European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com

e-ISSN: 2421-826X

DOI: 10.15405/epms.2022.10.57

ICONSPADU 2021
International Conference on Sustainable Practices, Development and Urbanisation

ANALYSE ON AVALANCHE EFFECT IN CRYPTOGRAPHY ALGORITHM

Kamsiah Mohamed (a)*, Mohd Nazran Mohammed Pauzi (b), Fakariah Hani Hj Mohd Ali (c), Suriyani Ariffin (d)
*Corresponding author

(a) Faculty of Communication, Visual Art and Computing, Universiti Selangor, Bestari Jaya, Malaysia, kamsh@unisel.edu.my
(b) Faculty of Engineering and Life Sciences, Universiti Selangor, Bestari Jaya, Malaysia, nazran@unisel.edu.my
(c) Faculty of Computer Science and Mathematical Sciences, Universiti Teknologi MARA, Malaysia, fakariah@tmsk.uitm.edu.my
(d) Faculty of Computer Science and Mathematical Sciences, Universiti Teknologi MARA, Malaysia

Abstract

Developments in computers and technologies have created an intense need for secure and trustworthy cryptography systems. Highly secure schemes are always desirable for real-world applications. Cryptography requires a secure technique to ensure that the enemy is prevented while securing legitimate users who have access to the data. The avalanche effect is one of the most preferred approaches for determining an algorithm's security in cryptography. In this paper, the experimental process is conducted to examine the sensitivity of the algorithm when a one-bit input is changed in the key, which causes changes on approximately half of the ciphertext. The experiment is performed based on the key avalanche in the proposed block cipher algorithm. These processes were done 32 times based on the 32-bit plaintext on the algorithm and the avalanche effect was calculated in each time based on the ciphertext generated. However, if a block cipher does not exhibit the avalanche effect to a significant degree, it indicates that it has weak randomisation. Hence, the input can be predicted by a cryptanalyst, while only being given the output. From the experiment, the findings revealed that the proposed block cipher algorithm met the key avalanche with a 50% output bit changed in the ciphertext. Therefore, the proposed block cipher scheme satisfies the avalanche effect property, resulting in improved diffusion.

Keywords: Avalanche, block cipher, cryptography, ciphertext, encryption

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

Cryptography has emerged as the most important approach for protecting data against unauthorized access. Cryptography has always been in our daily lives. Almost every time we use the Internet to make a payment, check an account, send and receive an email, make a purchase, and so on. However, data must be protected from hacking, noise, and interference due to the widespread use and sharing of data on the Internet (Yassein et al., 2017). Therefore, cryptography allows two or more parties to communicate securely. In order to communicate securely, the key is needed to hide and protect the information. Cryptography requires a secure technique to ensure that the enemy is prevented while securing legitimate users to gain access to information. Thus, the design of symmetric key cryptography is often enhanced to ensure that information is secure. Meanwhile, symmetric key cryptography is utilized in a variety of applications to protect data. This technique is called a secret key where the same key is used to encrypt or decrypt the data. Encryption means that the plaintext is converted into the ciphertext while decryption means that the ciphertext is converted into the plaintext. According to Latif et al. (2020) encryption is an excellent countermeasure against hackers' vulnerabilities, and it aids in the achievement of confidentiality, integrity, and authentication. For both processes, the key is required to encrypt and decrypt the data. Block cipher and stream cipher are two types of symmetric key ciphers. Block cipher contains the block of plaintext with the fixed-length while stream cipher is used to encrypt data one bit or byte at a time. The encryption algorithm is determined by the key in cryptography. If a single bit change in the key has an effect on the number of bits in the cipher (Singla & Bala, 2018). In this paper, the proposed algorithm is designed based on a block cipher. Moreover, Emami (2013) stated that to gain confidence in the security of these algorithms their analysis is always as important as their designs. Therefore, the proposed algorithm will be examined using the strict avalanche effect to determine the algorithm's security requirements. The structure of this paper as follows: In Section 1.1, an overview of an avalanche effect is discussed. The problem statement is stated in Section 2. Section 3 contains research questions and a proposed study is discussed in Section 4. In Section 5, a research method is described and in Section 6, a finding of the proposed algorithm is described and in Section 7, a conclusion is given.

