EFFICIENT DYNAMIC DNA-BASED BLOCK CIPHER ALGORITHM

By

CHNG CHERN WEI

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

July 2023

FSKTM 2023 2

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

EFFICIENT DYNAMIC DNA-BASED BLOCK CIPHER ALGORITHM

By

CHNG CHERN WEI

July 2023

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

The significance of block cipher algorithms lies in their versatility and resilience. They possess a wide range of applications, spanning from guaranteeing the security of web traffic through protocols like SSL/TLS to encrypting confidential data stored on hard drives. Block ciphers are designed with a specific focus on maximising speed and efficiency, making them highly suitable for use in both hardware and software systems. Ensuring sufficient non-linearity is a crucial factor in the design of S-Box. The use of non-linear S-Box is essential in preventing linear approximations that could lead to successful attacks, such as differential cryptanalysis. This form of assault exploits the correlations between changes in the input and their effects on the output. When an S-box displays a high degree of linearity, it becomes vulnerable to these assaults, hence undermining the security of the cipher and making it easier to decipher. ShiftRow and MixColumns are essential for achieving the required dispersion and obfuscation in a safe block cipher. Nevertheless, they provide unique challenges in relation to security.

Consequently, a Dynamic DNA-based S-box was proposed to enhance the non-linearity of the S-Box. The utilisation of four sets of 4 x 4 S-Box structures contributes to the simplicity and stability of the S-Box construction. The proposed method involves utilising DNA-based components consisting of the nucleotides {A, T, G, C} to generate a novel Dynamic DNA-based S-Box. The suggested method enhances the non-linearity of the S-Box, offering a dynamic solution that effectively defends against linear and differential cryptanalysis.

Additionally, a DNA-based ShiftRow function was proposed to enhance the execution of permutation by methodically displacing the rows of the state array using different offset values. This outcome is characterised by a linear procedure and lacks the ability to combine data from multiple rows. The suggested

ShiftRows algorithm utilises DNA-specific characteristics of the nucleotides {A, T, G, C}. The ShiftRow operation in this system, which is based on DNA, operates as a pseudo-random number generator. It generates encrypted random numbers for the encryption process. To guarantee that the random numbers generated by this DNA-based block cipher satisfy particular requirements and specifications, all values and parameters will conform to the standards established by the National Institute of Standards and Technology (NIST).

Moreover, a DNA-based MixColumns function was proposed to enhance the linear transformation executed in a finite field by employing fixed polynomials and preventing vulnerability to linear and differential attacks. The proposed MixColumns operation is designed to incorporate the unique characteristics of DNA, specifically the nucleotides {A, T, G, C}. The DNA-based MixColumns operation functions as a pseudo-random number generator, generating an encrypted random number for the purpose of encryption. In order to guarantee that the random numbers produced by the suggested DNA-based block cipher satisfy the necessary criteria, all values and parameters will conform to the requirements established by the National Institute of Standards and Technology (NIST).

Finally, the findings confirm that the proposed approaches have demonstrated enhancements, such as passing the randomness test, exhibiting the avalanche effect, and withstanding cryptanalysis. In general, the research has demonstrated encouraging evidence of the DNA-based block cipher's ability to enhance security and withstand linear and differential attacks.

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

ALGORITMA SIFIR BLOK YANG CEKAP BERASASKAN DINAMIK DNA

Oleh

CHNG CHERN WEI

Julai 2023

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

Kepentingan algoritma block cipher terletak pada kepelbagaian dan ketahanannya. Mereka memiliki pelbagai aplikasi, merentasi dari menjamin keselamatan trafik web melalui protokol seperti SSL/TLS hingga mengenkripsi data rahsia yang disimpan pada cakera keras. Block cipher direka dengan fokus khusus pada memaksimumkan kelajuan dan kecekapan, menjadikannya sangat sesuai untuk digunakan dalam sistem perkakasan dan perisian. Memastikan kecukupan bukan linear adalah faktor penting dalam reka bentuk S-Box. Penggunaan S-Box bukan linear adalah penting dalam mencegah penghampiran linear yang boleh membawa kepada serangan yang berjaya, seperti kriptanalisis berbeza. Bentuk serangan ini mengeksploitasi korelasi antara perubahan dalam input dan kesan mereka pada output. Apabila S-box menunjukkan tahap lineariti yang tinggi, ia menjadi rentan terhadap serangan ini, dengan itu menggugat keselamatan cipher dan menjadikannya lebih mudah untuk dipecahkan. ShiftRow dan MixColumns adalah penting untuk mencapai penyebaran dan pengaburan yang diperlukan dalam block cipher yang selamat. Namun, mereka menyediakan cabaran unik berkaitan dengan keselamatan.

Akibatnya, S-Box berasaskan DNA Dinamik telah dicadangkan untuk meningkatkan bukan lineariti S-Box. Penggunaan empat set struktur S-Box 4 x 4 menyumbang kepada kesederhanaan dan kestabilan pembinaan S-Box. Kaedah yang dicadangkan melibatkan penggunaan komponen berasaskan DNA yang terdiri daripada nukleotida {A, T, G, C} untuk menghasilkan S-Box berasaskan DNA Dinamik yang baru. Kaedah yang dicadangkan meningkatkan bukan lineariti S-Box, menawarkan penyelesaian dinamik yang berkesan melawan kriptanalisis linear dan berbeza.

