A NEW KD-3D-CA BLOCK CIPHER WITH DYNAMIC S BOXES BASED ON 3D CELLULAR AUTOMATA

AYMAN MAJID HAMID

FSKTM 2019 57

A NEW KD-3D-CA BLOCK CIPHER WITH DYNAMIC S BOXES BASED ON 3D CELLULAR AUTOMATA

By

AYMAN MAJID HAMID

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

July 2019

DEDICATION

To my beloved

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

A NEW KD-3D-CA BLOCK CIPHER WITH DYNAMIC S BOXES BASED ON 3D CELLULAR AUTOMATA

By

AYMAN MAJID HAMID

July 2019

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

Due to the ubiquity of digital communications and digital data in today's world, the development of techniques and tools to protect wireless communications and information transfer has become increasingly important. Currently, static substitution boxes (S-Boxes) are vulnerable to data and subkey attacks. Various techniques have been considered in the literature to improve S-Boxes using cellular automata (CA) with different rules such as 1-D, 2-D, and 3D CA rules.

S-Boxes could either be static or dynamic. While the previous work provides some form of security, the latter work is better. A strong key expansion mechanism makes the cipher more resistant to various forms of attacks, especially related-key model attacks. Rijndael is the most common block cipher and it was adopted by the National Institute of Standards and Technology, USA in 2001 as an Advanced Encryption Standard (AES). However, cryptanalysts have revealed the security weaknesses of Rijndael in terms of its vulnerability to related-key differential and linear attacks that are mainly caused by lack of nonlinearity in its key schedule. Most research in the literature used fixed key expansion algorithm for encryption and decryption. However, the fixed key expansion is vulnerable to square attack. On the other hand, the round key expansion algorithms are relatively simple. Nevertheless, they may also be attacked easily. Considering the aforementioned challenges, this research proposes a new model for 3D-CA block cipher.

First, potential problems in AES and CA block ciphers such as fixed key expansion, the static nature of S-Boxes, and the low level of data permutation for each round are identified and analyzed. The requirements of the intended KD-3D-CA block cipher and its rule for a key size of 128-bit are designed. After that, critical performance measurements and metrics used in 3D–CA are identified. The module of a KD-3D-

CA block cipher is designed and algorithms of the new KD-3D-CA block cipher are generated. KD-3D-CA cryptosystem security was tested using NIST statistical tools, Avalanche test, S-Box Evaluation Tool (SET) test, performance test, and complexity test. In this thesis, new algorithms are proposed for the key generation, encryption and decryption module of KD-3D-CA block cipher based on von Neumann (3D) cellular automata. The algorithms are tested for randomness and security by using the National Institute of Standards and Technology (NIST) statistical tests within nine datasets in the third and final rounds. Moreover, new dynamic S-Boxes are proposed and tested for their security characteristics using SET and CSET tools.

Avalanche test is carried out for KD-3D-CA block cipher to ensure a single bit change in the key or plaintext forms different rounds. Half of the ciphertexts changed for each round. Eight 3D-CA-S-Boxes were also tested for their security characteristics with a particular focus on resistance to linear and differential attacks. The findings show that the proposed KD-3D-CA block cipher is more secure than the existing CA block ciphers. The KD-3D-CA block cipher was tested using nine different datasets with the following criteria: Avalanche key, Avalanche plaintext, CBC mode, correlation key and plaintext, low and high density for both plaintext and the key. Furthermore, this block cipher passed the NIST statistical test which satisfies the randomness criteria in different rounds with alpha values 0.01 and 0.001. The proposed 3D S-Boxes meet the security requirements of an efficient S-Box such as balance, completeness, Strict Avalanche Criterion (SAC), nonlinearity, bit independence, differential uniformity (DU), inevitability, and non-contradiction. The S-Boxes exhibit an equal performance when compared with the AES S-Box and they are resistant to attacks such as differential and linear attacks. Moreover, the block cipher passes the Avalanche Effect Test with a result of 0.01, which indicates a satisfactory key expansion property.

Lastly, KD-3D-CA Block cipher is more complex and it outperforms AES with more than 25% for different key sizes. Deductively, the proposed KD-3D-CA block cipher algorithm is more secure than other block cipher algorithms and can be implemented for data encryption and decryption.

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

SIFER BLOK BARU 3D-CA DENGAN S BOX DINAMIK BERASASKAN 3D SELULAR AUTOMATA

Oleh

AYMAN MAJID HAMID

Julai 2019

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

Oleh kerana keleluasaan komunikasi digital dan data digital di dunia hari ini, pembangunan teknik-teknik dan alat untuk melindungi mereka telah menjadi semakin lebih penting. Pada masa ini, statik S-kotak mudah terdedah kepada serangan data dan serangan sub-utama. Pelbagai teknik digunakan dalam kesusasteraan untuk meningkatkan S-Box menggunakan automata selular dengan peraturan yang berbeza seperti 1-D, 2-D, atau kaedah-kaedah 3D CA. Juga, dinamik S-kotak

Adalah lebih baik daripada statik S-kotak. Pengembangan utama kuat menggalakkan cipher yang akan menjadi lebih tahan kepada pelbagai bentuk serangan, terutamanya dalam serangan model berkaitan utama. Rijndael adalah blok cipher paling biasa, dan ia telah diterima pakai oleh Institut Piawaian dan Teknologi Amerika Syarikat pada tahun 2001 sebagai Piawaian Penyulitan Lanjutan (AES). Walau bagaimanapun, beberapa kajian pada pembacaan sandi mendedahkan bahawa kelemahan keselamatan Rijndael merujuk kepada kelemahan kepada serangan pengkamiran berkaitan-utama serta serangan boomerang berkaitan utama, yang sebahagian besarnya disebabkan oleh kekurangan ketaklelurusan dalam jadual utama Rijndael. Kebanyakan algoritma yang digunakan algoritma pengembangan utama tetap untuk penyulitan dan penyahsulitan. Walau bagaimanapun, pengembangan kunci tetap terdedah kepada serangan persegi. Apabila pusingan algoritma pengembangan utama adalah agak mudah,

Mereka mungkin diserang dengan mudah. Objektif kajian ini adalah untuk mencadangkan model baru 3D-CA blok cipher. masalah yang mungkin berlaku dalam AES dan CA sifer blok seperti ditetapkan pada pengembangan utama juga, sifat statik daripada S-Box selain yang rendah atur data untuk setiap pusingan dikenal pasti dan dianalisis. Kemudian, keperluan KD-3D-CA blok cipher dikumpulkan bersama-sama

dengan peraturan untuk saiz kunci 128-bit. Selepas itu, ukuran prestasi kritikal dan metrik digunakan dalam 3D-CA dikenalpasti. Kemudian, modul yang KD-3D-CA blok cipher direka dan algoritma baru blok KD-3D-CA cipher baru dihasilkan. KD-3D-CA adalah dibangunkan kemudian diikuti dengan menguji keselamatan kriptografi KD-3D-CA menggunakan alat statistik NIST, dan runtuhan ujian, ujian SET, ujian prestasi, dan ujian kerumitan. Dalam kajian ini, algoritma baru dicadangkan untuk generasi utama, penyulitan dan modul penyahsulitan KD-3D-CA blok cipher berdasarkan Von Neumann (3D) automata selular. Selain itu, algoritma diuji untuk rambang dan keselamatan dengan menggunakan NIST ujian statistik dalam tempoh sembilan set data untuk pusingan tiga dan pusingan akhir. New dinamik S-Boxes dicadangkan dan diuji kepada ciri-ciri selamat menggunakan SET dan alat CSET.

Ujian runtuhan dijalankan untuk KD-3D-CA blok cipher untuk memastikan jika perubahan bit tunggal dalam kunci atau plaintext untuk pusingan yang berbeza, separuh daripada tulisan rahsia akan ditukar untuk pusingan ini. Juga, lapan 3D-CA-S-Boxes juga diuji untuk ciri-ciri selamat dan terutamanya aman daripada linear dan pengkamiran serangan. Dapatan kajian menunjukkan bahawa cadangan blok KD-3D-CA cipher adalah lebih selamat daripada sifer blok CA sedia ada. KD-3D-CA blok cipher menjalani ujian dengan sembilan set data yang berbeza masing-masing dengan kriteria: utama runtuhan, runtuhan plaintext, mod CBC, kunci korelasi dan plaintext, ketumpatan yang rendah, kepadatan tinggi untuk kedua-dua plaintext dan kunci. Juga, blok cipher ini lulus ujian statistik NIST yang memenuhi kriteria rawak dalam pusingan yang berbeza dengan alpha bersamaan dengan 0.01 dan 0.001. Juga, cadangan 3D-S-kotak memenuhi tahap keselamatan yang baik S-Box seimbang, kesempurnaan, ketat runtuhan kriteria (SAC), ketaklelurusan, sedikit kemerdekaan, pembezaan keseragaman (DU), tidak dapat dielakkan, bukan percanggahan. S-Boxes menunjukkan keputusan yang sama berbanding dengan AES S-Box dan mereka adalah penentangan terhadap apa-apa jenis menyerang seperti pembezaan dan serangan linear. Juga, cipher blok lulus Ujian Kesan Avalanche dengan keputusan yang sama dengan 0.005 yang menunjukkan ia mempunyai pengembangan utama yang baik. Dapatan terakhir adalah bahawa KD-3D-CA Blok cipher baru mempunyai prestasi lebih daripada AES kurang daripada 25% bagi saiz kekunci yang berbeza dan ia adalah lebih kompleks.

Untuk semua keputusan di atas kita boleh membuat kesimpulan bahawa menggunakan baru KD-3D-CA blok cipher untuk penyulitan data adalah mencukupi dan lebih selamat daripada algoritma blok cipher lain dan boleh melaksanakan untuk penyulitan dan penyahsulitan data.

ACKNOWLEDGEMENT

I am particularly grateful to my supervisor, Dr. Sharifah Yasin for the help and encouragement and support during the course of this research. I would also like to thank my supervisory committee members: Prof. Dr. Zuriati Binti Ahmad Zukarnain, Dr. Nur Izura udzir, and Dr. Sherzod Rustamovic Turaev for their support.

