encryption algorithm and still fulfil the confusion and diffusion properties in cryptography.

b) This research uses combination of determinant matrix computation, irreducible polynomials and affine transformation to generate not only one but different new determinant s-box to be used in each round of the DDBC transformations.

c) This research uses 4x4 determinant matrix computation to design a new permutation function namely RotateSwapDeterminant function in the DDBC algorithm. The structure of the components has a fixed block size of 128 bits and a key size of 128 bits.

d) The DDBC algorithm, like other secure block ciphers will be tested using the National Institute of Standards and Technology (NIST) statistical test suite to test for the quality and randomness of the output generated by the algorithm. The security criteria of all determinant s-boxes generated, avalanche effects, cryptanalysis, performance analysis and complexity analysis of the proposed DDBC algorithm will also be evaluated and presented in this research.

1.6 Organization of the Thesis

This thesis is organized into eight related chapters beginning with **Chapter 1** providing the introduction of the thesis which includes the research problems, research objectives, research scopes and contributions of the research.

Chapter 2 discusses the background study and literature surveys on the related work of the block cipher. The information includes the overview of cryptography narrowed down to symmetric block cipher, block cipher design structure, previous work of block ciphers, dynamic block ciphers and cryptanalysis, model with determinant functions and properties, terms and terminologies used in this thesis.

Chapter 3 describes the research methodology on how to conduct this research. This chapter also explains the experimental designs, the objective and benchmark of all security analysis that will be used in the process of measuring the confusion and diffusion of the DDBC block cipher as well as measuring the randomness of the DDBC output.

Chapter 4 presents the proposed design model of the determinant s-box and the proposed design model of the RotateSwapDeterminant. Brief summary on the properties of determinants matrix, irreducible polynomials and affine transformation are discussed with the aim to deliver a good view and understanding of the properties applies in the system. The design of the proposed determinant s-boxes and the proposed RotateSwapDeterminant function are illustrated and deliberated in details. The determinant s-boxes generated will then be used in the substitution layer and the RotateSwapDeterminant will be used as the permutation layer of the DDBC algorithm.

Chapter 5 presents the proposed design of the new dynamic determinant block cipher (DDBC). This chapter will illustrate the implementation of the new determinant s-boxes in the substitution layer and how the RotateSwapDeterminant function works as the permutation layer. The key addition layer are also explained in this section. This chapter also provides the whole operation flows of the DDBC algorithm.

Chapter 6 discusses the results of all Security Analysis involved in this research. Security Analysis I: S-box Test analysis for the new proposed determinant s-boxes providing the analysis of the confusion property of the DDBC. Security Analysis II: Avalanche effect where the results of the correlation coefficient performed on RotateSwapDeterminant function and correlation coefficient performed on all functions, including the key sensitivity test to fulfil the diffusion property of the DDBC is discussed. Security Analysis III: Randomness Test discusses the results of the randomness test performed on the output produced by the DDBC. The experiments were carried out using the NIST Statistical Test Suite application, which consists of 15 tests. Security Analysis IV: Cryptanalysis presents the attack on the DDBC algorithm. Several cryptanalysis attacks including linear, differential and short attack are calculated and comparisons of attempts needed are compared to the brute force attack.

Chapter 7 discusses the results of Analysis V: Performance Analysis which analysed DDBC in terms of the algorithm's encryption and decryption speed to prove the efficiency of the algorithm. This chapter also presents the result for Analysis VI: Complexity Analysis where the determinant s-boxes that have been tested through the s-box analysis test will go through the avalanche criteria computation and the results will be compared with the untested determinant s-boxes to test for the level of complexity produced by the DDBC algorithm.

Finally **Chapter 8** presents the conclusions of the whole research work carried out in this thesis. Some recommendations and suggestions for further efforts are proposed in this chapter.

REFERENCES

Abed, F., List, E., Lucks, S., Wenzel, J. (2013). Differential and linear cryptanalysis of reduced-round SIMON. Retrieved on 25 December 2014. http://eprint.iacr.org/2013/526.pdf.

Adams, C. (1997). The CAST-128 Encryption Algorithm. Retrieved on 17 April 2017. https://tools.ietf.org/pdf/rfc2144.pdf.

Adams, C., & Tavares, S. (1990). The structured design of cryptographically good S-boxes. *Journal of Cryptology*, *3*(1), 27-41.

Advanced Encryption Standard. Federal Information Processing Standard (FIPS), Publication 197, U.S. Department of Commerce, Washington D.C. National Institute of Standards and Technology. Nov. 2001.