1.1. Overview of an Avalanche Effect

According to Simion (2015) while developing cryptography primitives, they must meet several statistical criteria, which is a strict avalanche. The strict avalanche effect was introduced in 1985 by Webster and Tavares. It defines to a special and desirable characteristic of cryptographic algorithms. It describes a situation in which an input flips a single bit, causing the half-bit flip output to shift dramatically. For example, if a one-bit input change in plaintext or key causes the output bit to change with a probability of ½ bits in the ciphertext, meets the avalanche criterion based on the function $f:\{0,1\}n \rightarrow \{0,1\}n$. Besides, it is harder to perform an analysis of ciphertext, when trying to come up with an attack (Mohamed et al., 2014).

The avalanche effect is one of the most essential factors to consider when assessing a cryptographic algorithm's strength (Ramanujam & Karuppiah, 2011). A study by Nazeh et al. (2018) found that the avalanche effect reflects performance of cryptographic algorithm. In addition, Echeverri

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

(2017) stated that secure cryptographic algorithms must have a strong avalanche effect with a probability of a 50% change in output. Shi et al. (2011) analysed the avalanche effect on the AES S-box and inverse S-box, which then concluded that both S-boxes of AES have a good avalanche effect. Bhoge and Chatur (2014), also demonstrated a good avalanche effect of the AES block cipher. The results obtained were 0.3593, 0.4921, and 0.4453, respectively. Then, Shi et al. (2011) analysed the KASUMI block cipher based on the avalanche effect. When plaintext 50 and 51 bits were altered, 40 bits of the corresponding ciphertext were changed. The average change bit of the ciphertext was 32.2%, almost half of 64 bits. The result shows that the plaintext of the KASUMI algorithm has a good input avalanche effect. Alabaichi and Mechee (2015) analysed the Blowfish algorithm between plaintext and ciphertext. The result indicated different numbers of bits in ciphertext when there was a change of one bit in plaintext. From the results, the Blowfish algorithm presented a good avalanche with a total number of 64-bit sequences. According to Raju et al. (2017), the avalanche effect was considered an isolated check on the integrity of the algorithm. For the avalanche effect, DES has a good avalanche effect of 54.38%. Encarnacion et al. (2020) found that the SIMECK block cipher family's increased round function approach for testing security using the avalanche effect, runtime performance, and brute-force attack on the output ciphertext and its performance. Therefore, the avalanche effect is a desirable property of a block cipher. It is satisfied if each output bit changes with a 50% probability whenever a single input bit is complemented. The presented work resulted in a significant increase in the avalanche effect of the resulted ciphered word.

1.2. Research Questions

In accordance with the above discussion, this study aims to concentrate on the principal research question:

i. Is there an avalanche effect in the ciphertext?
ii. How avalanche effect ensure data security the algorithm?
iii. How to increase security requirements in the algorithm?

2. Purpose of the Study

The proposed block cipher is designed to improve the design of the substitution and permutation functions. For the proposed block cipher**,** the length of the input, output block, and the State were 128 bits. The State is a 4x4 matrix consists of rows and columns, $Nb = 4$ denotes the number of 32-bit words and columns in the State. The length of the cipher key, K, consists of 128 bits**.** The key length is represented by $Nk = 4$. The number of rounds was represented by Nr, where $Nr = 9$ when $Nk = 4$. The proposed block cipher algorithm's design is shown in Figure 1.