Finally, I would like to thank my parents, sisters, brothers and friends.

Thank You All!

This thesis was submitted to the Senate of the 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 Binti Md Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati Binti Ahmad Zukarnain, PhD
Professor
Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia.
(Member)

Nur Izura Binti Udzir, PhD
Assistant Professor
Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia.
(Member)

Sherzod Rustamovic Turaev, PhD
Assistant Professor
Kulliyyah of Information of Communication Technology,
International Islamic University, 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 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: Ayman Majid Hamid, GS41612

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) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Dr. Sharifah Binti Md Yasin

Signature: _____
Name of Member of Supervisory Committee: Professor Dr. Zuriati Binti Ahmad Zukarnain

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Nur Izura Binti Udzir

Signature: _____
Name of Member of Supervisory Committee: Assistant Professor Dr. Sherzod Rustamovic Turaev

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

r_{pc}	Correlation Coefficients Between Ciphertext And Plaintext
3D-CA	Three Dimensional Cellular Automata
3DES	Triple DES
AD	Algebraic Degree
AES	Advanced Encryption Standard
CA	Cellular Automata
CBC	Chaining Block Code
CBCM	Chaining Block Code Mode
CCS	Cylindrical Coordinate System
CCSDPB	Cylindrical Coordinate System With Dynamic Permutation Box
CRTT	Csm Randomness Test Tool
CSET	Cryptographic Evaluation Tool Named As S-Box Evaluation Tool
DES	Data Encryption Standards
DFD	Data Flow Diagram
DK-3D-CA	Dynamic Key-Dependent Three Dimensional Cellular Automata
DU	Differential Uniformity
ECB	Electronic Codebook
FIPS 46	Federal Information Processing Standard 46
FPGA	Field Programmable Gate Arrays
GF	Galois Field
HDK	High Density Key
HDP	High Density Plaintext
LDB	Left-Down-Back
LDI	Left-Down-Infrontof Rule
LDK	Low Density Key
LDP	Low Density Plaintext
LFSR	Linear Feedback Shift Register

LUB	Left-Up-Back
LUI	Left-Up-Infrontof Rule
LUT	Look-Up-Table
NBS	National Bureau Of Standards
NIST	National Institute Of Standards And Technology
NL	Non-Linearity
NSA	National Security Agency
PCA	Programmable Cellular Automata
PCC	Plaintext Ciphertext Correlation
PRNG	Pseudorandom Number Generator
RCA	Reversable Cellular Automata
RCA^2	Second-Order Reversible One-Dimensional Cellular Automata
RDB	Right_Down-Back
RDI	Right-Down-Infrontof
RPRK	Random Plaintext Random Key
RUB	Right-Up-Back
RUI	Right-Up-Infrontof
SAC	Strict Avalanche Criteria
S-Box	Substitution Box
SET	S-Box Evaluation Tool
SKA	Strict Key Avalanche
SNR	Signal-To-Noise Ratio
SPA	Strict Plaintext Avalanche
SPN	Substitution Permutation Network
SubWord	Substitution Word
XOR	Exclusive-Or

CHAPTER 1

INTRODUCTION

The cipher is an algorithmic program that codes (or encrypts) plaintext into cipher-text through a process named coding (or encryption). Conversion of the ciphertext back to its initial form or plaintext is called decoding (or decryption). A block cipher is a deterministic algorithm operating on a group of fixed-length bits, called a block, with an unvarying transformation specified by a symmetric key. Block ciphers are fundamental components of many cryptographic protocols and are widely used to facilitate data encryption. There are many block cipher algorithms; the most famous algorithms are Data Encryption Standards (DES), Triple DES (3DES) and Advanced Encryption Standard (AES).

1.1 Overview

Recent advancement in wireless communication channels is gradually making the world a global village, where people from different parts of the globe can connect in an unprecedented manner. However, this also raises security concerns, as people must be confident that their information is kept intact and not eavesdropped. As such, they are in search of better means to enhance the security of their communications. For this reason, cryptologists are making efforts to devise stronger channel security measures that will ensure protected users' data. Cryptography protects information and communications whether it is video, voice or text. It additionally protects people's privacy, obscurity and lives (James Paul Schneider, 2015).

One of the preferred cryptographic algorithms is the symmetric block cipher algorithm. This is due to its simplicity, speed and power. It also has applications in cloud storage. A symmetric block cipher is used to encrypt and decrypt information (Kamara and Papamanthou, 2013). Joan Daemen and Vincent Rijmen developed the AES block cipher with a block size of 128 bits or 16 bytes. Keys for the cipher are available in one of every 3 lengths: 128, 192 or 256 bits, i.e., 16, 24 or 32 bytes (Daemen et al., 1999; Khamis and Subair, 2018). AES is currently used in many factories (Daemen et al., 1999) and social media to secure users' information.

1.2 Problem Statements

In a typical block cipher, a master key of special length is manipulated using a key expansion algorithm to create round subkeys. A strong key expansion ensures a cipher is more resistant to various forms of attacks, especially in related-key model attacks. Rijndael is the most common block cipher and it was adopted by the National Institute of Standards and Technology, USA in 2001 as an Advanced Encryption Standard (AES). However, cryptanalysis of this algorithm revealed its security weaknesses in relation to vulnerability to related-key differential attack as well as related-key

boomerang attack. These weaknesses are mainly caused by lack of nonlinearity in key expansion. Most algorithms have used a fixed key expansion algorithm for encryption and decryption (Juremi et al., 2012; Vaicekauskas et al., 2016; Kazlauskas and Kazlauskas, 2009; Nejad et al., 2014; Reshma and Veena, 2012). The fixed key expansion is vulnerable to square attack as mentioned in (Daemen et al., 1999; Tiessen et al., 2015). Square attack is the process of speculating and determining the subkey of a symmetric block cipher. When the round key expansion algorithms are relatively simple, they may be attacked easily. Square attacks are similar (Yan and Chen, 2016) with respect to how the attacks are made. Since all the stages of AES decryption are inferable, it can be attacked easily by using linear and differential attacks without a strong key.

Several algorithms have been proposed to modify the static nature of the substitution boxes (S-Boxes) used in AES (Ahmad, Khan, & Ansari, 2014; Alkhaldi, Hussain, & Gondal, 2015; Belazi, Rhouma, & Belghith, 2015; Chen, 2008; Hussain, Shah, Gondal, Khan, & Mahmood, 2013; Hussain, Shah, Gondal, & Wang, 2011; Jamal, Attaullah, Shah, AlKhaldi, & Tufail, 2019; Kazlauskas, Smaliukas, & Vaicekauskas, 2016; Lambić, 2017; L. Li, Liu, & Wang, 2016b; W. Li, Panda, & Yaseen, 2012; Mahmood et al., 2018; Mroczkowski, 2009; Zahid, Arshad, & Ahmad, 2019; Zaïbi, Peyrard, Kachouri, Fournier-Prunaret, & Samet, 2010). Although most of the researches get dynamic S-Boxes but their results still need to improve in term of nonlinearity, strict avalanche criterion and differential uniformity.

The diffusion parts in AES block cipher for each round are ShiftRows and MixColumns. According to (Krishnamurthy and Ramaswamy, 2011), an AES algorithm without of a ShiftRows stage would have slight changes in the values of each round. This indicates a poor encryption quality that makes the ciphertext vulnerable to attacks (Al-wattar et al., 2015). Also, making dynamic ShiftRow increase the diffusion of block cipher and the attacker wants more time to break it (Abdulah, Al-Rawi, & Hammod, 2018). When the plaintext is encrypted, the diffusion obscures the redundant arrangements. Therefore, those repeated configurations can be hidden in the cipher text in terms of complexity and security (A. Ali, Hu, Hinds, Graham, & Hsieh, 2018). To overcome this problem the bits will shuffle in each round (Yaghouti Niyat, Moattar, & Niazi Torshiz, 2017) by using cellular automata.

1.3 Research Objectives

The objective of this research is to design a new symmetric block cipher inspired by Von Neumann three dimensional cellular automata (3D-CA block cipher) algorithm with dynamic key-dependent components**.** In this regard, we have the following objectives:

1. To propose new key expansion algorithms, based on key dependent dynamic 3D-CA S-Boxes to strength the key by increase the nonlinearity of round subkeys.
2. To propose a new dynamic key-dependent 3D-CA-S-Boxes and test their characteristics (Nonlinearity, Avalanche Effects and Differential Uniformity) to get a strong S-Boxes.
3. To propose a dynamic key-dependent ShiftRow with 3D-CA permutation bits for KD-3D-CA block cipher to increase complexity and security for block cipher.

1.4 Scope of this Study

This research aims to design and develop a new model of 3D-CA block cipher with the following features:

1. A block and key size of 128-bits each.
2. Electronic Code Book (ECB) and Chaining Block Code (CBC) modes of operation.
3. 3D Von Neumann operation rules.
4. Basic security requirements certification.

The proposed dynamic block cipher is required to pass all the fifteen standard tests using the National Institute of Standards and Technology (NIST) statistical test suite, randomness tests, Avalanche effect and several S-Box test. It should also be resistant against linear and differential cryptanalysis.

1.5 Contribution of this Study

The main contribution of this study is to propose a KD-3D-CA block cipher algorithm. This involves the design of its components, elements, operations and techniques. Furthermore, the concepts to be used within the symmetric block cipher for key generation, encryption and decryption modules are indicated. The main elements of the KD-3D-CA block cipher should have the confusion and diffusion characteristics of cryptography.

