Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 3544-3549*

Research Article

Improving Highest Security Lightweight block cipher (HISEC) Algorithm Using Key Dependent S-box

WarkaaSalimNajm[a], SufyanSalimMahmoodAldabbagh[b], Mustafa Ali Abuzaraida[c],AlyaaGhanim[d] Khalid Abdulkareem Al-Enezi[e]

[a,b]Department of Computer Science, University of Mosul, Iraq
[c]Data Science Res Lab, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia
[d]Software Department, University of Mosul, Iraq
[e]Computer Science Dept., Central Agency for Information Technology, Kuwait
Email:[a]wardalbaker@gmail.com, [b]sufyansalim_77@yahoo.com,
[c]abuzaraida@uum.edu.my,[d]alyaa.ghanim@uomosul.edu.iq, [e]alenezi.khaled@yahoo.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Information security is considered as a very critical issue in the transmission of information. Therforelossing or threatening the information transmission will therefore be a great loss in the process of transmitting the information. Recently, Lightweight block cipher Algorithms have gained wide acceptance and it is used in restricted applications, such as electronic passport, smart card, etc. In this study, a modified HISEC algorithm is proposed to enhance and improve the original HISEC algorithm by introducing the concept of a key dependent S-box. This proposal algorithm aims to generate a safer block of code and solve the problem of the fixed structure of the used S-box that was a vulnerability for the attacker. It was an impenetrable barrier facing the attacks of the (Linear cryptanalysis) and (Differential Cryptanalysis). The proposed algorithm showed some improvements when comparing it to the orginal algorithm.

Keywords: Security, Cryptography, Block Ciphers, Highest Security Lightweight block cipher, S-box

1. Introduction

There are many important applications that need high security lightweight block cipher algorithm like credit card, electronic passport, etc. After the evolution of electronic and communication applications, RFID technology has been used in many aspects of life, such as access control, parking and management, identification and goods tracking etc. [1]. In this type of new encryption algorithm, applications of RFID technology have limitations, such as poor computational power, and the small storage space of that traditional block encryption such as AES which is not suitable for this kind of very restrictive environment. Thus, in recent times, lightweight block cipher algorithms have encountered a lot of interest compared with traditional block ciphers, lightweight block cipher algorithms have three main characteristics:[2] [3].

- Security: Increasing the length of the key will increase security and cost, and vice versa.
- Performance: Increasing cycles will increase security and reduce performance and vice versa.
- Cost: The representation of the Hardware algorithm depends on cost.

High security lightweight block cipher algorithm have gained more attention recently. A recent study was handled by Jahan et al (2017) [4]. In this study, an investigation on the issue aiding write operations on the out-sourced data for clients using mobile devices was presented. The Ciphertext-Policy Attribute-based Encryption (CP-ABE) scheme was considered because it is convenient in aiding access control in outsourced cloud environments. One of the flaws of CP-ABE is that users can adjust the access policy stated by the data owner if write operations are included in the scheme. To solve this matter, a protocol was proposed for collaborative processing of outsourced data that allows the authorized users to carry out write operation without being able to change the access policy stated by the data owner. The scheme went along with a light weight signature scheme. The implementation and comprehensive performance analysis of the scheme indicated that the proposed scheme was satisfactory for real mobile applications. Moreover, the security analysis indicates that the security characteristics of the system were not exposed.

Another study was done by Jadoon et al (2018) [5]. A study about developments in vehicular networks from the point of view of lightweight cryptographic protocols and privacy maintaining algorithms were presented. They argued that lightweight cryptographic protocols play an important part in order to address the upcoming security issues in future automotive technology, especially regarding vehicular safety and Traffic efficiency. Security

concerns for the future automotive industry is acting as an obstacle in the broad distribution of vehicular networks commercially. There is a need for comprehending security risks and coming up with a resolution to secure automotive technology by either developing new lightweight cryptographic protocols or using existing algorithms in an efficient way. The public adoption for new technology in vehicular networks can only be guaranteed by improving the security and privacy of users.