Selain itu, fungsi ShiftRow berasaskan DNA telah dicadangkan untuk meningkatkan pelaksanaan permutasi dengan menggeser baris array keadaan

menggunakan nilai offset yang berbeza. Hasil ini dicirikan oleh prosedur linear dan kekurangan kemampuan untuk menggabungkan data dari beberapa baris. Algoritma ShiftRows yang dicadangkan menggunakan ciri-ciri khusus DNA nukleotida {A, T, G, C}. Operasi ShiftRow dalam sistem ini, yang berasaskan DNA, berfungsi sebagai penjana nombor rawak semu. Ia menghasilkan nombor rawak yang disulitkan untuk proses penyulitan. Untuk memastikan bahawa nombor rawak yang dihasilkan oleh block cipher berasaskan DNA ini memenuhi keperluan dan spesifikasi tertentu, semua nilai dan parameter akan mematuhi piawaian yang ditetapkan oleh Institut Standard dan Teknologi Kebangsaan (NIST).

Selanjutnya, fungsi MixColumns berasaskan DNA telah dicadangkan untuk meningkatkan transformasi linear yang dilaksanakan dalam medan terhingga dengan menggunakan polinomial tetap dan mengelakkan kerentanan terhadap serangan linear dan berbeza. Operasi MixColumns yang dicadangkan direka untuk menggabungkan ciri-ciri unik DNA, khususnya nukleotida {A, T, G, C}. Operasi MixColumns berasaskan DNA berfungsi sebagai penjana nombor rawak semu, menghasilkan nombor rawak yang disulitkan untuk tujuan penyulitan. Untuk memastikan bahawa nombor rawak yang dihasilkan oleh block cipher berasaskan DNA yang dicadangkan memenuhi kriteria yang diperlukan, semua nilai dan parameter akan mematuhi keperluan yang ditetapkan oleh Institut Standard dan Teknologi Kebangsaan (NIST).

Akhirnya, penemuan mengesahkan bahawa pendekatan yang dicadangkan telah menunjukkan peningkatan, seperti lulus ujian rawak, menunjukkan kesan avalanche, dan bertahan terhadap kriptanalisis. Secara umum, penyelidikan telah menunjukkan bukti yang menggalakkan mengenai kemampuan block cipher berasaskan DNA untuk meningkatkan keselamatan dan bertahan terhadap serangan linear dan berbeza.

ACKNOWLEDGEMENTS

I would like to begin by expressing my sincere gratitude and appreciation to my supervisor, Dr. Sharifah Bte Md. Yasin, as well as Associate Professor Dr. Nur Izura Binti Udzir and Associate Professor Dr. Mohd. Taufik Abdullah. Their invaluable assistance, advice, comments, and dedication of time have greatly contributed to the progress and success of this research endeavour. Through the guidance and support of knowledgeable individuals, I developed the essential self-assurance to effectively accomplish this research project within the designated time range.

I would like to express my sincere appreciation to Master Skill Tech Enterprise and Bites & Bytes Network for their considerable assistance.

Finally, I would like to express my appreciation to my parents, Mdm. Ewe Suan Kim and Ms. Soo Moong Wei and Chng Jia Qian, as well as my companions, for their consistent support and motivation.

I would want to extend my appreciation for the support you have provided.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Sharifah bte Md. Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

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

Mohd Taufik bin Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 8 February 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

UPM	Universiti Putra Malaysia
°C	degree Celsius
DNA	Deoxyribonucleic acid
MSB	Most significant bit
LSB	Least significant bit
NIST	National Institute of Standards and Technology
AES	Advanced Encryption Standard
ECB	Electronic Code Book
IOT	Internet of Things
PCR	Polymerase Chain Reaction
DES	Data Encryption Standard
DNA-PKC	DNA Public Key Cryptography
DNASC	DNA Signature System
DNA	Deoxyribonucleic acid
MSB	Most significant bit
LSB	Least significant bit

CHAPTER 1

INTRODUCTION

1.1 Introduction

The advent of advanced communication channels has endowed our civilization with the capacity to engage in rapid and secure communication. In the pursuit of enhancing communication security, researchers in the field of computer security from many academic institutions worldwide continue to explore and develop more effective approaches. In order to accomplish this goal, researchers in the field of cryptography continue to investigate security techniques with the aim of enhancing the security of vulnerable communication channels. In order to develop a highly effective cognitive algorithm for secure communication, it is imperative for researchers to thoroughly consider all pertinent elements of digital security. Of particular importance is the recognition that the primary goal of digital security is to serve as a standard against which performance may be measured (Saravanan & Kumar, 2018).

Upon the user's submission of data to the network, the data will undergo a transformation into a publicly accessible state, subsequently being permanently kept on the server. The tracking and consolidation of individual personal data, as well as its subsequent analysis, will persist through the involvement of third-party entities.

Cryptography has the capability to offer safeguarding measures for data and information that are being communicated across a network. The transmission of data, such as video, audio, or text, can be safeguarded to ensure the protection of privacy, ambiguity, and the overall security of human communication channels (Schneider, 2015).