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

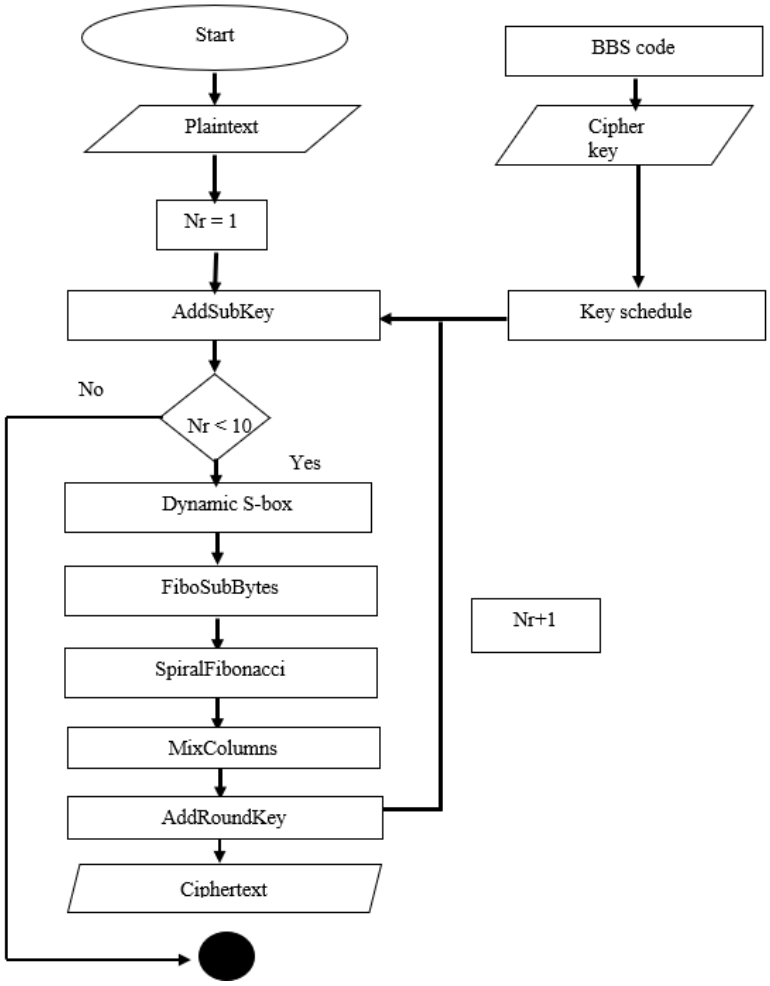

Figure 1. Proposed block cipher designed

At the start of the Cipher, the plaintext input was copied to the State array. Then, the algorithm took the cipher key, *K* from the BBS code (Blum-blum Shub). The BBS is a program used to generate a random cipher key. After that, it used a Key Expansion algorithm to create the Key Schedule. The Key Expansion was used to create a two-dimensional array of four-byte words. The Key Expansion process was similar to the AES block cipher module. The Key Expansion then generated a total of *Nb* (*Nr* + 1) words: the algorithm required an initial set of *Nb* words, and each of the *Nr* rounds required *Nb* words of key data. In the *AddSubKey()* transformation, a RoundKey was added to the State by a simple bitwise XOR operation. Then, the application of the *AddSubKey()* transformation to the *Nr* rounds of the Cipher occurred when $1 \leq round \leq Nr$. After an initial RoundKey addition, the State array was modified by applying a round function 9 times. Thus, an S-box was initialised using a key from the AddSubKey(). The proposed block cipher consisted of FiboSubBytes, SpiralFibonacci, MixColumns and AddRoundKey. *AddRoundKey()* was performed after *FiboSubBytes(), SpiralFibonacci() and MixColumns().* In the *AddRoundKey()*, a round key was added to the State by a simple bitwise XOR operation. Each processing round worked on an array of input State and produced an array of output State until the number of rounds became less than 10.

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

3. Research Methods

The experiment investigated the impact of the output if one bit of input is altered in plaintext or key. First, the data were prepared based on the 32-bit random key and plaintext. The data were generated through the BBS program as shown in Figure 2.