Also Usman et al (2017) [6] proposed a lightweight encryption algorithm which was named Secure IoT (SIT). It was based on a 64-bit block cipher and requires 64-bit key to encrypt the data. The architecture of the algorithm was a combination of feistel and a uniform substitution-permutation network. Their result showed the algorithm provides substantial security in just five encryption rounds. Another study was done by Avik et al (2018) [7]. Here, a lightweight sponge mode for AE focusing on the state size as well as optimizing the security was presented. It was instantiated with two versions, where the first version Beetle [Light+] aimed to be lightweight and the second version Beetle [Secure+] aims to be highly secure. Also, the hardware implementation results were presented, which demonstrated the effectiveness of their approach.

Another study was performed by Nilupulee A. Gunathilake et al (2019) [8], they discussed the execution, issues and futuristic applications of LWC algorithms for smart IoT devices, especially the efficiency of Long-Range Wide Area Network (LoRaWAN) which is an open standard that decribes the communication protocol for Low-Power Wide Area Network (LPWAN) technology. The final evaluation showed promising possibilities in the direction of successful implementation of LWC and its performance towards 5GN smart cities.

In this paper, an enhanced modified HISEC algorithm is proposed. The proposed algorithm showed a quality performences after passing some testing stages.

2.The Highest Security Lightweight Block Cipher Algorithm (Hisec)

In this algorithm the following features were used: splitting the plain text into two parts, using the S-box for the whole text, switching bits, is (rotation and XOR), as well as the process of exchanging between two parts and an action Key update. HISEC uses non-fixed size plain text and is processed on a 64-bit block and 80-bit key size. There are 16 rounds and, in each round, there are operations such as: Substitution with S-box, Bit Permutation, XOR, Rotate operation as well as key update, and moreover there is XOR between the encoder text and the key in the last session. HISEC has four layers as shown in figure 1. [2]

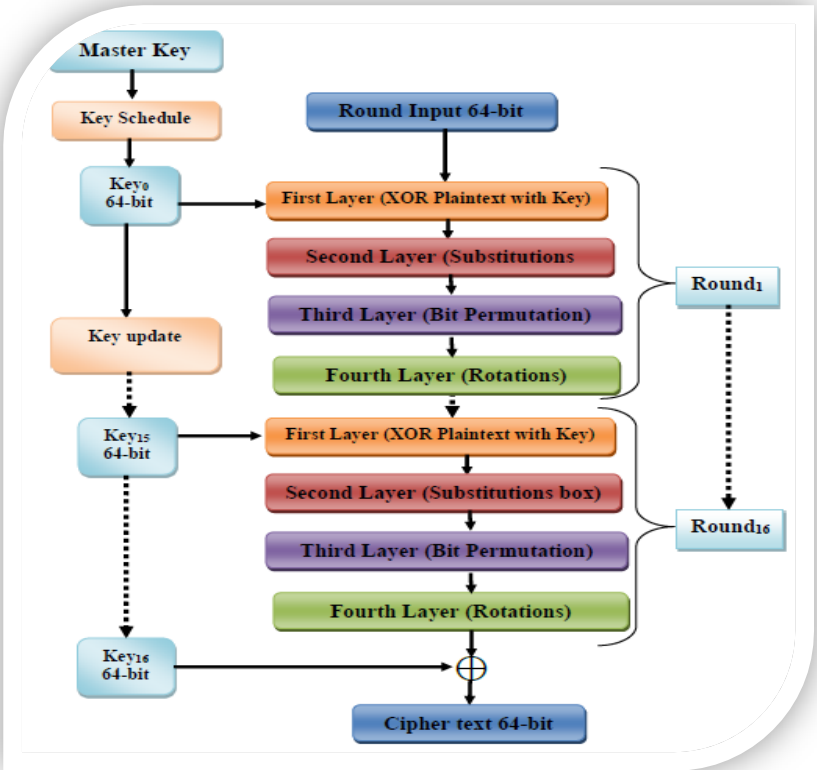

Figure (1): HISEC Layers

3.ImprovedHisec Algorithm

Layer 2 in HISEC is one of the most important layers and the fact that S-boxes depend on the unknown key is the major advantage of the algorithm; because linear cryptanalysis and differential cryptanalysis require well-known S-boxes. [2] Therefore, the process of improvement of the HISEC algorithm will be in that layer.