To achieve this main contribution, the sub-contributions of this study are as follows:

1. This research proposes a dynamic key expansion using 3D von Neumann rules applied to S-Box to increase the nonlinearity at the first three rounds rather than AES that requires 10 rounds to become secure. This is motivated by the significant role played by proper key selection to generate the round key in the symmetric block cipher and the limitations of the algorithms that uses static S-Box.
2. This research combines static AES S-Box and 3D von Neumann rules to generate eight new key-dependent 3D-CA-S-Boxes to be used in each round of encryption and decryption. These S-Boxes must be as strong in nonlinearity, strict avalanche effects and differential uniformity to get strong S-Boxes.
3. This study increases the diffusion layer of the block cipher by implement key dependent dynamic ShiftRows for each rounds and to shuffle the STATE matrix using 3D-CA permutation for each round to increase the complexity and security of the block cipher to make it immune to attacks and difficult for cryptanalysis to break it.

In this study, the NIST suite test is used to test the quality of random numbers generated by the proposed cipher according to NIST standards. The cryptographic statistical tests for random number generators, such as S-Boxes test criteria, KD-3D-CA block cipher Avalanche effects, and cryptanalysis, are also evaluated and presented in this study.

1.6 Organization of the Thesis

This thesis consists of seven chapters organized as follows:

Chapter 1 presents the research problem, objectives, scope, and contributions.

Chapter 2 reviews related works on cryptography and symmetrical block cipher. This covers the essential concepts and properties related to the structure, security investigation, and previous related studies on block cipher. This chapter also introduces the KD-3D-CA model procedures and structures as well as the fundamental procedures of the CA framework required to build the new block cipher.

Chapter 3 outlines the research methodology used in this thesis. It also details the experimental design, data requirements and description for tests carried out.

Chapter 4 discusses the system design of the presented KD-3D-CA block cipher. This includes the procedure for generating the new eight S-Boxes from static S-Boxes based on 3D von Neumann rules. Also, details are given on the techniques of selecting the keys for each round. The descriptions of a new key expansion that depends on the master key, new dynamic shiftRow, and new byte substitution using the 3D von Neumann rules, and the KD-3D-CA block cipher algorithm for encoding and decoding are given.

Chapter 5 demonstrates the S-Box tests criteria for the new static and dynamic S-Boxes. The criteria include adjusted, fulfillment, torrential slide, Strict Avalanche Criteria (SAC), nonlinearity, bit freedom (BIT), differential uniformity (DU), invertibility, and contradiction. This chapter also examines the results of the tests and the irregularity of the KD-3D-CA block cipher. The investigations are directed by the NIST Test Suite for the randomness of data, involving little information at each cycle round of the functions.

Chapter 6 presents the implementation of the proposed key-dependent KD-3D-CA block cipher algorithm with some examples of how each phase works for each round.

Chapter 7 measures and examines the diffusion property of the KD-3D-CA block cipher. The complexity of the entire proposed block cipher and the cryptanalysis of the proposed S-Boxes are tested.

Chapter 8 concludes the research presented in this thesis. Some recommendations and future works are also presented.

1.7 Conclusion

This thesis proposes a block cipher with dynamic S-Boxes based on 3D cellular automata. The design accelerates a secure computation of digital data encryption and decryption using AES algorithm. In this chapter, the challenges of cryptography are discussed to provide a framework for the objectives of this research. This chapter also covers the background, research motivation, research objectives, significance and scope of this work as well as the thesis organization.

REFERENCES

Abdo, A. A., Lian, S., Ismail, I. A., Amin, M., & Diab, H. (2013). A cryptosystem based on elementary cellular automata. *Communications in Nonlinear Science and Numerical Simulation*, *18*(1), 136–147. https://doi.org/10.1016/j.cnsns.2012.05.023

Abdulah, H. S., Al-Rawi, M. A. H., & Hammod, D. N. (2018). Analysis of AES Algorithm Effects on the Diffusion Property. *Al-Mansour Journal*, *2018*(29), 23–39.

Abed, F., List, E., Lucks, S., & Wenzel, J. (2013). Differential and Linear Cryptanalysis of Reduced-Round Simon. In *Revision From October 9, 2013* (pp. 1–31).

Abhilasha, C. P., & Nataraj, K. R. (2016). Software Implementation of AES Encryption Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6*(5), 201–205.

Abuel-reesh, J. Y. (2018). An Intelligent Tutoring System for Learning Classical Cryptography Algorithms (CCAITS). *International Journal of Academic and Applied Research (IJAAR)*, *2*(2), 1–11.

Adams, C., & Tavares, S. (1990). The structured design of cryptographically good s-boxes. *Journal of Cryptology*, *3*(1), 27–41. https://doi.org/10.1007/BF00203967

Agarwal, P., Singh, A., & Kilicman, A. (2018). Development of key-dependent dynamic S-Boxes with dynamic irreducible polynomial and affine constant. *Advances in Mechanical Engineering*, *10*(7), 1–18. https://doi.org/10.1177/1687814018781638

Ahmad, M., Ahmad, F., Nasim, Z., Bano, Z., & Zafa, S. (2015). Designing Chaos Based Strong Substitution Box. In *2015 Eighth International Conference on Contemporary Computing (IC3)*.

Ahmad, M., Khan, P. M., & Ansari, M. Z. (2014). A Simple and Efficient Key-Dependent S-Box Design Using Fisher-Yates Shuffle Technique. *Communications in Computer and Information Science*, *420 CCIS*, 540–550. https://doi.org/10.1007/978-3-642-54525-2_48

Ahmed, F., & Elkamchouchi, D. (2013). Strongest AES with S-Boxes Bank and Dynamic Key MDS Matrix (SDK-AES). *International Journal of Computer and Communication Engineering*, *2*(4), 530–534. https://doi.org/10.7763/IJCCE.2013.V2.242

Al-wattar, A. H., Mahmod, R., & Zukarnain, Z. A. (2015). A NEW DNA BASED APPROACH OF GENERATING KEY- DEPENDENTMIXCOLUMNS TRANSFORMATION. *International Journal of Computer Networks & Communications (IJCNC)*, *7*(2), 93–102.

Al-wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, I. (2015). A NEW DNA BASED APPROACH OF GENERATING KEY-DEPENDENT SHIFTROWS TRANSFORMATION. *International Journal of Network Security & Its Applications*, *7*(9).

Al-Wattar, A. S., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). Generating A New S-Box Inspired by Biological DNA. *International Journal of Computer Science and Application*, *4*(November). https://doi.org/10.12783/ijcsa.2015.0401.04

ALabaichi, A., Mahmod, R., & Ahmad, F. (2017). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB and CBC Modes. *Nternational Journal of Digital Content Technology and Its Applications(JDCTA) Volume7*, *7*(September).

Alabaichi, A., & Salih, A. I. (2015a). Enhance security of advance encryption standard algorithm based on key-dependent S-box. *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, 44–53. https://doi.org/10.1109/ICDIPC.2015.7323004

Alabaichi, A., & Salih, A. I. (2015b). Enhance Security of Advance Encryption Standard Algorithm Based on Key-dependent S-Box. In *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015* (pp. 44–53).

Alabaichi, Ashwak Mahmood. (2015). A Dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish Algorithm. *Indian Journal of Science and Technology*, *8*(30), 1–17. https://doi.org/10.17485/ijst/2015/v8i30/86800

Alabaichi, Ashwaq Mahmood, Mahmod, R., Ahmad, F., & Mechee, M. S. (2013). Randomness analysis on Blowfish block cipher using ECB and CBC modes, (June). https://doi.org/10.3923/jas.2013.768.789

Alani, M. M. (2010). Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests. *IJCSNS International Journal of Computer Science and Network Security*, *10*(4), 53–57.

Ali, A., Hu, Y., Hinds, C., Graham, J., & Hsieh, C. G. (2018). Diffusion Metrics of the AES Symmetric Cryptosystem. *Foundations of Computer Science*, 36–39. Retrieved from https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/FCS3586.pdf

Ali, N. H. M., Rahma, A. M. S., Jaber, A. M., & Yousef, S. (2014). A Byte-Oriented Multi Keys Shift Rows Encryption and Decryption Cipher Processes in Modified AES. *International Journal of Scientific & Engineering Research*, *5*(4), 953–955.

Alizadeh, J., Bagheri, N., Gauravaram, P., & Kumar, A. (2013). Linear Cryptanalysis of Round Reduced SIMON. *IACR Cryptology EPrint Archive*, *2013*, 1–26.

Alkhaldi, A. H., Hussain, I., & Gondal, M. A. (2015). A novel design for the construction of safe S-boxes based on TD ERC sequence. *Alexandria Engineering Journal*, *54*(1), 65–69. https://doi.org/10.1016/j.aej.2015.01.003

Alvarez, G., Hernandez, L., & Martin, A. (2003). Sharing secret color images using cellular automata with memory. *Computing Research Repository (CoRR), Cryptography and Security.CR/0312034}*, (December 2013). Retrieved from http://arxiv.org/abs/cs/0312034

Amirthalingam, S., & Latha, K. (2016). A study on encryption using three-dimensional cellular automata. *ScienceAsia 42S*, 42–48.

Amrutha, & Prashanth, N. R. (2016). Enhanced Key Expansion Algorithm for Advanced Encryption Standard using Different S- Box Implementation on FPGA. *Global Research and Development Journal for Engineering |*, *1*(5), 112–117.

Antonio, R. B., Sison, A. M., & Medina, R. P. (2019). A modified generation of S-box for advanced encryption standards. *ACM International Conference Proceeding Series*, *Part F1483*, 280–283. https://doi.org/10.1145/3322645.3322672

Anuroop, K. B., & Neema, M. (2017). Fully pipelined-loop unrolled AES with enhanced key expansion. In *IEEE International Conference On Recent Trends In Electronics Information Communication Technology* (pp. 988–992). https://doi.org/10.1109/RTEICT.2016.7807977

Ariffin, S., Aini, N., Hisan, M., Arshad, S., Helmy, S., & Abu, S. (2016). Square and Boomerang Attacks Analysis of Diffusion Property of 3D-AES Block Cipher. In *International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)* (pp. 862–867).