Ajish, S. (2015). Wavelet based advanced encryption standard algorithm for image encryption. *International Journal of Engineering Research and General Science*, *3*(1).

Al-Wattar, A.H., Mahmod, R., Zukarnain, Z.A. and Udzir, N. (2015). A new DNA based approach of generating key-dependent mix column transformation. International *Journal of Computer Networks & Communications, 7(2).* Page 93.

Alabaichi, A. M., Mahmod, R., and Ahmad, F. (2013). Randomness Analysis on Blowfish Block Cipher. *AWERProcedia Information Technology & Computer Science: 3rd World Conference on Innovation and Computer Science.* Antalya, Turkey. Pages 1116-1127.

Alabaichi, A., Mahmod, R., & Ahmad, F. (2014). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB mode. *(IJCSIS) International Journal of Computer Science and Information Security, 11* (10) Pages 8-21.

Alani, M. d M. (2010). Testing randomness in ciphertext of block-ciphers using DieHard tests. *International Journal of Computer Science and Network Security*, *10* (4). Pages 53-57.

Ali, F. H. M.. PhD Thesis. A New 128-bit Block Cipher. Universiti Putra Malaysia, 2009.

Alizadeh, J., Bagheri, N., Gauravaram, P., Kumar, A., & Sanadhya, S. K. (2013). Linear Cryptanalysis of Round Reduced SIMON. *IACR Cryptology ePrint Archive*. Page 663.

Anderson, R., Biham, E., Knudsen, L., & Technion, H. (1998, August). Serpent: A flexible block cipher with maximum assurance. In *The first AES candidate conference* Pages 589-606.

Arrag, S., Hamdoun, A., Tragha, A., & Khamlich, S. E. (2013). Replace AES key expansion algorithm by modified genetic algorithm. *Applied Mathematical Sciences*, *7*(144), 7161-7171.

Ariffin, S., Jaafar, A., Rezal, M., and Mahmod, R. (2012). Permutation Function to Improve Confusion Performance of Round Transformation in Symmetric Encryption Scheme. *Computer Science and its Applications, Lecture Notes in Electrical Engineering*. Springer. Pages 339-351.

Ariffin, S., Mahmod, R., Jaafar, A., Rezal, M. and Ariffin, K. (2012). An immune system-inspired byte permutation function to improve confusion performance of round transformation in symmetric encryption scheme. In *Computer Science and its Applications*. Springer Netherlands. Pages 339-351.

Avanzi, R. (2017). The QARMA block cipher family. *IACR Trans. Symmetric Cryptol*, 4-44.

Bansod, G., Pisharoty, N. and Patil, A. (2016). PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing. *Defence Science Journal*, *66*(3). Pages 259-265.

Bay, A., Huang, J. and Vaudenay, S., (2014). Improved linear cryptanalysis of reduced-round MIBS. In *Advances in Information and Computer Security*. Springer International Publishing. Pages 204-220.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference*. ACM. Page 175.

Belazi, A., El-Latif, A. A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, *88*, 37-50.

Bhowmik, S. and Acharyya, S. (2011). Image cryptography: The genetic algorithm approach. In *Computer Science and Automation Engineering (CSAE), IEEE International Conference on* (Vol. 2. Pages 223-227.

Biham, E. and Carmeli, Y. (2014). An improvement of linear cryptanalysis with addition operations with applications to FEAL-8X. In *Selected Areas in Cryptography—SAC.* Springer International Publishing. Pages 59-76.

Biham, E., Anderson, R. and Knudsen, L. (1998). Serpent: A new block cipher proposal. In *Fast Software Encryption*. Springer Berlin Heidelberg. Pages 222-238.

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

Biham, E. and Shamir, A. (2012). Differential cryptanalysis of the data encryption standard. Springer Science & Business Media.

Biryukov, A., Khovratovich, D. (2009). Related-Key Cryptanalysis of the Full AES-192 and AES-256. In *Matsui, M. (ed.) ASIACRYPT 2009.* LNCS, vol. 5912, pages 1–18. Springer, Heidelberg.

Biryukov, A., Derbez, P., Perrin, L. (2015). Differential Analysis and Meet-In-the-Middle Attack Against Round-Reduced TWINE. *International Association for Cryptologic Research*. Springer Berlin Heidelberg. Pages 3-27.

Blondeau, C., & Nyberg, K. (2013, May). New links between differential and linear cryptanalysis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* pages 388-404. Springer, Berlin, Heidelberg.