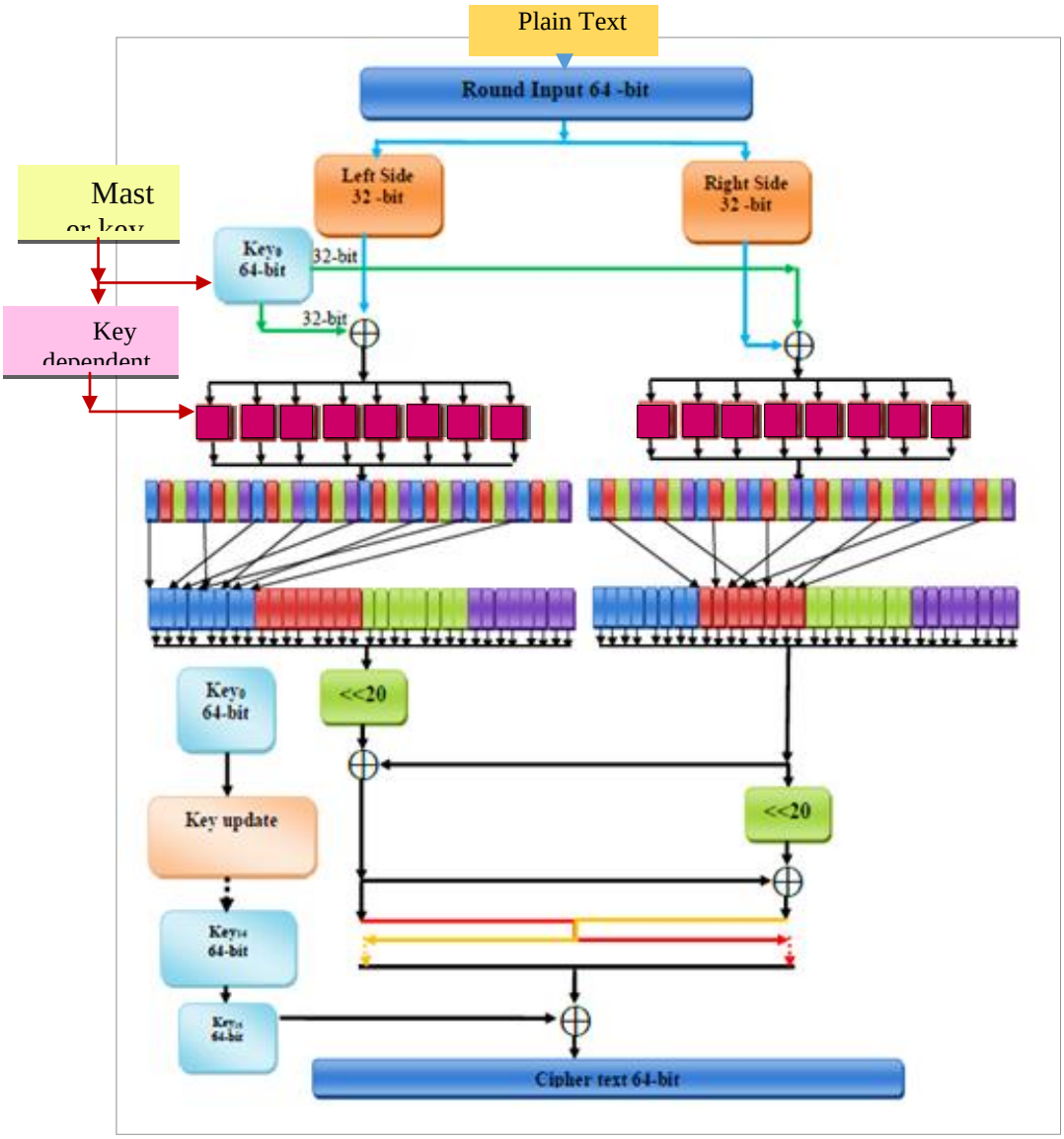

Figure (2) All layers of Proposed HISEC Algorith

The S-boxes as shown in Figure 4 are use in the proposed algorithm. These S-boxes will be used randomly depending on the key without any changes to the basic operations of the algorithm. This concept is called S-boxes Key dependent. When the S-box is static, it means that the S-box itself will be used in every cycle, and this represents a gateway for the attacker to enter (Linear & Differential cryptanalysis), which allows the attacker to study the S-box and find weaknesses in it. However, when the S-box is dynamic which means that it depends on the key, it is difficult for an attacker to study the S-box [9-11]

