
**UNIVERSITI PUTRA MALAYSIA**

***DEVELOPMENT OF DNA-BASED DYNAMIC KEY-DEPENDENT BLOCK CIPHER***

**AUDAY H. SAEED**

**FSKTM 2015 16**

# DEVELOPMENT OF DNA-BASED DYNAMIC KEY-DEPENDENT BLOCK CIPHER

By

AUDAY H. SAEED

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

October 2015

**DEDICATION**

*To my father, mother, my beloved wife, my daughters, Mayar, Fatemah, and Ethar, and my lovely son, Yaman.*

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

**DEVELOPMENT OF DNA-BASED DYNAMIC KEY-DEPENDENT BLOCK CIPHER**

By

**AUDAY H. SAEED**

**October 2015**

**Chair : Professor Ramlan Mahmod, PhD**
**Faculty : Computer Science and Information technology**

The need for an extremely effective means of achieving information security is constantly necessary and indispensable. The cryptographic algorithm is one of the strongest tools for providing appropriate security for systems and data transmissions. The symmetric block cipher is one of the most significant cryptographic algorithms. It is essential for institutions to build their own symmetric block cipher to address the newly emerging threats that are the result of new technologies. Hence, it is necessary to research and develop a secure symmetric cipher algorithm. Since the declaration of Rijndael as AES this cipher has been the target of many attacks, and the attempts to break it are ongoing and even increasing everyday by taking advantage of the rapid development in computing capabilities. The rise in the frequency of attacks against the AES has not been matched by the level of development in the capabilities of the algorithm to withstand these challenges and make the AES secure and immune to all risks. The byte substitution and permutation units in AES block cipher which produce diffusion and confusion have fixed structure for all rounds.

This thesis proposes a new secure symmetric block cipher called DNA-Based Block Cipher (DNAB), with key-dependent components inspired by DNA biology techniques. The thesis identifies the similarity elements, and highlights the essential computation elements, namely the DNA-strands, DNA-bases, Central dogma process that can be applied in symmetric block cipher that fulfills Shannon's confusion and diffusion properties.

The DNAB utilizes the DNA-based key-dependent components to enhance the security of cipher, and reduce the number of cipher-iterated rounds. Accordingly, for the substitution layer, the reality that the S-Boxes are unknown is one of the major strengths of the new cipher as the cryptanalysis requires known S-Boxes. For the permutation layer the use of key-dependent transformations and processes inspired by DNA techniques forces the attackers to try and devise hard new frameworks of cryptanalytic mechanisms.

The experimental findings presented the randomness of the output in the DNAB cipher, as secure cipher, and compared to AES, the number of iteration rounds is

reduced. The S-Box tests criteria presenting the new S-Boxes in DNAB cipher satisfy the balance, completeness, avalanche, strict avalanche, bit-independence, nonlinearity, differential-uniformity, invertability and non-contradiction criteria as good S-Box conditions.

The avalanche effect, correlation coefficient, bit error and key sensitivity of the DNAB cipher were laboratory tested, and they satisfied the confusion and diffusion properties. In spite of the fact that the S-Boxes of DNAB cipher have 8 bits for input and output, the output has the possibility of one of the $2^{n!}$, compared to $2^8$ possibilities for the static S-Box; also for each round, key-dependent and MixColumns transformations has $(2^8.2^{4!})$ possibilities each. This makes the cryptanalysis of these transformations difficult since it needs cryptanalysts to construct all the possibilities. It was confirmed that the DNAB cipher had successfully passed very demanding security analyses and justified that the DNAB cipher is a secure block-cipher. Accordingly, it will increase the protection of institutional information systems; also it will be considered as one of a symmetric block ciphers in information security research, and open the doors to matchmaking between computer security and biological systems research.

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

**PEMBANGUNAN SIFER BLOK DINAMIK BERASASKAN DNA BERSANDARKAN KUNCI**

Oleh

**AUDAY H. SAEED**

**Oktober 2015**

**Pengerusi : Professor Ramlan Mahmod, PhD**
**Fakulti : Sains Komputer dan Teknologi Maklumat**

Keselamatan maklumat sentiasa menjadi satu bidang yang sangat dititik beratkan dan keperluan untuk alat yang sangat efektif bagi mencapai keselamatan maklumat adalah penting dan sangat berharga. Dalam domain pengkomputeran, algoritma kriptografi adalah salah satu peralatan yang terkuat bagi menjamin keselamatan yang sesuai bagi sistem dan transmisi data. Sifer blok simetri adalah salah satu algoritma kriptografi yang paling signifikan. Bagi institusi, adalah penting untuk mereka membangunkan sifer blok simetri mereka sendiri bagi keperluan ancaman baharu kesan daripada teknologi baharu. Oleh yang sedemikian, adalah amat penting untuk mengkaji dan membangunkan satu algoritma sifer blok simetri yang selamat. Sejak masa pengisytiharan Rijndael sebagai AES, sifer ini telah menjadi sasaran banyak serangan dan kripanalisis, serta cubaan untuk memecahkannya masih berterusan, malah semakin meningkat setiap hari dengan memanfaatkan perkembangan pesat dalam keupayaan pengkomputeran. Peningkatan kekerapan serangan ke atas algoritma AES tidak dapat dipadani oleh tahap pembangunan dalam keupayaan algoritma untuk menahan cabaran ini dan menjadikan AES selamat dan imun terhadap semua risiko. Unit gantian bait dan permutasi dalam sifer blok AES yang menghasilkan difusi dan kekeliruan mempunyai struktur tetap bagi semua pusingan.

Tesis ini mencadangkan satu sifer blok simetri yang selamat dengan komponen bersandarkan kunci yang diinspirasikan oleh teknik DNA biologi yang dikenali sebagai Sifer Blok Berasaskan DNA (DNAB). Tesis ini mengenal pasti elemen yang sama dan mengetengahkan elemen kiraan yang penting seperti helaian DNA, tapak DNA, struktur heliks berganda asid nukleik, dogma pusat dengan prosesnya yang mampu diaplikasikan dalam sifer blok simetri yang memenuhi dua keperluan pengeliruan dan resapan Shannon.

Sifer DNAB menggunakan komponen kunci bersandar berasaskan DNA bagi meningkatkan keselamatan sifer dan untuk mengurangkan bilangan pusingan sifer terlelar. Sehubungan itu, bagi lapisan pengganti, realiti bahawa kotak S tidak diketahui merupakan satu daripada kekuatan utama bagi sifer baharu

memandangkan pemecahan tulisan rahsia memerlukan kotak S. Bagi lapisan permutasi dan proses penjadualan kunci, penggunaan transformasi dan proses bersandarkan kunci diinspirasikan oleh teknik DNA meningkatkan kerumitan bagi serangan daya kasar kepada kunci dan memaksa penyerang untuk mencuba dan mencipta rangka kerja mekanisme kripanalisisbaharu.

Dapatan eksperimental mempersembahkan kerawakan bagi output dalam sifer DNAB sebagai sifer blok selamat dan dibandingkan kepada sifer blok AES, bilangan pusingan lelaran telah dikurangkan. Ujian kotak S mempersembahkan kotak S baharu dalam sifer DNAB memenuhi kriteria keseimbangan, kesempurnaan, runtuhan, runtuhan tegas, bit bebas, ketaklinearan, keseragaman perbezaan, songsangan dan tidak bercanggah sebagai syarat kotak S yang baik bagi kedua-dua kotak S statik dan bersandarkan kunci.

Analisis kesan runtuhan bagi sifer DNAB telah diuji secara makmal menggunakan teks biasa dan kunci runtuhan serta korelasi koeffisien, kesalahan bit dan sensitiviti kunci dan ianya memenuhi keperluan pengeliruan dalam transformasi tidak linear bagi teks sifer yang dihasilkan dalam pusingan ketiga bagi sifer blok. Ujian makmal runtuhan secara empirikal menunjukkan yang perubahan hanya satu bit kunci sifer mewujudkan satu kotak S baharu yang berbeza. Ia turut mengukur keperluan resapan dalam transformasi linear menggunakan nombor cabang dalam menjangkakan kejayaan serangan perbezaan dan linear.

Meskipun kotak S bersandarkan kunci bagi sifer DNAB mempunyai 8 bit bagi input dan 8 bit bagi output, output mempunyai kebarangkalian satu daripada $2^{n!}$, berbanding kebarangkalian $2^8$ bagi kotak S statik; malah bagi setiap pusingan, transposisi bersandarkan kunci dan transformasi campuran lajur bersandarkan kunci masing-masing mempunyai kebarangkalian (28.24!). Ini menyebabkan kripanalisis bagi transformasi bersandarkan kunci kotak S menjadi sukar kerana ia mengkehendaki jurukripanalisis untuk membina kesemua kemungkinan kotak S dan mencubanya dalam transformasi gantian/permutasi. Ini mengesahkan bahawa sifer DNAB telah berjaya melepasi analisis keselamatan yang ketat dan mewajarkan sifer DNAB adalah sifer blok yang selamat. Sehubungan itu, ianya akan dapat meningkatkan perlindungan bagi sistem maklumat institusi; ia juga akan dianggap sebagai salah satu sifer blok simetri yang paling selamat dalam penyelidikan keselamatan informasi dan membuka pintu kepada penyelidikan yang menggabungkan keselamatan komputer dan sistem biologi.

## ACKNOWLEDGEMENTS

First and foremost, I am eternally thankful to Allah for His blessings, strength and perseverance bestowed on me, enabling me to complete this thesis.

I would like to take this opportunity to thank my supervisor, Prof. Dr. Ramlan Mahmod, for his support, guidance, and understanding. Special appreciation goes to him for his mentorship and constant support throughout this research. His comments and suggestions for further development as well as his assistance during writing this thesis are invaluable to me. His patience, humility, tutorship, interest, teaching and research style have provided for me an exceptional opportunity to learn and become a better researcher.