Bogdanov, A. and Rechberger, C. (2011). A 3-Subset Meet-In-The-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN. *Selected Areas in Cryptography*, *Lecture Notes in Computer Science*. Waterloo, Ontario, Canada. Pages 229-240.

Bogdanov, A. and Rijmen, V. (2014). Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Designs, codes and cryptography*,*70*(3). Pages 369-383.

Bogdanov, A. and Wang, M. (2012). Zero correlation linear cryptanalysis with reduced data complexity. *International Association for Cryptologic Research*, Volume 7549 of the series Lecture Notes in Computer Science. Springer. Pages 29-48.

Bogdanov, A., Khovratovich, D., Rechberger, C. (2011). Biclique cryptanalysis of the full AES. *ASIACRYPT'11 Proceedings of the 17^{th} International Conference on The Theory and Application of Cryptology and Information Security*. Springer-Verlag Berlin, Heidelberg. Pages 344-371.

Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C. (2007). *PRESENT: An ultra-lightweight block.* Springer Berlin Heidelberg. Pages 450-466.

Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C. and Rombouts, P. (2012). PRINCE–a low-latency block cipher for pervasive computing applications. In *Advances in Cryptology–ASIACRYPT 2012.* Springer Berlin Heidelberg. Pages 208-225.

Burak, D. (2015). Parallelization of a Block Cipher Based on Chaotic Neural Networks. In *Artificial Intelligence and Soft Computing*. Springer International Publishing. Pages 191-201.

Burwick, C., Coppersmith, D., D'Avignon, E., Gennaro, R., Halevi, S., Jutla, C., Matyas, S.M., O'Connor, L., Peyravian, M., Safford, D. and Zunic, N. (1999). The Mars Encryption Algorithm. *IBM, August*, *27*.

Canteaut, A., Fuhr, T., Gilbert, H., Naya-Plasencia, M. and Reinhard, J.R. (2014). Multiple differential cryptanalysis of round-reduced PRINCE. In *Fast Software Encryption*. Springer Berlin Heidelberg. Pages 591-610.

Castro, J. C. H., Sierra, J. M., Seznec, A., Izquierdo, A., and Ribagorda, A. (2005). The strict avalanche criterion randomness test. *Mathematics and Computers in Simulation.* Elsevier, 68(1). Pages 1-7.

Chakraborty, D. and Sarkar, P. (2006). A new mode of encryption providing a tweakable strong pseudo-random permutation. In *Fast Software Encryption.* Springer Berlin Heidelberg. Pages 293-309.

Chandrasekharappa, T. G. S., Prema, K. V., & Shama, K. (2011). S-boxes generated using affine transformation giving maximum avalanche effect. *International Journal on Computer Science and Engineering*, *3*(9), 3185.

Chang, D., Ghosh, M., Sanadhya, S. (2015). Biclique cryptanalysis of full round AES-128 based hashing modes. Department of Computer Science and Engineering. Technical report, Indraprastha Institute of Information Technology.

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

Chen, J., Wang, M. and Preneel, B. (2012). Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT. In *Progress in Cryptology-AFRICACRYPT.* Springer Berlin Heidelberg. Pages 117-137.

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

Cheung, J. M. (2010). *The design of S-boxes* (Doctoral dissertation, San Diego State University).

Cobas, J., & Brugos, J. (2005). Complexity-theoretical approaches to the design and analysis of cryptographical boolean functions. *Computer Aided Systems Theory–EUROCAST 2005*, 337-345.

Courtois, N., Mourouzis, T., Song, G., Sepehrdad, P. and Susil, P. (2014). Combined algebraic and truncated differential cryptanalysis on reduced-round Simon. In *SECRYPT 2014-Proceedings of the 11th International Conference on Security and Cryptograph.* Science and Technology Publications. Vol. 11. Pages 399-404.

Crowley, P. (2005). Truncated differential cryptanalysis of five rounds of Salsa20. *International Association of Cryptologic Research.*

Cui, J., Huang, L., Zhong, H., Chang, C., & Yang, W. (2011). An improved AES S-Box and its performance analysis. *International Journal of Innovative Computing, Information and Control*, *7*(5), 2291-2302.

Cyber Security Research, Cyber Security Malaysia, http://www.cybersecurity.my/en/our_services/research/main/detail/2331/index.html (accessed July 2017).

Daemen, J., Knudsen, L. and Rijmen, V. (1997). The block cipher Square. In *Fast software encryption*. Springer Berlin Heidelberg. Pages 149-165.

