ENHANCING THE PRESENT BLOCK CIPHER FOR IOT APPLICATIONS: DEVELOPMENT AND COMPARATIVE ANALYSIS OF A LIGHTWEIGHT ALGORITHM WITH IMPROVED KEY SCHEDULE ALGORITHM

MARIA IMDAD

A thesis submitted in
fulfillment of the requirement for the award of the
Doctor of Philosophy in Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

APRIL 2023

DEDICATION

In the name of Allah, the Most Merciful. Special dedication to my family, Imdad Hussain, Late Robina Khanum, my support system, and my mentors, Dr. Sofia Najwa Binti Ramli, and Assoc. Prof. Ts. Dr. Hairulnizam Bin Mahdin. Heartly thanks for the love, support, motivation, and encouragement throughout this journey. Thanks for ensuring that my learning process never stops. My life and this success are incomplete without your efforts and prayers. This dissertation is dedicated to all of you.

ACKNOWLEDGEMENT

Praise Almighty Allah for the courage to start and the strength to complete this journey. First of all, I would love to express my special gratitude to my precious supervisors, Dr. Sofia Najwa Binti Ramli, and Assoc. Prof. Ts. Dr. Hairulnizam Bin Mahdin for being incredibly supportive throughout this journey. For her kindness, guidance, patience, advice, and knowledge-pouring sessions till I saw the light on the other side of the tunnel. Her never-ending help as comments and suggestions throughout the experiments and dissertation have contributed to the accomplishment of this research.

I would like to thank the Centre of Graduate Studies (CGS) and Ministry of Higher Education (MOHE), Fundamental Research Grant Scheme (FRGS/1/2019/ICT03/UTHM/03/1) for supporting this research.

I am obliged to my dearest family for their endless support, love, and prayers. I appreciate all my postgraduate friends' knowledge sharing and moral support. Thanks for making this journey memorable and being my friend in tough times. Extending my acknowledgment to the Faculty of Computer Science and Information Technology for their cooperation and accommodations. At last, I would like to thank everyone who helped me directly or indirectly in this journey, and this would have been impossible without you all.

ABSTRACT

The Internet of Things (IoT) has massive connectivity of resource-constrained devices, and enormous data exchange between devices has made it susceptible to various attacks ranging such as tag cloning, identity spoofing, node tempering and denial-of-service attacks. The PRESENT block cipher is a lightweight block cipher that ensures security, with good speed and performance in resource-constrained devices. However, the algorithm has slow confusion and diffusion properties because of the linear relationship between round keys from the Key Schedule Algorithm (KSA) and static bits in the permutation layer during encryption. Therefore, this research presents an enhanced KSA generating random round keys for better confusion and encryption with Deoxyribonucleic Acid (DNA) replication process as a low-cost diffusion solution. The proposed algorithm has been evaluated for KSA and encryption algorithm independently, where the improved KSA has achieved better randomness in round keys. For high- and low-density key datasets, the bit difference value between round keys ranges from 20% to 44% using KSA PRESENT whereas for improved KSA-PRESENT these value range between 53% to 56%, successfully surpassing the minimum 50% criteria. Meanwhile, DNA-PRESENT block cipher has been validated in terms of security, statistical, cost, and performance analysis. The results prove that the value of avalanche effect has increased from 52.26% to 57.38% using DNA-PRESENT and a value of 50%-bit error rate, along with better ciphertext randomness has been achieved. Throughput and hardware efficiency have increased as 176.47 kbps and 43.41 kbps, respectively using DNA-PRESENT. The Gate Equivalence (GE) has increased by 33% using DNA-PRESENT, while the execution time has decreased by 0.0828 seconds. The increase in hardware cost is a trade-off for the security advancements achieved. Hence, lightweight DNA-PRESENT can be considered as an alternate solution to PRESENT block cipher for IoT applications. In the future, PRESENT-80 bits can also be enhanced using the same strategy, and the comprehensive evaluation metrics can be used to evaluate other lightweight cryptographic solutions.

ABSTRAK

Internet Benda (Iot) mempunyai hubungan yang besar antara peranti yang mempunyai sumber terhad, dan kekerapan pertukaran data antara peranti menjadikannya terdedah kepada pelbagai serangan seperti pengklonan tag, penipuan identiti, pencerobohan nod dan serangan penafian perkhidmatan. PRESENT ialah kod penyulitan blok yang ringkas yang memastikan keselamatan data, dengan kelajuan dan prestasi yang baik dalam peranti sumber terhad. Namun, algoritma tersebut mempunyai sifat kekeliruan dan resapan yang perlahan, kerana hubungan linear antara kekunci pusingan daripada *Key Schedule Algorithm* (KSA) dan bit yang statik pada lapisan pilih atur semasa penyulitan data. Justeru, penyelidikan ini membentangkan tentang KSA yang telah dipertingkatkan dalam menjana kunci pusingan yang rawak untuk menghasilkan sifat kekeliruan dan penyulitan yang lebih baik dengan proses replikasi Asid Deoksiribonukleik (DNA) sebagai penyelesaian resapan berkos rendah. Algoritma yang dicadangkan telah dinilai untuk KSA dan algoritma penyulitan data secara berasingan, di mana KSA yang dipertingkatkan telah mencapai sifat rawak yang lebih baik bagi kekunci pusingan. Untuk set data kunci berketumpatan tinggi dan rendah, nilai perbezaan bit antara kunci pusingan berjulat dari 20% hingga 44% menggunakan KSA PRESENT manakala untuk KSA-PRESENT yang dipertingkatkan, nilai ini berjulat antara 53% hingga 56%, berjaya melepasi kriteria minimum 50%. Sementara itu, DNA-PRESENT telah disahkan dari segi analisis keselamatan, statistik, kos dan prestasi. Keputusan membuktikan peningkatan nilai kesan avalanche daripada 52.26% kepada 57.38% menggunakan DNA-PRESENT dan nilai kadar ralat bit sebanyak 50% juga peningkatan sifir teks rawak telah dicapai. Kecekapan daya pemprosesan dan perkakasan DNA-PRESENT meningkat kepada 176.47 kbps dan 43.41 kbps. *Gate Equivalence* (GE) meningkat sebanyak 33%, manakala masa pelaksanaan berkurangan sebanyak 0.0828 saat. Peningkatan dalam kos perkakasan merupakan tukar-ganti bagi mencapai peningkatan keselamatan. Oleh itu, DNA-PRESENT ringkas boleh dianggap sebagai penyelesaian alternatif kepada PRESENT untuk aplikasi IoT. Pada masa hadapan, PRESENT-80 bit juga boleh dipertingkatkan menggunakan strategi yang sama, dan metrik penilaian komprehensif boleh digunakan untuk menilai penyelesaian kriptografi ringkas yang lain.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AE	-	Avalanche Effect
AES	-	Advance Encryption Standard
ARX	-	Add Rotate XOR
ASCII	-	American Standard Code for Information Interchange
BER	-	Bit Error Rate
CBCM	-	Cipher Block Chain Mode
CC	-	Correlation Coefficient
CDMB	-	Central Dogma of Molecular Biology
CMOS	-	Complementary metal-oxide-semiconductor
DNA	-	Deoxyribonucleic Acid
FN	-	Feistel Network
FoM	-	Figure of Merit
GE	-	Gate Equivalence
GFN	-	General Feistel Network
HDK	-	High Density Key
HDP	-	High Density Plaintext
HE	-	Hardware Efficiency
IoT	-	Internet of Things
KSA	-	Key Schedule Algorithm
LDK	-	Low Density Key
LDP	-	Low Density Plaintext
LED	-	Lightweight Encryption Device
LWC	-	Lightweight Cryptography
NIST	-	National Institute of Standards and Technology
NLFSR	-	Non-linear Feedback Shift Register
p-box	-	Permutation box
pLayer	-	Permutation box

PCC	-	Plaintext Ciphertext Correlation
RC	-	Research Contribution
RFID	-	Radio Frequency Identification
RPRK	-	Random Plaintext Random Key
RO	-	Research Objective
RP	-	Research Process
s-box	-	Substitution box
sLayer	-	Substitution box
SPN	-	Substitution Permutation Network
TP	-	Throughput
XOR	-	Bit wise XOR operation
✓	-	Meets the required value
×	-	Does not meet the required value
✓(↑)	-	Meets the required value with increased number of observations
↑	-	Increased Value
↓	-	Decreased Value

LIST OF APPENDICES

LIST OF PUBLICATIONS

i. **Imdad, M**., Jacob, D. W., Mahdin, H., Baharum, Z., Shaharudin, S. M., & Azmi, M. S. (2020). Internet of things (IoT); security requirements, attacks and counter measures. *Indonesian Journal of Electrical Engineering and Computer Science*, *18*(3), 1520-1530.

ii. **Imdad, M**., Ramli, S. N., Mahdin, H., Mouni, B. U., & Sahar, S. (2020, October). An Enhanced DNA Sequence Table for Improved Security and Reduced Computational Complexity of DNA Cryptography. In *EAI International Conference on Body Area Networks* (pp. 106-120). Springer, Cham.

iii. **Imdad, M**., Ramli, S. N., & Mahdin, H. (2021). Increasing Randomization of Ciphertext in DNA Cryptography. *International Journal of Advanced Computer Science and Applications*, *12*(10).

iv. **Imdad M,** Ramli SN, Mahdin H. An Enhanced Key Schedule Algorithm of PRESENT-128 Block Cipher for Random and Non-Random Secret Keys. *Symmetry*. 2022; 14(3):604. https://doi.org/10.3390/sym14030604.

CHAPTER 1

INTRODUCTION

1.1 Research background

The rapid advancements in ubiquitous computing have introduced more embedded devices into modern human life than ever. The ever-growing, interconnection of these pervasive and resource-constrained devices leads to the new vision of the Internet of Things (IoT) (Rahim *et al.*, 2021). The backbone of IoT network is Internet, which not only facilitates to access the devices, but also gathers, processes, and transmits sensitive data between devices, as depicted in Figure 1.1(Khan & Salah, 2018).

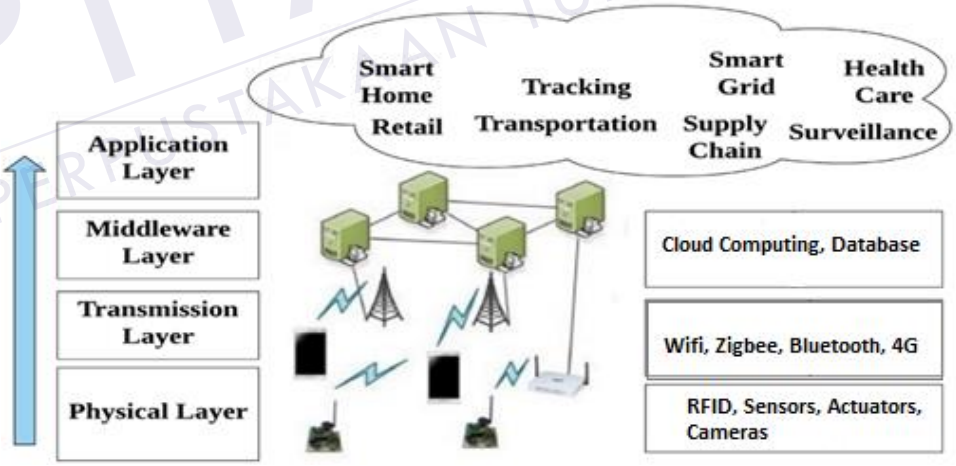

Figure 1.1: Four-layer architecture of Internet of Things (Khan & Salah, 2018)

The four-layer architecture of Internet of Things comprises of Physical, Transmission, Middleware, and Application layer. The Physical layer has resource-constrained devices such as sensors, actuators, and Radio Frequency Identification (RFID) tags. These devices have very low storage, computation power, and a limited

REFERENCES

Abd Zaid, M. M. & Hassan, S. (2022). Proposal Framework to Light Weight Cryptography Primitives. *Engineering and Technology Journal*, *40(04)*, pp. 516-526.