I would also like to thank the committee members, Associate Professor Dr.Zuriati Ahmad Zukarnaine and Associate Professor Dr. Nur Izura Udzir for their help and valuable suggestions.

Above all I am very grateful to my father and mother for their encouragement, my loving and caring wife and my adorable children for their support and love in my efforts to successfully complete this work. For those others who have either directly or indirectly helped me in carrying out my work, I thank you all. Lastly, my heartfelt thanks to the Universiti Putra Malaysia and kind Malaysia for their support, and make me feel at home.

I certify that a Thesis Examination Committee has met on 26 October 2015 to conduct the final examination of Auday H.Saeed on his thesis entitled "Development of DNA-Based Dynamic Key-Dependent Block Cipher" 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:

**Azmi bin Jaafar, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

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

**Mohamad Rushdan bin Md Said, PhD**
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

**Siddeeq Yousif Ameen, PhD**
Professor
Gulf University
Bahrain
(External Examiner)

**ZULKARNAIN ZAINAL, PhD**
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 15 December 2015

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:

**Ramlan Mahmod, PhD**
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

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

**Nur Izura Udzir, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

_____
**BUJANG BIN KIM HUAT, 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.: Auday H. Saeed GS 28463

**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: Ramlan Mahmod, PhD

Signature: _____

Name of Member of Supervisory Committee: Zuriati Ahmad Zukarnain, PhD

Signature: _____

Name of Member of Supervisory Committee: Nur Izura Udzir, PhD

## TABLE OF CONTENTS


| | | Page |
|---|---|---|
| **ABSTRACT** | | i |
| ***ABSTRAK*** | | ii |
| **ACKNOWLEDGEMENTS** | | vi |
| **APPROVAL** | | vii |
| **DECLARATION** | | ix |
| **LIST OF TABLES** | | xiii |
| **LIST OF FIGURES** | | xvii |
| **LIST OF ABBREVIATIONS** | | xxi |
| **CHAPTER** | | |
| **1** | **INTRODUCTION** | **1** |
| 1.1 | Introduction | 1 |
| 1.2 | Problem statement | 2 |
| 1.3 | Research objectives | 4 |
| 1.4 | Scope of the study | 4 |
| 1.5 | Contribution of the study | 5 |
| 1.6 | Organization of the thesis | 6 |
| **2** | **LITERATURE REVIEW** | **7** |
| 2.1 | Introduction | 7 |
| 2.2 | Computer security concept | 7 |
| 2.2.1 | Cryptology | 8 |
| 2.2.2 | The cryptography | 8 |
| 2.2.3 | Cryptography in history | 8 |
| 2.2.4 | Cryptography algorithms | 9 |
| 2.2.5 | Cryptography categorization | 9 |
| 2.3 | Block ciphers | 11 |
| 2.3.1 | Confusion | 12 |
| 2.3.2 | Diffusion | 13 |
| 2.4 | Symmetric block cipher construction design | 13 |
| 2.4.1 | Iterative block cipher | 13 |
| 2.4.2 | Key-alternating block ciphers | 16 |
| 2.4.3 | Key-iterated block ciphers | 16 |
| 2.4.4 | Wide Trail strategy | 17 |
| 2.5 | Static and key-dependent S-Boxes | 18 |
| 2.6 | Security test of block cipher | 19 |
| 2.7 | AES block cipher (Rijndael) | 20 |
| 2.7.1 | Notions and terminologies for AES block cipher | 21 |
| 2.7.2 | AES S-Box description | 22 |
| 2.7.3 | 4-byte vectors | 23 |
| 2.7.4 | Maximum distance separable matrix (MDS) | 25 |
| 2.8 | Overview of recent block cipher | 26 |

| | | | |
|---|---|---|---|
| | 2.9 | Summary | 29 |
| **3** | **DNA SYSTEM AS INSPIRATION** | | **30** |
| | 3.1 | Introduction | 30 |
| | 3.2 | DNA background | 30 |
| | | 3.2.1 The natural DNA properties | 33 |
| | | 3.2.2 Limitation of DNA cryptography | 33 |
| | | 3.2.3 Pseudo DNA cryptography | 33 |
| | 3.3 | Conceptual metaphor | 33 |
| | 3.4 | DNA computing | 34 |
| | 3.5 | DNA cryprography | 35 |
| | 3.6 | DNA processes | 36 |
| | 3.7 | Application within block cipher | 38 |
| | 3.8 | Summary | 39 |
| **4** | **RESEARCH METHODOLOGY** | | **40** |
| | 4.1 | Introduction | 40 |
| | 4.2 | Research methodology | 40 |
| | | 4.2.1 Literature review | 40 |
| | | 4.2.2 Identifying the problem | 42 |
| | | 4.2.3 System design | 42 |
| | | 4.2.4 Implementation and coding | 42 |
| | | 4.2.5 Analysis | 44 |
| | | 4.2.6 Documentation | 44 |
| | 4.3 | Security test of block cipher | 44 |
| | | 4.3.1 S-Box tests criteria | 44 |
| | | 4.3.2 NIST Suite randomness test | 48 |
| | | 4.3.3 Avalanche effect of whole algorithm | 53 |
| | | 4.3.4 Cryptanalysis | 54 |
| | 4.4 | Experimental design | 56 |
| | | 4.4.1 Data preparation | 56 |
| | | 4.4.2 Experimental process | 57 |
| | | 4.4.3 Results and security evaluation (analysis) | 60 |
| | 4.5 | Summary | 63 |
| **5** | **DESIGN AND IMPLEMNTAION OF THE DNA-BASED KEY-DEPENDENT BLOCK CIPHER (DNAB)** | | **64** |
| | 5.1 | Introduction | 64 |
| | 5.2 | System general view | 64 |
| | | 5.2.1 Notation | 66 |
| | | 5.2.2 Input and output | 68 |
| | | 5.2.3 Key blending function | 69 |
| | | 5.2.4 Key scheduling function KS | 69 |
| | 5.3 | Preliminaries and definitions | 69 |
| | | 5.3.1 DNA sequences | 69 |
| | | 5.3.2 DNA binary coding | 70 |
| | | 5.3.3 DNA logical operations | 71 |
| | | 5.3.4 Reverse complement | 71 |
| | | 5.3.5 Central dogma | 72 |

| | | | | |
|---|---|---|---|---|
| | 5.4 | Substitution transformation | | 72 |
| | | 5.4.1 | Static DNA-based S-Box | 72 |
| | | 5.4.2 | Key-dependent dynamic DNA-based S-Boxes (*KdD_S*) | 76 |
| | 5.5 | Permutation transformation | | 86 |
| | | 5.5.1 | Key-dependent DNA-based dynamic transposition (*KdD_T*) | 87 |
| | | 5.5.2 | Key-dependent DNA-based MixColumns (*KdD_MX*) | 90 |
| | 5.6 | AddRoundKey ($AD_{\mathrm{r}}$) | | 92 |
| | 5.7 | Round structure | | 92 |
| | 5.8 | Encryption and decryption processes | | 95 |
| | 5.9 | Summary | | 98 |
| **6** | **S-BOX SECURITY TEST** | | | **99** |
| | 6.1 | Introduction | | 99 |
| | 6.2 | S-Box test criteria | | 99 |
| | | 6.2.1 | Balanced | 100 |
| | | 6.2.2 | Completeness | 100 |
| | | 6.2.3 | Avalanche criterion | 101 |
| | | 6.2.4 | Strict avalanche (SAC) | 101 |
| | | 6.2.5 | Nonlinearity | 102 |
| | | 6.2.6 | Bit independence (BIC) | 102 |
| | | 6.2.7 | Differential uniformity | 103 |
| | | 6.2.8 | Invertability | 103 |
| | | 6.2.9 | Non-contradiction | 103 |
| | 6.3 | Avalanche effect due to one bit change in key (key-dependent S-Boxes) | | 104 |
| | 6.4 | Avalanche effect due to one bit change in key | | 105 |
| | 6.5 | Key sensitivity analysis | | 106 |
| | 6.6 | Correlation coefficient | | 107 |
| | | 6.6.1 | Correlation coefficient on permutation transformation | 108 |
| | | 6.6.2 | Correlation coefficient on all transformations | 110 |
| | 6.7 | Bit error analysis | | 112 |
| | 6.8 | Summary | | 115 |
| **7** | **RANDOMNESS TEST** | | | **116** |
| | 7.1 | Introduction | | 116 |
| | 7.2 | Preliminary test | | 116 |
| | 7.3 | Random plaintext with random key | | 119 |
| | 7.4 | Low density plaintext and low density key | | 122 |
| | 7.5 | High density plaintext and low density key | | 123 |
| | 7.6 | 128 bit key avalanche and plaintext avalanche | | 124 |
| | | 7.6.1 | Key avalanche | 124 |

| | | | |
|---|---|---|---|
| | 7.6.2 | Plaintext avalanche | 125 |
| 7.7 | | Randomness test compared with AES block cipher | 127 |
| 7.8 | | Summary | 129 |
| **8** | **CRYPTANALYSIS** | | **130** |
| 8.1 | | Introduction | 130 |
| 8.2 | | Avalanche effect due to one bit change in plaintext | 130 |
| 8.3 | | Plaintext sensitivity analysis | 132 |
| 8.4 | | Analysis of information entropy | 133 |
| 8.5 | | Cryptanalysis | 133 |
| 8.6 | | Summary | 135 |
| **9** | **CONCLUSION AND FUTURE WORK** | | **136** |
| 9.1 | | Introduction | 136 |
| 9.2 | | Conclusion | 136 |
| 9.3 | | Recommendations for future works | 139 |
| **REFERENCES/BIBLIOGRAPHY** | | | **140** |
| **APPENDICES** | | | **158** |
| **BIODATA OF STUDENT** | | | **198** |
| **LIST OF PUBLICATIONS** | | | **199** |