The symmetric block cipher algorithm is well recognized as a prominent cryptographic technique within the field of cryptography due to its notable attributes of simplicity, speed, and robustness. Symmetric block cipher algorithms are widely utilized in the realm of information security systems, particularly in the context of cloud storage services. The utilization of symmetric block encryption is employed for the purpose of both encrypting and decrypting data throughout its storage (Kamara & Papamanthou, 2013).

Joan Daemen together with Vincent Rijmen developed an AES block cipher with a block size of 128 bits or sixteen bytes. The key size for AES cipher has three types which is consist of 128 bits, 192 bits or 256 bits, which is sixteen bytes, twenty-four bytes, or thirty-two bytes (Daemen, Daemen, Rijmen, Rijmen, & Leuven, 1999) and (Khamis, 2019). AES is popular used block cipher today to protect data, especially widely used in the social media industry as well as users' personal information.

The motivation for studying DNA-based block cipher stems from the necessity for innovative and effective approaches to tackle the increasing intricacies of data security risks. Amidst the increasing computational capabilities and advanced approaches, classic cryptographic systems face challenges. However, DNA-based block cipher emerges as a promising and unique solutions. The deep and diversified character of DNA computing enhances security. This area of research not only offers the potential to enhance data protection, but also to greatly simplify and accelerate security procedures. In the face of growing and complex cyber-attacks, DNA-based block cipher provides a proactive solution by harnessing the DNA-based capabilities of genetic coding to strengthen the digital domain for future generations.

1.2 Problem Statement

The S-Box (Elumalai & Reddy, 2011; NIST, 2001; Al-wattar, Mahmod, Zukarnain, & Udzir, 2015) is a crucial component of the 3D-DNA algorithm, is deliberately constructed to possess non-linearity and complexity in order to effectively counteract linear and differential cryptanalysis. However, the structure of the system, which consists of four sets of 4 x 4 matrices, may contain inherent weaknesses that could be prone to these specific types of attacks. The static aspect of the S-Box in the 3D-DNA method improves performance and simplicity, but it also poses significant hazards for linear and differential cryptanalysis (Ayman, 2019).

The ShiftRow function (Daemen et al., 1999; Al-wattar et al., 2015; Ali Ari, 2023) in the 3D-DNA algorithm executes permutation by systematically shifting the rows of the state array by varying offsets. While this contributes to data rearrangement within each row, the 3D-DNA ShiftRow (Ayman, 2019) remains a linear operation, lacking the capability to intermix data across different rows or columns. As a deterministic process that operates independently of any direct key material, its predictable nature could potentially be exploited by an attacker familiar with the 3D-DNA algorithm. The absence of additional complexifying steps in the algorithm means this predictability might pose a security vulnerability of linear and differential cryptanalysis.

In the 3D-DNA algorithm, the MixColumns is a linear transformation that is performed within a finite field using fixed polynomials. The diffusion components for each round encompass the MixColumns operations. This singularity indicates a diminished encryption quality, rendering the ciphertext susceptible to potential attacks. This leads to a consistent and predictable approach to byte blending. By analysing both the plaintext and its associated ciphertext, it is possible to break the linear features of MixColumns, as noted by Al-wattar et al. in 2015 and Ayman in 2019. To address this issue, a solution is proposed wherein bits are shuffled in each round using DNA-based, as suggested by Al-Wattar et al., in 2015, Ayman in 2019 and Nik Azura et al., in 2022.

1.3 Objective of the Research

The objective of this research is to design a secure DNA-based block cipher that is inspired by the human biology system. To achieve that goal, the following process will be executed.

a) To propose a new Dynamic DNA-based S-Box that it satisfies the minimum-security requirement to increase the non-linearity of the DNA-based Block Cipher.

b) To propose a DNA-based ShiftRow function, which contains DNA-based components, {A, T, G, C}, to increase the security of the DNA-based block cipher and satisfies the minimum-security requirement.

c) To propose a DNA-based MixColumns function, which contains DNA-based components, {A, T, G, C}, to increase the security of the DNA-based block cipher and satisfies the minimum-security requirement.

1.4 Scope of the Research

This research aims to produce a new proposed DNA-based block cipher and the following features to be considered:

a) 128 bits for key length;

b) 128 bits for block size length;

c) Electronic Code Book (ECB) is used as the process of controlling the encryption process for each block;

d) Proposed DNA-based block cipher are required to meet the NIST randomness tests, avalanche effects and resist against linear cryptanalysis and differential cryptanalysis for the security requirements.

1.5 Contribution of the Research

This research outcome will contribute to the following areas:

a) This study utilizes DNA-based components to develop a novel Dynamic DNA-based S-Box. The recently developed Dynamic DNA-based S-Box has demonstrated the capability to enhance the complexity associated with generating the sub-keys and state-keys within the Function Layer of the algorithm. This enhances the efficacy of memory utilization. The novel Dynamic DNA-based S-Box, which is based on DNA, utilizes the security features inherent in substitution and permutation transformations. The substitution transformation encompasses the application of substitute approaches using the newly Dynamic proposed DNA-based S-Box.