Ariffin, S., Mahmod, R., Jaafar, A., & Rezal, M. (2012). An Immune System-Inspired Byte Permutation Function to Improve Confusion Performance of Round Transformation in Symmetric Encryption Scheme. *Computer Science and Its Applications. Lecture Notes in Electrical Engineering*, *203*, 339–351. https://doi.org/10.1007/978-94-007-5699-1

Arrag, S., Hamdoun, A., & Tragha, A. (2013). Replace AES Key Expansion Algorithm By Modified Genetic Algorithm. *Applied Mathematical Sciences*, *7*(144), 7161–7171.

Arrag, S., Hamdoun, A., Tragha, A., & Khamlich Salah, E. (2013). Implementation of stronger AES by using dynamic S-box dependent of master key. *Journal of Theoretical and Applied Information Technology*, *53*(2), 196–204.

Avanzi, R. (2017). The QARMA Block Cipher Family. *IACR Transactions on Symmetric Cryptology*, *0*(0), 1–40.

Azad, S., & Pathan, A. K. (2014). *PRACTICAL CRYPTOGRAPHY Algorithms and Implementations Using C++*.

Azura, N., Abdullah, N., Chew, L., Chew, N., & Zakaria, A. A. (2015). The Comparative Study of Randomness Analysis between Modified Version of LBlock Block Cipher and its Original Design. *International Journal of Computer and Information Technology*, *04*(06), 867–875.

Bakhshandeh, A., & Eslami, Z. (2013). An authenticated image encryption scheme based on chaotic maps and memory cellular automata. *Optics and Lasers in Engineering*, *51*(6), 665–673. https://doi.org/10.1016/j.optlaseng.2013.01.001

Bansod, G., Pisharoty, N., & Patil, A. (2017). PICO : An Ultra lightweight and Low power encryption design for pervasive computing. *Frontiers of Information Technology & Electronic Engineering*, *10*.

Barker, E., & Nicky, M. (2017). *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*.

Bassi, A. S., Zhu, J. X., Lan, Q., Margaritis, A., & Zheng, Y. (2006). METHOD AND SYSTEM FOR SECURING COMMUNICATION. https://doi.org/10.1038/incomms1464

Beaulieu, R., & Treatman-clark, S. (2013). The Simon and Speck Families of Lightweight Block Ciphers. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1–42).

Belazi, A., El-latif, A. A. A., Diaconu, A., & Rhouma, R. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, *88*, 37–50. https://doi.org/10.1016/j.optlaseng.2016.07.010

Belazi, A., Rhouma, R., & Belghith, S. (2015). A novel approach to construct S-box based on Rossler system. *IWCMC 2015 - 11th International Wireless Communications and Mobile Computing Conference*, 611–615. https://doi.org/10.1109/IWCMC.2015.7289153

Bhowmik, S. (2011). Image Cryptography : The Genetic Algorithm Approach. In *2011 IEEE International Conference on Computer Science and Automation Engineering* (pp. 223–227).

Biham, E. (2002). How to decrypt or even substitute DES-encrypted messages in 228 steps. *Information Processing Letters*, *84*(3), 117–124. https://doi.org/10.1016/S0020-0190(02)00269-7

Biham, E., & B, Y. C. (2014). An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X. In *International Conference on Selected Areas in Cryptography. Selected Areas in Cryptography -- SAC 2014* (pp. 59–76). https://doi.org/10.1007/978-3-319-13051-4

Biryukov, A., & Derbez, P. (2015). Differential Analysis and Meet-in-the-Middle Attack against Round-Reduced TWINE. *International Association for Cryptologic Research*, (February).

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A. (2010). Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6110 LNCS*, 299–319. https://doi.org/10.1007/978-3-642-13190-5_15

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. In *International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2011: Advances in Cryptology – ASIACRYPT 2011* (pp. 344–371).

Bogdanov, A., & Rechberger, C. (2011). A 3-Subset Meet-in-the-Middle Attack : Cryptanalysis of the Lightweight Block Cipher. In *International Workshop on Selected Areas in Cryptography SAC 2010: Selected Areas in Cryptography* (pp. 229–240).

Bogdanov, A., & Rijmen, V. (2014). Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. *Designs, Codes and Cryptography*, *70*(3), 369–383.

Bogdanov, A., & Wang, M. (2012). Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In *IInternational Workshop on Fast Software Encryption FSE 2012: Fast Software Encryption* (pp. 29–48).

Borghof, J., Canteaut, A., G¨uneysu, T., Kavun, E. B., Kne˘zevi´, M., Knudsen, L. R., … Yal¸cın, T. (2012). PRINCE – A Low-latency Block Cipher for Pervasive Computing Applications. *Advances in Cryptology – ASIACRYPT 2012*, *1*(10), 08–225.

Burak, D. (2015). Parallelization of a Block Cipher Based Description of the Block Cipher Based on Chaotic. In *International Conference on Artificial Intelligence and Soft Computing ICAISC 2015: Artificial Intelligence and Soft Computing* (pp. 191–201). https://doi.org/10.1007/978-3-319-19369-4

Canteaut, A., Fuhr, T., & Gilbert, H. (2014). Multiple differential cryptanalysis of round-reduced PRINCE (Full version). In *International Workshop on Fast Software Encryption FSE 2014: Fast Software Encryption* (pp. 591–610).

Chang, D., Ghosh, M., & Sanadhya, S. (2015). Biclique Cryptanalysis of full round AES-128 based hashing modes. In *International Conference on Information Security and Cryptology Inscrypt 2015: Information Security and Cryptology* (pp. 3–21).

Chen, G. (2008). A novel heuristic method for obtaining S-boxes. *Chaos, Solitons and Fractals*, *36*(4), 1028–1036. https://doi.org/10.1016/j.chaos.2006.08.003

Cheung, J. M. (2010). *THE DESIGN OF S-BOXES*.

Chyun, K. (2017). An In-Depth Mathematica Analysis of the Rjindael Cipher and the American Encryption Standard. *Analysis of Applied Mathmatics*, *8*(January), 41–56.

Courtois, N., Mourouzis, T., Song, G., Sepehrdad, P., & Susil, P. (2014). Combined Algebraic and Truncated Differential Cryptanalysis on Reduced-round Simon. In *11th International Conference on Security and Cryptography (SECRYPT), Vienna* (pp. 1–6).

Courtois, N. T., & Misztal, M. (2011). *Differential Cryptanalysis of GOST Introduction on GOST The Official Status of GOST*.

CSM. (2016). *CRYPTOLOGY 2016 : A BIG STEP TOWARDS ENHANCING AND* (Vol. 2007).

Daemen, J., & Rijmen, V. (1999). *AES Proposal : Rijndael*.

Daemen, J., & Rijmen, V. (2002). The Wide Trail Design Strategy. In *IMA International Conference on Cryptography and Coding Cryptography and Coding 2001: Cryptography and Coding* (pp. 222–238).

Davies, P. (2009). 3D Cellular Automata. *BPC Research Bulletin*, *1*(4), 4–10.

Dawood, Omar A., O. I. H. (2017). A Developed Realistic Urban Road Traffic in Erbil City Using Bi-directionally Coupled Simulations. *The 1st International Conference on Information Technology (ICoIT'17) Lebanese*, (September). https://doi.org/10.25212/ICoIT17.003

Dawood, Omar A., O. I. H. (2018). A Developed Realistic Urban Road Traffic in Erbil City Using Bi-directionally Coupled Simulations. In *The 1st International Conference on Information Technology (ICoIT'17) Lebanese* (pp. 28–35).

De Los Reyes, E. M., Sison, A. M., & Medina, R. P. (2019). Modified AES cipher round and key schedule. *Indonesian Journal of Electrical Engineering and Informatics*, *7*(1), 28–35. https://doi.org/10.11591/ijeei.v7i1.652

Deukjo Hong1(B), Jung-Keun Lee1, Dong-Chan Kim1, Daesung Kwon1, Kwon Ho Ryu1, and D.-G. L. (2014). LEA : A 128-Bit Block Cipher for Fast Encryption on Common Processors. *Information Security Applications*, *1*, 3–27. https://doi.org/10.1007/978-3-319-05149-9

Dey, D., Giri, D., Jana, B., Maitra, T., & Mohapatra, R. N. (2018). Linear-feedback shift register-based multi-ant cellular automation and chaotic map-based image encryption. *Security and Privacy*, (September), e52. https://doi.org/10.1002/spy2.52

Doganaksoy, A., Ege, B., Kocak, O., & Sulak, F. (2010). Cryptographic Randomness Testing of Block Ciphers and Hash Functions. *IACR Cryptology EPrint Archive*, 564.

Dunkelman, O., Keller, N., & Shamir, A. (2010). Improved Single-Key Attacks on 8-round AES-192 and AES-256. In *Advances in Cryptology - ASIACRYPT 2010* (pp. 1–29).

El-Ramly, S. H., El-Garf, T., & Soliman, A. H. (2001). Dynamic generation of s-boxes in block cipher systems. *National Radio Science Conference, NRSC, Proceedings*, *2*, 389–397. https://doi.org/10.1109/NRSC.2001.929396

El-sheikh, H. M., El-mohsen, O. A., Member, S., & Elgarf, T. (2012). A New Approach for Designing Key-Dependent S-Box Defined over GF (2 4) in AES. *International Journal of Computer Theory and Engineering*, *2*(May). https://doi.org/10.7763/IJCTE.2012.V4.442

Elkamchouchi, H. M., & Makar, M. A. (2004). Kamkar symmetric block cipher. *2lSt National Radio Science Conference (NRSC2004)*, 1–8.

Faraoun, K. M. (2014). Expert Systems with Applications A genetic strategy to design cellular automata based block ciphers. *EXPERT SYSTEMS WITH APPLICATIONS*, *41*(17), 7958–7967. https://doi.org/10.1016/j.eswa.2014.06.048

Fasihah, N., Esa, M., & Abdul-latip, S. F. (2018). Recent Advances on the Theory of S-box Design Strategies. *International Journal of Cryptology Research*, *26*, 1–26.

Forhad, M. S. A., Riaz, S., Hossain, M. S., & Das, M. (2018). An Improvement of Advanced Encryption Standard. *International Journal of Computer Science and Network Security (IJCSNS) (Thomson Reuters)*, *18*(11), 159–166.