## LIST OF TABLES


| Table | | Page |
|---|---|---|
| 2.1 | The Number of AES rounds according to key sizes | 20 |
| 2.2 | Description of the notation for AES block diagram in Figure 2.13 | 24 |
| 4.1 | Definitions of some term used in NIST test suite Statistical Tests | 49 |
| 4.2 | Symbols used in the NIST test suite Statistical Tests | 49 |
| 4.3 | The 15 core statistical tests of the NIST Statistical Test Suite | 50 |
| 4.4 | Data sets for the NIST Test Suite Statistical tests | 52 |
| 4.5 | Input parameters of NIST test suite Statistical Tests | 53 |
| 4.6 | Analysis of P-values in terms of randomness | 61 |
| 4.7 | Accepted range values for interpreting the correlation coefficient | 62 |
| 5.1 | Description of the notation for DNAB block cipher diagram | 67 |
| 5.2 | Hexadecimal and DNA bases representation of bit | 68 |
| 5.3 | Binary representation of DNA bases | 70 |
| 5.4 | The possible binary coding of DNA bases | 70 |
| 5.5 | Transposition key values | 87 |
| 6.1 | Rate of ciphertext change for one digit key difference | 107 |
| 6.2 | Correlation test, $r_{xy}$ of $KdD\_T_r$ transformation for sequence number 1-128 | 109 |
| 6.3 | Correlation test, $r_{xy}$ on DNAB block cipher for sequence number 1- 84 | 110 |
| 6.4 | Correlation test, $r_{xy}$ on DNAB block cipher for sequence number 85-128 | 111 |
| 6.5 | Bit error results for sequence number 1- 34 | 112 |

| | | |
|---|---|---|
| 6.6 | Bit error results for sequence number 35- 86 | 113 |
| 6.7 | Bit error results for sequence number 87- 128 | 114 |
| 7.1 | DNAB block cipher frequency test result over zero input | 116 |
| 7.2 | Breakdown of 15 statistical tests applied during experimentation | 120 |
| 7.3 | The p-value of Frequency Test with low density key for non-passing sequences for rounds 1,2 and 3 for sequence number 1- 300 | 122 |
| 7.4 | The p-value of Frequency Test with low density plaintext for non-passing sequences over 300 sequences for round 1,2 and 3 for sequence number 1- 300 | 122 |
| 7.5 | The p-value of Frequency Test with high density key for non-passing sequences for rounds 1, 2 and 3 1 for sequence number 1- 300 | 123 |
| 7.6 | The p-value of Frequency Test with high density plaintext for non passing sequences for rounds 1, 2 and 3 for sequence number 1- 300 | 123 |
| 7.7 | NIST statistical test results for AES block cipher | 128 |
| 7.8 | NIST statistical test results for DNAB block cipher | 128 |
| 8.1 | Rate of ciphertext change for one bit plaintext difference | 132 |

## LIST OF FIGURES


| Figure | | Page |
|---|---|---|
| 2.1 | Overview of cryptology | 8 |
| 2.2 | Iterative block cipher with four rounds | 14 |
| 2.3 | Single round of block cipher Shark, based on the uniform transformation structure. | 15 |
| 2.4 | Key-alternating block ciphers with three rounds | 16 |
| 2.5 | Block cipher taxonomy | 17 |
| 2.6 | Formation of block cipher of Wide Trial Strategy | 18 |
| 2.7 | Block cipher main evaluation criteria | 19 |
| 2.8 | Evaluation criteria of cryptographic algorithm security | 20 |
| 2.9 | Forward AES S-Box | 23 |
| 2.10 | Rijndael (AES) block diagram | 25 |
| 3.1 | DNA structure | 30 |
| 3.2 | Fundamental components of DNA | 31 |
| 3.3 | The detail of Deoxyribe Nucletides | 31 |
| 3.4 | The structure of DNA strands | 32 |
| 3.5 | Overview of Central Dogma process | 36 |
| 3.6 | Central Dogma process for DNA segment. | 37 |
| 3.7 | Overview of Central Dogma process from the perspective of symmetric encryption | 38 |
| 4.1 | Map steps of research methodology | 41 |
| 4.2 | Research design frame | 43 |
| 4.3 | Thesis experimental stages | 56 |
| 4.4 | Experiment process of S-Box test criterion | 58 |
| 4.5 | Experiment process on randomness test | 59 |
| 4.6 | Experiment process on avalanche test | 60 |
| 5.1 | General concept of the proposed block cipher (DNAB) | 65 |
| 5.2 | General structure of DNAB block cipher | 66 |
| 5.3 | Ordering bytes of the proposed block cipher | 68 |
| 5.4 | The XOR operation over DNA bases | 71 |
| 5.5 | The XOR of binary representation of the DNA bases | 71 |
| 5.6 | Reverse DNA sequence | 71 |

| | | |
|---|---|---|
| 5.7 | Reverse-complement DNA sequence | 71 |
| 5.8 | Constructing of Init S-Box matrix | 73 |
| 5.9 | Binary representation of Init S-Box matrix | 74 |
| 5.10 | Pseudo code algorithm of New S-Box elements allocating | 75 |
| 5.11 | Constructing of New S-Box matrix | 75 |
| 5.12 | A 4×4 matrix as sample S-Box S-Box-S | 76 |
| 5.13 | Expand key-matrix elements generating by shift rows process | 78 |
| 5.14 | Expand key-matrix elements generating by key-segment process | 79 |
| 5.15 | Overview of key-matrix generation steps for S-Box-S | 79 |
| 5.16 | Pseudo code of columns transcription process | 81 |
| 5.17 | Example for column transcription | 82 |
| 5.18 | Pseudo code of row transcription process concept | 83 |
| 5.19 | Example for row transcription | 83 |
| 5.20 | Generating dynamic key-depended S-Box-S using column transcription technique | 84 |
| 5.21 | Generating dynamic key-dependent S-Box-S using row transcription | 85 |
| 5.22 | Generating dynamic key-dependent S-Box-S using column transcription and key rotation techniques | 85 |
| 5.23 | Generating dynamic key-dependent S-Box-S using column and row transcription techniques | 86 |
| 5.24 | The state row transposition process depending on key | 88 |
| 5.25 | Key-dependent transposition inspired by DNA processes | 89 |
| 5.26 | Pseudo code of KdD_transposition | 89 |
| 5.27 | Figure 5.26: A 4×4 MDS | 90 |
| 5.28 | Generating new key-dependent MDS matrix | 91 |
| 5.29 | Generating new key-dependent MDS matrix (MOK) matrix | 91 |
| 5.30 | Three rounds of DNAB block cipher | 93 |
| 5.31 | Sequence of steps of 2 rounds transformation, followed by a key addition | 94 |
| 5.32 | Encryption and decryption functions of DNAB block cipher | 96 |
| 5.33 | Pseudo code of encryption algorithm | 97 |
| 5.34 | Pseudo code of decryption algorithm | 97 |
| 5.35 | Execution of DNAB block cipher | 98 |

| | | |
|---|---|---|
| 6.1 | A number of key-dependent S-Boxes | 100 |
| 6.2 | The Avalanche effect for sample of the S-boxes generated using column transcription method | 101 |
| 6.3 | A key dependent S-Box generated using the proposed method | 104 |
| 6.4 | S-box generated using the proposed method after changing one bit of the key used in generating the S-Box | 104 |
| 6.5 | Avalanche effect of changing one bit of key sequences (1-64) with resulted cipher text | 105 |
| 6.6 | Avalanche effect of changing one bit of key sequences (65-128) with resulted cipher text | 106 |
| 6.7 | Key sensitivity analysis | 107 |
| 6.8 | Laboratory experiment process of correlation coefficient DNAB $KdD\_T_r$ function | 108 |
| 6.9 | Scatter chart of the correlation test results on $KdD\_T_r$ function only | 109 |
| 6.10 | Scatter chart of the correlation test results on DNAB block cipher | 111 |
| 6.11 | Scatter chart of the bit error test results | 115 |
| 7.1 | P-values of the Frequency Test at round 1 and 2 | 117 |
| 7.2 | P-values of the Frequency Within Block Test at round 1 and 2 | 118 |
| 7.3 | P-values of the Runs Test at rounds 1 and 2 | 119 |
| 7.4 | Randomness tests results of DNAB block cipher in round 1 | 121 |
| 7.5 | Randomness tests results of DNAB block cipher in round 2 | 121 |
| 7.6 | Randomness tests results of DNAB block cipher in round 3 | 121 |
| 7.7 | P-values of the Frequency Test for key avalanche in round 3 | 124 |
| 7.8 | P-values of the Frequency Within Block Test for key avalanche in round 3 | 125 |
| 7.9 | P-values of the Run Test for key avalanche in round 3 | 125 |
| 7.10 | P-values of the Frequency Test for plaintext avalanche in round 3 | 126 |
| 7.11 | P-values of the Frequency Within Block Test for plaintext avalanche in round 3 | 126 |
| 7.12 | P-values of the Run Test for plaintext avalanche in round 3 | 127 |
| 7.13 | The chart for the p-values between 1000,000 bits generated from AES and DNAB block ciphers | 129 |
| 8.1 | Avalanche effect of changing one bit of plaintext sequences (1-64) with resulting ciphertext | 131 |

8.2 Avalanche effect of changing one bit of plaintext sequences (65-128) with resulting ciphertext 131

8.3 Plaintext sensitivity analysis 132

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| BBS | Blum Blum Shub |
| BIC | Bit of Independence |
| DFD | Data Flow Diagram |
| DNA | Deoxyribonucleic Acid |
| DNAB | DNA-based Block Cipher |
| EBI | European Bioinformatics Institute |
| ECB | Electronic Codebook Mode |
| GF | Galois Field |
| ITU | International Telecommunication Union |
| ITU-U | ITU Telecommunication Standardization Sector |
| mRNA | Messenger Ribonucleic Acid |
| MDS | Maximum distributing Separator |
| NCIB | National Center for Biotechnology Information |
| NIST | National Institute of Standards and Technology |
| OSI | Open System Interconnection |
| P-value | Probability Value |
| RNA | Ribonucleic Acid |
| SAC | Strict Avalanche Criterion |
| SPN | Substitution-permutation network |
| S-Box | Substitution box |
| XOR | Exclusive OR |

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

□,□Q□□□J□H□Q□H□U□D□O□□□□□V□H□F□X□U□L□W□\□□□L□V□□□F□R□Q□F□H□ computer science perspective, it is the deterrence of, or safeguard against, unauthorized access to data as well as, premeditated demolition, modification and alteration of that data. Since earliest times passing through the invention of the advent of computer science until the present, information has been and continues to be a critical element in need of protection; it needs security. Today secure connections represent a major priority for most areas of modern life, for instance, e-Government, trading, CCTV, banking transactions, connectivity, and many other fields. Through the rapid expansion of the Internet and increased reliance in all fields of life, the need for an extremely effective means of achieving information and data security is crucial.