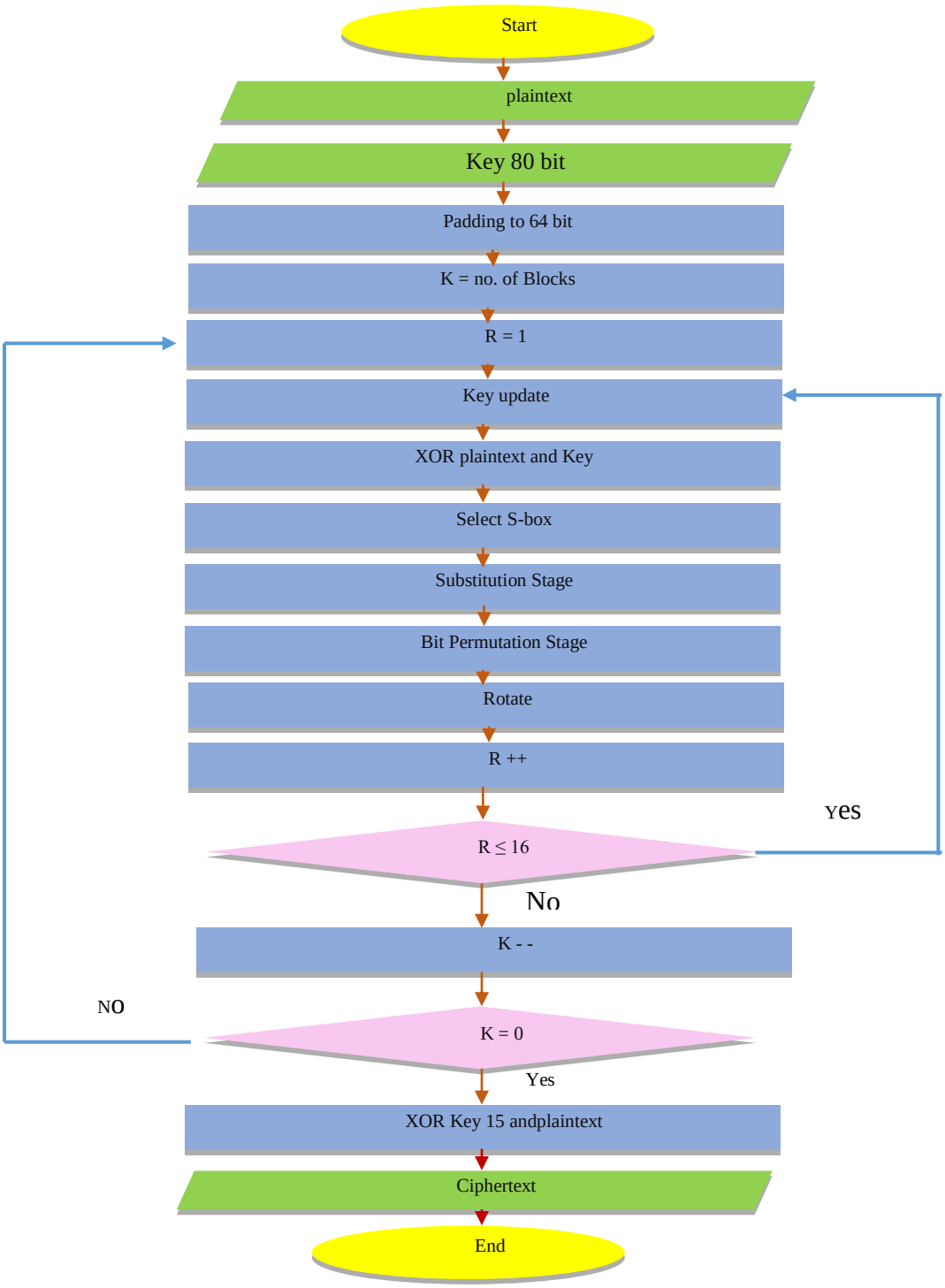

Figure (3) Flowchart of proposed HISEC Algorithm

S0:	3	8	15	1	10	6	5	11	14	13	4	2	7	0	9	12
S1:	15	12	2	7	9	0	5	10	1	11	14	8	6	13	3	4
S2:	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2
S3:	0	15	11	8	12	9	6	3	13	1	2	4	10	7	5	14
S4:	1	15	8	3	12	0	11	6	2	5	4	10	9	14	7	13
S5:	15	5	2	11	4	10	9	12	0	3	14	8	13	6	7	1
S6:	7	2	12	5	8	4	6	11	14	9	1	15	13	3	10	0
S7:	1	13	15	0	14	8	2	11	7	4	12	10	9	3	5	6

