International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 11, Issue 9 [September. 2022] PP: 43-46

Security Criterion Analysis for Block Cipher Using S-Box Evaluation Tool and Cryptanalysis Tool

ChngChern Wei[1], Siew Woei Shen[2], Law Teng Yi[3], Tee Eng Hong[4]
[1,2,3,4]*Faculty of Computer Science & Information Computing Technology,*
New Era University College, Kajang, MALAYSIA
Corresponding Author:ChngChern Wei

ABSTRACT

Cryptography is a technique used to secure communication and transmission of data through an insecure network with a cryptographic system. It that means the data sent has been encrypt. A cryptographic system is a set of cryptographic algorithms that can improve the data security in order to maintain trust in the protection of more secure data [4][13]. To ensure the cryptographic algorithm is secure and able to provide high resistance against the cyber-attacks, the S-bot Evaluation Tools (SET), Linear Cryptanalysis Tools (LCT) and Differential Cryptanalysis Tool (DCT) are the relevant tools to evaluate the security strength for the block cipher algorithm. SET, LCT and DCT is able to provide an accurate computation analysis for the block cipher algorithm.

KEYWORDS:S-Box, SET, cryptographic, Linear Cryptanalysis, Differential Cryptanalysis

---

Date of Submission: 01-09-2022 Date of Acceptance: 13-09-2022

---

1. INTRODUCTION

Cryptography is a technique used to secure communication and transmission of data through an insecure network with a cryptographic system. It that means the data sent is encrypted. A cryptographic system is a set of cryptographic algorithms that can improve the data security in order to maintain trust in the protection of more secure data [4][13].There are two ways of encryption techniques, namely asymmetric encryption and symmetric encryption. The algorithm of asymmetric encryption is involve complex mode of encryption. This is because the asymmetric encryption is contains of keys and the algorithm involve the process of keys distribution during the data encryption and decryption for the data security [10][11][12].

2. LITERATURE REVIEW

According to the researcher Wang's [2], the strong S-box is a critical part for ensuring the block cipher able to provide the security to the algorithm.In order to provide the strength of the s-box, the design of an evaluation on the security of the S-box and the design of the performance of the S-box is an important criterial[1][3]. Performance criteria are Balance, Bijective, Nonlinearity, Avalanche Effect, Bit Independence Criterion and Strict Avalanche Criterion [5][6][7][11] as projected in the Table 1.

Performance criteria	Jie, C., Wei, Y., & Hong, Z. (2015) [5]	Wei, C.C., Sharifah, Taufik, M., Udzir, N.I. (2018) [11]	Ronielle, B.A., Ariel, M.S., &Ruji, P.M. (2019) [6]	Ardabek, et al., (2022) [7]
Balance	√	√	√	√
Bijective	√	√	√	√
Nonlinearity	√	√	√	√
Avalanche Effect	√	√	√	√
Bit Independence Criterion	√	√	√	√
Strict Avalanche Criterion	√	√	√	√

Table 1: S-Box Performance Criteria [5][6][7][11]

2.1 Linear Cryptanalysis Tool (LCT)

Linear Cryptanalysis is a technique for attacking an SPN. It uses a linear approximation to an S-box to form a probabilistic assessment of the plaintext corresponding to an encoded message [1].
Denote the input bits to an S-box by $X_1X_2...\ X_n$ and the bits of the corresponding output by $Y_1Y_2...Y_n$.
Perfect secrecy requires that the ciphertext give not indication as to the contents of the plaintext, so that for any i and j,$X_i$xorY_j= 0 and $X_i$xorY_j= 1, should each have probability of half [10][11][12].

2.2 Differential Cryptanalysis Tool (DCT)

Differential Cryptanalysis classified as a non-generic cryptanalysis technique. The purpose of this technique is to find the loophole of the block cipher and break the block cipher [11].