Cryptography, which is considered a science and an art has been and is still undoubtedly the most efficient means used to attain secrecy. All security concepts can be achieved via cryptographic algorithms including confidentiality, integrity and authentication, besides other concerns such as availability, privacy and access control. Since 2000 B.C., cryptography has been documented as a tool used by the Egyptian scrivener when he made unusual hieroglyphs in his engraving (Singh, 2011). It has since continued to be used from that early era to the present day with different and variant applications in all aspects of life and in both peace and war time. The extensive growth and expansion of using computers in all aspects of life, especially in communications has led to the emergence of various new forms of cryptography□□

The entire process that supplies the required degree of security includes network protocols and algorithms of data encryption can be described through the RFC □□□□□□□□□□□ □L□G□H□Q□W□L□I□L□F□D□W□L□R□Q□□ □R□I□□ □W□K□H□□ □F□ algorithms together with key management processes that support the use of the □D□O□J□R□U□L□W□K□P□V□□□L□(Shirey, 2000).□P□H□□□D□S□S□O□L□F□D□W□L□R

The Symmetric Block cipher is a significant cryptographic algorithm because of its simplicity, speed and robustness and this cryptographic algorithm is used in performing the encryption and decryption for most modern security applications, especially in the communications field. The significant increase of exchanging data through the Internet has imposed numerous challenges including data accessibility, availability and low cost, with many scenarios and techniques proposed and designed, including cloud storage, which is a model of cloud computing (Mell & Grance, 2011), where data are saved in virtually depository

pools, which are usually remote servers supervised by third parties, that can be accessed through the Internet by the client. Although this system represents one of the most successful scenarios and makes available an abundance of data, but this availability alone is not sufficient as it requires privacy for sensitive data such as secret military and government documents, enterprise data for institutions and medical data.

The use of suitable symmetric block cipher to encrypt the data is the best and standard modus operandi to achieve privacy for storage systems especially in cloud storage (Kamara & Papamanthou, 2013). Also, the wide and daily increase in the use of wireless network low-end equipment such as wireless sensor nodes, and RFID cards which would be considered useless if they were not secured as it would duplicate the attention and effort needed to deal with the works that are focused on symmetric block since this security technique is the standard approach used to achieve security for wireless network equipment.

The considerable achievements that have been witnessed recently in biological techniques have revealed that they have distinctive characteristics that can be relied upon in the security domain, especially in designing new strong security systems. DNA (Deoxyribonucleic Acid) and RNA (Ribonucleic acid) with their structures, properties, and operations are considered as an ideal area to be used for this domain.

## 1.2 Problem Statement

Given the importance of (AES) block cipher (Daemen & Rijmen, 2002) in computer security, many attempts have focused on designing new algorithms that adopt the same principle of the AES algorithm with less cost and requirements. The confusion properties are obtained using the substitution-Box (S-Box), while, diffusion properties are generated using some round iteration to produce a secure data transmission (Menezes et al., 1996). Substitution and permutation functions are commonly used in block ciphers to make them much harder and more efficient ciphers.

Since the declaration time of Rijndael as AES this cipher has been the target of many attacks and cryptanalysis and the attempts to break it are ongoing but, on the contrary, increased day by day taking advantage of the rapid development in computing capabilities (Zhang et al., 2007; Biryukov & Khovratovich, 2009; Daemen & Rijmen, 2010; Mala et al., 2010; Zhonglin & Zhihua, 2011).The rise in frequency of attacks against the AES algorithm has not been matched by the level of development in the capabilities of the algorithm to withstand these challenges and make the AES secure and immune to all risks.

, we know that AES block cipher has constant transformations which make it less secure, compared to the dynamic key-dependent structures. So that, the byte

substitutions unit in AES block cipher has a fixed structure S-Box with no relation to the cipher key and no share key is available in creating this S-Box. Implementing the key-dependent S-Box increases the security of the block cipher. Whether the fixed key S-Box cipher is weaker security and less immune against attacks than the dynamic key-dependent S-Box cipher, since it has less key-space (Fahmy et al., 2005; Krishnamurthy & Ramaswamy, 2008).

Furthermore, fixed S-Box permits attackers to study S-Box and find weak points (Janadi & Anas Tarah, 2008; Kazlauskas & Kazlauskas, 2009; Das et al., 2012; Juremi et al., 2012; Pradeep & Bhattacharjya, 2013) . It is clear that ciphers with key-dependent S-Box are generally more secure than fixed S-Box, and the dynamic structure of S-Box increases the strength of the cipher (Elkamchouchi & Makar, 2004). The dynamic key-dependent S-□%□R□[□□ □L□Q□F□U□H□D□V□H□V□□ immunity to linear and differential cryptanalysis (Keliher & Meijer, 1997), Key-dependent S-Boxes represent a form of security margin against unknown attacks (Nechvatal et al., 2000).

Within the substitution layer also, the S-Box of AES block cipher is generated depending on getting multiplicative inverse with finite field, using the affine transformation, the operations of which rely on mathematical operations as multiplication, division and adding besides the modular. All this consumes time and requires calculations, thus making the byte substitutions ineffective for the low resource devices as well as introducing linear and algebraic properties that can be used by attackers (RezaeiPour et al., 2009). It would be more effective if the byte substitutions unit S-Box is generated using alternating techniques to reduce the amount of mathematical operations.

In addition to byte substitutions, the second unit of the AES block cipher is the byte permutations, consisting of two fixed components for all rounds: ShiftRows and MixColumns transformations. The ShiftRows move the bytes of the state with the same offsets for all rounds, while the MixColumns use the same MDS matrix to product with the state byte for all rounds.

The constant ShiftRows transformation means less degree of diffusion and easier in key breaking than the key-dependent dynamic ShiftRows transformation. The dynamic key-dependent ShiftRows raises the complexity of the block cipher (Ismil et al., 2012), and the key-dependent MixColumns transformation is more immune and secure than the static one (Malik & No, 2011). The design of dynamic key-dependent ShiftRows to increase the diffusion is one of the problems considered in this thesis.

For the MixColumns transformation, the use of fixed MDS matrix for all the rounds makes the transformation more vulnerable to some forms of attack, whereas the use of key-dependent MDS matrices increases the resistance of the cipher against attacks (Murtaza et al., 2011). The design of dynamic key-dependent MixColumns is one of the problems considered in this thesis.

Since the establishment of DNA computing by Adleman in 1944 (Adleman, 1994), many other studies have been done on DNA cryptography. From these many studies, a number have become more familiar in the application of techniques, attributes and characteristics of the DNA system in the design and development of security algorithms or model applications (Amin et al., 2006; Cui et al., 2008; Shaw & Hussein, 2008; Sadeg et al., 2010; Wang et al., 2010). The literature suggests that there should be further work done to investigate and better understand the involvement of the DNA system in its application to the block ciphers. Despite the many features, properties and attributes which characterize biological DNA, to the best knowledge of this researcher, there has not been any work done to take advantage of these properties in designing a new SPN symmetric block cipher with key-dependent permutation transformations. Additionally, all the existing dynamic block ciphers were designed and developed utilizing traditional methods which are calculations, time consumption, and less secure.

This thesis will define the biological DNA approaches to cryptographic algorithm, pointing out the equivalent and different elements, and indicating essential elements that can be applied to ciphers. These substantial elements of the biological DNA system can be related to the diffusion and confusion cryptography characteristics. It is only natural to use the biological DNA techniques to improve the design of a new block cipher called DNA-based dynamic key-dependant block cipher (DNAB block cipher). The structure of the components has a fixed block size of 128 bits, a key size of 128 bits, and operates on a 4X4 array of bytes. .

## 1.3 Research Objectives

The objective of this research is to design a new symmetric encryption block cipher inspired by real biology processes of DNA with dynamic key-dependent components In order to achieve the objective, the following tasks will be carried out:

a) Identification of characteristic, components, operations, and the behavior of biology DNA system that will be used to design a novel block cipher.
b) Construction of a set of methods based on real biology DNA operations and structures to be employed in the creation of the new block cipher.
c) Security analysis of the proposed block with all its components to guarantee that it satisfies the minimum security requirement.

## 1.4 Scope of the Study

The scope of this study is to design and develop a new secure symmetric block cipher that has the subsequent characteristics which are taken into account:

a) The size of the block is 128 bits.
b) The size of the key is 128 bits.
c) The electronic codebook (ECB) is a mode of operation of the encryption process for every block.

d) The proposed block cipher should satisfy several security tests, pass a number of standard randomness tests, and show good resistance to linear and differential attacks.
e) The proposed static and key-dependent S-Boxes should achieve several S-Box tests criteria.