Forouzan, B. A. (2007). *Cryptography and Network Security*.

G´erard, B., Grosso, V., Naya-Plasencia3, M., & Standaert, F.-X. (2012). Block Ciphers that are Easier to Mask : How Far Can we Go ? *Cryptographic Hardware and Embedded Systems, 2010*, 383–399.

Gandh, D. R., Kamalakannan, V., Balamurugan, R., & Tamilselvan, S. (2014). FPGA implementation of enhanced key expansion algorithm for Advanced Encryption Standard. In *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014* (pp. 409–413). IEEE. https://doi.org/10.1109/IC3I.2014.7019744

Gangadari, B. R., & Ahamed, S. R. (2016a). Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. *Healthcare Technology Letters*, *3*(3), 177–183. https://doi.org/10.1049/htl.2016.0033

Gangadari, B. R., & Ahamed, S. R. (2016b). Low Power S-Box Architecture for AES Algorithm using Programmable Second Order Reversible Cellular Automata: An Application to WBAN. *Journal of Medical Systems*, *40*(12). https://doi.org/10.1007/s10916-016-0622-2

Gangadari, B. R., & Ahamed, S. R. (2018). Programmable Cellular Automata-Based Low-Power Architecture to S-Box : An Application to WBAN. *Circuits, Systems, and Signal Processing*, *37*(3), 1116–1133. https://doi.org/10.1007/s00034-017-0592-8

Gangadari, B. R., Ahamed, S. R., Mahapatra, R., & Sinha, R. K. (2015). Design of cryptographically secure AES S-Box using cellular automata. *International Conference on Electrical, Electronics, Signals, Communication and Optimization, EESCO 2015*, 1–6. https://doi.org/10.1109/EESCO.2015.7253950

Gangadari, B. R., & Rafi Ahamed, S. (2016). Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. *Healthcare Technology Letters*, *3*(3), 177–183. https://doi.org/10.1049/htl.2016.0033

Ganguly, N., Sikdar, B. K., Deutsch, A., Canright, G., & Chaudhuri, P. P. (2003). A Survey on Cellular Automata. *Engineering*, 1–30. https://doi.org/http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.107.7729

Garg, S. (2017). Secure Message Transfer using Triple DES. *International Journal of Computer Applications (0975 – 8887)*, *165*(8), 1–4.

Georgescu, C., Nita, A., & Toma, A. (2017). A View On NIST Randomness Tests (In)Dependence. *Electronics, Computers and Artificial Intelligence*, *9*.

Gerberick, D. A. (1990). Cryptographic key management. *ACM SIGSAC Review*, *8*(2), 12–23. https://doi.org/10.1145/101126.101128

Gilbert, H., & Peyrin, T. (2010). Super-Sbox Cryptanalysis : Improved Attacks for AES-like permutations. *IACR Cryptology EPrint Archive*, *531*.

Gong, Z., Nikova, S., & Law, Y. W. (2012). KLEIN : A New Family of Lightweight Block Ciphers. *Springer-Verlag Berlin Heidelberg*, *7055*, 1–18.

Grocholewska-czurylo, A. (2011). Cryptographic properties of modified AES-like S-boxes. *Annales UMCS, Informatica*, *2*(2), 37–48. https://doi.org/10.2478/v10065-011-0009-4

Grocholewska-Czuryło, A. (2011). Cryptographic properties of modified AES-like S-boxes. *Annales UMCS, Informatica*, *11*(2), 37–48. https://doi.org/10.2478/v10065-011-0009-4

Guo, J., Peyrin, T., Poschmann, A., & Robshaw, M. (2011). The LED Block Cipher. *Springer-Verlag Berlin Heidelberg*, 326–341.

Gutowitz, H. (1996). *Cryptography with Dynamical Systems*.

Hameed, M. E., Ibrahim, M. M., & Manap, N. A. (2018). Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution , Differential Cryptanalysis and Level of Security. *Journal of Telecommunication, Electronic and Computer Engineering*, *10*(1), 139–145.

Hanis, S., & Amutha, R. (2018). Double image compression and encryption scheme using logistic mapped convolution and cellular automata. *Multimed Tools Appl*, *77*, 6897–6912. https://doi.org/10.1007/s11042-017-4606-0

Hassanain, K., Shaarawy, M., & Hesham, E. (2010). A Proposal for a Biometric Key Dependent. *Global Journal of Computer Science and Technology*, *10*(11), 42–47.

Hei, X., Song, B., & Ling, C. (2018). SHIPHER : A New Family of Light-weight Block Ciphers based on Dynamic Operators. In *EEE ICC,Paris* (pp. 1–7). https://doi.org/10.1109/ICC.2017.7996731

Heys, H. M. (2002). A Tutorial on Linear and Differential Cryptanalysis. *Cryptologia*, *26*(3), 189–221.

Hosseinkhani, R., & Javad, H. H. S. (2012). Using Cipher Key to Generate Dynamic S-Box in AES Cipher System. *International Journal of Computer Science and Security (IJCSS), Volume (*, (6), 19–28.

Hussain, I., Shah, T., Gondal, M. A., & Khan, W. A. (2011). Construction of Cryptographically Strong 8x8 S-boxes. *World Applied Sciences Journal*, *13*(11), 2389–2395.

Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, *23*(1), 97–104. https://doi.org/10.1007/s00521-012-0914-5

Hussain, I., Shah, T., Gondal, M. A., & Wang, Y. (2011). Analyses of SKIPJACK S-box. *World Applied Sciences Journal*, *13*(11), 2385–2388.

Hussien, Hassan Mansour, Muda, Z., & Yasin, S. M. (2017). Enhance The Robustness Of Secure Rijndael Key Expansion Function Based On Increment Confusion. In *6th International Conference on Computing & Informatics* (pp. 722–728).

Hussien, Hassan Mansur, Muda, Z., & Yasin, S. (2018). NEW KEY EXPANSION FUNCTION OF RIJNDAEL 128-BIT RESISTANCE TO THE RELATED-KEY ATTACKS. *Journal of Information and Communication Technology*, *3*(3), 409–434.

Iap, I., Akin, H., & Şah, F. (2010). Garden of eden configurations for 2-D cellular automata with rule 2460 N. *Information Sciences*, *180*(18), 3562–3571. https://doi.org/10.1016/j.ins.2010.05.039

Isa, H., Jamil, N., & Z'aba, M. R. (2016). Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance. *New Generation Computing*, *34*(3), 221–238. https://doi.org/10.1007/s00354-016-0302-2

Isa, H., Jamil, N., & Z, M. R. (2017). Hybrid Heuristic Methods in Constructing Cryptographically Strong S-boxes. *International Journal of Cryptology Research*, *6*(October 2016), 1–15.

Jaberi, A., Ayanzadeh, R., & Mousavi, A. S. Z. (2012). Two-layer Cellular Automata Based Cryptography. *Trends in Applied Sciences Research*, *7*(1), 68–77. https://doi.org/10.3923/tasr.2012.68.77

Jacob, G., Nadu, T., & Murugan, A. (2015). Towards the Generation of a Dynamic Key-Dependent S-Box to Enhance. *IACR Cryptology EPrint Archive*, (February), 1–5.

Jamal, S. S., Attaullah, Shah, T., AlKhaldi, A. H., & Tufail, M. N. (2019). Construction of new substitution boxes using linear fractional transformation and enhanced chaos. *Chinese Journal of Physics*, *60*(February), 564–572. https://doi.org/10.1016/j.cjph.2019.05.038

James Paul Schneider. (2015). USERNAMEBASED AUTHENTCATION AND KEY GENERATION. https://doi.org/10.1145/634067.634234.

Jamil, N., Mahmod, R., Z, M. R., Udzir, N. I., & Zukarnain, Z. A. (2013). Diffusion Analysis of Message Expansion in STITCH-256. *Journal of Information Security*, *4*(July), 129–137.

Jamil, N., Mahmood, R., Z, M. R., Udzir, N. I., & Zukarnaen, A. (2012). A New Cryptographic Hash Function Based on Cellular Automata. *International Conference on Information and Computer Networks*, *27*(Icicn), 163–169.

Jean, J., Nikolić, I., & Peyrin, T. (2014). Tweaks and Keys for Block Ciphers : the TWEAKEY Framework. In *International Conference on the Theory and Application of Cryptology and Information Security -Advances in Cryptology – ASIACRYPT 2014* (pp. 274–288).

Jin, J. (2012). An image encryption based on elementary cellular automata. *Optics and Lasers in Engineering*, *50*(12), 1836–1843. https://doi.org/10.1016/j.optlaseng.2012.06.002

Juremi, J., Mahmod, R., Sulaiman, S., & Ramli, J. (2012). Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key. *International Journal of Cyber-Security and Digital Forensics*, *1*(3), 183–188.

Juremi, J., Mahmod, R., Zukarnain, Z. A., & Yasin, S. M. (2017). Modified AES S-Box Based on Determinant Matrix Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(1), 584–587. https://doi.org/DOI: http://dx.doi.org/10.26483/ijarcs.v8i5.4021

Kadhim, A., & Ali, R. S. (2019). Enhancement AES based on 3D Chaos Theory and DNA Operations Addition. *Karbala International Journal of Modern Science*, *5*(2). https://doi.org/10.33640/2405-609x.1137

Kakkar, A., Singh, M. L., & Bansal, P. K. (2012). Mathematical analysis and simulation of multiple keys and S-Boxes in a multinode network for secure transmission. *International Journal of Computer Mathematics*, *89*(16), 2123–2142. https://doi.org/10.1080/00207160.2012.704022

Kamara, S., & Papamanthou, C. (2013). Parallel and Dynamic Searchable Symmetric Encryption. *Financial Cryptography and Data Security*, *7859*, 258–274. Retrieved from http://link.springer.com/10.1007/978-3-642-39884-1_22

Kamilya, S., & Das, S. (2019). A Study of Chaos in Non-uniform Cellular Automata. *Communications in Nonlinear Science and Numerical Simulation*, *76*, 116–131. https://doi.org/10.1016/j.cnsns.2019.04.020

Kavut, S., & Yücel, M. D. (2014). On Some Cryptographic Properties of Rijndael On Some Cryptographic Properties of Rijndael. *Information Assurance in Computer Networks*, (May). https://doi.org/10.1007/3-540-45116-1

Kazlauskas, K., & Kazlauskas, J. (2009). Key-dependent S-box generation in AES block cipher system. *Informatica*, *20*(1), 23–34. https://doi.org/10.15388/Informatica.2015.38

Kazlauskas, K., Smaliukas, R., & Vaicekauskas, G. (2016). A Novel Method to Design S-Boxes Based on Key- Dependent Permutation Schemes and its Quality Analysis. *IJACSA) International Journal of Advanced Computer Science and Applications*, *7*(4), 93–99. Retrieved from www.ijacsa.thesai.org

Keliher, L. (1997). *Substitution-Permutation Network Cryptosystems Using Key-Dependent S-Boxes*.