Abdel-Halim, I. T. & Zayan, H. M. (2022). Evaluating the Performance of Lightweight Block Ciphers for Resource-Constrained IoT Devices. *2022 4th Novel Intelligent and Leading Emerging Sciences Conference (NILES)*. Giza, Egypt: IEEE. pp. 39-44.

Abdel-Basset, M., Manogaran, G., Mohamed, M. & Rushdy, E. (2019). Internet of things in smart education environment: Supportive framework in the decision making process. *Concurrency and Computation: Practice and Experience*, *31(10)*, pp. 4515-4523.

Abdul, A., Narayana, G., Kishore, R. S., Srikanth, B., Kumar, K. K. & Indira, D. (2023). LWC: Efficient Lightweight Block Ciphers for Providing Security to Constrained Devices a Solution for IoT Devices. *Journal of Theoretical and Applied Information Technology*, *101(7)*, pp. 27-41.

Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H. & Elkhediri, S. (2019). CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. Riyadh, Saudi Arabia: IEEE. pp. 1-6.

Abdulraheem, M., Awotunde, J. B., Jimoh, R. G. & Oladipo, I. D. (2020). An efficient lightweight cryptographic algorithm for IoT security. *International Conference on Information and Communication Technology and Applications*. Cham: Springer. pp. 444-456.

Abed, S. E., Jaffal, R., Mohd, B. J. & Al-Shayeji, M. (2021). An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. *Cluster Computing*, *24(4)*, pp. 3065-3084.

Abinaya, M. & Prabakeran, S. (2022). Lightweight Block Cipher for Resource Constrained IoT Environment, An Survey, Performance, Cryptanalysis and Research Challenges. *IoT Based Control Networks and Intelligent Systems: Proceedings of 3rd ICICNIS 2022.* . Singapore. pp. 347-365.

Aboshosha, B. W., Dessouky, M. M., Ramadan, R. A., El-Sayed, A. & Galalb, F. H. (2020). Evaluation of lightweight block ciphers based on general feistel structure (GFS). *WAS Sci. Nat, 2(1)*, pp. 1-8.

Aboushosha, B., Ramadan, R. A., Dwivedi, A. D., El-Sayed, A. & Dessouky, M. M. (2020). SLIM: A lightweight block cipher for internet of health things. *IEEE Access, 8(3)*, pp. 203747-203757.

Abutaha, M., Atawneh, B., Hammouri, L. & Kaddoum, G. (2022). Secure lightweight cryptosystem for IoT and pervasive computing. *Scientific reports, 12(1)*, pp. 19649-19662.

Adithya, B. & Santhi, G. (2022). A Bio-Inspired DNA Cryptographic-Based Morse Code Ciphering Strategy for Secure Data Transmission. *International Journal of Knowledge-Based Organizations (IJKBO), 12(3)*, pp. 1-18.

Adleman, L. M. (1994). Molecular computation of solutions to combinatorial problems. *Science, 266(5187)*, pp. 1021-1024.

Afzal, S., Yousaf, M., Afzal, H., Alharbe, N. & Mufti, M. R. (2020). Cryptographic Strength Evaluation of Key Schedule Algorithms. *Security and Communication Networks, 2020(5)*, pp. 1-9.

Ahmad, W., Rasool, A., Javed, A. R., Baker, T. & Jalil, Z. (2022). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics, 11(1)*, pp. 16-23.

Aitzhan, N. Z. & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing, 15(5)*, pp. 840-852.

Akiwate, B. & Parthiban, L. (2021). A DNA cryptographic solution for secured image and text encryption. *International Journal of Advanced Computer Science and Applications, 12(2)*, pp. 397-407.

Akkasaligar, P. T. & Biradar, S. (2020). Selective medical image encryption using DNA cryptography. *Information Security Journal: A Global Perspective, 29(2)*, pp. 91-101.

Al-Aboosi, A. M. M., Kamil, S., Abdullah, S. N. H. S. & Ariffin, K. a. Z. (2021). Lightweight cryptography for resource constraint devices: Challenges and recommendation. *2021 3rd International Cyber Resilience Conference (CRC)*. Langkawi Island, Malaysia: IEEE. pp. 1-6.

Al-Ahdal, A. H. (2021). Security Analysis of a Robust Lightweight Algorithm for Securing Data in Internet of Things Networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(12)*, pp. 133-143.

Al-Husainy, M. a. F., Al-Shargabi, B. & Aljawarneh, S. (2021). Lightweight cryptography system for IoT devices using DNA. *Computers and Electrical Engineering*, *95(7)*, pp. 107418-107429.

Al-Omari, A. H. (2019). Lightweight Dynamic Crypto Algorithm for Next Internet Generation. *Engineering, Technology & Applied Science Research*, *9(3)*, pp. 4203-4208.

Al-Rahman, S. Q. A., Sagheer, A. & A Dawood, O. (2021). A Hybrid Lightweight Cipher Algorithm. *International Journal of Computing and Digital System*, *11(1)*, pp. 463-475.

Al-Saadi, H. M. & Alshawi, I. (2023). Provably-Secure LED Block Cipher Diffusion and Confusion based on Chaotic Maps. *Informatica*, *47(6)*, pp. 105-114.

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A. & Udzir, N. I. (2015). A new DNA-based S-box. *Int. J. Eng. Technol*, *15(4)*, pp. 1-9.

Al-Shargabi, B. & Dar Assi, A. (2023). A modified lightweight DNA-based cryptography method for internet of things devices. *Expert Systems*, *67(7)*, pp. 13270-13281.

Alahdal, A., Al-Rummana, G. A., Shinde, G. & Deshmukh, N. K. (2020). NLBSIT: A new lightweight block cipher design for securing data in IOT devices. *International Journal of Computer Sciences and Engineering*, *8(10)*, pp. 164-173.

Alahdal, A. & Deshmukh, N. K. (2020). A systematic technical survey of lightweight cryptography on Iot environment. *International Journal of Scientific & Technology Research*, *9(3)*, pp. 6246-6261.

Alassaf, N. & Gutub, A. (2019). Simulating light-weight-cryptography implementation for IoT healthcare data security applications. *International Journal of E-Health and Medical Communications (IJEHMC)*, *10(4)*, pp. 1-15.

Alassaf, N., Gutub, A., Parah, S. A. & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications, 78(8)*, pp. 32633-32657.

Albrecht, M. R., Driessen, B., Kavun, E. B., Leander, G., Paar, C. & Yalçın, T. (2014). Block ciphers–focus on the linear layer (feat. PRIDE). *Annual Cryptology Conference*. Berlin, Heidelberg: Springer. pp. 57-76.

Alemami, Y., Mohamed, M. A. & Atiewi, S. (2019). Research on various cryptography techniques. *International Journal of Recent Technology and Engineering (IJRTE), 8(23)*, pp. 395-405.

Alfa, A. A., Alhassan, J. K., Olaniyi, O. M. & Olalere, M. (2020). Sooner Lightweight Cryptosystem: Towards Privacy Preservation of Resource-Constrained Devices. *International Conference on Information and Communication Technology and Applications*. Tashkent, Uzbekistan: Springer. pp. 415-429.

Alhija, M., Turab, N., Abuthawabeh, A., Abuowida, H. & Al Nabulsi, J. (2022). DNA Cryptographic Approaches: State of Art Opportunities and Cutting Edge Perspectives. *J. Theor. Appl. Inf. Technol., 100(18)*, pp. 5346-5358.

Ali, A. (2023). CDIEA: Chaos and DNA Based Image Encryption Algorithm. *Turkish Journal of Science and Technology, 18(1)*, pp. 261-273.

Alluhaidan, A. S. & Prabu, P. (2023). End to End encryption in resource-constrained IoT device. *IEEE Access, 11(9)*, pp. 70040-70051.

Alrubaie, A. H., Khodher, M. a. a. A. & Abdulameer, A. T. (2023). Image encryption based on 2DNA encoding and chaotic 2D logistic map. *Journal of Engineering and Applied Science, 70(1)*, pp. 1-21.

Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Alqahtani, H. F., Alqahtani, N. N. & Ali, A. A. (2020). Image encryption based on AES and RSA algorithms. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. Riyadh, Saudi Arabia: IEEE. pp. 1-5.

Ammar, M., Russello, G. & Crispo, B. (2018). Internet of Things: A Survey on The Security of IoT Frameworks. *Journal of Information Security and Applications, 38(9)*, pp. 8-27.

Anajemba, J. H., Iwendi, C., Mittal, M. & Yue, T. (2020). Improved advance encryption standard with a privacy database structure for IoT nodes. *2020 IEEE 9th international conference on communication systems and network technologies (CSNT)*. Gwalior, India: IEEE. pp. 201-206.

Anderson, R., Biham, E. & Knudsen, L. (1998). Serpent: A proposal for the advanced encryption standard. *NIST AES Proposal*, *174(21)*, pp. 1-23.

Andrea, I., Chrysostomou, C. & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE symposium on computers and communication (ISCC)*. Larnaca, Cyprus: IEEE. pp. 180-187.

Apolinarski, M. (2019). Randomness Evaluation of PP-1 and PP-2 Block Ciphers Round Keys Generators. *Advances in Soft and Hard Computing*. Cham: Springer. pp. 272-281.

Arthi, G., Thanikaiselvan, V. & Amirtharajan, R. (2022). 4D Hyperchaotic map and DNA encoding combined image encryption for secure communication. *Multimedia Tools and Applications*, *81(11)*, pp. 15859-15878.

Ashraf, Q. M., Tahir, M., Habaebi, M. H. & Isoaho, J. (2023). Towards Autonomic Internet of Things: Recent Advances, Evaluation Criteria and Future Research Directions. *IEEE Internet of Things Journal*, *10(16)*, pp. 14725-14748.

Ashraf, Z., Sohail, A. & Yousaf, M. (2023). Robust and lightweight symmetric key exchange algorithm for next-generation IoE. *Internet of Things*, *22(1)*, pp. 100703-100721.

Aslan, B., Yavuzer Aslan, F. & Sakallı, M. T. (2020). Energy consumption analysis of lightweight cryptographic algorithms that can be used in the security of Internet of Things applications. *Security and Communication Networks*, *2020(5)*, pp. 1-15.

August, D. A. & Smith, A. C. (2023). Characterizing a Time–Memory Tradeoff Against PudgyTurtle. *SN Computer Science*, *4(5)*, pp. 486-495.

Aumasson, J.-P. (2019). Too Much Crypto. *Cryptology ePrint Archive*, *11(3)*, pp. 21-36.

Azimi, Z. & Ahadpour, S. (2020). Color image encryption based on DNA encoding and pair coupled chaotic maps. *Multimedia Tools and Applications*, *79(3)*, pp. 1727-1744.

Babaei, A., Motameni, H. & Enayatifar, R. (2020). A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. *Optik, Elsevier*, *203(2)*, pp. 164000-164013.

Babaei, M. (2013). A novel text and image encryption method based on chaos theory and DNA computing. *Natural computing*, *12(1)*, pp. 101-107.

Badel, S., Dağtekin, N., Nakahara, J., Ouafi, K., Reffé, N., Sepehrdad, P., Sušil, P. & Vaudenay, S. (2010). ARMADILLO: A multi-purpose cryptographic primitive dedicated to hardware. *International Workshop on Cryptographic Hardware and Embedded Systems*. Berlin, Heidelberg: Springer. pp. 398-412.

Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M. & Todo, Y. (2017). GIFT: A small present: Towards reaching the limit of lightweight encryption. *Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference*. Taipei, Taiwan: Springer. pp. 321-345.

Bansod, G., Raval, N. & Pisharoty, N. (2014). Implementation of a new lightweight encryption design for embedded security. *IEEE Transactions on Information Forensics and Security, 10(1)*, pp. 142-151.

Barker, E. & Roginsky, A. (2011). Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths. *NIST Special Publication, 800(1)*, pp. 131-145.