In this study the security requirement is considered as the most important factor in designing the symmetric block cipher owing to this classification of assessment (Nechvatal, Barker, Bassham, Burr, & Dworkin, 2000). It is imperative to guarantee that the proposed block cipher is secure and immune before undertaking the assessment of other terms such as speed or efficiency.

## 1.5 Contribution of the Study

The research will contribute to the following:

This research defines the biology of the DNA system with its components, elements, operations, and techniques, which are used to inspire the design of the new block cipher, as well as indicate the concepts that can be used within the symmetric block cipher. The main elements of the DNA system can be related to confusion and diffusion characteristics of cryptography.

This study uses some of the DNA processes and techniques to improve the design of the new block cipher by creating a new static S-Box, which does not use the multiplicative inverse, with less use of mathematics operations but keeping the same security level of AES S-Box. The use of pseudo segments of DNA in creating this S-Box makes this segment act as a new key in addition to the symmetric 128 key, which increases the key-space.

This study uses some of the DNA processes and techniques to improve the design of the new block cipher by creating new key-dependent functions including substitution and permutation transformations. The substitution transformation consists of key-dependent-S-Boxes, while permutation transformation consists of key-dependent ShiftRows, and key-dependent MixColumns. The use of dynamic key-dependent transformation will increase the security of block ciphers and make them more immune against the attacks and more difficult for cryptanalysis.

The DNAB block cipher within the counter mode like other secure block ciphers acts as pseudo-random number generators. In this study the NIST suite test is used to test the quality of random numbers generated by the proposed cipher according to standards stipulated by the National Institute of Standards and Technology (NIST). The cryptographic statistical tests for random number generators, S-Boxes test criteria, DNAB block cipher avalanche effects, and cryptanalysis were evaluated and presented in this study.

## 1.6 Organization of the thesis

This thesis consists of nine chapters, starting with Chapter 1, which provides the introduction of the thesis comprising the research problem, research objectives, scope, and contributions of the research.

Chapter 2 provides the background information of the related work on the security in computing, cryptography and symmetric block cipher. This chapter covers the concepts, fundamentals, and basics of properties, design structure, security analysis, previous researches and works on block ciphers. Finally, the expressions, terminology perceptions and idioms used in this thesis are defined.

Chapter 3 presents the applied model based on DNA processes and structures. It describes the essential techniques and processes of the biological DNA system to be employed in building the new block cipher.
Chapter 4 illustrates the research methodology for carrying out this research. It includes the description of the experimental design, which will be utilized to choose the testing data.

Chapter 5 presents and discusses the proposed design of the DNAB block cipher. This includes declaration of the overall structure of the new block cipher, the design of the static DNA-based S-Box, the design of Column/Row transcription-based key-dependent dynamic S-Boxes, the design of new Column/Row transcription key-dependent MixColumns transformation.

Chapter 6 shows the S-Box tests criteria for the new static and dynamic S-Boxes including balanced, completeness, avalanche, strict avalanche (SAC), nonlinearity, bit independence (BIT), differential uniformity, invertability, and non-contradiction. All the results of these criteria tests are reviewed in this chapter. It also present and analyzes the confusion property of the DNAB block.

Chapter 7 reviews the outcomes of the analysis, and the randomness of output generated from the DNAB block cipher. The experiments will be conducted by the NIST Test Suite randomness software, comprising some kinds of data at every iteration round of the functions.

Chapter 8 presents measures and analyzes the diffusion property of the DNAB block cipher, where the avalanche of the whole proposed block cipher, branch number, and the cryptanalysis of the proposed block cipher will be tested .

Chapter 9 provides the conclusions of the research presented in this thesis followed by some recommendations to investigate and expand the field of research in relation to DNAB block cipher.

## REFERENCES


Adams, C., & Tavares, S. (1990a). *Good S-boxes are easy to find*.Advances in Cryptology□²□&□5□<□3□7□2□¶□□□□□□□3□U□R□F□H□H□G□L□Q□J□V□□

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

Adleman, L. M. (1994). Molecular computation of solutions to combinatorial problems. *Science-AAAS-Weekly Paper Edition, 266*(5187): 1021-1023.

Ahmad, M., Gupta, S., & Mohapatra, A. (2014). *A Bio-Chaotic Block Cryptosystem for Privacy Protection of Multimedia Data*.Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013.

Ahmad, N., Hasan, R., & Jubadi, W. M. (2010). *Design of AES S-Box using combinational logic optimization*.Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium on.

Al-Janabi, S. T. F. (2011). *Nahrainfish: A green cryptographic block cipher*.Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International.

Ali, M., & Hani, F. (2004). *A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bitwise Operations.* Universiti Putra Malaysia.

Alsultanny, Y. A., & Jarrar, H. J. (2006). Generating and testing random key for image encryption using ECB and CBC modes. *JORDAN JOURNAL OF APPLIED SCIENCE NATURAL SCIENCES, 8*(1): 1.

Amador, J. J., & Green, R. W. (2005). Symmetric-key block cipher for image and text cryptography. *International Journal of Imaging Systems and Technology, 15*(3): 178-188.

Amin, S. T., Saeb, M., & El-Gindi, S. (2006). *A DNA-based Implementation of YAEA Encryption Algorithm*.IASTED International Conference on Computational Intelligence, San Francisco.

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., & Tokita, T. (2001). *Camellia: A 128-bit block cipher suitable for multiple platforms ²design andanalysis* .Selected Areas in Cryptography.

Balamurugan, J., & Logashanmugam, E. (2013). Design of Efficient AES using modified mix-column architecture.

Barish, R. D., Rothemund, P. W., & Winfree, E. (2005). Two computational primitives for algorithmic self-assembly: Copying and counting. *Nano Letters, 5*(12): 2586-2592.

Bassham III, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., Leigh, S. D., Levenson, M., Vangel, M., & Banks, D. L. (2010). SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.

Bell, G. I., & Torney, D. C. (1993). Repetitive DNA sequences: some considerations for simple sequence repeats. *Computers & chemistry, 17*(2): 185-190.

Benson, D. A., Cavanaugh, M., Clark, K., Karsch-Mizrachi, I., Lipman, D. J., Ostell, J., & Sayers, E. W. (2012). GenBank. *Nucleic acids research*: gks1195.

Benson, D. A., Karsch-Mizrachi, I., Lipman, D. J., Ostell, J., & Wheeler, D. L. (2005). GenBank. *Nucleic acids research, 33*(suppl 1): D34-D38.

Berg, J. M., Tymoczko, J. L., & Stryer, L. (2002). DNA polymerases require a template and a primer.

Biham, E. (1994). New types of cryptanalytic attacks using related keys. *Journal of Cryptology, 7*(4): 229-246.

Biham, E. (1995). *On Matsui's linear cryptanalysis*.Advances in Cryptology□² EUROCRYPT'94.

Biham, E., Anderson, R., & Knudsen, L. (1998). *Serpent: A new block cipher proposal*.Fast Software Encryption.

Biham, E., & Shamir, A. (1992). *Differential cryptanalysis of snefru, khafre, redoc-ii, loki and lucifer*.Advances in Cryptology□²□&□5□<□3□7□2□¶□□□□□□

Biryukov, A. (2003). *Analysis of involutional ciphers: Khazad and Anubis*.Fast Software Encryption.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A. (2009). Key recovery attacks of practical complexity on AES variants with up to 10 rounds. *IACR eprint server, 374*.

Biryukov, A., & Khovratovich, D. (2009). Related-key Cryptanalysis of the Full AES-192 and AES-256 *Advances in Cryptology ±ASIACRYPT 2009* (1-18): Springer.

Bishop, M., & Matt, B. (2006). *Introduction to computer security*: Pearson Education India.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher *Cryptographic Hardware and Embedded Systems-CHES 2007* (450-466): Springer.

Bogdanov, A., Knudsen, L. R., Leander, G., Standaert, F.-X., Steinberger, J., & Tischhauser, E. (2012). Key-Alternating ciphers in a provable setting: encryption using a small number of public permutations *Advances in Cryptology ±EUROCRYPT 2012* (45-62): Springer.

Borda, M. (2011). *Fundamentals in information theory and coding*: Springer Science & Business Media.

Braeken, A. (2006). *Cryptographic properties of Boolean functions and S-boxes.* phd thesis-2006.

Callejas, D. G. (2007). Biology and Economics: Metaphors that Economists usually take from Biology. *Ecos de Economía, 11*(24): 153-164.

Canteaut, A., & Videau, M. (2005). Symmetric boolean functions. *Information Theory, IEEE Transactions on, 51*(8): 2791-2811.

Carlet, C., & Ding, C. (2007). Nonlinearities of S-boxes. *Finite Fields and Their Applications, 13*(1): 121-135.

Casakin, H. (2007). Factors of metaphors in design problem-solving: Implications for design creativity. *International Journal of Design, 1*(2): 21-33.

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

Chakraborty, D., & Sarkar, P. (2006). *A general construction of tweakable block ciphers and different modes of operations*.Information Security and Cryptology.

Chavan, S. (2013). DNA Cryptography Based on DNA Hybridization and One Time pad scheme. *International Journal of Engineering, 2*(10).

Chen, J. (2003). *A DNA-based, biomolecular cryptography design*.Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on.

Chen, S., Wang, R., Wang, X., & Zhang, K. (2010). *Side-channel leaks in web applications: A reality today, a challenge tomorrow*.Security and Privacy (SP), 2010 IEEE Symposium on.

Cheng, H., Heys, H. M., & Wang, C. (2008). *Puffin: A novel compact block cipher targeted to embedded digital systems*.Digital System Design

Architectures, Methods and Tools, 2008. DSD'08. 11th EUROMICRO Conference on.

Cook, D. L. (2006). *Elastic block ciphers.* Columbia University.