b) The newly proposed DNA-based block cipher incorporates DNA-specific features of {A, T, G, C}. The DNA-based ShiftRow operation in this system functions as a pseudo-random number generator, producing encrypted random numbers for the encryption procedure. In order to ensure that the random numbers produced by this DNA-based block cipher meet specific requirements and specifications, all values and parameters will adhere to the standards set by the National Institute of Standards and Technology (NIST). The statistical properties of the random numbers generated by the DNA-based block cipher are assessed by employing NIST's statistical testing tools. Furthermore, the avalanche effect is examined, and cryptanalysis is performed.

c) The newly proposed DNA-based block cipher integrates DNA-specific features of {A, T, G, C}. DNA-based MixColumns operation that acts as a pseudo-random number generator, creating an encrypted random number for encryption purposes. To ensure the generated random numbers from the proposed DNA-based block cipher meet the required standards, all values and parameters will adhere to the guidelines set by the National Institute of Standards and Technology (NIST). The statistical randomness of the random numbers produced by the DNA-based block cipher is evaluated using NIST's statistical test tools, alongside assessments of the avalanche effect and cryptanalysis.

1.6 Organization of the Thesis

This chapter will provide a comprehensive overview of the study objectives to be attained and delineate the scope of the investigation. This chapter serves as the first foundation for the present study. The organization of this thesis is as follows:

Chapter 2 provides an in-depth analysis of the existing literature and background research pertaining to various works that are relevant to the present inquiry. The literature review will encompass an examination of the foundational principles of cryptography, an exploration of the mechanisms underlying cryptographic techniques, and an analysis of existing research pertaining to DNA-based block cipher.

Chapter 3 provides a comprehensive exposition of the research methodologies employed in the study. This chapter will additionally address the various experimental designs to be conducted, along with the determination of the number of rotations and measurement procedures. It will also explore the comprehension, propagation, and frequency of the suggested novel DNA-based block cipher.

Chapter 4 discusses the selection of an appropriate system design for the investigation. This chapter also provides a comprehensive explanation of a newly introduced block cipher algorithm. The components encompassed within this framework consist of decision, notation and convention, as well as the early specification of the mathematical procedure and specification. Additionally, it provides verification of the employed methodology. This chapter additionally addresses the topics of algorithm encoding and execution. This phase is a critical juncture at which the established protocol will be converted into a set of controls specified using suitable computer programming language tools. Prior to executing the coding for a new system, it is imperative to do thorough testing to ensure that the implemented system is devoid of computer errors and maintains accurate logical flow.

Chapter 5 specifically examines the research results, with a special emphasis on analysing the randomness test outputs for both the DNA-based block cipher and DNA Cryptographic Algorithm. The analysis focuses on the testing outcomes of the DNA-based block cipher, utilising multiple criteria such as the Frequency Test and investigating various densities of plaintext and key (Random, Low-Density, High-Density). Furthermore, it incorporates evaluations such as the NIST Randomness Test, Avalanche Effect, Correlation Coefficient, Bit Error Analysis, and Key Sensitivity Analysis, employing distribution charts to conduct a thorough review. This chapter also focuses on the association between the branch number and key parts of linear and differential cryptanalysis, providing a more profound comprehension of the security and efficacy of the DNA-based block cipher.

Chapter 6 is the final chapter for this thesis. This chapter discusses about the conclusion of the study and future research.

1.7 Summary

This chapter offers a summary and justification for the initiation and driving forces behind the current investigation. Additionally, the researchers highlight the study's breadth and its importance to the research domain. The chapter also tackles the problem statement concerning cryptographic challenges, setting the stage for the study's objectives. It delivers an extensive outline of the research context, motivation, objectives, as well as the scope and structural organization of the thesis.

REFERENCES

Abutaha, M., Farajallah, M., Tahboub, R. & Odeh, M. (2015). Survey Paper: Cryptography is the Science of Information Security. International Journal of Computer Science and Security, Vol.(5), Issue(3), 2011.

Alabaichi, A. M. (2015). A Dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish Algorithm, Indian Journal of Science and Technology, vol. 8, no. 30, pp. 1-17.

Alabaichi, A. M., 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, 10(4), 53–57.

Ali, D., Bar, E., Onur, K., & Fatih, S. (2010). Cryptographic randomness testing of block ciphers and hash functions. Cryptology ePrint Archive, Report 2010/564.

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

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). Generating A New S-Box Inspired byBiological DNA. International Journal of Computer Science and Application vol. 4, p. 10.

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). A new DNA-based S-box. International Journal of Engineering & Technology IJET-IJENS, 15(04),1-9.

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). A New DNA-Based Approach of Generating Key-dependent ShiftRows Transformation. arXiv preprint arXiv:1502.03544

Al-wattar, A., et al. (2020). A DNA-Based Block Cipher with Improved Security. Journal of Cryptology, 33(2), 193-208.

An, X., Hu, K., & Wang, M. (2020, July). MixColumns Coefficient Property and Security of the AES with A Secret S-Box. In International Conference on Cryptology in Africa (pp. 114-131). Springer, Cham. https://dx.doi.org/10.1007%2F978-3-030-51938-4_6

Anam, Beenish et al. (2010). Review on the Advancements of DNA Cryptography, eprintarXiv:1010.0186.

Anu, Shree, D., & Ahlawat, S. (2017). A Review on Cryptography, Attacks and Cyber Security. International Journal of Advanced Research in Computer Science. Issue 8(5), May-June 2017.