Khamis, A. D. (2019). Security Framework for Distributed Database System. *Journal of Data Analysis and Information Processing*, *07*(01), 1–13. https://doi.org/10.4236/jdaip.2019.71001

Khan, M., & Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. *Neural Computing and Applications*, *29*(4), 993–999. https://doi.org/10.1007/s00521-016-2511-5

Kim, S. H., & Han, G. T. (2016). Enhanced hybrid encryption method using the Half-Key exchange and the dynamic S-Box and Shift-Row in AES. *Information (Japan)*, *19*(2), 683–693.

Kolay, S., & Mukhopadhyay, D. (2014). Khudra : A New Lightweight Block Cipher for FPGAs. *Lecture Notes in Computer Science. Springer, Cham*, *8804*, 126–145. https://doi.org/10.1007/978-3-319-12060-7

Konstantynyuk, O., Tanasyuk, Y., & Ostapov, S. (2018). Deploying multydimensional cellular automata in the hash function construction. *14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 - Proceedings, 2018-April*, 158–163. https://doi.org/10.1109/TCSET.2018.8336177

Krishnamurthy, G. N., & Ramaswamy, V. (2008). Making AES Stronger : AES with Key Dependent S-Box. *IJCSNS International Journal of Computer Science and Network Security*, *8*(9), 388–398.

Krishnamurthy, G. N., & Ramaswamy, V. (2011). Study of Effect of Removal of Shiftrows and Mixcolumns Stages of AES and AES-KDS on their Encryption Quality and Hence Security. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *5*(2), 394–407.

Kumar, A., & Tewari, R. R. (2017). Expansion of Round Key Generations in Advanced Encryption Standard for Secure Communication. *International Journal of Computational Intelligence Research*, *13*(7), 1679–1698.

Kumar, J., Jeyaprakash, K., Sekar, J. G., & Villayutham, K. (2016). KAMAR : A Lightweight Feistel Block Cipher Using Cellular Automata. *Circuits and Systems*, *7*(April), 222–230.

Kumar, M., Pal, S. K., & Panigrahi, A. (2014). FeW : A Lightweight Block Cipher. *Cryptology EPrint*.

Lambi´, D. (2018). Security analysis of the pseudo-random bit generator based on multi-modal maps.

Lambić, D. (2017). A novel method of S-box design based on discrete chaotic map. *Nonlinear Dynamics*, *87*(4), 2407–2413. https://doi.org/10.1007/s11071-016-3199-x

Latha, K., & Amirthalingam, S. (2014). Application of Linear and Non Linear Modified 3D Cellular Automata Rules in Cryptography for Improved Security of Transmitted Data. *Applied Mechanics and Materials*, *573*, 600–604. https://doi.org/10.4028/www.scientific.net/AMM.573.600

Li, L., Liu, B., & Wang, H. (2016a). QTL : A new ultra-lightweight block cipher. *Microprocessors and Microsystems*, *45*, 45–55. https://doi.org/10.1016/j.micpro.2016.03.011

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

Li, W., Panda, B., & Yaseen, Q. (2012). Information Security and Privacy Research. *IFIP Advances in Information and Communication Technology*, *376*(September 2015), 211–222. https://doi.org/10.1007/978-3-642-30436-1

Li, X. W., Kim, S. T., & Wang, Q. H. (2017). Designing Three-Dimensional Cellular Automata Based Video Authentication with an Optical Integral Imaging Generated Memory-Distributed Watermark. *IEEE Journal on Selected Topics in Signal Processing*, *11*(7), 1200–1212. https://doi.org/10.1109/JSTSP.2017.2714838

Lian, S. (2009). Neurocomputing A block cipher based on chaotic neural networks. *Neurocomputing*, *72*, 1296–1301. https://doi.org/10.1016/j.neucom.2008.11.005

Lin, A., & Tong, Z. (2018). Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). *Journal of Physics*, *954*, 1–8.

Liu, N., Cai, J., Zeng, X., Lin, G., & Chen, J. (2017). Cryptographic Performance for Rijndael and RC6 Block Ciphers. In *Anti-counterfeiting, Security, and Identification (ASID)* (pp. 36–39).

Liu, Y., Wang, J., Fan, J., & Gong, L. (2016). Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. *Multimed Tools Appl*, *75*, 4363–4382. https://doi.org/10.1007/s11042-015-2479-7

M, Cimi Thomas, S. S. (2017). Secure Symmetric Encryption Scheme Using Genetic Algorithm. *International Journal of Applied Engineering Researc*, *12*(21), 10828–10833.

Mahmood, S., Farwa, S., Rafiq, M., Riaz, S. M. J., Shah, T., & Jamal, S. S. (2018). To Study the Effect of the Generating Polynomial on the Quality of Nonlinear Components in Block Ciphers. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/5823230

Mahmoud, E. M., Abd, A., Hafez, E., Elgarf, T. A., Mahmoud, E. M., Abd, A., … Talaat, A. (2013). Dynamic AES-128 with Key-Dependent S-box. *International Journal of Engineering Research and Applications (IJERA)*, 1662–1670.

Maiti, N. S., Ghosh, S., Shikdar, B. K., & Pal Chaudhuri, P. (2010). Programmable Cellular Automata (PCA) based Advanced Encryption Standard (AES) hardware architecture. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6350 LNCS*, 271–274. https://doi.org/10.1007/978-3-642-15979-4_29

Mara, U. T. (2017). RANDOMNESS ANALYSIS ON 3D-AES BLOCK. *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, 331–335.

Maram, B. (2016). Light Weight Cryptographic Algorithm To Improve Avalanche Effect For Data Light Weight Cryptographic Algorithm To Improve Avalanche Effect For Data Security Using Prime Numbers And Bit Level Operations. *International Journal of Applied Engineering Research*, (November 2015).

Marshall, R. G., & Plymouth, N. (2017). KAFKA: A CELLULAR AUTOMATION / COMPLEX FIBONACCI SEQUENCES-BASED TECHNIQUE FOR ENCRYPTING AND DECRYPTING AUDIO, VIDEO AND TEXT MESSAGE.

Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology EUROCRYPT'93*, *765*, 386–397. https://doi.org/10.1007/3-540-48285-7

Mejia, M., & Murguia, J. S. (2012). Numerical implementation of a real-time encryption system. *Procedia Engineering*, *35*, 182 – 191. https://doi.org/10.1016/j.proeng.2012.04.179

Mennink, B. (2016). XPX : Generalized Tweakable Even-Mansour with Improved Security Guarantees. *36th Annual International Cryptology Conference on Advances in Cryptology --- CRYPTO*, *1*(1), 64–94.

Merkle, R. C. (1991). Fast Software Encryption Functions. *Advances in Cryptology - CRYPT0, 90*, 476–501.

Mewada, S. (2016). Classification of Efficient Symmetric Key Cryptography Algorithms. *International Journal of Computer Science and Information Security*, *14*(2), 105–110.

Mister, S., & Adams, C. (1996). Practical S-box design. *Workshop on Selected Areas in Cryptography, SAC*, 1–17. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.40.7715&rep=rep1&type=pdf

Mohamed, K., Hani, F., Mohd, H., Ariffin, S., Zakaria, N. H., Nazran, M., & Pauzi, M. (2018). An Improved AES S-box Based on Fibonacci Numbers and Prime Factor. *International Journal of Network Security*, *20*(1), 1–9. https://doi.org/10.6633/IJNS.201803.20(x).xx

Mohammad, F. Y., Rohiem, A. E., & Elbayoumy, A. D. (2015). A Novel S-box of AES Algorithm Using Variable Mapping Technique. *AEROSPACE SCIENCES & AVIATION TECHNOLOGY*, *13*, 1–9.

Mohammed, E., Zekry, A., Hafez, A. A. El, & Elgarf, T. A. (2014). Enhancing Channel Coding using AES Block Cipher Enhancing Channel Coding using AES Block Cipher. *International Journal of Computer Applications*, (January 2014), 28–33. https://doi.org/10.5120/9933-4568

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

Moharir, M. (2010). Analysis of Advanced Encryption Standards. *INTERNATIONAL JOURNAL ON COMPUTING*, *1*(1), 145–149.

Mohini. (2017). Data Security Using 2D Cellular. *International Journal of Students' Research in Technology & Management*, *5*(1), 8–11.

Mourouzis, T., Song, G., Courtois, N., & Christofi, M. (2014). Advanced Differential Cryptanalysis of Reduced-Round SIMON 64/128 Using Large-Round Statistical Distinguishers. *IACR Cryptology EPrint Archive 2015*, (July 2013).

Mroczkowski, P. (2009). Generating Pseudorandom S-Boxes – a Method of Improving the Security of Cryptosystems Based on Block Ciphers. *Journal of Telecommunications and Information Technology*, *2*, 74–79. Retrieved from https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BAT8-0016-0023

Muda, Z., SULAIMAN, S., YASIN, S. M., & MAHMOD, R. (2015). TSHIFTCOLUMN : A NEW TRANSFORMATION IN 128-BIT RIJNDAEL KEY EXPANSION TO IMPROVE SECURITY. *Journal of Theoretical and Applied Information Technology*, *73*(1), 130–136.