Coskun, B., & Memon, N. (2006). *Confusion/diffusion capabilities of some robust hash functions*.Information Sciences and Systems, 2006 40th Annual Conference on.

Courtois, N. T., & Bard, G. V. (2007). Algebraic cryptanalysis of the data encryption standard *Cryptography and Coding* (152-169): Springer.

Courtois, N. T., & Pieprzyk, J. (2002). Cryptanalysis of block ciphers with overdefined systems of equations *Advances in Cryptology² ASIACRYPT 2002* (267-287): Springer.

Crick, F. (1970). Central dogma of molecular biology. *Nature, 227*(5258): 561-563.

Cui, G., Qin, L., Wang, Y., & Zhang, X. (2007). *Information security technology based on DNA computing*.Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on.

Cui, G., Qin, L., Wang, Y., & Zhang, X. (2008). *An encryption scheme using DNA technology*.Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on.

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).

Cui, L., & Cao, Y. (2007). A new S-box structure named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control, 3*(3): 751-759.

D'yachkov, A. G., Erdös, P. L., Macula, A. J., Rykov, V. V., Torney, D. C., Tung, C.-S., Vilenkin, P. A., & White, P. S. (2003). Exordium for DNA codes. *Journal of Combinatorial Optimization, 7*(4): 369-379.

Daemen, J., Govaerts, R., & Vandewalle, J. (1994). *A new approach to block cipher design*.Fast Software Encryption.

Daemen, J., Knudsen, L., & Rijmen, V. (1997). *The block cipher Square*.Fast Software Encryption.

Daemen, J., & Rijmen, V. (1998a). AES proposal: Rijndael.

Daemen, J., & Rijmen, V. (1998b). *AES proposal: Rijndael*.First Advanced Encryption Standard (AES) Conference.

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

Daemen, J., & Rijmen, V. (2000). *The block cipher Rijndael*.Smart Card Research and Applications.

Daemen, J., & Rijmen, V. (2001). The wide trail design strategy *Cryptography and Coding* (222-238): Springer.

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

Daemen, J., & Rijmen, V. (2010). On the related-key attacks against AES. *status: published*.

Dalen, D. (2004). *Logic and Structure*: Springer.

Das, I., Nath, S., Roy, S., & Mondal, S. (2012). *Random S-Box generation in AES by changing irreducible polynomial*.Communications, Devices and Intelligent Systems (CODIS), 2012 International Conference on.

Dawson, M., & Tavares, S. E. (1991). *An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks*.Advances in Cryptology□²□(□8□5□2□&□5□<□3□7□¶□□□□□□

□'□H□□ □&□D□Q□Q□L□H□U□H□□□□ □&□□□□□□ □'□X□Q□N□H□O□P□D□Q□□□□ KTANTAN□²a family of small and efficient hardware-oriented block ciphers *Cryptographic Hardware and Embedded Systems-CHES 2009* (272-288): Springer.

Dewangan, C. P., & Agrawal, S. (2012). A Novel Approach to Improve Avalanche Effect of AES Algorithm. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1*(8): pp: 248-252.

□'□,□)□'□/□-□2□+□□□□□*□□□□□,□□□□□(□□□□□7□□□□□%□□□□□□□(□%□8□%□□ UIF, O. Q. B. European Bioinformatics Institute. *Research at a Glance 2014*: 77.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on, 22*(6): 644-654.

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

Dorigo, M., & Gambardella, L. M. (1997). Ant colony system: a cooperative learning approach to the traveling salesman problem. *Evolutionary Computation, IEEE Transactions on, 1*(1): 53-66.

Doroshenko, S., Fionov, A., Lubkin, A., Monarev, V., Ryabko, B., & Shokin, Y. I. (2008). Experimental Statistical Attacks on Block and Stream Ciphers *Computational Science and High Performance Computing III* (155-164): Springer.

El-Ramly, S., El-Garf, T., & Soliman, A. (2001). *Dynamic generation of S-boxes in block cipher systems*.Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National.

El-Sheikh, H. M., El-Mohsen, O. A., Elgarf, T., & Zekry, A. A New Approach for Designing Key-Dependent S-Box Defined over GF (2 4) in AES.

El-Sheikh, H. M., El-Mohsen, O. A., Elgarf, T., & Zekry, A. (2012). A new approach for designing key-dependent S-box defined over GF (2 4) in AES. *International Journal of Computer Theory and Engineering, 4*(2): 158-164.

El Shafee, A. (2012). A 64 bits Dynamically Key Controlled Symmetric Cipher (KAMFEE-X64). *International Journal of Computer Applications, 57*.

Elbirt, A. J. (2009). *Understanding and applying cryptography and data security*: Auerbach Publications.

Elkamchouchi, H., & Elshafee, A. (2003). *Dynamically key-controlled symmetric block cipher KAMFEE*.Radio Science Conference, 2003. NRSC 2003. Proceedings of the Twentieth National.

ElKamchouchi, H., & ElShafee, A. (2007). *New Rotor Based Symmetric Cipher*.Signal Processing and Communications, 2007. ICSPC 2007. IEEE International Conference on.

ElKamchouchi, H., & ElShafee, A. (2008). *URESC, Unbalanced Rotor Enhanced Symmetric Cipher*.Electrotechnical Conference, 2008. MELECON 2008. The 14th IEEE Mediterranean.

Elkamchouchi, H., & Makar, M. (2004). *Kamkar symmetric block cipher*.Radio Science Conference, 2004. NRSC 2004. Proceedings of the Twenty-First National.

ElShafee, A. (2012). KAMFEE-X64 Cipher. *International Journal of Computer Science & Network Security, 12*(10).

ElShafee, A. (2013). A 64 BITS ROTOR ENHANCED BLOCK CIPHER (REBC3). *International Journal of Network Security & Its Applications, 5*(2).

Elumalai, R., & Reddy, A. R. (2011). Improving diffusion power of AES Rijndael with 8x8 MDS matrix. *International Journal on Computer Science & Engineering, 3*(1).

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

Feistel, H. (1973). Cryptography and computer privacy. *Scientific american, 228*: 15-23.

Feistel, H., Notz, W. A., & Smith, J. L. (1975). Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE, 63*(11): 1545-1554.

Feldman, J., & Narayanan, S. (2004). Embodied meaning in a neural theory of language. *Brain and language, 89*(2): 385-392.

FIPS, P. (2001). 197: Advanced encryption standard (AES). *National Institute of Standards and Technology*.

Fujiwara, A., Matsumoto, K.-i., & Chen, W. (2003). *Addressable procedures for logic and arithmetic operations with DNA strands*.Parallel and Distributed Processing Symposium, 2003. Proceedings. International.

Gao, Q. (2011). *A few DNA-based security techniques*.Systems, Applications and Technology Conference (LISAT), 2011 IEEE Long Island.

Gao, S., Ma, W., & Zhu, J. (2012). Nonlinearity Profile Test for an S-Box *Future Wireless Networks and Information Systems* (639-644): Springer.

Gehani, A., LaBean, T., & Reif, J. (1999). *DNA-based cryptography*.5th DIMACS workshop on DNA Based Computers, MIT.

Geng, X., Pan, L., & Xu, J. (2008). A DNA sticker algorithm for bit-substitution in a block cipher. *Journal of Parallel and Distributed Computing, 68*(9): 1201-1206.

Gong, G., Tan, Y., & Zhu, B. Enhanced Criteria on Differential Uniformity and Nonlinearity of Cryptographically Significant Functions.

Gong, Z., Nikova, S., & Law, Y. W. (2012). KLEIN: a new family of lightweight block ciphers *RFID. Security and Privacy* (1-18): Springer.

Goodrich, M., & Tamassia, R. (2010). *Introduction to computer security*: Addison-Wesley Publishing Company.

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

Gupta, K. C., & Ray, I. G. (2013). On constructions of MDS matrices from companion matrices for lightweight cryptography *Security Engineering and Intelligence Informatics* (29-43): Springer.

Gustafson, H., Dawson, E., & Caelli, B. (1990). *Comparison of block ciphers*.Advances in Cryptology□²AUSCRYPT'90.

Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1991). *A secret key cryptosystem by iterating a chaotic map*.Advances in Cryptology□² □(□8□5□2□&□5□<□3□7□¶□□□□□□

Hagan, M. T., Demuth, H. B., & Beale, M. H. (1996). *Neural network design*: Pws Pub. Boston.

Heider, D., & Barnekow, A. (2007). DNA-based watermarks using the DNA-Crypt algorithm. *BMC bioinformatics, 8*(1): 176.

Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia, 26*(3): 189-221.

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

Hsu, H., & Lee, R. (2006). *Dna based encryption methods*.The 23rd Workshop on Combinatorial Mathematics and Computation Theory, National Chi Nan University Puli, Nantou Hsies, Taiwan.

Hussain, I., Shah, T., Gondal, M. A., & Khan, W. A. (2011). Construction of cryptographically strong 8× 8 S-boxes. *World Appl. Sci. J, 13*(11): 2389-2395.

Hussain, U. N., Chithralekha, T., Raj, A. N., Sathish, G., & Dharani, A. (2012). Hybrid DNA Algorithm for DES using Central Dogma of Molecular Biology (CDMB). *International Journal of Computer Applications, 42*.

Ismil, I., Galal-Edeen, G. H., Khattab, S., & BAHTITY, M. A. E. I. M. (2012). Performance examination of aes encryption algorithm with constant and dynamic rotation. *International Journal of Reviews in Computing, 12*.

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

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

Junod, P., & Vaudenay, S. (2005). *FOX: a new family of block ciphers*.Selected Areas in Cryptography.

Juremi, J., Mahmod, R., & Sulaiman, S. (2012). *A proposal for improving AES S-box with rotation and key-dependent*.Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on.

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

Kandel, E. R. (2001). The molecular biology of memory storage: a dialogue between genes and synapses. *Science, 294*(5544): 1030-1038.