National Institute of Standards and Technology (NIST) (2018). *Transitioning the use of cryptographic algorithms and key lengths.* United States: 800-131A.

Basu, S., Karuppiah, M., Nasipuri, M., Halder, A. K. & Radhakrishnan, N. (2019). Bio-inspired cryptosystem with DNA cryptography and neural networks. *Journal of Systems Architecture, 94(6225)*, pp. 24-31.

Batina, L., Chow, S. S., Hancke, G. & Liu, Z. (2019). Introduction to the special issue on cryptographic engineering for Internet of Things: Security foundations, lightweight solutions, and attacks, ACM New York, NY, USA**:** pp. 1-3.

Bednáriková, A. & Zajac, P. (2021). A new representation of S-boxes for algebraic differential cryptanalysis. *Work of the Croatian Academy of Sciences and Arts. mathematical sciences 546(25)*, pp. 33-49.

Belazi, A., Talha, M., Kharbech, S. & Xiang, W. (2019). Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access, 7(5)*, pp. 36667-36681.

Bellini, E. & Huang, Y. J. (2022). Randomness testing of the NIST light weight cipher finalist candidates. *NIST Lightweight Cryptography Workshop*. Madrid: NIST. pp. 1-26.

Bhagat, V., Kumar, S., Gupta, S. K. & Chaube, M. K. (2023). Lightweight cryptographic algorithms based on different model architectures: A systematic

review and futuristic applications. *Concurrency and Computation: Practice and Experience, 35(1)*, pp. 7425-7432.

Bhattasali, T. (2013). Licrypt: Lightweight cryptography technique for securing smart objects in internet of things environment. *CSI Communications, 5(1)*, pp. 26-36.

Biham, E., Dunkelman, O., Keller, N. & Shamir, A. (2011). New data-efficient attacks on reduced-round idea. *Cryptology ePrint Archive, 49(3)*, pp. 21-34.

Biham, E. & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY, 4(1)*, pp. 3-72.

Biryukov, A. & Khovratovich, D. (2009). Related-key cryptanalysis of the full AES-192 and AES-256. *International Conference on the Theory and Application of Cryptology and Information Security*. Berlin, Heidelberg: Springer. pp. 1-18.

Blanc, S., Lahmadi, A., Le Gouguec, K., Minier, M. & Sleem, L. (2022). Benchmarking of lightweight cryptographic algorithms for wireless IoT networks. *Wireless Networks, 28(8)*, pp. 3453-3476.

Bogdanov, A., Khovratovich, D. & Rechberger, C. (2011). Biclique cryptanalysis of the full AES. *International conference on the theory and application of cryptology and information security*. Berlin, Heidelberg: Springer. pp. 344-371.

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. *International workshop on cryptographic hardware and embedded systems*. Berlin, Heidelberg: Springer. pp. 450-466.

Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C. & Rechberger, C. (2012). PRINCE–a low-latency block cipher for pervasive computing applications. *International conference on the theory and application of cryptology and information security*. Berlin, Heidelberg: Springer. pp. 208-225.

Buja, A. G., Abdul-Latip, S. F. & Ahmad, R. (2016). Repeated Differential Properties of PRESENT Key Schedules. *Proceedings of the 4th International Conference on Information and Network Security*. Kuala Lumpur, Malaysia: ACM. pp. 24-28.

Cao, Z., Chen, Z., Shang, W. & Zhu, Y. (2023). Efficient Revocable Anonymous Authentication Mechanism for Edge Intelligent Controllers. *IEEE Internet of Things Journal*, *10(12)*, pp. 10357-10367.

Çavuşoğlu, Ü. & Kaçar, S. (2019). A novel parallel image encryption algorithm based on chaos. *Cluster Computing*, *22(1)*, pp. 1211-1223.

Cayabyab, G. T., Sison, A. M. & Medina, R. P. (2019). A Secure Key Scheduling Operation for International Data Encryption Algorithm using Serpent Key Schedule Operation. *Proceedings of the 2nd International Conference on Computing and Big Data*. Taichung Software Park, Taichung, Taiwan: ACM. pp. 63-67.

Cazorla, M., Marquet, K. & Minier, M. (2013). Survey and benchmark of lightweight block ciphers for wireless sensor networks. *2013 international conference on security and cryptography (SECRYPT)*. Reykjavík, Iceland: IEEE. pp. 1-6.

Chanal, P. M. & Kakkasageri, M. S. (2020). Security and privacy in IOT: a survey. *Wireless Personal Communications*, *115(2)*, pp. 1667-1693.

Chandra, S., Paira, S., Alam, S. S. & Sanyal, G. (2014). A comparative survey of symmetric and asymmetric key cryptography. *2014 international conference on electronics, communication and computational engineering (ICECCE)*. Hosur, India: IEEE. pp. 83-93.

Chaturvedi, S. P., Mukherjee, R. & Yadav, A. (2022). Comparison between Ultra Lightweight Cryptographic Techniques on Microcontrollers for Smart Agriculture. *2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*. Naya Raipur, India: IEEE. pp. 62-65.

Chaudhary, R. R. K. & Chatterjee, K. (2020). An efficient lightweight cryptographic technique for IoT based E-healthcare system. *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*. Noida, India: IEEE. pp. 991-995.

Chauhan, J. A., Patel, A. R., Parikh, S. & Modi, N. (2022). An Analysis of Lightweight Cryptographic Algorithms for IoT-Applications. *International Conference on Advancements in Smart Computing and Information Security*. Cham: Springer. pp. 201-216.

Chen, H.-C. (2019). Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application. *Mobile Networks and Applications, 24(3),* pp. 839-852.

Chen, J., Gong, Z., Tang, Y. & Dong, X. (2022). A comprehensive analysis of lightweight 8-bit sboxes from iterative structures. *Journal of Information Security and Applications, 70(4),* pp. 103302-103328.

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

Cho, W.-L., Kim, K.-B. & Shin, K.-W. (2016). A hardware design of ultra-lightweight block cipher algorithm PRESENT for IoT applications. *Journal of the Korea Institute of Information and Communication Engineering, 20(7),* pp. 1296-1302.

Chuengsatiansup, C., Ronen, E., Rose, G. G. & Yarom, Y. (2023). Row, Row, Row your boat: How to not find weak keys in pilsung. *The Computer Journal, 66(6)*, pp. 1335-1341.

Ciardiello, F. & Di Liddo, A. (2020). Privacy accountability and penalties for IoT firms. *Risk Analysis, 42(8),* pp. 1784-1805.

Civino, R., Blondeau, C. & Sala, M. (2019). Differential attacks: using alternative operations. *Designs, Codes and Cryptography, 87(3),* pp. 225-247.

Collard, B. & Standaert, F.-X. (2009). A statistical saturation attack against the block cipher PRESENT. *Cryptographers' Track at the RSA Conference*. Berlin, Heidelberg: Springer. pp. 195-210.

Daemen, J., Peeters, M., Van Assche, G. & Rijmen, V. (2000). Nessie proposal: NOEKEON. *First open NESSIE workshop*. Heverlee, Belgium: Noekeon. pp. 213-230.

Daemen, J. & Rijmen, V. (1999). *AES proposal: Rijndael, AES algorithm submission*. Retrieved on August 16, 2023, from http://www.nist.gov/CryptoToolKit

Dagadu, J. C., Li, J.-P. & Aboagye, E. O. (2019). Medical image encryption based on hybrid chaotic DNA diffusion. *Wireless Personal Communications, 108(1),* pp. 591-612.

Damodharan, J., Susai Michael, E. R. & Shaikh-Husin, N. (2023). High Throughput PRESENT Cipher Hardware Architecture for the Medical IoT Applications. *Cryptography*, *7(1)*, pp. 6-18.

Dang, T. N. & Vo, H. M. (2019). Advanced AES algorithm using dynamic key in the internet of things system. *2019 IEEE 4th international conference on computer and communication systems (ICCCS)*. Singapore: IEEE. pp. 682-686.

Das, P. & Saif, S.Intrusion Detection in IoT-Based Healthcare Using ML and DL Approaches: A Case Study In *Artificial Intelligence and Cyber Security in Industry 4.0*: Springer: pp. 271-294; (2023).

De Canniere, C., Dunkelman, O. & Knežević, M. (2009). KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. *International Workshop on Cryptographic Hardware and Embedded Systems*. Berlin, Heidelberg: Springer. pp. 272-288.

Deb, S. & Bhuyan, B. (2020). Performance analysis of current lightweight stream ciphers for constrained environments. *Sādhanā*, *45(4)*, pp. 1-12.

Devi, P. B. & Kumar, R. K. (2018). Inspired feistel DNA based crypto system using D-Box. *International Journal of Applied Engineering Research*, *13(5)*, pp. 2847-2856.

Dhanda, S. S., Singh, B. & Jindal, P. (2020). Lightweight cryptography: A solution to secure IoT. *Wireless Personal Communications*, *112(3)*, pp. 1947-1980.

Dinu, D., Corre, Y. L., Khovratovich, D., Perrin, L., Großschädl, J. & Biryukov, A. (2019). Triathlon of lightweight block ciphers for the internet of things. *Journal of cryptographic Engineering*, *9(3)*, pp. 283-302.

Dofe, J. & Rai Saini, K. (2022). Internet of Things World: A New Security Perspective. *SN Computer Science*, *4(1)*, pp. 36-48.

Duta, C.-L., Mocanu, B.-C., Vladescu, F.-A. & Gheorghe, L. (2014). Randomness evaluation framework of cryptographic algorithms. *International Journal on Cryptography and Information Security*, *4(1)*, pp. 31-49.

Dutta, I. K., Ghosh, B. & Bayoumi, M. (2019). Lightweight cryptography for internet of insecure things: A survey. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. Las Vegas, NV, USA: IEEE. pp. 0475-0481.

Dworkin, M. J., Barker, E. B., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E. & Dray Jr, J. F. (2001). Advanced encryption standard (AES). *Federal Inf.*

Process. Stds.(NIST FIPS), National Institute of Standards and Technology, Gaithersburg., *197(4)*, pp. 142-163.

El-Banby, G. M., Elazm, L. a. A., El-Shafai, W., El-Bahnasawy, N. A., El-Samie, F. E. A., Elazm, A. A. & Siam, A. I. (2023). Security enhancement of the access control scheme in IoMT applications based on fuzzy logic processing and lightweight encryption. *Complex & Intelligent Systems*, *23(5)*, pp. 1-20.

El-Hajj, M., Mousawi, H. & Fadlallah, A. (2023). Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. *Future Internet*, *15(2)*, pp. 54-65.

El-Shafai, W., Khallaf, F., El-Rabaie, E.-S. M. & Abd El-Samie, F. E. (2021). Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, *12(1)*, pp. 1-29.

El Hadj Youssef, W., Abdelli, A., Dridi, F. & Machhout, M. (2020). Hardware implementation of secure lightweight cryptographic designs for IoT applications. *Security and Communication Networks*, *2020(4)*, pp. 1-13.

El Khediri, S. (2022). Wireless sensor networks: a survey, categorization, main issues, and future orientations for clustering protocols. *Computing*, *104(8)*, pp. 1775-1837.

Elamir, M. M. & Mabrouk, M. S. (2022). Secure framework for IoT technology based on RSA and DNA cryptography. *Egyptian Journal of Medical Human Genetics*, *23(1)*, pp. 1-7.

Elkamchouchi, D. H., Mohamed, H. G. & Moussa, K. H. (2020). A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion. *Entropy*, *22(2)*, pp. 180-195.

Engels, D., Fan, X., Gong, G., Hu, H. & Smith, E. M. (2010). Hummingbird: ultra-lightweight cryptography for resource-constrained devices. *International conference on financial cryptography and data security*. Berlin, Heidelberg: Springer. pp. 3-18.

Engels, D., Saarinen, M.-J. O., Schweitzer, P. & Smith, E. M. (2011). The Hummingbird-2 lightweight authenticated encryption algorithm. *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Amherst, MA, USA: Springer. pp. 19-31.