Anwar, T., Kumar, A., & Paul, S. (2015). DNA Cryptography Based on Symmetric Key Exchange. International Journal of Engineering and Technology (IJET).

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, 862–867.

Ariffin, S., Mahmod, R., Jaafar, A., & Rezal, M. (2012). An Immune System-Inspired Byte Permutation Function to Improve Confusion Performance of Round ansformation in Symmetric Encryption Scheme, 339–351. https://doi.org/10.1007/978-94-007-5699-1.

Armknecht, F., Iwata, T., Nyberg, K., & Preneel, B. (2016). Symmetric Cryptography (Dagstuhl Seminar 16021). In Dagstuhl Reports (Vol. 6, No. 1). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Aslan, F. Y., Sakalli, M. T., & Aslan, B. (2010, December). On the MixColumns linear transformation used in AES cipher. In National Conference on Electrical, Electronics and Computer Engineering (pp. 563-568). IEEE.

Ayman, M. M. (2020). New KD-3D-CA Block Cipher with Dynamic S-BOXES Base on 3D Cellular Automata. [Doctoral dissertation, Universiti Putra Malaysia]

Babita, E. & Kaur, E.G. (2017). A Review: Network Security Based on Cryptography & Steganography Techniques. International Journal of Advanced Research in Computer Science, Vol.8(4), May 2017.

Barker, E., & Nicky, M. (2017). Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. NIST SP800-67 Revision 2. November 2017. https://doi.org/10.6028/NIST.SP.800-67r2

Bassham III, L. E. et al. (2010). SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST.

Becky, M. (2017). Fundamental Objective of Information Security. Sage Data Security, https://www.sagedatasecurity.com/blog/fundamental-objectives-of-inform.

Bellovin, Steven, Bush & Randy (2018). Security Through Obscurity Considered Dangerous. Internet Engineering Task Force (IETF).

Biham, E., & B, Y. C. (2014). An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X, 59–76. https://doi.org/10.1007/978-3-319-13051-4.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A.(2009). Key Recovery Attacks of Practical Complexity on AES Variant with Up To 10 Rounds. http://www.wisdom.weizmann.ac.il/~orrd/crypt/PracticalAES256.pdf

Bogdanov, A., & Rijmen, V. (2014). Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011, December). Biclique cryptanalysis of the full AES. In International conference on the theory and application of cryptology and information security (pp. 344-371). Springer, Berlin, Heidelberg.
Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011, December). Biclique cryptanalysis of the full AES. In International conference on the theory and application of cryptology and information security (pp. 344-371). Springer, Berlin, Heidelberg.
Breckling, J., Ed. (1989). The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, vol. 61.

Canright, D. (2005). A very compact s-box for AES, ACM: Springer-Verlag Berlin.

Charles, P.P, Shari, L.P & Jonathan, M. (2015). Security In Computing. Pearson Education Inc, USA.

Chen, J. (2003, May). A DNA-based, biomolecular cryptography design. In Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03. (Vol. 3, pp. III-III). IEEE.

Chen, L., Zhang, Q., Ma, J., & Li, K. (2019). Research on neural network chaotic encryption algorithm in wireless network security communication. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-10.

Choy, J., Zhang, A., Khoo, K., Henricksen, M., & Poschmann, A. (2011, June). AES variants secure against related-key differential and boomerang attacks. In IFIP International Workshop on Information Security Theory and Practices (pp. 191-207). Springer, Berlin, Heidelberg.

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

Commerce, Computer Security Division. (2018). Modes Development - Block Cipher Techniques - CSRC. Information Technology Laboratory, National Institute of Standards and Technology, USA.

Cui, G., Qin, L., Wang, Y., & Zhang, X. (2008). An encryption scheme using DNA technology. In Bio-Inspired Computing: Theories and Applications, IEEE International Conference on,pp. 37-42.

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, Vol.7(5).

Daemen, J. & Rijmen, V. (2001). The Design of Rijndael. Springer-Verlag Berlin Heidelberg New York.

Daniyal, M. A., Syed, H. H. & Mohamed, S. T. (2013). Stream Ciphers: A Comparative Study of Attacks and Structures, International Journal of Computer Application, Vol.83 (1).

Das, I., Sanjoy, R., Subhrapratim, N. & Subhash, M. (2013). Random S0Box Generation in ASE by Changing Irreducible Polynomial, Meghnad Saha Institute of Technology.

Das, S., Uz Zaman, J. K. M. S. & Ghosh, R. (2013). Generation of AES S-Boxes with Various Modules and Additive Constant Polynomials and Testing Their Randomization, Procedia Technology, vol. 10, pp. 957-962.

Deepak, K., & Shailendra, S. (2011). Secret data writing using DNA sequences. In Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference on, pp. 402-40.

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

Easttom, C. (2015). Modern Cryptography, New York City, New York: McGraw Hill.

Forouzan, A. (2007). Cryptography and Network Security. First Edition. McGraw-Hill, USA.

Gehani, A., & Reif, J. (1999). Micro flow bio-molecular computation. Biosystems, 52(1-3), 197-216.

Georgescu, C., Nita, A., & Toma, A. (2017). A View On NIST Randomness Tests In Dependence. International Conference of Computers and Artificial Interlligence, 9th Edition Electronics, Targoviste, Romania.