Kartalopoulos, S. V. (2005). *DNA-inspired cryptographic method in optical communications, authentication and data mimicking*.Military Communications Conference, 2005. MILCOM 2005. IEEE.

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

Kazlauskas, K., & Kazlauskas, J. (2009). Key-dependent S-box generation in AES block cipher system. *Informatica, 20*(1): 23-34.

Kazymyrov, O., & Kazymyrova, V. Extended Criterion for Absence of Fixed Points.

Kazymyrov, O., Kazymyrova, V., & Oliynykov, R. A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent.

Keliher, L., & Meijer, H. (1997). A New Substitution-Permutation Network Cipher Using Key-Dependent S-Boxes.

Knudsen, L., Leander, G., Poschmann, A., & Robshaw, M. J. (2010). PRINTcipher: a block cipher for IC-printing *Cryptographic Hardware and Embedded Systems, CHES 2010* (16-32): Springer.

Knudsen, L. R., & Robshaw, M. (2011). The Block Cipher Companion. Information security and cryptography. *Springer, 6*: 17-35.

Kocarev, L., & Lian, S. (2011). *Chaos-based cryptography*: Springer.

Krishnamurthy, G., & 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.

Kruppa, H., & Shahy, S. U. A. (1998). Differential and Linear Cryptanalysis in Evaluating AES Candidate Algorithms.

Kwon, D., Kim, J., Park, S., Sung, S. H., Sohn, Y., Song, J. H., Yeom, Y., Yoon, E.-J., Lee, S., & Lee, J. (2004). New block cipher: ARIA *Information Security and Cryptology-ICISC 2003* (432-445): Springer.

Labarga, A., Valentin, F., Anderson, M., & Lopez, R. (2007). Web services at the European bioinformatics institute. *Nucleic acids research, 35*(suppl 2): W6-W11.

Lai, X. (1992). *On the design and security of block ciphers.* Diss. Techn. Wiss ETH Zürich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. Bühlmann.

Lai, X., Massey, J. L., & Murphy, S. (1991). *Markov ciphers and differential cryptanalysis*.Advances in Cryptology□²□(□8□5□2□&□5□<□3□7□¶□□□□□□

law Szaban, M., & Seredynski, F. CA-based S-boxes for Secure Ciphers.

Leier, A., Richter, C., Banzhaf, W., & Rauhe, H. (2000). Cryptography with DNA binary strands. *BioSystems, 57*(1): 13-22.

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

Lim, C. H. (1998). CRYPTON: A new 128-bit block cipher. *NIsT AEs Proposal*.

Lim, C. H., & Korkishko, T. (2006). mCrypton□A lightweight block cipher for security of low-cost RFID tags and Sensors *Information Security Applications* (243-258): Springer.

Limin, F., Dengguo, F., & Yongbin, Z. (2008). A fuzzy-based randomness evaluation model for block cipher. *Journal of Computer Research and Development, 45*(12): 2095-2010.

Lipton, R. J. (1996). Breaking DBS Using a Molecular Computer Dan Boneh Christopher Dimworth. *DNA based computers, 27*: 37.

Liskov, M., Rivest, R. L., & Wagner, D. (2002). Tweakable block ciphers *Advances in Cryptology ² CRYPTO 2002* (31-46): Springer.

Liu, F., Ji, W., Hu, L., Ding, J., Lv, S., Pyshkin, A., & Weinmann, R.-P. (2007). *Analysis of the SMS4 block cipher*.Information Security and Privacy.

MacWilliams, F. J., & Sloane, N. J. A. (1977). *The theory of error-correcting codes* (Vol. 16): Elsevier.

Makinson, D. (2012). *Sets, logic and maths for computing*: Springer.

Mala, H., Dakhilalian, M., Rijmen, V., & Modarres-Hashemi, M. (2010). Improved impossible differential cryptanalysis of 7-round AES-128 *Progress in Cryptology-INDOCRYPT 2010* (282-291): Springer.

Malik, M. Y., & No, J.-S. (2011). Dynamic MDS Matrices for Substantial Cryptographic Strength. *arXiv preprint arXiv:1108.6302*.

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

Massey, J. L. (1994). *SAFER K-64: A byte-oriented block-ciphering algorithm*.Fast Software Encryption.

Masuda, N., Jakimoski, G., Aihara, K., & Kocarev, L. (2006). Chaotic block ciphers: from theory to practical algorithms. *Circuits and Systems I: Regular Papers, IEEE Transactions on, 53*(6): 1341-1352.

Mathur, C. N., Narayan, K., & Subbalakshmi, K. (2006). *High diffusion cipher: Encryption and error correction in a single cryptographic primitive*.Applied Cryptography and Network Security.

Matsui, M. (1994a). *The first experimental cryptanalysis of the Data Encryption Standard*.Advances in Cryptology□²□&□U□\□S□W□R□¶□□□□□□

Matsui, M. (1994b). *Linear cryptanalysis method for DES cipher*.Advances in Cryptology□²□(□8□5□2□&□5□<□3□7□¶□□□□□□

Meier, W., & Staffelbach, O. (1990). *Nonlinearity criteria for cryptographic functions*.Advances in Cryptology□²□(□8□5□2□&□5□<□3□7□¶□□□□□□

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST Special Publication, 800*(145): 7.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*: CRC press.

Merkle, R. C. (1991). Fast software encryption functions *Advances in Cryptology- & 5 < 3 7* ¶(477-501): Springer.

Mihajloska, H., & Gligoroski, D. (2012). *Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4*.SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies.

Minematsu, K. (2009). *Beyond-birthday-bound security based on tweakable block cipher*.Fast Software Encryption.

Mister, S., & Adams, C. (1996). *Practical S-box design*.Workshop on Selected Areas in Cryptography, SAC.

Mohan, H., Reddy, A. R., & Manjunath, T. (2011). Improving the Diffusion power of AES Rijndael with key multiplication. *International Journal of Computer Applications, 30*.

Murphy, S., & Robshaw, M. (2003). Comments on the Security of the AES and the XSL Technique. *Electronic Letters, 39*(1): 36-38.

Murphy, S., & Robshaw, M. J. B. (2002). Key-dependent S-boxes and differential cryptanalysis. *Designs, Codes and Cryptography, 27*(3): 229-255.

Murtaza, G., & Ikram, N. (2008). New Methods of Generating MDS Matrices. *Proceedings of ICWC*: 129-133.

Murtaza, G., Khan, A. A., Alam, S. W., & Farooqi, A. (2011). Fortification of AES with Dynamic Mix-Column Transformation. *IACR Cryptology ePrint Archive, 2011*: 184.

Nawaz, Y. (2004). Cryptanalysis of Block Ciphers.

Nechvatal, J., Barker, E., Bassham, L., Burr, W., & Dworkin, M. (2000). Report on the development of the Advanced Encryption Standard (AES): DTIC Document.

Ning, K. (2009). A pseudo DNA cryptography method. *arXiv preprint arXiv:0903.2693*.

NIST Computer Security Division's (CSD) Security Technology Group (STG). ((2013), , Last updated: December 26, 2013 ). "Block cipher modes". *Cryptographic Toolkit. NIST. .* Page created: January 25, 2001. 2013, , from http://csrc.nist.gov/groups/ST/toolkit/BCM/index.html

Nyberg, K. (1994). *Differentially uniform mappings for cryptography*.Advances in cryptology□²□(□X□U□R□F□U□\□S□W□¶□□□□□□

Ojha, S. K., Kumar, N., & Jain, K. (2009). TWIS□A Lightweight Block Cipher *Information Systems Security* (280-291): Springer.

Özkaynak, F., & Özer, A. B. (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. *Physics Letters A, 374*(36): 3733-3738.

Patidar, V., Sud, K. K., & Pareek, N. K. (2009). A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing. *Informatica (03505596), 33*(4).

Peng, J., Jin, S., Lei, L., & Liao, X. (2012). *Construction and analysis of dynamic S-boxes based on spatiotemporal chaos*.Cognitive Informatics & Cognitive Computing (ICCI* CC), 2012 IEEE 11th International Conference on.

Pieprzyk, J., & Finkelstein, G. (1988). Towards effective nonlinear cryptosystem design. *Computers and Digital Techniques, IEE Proceedings E, 135*(6): 325-335.

Poschmann, A., Leander, G., Schramm, K., & Paar, C. (2007). *New Light-Weight Crypto Algorithms for RFID*.ISCAS.

Prabhu, D., & Adimoolam, M. (2011). Bi-serial DNA Encryption Algorithm (BDEA). *arXiv preprint arXiv:1101.2577*.

Pradeep, L., & Bhattacharjya, A. (2013). Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks *Security in Computing and Communications* (63-69): Springer.

Pub, N. F. 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, November 26, 2001. Available from the NIST website.

Ramanujam, S., & Karuppiah, M. (2011a). Designing an algorithm with high avalanche effect. *IJCSNS, 11*(1): 106.

Ramanujam, S., & Karuppiah, M. (2011b). Designing an algorithm with high avalanche effect. *IJCSNS International Journal of Computer Science and Network Security, 11*(1): 106-111.

RezaeiPour, D., Said, M. R., & Rushdan, M. (2009). New Directions in Cryptanalysis of Block Ciphers. *Journal of Computer Science, 5*(12): 1091.

Rijmen, V. (1997). *Cryptanalysis and design of iterated block ciphers.* Doctoral Dissertation, October 1997, KU Leuven.

Rijmen, V. (2013). Introduction to Design & Cryptanalysis of Block Ciphers. *status: published*.

Rijmen, V., & Daemen, J. (1998). *AES proposal: Rijndael.*1st AES Conference.

Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., & De Win, E. (1996). *The cipher SHARK*.Fast Software Encryption.

Ritter, T. (1991). Transposition cipher with pseudo-random shuffling: The dynamic transposition combiner. *Cryptologia, 15*(1): 1-17.