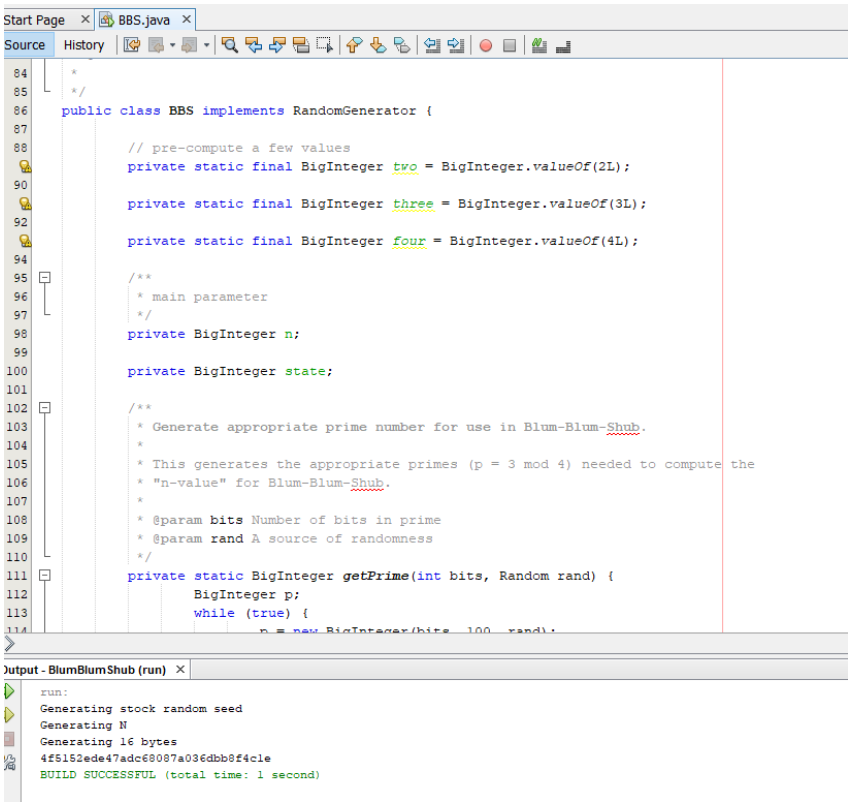

Figure 2. BBS code generator

In the random key data block, one bit in the 32-bit key was changed for the key avalanche effect. For the plaintext avalanche effect, one bit in the 32 bits plaintext was changed in the plaintext block. Then, an experimental process was performed to encrypt the key and the plaintext block to derive the initial ciphertext. This process was performed on the algorithm by 32 times and the effect of the avalanche was calculated each time based on the generated ciphertext. Based on Antonio et al. (2019) ciphertext was mapped in binary code to determine an avalanche effect as stated in Equation 3.1.

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in ciphertext}}{\text{Number of bits in ciphertext}} \quad (3.1)$$

Figure 3 shows the key and the plaintext (original text) of the proposed block cipher. Based on the experiment, the sensitivity of the algorithm is examined when one-bit input is changed in the key. For example, the key is “b3 e3 6d 9f c5 bc 20 f4 c0 f9 f3 35 13 d8 5e bb” , the plaintext is “The Secret Data2” and ciphertext is “df 14 f6 7C 3e bb f5 2f 8e f5 4e a7 46 e9 cf d4”.

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

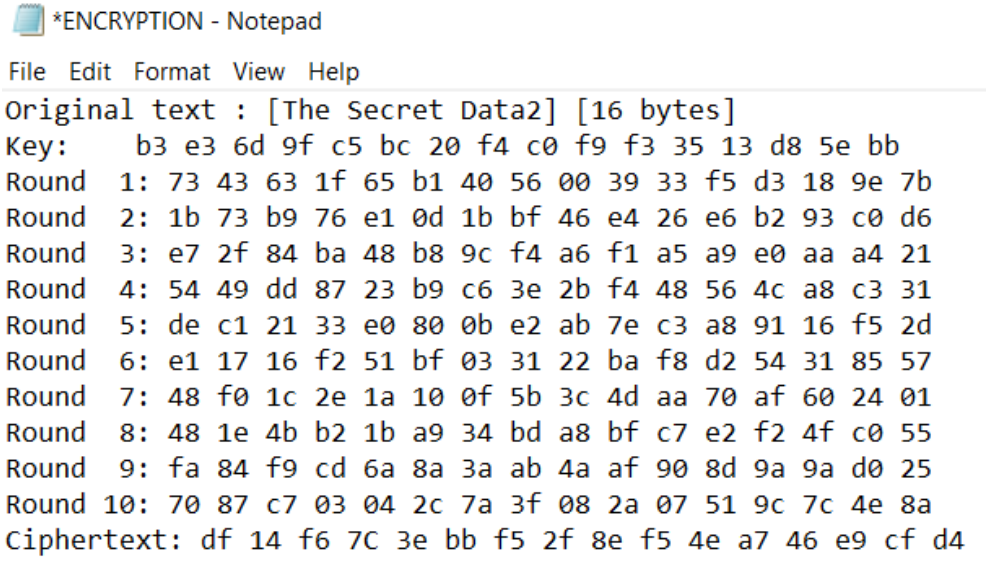

Figure 3. Proposed block cipher data

Before the proposed block cipher encrypts the encryption key and inputs plaintext, they are mapped into separate binary codes. Finally, the result was analysed based on a small change in the key with a significant change in the ciphertext. Therefore, if a block cipher does not exhibit the avalanche effect to a significant degree, it indicates that it has poor randomisation, thus allowing a cryptanalyst to make predictions about the input being given only the output..