Murphy, S., & Robshaw, M. J. B. (2002). Essential Algebraic Structure Within the AES. *Crypto 2002*, *2442*, 1–16. https://doi.org/10.1007/3-540-45708-9_1

Nag, S., Bhuvaneswari, & Nuthan. (2013). IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD-192 BIT USING MULTIPLE KEYS. In *Challenges in Research & Technology*.

Nagara, S., Bhamidipati, K., & Ramachandra, M. (2010). Formal Method of Encryption Using 9 ' S Complement. *International Journal of Computer Applications*, *8*(5), 23–25.

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. *Springer International Publishing Switzerland 2015*, *10*(1007), 167–182. https://doi.org/10.1007/978-3-319-26059-4

Nandi, S., Kar, B. K., & Chaudhuri, P. P. (1994). Theory and Applications of Cellular Automata in Cryptography. *IEEE Transactions on Computers*, *43*(12), 1346–1357. https://doi.org/10.1109/12.338094

Oliynykov, R., Gorbenko, I., Kazymyrov, O., Ruzhentsev, V., Kuznetsov, O., Gorbenko, Y., … Pushkaryov, A. (2015). A New Encryption Standard of Ukraine : The Kalyna Block Cipher. *IACR Cryptology EPrint Archive 2015*, 1–113.

Özkaynak, F., Çelik, V., & Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing*, *11*(4), 659–664. https://doi.org/10.1007/s11760-016-1007-1

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. https://doi.org/10.1007/978-3-642-04101-3

Panda, S. P., Sahu, M., Rout, U. P., & Nanda, S. K. (2011). Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography. *International Journal of Communication Network & Security*, *1*(1), 18–23. Retrieved from http://www.idc-online.com/technical_references/pdfs/data_communications/Encryption and Decryption.pdf

Pandya, D., Narayan, K. R., & Thakkar, S. (2015). Brief History of Encryption. *International Journal of Computer Applications*, *131*(9), 28–31.

Partheeban, P., & Kavitha, V. (2018). Dynamic key dependent AES S-box generation with optimized quality analysis. *Cluster Computing*, *6*, 1–11. https://doi.org/10.1007/s10586-018-2386-6

Peñate, A. A., & Arrozarena, P. F. (2018). How secure is the Advanced Encryption Standard with random ShiftRows against Fault Analysis. *Journal of Science and Technology on Information Security*, *1*(07), 14–21.

Picek, S. (2016). Evolving Algebraic Constructions for Designing Bent Boolean Functions. In *proceedings of the Genetic and Evolutionary Computation Conference* (pp. 781–788).

Picek, S., Batina, L., Jakobović, D., Ege, B., Golub, M., Picek, S., … Match, A. (2016a). S-box, SET, Match: A Toolbox for S-box Analysis. *Reative Commons Attribution*, *4*, 0–10.

Picek, S., Batina, L., Jakobović, D., Ege, B., Golub, M., Picek, S., … Match, A. (2016b). S-box, SET, Match: A Toolbox for S-box Analysis. *Creative Commons Attribution*, *4*, 0–10.

Picek, S., Miller, J. F., & Jakobovic, D. (2015). Cartesian Genetic Programming Approach for Generating Substitution Boxes of Different Sizes. In *GECCO 2015* (pp. 1457–1458).

Porzio, A. (2017). Quantum Cryptography : Approaching Communication Security from a Quantum Perspective. *IEEE Security & Privacy*, *15*(4), 51–57.

Praveen, A., Singh, A., & Kilicman, A. (2018). Development of key-dependent dynamic S-Boxes with dynamic irreducible polynomial and affine constant. *Advances in Mechanical Engineering*, *10*(7), 1–18. https://doi.org/10.1177/1687814018781638

Rani, S., & Kaur, H. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms. *Nternational Journal of Advanced Research in Computer Science*, *8*(4).

Rao, S. K., Mahto, D., & Khan, D. A. (2017a). A Survey on Advanced Encryption Standard. *International Journal of Science and Research (IJSR)*, *6*(391), 711–724. https://doi.org/10.21275/ART20164149

Rao, S. K., Mahto, D., & Khan, D. A. (2017b). A Survey on Advanced Encryption Standard. *Nternational Journal of Science and Research (IJSR)*, *6*(391), 711–724. https://doi.org/10.21275/ART20164149

Raphaël Bost, P.-A. F. (2016). Verifiable Dynamic Symmetric Searchable Encryption Optimality and Forward Security. *IACR Cryptology EPrint Archive*, 1–40.

Raza, S. F., & Satpute, V. R. (2018). Practo: Pseudo random bit generator for cryptographic application. *KSII Transactions on Internet and Information Systems*, *12*(12), 6161–6176. https://doi.org/10.3837/tiis.2018.12.029

Rivain, M. (2013). Another Nail in the Coffin of White-Box AES Implementations.

Riyaldhi, R., Rojali, & Kurniawan, A. (2017). Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix Column. *Procedia Computer Science*, *116*, 401–407. https://doi.org/10.1016/j.procs.2017.10.079

Ronald L. Rivest , M.J.B. Robshaw , R. Sidney, and Y. L. Y. 1. (1998). The RC6 Block Cipher. In *conference proceedng v1.1- August* (pp. 1–21).

Rosal, E. Del, & Kumar, S. (2017). A Fast FPGA Implementation for Triple DES Encryption Scheme. *Circuits and System*, *8*, 237–246. https://doi.org/10.4236/cs.2017.89016

Roy, S., Karjee, J., Rawat, U. S., Dayama Pratik, N., & Dey, N. (2016). Symmetric Key Encryption Technique: A Cellular Automata based Approach in Wireless Sensor Networks. *Physics Procedia*, *78*, 408–414. https://doi.org/10.1016/j.procs.2016.02.082

Rozier, O., & Narteau, C. (2013). A real-space cellular automaton laboratory. In *EARTH SURFACE PROCESSES AND LANDFORMS Earth Surf. Process. Landforms*. https://doi.org/10.1002/esp.3479

Rukhin, A., Soto, J., & Nechvatal, J. (2010). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*.

Rumao, M., Kaul, V., Shah, D., & Prof, A. (2017). Performance Analysis of Application for Security Enhancements using Cryptanalysis. *International Research Journal of Engineering and Technology(IRJET)*, *4*(9), 1251–1256. Retrieved from https://irjet.net/archives/V4/i9/IRJET-V4I9237.pdf

S´YS, M., Riha, Z., Matyas, V., Marton, K., & Suciu, A. (2015). On the Interpretation of Results from the NIST Statistical Test Suite. *Romanian Journal of Information Science and Technology*, *18*(1), 18–32.

Saberi, I., Shojaie, B., & Salleh, M. (2011). Enhanced Key Expansion for AES-256 by using Even-Odd method. *2011 International Conference on Research and Innovation in Information Systems, ICRIIS'11*, 1–5. https://doi.org/10.1109/ICRIIS.2011.6125708

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

Sadiq, A. T., & Faisal, F. H. (2015). Modification AES algorithm based on Extended Key and Plain Text. *Journal of Advanced Computer Science and Technology Research*, *5*(4), 104–112.

Saha, R., Geetha, G., Kumar, G., & Kim, T. H. (2018). RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys. *Security and Communication Networks*, *2018*, 11. https://doi.org/10.1155/2018/9802475

Sahoo, S., Choudhury, P. P., & Pal, A. (2002). Solutions on 1D and 2D Density Classification Problem Using Programmable Cellular Automata. *Journal of Cellular Automata*, *9*(1).

Sajadieh, M., Mirzaei, A., Mala, H., & Rijmen, V. (2017). A new counting method to bound the number of active S-boxes in Rijndael and 3D. *Designs, Codes and Cryptography*, *83*(2), 327–343. https://doi.org/10.1007/s10623-016-0217-4

Sajjad, A., Jamal, S., & Shah, T. (2018). A Novel Algebraic Technique for the Construction of Strong Substitution Box. *Wireless Personal Communications*, *99*(1), 213–226. https://doi.org/10.1007/s11277-017-5054-x

Saravanan, T., & Kumar, S. V. (2018). A Review Paper on Cryptography-Science of Secure Communication. *International Journal of Computer Science Trends and Technology (IJCST)*, *6*(4), 131–134.

Sarkar, P. (2000). A brief history of cellular automata. *ACM Computing Surveys*, *32*(1), 80–107. https://doi.org/10.1145/349194.349202

Schneier, B, & Whiting, D. (2000). A Performance Comparison of the Five AES Finalists. *Proc 3rd Advanced Encryption Standard AES Candidate Conf*, *3*, 123–135. https://doi.org/http://dx.doi.org/10.1111/j.1365-3156.2011.02994_3.x

Schneier, Bruce. (1993). Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). In *Fast Software Encryption* (pp. 191–204).

Schneier, Bruce, Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). Twofish : A 128-Bit Block Cipher, 1–68.

Scripcariu, L., & Frunză, M. D. (2012). Modified Advanced Encryption Standard. In *11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania* (Vol. 3, pp. 23–26).

Seredynski, M., & Bouvry, P. (2004). Block Encryption Using Reversible Cellular Automata. *ACRI*, *3305*(January 2015). https://doi.org/10.1007/978-3-540-30479-1

Shehab, E. (2014). An Image Encryption Technique based on DNA Encoding and Round-reduced AES Block Cipher. *International Journal OfComputer Applications (0975 8887)*, *107*(20), 1–7.

Shibutani, K., Isobe, T., Hiwatari, H., & Mitsuda, A. (2011). Piccolo : An Ultra-Lightweight Blockcipher. *Cryptographic Hardware and Embedded Systems – CHES 2011*, 342–357.

Shivkumar, S. (2011). Performance Comparison of Advanced Encryption Standard (AES) and AES key dependent S-box - Simulation using MATLAB. *IEEE Security and Privacy*, 1–6.