Rogaway, P. (2011). Evaluation of some blockcipher modes of operation. *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*.

Rukhin, A., Soto, J., Nechvatal, J., Barker, E., Leigh, S., Levenson, M., Banks, D., Heckert, A., Dray, J., & Vo, S. (2010). Statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications: DTIC Document.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2008). A statistical test suite for random and pseudorandom number generators for cryptographic applications: DTIC Document.

Sadeg, S., Gougache, M., Mansouri, N., & Drias, H. (2010). *An encryption algorithm inspired from DNA*.Machine and Web Intelligence (ICMWI), 2010 International Conference on.

Schneier, B. (1994). The Blowfish encryption algorithm. *Dr Dobb's Journal-Software Tools for the Professional Programmer, 19*(4): 38-43.

Schneier, B. (1996). Applied cryptography: protocols, algorithms, and source code in C: John Wiley & Sons, Inc.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*: john wiley & sons.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*: Wiley. com.

Schneier, B., & Kelsey, J. (1996). *Unbalanced Feistel networks and block cipher design*.Fast Software Encryption.

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

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1999). *The Twofish encryption algorithm: a 128-bit block cipher*: John Wiley & Sons, Inc.

Seredynski, M., & Bouvry, P. (2005). Block cipher based on reversible cellular automata. *New Generation Computing, 23*(3): 245-258.

Shannon, C. E. (1949a). Communication theory of secrecy systems. *Bell system technical journal, 28*(4): 656-715.

Shannon, C. E. (1949b). Communication Theory of Secrecy Systems*. *Bell system technical journal, 28*(4): 656-715.

Shaw, H., & Hussein, S. (2008). *A DNA-Inspired Encryption Methodology for Secure, Mobile Ad-Hoc Networks (MANET)* ûProceedings of the First International Conference on Biomedical Electronics and Devices, BIOSIGNALS.

Shimoyama, T., Yanami, H., Yokoyama, K., Takenaka, M., Itoh, K., Yajima, J., Torii, N., & Tanaka, H. (2002). *The block cipher SC2000*.Fast Software Encryption.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., & Iwata, T. (2007). *The 128-bit blockcipher CLEFIA*.Fast software encryption.

Shirey, R. (2000). RFC 2828: Internet security glossary. *The Internet Society*.

Shyam, M., Kiran, N., & Maheswaran, V. (2007). *A novel encryption scheme based on DNA computing*.14th IEEE International Conference.

Simplicio Jr, M., Barreto, P. S., Carvalho, T. C., Margi, C. B., & Näslund, M. (2008). The CURUPIRA-2 block cipher for constrained platforms: Specification and benchmarking.

Singh, H., Chugh, K., Dhaka, H., & Verma, A. (2010). DNA based Cryptography: an Approach to Secure Mobile Networks. *International Journal of Computer Applications, 1*(19).

Singh, S. (2011). *The code book: the science of secrecy from ancient Egypt to quantum cryptography*: Random House Digital, Inc.

Sisalem, D., Floroiu, J., Kuthan, J., Abend, U., & Schulzrinne, H. (2009). *SIP security*: John Wiley & Sons.

Soto, J., & Bassham, L. (1999). *Randomness testing of the advanced encryption standard candidate algorithms*: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Soto, J., & Bassham, L. (2000). Randomness testing of the advanced encryption standard finalist candidates: DTIC Document.

Stallings, W. (2010). Network security essentials: Prentice Hall (2nd edition 2002).

Standaert, F.-X., Piret, G., Rouvroy, G., Quisquater, J.-J., & Legat, J.-D. (2004). *ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware*.Fast Software Encryption.

Standard, D. E. (1977). FIPS PUB 46. *Appendix A, Federal Information Processing Standards Publication*.

Stoianov, N. (2010). One software tool for testing square s-boxes. *arXiv preprint arXiv:1009.2476*.

Sulaiman, S., Muda, Z., Juremi, J., Mahmod, R., & 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): 160-166.

Sumathy, V., & Navaneethan, C. (2013). Enhanced AES Algorithm for Strong Encryption. *International Journal of Computer Science & Network Security, 13*(8).

Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, E. (2013). \ *textnormal {\ textsc {TWINE}}: A Lightweight Block Cipher for Multiple Platforms*.Selected Areas in Cryptography.

Tan, Y., GONG, G., & Zhu, B. (2015). Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions.

Taylor, R. (1990). Interpretation of the correlation coefficient: a basic review. *Journal of diagnostic medical sonography, 6*(1): 35-39.

Terec, R., Vaida, M.-F., Alboaie, L., & Chiorean, L. (2011a). DNA Security using Symmetric and Asymmetric Cryptography. *International Journal of New Computer Architectures and Their Applications (IJNCAA), 1*(1): 34-51.

Terec, R., Vaida, M.-F., Alboaie, L., & Chiorean, L. (2011b). DNA Security using Symmetric and Asymmetric Cryptography. *International Journal of New Computer Architectures and Their Applications (IJNCAA), 1*(1): 35-51.

Torkaman, N., Reza, M., Kazazi, N. S., & Rouddini, A. (2012). Innovative Approach to Improve Hybrid Cryptography by Using DNA Steganography. *International Journal of New Computer Architectures & their Applications, 2*(1).

Venkaiah, V. C., Srinathan, K., & Bruhadeshwar, B. (2006). Variations to S-box and MixColumn Transformations of AES: Technical Report, Deemed University.

Vergili, I., & Yücel, M. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen× S-Boxes. *Turk J Elec Engin, 9*(2): 137-145.

Wang, X.-y., & Yu, Q. (2009). A block encryption algorithm based on dynamic sequences of multiple chaotic systems. *Communications in Nonlinear Science and Numerical Simulation, 14*(2): 574-581.

Wang, X., Zhang, Q., & Wei, X. P. (2010). A New Encryption Method Based on Rijndael Algorithm and DNA Computing. *Applied Mechanics and Materials, 20*: 1241-1246.

Wang, Y., Wong, K.-W., 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.

Webster, A., & Tavares, S. E. (1986). *On the design of S-boxes*.Advances in Cryptology□²□&□5□<□3□7□2□¶□□□□□□□3□U□R□F□H□H□G□L□Q□J□V□□

Wei, P., Yang, H., Hang, Q., & Shi, X. (2011). A Novel Block Encryption Based on Chaotic Map *Intelligent Computing and Information Science* (360-367): Springer.

Weinmann, R.-P. (2006). *The SMS4 Block Cipher*.5. Krypto-Tag□Workshop über Kryptographie Universität Kassel.

Wen, Q.-y., Niu, X., & Yang, Y. (2000). The Boolean Functions in modern cryptology: Beijing: Science Press.

William, S. (2008). *Network security essentials*: Pearson Education India.

William, S., & Stallings, W. (2006). *Cryptography and Network Security, 4/E*: Pearson Education India.

Williamson, M. M. (2002). Biologically inspired approaches to computer security. *Information Infrastructure Laboratory, HP Laboratories Bristol*.

Wong, K. (2010). Interpretation of correlation coefficients. *Hong Kong Medical Journal, 16*: 237.

Wu, S., & Wang, M. (2011). Security Evaluation against Differential Cryptanalysis for Block Cipher Structures. *IACR Cryptology ePrint Archive, 2011*: 551.

Wu, W., & Zhang, L. (2011). *LBlock: a lightweight block cipher*.Applied Cryptography and Network Security.

Wu, Y., Noonan, J. P., & Agaian, S. (2010). *Binary data encryption using the Sudoku block cipher*.Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on.

Xiang, T., Liao, X., Tang, G., Chen, Y., & Wong, K.-w. (2006). A novel block cryptosystem based on iterating a chaotic map. *Physics Letters A, 349*(1): 109-115.

Xiao-Jun, T., Zhu, W., & Ke, Z. (2012). A novel block encryption scheme based on chaos and an S-box for wireless sensor networks. *Chinese Physics B, 21*(2): 020506.

Xiao, G., Lu, M., Qin, L., & Lai, X. (2006). New field of cryptography: DNA cryptography. *Chinese Science Bulletin, 51*(12): 1413-1420.

Yunpeng, Z., Yu, Z., Zhong, W., & Sinnott, R. O. (2011). *Index-based symmetric DNA encryption algorithm*.Image and Signal Processing (CISP), 2011 4th International Congress on.

Zhang, M., Cheng, M. X., & Tarn, T.-J. (2006). A mathematical formulation of DNA computation. *NanoBioscience, IEEE Transactions on, 5*(1): 32-40.

Zhang, M., Sabharwal, C. L., Tao, W., Tarn, T.-J., Xi, N., & Li, G. (2004). Interactive DNA sequence and structure design for DNA nanoapplications. *NanoBioscience, IEEE Transactions on, 3*(4): 286-292.

Zhang, Q., Guo, L., Xue, X., & Wei, X. (2009). *An image encryption algorithm based on DNA sequence addition operation*.Bio-Inspired Computing, 2009. BIC-TA'09. Fourth International Conference on.

Zhang, Q., & Liu, L. (2013). DNA Coding and Chaos-Based Image Encryption Algorithm. *Journal of Computational and Theoretical Nanoscience, 10*(2): 341-346.

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

Zhang, W., Wu, W., & Feng, D. (2007). New results on impossible differential cryptanalysis of reduced AES *Information Security and Cryptology-ICISC 2007* (239-250): Springer.

Zhonglin, H., & Zhihua, H. (2011). *A New Method for Impossible Differential Cryptanalysis of 8-Round AES-128*.Intelligence Information Processing and Trusted Computing (IPTC), 2011 2nd International Symposium on.

Zhou, Q., Liao, X., Wong, K.-w., Hu, Y., & Xiao, D. (2009). True random number generator based on mouse movement and chaotic hash function. *information sciences, 179*(19): 3442-3450.