Figure (4): All S-boxes used in improved HISEC

S-box Key dependent in improved HISCE algorithm is discribed in Figure 5. The size of the main key is 80 bits and the primary key was taken from the left side. From the position of the primary key, 3 bits will be obtained to represent the number of the S-box.

It is worth noting in the improved HISEC algorithm that the probability of selecting the S-box is $(2)^3$ and since there are eight S-boxes, the probability of selecting eight S-boxes in one round is $(2)^{24}$ as the improved HISEC algorithm consists of 16 a cycle. The total probability of all rounds of selecting a S-box is $(2)^{384}$, which is a large number that is difficult to be known and guessed when S-box is chosen.

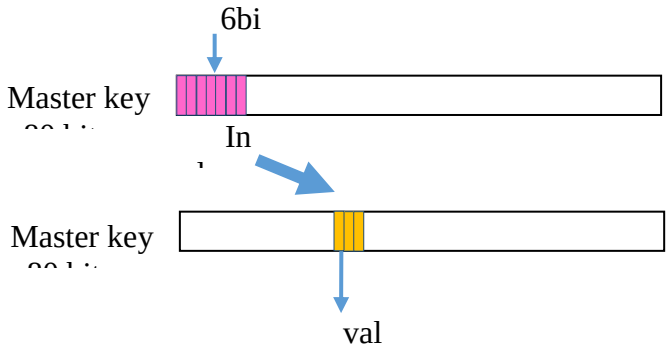

Figure (5) Process of key dependent S-box in proposed HISEC Algorithm

4.Security Discussion

Cryptanalysis is a major element in examining the security of the algorithm as it is used to evaluate the security of any algorithm and this is done by using the cryptanalysis test. One of the famous attack is the differential attack where it is the most effective method to determine the resistance of any encryption algorithm against the differential cryptanalysis is to count the minimum active S-box. The number of active S-box for the proposed **HISEC** algorithm after 16 rounds is 124 while this attack can not count the minimum active s-box for the proposed algorithm because the s-boxes are unknown.

5.Cost Discussion

The cost of the algorithm is an important factor in the design of any algorithm [12, 13]. Here, it shows thecalculated cost of the proposed HISEC algorithm according to each operation in the algorithm based on what will be done and what it requires from GE. As the process of storing one bit of data requires (6 GE), the use of one S-box requires (22) GE), OR requires (1.33GE), MUX (Multiplexing) requires (2.67GE). [2].

The cost will be calculated as follows:

• 64-bit size plaintext: the cost is 64 x 6 = 384 GE.

• 80 bits the size of the master key: the cost is 80 x 6 = 480 GE.

• 16 S-boxes for both the left and right sides: the cost is 16 x 22 = 352 GE.

• 4 XOR operations per 32 bits: the cost is 4 x 87 = 384 GE.

• 50 GE additional cost.

• a key update process in every cycle: we use one of the S-box x 22 + the used S-box selection (MUX) 4 bits x multiplied by 2.67 + plus 8 bits x 2.76 = 22 + 22.08 + 10.68, so the total is 54.76 GE.

• The total product is 384 + 480 + 352 + 384 + 50 + 54.76 = 1704.76 GE.

The cost of HISEC is 1694GE which is roughly equal to the cost of proposed HISEC algorithm.