4. Findings

The experiment was conducted to examine the sensitivity of the algorithm when a one-bit input is changed in the key or plaintext, which causes changes on approximately half of the ciphertext. If a block cipher does not exhibit the avalanche effect to a significant degree, then it has poor randomisation, which would allow a cryptanalyst to make predictions about the input, being given only the output. The experiment was performed based on the key avalanche avalanche as follows.

4.1. Key Avalanche Effect

In this experiment, for the key avalanche effect, one character in the 32-bit key was changed. This process was carried out in 32 times on the algorithm and the avalanche effect was determined based on the generated ciphertext. The result showed that half of the ciphertext was changed by a single bit change in the key. A value of the avalanche effect close to 0.5 is considered sufficient. From the result explained in Table 1, the key avalanche effect values of the proposed block cipher were provided. The small value of the avalanche effect was 52(0.4063) while the highest value was 73(0.5703). It was obvious that the average avalanche effect value of the algorithm was equal to 0.5.

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Table 1. Key Avalanche Effect

Point location changed	*Key*	*Cipher text of proposed block cipher*	*Avalanche effect*
	B3E36D9FC5BC20F4C0F9F33513D85EBB	DF14F67C3EBBF52F8EF54EA746E9CFD4	
1	**1**3E36D9FC5BC20F4C0F9F33513D85EBB	0865073D3DC8D20DB0E0BC4283A6E954	61(0.4766)
2	B**1**E36D9FC5BC20F4C0F9F33513D85EBB	FB741ED4A76FED9760435BE870A2CF37	57(0.4453)
3	B3**1**36D9FC5BC20F4C0F9F33513D85EBB	3E45DB5EB50EC1CCF855F29C1DC96EC5	58 (0.4531)
4	B3E**1**6D9FC5BC20F4C0F9F33513D85EBB	57C5D2CE8FF4AB775AAF69227EA29C40	59(0.4609)
5	B3E3**1**D9FC5BC20F4C0F9F33513D85EBB	900BD261B38B64904DE7EFEC41B592E1	61(0.4766)
6	B3E36**1**9FC5BC20F4C0F9F33513D85EBB	5A8CFB14C045515A0FA90BD402A01E11	61(0.4766)
7	B3E36D**1**FC5BC20F4C0F9F33513D85EBB	F15D2CB09B42366870AE8580C8DED8FD	71(0.5547)
8	B3E36D9**1**C5BC20F4C0F9F33513D85EBB	515432447D646A24B5A415D30747957F	63(0.4922)
9	B3E36D9F**1**5BC20F4C0F9F33513D85EBB	8E3D42C7454F7B4C20585B933A2C73FE	68(0.5313)
10	B3E36D9FC**1**BC20F4C0F9F33513D85EBB	4FFAA050542875F1836D030A6822B4DA	63(0.4922)
11	B3E36D9FC5**1**C20F4C0F9F33513D85EBB	7C2E79EA33D7B7315CC7B2697179D197	62(0.4844)
12	B3E36D9FC5B**1**20F4C0F9F33513D85EBB	043D94AC2FDD7281BB26A6BEE1F77B73	64(0.5000)
13	B3E36D9FC5BC**1**0F4C0F9F33513D85EBB	8DDEBD06F993BB0279BB237A78600CB8	69(0.5391)
14	B3E36D9FC5BC2**1**F4C0F9F33513D85EBB	184A65F4B85FD5533C6C8678DDE07417	64(0.5000)
15	B3E36D9FC5BC20**1**4C0F9F33513D85EBB	208FAE79D170948FBAAC8F97BE49D855	60(0.4688)
16	B3E36D9FC5BC20F**1**C0F9F33513D85EBB	E829295B9D82B2605B83302491F3F68A	75(0.5859)
17	B3E36D9FC5BC20F4**1**0F9F33513D85EBB	8C560CD6E13BE0E098E627A3059A4486	59(0.4609)
18	B3E36D9FC5BC20F4C**1**F9F33513D85EBB	E7731DD1EF62A6735399810F21D793C9	73(0.5703)
19	B3E36D9FC5BC20F4C0**1**9F33513D85EBB	EEB9641CC373575BA133F091E81C4472	68(0.5313)
20	B3E36D9FC5BC20F4C0F**1**F33513D85EBB	817009614C5913CCCCD8F95AA5AD3FF9	71(0.5547)
21	B3E36D9FC5BC20F4C0F9**1**33513D85EBB	E0F484B64474846524BECE2669FBBFCB	61(0.4766)
22	B3E36D9FC5BC20F4C0F9F**1**3513D85EBB	6A00A8DFFF9019624301A4553645A9F8	66(0.5156)
23	B3E36D9FC5BC20F4C0F9F3**1**513D85EBB	BBDC03DE5A78418980E60FB3D0777D90	55(0.4297)
24	B3E36D9FC5BC20F4C0F9F33**1**13D85EBB	AB05E8033C1D6B7C42A47DFB5FB63AB7	65(0.5781)
25	B3E36D9FC5BC20F4C0F9F335**0**3D85EBB	BFF0579A2A71E5948957B8DBB46EB3AD	63(0.4922)
26	B3E36D9FC5BC20F4C0F9F33511**1**D85EBB	935660A50764FD87B62419BC0D2567A6	60(0.4688)
27	B3E36D9FC5BC20F4C0F9F33513**1**85EBB	F194CA07D145325DEA4DA9D19D77C297	72(0.5625)
28	B3E36D9FC5BC20F4C0F9F33513D**1**5EBB	93B95B045F7E5E45DBAFC022A18FE7BF	66(0.5156)
29	B3E36D9FC5BC20F4C0F9F33513D8**1**EBB	09BA04A8F2D0A51FB20C6016E61646AC	67(0.5234)
30	B3E36D9FC5BC20F4C0F9F33513D851**B**B	70D7AF0DDB56F3211EFA7F1FDD45281F	67(0.5234)
31	B3E36D9FC5BC20F4C0F9F33513D85E**1**B	A3F33A6F7E26F24905E372CE22CCC82F	62(0.4844)
32	B3E36D9FC5BC20F4C0F9F33513D85EB**1**	85DE5361AB9284B64BEBCEB607A1C6C9	52(0.4063)