Ettiyan, R. & Geetha, V. (2023). A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems. *Healthcare Analytics*, *3(4)*, pp. 100149-100166.

Farhan, A. K., Ali, R. S., Yassein, H. R., Al-Saidi, N. M. G. & Abdul-Majeed, G. H. (2020). A new approach to generate multi S-boxes based on RNA computing. *Int J Innov Comput Inf Control*, *16(5)*, pp. 331-348.

Fathy, C. & Ali, H. M. (2023). A secure IoT-based irrigation system for precision agriculture using the expeditious cipher. *Sensors*, *23(4)*, pp. 2091-2113.

Flórez-Gutiérrez, A. & Naya-Plasencia, M. (2020). Improving key-recovery in linear attacks: Application to 28-round PRESENT. *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Zagreb, Croatia: Springer. pp. 221-249.

Fotovvat, A., Rahman, G. M., Vedaei, S. S. & Wahid, K. A. (2020). Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. *IEEE Internet of Things Journal*, *8(10)*, pp. 8279-8290.

Galas, E. M. & Gerardo, B. D. (2019). Implementing randomized salt on round key for corrected block tiny encryption algorithm (XXTEA). *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*. Chongqing, China: IEEE. pp. 795-799.

Garg, D., Bhatia, K. K. & Gupta, S. (2022). A novel genetic algorithm based encryption technique for securing data on fog network using DNA cryptography. *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*. Gautam Buddha Nagar, India: IEEE. pp. 362-368.

Gava, J., Moura, N., Lucena, J., Rocha, V., Garibotti, R., Calazans, N., Cuenca-Asensi, S., Bastos, R. P., Reis, R. & Ost, L. (2023). Assessment of Radiation-Induced Soft Errors on Lightweight Cryptography Algorithms Running on a Resource-constrained Device. *IEEE Transactions on Nuclear Science*, *10(1)*, pp. 455-472.

Gawade, A. & Shekokar, N. (2018). Lightweight Cipher Using GRP Bit Permutation and Tweak. *International Conference on Intelligent Systems Design and Applications*. Cham: Springer. pp. 1050-1059.

Gimenez-Aguilar, M., De Fuentes, J. M., Gonzalez-Manzano, L. & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems, 124(5)*, pp. 91-118.

Gong, Z., Nikova, S. & Law, Y. W. (2011). KLEIN: a new family of lightweight block ciphers. *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Amherst, MA, USA: Springer. pp. 1-18.

Guang, Y., Yu, L., Dong, W., Wang, Y., Zeng, J., Zhao, J. & Ding, Q. (2022). Chaos-Based Lightweight Cryptographic Algorithm Design and FPGA Implementation. *Entropy, 24(11)*, pp. 1610-1621.

Gunathilake, N. A., Al-Dubai, A. & Buchana, W. J. (2020). Recent Advances and Trends in Lightweight Cryptography for IoT Security. *2020 16th International Conference on Network and Service Management (CNSM)*. Izmir, Turkey: IEEE. pp. 1-5.

Gunathilake, N. A., Buchanan, W. J. & Asif, R. (2019). Next generation lightweight cryptography for smart IoT devices, implementation, challenges and applications. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. Limerick, Ireland: IEEE. pp. 707-710.

Guo, J., Peyrin, T., Poschmann, A. & Robshaw, M. (2011). The LED block cipher. *International workshop on cryptographic hardware and embedded systems*. Nara, Japan: Springer. pp. 326-341.

Guo, Z. & Sun, P. (2022). Improved reverse zigzag transform and DNA diffusion chaotic image encryption method. *Multimedia Tools and Applications, 81(8)*, pp. 11301-11323.

Gupta, D. N. & Kumar, R. (2019). Lightweight cryptography: an IoT perspective. *Trivium, 80(1)*, pp. 2580-2592.

Gupta, D. N. & Kumar, R. (2021). Sponge based lightweight cryptographic hash functions for IoT applications. *2021 International Conference on Intelligent Technologies (CONIT)*. Hubli, India: IEEE. pp. 1-5.

Gupta, K. C., Pandey, S. K. & Samanta, S. (2022). FUTURE: a lightweight block cipher using an optimal diffusion matrix. *International Conference on Cryptology in Africa*. Fes, Morocco: Springer. pp. 28-52.

Hanley, N. & Oneill, M. (2012). Hardware comparison of the ISO/IEC 29192-2 block ciphers. *2012 IEEE computer society annual symposium on VLSI*. Hsinchu, Taiwan: IEEE. pp. 57-62.

Harmouch, Y. & El Kouch, R. (2019). The benefit of using chaos in key schedule algorithm. *Journal of Information Security and Applications, 45(6)*, pp. 143-155.

Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., Ciro Rodriguez, R. & Vargas, D. E. (2021). Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications. *Complexity*, *2021(6)*, pp. 1-13.

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of cryptographic Engineering*, *8(2)*, pp. 141-184.

Hernandez-Castro, J. C., Peris-Lopez, P. & Aumasson, J.-P.On the key schedule strength of present.In *Data Privacy Management and Autonomous Spontaneus Security*. Leuven, Belgium: Springer: pp. 253-263; (2011).

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C. & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. Hammamet, Tunisia: IEEE. pp. 1-6.

Hua, Z., Xu, B., Jin, F. & Huang, H. (2019). Image encryption using Josephus problem and filtering diffusion. *IEEE Access*, *7(5)*, pp. 8660-8674.

Huang, J., Vaudenay, S. & Lai, X. (2014). On the key schedule of lightweight block ciphers. *International Conference on Cryptology in India*. New Delhi: Springer. pp. 124-142.

Huang, J., Yan, H. & Lai, X. (2017). Transposition of AES key schedule. *Information Security and Cryptology: 12th International Conference, Inscrypt 2016*. Beijing, China: Springer. pp. 84-102.

Huang, K.-P., Lo, S.-T. & Sutthiphisal, D. (2023). From Data Transparency and Security to Interfirm Collaboration-A Blockchain Technology Perspective. *ABAC Journal*, *43(3)*, pp. 1-15.

Huang, Z.-W. & Zhou, N.-R. (2022). Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion. *Optics & Laser Technology*, *149(17)*, pp. 107879-107892.

Hurrah, N. N., Parah, S. A., Sheikh, J. A., Al-Turjman, F. & Muhammad, K. (2019). Secure data transmission framework for confidentiality in IoTs. *Ad Hoc Networks, 95(5)*, pp. 101989-101012.

Hussain, I., Negi, M. C. & Pandey, N. (2017). A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer. *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)*. Dubai, United Arab Emirates: IEEE. pp. 464-470.

Hussain, U. N., Chithralekha, T., Raj, A. N., Sathish, G. & Dharani, A. (2012). A hybrid DNA algorithm for DES using central dogma of molecular biology (CDMB). *International Journal of Computer Applications, 42(20)*, pp. 1-4.

Ibrahim, H. M., Abunahla, H., Mohammad, B. & Alkhzaimi, H. (2022). Memristor-based PUF for lightweight cryptographic randomness. *Scientific reports, 12(1)*, pp. 8633-8642.

Ibrahim, N. & Agbinya, J. (2023). Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices. *Applied Sciences, 13(7)*, pp. 4398-4411.

Ibrahim, N. F. & Agbinya, J. I. (2021). A review of lightweight cryptographic schemes and fundamental cryptographic characteristics of boolean functions. *Advances in Internet of Things, 12(1)*, pp. 9-17.

Iftikhar, U., Asrar, K., Waqas, M. & Ali, S. A. (2021). Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices. *Engineering, Technology & Applied Science Research, 11(6)*, pp. 7867-7874.

Indesteege, S., Keller, N., Dunkelman, O., Biham, E. & Preneel, B. (2008). A practical attack on KeeLoq. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Istanbul, Turkey: Springer. pp. 1-18.

Indira, K. & Suresh, D. (2023). Comparison of some parameters based on different key sizes for certain class of cryptographic algorithms. *AIP Conference Proceedings*. Anaheim, US: AIP Publishing. pp. 12-34.

Iqbal, M. A., Olaleye, O. G. & Bayoumi, M. A. (2017). A review on internet of things (IoT): security and privacy requirements and the solution approaches. *Global Journal of Computer Science and Technology, 16(7)*, pp. 1-10.

Irfan Alam, M. & Singh, S. N. (2021). Designing and Implementing Cloud Security Using Multi-layer DNA Cryptography in Python. *Trends in Wireless Communication and Information Security*. Singapore: Springer. pp. 375-385.

Iso, I. O. F. S. *Information Security,Lightweight Cryptography,Part 2: Block Ciphers*. Geneva, Switzerland,ISO/IEC 29192-2:2019.2019

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

Jacak, M. M., Jóźwiak, P., Niemczuk, J. & Jacak, J. E. (2021). Quantum generators of random numbers. *Scientific reports, 11(1)*, pp. 16108-16119.

Jacaman, I. & Farajallah, M. (2023). A Lightweight Spatial Domain Image Encryption Algorithms: A Review Paper. *Journal of Theoretical and Applied Information Technology, 101(3)*, pp. 1275-1290.

Jallouli, O., El Assad, S. And Chetto, M (2016). Robust chaos-based stream-cipher for secure public communication channels. *11th, International Conference for Internet Technology and Secured Transactions (ICITST) IEEE*. Barcelona, Spain. pp. 23-26.

Jangra, M. & Singh, B. (2019). Performance analysis of CLEFIA and PRESENT lightweight block ciphers. *Journal of Discrete Mathematical Sciences and Cryptography, 22(8)*, pp. 1489-1499.

Jassim, S. A. & Farhan, A. K. (2021). A Survey on Stream Ciphers for Constrained Environments. *2021, 1st Babylon International Conference on Information Technology and Science (BICITS)*. Babil, Iraq: IEEE. pp. 228-233.

Jeong, K., Kang, H., Lee, C., Sung, J. & Hong, S. (2012). Biclique Cryptanalysis of Lightweight Block Ciphers PRESENT, Piccolo and LED. *IACR Cryptol. ePrint Arch., 2012(4)*, pp. 621-632.

Jing, S., Guo, Y. & Chen, W. (2021). Meaningful ciphertext encryption algorithm based on bit scrambling, discrete wavelet transform, and improved chaos. *IET Image Processing, 15(5)*, pp. 1053-1071.

John, J. (2012). Cryptography for resource constrained devices: A survey. *International Journal on Computer Science and Engineering, 4(11)*, pp. 1766-1772.

Kadhim, A. N. & Manaa, M. E. (2022). Improving IoT data Security Using Compression and Lightweight Encryption Technique. *2022, 5th International*

Conference on Engineering Technology and its Applications (IICETA). Al-Najaf, Iraq: IEEE. pp. 187-192.

Kakkar, A. & Singh, M. (2023). Performance Analysis of a Lightweight Robust Chaotic Image Re-encryption Scheme for 5G Heterogeneous Networks. *Wireless Personal Communications, 129(4)*, pp. 2607-2631.

Kandhoul, N. & Dhurandher, S. K. (2018). An asymmetric RSA-based security approach for opportunistic IoT. *International Conference on Wireless Intelligent and Distributed Environment for Communication*. Toronto, ON, Canada: Springer. pp. 47-60.

Kapalova, N., Sakan, K., Algazy, K. & Dyusenbayev, D. (2022). Development and Study of an Encryption Algorithm. *Computation, 10(11)*, pp. 198-204.

Kaps, J.-P. (2008). Chai-tea, cryptographic hardware implementations of XTEA. *International Conference on Cryptology*. Melbourne, Australia: Springer. pp. 363-375.

Kate, H. K., Razmara, J. & Isazadeh, A. (2018). A novel fast and secure approach for voice encryption based on DNA computing. *3D Research, 9(2)*, pp. 1-11.

Kaur, I., Bharti, S. K. & Saxena, S.Pre-requisite Concepts for Security and Privacy In *Internet of Things: Security and Privacy in Cyberspace*: Springer: pp. 1-22; (2022).