Shtewi, A. A., Hasan, B. E. M., El, A., & Hegazy, F. A. (2010). An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. *International Journal of Computer Science and Network Security*, *10*(2), 226–232.

Siddiqui, N., & Afsar, U. (2016). A Novel Construction of S16 AES S-boxes. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(8), 810–818.

Singh, A., Agarwal, P., & Chand, M. (2017). Analysis of Development of Dynamic S-Box Generation. *Computer Science and Information Technology*, *5*(5), 154–163. https://doi.org/10.13189/csit.2017.050502

Singh, P. (2015). Cryptography : An Art of Data Hiding Cryptography : An Art of Data Hiding. *International Journal of Computer and Communication System Engineering (IJCCSE)*, *1*(2), 117–120.

Sisalem, D., Floroiu, J., Kuthan, J., Abend, U., & Schulzrinne, H. (2009). *SIP Security*.

Somanath, T., & Nandi, S. (2009). LCASE : Lightweight Cellular Automata-based Symmetric-key Encryption. *International Journal of Network Security*, *8*(January), 243–252.

Soto, J. (1999). *Randomness Testing of the AES Candidate Algorithms*.

Soto, J., & Bassham, L. (2000). *Randomness Testing of the Advanced Encryption Standard Finalist Candidates*.

Srinath, N., Rohith, S., & Kolli, C. (2017). Implementation of AES Using Reversible Cellularautomata Based S-Box on FPGA. *International Journal of Scientific Engineering and Research (IJSER)*, *5*(5), 2015–2017.

Stallings, W. (2005). *Cryptography and Network Security: Principles and Practices*. *Cryptography and Network Security*. https://doi.org/10.1007/11935070

Stallings, W. (2010). *N ETWORK S ECURITY E SSENTIALS : A PPLICATIONS AND S TANDARDS*.

Stoianov, I., & Zorzi, M. (2012). Emergence of a 'visual number sense' in hierarchical generative models. *NATURE NEUROSCIENCE*, *15*(2). https://doi.org/10.1038/nn.2996

Støvneng, O. M. T. (2014). *2D and 3D On-Chip Development of Cellular Automata Machines*.

Suciu, A., Toma, R. A., & Márton, K. (2014). Parallel Object-Oriented Implementation of the TestU01 Statistical Test Suites. In *Parallel Object-Oriented Implementation of the TestU01 Statistical Test Suites* (pp. 311–315).

Sulaiman, S. (2012). A New ShiftColumn Transformation : An Enhancement of Rijndael Key Scheduling. *International Journal of Cyber-Security and Digital Forensics*, *1*(3), 160–166.

Sulak, F., Doğanaksoy, A., Ege, B., & Koçak, O. (2010). Evaluation of Randomness Test Results for Short Sequences. *Springer-Verlag Berlin Heidelberg 2010*, 309–319.

SULAK, F., UĞUZ, M., KOÇAK, O., & DOĞANAKSOY, A. (2017). On the independence of statistical randomness tests included in the NIST test suite. *Turkish Journal of Electrical Engineering & Computer Sciences*, *25*, 3673–3683. https://doi.org/10.3906/elk-1605-212

Sumathy, V., & Navaneethan, C. (2012). Enhanced Aes Algorithm for Strong Encryption. *International Journal of Advances in Engineering & Technology*, *4*(2), 547–553.

Suri, P. R., & Deora, S. S. (2011). 3D Array Block Rotation Cipher : An Improvement using shift. *Global Journal of Computer Science and Technology*, *11*(19).

Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, E. (2012). TWINE : A Lightweight , Versatile Block Cipher. *ECRYPT Workshop on Lightweight Cryptography*, *1*(1), 1–24.

Szaban, M., & Seredynski, F. (2012). Dynamic Cellular Automata-Based S-Boxes. *Computer Aided Systems Theory - Eurocast 2011, Pt I*, *6927*, 184–191.

Tanasyuk, Y., & Ostapov, S. (2018). DEVELOPMENT AND RESEARCH OF CRYPTOGRAPHIC HASH FUNCTIONS BASED ON TWO-DIMENSIONAL CELLULAR AUTOMATA. *Journal of Computing and Information Technology*, *23*(4), 24–27. https://doi.org/10.5604/01.3001.0010.8638

Tavares, A. F. W. and S. E. (1986). ON THE DESIGN OF S-BOXES. *Advances in Cryptology - CRYPT0, 10870*(4), 1049–1050.

Tay, J. J., Wong, M. M., & Hijazin, I. (2014). Compact and low power AES block cipher using lightweight key expansion mechanism and optimal number of S-Boxes. *IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, *1*(4), 108–114. https://doi.org/10.1109/ISPACS.2014.7024435

Tech, J. N. R., Chandrapal, A., & Tech, S. M. (2012). A Novel Encryption System using Layered Cellular Automata. *World Congress on Engineering 2011*, *1*(6), 912–917.

Telagarapu, P., Biswal, B., & Guntuku, V. S. (2011). Design and analysis of multimedia communication system. In *3rd International Conference on Advanced Computing, ICoAC 2011* (pp. 193–197). IEEE. https://doi.org/10.1109/ICoAC.2011.6165174

Tripathy, S., & Nandi, S. (2009). LCASE: Lightweight cellular automata-based symmetric-key encryption. *International Journal of Network Security*, *8*(3), 243–252.

Vasantha, S., Shivakumar, N., & Rao, D. S. (2015). A New Encryption and Decryption Algorithm for Block Cipher Using Cellular Automata Rules. *International Journal of Emerging Engineering Research and Technology*, *3*(8), 130–136.

Verma, A. (2017). DESIGN AND DEVELOPMENT OF ROBUST ALGORITHM FOR CRYPTOGRAPHY. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(March).

Wadi, S. M., & Zainal, N. (2013). A low cost implementation of modified advanced encryption standard algorithm using 8085A microprocessor. *Journal of Engineering Science and Technology*, *8*(4), 406–415.

Wang, Yanfeng, Wu, W., Guo, Z., & Yu, X. (2014a). Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro. *Springer International Publishing Switzerland 2014*.

Wang, Yanfeng, Wu, W., Guo, Z., & Yu, X. (2014b). Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro. *Springer International Publishing Switzerland 2014*, 308–323.

Wang, Yong, Wong, K., Liao, X., & Xiang, T. (2009). A block cipher with dynamic S-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation*, *14*(7), 3089–3099. https://doi.org/10.1016/j.cnsns.2008.12.005

Wang, Yong, Zhao, Y., Zhou, Q., & Lin, Z. (2018). Image encryption using partitioned cellular automata. *Neurocomputing*, *275*, 1318–1332. https://doi.org/10.1016/j.neucom.2017.09.068

Wolfram, S. (2013). One-Dimensional Cellular Automata. In *cellular automata prenciples* (pp. 35–78).

Wu, W., & Zhang, L. (2011). LBlock : A Lightweight Block Cipher. *Springer-Verlag Berlin Heidelberg*, 327–344.

Yaghouti Niyat, A., Moattar, M. H., & Niazi Torshiz, M. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics and Lasers in Engineering*, *90*(November 2016), 225–237. https://doi.org/10.1016/j.optlaseng.2016.10.019

Yan, J., & Chen, F. (2016a). An Improved AES Key Expansion Algorithm. *International Conference on Electrical, Mechanical and Industrial Engineering*, (Icemie), 113–116.

Yan, J., & Chen, F. (2016b). An Improved AES Key Expansion Algorithm. In *International Conference on Electrical, Mechanical and Industrial Engineering* (pp. 113–116).

Ye liu, Wei Gong, W. F. (2018). Application of AES and RSA Hybried Algorithm in E-mail. *IEEE, ICIS 2018, June 6-8, 2018, Singapore, 978-1-5386-5892-5/18/ ©2018*, 701–703.

Yuan, Y., Xu, Z., & Liu, Q. (2015). High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion. *IET Computers & Digital Techniques*, *9*(3), 175–184. https://doi.org/10.1049/iet-cdt.2014.0101

Zahid, A. H., Arshad, M. J., & Ahmad, M. (2019). A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy*, *21*(3), 1–13. https://doi.org/10.3390/e21030245

Zaïbi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., & Samet, M. (2010). A new design of dynamic S-Box based on two chaotic maps. *2010 ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2010*, (3). https://doi.org/10.1109/AICCSA.2010.5586946

Zaïbi, G., Peyrard, F., Kachouri, A., & Samet, M. (2010). A new design of dynamic S - Box based on two chaotic maps . *Computer Systems and Applications*, *10*(1109).

Zhang, R., & Chen, L. (2008). A Block Cipher Using Key-Dependent S-box and P-box. *EEE International Symposium on Industrial Electronics*, 1463–1468.

Zhang, Wentao, Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2015). RECTANGLE : A Bit-slice Lightweight Block Cipher Suitable for Multiple Platforms. *SCIENCE CHINA Information Sciences*, *58*(15). https://doi.org/10.1007/s11432-015-5459-7

Zhang, Wenying, & Han, G. (2018). Construction of rotation symmetric bent functions with maximum algebraic degree. *SCIENCE CHINA Information Sciences*, *61*(March), 3–5. https://doi.org/10.1007/s11432-017-9123-2

Zhang, X., Lu, R., Zhang, H., & Xu, C. (2014). A New Public Key Encryption Scheme based on Layered Cellular Automata. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, *8*(10), 3572–3590.

Zhang, X., Zhang, H., & Xu, C. (2016). Reverse Iterative Image Encryption Scheme Using 8-layer Cellular Automata. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, *10*(7), 3397–3413.

Zhang, Y. (2018). Test and Verification of AES Used for Image Encryption. *3D Research*, *9*(1). https://doi.org/10.1007/s13319-017-0154-7

Zhihua, H. U., & Kuanjiang, X. (2016). A Novel Key Scheduling Scheme for AES Algorithm. *Journal of Natural Sciences*, *21*(2), 110–114. https://doi.org/10.1007/s11859-016-1145-x