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

Daemen, J., Knudsen, L. and Rijmen, V. (2002). The design of Rijndael: *AES-the advanced encryption standard*: Springer.

Dara, S., & Fluhrer, S. (2014, October). FNR: Arbitrary length small domain block cipher proposal. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer, Cham. Pages 146-154.

Das, I., Nath, S., Roy, S., & Mondal, S. (2012, December). Random S-Box Generation in AES by changing Irreducible polynomial. In *Communications, Devices and Intelligent Systems (CODIS), 2012 International Conference on* pages 556-559. IEEE.

Doganaksoy, A., Ege, B., Koçak, O., and Sulak, F. (2010). Cryptographic Randomness Testing of Block Ciphers and Hash Functions. *IACR Cryptology ePrint Archive*. 564, Pages 1-12.

Dunkelman, O., Keller, N., Shamir, A. (2010). Improved Single-Key Attacks on 8-Round AES-192 and AES-256. *International Association for Cryptologic Reseach ASIACRYPT 2010*. Pages 158-176.

El-Ramly, S. H., El-Garf, T., & Soliman, A. H. (2001). Dynamic generation of S-boxes in block cipher systems. In *Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National* (Vol. 2, Pages 389-397). IEEE.

Elkamchouchi, H. M., & Makar, M. A. (2004, March). Kamkar symmetric block cipher. In *Radio Science Conference, 2004. NRSC 2004. Proceedings of the Twenty-First National* (pp. C1-1). IEEE.

Emami, S., & McDonald, C. Truncated Differential Analysis of Reduced-Round.

Fahmy, A., Shaarawy, M., El-Hadad, K., Salama, G., and Hassanain, K. (2005). A proposal For A key-dependent AES. *3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications.* Tunisia: SETIT.

Faraoun, K.M. (2014). A genetic strategy to design cellular automata based block ciphers. *Expert Systems with Applications*, *41*(17). Pages 7958-7967.

Forouzan, B. A. (2008). *Introduction to Cryptography and Network Security.* McGrawHill.

Gérard, B., Grosso, V., Naya-Plasencia, M. and Standaert, F.X. (2013). Block ciphers that are easier to mask: how far can we go?. In *Cryptographic Hardware and Embedded Systems-CHES.* Springer Berlin Heidelberg. Pages 383-399.

Gilbert, H., and Peyrin, T. (2010). Super S-box Cryptanalysis: Improved Attacks for AES-like Permutations. In Hong and Iwata. Pages 365–383.

Golić, J. D. (1996, May). Fast low order approximation of cryptographic functions. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 268-282). Springer, Berlin, Heidelberg.

Gong, Z., Nikova, S. and Law, Y.W. (2011). *KLEIN: a new family of lightweight block ciphers*. Springer Berlin Heidelberg. Pages 1-18.

Grocholewska-Czurylo, A. (2011, April). Cryptographic properties of modified AES-like S-boxes. In *Annales Universitatis Mariae Curie-Sklodowska* (Vol. 11, No. 2, p. 37). De Gruyter Open Sp. z oo.

Guilley, S., Hoogvorst, P., & Pacalet, R. (2004). Differential power analysis model and some results. *Smart Card Research and Advanced Applications Vi*. Pages 127-142.

Guo, J., Peyrin, T., Poschmann, A. and Robshaw, M. (2011). The LED block cipher. In *Cryptographic Hardware and Embedded Systems–CHES 2011*. Springer Berlin Heidelberg. Pages 326-341.

Halevi, S. and Rogaway, P. (2003). A tweakable enciphering mode. In *Advances in Cryptology-CRYPTO.* Springer Berlin Heidelberg. Pages 482-499.

Heys, H. M. (2001). A tutorial on linear and differential cryptanalysis. *Cryptologia*. *Taylor & Francis, 26*(3). Pages 189-221.

Hill, L. S. (1929). Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, *36*(6). Pages 306-312.

Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.S., Lee, C., Chang, D., Lee, J., Jeong, K. and Kim, H. (2006). HIGHT: A new block cipher suitable for low-resource device. In *Cryptographic Hardware and Embedded Systems-CHES.* Springer Berlin Heidelberg. Pages 46-59.

Hong, D., Lee, J.K., Kim, D.C., Kwon, D., Ryu, K.H. and Lee, D.G. (2013). LEA: A 128-bit block cipher for fast encryption on common processors. In *Information Security Applications.* Springer International Publishing. Pages 3-27.