Kavallieratos, G., Katsikas, S. & Gkioulos, V. (2020). Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey. *Future Internet, 12(4)*, 65.

Kelsey, J. & Schneier, B. (2000). Key-schedule cryptanalysis of DEAL. *Selected Areas in Cryptography: 6th Annual International Workshop, SAC'99*. Kingston, Ontario, Canada: Springer. pp. 118-134.

Kempen, A. (2021). DNA Vital evidence to convict criminals. *Servamus Community-based Safety and Security Magazine, 114(8)*, pp. 38-39.

Khalil, A. A., Hammood, M. M. & Gaftan, A. M. (2023). Round S-Boxes Development for Present-80 Lightweight Block Cipher Encryption Algorithm. *International Journal of Intelligent Systems and Applications in Engineering, 11(2)*, pp. 381-394.

Khan, M. A. & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82(5)*, pp. 395-411.

Khattabi, Y. M., Matalgah, M. M. & Olama, M. M. (2020). Revisiting lightweight encryption for IoT applications: Error performance and throughput in wireless fading channels with and without coding. *IEEE Access*, *8(9)*, pp. 13429-13443.

Kietzmann, P., Schmidt, T. C. & Wählisch, M. (2021). A guideline on pseudorandom number generation (PRNG) in the IoT. *ACM Computing Surveys (CSUR)*, *54(6)*, pp. 1-38.

Kifouche, A., Azzaz, M. S., Hamouche, R. & Kocik, R. (2022). Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications. *International Journal of Information Security*, *21(6)*, pp. 1247-1262.

Kim, H., Jeon, Y., Kim, G., Kim, J., Sim, B.-Y., Han, D.-G., Seo, H., Kim, S., Hong, S. & Sung, J. (2021). A new method for designing lightweight S-boxes with high differential and linear branch numbers, and its application. *IEEE Access*, *9(2)*, pp. 150592-150607.

Kim, N., Shin, D. & Kim, B. (2015). Benchmark of Lightweoght Block Ciphers (HIGHT & PRESENT) for Arduino. *Proceedings of the Korea Information Processing Society Conference*. Korea: Korea Information Processing Society. pp. 875-877.

Knežević, M., Nikov, V. & Rombouts, P. (2012). Low latency encryption is "lightweight light wait". *International Workshop on Cryptographic Hardware and Embedded Systems*. Leuven, Belgium: Springer. pp. 426-446.

Knudsen, L. R. (2000). A detailed analysis of SAFER K. *Journal of CRYPTOLOGY*, *13(2)*, pp. 417-436.

Knudsen, L. R. & Leander, G. PRESENT-block cipher.In *Encyclopedia of Cryptography and Security*: Springer: pp. 953-955; (2011).

Koubaâ, K. & Derbel, N. (2023). DNA Image Encryption Scheme Based on a Chaotic LSTM Pseudo-Random Number Generator. *International Journal of Bifurcation and Chaos*, *33(06)*, pp. 2350067-2230075.

Kousalya, R. (2021). Security Analysis against Differential Cryptanalysis using Active S-Boxes. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12(13)*, pp. 701-709.

Krishna, A. K. & Kumar, B. J. S. M. (2023). Breaking the Boundaries using DNA Technologies to Advance Computing. *CVR Journal of Science and Technology*, *24(1)*, pp. 13-23.

Krishna, B. M., Gopinath, D. S., Kiran, M. & Javid, S. (2020). Reconfigurable Asymmetric Lightweight Cryptosystem. *International Journal*, *8(5)*, pp. 1678-1684.

Kubba, Z. M. J. & Hoomod, H. K. (2020). Developing a lightweight cryptographic algorithm based on DNA computing. *AIP Conference Proceedings*. Karbala, Iraq: AIP Publishing. pp. 040013-040026.

Kumar, C., Prajapati, S. S. & Verma, R. K. (2022). A Survey of Various Lightweight Cryptography Block ciphers for IoT devices. *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*. Bhopal, India: IEEE. pp. 1-6.

Kumar, M., Yadav, P. & Kumari, M. (2010). Flaws in Differential Cryptanalysis of Reduced Round PRESENT. *IACR Cryptol. ePrint Arch*, *2010(9)*, pp. 407-416.

Kumar, S., Kumar, R., Kumar, S. & Kumar, S. (2019). Cryptographic construction using coupled map lattice as a diffusion model to enhanced security. *Journal of Information Security and Applications*, *46(4)*, pp. 70-83.

Kumar, V., Malik, N., Singla, J., Jhanjhi, N., Amsaad, F. & Razaque, A. (2022). Light weight authentication scheme for smart home iot devices. *Cryptography*, *6(3)*, pp. 37-53.

Kumari, P. & Mondal, B. (2023). Lightweight image encryption algorithm using NLFSR and CBC mode. *The Journal of Supercomputing*, *79(14)*, pp. 1-21.

Kuznetsov, A., Gorbenko, Y. I., Prokopovych-Tkachenko, D., Lutsenko, M. & Pastukhov, M. (2019). NIST PQC: code-based cryptosystems. *Telecommunications and Radio Engineering*, *78(5)*, pp. 127-144.

Labio, R. D. & Festijo, E. D. (2020). D-PRESENT: A Lightweight Block Cipher with Dynamic Key-Dependent Substitution Boxes. *2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. Depok, Indonesia: IEEE. pp. 27-32.

Lara-Nino, C. A., Diaz-Perez, A. & Morales-Sandoval, M. (2018). FPGA-based assessment of midori and gift lightweight block ciphers. *International conference on information and communications security*. Lille Douai, France: Springer. pp. 745-755.

Lata, N. & Kumar, R. (2022). DSIT: A Dynamic Lightweight Cryptography Algorithm for Securing Image in IoT Communication. *International Journal of Image and Graphics*, *23(4)*, pp. 2350035-2350043.

Latif, M. A., Ahmad, M. B. & Khan, M. K. (2020). A review on key management and lightweight cryptography for IoT. *2020 Global Conference on Wireless and Optical Technologies (GCWOT)*. University of Malaga, Spain: IEEE. pp. 1-7.

Le, T.-V. (2023). Cross-Server End-to-End Patient Key Agreement Protocol for DNA-Based U-Healthcare in the Internet of Living Things. *Mathematics, 11(7),* pp. 1638-1648.

Leander, G. (2011). On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Tallinn, Estonia: Springer. pp. 303-322.

Lee, J. Y. & Lee, J. (2021). Current research trends in IoT security: a systematic mapping study. *Mobile Information Systems, 2021(4),* pp. 1-25.

Lee, T. R., Teh, J. S., Jamil, N., Yan, J. L. S. & Chen, J. (2021). Lightweight block cipher security evaluation based on machine learning classifiers and active S-Boxes. *IEEE Access, 9(5),* pp. 134052-134064.

Lewandowski, M. & Katkoori, S. (2021). Enhancing PRESENT-80 and Substitution-Permutation Network Cipher Security with Dynamic "Keyed" Permutation Networks. *2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. Tampa, FL, USA: IEEE. pp. 350-355.

Li, C., Zhao, F., Liu, C., Lei, L. & Zhang, J. (2019). A hyperchaotic color image encryption algorithm and security analysis. *Security and Communication Networks, 2019(12),* pp. 1-9.

Liang, Q. & Zhu, C. (2023). A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. *Optics & Laser Technology, 160(2),* pp. 109033-109045.

Lim, C. H. (1999). A revised version of CRYPTON: CRYPTON V1. 0. *International Workshop on Fast Software Encryption*. Springer. pp. 31-45.

Lim, C. H. & Korkishko, T. (2005). mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors. *International workshop on information security applications*. Springer. pp. 243-258.

Liu, B. (2019). BioSeq-Analysis: a platform for DNA, RNA and protein sequence analysis based on machine learning approaches. *Briefings in bioinformatics, 20(4),* pp. 1280-1294.

Lo'ai, A. T. & Tawalbeh, H. (2017). Lightweight crypto and security. *Security and Privacy in Cyber Physical Systems: Foundations, Principles and Applications, 23(4)*, pp. 243-261.

Luo, H., Chen, W., Ming, X. & Wu, Y. (2021). General differential fault attack on PRESENT and GIFT cipher with nibble. *IEEE Access, 9(2)*, pp. 37697-37706.

Madarro-Capó, E. J., Legón-Pérez, C. M., Rojas, O., Sosa-Gómez, G. & Socorro-Llanes, R. (2020). Bit independence criterion extended to stream ciphers. *Applied Sciences, 10(21)*, pp. 7668-7679.

Madushan, H., Salam, I. & Alawatugoda, J. (2022). A review of the nist lightweight cryptography finalists and their fault analyses. *Electronics, 11(24)*, pp. 4199-4209.

Maitra, S., Richards, D., Abdelgawad, A. & Yelamarthi, K. (2019). Performance evaluation of IoT encryption algorithms: memory, timing, and energy. *2019, IEEE sensors applications symposium (SAS)*. Sophia Antipolis, France: IEEE. pp. 1-6.

Manikandan, N. & Subha, S. (2018). Parallel AES algorithm for performance improvement in data analytics security for IoT. *International Journal of Networking and Virtual Organisations, 18(2)*, pp. 112-129.

Manucom, E. M. M., Gerardo, B. D. & Medina, R. P. (2019). Analysis of Key Randomness in Improved One-Time Pad Cryptography. *2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID)*. Xiamen, China: IEEE. pp. 11-16.

Maolood, A. T., Farhan, A. K., El-Sobky, W. I., Zaky, H. N., Zayed, H. L., Ahmed, H. E. & Diab, T. O. (2023). Fast Novel Efficient S-Boxes with Expanded DNA Codes. *Security and Communication Networks, 2023(4)*, pp. 51-76.

Maram, B. & Gnanasekar, J. (2018). A block cipher algorithm to enhance the avalanche effect using dynamic key-dependent S-box and genetic operations. *International Journal of Pure and Applied Mathematics, 119(10)*, pp. 399-418.

Marin, L., Pawlowski, M. P. & Jara, A. (2015). Optimized ECC implementation for secure communication between heterogeneous IoT devices. *Sensors, 15(9)*, pp. 21478-21499.

Marinakis, G. (2021). Sampling methods for cryptographic tests. *Cryptology ePrint Archive, 765(45)*, pp. 71-89.

Marinakis, G. (2021). Selection of sampling keys for cryptographic tests. *Cryptology ePrint Archive*, *908(5)*, pp. 1-11.

Marinakis, G. (2022). Rating the Security Strength of Cryptographic Algorithms. *Journal of Applied Mathematics and Bioinformatics, 12(1)*, pp. 35-46.

Marton, K. & Suciu, A. (2015). On the interpretation of results from the NIST statistical test suite. *Science and Technology*, *18(1)*, pp. 18-32.

Marzan, R. M. & Sison, A. M. (2019). An enhanced key security of playfair cipher algorithm. *Proceedings of the 2019 8th International Conference on Software and Computer Applications*. Cairo, Egypt. pp. 457-461.

Mawla, N. A. & Khafaji, H. K. (2023). An Ultra Lightweight Cipher Algorithm For IoT Devices and Unmanned Aerial Vehicles. *2023, International Conference On Cyber Management And Engineering (CyMaEn)*. Bangkok: IEEE. pp. 240-244.

May, L., Henricksen, M., Millan, W., Carter, G. & Dawson, E. (2002). Strengthening the Key Schedule of the AES. *Information Security and Privacy: 7th Australasian Conference, ACISP 2002*. Melbourne, Australia: Springer. pp. 226-240.

Medileh, S., Laouid, A., Euler, R., Bounceur, A., Hammoudeh, M., Alshaikh, M., Eleyan, A. & Khashan, O. A. (2020). A flexible encryption technique for the internet of things environment. *Ad Hoc Networks*, *106(5)*, pp. 102240-102256.

Melosik, M., Galan, M., Naumowicz, M., Tylczyński, P. & Koziol, S. (2023). Cryptographically Secure PseudoRandom Bit Generator for Wearable Technology. *Entropy*, *25(7)*, pp. 976-989.