6.Experiments And Results

In the cryptography field, the Avalanche test refers to the random characteristic of cryptographic algorithms in general [8]. It is an examination through which it is possible to know the extent of the randomness of the algorithm used for encoding. In this experiment, a 64-bit Plaintext (Abdallah) with an 80-bit Key (ComputerSc) in the first case was used. Then using the same plaintext with one bit change in the key (CnmputerSc) also is encoded. It is found that the value of Avalanche test is nearly half as in Table (1). In block cipher algorithms, when a small change occurs in the original text or key, it leads to a very large change in the ciphertext. If the encoded text achieves the Avalanche test with a value much more than half or with a value much less than half, this indicates weakness of randomness. Avalanche test is calculated according to Equation 1 [12-15].

$$\text{Avalanche Test} = \frac{\text{No.of bits flipped in cipher text}}{\text{Total no. of bits in cipher text}} \qquad \text{Equation (1)}$$

Table (1) An example to explain Avalanche Test in proposed HISEC algorithm

	The data before the bit changed in the key	The data after the bit changed in the key
Plaintext	Abdallah (64bit)	Abdallah (64bit)
Key	ComputerSc(80bit)	Cnmputer Sc (80bit)
Ciphertxt	1100110010000000100101000000101011011111001001000010011111110010	1101100000100001111000001110110001111110001000110110100110101010
Avalanche test	0, 453125	

7.Conclusions

In this paper, an improved HISEC algorithm was proposed. Through the results of the work in this research, the proposed algorithm passed the Avalanche test and it achieved high security results in encrypting electronic passport data because the S-box is not fixed and its choice depends on the key used in the encryption. Also, the improved HISEC algorithm is resistant to linear cryptanalysis and Differential Cryptanalysis. Last, the cost of the improved HISEC algorithm is nearly equal to the cost of HISEC algorithm.

References

M. D. Shutin and D. V. Dolgov, "Creating a Digital Passport of the Object During the Survey of Transport Infrastructure," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 2019, pp. 1485-1487.

S. S. M. AlDabbagh, et al., "Hisec: A new lightweight block cipher algorithm," in Proceedings of the 7th International Conference on Security of Information and Networks, 2014, p. 151.

Bhattasali, T., "Licrypt: Lightweight cryptography technique for securing smart objects in internet of things environment", CSI Communications 2013.

Jahan, Mosarrat, Mohsen Rezvani, Qianrui Zhao, ParthaSarathi Roy, Kouichi Sakurai, ArunaSeneviratne, and Sanjay Jha. "Light weight write mechanism for cloud data." IEEE Transactions on Parallel and Distributed Systems 29, no. 5 (2017): 1131-1146.

Jadoon, Ahmer Khan, Licheng Wang, Tong Li, and Muhammad Azam Zia."Lightweight cryptographic techniques for automotive cybersecurity."Wireless Communications and Mobile Computing 2018 (2018).

Usman, Muhammad, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, and Usman Ali Shah. "SIT: a lightweight encryption algorithm for secure internet of things." arXiv preprint arXiv:1704.08688 (2017).

Chakraborti, Avik, NilanjanDatta, Mridul Nandi, and Kan Yasuda. "Beetle family of lightweight and secure authenticated encryption ciphers." IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 218-241.

Gunathilake, Nilupulee A., William J. Buchanan, and RameezAsif. "Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications." In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pp. 707-710. IEEE, 2019.

Y. S. Chauhan and T. N. Sasamal, "Enhancing Security of AES Using Key Dependent Dynamic Sbox," International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 468-473.

Kazlauskas, K. et al. "An Algorithm for Key-Dependent S-Box Generation in Block Cipher System." Informatica 26 (2015): 51-65.

Bhanot, R., & Hans, R., "A review and comparative analysis of various encryption algorithms", International Journal of Security and Its Applications, 9(4),2015, 289-306.

Singh, B., Alexander, L., &Burman, S., "On Algebraic Relations of Serpent S-Boxes", IACR Cryptology ePrint Archive, 2009, 38.

Krishnamurthy, G. N., &Ramaswamy, V., "Making AES stronger: AES with key dependent S-box", IJCSNS International Journal of Computer Science and Network Security, 8(9), 2008, 388-398.

Azzawi, H. M., "Enhancing the encryption process of Advanced Encryption Standard (AES) By Using Proposed Algorithm To Generate S-Box", Journal of Engineering and Sustainable Development, 18(2),2015, 89-105.

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., &Udzir, N. I., "A New DNA-Based S-Box", Int. J. Eng. Technol, 15, 2015, 1-9.