Ghosh, M., Sanadhya, S. K., & Chang, D. (2016). Analysis of block cipher constructions against biclique and multiset attacks (Doctoral dissertation).

Grass, R. N., Heckel, R., Dessimoz, C., & Stark, W. J. (2020). Genomic encryption of digital data stored in synthetic DNA. Angewandte Chemie, 132(22), 8554-8558.

Grassi, L. (2018, April). MixColumns properties and attacks on (round-reduced) AES with a single secret S-box. In Cryptographers' Track at the RSA Conference (pp. 243-263). Springer, Cham.

Hamdan, O. A., Zaidan, B. B., Zaidan, A. A., Hamid, A. J., Shabbir, M. & Al-Nabhani, Y. (2010). New Comparative Study Between DES, 3DES and AES within Nine Factors, Journal of Computing, vol. 2, no. 3.

Hamdy, N., Shehata, K. & Eldemerdash, H. (2011). Design and Implementation of Encryption Unit Based on Customized AES Algorithm, International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 11(1).

Hosseinkhani, R. & Javadi, H. H. S. (2012). Using Cipher Key to Generate Dynamic S-Box in AES Cipher System, International Journal of Computer Science and Security, vol. 6(1).

Huang, C., Chan, Y. W., & Yen, N. (Eds.). (2020). Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA 2019) (Vol. 1088). Springer Nature.

Huang, K., Chiu, J. & Shen, S. (2013). A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Cipers, International Journal of Network Security & Its Applications (IJNSA). Vol.5 (1).

Huang, T., Tjuawinata, I., & Wu, H. (2015). Differential-Linear Cryptanalysis of ICEPOLE.

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

Ibrahim, Fatma E., Moussa, M. I., & Abdalkader, H. M. (2014). A Symmetric Encryption Algorithm based on DNA Computing. International Journal of Computer Applications (0975 – 8887) Volume 97– No.16, pp. 41-45.

Iliyasu, M. A., Abisoye, O. A., Bashir and, S. A. & Ojeniyi, S. A. (2021). "A Review of Dna Cryptograhic Approaches," 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), pp. 66-72, doi: 10.1109/CYBERNIGERIA51635.2021.9428855.

Isa, H., Jamil, N., & Zaba, 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., & Zaba, M. R. (2017). Hybrid Heuristic Methods in Constructing Cryptographically Strong S-boxes (October 2016).

Jain, A., Agarwal, P., Jain, R. & Singh, V. (2014). Chaotic Image Encryption Technique using S-Box based on DNA Approach, International Journal of Computer Applications, vol. 92, no.13, pp. 30-34.

Jain, S. & Bhatnagar, V. (2014). "Analogy of various DNA based security algorithms using cryptography and steganography," 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp. 285-291, doi: 10.1109/ICICICT.2014.6781294.

Jangala, S., Anusha, Vijaykumar, A. & Kavya, M. (2017). Cryptography: The Science of Secure Communication. International Journal of Computer Science and Network Security.

Jin, X., Min, L., Zhao, G., & Zhen, P. (2016). Chaos-based image encryption scheme combining DNA coding and entropy. Multimedia Tools and Applications, 75(11), 6303-6319.

Johnson, J., et al. (2010). Secure DNA-Based Block Cipher. Journal of Cryptology, 24(2), 157-174.

Juremi, J., Ramlan, M., Sulaiman, S. & Ramli, J. (2012) Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key, International Journal of Cyber-Security and Digital Forensics, Vol.1(3).

Kamaljit, K. & Gurpreet, S. (2015). A Review to an invincible cryptographic approach: DNA Cryptography. International Journal of Advanced Research in Computer Communication Engineering, Vol.4(1).

Kazlauskas, K., Vaicekauskas, G. & Smaluikas, R. (2015). An Algorithm for Key-Dependent S-Box Generation in Block Cipher System, INFORMATICA, Vol. 26 (1).

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, C.H. (2010). Differential fault analysis against AES-192 and AES-256 with minimal faults. The 7th International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010, pp. 3–9, USA, August 2010.

Kim, J. (2018). DNA-Based Block Cipher with Low Power Consumption. Journal of Cryptology, 31(3), 293-308.

Knudsen, L. R. & Robshaw, M.J.B. (2011). The Block Cipher Companion, Springer.

Kolate, V., & Joshi, R. B. (2020). An Information Security Using DNA Cryptography along with AES Algorithm. International Journal of Future Generation Communication and Networking, 13(3), 3191–3196

Kuchta, T., Knutsson, R., Fiore, A., Kudirkiene, E., Höhl, A., Horvatek Tomic, D., ... & De Medici, D. (2014). A decade with nucleic acid-based microbiological methods in safety control of foods. Letters in applied microbiology, 59(3), 263-271.

Lai, X.J., Lu, M.X., Qin, L., Han, J.S. & Fang, X.W. (2010). Asymmetric encryption and signature method with DNA technology. Science China: Information Sciences, Vol.53(3).

Lee, S. (2015). DNA-Based Block Cipher with High Performance. Journal of Cryptology, 29(2), 175-192.

Leier, A., Richter, C., Banzhaf, W. & Rauhe, H. (2000). Cryptography with DNA Binary Strands, BioSystem, Vol.57(1).