Mengdi, Z., Xiaojuan, Z., Yayun, Z. & Siwei, M. (2021). Overview of Randomness Test on Cryptographic Algorithms. *Journal of Physics: Conference Series*. IOP Publishing. pp. 012009-012017.

Mhaibes, H. I., Abood, M. H. & Farhan, A. K. (2022). Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices. *International Journal of Interactive Mobile Technologies, 16(20)*, pp. 21-34.

Mishra, G., Krishna Murthy, S. & Pal, S. (2021). Dependency of lightweight block ciphers over S-boxes: A deep learning based analysis. *Journal of Discrete Mathematical Sciences and Cryptography, 2021(11)*, pp. 1-21.

Mishra, Z. & Acharya, B. (2023). High throughput compact area architecture of XXTEA for IoT application. *Sādhanā, 48(2)*, pp. 1-7.

Mohammad, H. M. & Abdullah, A. A. (2022). Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(3)*, pp. 551-560.

Mohammad Shah, I. N. B. B. I., E. S. (2020). Randomness Analysis on Lightweight Block Cipher, PRESENT. *Journal of Computer Science, 16(11)*, pp. 1639-1647.

Mohanapriya, R. & Kumar, N. (2023). Optimized Implementation of S-box and Inverse S-box for PRESENT Lightweight Block Cipher. *2023, 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*. Vellore, India: IEEE. pp. 1-5.

Mohd, B. J. & Hayajneh, T. (2018). Lightweight block ciphers for IoT: energy optimization and survivability techniques. *IEEE Access, 6(3)*, pp. 35966-35978.

Momand, A., Jan, S. U. & Ramzan, N. (2023). A Systematic and Comprehensive Survey of Recent Advances in Intrusion Detection Systems Using Machine Learning: Deep Learning, Datasets, and Attack Taxonomy. *Journal of Sensors, 2023(2)*, pp. 32-46.

Mondal, B. & Mandal, T. (2017). A light weight secure image encryption scheme based on chaos & DNA computing. *Journal of King Saud University-Computer and Information Sciences, 29(4)*, pp. 499-504.

Moradi, A., Poschmann, A., Ling, S., Paar, C. & Wang, H. (2011). Pushing the limits: A very compact and a threshold implementation of AES. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. pp. 69-88.

Mousavi, S. K., Ghaffari, A., Besharat, S. & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks, 27(2)*, pp. 1515-1555.

Mukherjee, P., Pradhan, C., Barik, R. K. & Dubey, H. (2023). Emerging DNA cryptography-based encryption schemes: A review. *International Journal of Information and Computer Security, 20(2)*, pp. 27-47.

Mumtaz, S., Sanam, N. & Ul Haq, T. (2023). An LA-group based design of the non-linear component of block cipher. *Integration, 93(11)*, pp. 1-15.

Muthavhine, K. D. & Sumbwanyambe, M. (2018). An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect. *2018 International Conference on Information and Communications Technology (ICOIACT)*. IEEE. pp. 114-119.

Muthukrishnan, M. V., Vattam, J., Mangal, M., Sanghavi, A., Pandey, V. & Pal, M. (2022). Security Framework Based on Shannon's Theory and Genetic Cryptography for Cloud Computing Framework. *Available at SSRN*, *34(5)*, pp.12-23.

Nabeel, N., Habaebi, M. H. & Islam, M. R. (2021). Security analysis of LNMNT-lightweight crypto hash function for IoT. *IEEE Access*, *9(5)*, pp. 165754-165765.

Namasudra, S. (2020). Fast and secure data accessing by using DNA computing for the cloud environment. *IEEE Transactions on Services Computing*, *15(4)*, pp. 2289-2300.

Namasudra, S. (2022). A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure. *Computers and Electrical Engineering*, *104(2)*, pp. 108426-108432.

Naseer, Y., Shah, T., Shah, D. & Hussain, S. (2019). A novel algorithm of constructing highly nonlinear Sp-boxes. *Cryptography*, *3(1)*, pp. 6-17.

Naser, N. M. & Naif, J. R. (2022). A systematic review of ultra-lightweight encryption algorithms. *International Journal of Nonlinear Analysis and Applications*, *13(1)*, pp. 3825-3851.

Nayancy, Dutta, S. & Chakraborty, S. (2020). A survey on implementation of lightweight block ciphers for resource constraints devices. *Journal of Discrete Mathematical Sciences and Cryptography*, *25(5)*, pp. 1-22.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21(3)*, pp. 2702-2733.

Nikitha, G. A., Kathrine, G. J. W., Duthie, C. R., Ebenezer, V. & Silas, S. (2023). Hybrid Cryptographic Algorithm to Secure Internet of Things. *2023, 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*. Madurai, India: IEEE. pp. 1556-1562.

Niu, Y., Zhao, K., Zhang, X. & Cui, G. (2020). Review on DNA cryptography. *14th International Conference, BIC-TA 2019: Bio-inspired Computing: Theories and Applications* Zhengzhou, China: Springer. pp. 134-148.

Noura, H., Salman, O., Couturier, R. & Chehab, A. (2023). Lesca: Lightweight stream cipher algorithm for emerging systems. *Ad Hoc Networks, 138(4)*, pp. 102999-103009.

Noura, H. N., Chehab, A. & Couturier, R. (2020). Overview of efficient symmetric cryptography: Dynamic vs Static approaches. *2020, 8th International Symposium on Digital Forensics and Security (ISDFS)*. Beirut, Lebanon: IEEE. pp. 1-6.

Noura, H. N., Salman, O., Couturier, R. & Chehab, A. (2022). LoRCA: Lightweight round block and stream cipher algorithms for IoV systems. *Vehicular Communications, 34(2)*, pp. 100416-100427.

Olaniyi, O. M., Alfa, A. A., Dauda, I. A. & Abdulaziz, B. (2023). A Survey of Lightweight Cryptosystems for Smart Home Devices. *Covenant Journal of Informatics and Communication Technology*, *11(1)*, pp. 3769-3781.

Omran, O. & Alexan, W. (2023). Cellular Automata, S-Box and DNA Coding Based SPN for Image Encryption. *2023, 5th International Congress on Human Computer Interaction, Optimization and Robotic Applications (HORA)*. Istanbul, Turkey: IEEE. pp. 1-6.

Ovilla-Martínez, B., Mancillas-López, C., Martínez-Herrera, A. F. & Bernal-Gutiérrez, J. A. (2020). FPGA implementation of some second round NIST lightweight cryptography candidates. *Electronics, 9(11)*, pp. 1940-1952.

Oza, S., Ambre, A., Kanole, S., Kshirsagar, P., Dhabekar, N., Paliwal, K. & Hendre, V.IoT: The Future for Quality of Services.In *ICCCE 2019*: Springer: pp. 291-301; (2020).

Özen, O., Varıcı, K., Tezcan, C. & Kocair, Ç. (2009). Lightweight block ciphers revisited: Cryptanalysis of reduced round PRESENT and HIGHT. *Australasian Conference on Information Security and Privacy*. Brisbane, QLD, Australia: Springer. pp. 90-107.

Pal, S., Selvanambi, R., Malik, P. & Karuppiah, M. (2023). A Chaotic System and Count Tracking Mechanism-based Dynamic S-Box and Secret Key Generation. *International Journal of Mathematical, Engineering and Management Sciences*, *8(2)*, pp. 230-245.

Panahi, P., Bayılmış, C., Çavuşoğlu, U. & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering, 46(4)*, pp. 4015-4037.

Panchami, V. & Mathews, M. M. (2023). A Substitution Box for Lightweight Ciphers to Secure Internet of Things. *Journal of King Saud University–Computer and Information Sciences, 35(3)*, pp. 75-89.

Parida, P., Pradhan, C., Gao, X.-Z., Roy, D. S. & Barik, R. K. (2021). Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. *IEEE Access, 9(2)*, pp. 76191-76204.

Park, M., Oh, H. & Lee, K. (2019). Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors, 19(9)*, pp. 2148-2156.

Patil, P., Narayankar, P., Narayan, D. & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science, 78(2)*, pp. 617-624.

Perrin, L. (2019). Partitions in the S-Box of Streebog and Kuznyechik. *IACR Transactions on Symmetric Cryptology, 2019(1)*, pp. 302-329.

Plos, T., Dobraunig, C., Hofinger, M., Oprisnik, A., Wiesmeier, C. & Wiesmeier, J. (2012). Compact hardware implementations of the block ciphers mCrypton, NOEKEON, and SEA. *International Conference on Cryptology in India*. Kolkata, India: Springer. pp. 358-377.

Poojari, A. & Nagesh, H. (2021). FPGA implementation of random number generator using LFSR and scrambling algorithm for lightweight cryptography. *International Journal of Applied Science and Engineering, 18(6)*, pp. 1-9.

Por, L. Y., Yang, J., Ku, C. S. & Khan, A. A. (2023). Special Issue on Cryptography and Information Security. *Applied Sciences, 13(10)*, pp. 6042-6051.

Poriye, M. & Upadhyaya, S. (2023). DNA-SKA: A DNA congruous secure symmetric key generation algorithm. *International Journal of Applied Management Science, 15(2)*, pp. 51-67.

Poriye, M. & Upadhyaya, S. (2023). A DNA Based Framework for Securing Information Using Asymmetric Encryption. *Wireless Personal Communications, 129(3)*, pp. 1717-1733.

Pourasad, Y., Ranjbarzadeh, R. & Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. *Entropy, 23(3)*, pp. 341-359.

Qaid, G. R. & Ebrahim, N. S. (2023). A Lightweight Cryptographic Algorithm Based on DNA Computing for IoT Devices. *Security and Communication Networks, 2023(1)*, pp. 52-63.

Qasaimeh, M., Al-Qassas, R. S. & Ababneh, M. (2021). Software Design and Experimental Evaluation of a Reduced AES for IoT Applications. *Future Internet, 13(11)*, pp. 273-285.

Qasaimeh, M., Al-Qassas, R. S., Mohammad, F. & Aljawarneh, S. (2020). A novel simplified aes algorithm for lightweight real-time applications: Testing and discussion. *Recent Advances in Computer Science and Communications 13(3)*, pp. 435-445.

Qasaimeh, M., Al-Qassas, R. S. & Tedmori, S. (2018). Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT security. *Multimedia Tools and Applications, 77(6)*, pp. 18415-18449.

Radosavljević, N. & Babić, D. (2021). Power Consumption Analysis Model in Wireless Sensor Network for Different Topology Protocols and Lightweight Cryptographic Algorithms. *Journal of Internet Technology, 22(1)*, pp. 71-80.

Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A. & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications, 27(1)*, pp. 100285-100298.

Rahman, M. & Paul, G. (2022). Grover on KATAN: Quantum resource estimation. *IEEE Transactions on Quantum Engineering, 3(1)*, pp. 1-9.

Rajasekar, P. & Mangalam, H. (2020). Design and implementation of power and area optimized AES architecture on FPGA for IoT application. *Circuit World, 47(2)*, pp. 153-163.

Rajesh, S., Paul, V., Menon, V. G. & Khosravi, M. R. (2019). A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. *Symmetry, 11(2)*, pp. 293-302.

Rama Devi, K. & Bhuvaneswari, E. (2023). An Enhancement in Data Security Using Trellis Algorithm with DNA Sequences in Symmetric DNA Cryptography. *Wireless Personal Communications, 129(1)*, pp. 387-398.

Ramamurthy, R., Bauckhage, C., Buza, K. & Wrobel, S. (2017). Using echo state networks for cryptography. *International Conference on Artificial Neural Networks*. Alghero, Italy: Springer. pp. 663-671.

Ramaswamy, G. & Prasad, R. S. (2022). Deep Learning-Based Key Generation for DNA ASCII Table-Based Encryption. *Journal of Optoelectronics Laser*, *41(11)*, pp. 195-208.