Hosseinkhani, R., & Javadi, H. H. S. (2012). Using cipher key to generate dynamic S-box in AES cipher system. *International Journal of Computer Science and Security (IJCSS)*, *6*(1), Pages 19-28.

Huang, T., Tjuawinata, I. and Wu, H. (2015). Differential-linear cryptanalysis of ICEPOLE. In *Fast Software Encryption*. Springer Berlin Heidelberg. Pages 243-263.

Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, U. Y. (2011). Some analysis of S-box based on residue of prime number. *Proc Pak Acad Sci*, *48*(2).Pages 111-115.

Ismail, I. A., Amin, M., & Diab, H. (2006). How to repair the Hill cipher. *Journal of Zhejiang University-Science A*, *7*(12).Pages 2022-2030.

Izadi, M., Sadeghiyan, B., Sadeghian, S.S. and Khanooki, H.A. (2009). MIBS: a new lightweight block cipher. In *Cryptology and Network Security.* Springer Berlin Heidelberg. Pages 334-348.

Jacob, G., Murugan, A., & Viola, I. (2015). Towards the Generation of a Dynamic Key-Dependent S-Box to Enhance Security. *IACR Cryptology ePrint Archive*, *2015*, 92.

Jamil, N., Mahmod, R., Z`aba, M. R., Udzir, N. I., and Zukarnain, Z. A. (2013). Diffusion and Statistical Analysis of STITCH-256. *Journal of Applied Sciences, 13: 673-682.*

Janadi, A., & Tarah, D. A. (2008, April). AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes. In *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*. IEEE. Pages 1-6.

Jean, J., Nikolic, I. and Peyrin, T. (2014). Tweaks and keys for block ciphers: the TWEAKEY framework. In *Advances in Cryptology–ASIACRYPT.* Springer Berlin Heidelberg. Pages 274-288.

Junod, P., & Vaudenay, S. (2004, August). FOX: a new family of block ciphers. In *International Workshop on Selected Areas in Cryptography*. Pages 114-129. Springer, Berlin, Heidelberg.

Kamali, S.H. and Maysam Hedayati, (2010). A new modified version of advanced encryption standard based algorithm for image encryption. *International Conference on Electronics and Information Engineering (ICEIE),* Islamic Azad University Qazvin Branch, Iran. Volume 1, 141-145.

Kamara, S., and Papamanthou, C. (2013). Parallel and dynamic searchable symmetric encryption. *Financial Cryptography and Data Security, FC*. Pages 258-274.

Katos, V. (2005). A randomness test for block ciphers. *Applied mathematics and computation.* Elsevier,162(1). Pages 29-35.

Kavut, S., & Yücel, M. D. (2001, May). On some cryptographic properties of Rijndael. In *MMM-ACNS* .Pages 300-312.

Kazlauskas, K., Vaicekauskas, G., & Smaliukas, R. (2015). An algorithm for key-dependent S-box generation in block cipher system. *Informatica*, *26*(1), Pages 51-65.

Kazymyrov, O., Kazymyrova, V., & Oliynykov, R. (2013). A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent. *IACR Cryptology ePrint Archive*, *2013*. Page 578.

Keliher, L., & Meijer, H. (1997). A New Substitution-Permutation Network Cipher Using Key-Dependent S-Boxes. In *Proc. of Fourth Annual Workshop on Selected Areas in Cryptography (SAC97)*. Page 1326.

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

Kolay, S. and Mukhopadhyay, D. (2014). Khudra: A new lightweight block cipher for FPGAs. In *Security, Privacy, and Applied Cryptography Engineering.* Springer International Publishing. Pages 126-145.

Koyama, T., Wang, L., Sasaki, Y., Sakiyama, K., Ohta, K.: New Truncated Differential Cryptanalysis on 3D Block Cipher. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232. Pages 109–125. Springer, Heidelberg (2012)

Kumar, M., Pal, S.K. and Panigrahi, A. (2014). FeW: A Lightweight Block Cipher. *IACR Cryptology ePrint Archive*. Page 326.

L'ecuyer, P. and Simard, R. 2007. TestU01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software*. Vol. 33, No. 4, Article 22.

Lai, X. and Massey, J.L. (1991). A Proposal for a New Block Encryption Standard, Advances in Cryptology-Eurocypt'90. Springer-Verlag, Berlin. Pages 389-404.

Li, L., Liu, B., & Wang, H. (2016). QTL: a new ultra-lightweight block cipher. *Microprocessors and Microsystems*, *45*. Pages 45-55.