https://doi.org/10.15405/epms.2022.10.57
Corresponding Author: Kamsiah Mohamed
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Figure 4 shows the scatter plot in the proposed algorithm for the key avalanche effect. The value of the avalanche effect was nearly 0.5, which is considered sufficient. From these results, it appears that the proposed block cipher algorithm exhibited a good avalanche effect to have better randomness. The outcome of this analysis is that the proposed algorithm has satisfied the key avalanche effect with a 50% output bit changed in ciphertext. It shows a significant increase in the key avalanche effect on the algorithm. Therefore, this result indicated that the proposed block cipher algorithm satisfied the avalanche effect.

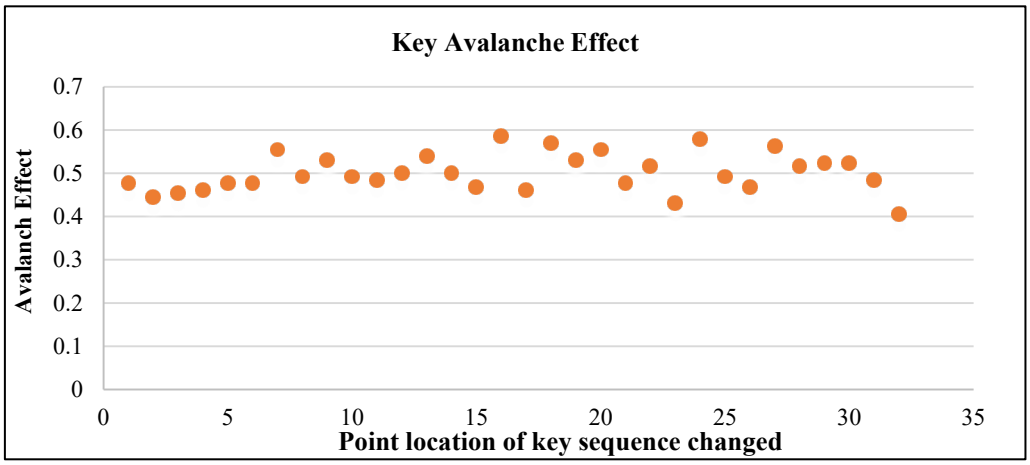

Figure 4. Result of Key Avalanche

In fact, the Data Encryption Standard (DES) has a good avalanche effect of 54.38% similar to the proposed block cipher algorithm, the results demonstrated that the avalanche effect satisfied with a 50% output bit change. It can be concluded that the proposed algorithm has fulfilled the avalanche effect property resulting in better diffusion.