Rana, M., Mamun, Q. & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129(4)*, pp. 77-89.

Rana, S., Hossain, S., Shoun, H. I. & Kashem, M. A. (2018). An effective lightweight cryptographic algorithm to secure resource-constrained devices. *International Journal of Advanced Computer Science and Applications*, *9(11)*, pp. 403-419.

Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K. & Choi, C. (2021). Threats and corrective measures for IoT security with observance of cybercrime: A survey. *Wireless communications and mobile computing*, *2021(4)*, pp. 1-30.

Rani, S. S., Alzubi, J. A., Lakshmanaprabu, S., Gupta, D. & Manikandan, R. (2020). Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. *Multimedia Tools and Applications*, *79(3)*, pp. 35405-35424.

Rashidi, B. (2019). High-throughput and lightweight hardware structures of HIGHT and PRESENT block ciphers. *Microelectronics Journal*, *90(1)*, pp. 232-252.

Ravichandran, D., Fathima, S., Balasubramanian, V., Banu, A. & Amirtharajan, R. (2019). DNA and chaos based confusion-diffusion for color image security. *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*. Vellore, India: IEEE. pp. 1-6.

Reddy, M. I., Kumar, A. S. & Reddy, K. S. (2020). A secured cryptographic system based on DNA and a hybrid key generation approach. *Biosystems*, *197(1)*, pp. 104207-104213.

Rohmad, M. S., Saparon, A., Amaran, H., Arif, N. & Hashim, H. (2017). Lightweight block cipher on VHDL. *2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. Langkawi, Malaysia: IEEE. pp. 87-94.

Roldán Lombardía, S., Balli, F. & Banik, S. (2021). Six shades lighter: a bit-serial implementation of the AES family. *Journal of cryptographic Engineering*, *11(4)*, pp. 417-439.

Roma, C. A., Tai, C.-E. A. & Hasan, M. A. (2021). Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms. *IEEE Access*, *9(2)*, pp. 71295-71317.

Rosa, P., Souto, A. & Cecílio, J. (2023). Light-SAE: A lightweight authentication protocol for large-scale IoT environments made with constrained devices. *IEEE Transactions on Network and Service Management, 2023(1)*, pp. 12-32.

Rosero-Montalvo, P. D. & Alvear-Puertas, V. E. (2022). Efficient Lightweight Cryptography Algorithm in IoT Devices with Real-time Criteria. *Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS2022)*. pp. 103-109.

Rostam, H. E., Motameni, H. & Enayatifar, R. (2022). Privacy-preserving in the Internet of Things based on steganography and chaotic functions. *Optik, 258(3)*, pp. 168864-166873.

Roy, S., Stavrou, A., Mark, B. L., Zeng, K., Pd, S. M. & Khasawneh, K. N. (2022). Characterization of AES Implementations on Microprocessor-based IoT Devices. *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. Austin, Texas: IEEE. 55-60.

Saba, S. J., Al-Nuaimi, B. T. & Suhail, R. A. (2023). A review of traditional, lightweight and ultra-lightweight cryptography techniques for IoT security environment. *AIP Conference Proceedings*. Diyala, Iraq: AIP Publishing. pp. 13-22.

Saddam, M. J., Ibrahim, A. A. & Mohammed, A. H. (2020). A lightweight image encryption and blowfish decryption for the secure internet of things. *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. Istanbul, Turkey: IEEE. pp. 1-5.

Sadkhan, S. B. & Hamza, Z. (2017). Cryptosystems used in IoT-current status and challenges. *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*. Sulaymaniyah, Iraq: IEEE. pp. 58-62.

Sadkhan, S. B. & Salman, A. O. (2018). A survey on lightweight-cryptography status and future challenges. *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*. Wasit Kut, Iraq: IEEE. pp. 105-108.

Saif, S., Das, P. & Biswas, S.LSEA-IOMT: On the Implementation of Lightweight Symmetric Encryption Algorithm for Internet of Medical Things (IoMT).In *Frontiers of ICT in Healthcare: Proceedings of EAIT 2022*: Springer: pp. 565-575.

Saini, A., Tsokanos, A. & Kirner, R. (2023). CryptoQNRG: A new framework for evaluation of cryptographic strength in quantum and pseudorandom number generation for key-scheduling algorithms. *The Journal of Supercomputing, 79(2)*, pp. 1-19.

Salam, A., Rachmawanto, E. H. & Sari, C. A. (2019). ShiftMod cipher: A symmetrical cryptosystem scheme. *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*. Semarang, Indonesia: IEEE. pp. 1-5.

Salami, Y., Khajevand, V. & Zeinali, E. (2023). Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges. *Journal of Computer & Robotics, 16(2)*, pp. 46-56.

Sallam, A. I., Faragallah, O. S. & El-Rabaie, E.-S. M. (2017). HEVC selective encryption using RC6 block cipher technique. *IEEE Transactions on Multimedia, 20(7)*, pp. 1636-1644.

Samiullah, M., Aslam, W., Khan, M. A., Alshahrani, H. M., Mahgoub, H., Abdullah, A. M., & Chen, C. M (2022). Rating of modern color image cryptography: A next-generation computing perspective. *Wireless communications and mobile computing, 2022(3)*, pp. 13-27.

Sankaran, S. (2016). Lightweight security framework for IoTs using identity based cryptography. *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. Jaipur, India: IEEE. pp. 880-886.

Sarker, V. K., Gia, T. N., Tenhunen, H. & Westerlund, T. (2020). Lightweight security algorithms for resource-constrained IoT-based sensor nodes. *2020 IEEE International Conference on Communications (ICC 2020)*. Dublin, Ireland: IEEE. pp. 1-7.

Şatir, E. & Kendirli, O. (2022). A symmetric DNA encryption process with a biotechnical hardware. *Journal of King Saud University-Science, 34(3)*, pp. 101838-101845.

Saxena, S. & Zou, L. (2022). Hallmarks of DNA replication stress. *Molecular cell, 82(12)*, pp. 2298-2314.

Sehrawat, D. & Gill, N. (2020). Ultra BRIGHT: A tiny and fast ultra lightweight block cipher for IoT. *International Journal of Scientific & Technology Research, 9(2)*, pp. 1063-1074.

Sehrawat, D., Gill, N. S. & Devi, M. (2019). Comparative analysis of lightweight block ciphers in IoT-enabled smart environment. *2019, 6th International Conference on Signal Processing and Integrated Networks (SPIN)*. Noida, India IEEE. pp. 915-920.

Seok, B., Sicato, J. C. S., Erzhena, T., Xuan, C., Pan, Y. & Park, J. H. (2019). Secure D2D communication for 5G IoT network based on lightweight cryptography. *Applied Sciences, 10(1)*, pp. 217-229.

Sha, Y., Bo, S., Yang, C., Mou, J. & Jahanshahi, H. (2022). A chaotic image encryption scheme based on genetic central dogma and kmp method. *International Journal of Bifurcation and Chaos, 32(12)*, pp. 225018-225031.

Shafagh, H., Hithnawi, A., Burkhalter, L., Fischli, P. & Duquennoy, S. (2017). Secure sharing of partially homomorphic encrypted iot data. *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. Delft, Netherlands. pp. 1-14.

Shafique, A., Rehman, M. U., Khan, K. H., Jamal, S. S., Mehmood, A. & Chaudhry, S. A. (2023). Securing High-Resolution Images from Unmanned Aerial Vehicles with DNA Encoding and Bit-Plane Extraction Method. *IEEE Access, 11(2)*, pp. 44559 - 44577.

Shakir, H. R., Mehdi, S. A. & Hattab, A. A. (2023). A New Method for Color Image Encryption Using Chaotic System and DNA Encoding. *Mustansiriyah journal of pure and Applied Sciences, 1(1)*, pp. 68-79.

Shamala, L. M., Zayaraz, G., Vivekanandan, K. & Vijayalakshmi, V. (2021). Lightweight cryptography algorithms for Internet of Things enabled networks: an overview. *Journal of Physics: Conference Series*. Tamil Nadu, India: IOP Publishing. pp. 012072-012086.

Shan, R., Di, S., Calhoun, J. C. & Cappello, F. (2022). Exploring light-weight cryptography for efficient and secure lossy data compression. *2022, IEEE International Conference on Cluster Computing (CLUSTER)*. Heidelberg, Germany: IEEE. pp. 23-34.

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

Shanthi Rekha, S. & Saravanan, P. (2019). Low-cost AES-128 implementation for edge devices in IoT applications. *Journal of Circuits, Systems and Computers, 28(04)*, pp. 1950062-1950074.

Sharmila, S. & Vijayarani, S. (2022). Machine to Machine (M2M), Radio-frequency Identification (RFID), and Software-Defined Networking (SDN): Facilitators of the Internet of Things. *Artificial Intelligence-based Internet of Things Systems, 2022(1)*, pp. 219-242.

Sheikhpour, S., Ko, S.-B. & Mahani, A. (2021). A low cost fault-attack resilient AES for IoT applications. *Microelectronics Reliability, 123(3)*, pp. 114202-114213.

Shetty, V. S., Anusha, R., Mj, D. K. & Hegde, P. (2020). A survey on performance analysis of block cipher algorithms. *2020 International Conference on Inventive Computation Technologies (ICICT)*. Coimbatore, India: IEEE. pp. 167-174.

Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. & Shirai, T. (2011). Piccolo: an ultra-lightweight blockcipher. *International workshop on cryptographic hardware and embedded systems*. Nara, Japan: Springer. pp. 342-357.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S. & Iwata, T. (2007). The 128-bit blockcipher CLEFIA. *International workshop on fast software encryption*. Luxembourg City: Springer. pp. 181-195.

Silva, C., Cunha, V. A., Barraca, J. P. & Aguiar, R. L. (2023). Analysis of the Cryptographic Algorithms in IoT Communications. *Information Systems Frontiers, 2023(2)*, pp. 1-18.

Simion, E. (2015). The relevance of statistical tests in cryptography. *IEEE Security & Privacy, 13(1)*, pp. 66-70.

Singh, A. K., Chatterjee, K. & Singh, A. (2022). An image security model based on chaos and DNA cryptography for IIoT images. *IEEE Transactions on Industrial Informatics, 19(2)*, pp. 1957-1964.

Singh, G. & Yadav, R. K. (2020). Improvement of Performance Metrics and Security of AODV Routing Protocol using Central Dogma of Molecular Biology Based DNA Cryptography. *International Journal of Innovative Technology and Exploring Engineering (IJITEE) 9(4)*, pp. 13-34.

Sleem, L. & Couturier, R. (2020). TestU01 and Practrand: Tools for a randomness evaluation for famous multimedia ciphers. *Multimedia Tools and Applications, 79(3)*, pp. 24075-24088.

Sleem, L. & Couturier, R. (2021). Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. *Multimedia Tools and Applications, 80(1)*, pp. 17067-17102.

Sliman, L., Omrani, T., Tari, Z., Samhat, A. E. & Rhouma, R. (2021). Towards an ultra lightweight block ciphers for Internet of Things. *Journal of Information Security and Applications, 61(6)*, pp. 102897-102909.

Standaert, F.-X., Piret, G., Gershenfeld, N. & Quisquater, J.-J. (2006). SEA: A scalable encryption algorithm for small embedded applications. *International Conference on Smart Card Research and Advanced Applications*. Graz, Australia: Springer. pp. 222-236.

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. *International Workshop on Fast Software Encryption*. Delhi, India: Springer. pp. 279-298.

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)*, pp. 160-166.

Sultan, I., Lone, M. Y., Nazish, M. & Banday, M. T. (2023). A Secure Key Expansion Algorithm for PRESENT. *IEEE Sensors Journal, 2023(1)*, pp. 1-14.

Susanti, B. H., Jimmy, J. & Ardyani, M. W. (2021). ENT Randomness Test on DM-PRESENT-80 and DM-PRESENT-128-based Pseudorandom Number Generator. *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE. pp. 324-328.