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

Lin, R.M., & Ng, T.Y. (2018). Secure Image Encryption Based on an Ideal New Nonlinear Discrete Dynamical System. Mathematical Problems In Engineering, Vol. 2018, Article ID 6797386.

Liu, J., Jiao, Y., Wang, Y., Li, H., Zhang, X., & Cui, G. (2019). Research on the Application of DNA Cryptography in Electronic Bidding System. In International Conference on Bio-Inspired Computing: Theories and Applications (pp. 221-230). Springer, Singapore.

Lucks, S. (2000, April). Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys. In AES Candidate Conference (Vol. 2000).

Mahmoud, E. M., Hafez, A. A. & Talaat, A. (2013). Dynamic AES-128 with Key-Dependent S-Box, International Journal of Engineering Research and Applications, Vol. 3 (1).

Majumdar, A., Biswas, A., Majumder, A., Sood, S. K., & Baishnab, K. L. (2021). A novel DNA-inspired encryption strategy for concealing cloud storage. Frontiers of Computer Science, 15(3), 1-18.

Manisha & Pooja, A. (2015). A Survey on DNA Based Cryptography. International Journal of Scientific Engineering and Research, Vol.3(4).

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.

Meng, R., Cui, Q., Zhou, Z., Fu, Z., & Sun, X. (2019). A steganography algorithm based on CycleGAN for covert communication in the Internet of things. IEEE Access, 7, 90574-90584.

Mewada, S. (2016). Classification of Efficient Symmetric Key Cryptography Algorithms, 14(2), 105–110.

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, 20(x), 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, 1–10.

Mohammed, E., Abd, A., & Hafez, E. (2014). Enhancing Channel Coding using AES Block Cipher Enhancing Channel Coding using AES Block Cipher, (January 2013). https://doi.org/10.5120/9933-4568.

Monika, A. & Pradeep, M. (2012). A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering (IJCSE), Vol. 4, PP877-882.

Najaftorkaman, M. & Kazazi, N.S. (2015). A Method to Encrypt Information with DNA-Based Cryptography. International Journal of Cyber-Security and Digital Forensics, Vol.4(3).

Namasudra, S. & Deka, G. C. (2018). Introduction of DNA computing in cryptography. UK: Taylor & Francis Group Publication.

Nath, A., & Roy, A. (2016). DNA encryption algorithms: Scope and challenges in symmetric key cryptography. International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume, 3.

Nejad, F. H., Sabah, S., & Jam, A. J. (2014). Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys. 2014 International Conference on Computational Science and Technology, ICCST 2014.

Nikita, C. & Priya, P. (2016). Secure Online Payment System using Visual Cryptography. International Journal of Advanced Research in Computer and Communication Engineering.

Niu, Y., & Zhang, X. (2020). An Effective Image Encryption Method Based on Space Filling Curve and Plaintext-Related Josephus Traversal. IEEE Access, 8, 196326-196340

Noorul, H.U.R., Chithralekha, B., & Rajapandian, M. (2015). A Novel DNA Computing based Encryption and Decryption Algorithm. Procedia Computer Science 46 pp.463 – 475.

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, 1–113.

Oswald, E., Daemen, J., & Rijmen, V. (2002). AES-The State of the Art of Rijndael's Security. Prieiga internetu: http://books. google. lt/books/about/The_Design_of_Rijndael. html.

Paar, C., Pelzl, J. (2010). Understanding Cryptography, Springer-Verlag Berlin Heidelberg.

Partheeban, P., & Kavitha, V. (2018). Dynamic key dependent AES S-box generation with optimized quality analysis. Cluster Computing, 6, 1–11.

Peng, W., Cheng, D. & Song, C. (2018). One-time-pad cryptography scheme based on a three-dimensional DNA self-assembly pyramid structure. PLoS ONE 13(11): e0206612. https://doi.org/10.1371/journal.pone.0206612.

Popli, M. (2019, February). DNA cryptography: a novel approach for data security using flower pollination algorithm. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.

Punita, M. (2011). AES: Asymmetric key cryptographic System. International Journal of Information Technology and Knowledge Management, Vol, No. 4 pp. 113-117.

Rahul, S., Geetha, G., Gulshan, K., & Tai-hoon, K. (2018). RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys. Security and Computer Networks, Vol. 2018, Article ID 9802475.

Rani, S. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms, 8(4).

Ritu, M. & Praveen, K. (2015). A Review Paper of DNA Based Cryptographic. National Conference on Innovative Trends in Computer Science Engineering: Proceedings.

Ruisanchez, C.P. (2015). A New Algorithm to Construct SBoxes with High Diffusion, International Journal of Soft Computing, Mathematics and Contorl, Vol. 4 (3).

Rukhin, A., Soto, J., et al. (2008). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST, Technology Administration, U.S.Department of Commerce.

Sabry, M., Hashem, M., Nazmy, T., & Khalifa, M. E. (2015, December). Design of DNA-based advanced encryption standard (AES). In 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS) (pp. 390-397). IEEE.

Sadique, J.K.M. & Ranjan, G. (2012). Review on fifteen Stitistical Tests Proposed by NIST, Journal of Theoretical Physics & Cryptography: Vol.1.