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

Lim, C.H. and Korkishko, T. (2005). mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors. In *Information Security Applications*. Springer Berlin Heidelberg. Pages 243-258.

Limin, F., Dengguo, F., and Yongbin, Z. (2008). A fuzzy-based randomness evaluation model for block cipher. *Journal of Computer Research and Development*, *45*(12). Pages 2095-2101.

Liskov, M., Rivest, R.L. and Wagner, D. (2002). Tweakable block ciphers. In *Advances in Cryptology—CRYPTO.* Springer Berlin Heidelberg. Pages 31-46.

Liu, Y., Wang, J., Fan, J., & Gong, L. (2016). Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. *Multimedia Tools and Applications*, *75*(8), 4363-4382.

Luo, Y., & Lai, X. (2017). Improvements for Finding Impossible Differentials of Block Cipher Structures. *Security and Communication Networks*, *2017*.

Mahmoud, Eman Mohammed, Abdelhalim Zekry, Ahmed Abd El Hafez, and Talaat A. Elgarf. (2013) "Enhancing channel coding using AES block cipher." *International Journal of Computer Applications* 61, no. 6 (2013).

Mamadolimov, A., Isa, H., & Mohamad, M. S. (2013). Practical bijective S-box design. *arXiv preprint arXiv:1301.4723*.

Marsaglia, G. (1995). The Marsaglia Random Number CDROM including the DieHard Battery of Tests of Randomness. Available from http://www.stat.fsu.edu/pub/diehard.

Matsui, M. (1993). Linear cryptanalysis method for DES cipher. In *Advances in Cryptology EUROCRYPT 93*. Springer Berlin Heidelberg. Pages 386-397.

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

Mennink, B. (2016, August). XPX: generalized tweakable Even-Mansour with improved security guarantees. In *Annual Cryptology Conference.* Pages 64-94. Springer Berlin Heidelberg.

Merkle, R.C. (1989). Fast Software Encryption Functions (PDF/PostScript). Advances in Cryptology-CRYPTO '90. Santa Barbara, California: Springer-Verlag. Pages 476–501.

Mister, S., & Adams, C. (1996, August). Practical S-box design. In *Workshop on Selected Areas in Cryptography, SAC*(Vol. 96. Pages 61-76.

Mohammad, F. Y., Rohiem, A. E., and Elbayoumy, A. D. (2009). A novel S-box of AES algorithm using variable mapping technique. *Proceedings of the*

13th International Conference on Aerospace Sciences and Aviation Technology. Kobry Elkobbah, Cairo, Egypt. Pages 1-10.

Mohamed, K., Pauzi, M. N. M., Ali, F. H. H. M., Ariffin, S., & Zulkipli, N. H. N. (2014, September). Study of S-box properties in block cipher. In *Computer, Communications, and Control Technology (I4CT), 2014 International Conference on* pages 362-366. IEEE.

Mohan, H. S., and Reddy, A. R. (2011). Performance Analysis of AES and MARS Encryption Algorithms. *International Journal of Computer Science Issues (IJCSI), 8*(4). Pages 363-368.

Mourouzis, T., Song, G., Courtois, N. and Christofii, M. (2015). Advanced Differential Cryptanalysis of Reduced-Round SIMON64/128 Using Large-Round Statistical Distinguishers. *IACR Cryptology ePrint Archive*. Page 481.

Nagaraj, V., Vijayalakshmi, V., & Zayaraz, G. (2013). Overview of digital steganography methods and its applications. *International Journal of Advanced Science and Technology*, *60*, 45-58.

Naito, Y. (2015). Full PRF-secure message authentication code based on tweakable block cipher. In *International Conference on Provable Security*. Pages 167-182. Springer, Cham.

Nakahara, J.J. (2008). 3D: A three-dimensional block cipher. In *Cryptology and Network Security*. Springer Berlin Heidelberg. Pages 252-267.

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.

Obimbo, C., & Salami, B. (2007). A Parallel Algorithm for determining the inverse of a matrix for use in blockcipher encryption/decryption. *The Journal of Supercomputing*, *39*(2), pages 113-130.

Oliynykov, R., Gorbenko, I., Kazymyrov, O., Ruzhentsev, V., Kuznetsov, O., Gorbenko, Y., Dyrda, O., Dolgov, V., Pushkaryov, A., Mordvinov, R. and Kaidalov, D. (2015). *A new encryption standard of Ukraine: The Kalyna block cipher*. Cryptology ePrint Archive. Report 2015/650. Available at http://eprint. iacr. org/2015/650.pdf.