Suwais, K. (2022). Stream Cipher Based on Game Theory and DNA Coding. *Intelligent Automation & Soft Computing, 33(3)*, pp. 34-43.

Suzaki, T., Minematsu, K., Morioka, S. & Kobayashi, E. (2011). Twine: A lightweight, versatile block cipher. *ECRYPT Workshop on Lightweight Cryptography*. Belgium.

Sýs, M., Klinec, D., Kubíček, K. & Švenda, P. (2017). BoolTest: The fast randomness testing strategy based on boolean functions with application to DES, 3-DES, MD5, MD6 and SHA-256. *International Conference on E-Business and Telecommunications*. Madrid, Spain: Springer. pp. 123-149.

Tang, Z., Cui, J., Zhong, H. & Yu, M. (2016). A Random PRESENT encryption algorithm based on dynamic S-BOX. *International journal of security and its applications, 10(3)*, pp. 383-392.

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M. & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences, 10(12)*, pp. 4102-4116.

Teodoro, A. A., Gomes, O. S., Saadi, M., Silva, B. A., Rosa, R. L. & Rodríguez, D. Z. (2021). An FPGA-based performance evaluation of artificial neural network architecture algorithm for IoT. *Wireless Personal Communications, 2021(5)*, pp. 1-32.

Thabit, F., Alhomdy, S. & Jagtap, S. (2021). A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. *International Journal of Intelligent Networks, 2(9)*, pp. 18-33.

Thakor, V. A., Razzaque, M. A., Darji, A. D. & Patel, A. R. (2023). A novel 5-bit S-box design for lightweight cryptography algorithms. *Journal of Information Security and Applications, 73(4)*, pp. 103444-103458.

Thakor, V. A., Razzaque, M. A. & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access, 9(3)*, pp. 28177-28193.

Thorat, C. & Inamdar, V. (2018). Implementation of new hybrid lightweight cryptosystem. *Applied computing and Informatics, 16(2)*, pp. 195-206.

Tian, Y. & Lu, Z. (2017). Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation. *AIP Advances, 7(8)*, pp. 085008-085013.

Tiwari, V., Jampala, N., Tentu, A. N. & Saxena, A. (2021). Towards Finding Active Number of S-Boxes in Block Ciphers using Mixed Integer Linear Programming. *Informatica, 45(6)*, pp. 21-34.

To'xtajon, Q. (2023). LIGHTWEIGHT CRYPTOGRAPHY IN IOT NETWORKS. *Innovations in Technology and Science Education, 2(10)*, pp. 999-1007.

Todo, Y. & Sasaki, Y. (2021). Designing S-Boxes Providing Stronger Security Against Differential Cryptanalysis for Ciphers Using Byte-Wise XOR. *International Conference on Selected Areas in Cryptography*. BC, Canada: Springer. pp. 179-199.

Tripathi, S. K., Gupta, B. & Pandian, K. S. (2021). An alternative practical public-key cryptosystems based on the Dependent RSA Discrete Logarithm Problems. *Expert Systems with Applications, 164(4)*, pp. 114047-114056.

Tsantikidou, K. & Sklavos, N. (2022). Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare. *Cryptography, 6(3)*, pp. 45-56.

Ubaidurrahman, N. H., Balamurugan, C. & Mariappan, R. (2015). A novel DNA computing based encryption and decryption algorithm. *Procedia Computer Science, 46(2)*, pp. 463-475.

Ullah, F., Habib, M. A., Farhan, M., Khalid, S., Durrani, M. Y. & Jabbar, S. (2017). Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. *Sustainable cities and society, 34(5)*, pp. 90-96.

Umapathy, B. & Kalpana, G. (2023). A Key Generation Algorithm for Cryptographic Algorithms to Improve Key Complexity and Efficiency. *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*. Tirunelveli, India: IEEE. pp. 647-652.

Vaida, M.-F., Terec, R., Tornea, O., Ligia, C. & Vanea, A. (2010). DNA Alternative Security, Advances in Intelligent Systems and Technologies *Proceedings ECIT-2010, 6th European Conference on Intelligent Systems and Technologies*. Romania. pp. 07-18.

Van Dongen, J., Gordon, S. D., Mcrae, A. F., Odintsova, V. V., Mbarek, H., Breeze, C. E., Sugden, K., Lundgren, S., Castillo-Fernandez, J. E. & Hannon, E. (2021). Identical twins carry a persistent epigenetic signature of early genome programming. *Nature communications, 12(1)*, pp. 1-14.

Van Tanh, N., Tri, N. Q., Giang, N. L. & Duy, T.-L. (2021). A Solution to Improve the Security of the Internet of Things Network with Lightweight Encryption Methods. *Journal of Physics: Conference Series*. IOP Publishing. pp. 012042-012056.

Veluvarthi, R., Rameswarapu, A., Kalyan, K. S., Piri, J. & Acharya, B. (2023). Security and Privacy Threats of IoT Devices: A & Short Review. *2023 4th International Conference on Signal Processing and Communication (ICSPC)*. Tamilnadu, India: IEEE. pp. 32-37.

Vikram, A., Kalaivani, S. & Gopinath, G. (2019). A Novel Encryption Algorithm based on DNA Cryptography. *2019 International Conference on*

Communication and Electronics Systems (ICCES). Coimbatore, India: IEEE. pp. 1004-1011.

Vinay, S., Pujar, A., Kedlaya, H. & Shahapur, V. S. (2019). Implementation of DNA cryptography based on dynamic DNA sequence table using cloud computing. *International Journal of Engineering Research & Technology (IJERT), 7(8),* pp. 1-4.

Wang, C. & Heys, H. M. (2009). An ultra compact block cipher for serialized architecture implementations. *2009 Canadian Conference on Electrical and Computer Engineering*. St. John's, NL, Canada: IEEE. pp. 1085-1090.

Wang, M. (2008). Differential cryptanalysis of reduced round PRESENT. *International Conference on Cryptology in Africa*. Casablanca, Morocco: Springer. pp. 40-49.

Wang, T. & Wang, M.-H. (2020). Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. *Optics & Laser Technology*, *132(14),* pp. 106355-106367.

Wei, C. C. & Nyamasvisva, T. E. (2022). DNA-based Approach of Security Analysis for Cloud-based ERP System. *International Journal of Engineering Research and Applications*, *12(9),* pp. 38-42.

Williams, D. (2008). The tiny encryption algorithm (TEA). *Network Security*, *26(4),* pp. 1-14.

Windarta, S., Suryadi, S., Ramli, K., Lestari, A. A., Wildan, W., Pranggono, B. & Wardhani, R. W. (2023). Two New Lightweight Cryptographic Hash Functions Based on Saturnin and Beetle for the Internet of Things. *IEEE Access*, *8(1),* pp. 58-69.

Wu, J., Shi, J. & Li, T. (2020). A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion. *Entropy*, *22(1),* pp. 5-16.

Wu, W. & Zhang, L. (2011). LBlock: A lightweight block cipher. *International conference on applied cryptography and network security*. Rome, Italy: Springer. pp. 327-344.

Wu, Z., Pan, P., Sun, C. & Zhao, B. (2021). Plaintext-related dynamic key chaotic image encryption algorithm. *Entropy*, *23(9),* pp. 1159-1167.

Xu, S., Wang, Y., Wang, J. & Tian, M. (2008). Cryptanalysis of two chaotic image encryption schemes based on permutation and xor operations. *2008*

International Conference on Computational Intelligence and Security. Suzhou, China: IEEE. pp. 433-437.

Yan, H., Luo, Y., Chen, M. & Lai, X. (2019). New observation on the key schedule of RECTANGLE. *Science China Information Sciences, 62(3)*, pp. 1-13.

Yao, G., Zhang, F., Wang, F., Peng, T., Liu, H., Poppleton, E., Šulc, P., Jiang, S., Liu, L. & Gong, C. (2020). Meta-DNA structures. *Nature chemistry, 12(11)*, pp. 1067-1075.

Yap, H., Khoo, K., Poschmann, A. & Henricksen, M. (2011). EPCBC-a block cipher suitable for electronic product code encryption. *International Conference on Cryptology and Network Security*. Nerja (Malaga), Spain: Springer. pp. 76-97.

Yasser, I., Khalil, A. T., Mohamed, M. A., Samra, A. S. & Khalifa, F. (2021). A robust chaos-based technique for medical image encryption. *IEEE Access, 10(3)*, pp. 244-257.

Z'aba, M. R., Jamil, N., Rusli, M. E., Jamaludin, M. Z. & Yasir, A. a. M. (2014). I-present tm: An involutive lightweight block cipher. *Journal of Information Security, 2014(5)*, pp. 114-122.

Zahid, A. H., Arshad, M. J., Ahmad, M., Soliman, N. F. & El-Shafai, W. (2023). Dynamic S-Box Generation Using Novel Chaotic Map with Nonlinearity Tweaking. *Computers, Materials & Continua, 75(2)*, pp. 3012-3026.

Zakaria, A. A., Azni, A., Ridzuan, F., Zakaria, N. H. & Daud, M. (2020). Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT. *IEEE Access, 8(2)*, pp. 198646-198658.

Zakaria, A. A., Azni, A., Ridzuan, F., Zakaria, N. H. & Daud, M. (2020). Modifications of Key Schedule Algorithm on RECTANGLE Block Cipher. *International Conference on Advances in Cyber Security*. Penang, Malaysia: Springer. pp. 194-206.

Zakaria, A. A., Azni, A., Ridzuan, F., Zakaria, N. H. & Daud, M. (2020). Modifications of key schedule algorithm on RECTANGLE block cipher. *Advances in Cyber Security: Second International Conference, ACeS 2020*. Penang, Malaysia: Springer. pp. 194-206.

Zhang, C., Chen, J., Chen, D., Wang, W., Zhang, Y. & Zhou, Y. (2023). Exploiting Substitution Box for Cryptanalyzing Image Encryption Schemes with DNA Coding and Nonlinear Dynamics. *IEEE Transactions on Multimedia, 2023(2)*, pp. 12-32.

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

Zhang, X., Chen, J., Li, T., Dai, G. & Wang, C. (2023). LILP: A Lightweight Enciphering Algorithm to Encrypt Arbitrary-Length Messages. *Symmetry, 15(1)*, pp. 177-185.

Zhang, X. & Wang, X. (2019). Multiple-image encryption algorithm based on DNA encoding and chaotic system. *Multimedia Tools and Applications, 78(6)*, pp. 7841-7869.

Zhang, X., Zhou, Z. & Niu, Y. (2018). An image encryption method based on the feistel network and dynamic DNA encoding. *IEEE Photonics Journal, 10(4)*, pp. 1-14.

Zhu, D., Wang, S., Huang, Z., Zhou, C. & Zhang, L. (2023). A JAYA algorithm based on normal clouds for DNA sequence optimization. *Cluster Computing, 2023(6)*, pp. 1-17.

Zhu, R., Zhang, X., Liu, X., Shu, W., Mao, T. & Jalaian, B. (2015). ERDT: Energy-efficient reliable decision transmission for intelligent cooperative spectrum sensing in industrial IoT. *IEEE Access, 3(2)*, pp. 2366-2378.

Zou, C., Wang, X., Zhou, C., Xu, S. & Huang, C. (2022). A novel image encryption algorithm based on DNA strand exchange and diffusion. *Applied Mathematics and Computation, 430(2)*, pp. 127291-127306.

VITA

The author of this thesis is Maria Imdad, born in Pakistan on 6th February 1991. She did her degree in Software Engineering from Riphah International University Islamabad in 2013. In 2017 she did her MS in Information Security from Air University Islamabad. During her MS, she worked as an intern in the research and development wing of Military College of Signals (MCS) Rawalpindi, Pakistan. After completing her MS she started working as a lecturer in University of Lahore Islamabad Campus for two years. Her passion of research and improving the knowledge in Information Security, she completed her PhD research at Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia. Additionally, she has published numerous international conference and journal papers during her PhD. Her research interests are in the area of, information security, DNA-based cryptography, and software engineering.