Sandeep, T., Nipin, G., Pankaj, G., Deepak. G, & Monika, G. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology ISSN.

Saravanan, T., & Venkatesh Kumar, S. (2018). A Review Paper on Cryptography-Science of Secure Communication. International Journal of Computer Science Trends and Technology 6(4), Jul-Aug 2018.

Sarita, K. (2017). A research Paper on Cryptography Encryption and Decryption. International Journal Of Engineering And Computer Science.

Saxena, A., Kaushik, N., & Kaushik, N. (2018). Encryption and Decryption Technique using java. In Cyber Security: Proceedings of CSI 2015 (pp. 427-436). Springer Singapore.

Scripcariu, L., & Frunza, M. D. (2012). Modified Advanced Encryption Standard, 3(23), 23–26.

Sharifah, M. Y., Ayman, M. H., Izura, U., Sherzod, T., & Muhammad Rezal, A.K. (2020). Key Dependent Dynamic S-Boxes Based on 3D Cellular Automata For Block Cipher. Journal of Theoretical and Applied Information Technology (JATIT), Vol. 98 No. 23, pp. 3808-3822.

Shipra, J. & Vishal, B. (2014). A Novel DNA Sequence Dictionary method/or Securing Data in DNA using Spiral Approach and Framework 0/ DNA Cryptography, IEEE.

Shipra, J. & Vishal, B. (2014). Anology of Various DNA Based Security Algorithms Using Cryptography and Steganography, IEEE.

Siddharth, G. (2013). Network Security: Attacks, Tools and Techniques. IJARCSSE, Volume 3, Issue 6.

Singh, P. (2015). Cryptography : An Art of Data Hiding Cryptography : An Art of Data Hiding, (February).

Sinha, S. & Arya, C. (2012). Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box, Defence Science Journal, vol. 62(1).

Smith, J., Stein, L. & Brooks, C. (2008). A DNA-Based Block Cipher. Journal of Cryptology, 21(3), 257-274.

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

Soto, J., & Bassham, L. (2000). Randomness Testing of the Advanced Encryption Standard Finalist Candidates 1.

Stallings, W. (2014). Cryptography and Network Security (6th ed.). Upper Saddle River, N.J.: Prentic Hall. pp. 67–68.

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

Sulaiman, S. (2012). A New ShiftColumn Transformation: An Enhancement of Rijndael Key Scheduling, 1(3), 160–166.

Tausif, A., Abhishek, K. & Sanchita, P. (2015). DNA Cryptography Based on Symmetric Key Exchange. International Journal of Engineering and Technology (IJET).

Tausif, A., Sanchita, P. & Shailendra, K.S. (2014). Message Transmission Based on DNA Cryptography: Review. International Journal of Bio-Science and Bio-Technology, Vol.6(5), pp.215-222.

Thambiraja, E., Ramesh, G. & Umarani, R. (2012). A survey on various most common encryption techniques. International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7.

Thiruthuvadoss, A. P. (2012). Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography. A M. Sc. dissertation, Dept. of System on Chip Design, Royal Institute of Technology.

Tiessen, T., Knudsen, L. R., Kölbl, S., & Lauridsen, M. M. (2015). Security of the AES with a secret S-Box. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 9054). https://doi.org/10.1007/978-3-662-48116-5_9.

UbaidurRahman, N.H., Balamurugan, C. & Mariappan, R. (2015). A Novel DNA Computing Based Encryption and Decryption Algorithm. Procedia Computer Science, Vol.46.

Vishnu, S.B. & Helen, K.J. (2015). A study on combine cryptography and steganography. IJRSCSE International Journal of Research Studies in Computer Science and Engineering, Volume 2, Issue 5, PP 45-49.

Wang, Y., Wu, W., Guo, Z., & Yu, X. (2014a). Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro, (Algorithm 1).

Wang, Y., Wu, W., Guo, Z., & Yu, X. (2014b). Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro, 308–323.

Wegmuller, M., Weid,J.P., Oberson, P., & Gisin, N. (2000). High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, paper 11.3.4, p. 109.

Williams, J. (2012). DNA-Based Block Cipher with Enhanced Security. Journal of Cryptology, 26(3), 275-292.

Wu, W., & Zhang, L. (2011). LBlock: A Lightweight Block Cipher, 327–344.

Zhang, Q., Guo, L., & Wei, X. (2013). A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-International Journal for Light and Electron Optics.

Zhang, R., & Chen, L. (2008). A Block Cipher Using Key-Dependent S-box and P-box, 1463–1468.

Zhang, S., Zhu, C., Sin, J . K. O., & Mok, P.K.T. (1999). A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571.

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.

Zhang, Y. P. & Fu, B. C. (2012). Research on DNA Cryptography, Applied Cryptography and Network (12) Security, Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0218-2.

Zhang, Y., Fu, B., & Zhang, X. (2012). DNA cryptography based on DNA Fragment assembly. In Information Science and Digital Content Technology (ICIDT), IEEE International Conference on, vol. 1, pp. 179-182.

Zhang, Y., Liu, X., Ma, Y., & Cheng, L. C. (2017). An optimized DNA based encryption scheme with enforced secure key distribution. Cluster Computing, 20(4), 3119-3130.

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