Paar, C., Pelzl J. (2010). *Understanding Cryptography. AText Book for Students and Practitioners.* Springer-Verlag Berlin Heidelberg.

Picek, S., Batina, L., Jakobović, D., Ege, B., & Golub, M. (2014, June). S-box, SET, match: a toolbox for S-box analysis. In *IFIP International Workshop on Information Security Theory and Practice*. Pages 140-149. Springer, Berlin, Heidelberg.

Piscitelli, R., Bhasin, S., & Regazzoni, F. (2017). Fault attacks, injection techniques and tools for simulation. In *Hardware Security and Trust*. Pages 27-47. Springer International Publishing.

Raddum, H. (2005, May). More dual rijndaels. In *International Conference on Advanced Encryption Standard*. Pages 142-147. Springer, Berlin, Heidelberg.

Rasoolzadeh, S., Ahmadian, Z., Salmasizadeh, M., & Aref, M. R. (2014). Total break of Zorro using linear and differential attacks. *The ISC International Journal of Information Security*, *6*(1), pages 23-34.

Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A. and De Win, E. (1996). The cipher SHARK. In *Fast Software Encryption.* Springer Berlin Heidelberg. Pages 99-111.

Rivest, R.L., Robshaw, M.J.B., Sidney, R. and Yin, Y.L. (1998). The $\mathrm{RC6}^{\mathrm{TM}}$ block cipher. In *First Advanced Encryption Standard (AES) Conference*.

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. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic application*s. Technical report, National Institute of Standards and Technology Special Publication. Report number: 800-22.

Sabry, M., Hashem, M., Nazmy, T. and Khalifa, M.E. (2015). Design of DNA-based Advanced Encryption Standard (AES). In *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS).* Pages 390-397. IEEE.

Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In *Fast Software Encryption*. Springer Berlin Heidelberg. Pages 191-204.

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

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N. (1998). Twofish: A 128-bit block cipher. *NIST AES Proposal*,15.

Schneier, B., 2015, Schneier on Security, https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html (accessed 15 August 2015).

Sen, S., Shaw, C., Chowdhuri, D.R., Ganguly, N. and Chaudhuri, P.P. (2002). Cellular automata based cryptosystem (CAC). In *Information and Communications Security.* Springer Berlin Heidelberg. Pages 303-314.

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

Shehab, E., Farag, A.K. and Keshk, A. (2014). An Image Encryption Technique based on DNA Encoding and Round-reduced AES Block Cipher. *International Journal of Computer Applications*, *107*(20).

Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T. (2011). Piccolo: an ultra-lightweight blockcipher. In *Cryptographic Hardware and Embedded Systems–CHES.* Springer Berlin Heidelberg. Pages 342-357.

Shimizu, A. and Miyaguchi, S. (1988). Fast data encipherment algorithm FEAL, Advances in Cryptology — Eurocrypt '87, Springer-Verlag. Pages 267–280.

Soleimany, H. and Nyberg, K. (2014). Zero-correlation linear cryptanalysis of reduced-round LBlock. *Designs, Codes and Cryptography*, *73*(2). Pages 683-698.

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. (1999). Randomness testing of the AES candidate algorithms. Technical report, National Institute of Standards and Technology.

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

Standaert, F.X., Piret, G., Gershenfeld, N. and Quisquater, J.J. (2006). SEA: A scalable encryption algorithm for small embedded applications. In *Smart Card Research and Advanced Applications.* Springer Berlin Heidelberg. Pages 222-236.

Standaert, F. X., Piret, G., Quisquater, J. (2003). Cryptanalysis of Block Cipher : A Survey. Technical report, UCL Crypto Group Technical Report Series.

Stoianov, I., & Zorzi, M. (2012). Emergence of a'visual number sense'in hierarchical generative models. *Nature neuroscience*, *15*(2), pages 194-196.

Sulaiman, S., Muda, Z., Juremi, J., Mahmod, R., and Yasin, S.M. (2012). A New ShiftColumn Transformation : An Enhancement of Rijndael Key Scheduling. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1*(3). Pages 160–166.

Sulak, F., Doganaksoy, A., Ege, B., and Koak, O. (2010). Evaluation of randomness test results for short sequences. In *Sequences and Their Applications–SETA 2010.* Springer Berlin Heidelberg. Pages 309-319.