Cryptanalysis Tool	Guo, Q.L. & Chen, H.J. (2016) [8]	Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., &Udzir, N. I. (2015) [12]	Lucia, L.B. (2011) [9]	Ayman, M.H. (2020) [10]
Linear Cryptanalysis Tool (LCT)	√	√	√	√
Differential Cryptanalysis Tool (DCT)		√	√	√

Table 2: Linear & Differential Cryptanalysis Tools Used by the Researchers [8][9][10][12]

3. RESULT VIEW

The experimental results shown in the Figure 1, Figure 2 and Figure 3 for the S-Box Evaluation Tool (SET), Linear Cryptanalysis Tool (LCT) and Differential Cryptanalysis Tool (DCT).

3.1 S-Box Evaluation Tool (SET)

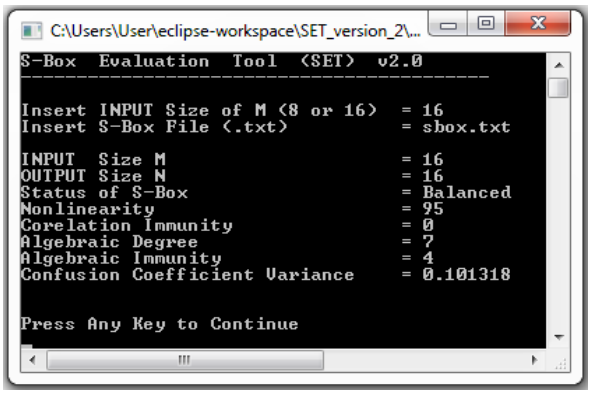

Figure 1: Result of S-Box Evaluation for the DNA-Based Block Cipher

3.2 Linear Cryptanalysis Tool (LCT)

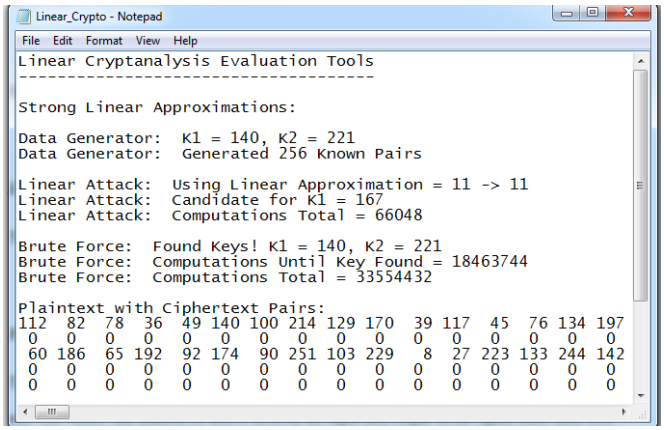

Figure 2: Result of Linear CryptanalysisAnalysis for the DNA-Based Block Cipher

3.3 Differential Cryptanalysis Tool (DCT)

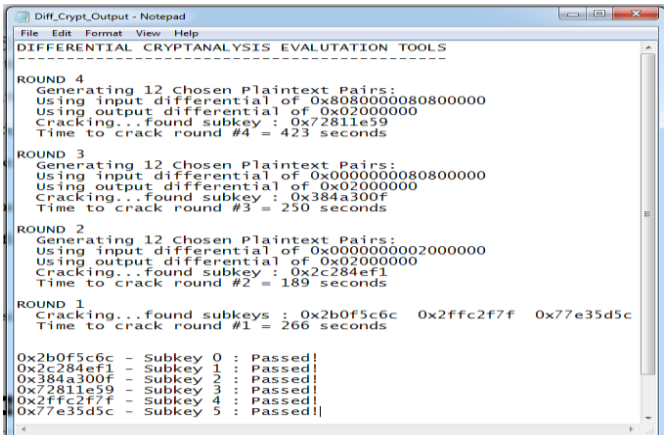

Figure 3: Result of Differential Cryptanalysis Analysis for the DNA-Based Block Cipher