5. Conclusion

In conclusion, an avalanche effect shows that when an input is slightly changed, the output dramatically changes the proposed block cipher algorithm. Through experiment, the results showed that the proposed block cipher algorithm satisfied the avalanche effect with a 50% output bit changed. It can be concluded that, the proposed block cipher algorithm fulfilled the avalanche effect property resulting in better diffusion. Thus, the results obtained proved that the output of the proposed block cipher algorithm is random irrespective of the input. It shows that the algorithm hides all useful information about the original data. Therefore, the proposed block cipher algorithm has the potential to raise security requirements.

References

Alabaichi, A., & Mechee, M. S. (2015). Evaluation of a Dynamic 3D S-Box Based on Cylindrical Coordinate System for Blowfish Algorithm. *Journal of Applied Sciences, 15*(5), *728-740*. https://doi.org/10.3923/jas.2015.728.740

Antonio, R. B., Sison, A. M., & Medina, R. P. (2019). A modified generation of S-box for advanced encryption standards. *In Proceedings of the 2019 2nd International Conference on Information Science and Systems* (pp. 280-283). https://doi.org/10.1145/3322645.3322672

Bhoge, J. P., & Chatur, P. N. (2014). Avalanche Effect of AES Algorithm. *International Journal of Computer Science and Information Technologies, 5*(3), 2014, 3101-3103. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.659.9331&rep=rep1&type=pdf

Echeverri, C. (2017). Visualization of the Avalanche Effect in CT2 [Doctoral dissertation, University of Mannheim]. https://www.cryptool.org/assets/ctp/documents/BA_Echeverri.pdf

Emami, S. S. (2013). Security analysis of cryptographic algorithms. A thesis for the degree of Doctor of Philosophy. *Department of Computing, Faculty of Science Macquarie University*.

Encarnacion, P. C., Gerardo, B. D., & Hernandez, A. A. (2020). Performance Analysis on Enhanced Round Function of SIMECK Block Cipher. In *2020 12th International Conference on Communication Software and Networks (ICCSN)* (pp. 270-275). IEEE. https://doi.org/10.1109/ICCSN49894.2020.9139059

Latif, M. A., Ahmad, M. B., & Khan, M. K. (2020). A Review on Key Management and Lightweight Cryptography for IoT. In *2020 Global Conference on Wireless and Optical Technologies (GCWOT)* (pp. 1-7). IEEE. https://doi.org/10.1109/GCWOT49901.2020.9391613

Mohamed, K., Pauzi, M. N. M., Ali, F. H. H. M., Ariffin, S., & Zulkipli, N. H. N. (2014). Study of S-box properties in block cipher. In *2014 International Conference on Computer, Communications, and Control Technology (I4CT)* (pp. 362-366). IEEE. https://doi.org/10.1109/I4CT.2014.6914206

Nazeh, A. W. M., Ali, A., Esparham, B., & Marwan, Md. (2018). A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. *Journal of Computer Science Applications and Information Technology, 3*(2), 1-7. http://doi.org/10.15226/2474-9257/3/2/00132

Raju, B. B., Krishna, A., & Mishra, G. (2017). Implementation of an efficient dynamic AES algorithm using ARM based SoC. In *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON) (pp. 39-43).* IEEE. https://doi.org/10.1109/UPCON.2017.8251019

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high Avalanche Effect. *IJCSNS International Journal of Computer Science and Network Security*, *11*(1), 106-111. http://paper.ijcsns.org/07_book/201101/20110116.pdf

Shi, H., Deng, Y., & Guan, Y. (2011). Analysis of the avalanche effect of the AES S box. In *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)* (pp. 5425-5428). IEEE. https://doi.org/10.1109/AIMSEC.2011.6009935

Simion, E. (2015). The relevance of statistical tests in cryptography. *IEEE Security & Privacy*, *13*(1), 66-70. https://doi.org/10.1109/MSP.2015.16

Singla, S., & Bala, A. (2018). A review: cryptography and steganography algorithm for cloud computing. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 953-957). IEEE. https://doi.org/10.1109/ICICCT.2018.8473109

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 International Conference On Engineering And Technology (ICET)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICEngTechnol.2017.8308215