Suri, Pushpa R, & Deora, S. S. (2011). 3D array block rotation cipher: An improvement using lateral shift. *Global Journal of Computer Science and Technology*, *11*(19). Pages 1-8.

Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E. (2012). TWINE: A Lightweight Block Cipher for Multiple Platforms. In *Selected Areas in Cryptography.* Springer Berlin Heidelberg. Pages 339-354.

Szaban, M., & Seredynski, F. (2011, February). Dynamic cellular automata-based S-boxes. In *International Conference on Computer Aided Systems Theory*. Pages 184-191). Springer, Berlin, Heidelberg.

Szidarovszky, F. and Molnar, S.. (2001). *Introduction to Matrix Thory with Applications to Business and Economics.* World Scientific.

Taylor, R. (1990). Interpretation of the correlation coefficient: A basic review. *JDMS*,1:35-39.

Tezcan, C. (2016). Truncated, Impossible, and Improbable Differential Analysis of ASCON. *IACR Cryptology ePrint Archive*, *2016*, page 490.

Toorani, M., & Falahati, A. (2009, July). A secure variant of the Hill cipher. In *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on* pages 313-316). IEEE.

Urias, J., Ugalde, E. and Salazar, G. (1998). A cryptosystem based on cellular automata. *Chaos: An Interdisciplinary Journal of Nonlinear Science*,*8*(4). Pages 819-822.

Valizadeh, M. H. (2016). Healing the Hill Cipher, Improved Approach to Secure Modified Hill against Zero-plaintext Attack. *IACR Cryptology ePrint Archive*, *2016*, 806.

Vasantha, S., Shivakumar, N. and Rao, D.S. (2015). A New Encryption and Decryption Algorithm for Block Cipher Using Cellular Automata Rules. *International Journal*. Page 130.

Vaudenay, S. (1994, December). On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In *International Workshop on Fast Software Encryption* (pp. 286-297). Springer, Berlin, Heidelberg.

Vergili, I., & Yücel, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n\times n S-Boxes. *Turkish Journal of Electrical Engineering & Computer Sciences*, *9*(2). Pages 137-146.

Wang, Y., Wong, K.-W., Liao, X., and Xiang, T. (2009). A block cipher with dynamic s-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation*, 14(7). Pages 3089-3099.

Wang, Y., Wu, W., Guo, Z. and Yu, X., (2014). Differential cryptanalysis and linear distinguisher of full-round Zorro. In *Applied Cryptography and Network Security*. Springer International Publishing. Pages 308-323.

Webster, A. F., and Tavares, S. E. (1986). On the design of S-Boxes. In Williams, H., editor, *Advances in Cryptology—CRYPTO'85 Proceedings.* Springer Berlin Heidelberg. Pages 523-534.

Wen, L., Wang, M., Bogdanov, A. (2014). Multidimensional zero-correlation linear cryptanalysis of E2. In *Progress in Cryptology - AFRICACRYPT*. Springer International Publishing Switzerland. Pages 147-164.

Wu, W. and Zhang, L. (2011). LBlock: A lightweight block cipher. In *Applied Cryptography and Network Security.* Springer Berlin Heidelberg. Pages 327-344.

Yang, Q., Hu, L., Sun, S., & Song, L. (2016, September). Related-key impossible differential analysis of full khudra. In *International Workshop on Security* (pp. 135-146). Springer International Publishing.

Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., & Samet, M. (2010, May). A new design of dynamic S-Box based on two chaotic maps. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on* (pp. 1-6). IEEE.

Zakaria, N. H.. PhD Thesis. A Block Cipher Based on Genetic Algorithm. Universiti
Putra Malaysia, 2017.

Zakaria, A. A., Abdullah, N. A. N., Omar, W. Z., Yusof, N. A. M., & Rani, H. A. (2016). Automated analysis report generation using CSMS-Box Evaluation Tool (CSET). International Journal of Cryptology Research 6(1): 47 - 63 (2016).

Zakaria N., Mahmod R., Udzir N.I., and Zukarnain Z. A., and Ariffin S., 2015. Designing New Block Cipher Based On Genetic Algorithm Approach. International Journal of Computer Science and Information Security. ISSN: 1947-5500.

Zhang, R., & Chen, L. (2008, June). A block cipher using key-dependent S-box and P-boxes. In *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on* (pp. 1463-1468). IEEE.

Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B. and Verbauwhede, I. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, *58*(12). Pages 1-15.

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*. Elsevier, *179*(19). Pages 3442-3450.