4. RESULTS

The S-box Evaluation Tool (SET) has evaluated the AES block cipher algorithm and DNA-based block cipher algorithm using the properties of balance, bijective, nonlinearity, bit independence criterion and strict avalanche criterion. The results have met the balance and the properties of both AES block cipher algorithm and the DNA-based block cipher algorithm. The simulation results of nonlinearity tested using S-box Evaluation Tool (SET) and achieved a result of 95; the Strict Avalanche Criterion (SAC) valued of 0.5334, and the Bit Independence Criterion (BIC) has valued of -0.0264. The results of Linear Cryptanalysis for the DNA-based Block Cipher using the Linear Cryptanalysis Tool (LCT) shown the results is strong Linear Approximations with the computation in total of 66,048 seconds for the Linear Attack and computation until key found is 18,463,744 seconds for the Brute Force attacks.The results of Differential Cryptanalysis for the DNA-based Block Cipher using the Differential Cryptanalysis Tool (DCT) shown the results is able to provide the strong sub-key.

5. CONCLUSION

Using the S-Box Evaluation Tool (SET), Linear Cryptanalysis Tool (LCT) and Differential Cryptanalysis Tool (DCT) is able to simulate the results of security analysis for the S-Box, and the block cipher algorithm for the Linear and Differential attacks. As the results, the DNA-based Block Cipher is able to provide the security of against resistance of Linear Cryptanalysis and Differential Cryptanalysis for the DNA-based Block Cipher.

REFERENCE

[1]. Singh, A., Agarwal, P., & Chand, M. (2017). Analysis of Development of Dynamic S-Box Generation. Computer Sci. Inf. Technol., Vol. 5, No. 5, pp. 154-163.

[2]. Wang, Y., Lei, P., &Wong, K.W. (2015). A Method for Constructing Bijective S-Box with High Nonlinearity Based on Chaos and Optimization. Int. J. Bifurc. Chaos, vol. 25, no. 10, p. 1550127, 2015.

[3]. Wang, Y., Xie, Q., Wu, Y., & Du, B. (2009). A software for S-box performance analysis and test. Proc. - 2009 Int. Conf. Electron. Commer. Bus. Intell. ECBI 2009, pp. 125–128, 2009.

[4]. Goutam, R.K. (2015). Importance of Cyber Security. Int. J. Comput. Appl., vol. 111, no. 7, pp. 975--8887

[5]. Jie, C., Wei, Y., & Hong, Z. (2015). An Improved AES S-Box and Its Performance Analysis. International Journal of Innovative Computing, Information and Control Volume 7, Number 5(A), May 2011

[6]. Ronielle, B.A., Ariel, M.S., &Ruji, P.M. (2019). Performance Analysis of the Modified Generated S-Box for Advanced Encryption Standards. DSIT 2019: Proceedings of the 2019 2nd International Conference on Data Science and Information Technology, July 2019 p.p. 117–121 https://doi.org/10.1145/3352411.3352429.

[7]. Ardabek, K., Nursulu, K., Kunbolat, A., Dimukhanbet, D. &Kairat, S. (2022). Design of Substitution Nodes (S-Boxes) of a Block Cipher Intended for Preliminary Encryption of Confidential Information. Cogent Engineering, 9:1, 2080623, DOI: 10.1080/23311916.2022.2080623

[8]. Guo, Q.L. & Chen, H.J. (2016). Linear Cryptanalysis of PRESENT-like Ciphers with Secret Permutation. Security in Computer Systems and Networks The Computer Journal, Vol. 59 No. 4, 2016

[9]. Lucia, L.B. (2011). Linear and Differential Cryptanalysis of Reduced-Round AES. Tatra Mathematical Publications 50(2011), pp. 51-61. DOI:10.2478/v10127-011-0036-y

[10]. Ayman, M.H. (2020). A New KD-3D-CA Block Cipher with Dynamic S-Box Based on 3D Cellular Automata. Universiti Putra Malaysia.

[11]. Wei, C.C., Sharifah, Taufik, M., Udzir, N.I. (2018). New DNA Based Dynamical S-Box for Block Cipher. International Journal of Engineering Research and Applications (IJERA), vol. 8, no.7, 2018, pp.64-69

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

[13]. Wei, C.C. (2014). DNA Approach for Password Conversion Generator. IEEE: 2014 International Symposium on Biometrics and Security Technologies (ISBAST)