HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Vol. 3, No. 1, (2019)

# A Study of Fibonacci Number in S-box Block Cipher

Kamsiah Mohamed[1*], Fakariah Hani Hj. Mohd Ali[2], Suriyani Ariffin[3], Mohd Nazran Mohammed Pauzi[4]

[1] Faculty of Communication, Visual Art and Computing, Universiti Selangor
kamsh@unisel.edu.my
[2,3] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA
fakariah@tmsk.uitm.edu.my, suriyani@tmsk.uitm.edu.my
[4] Faculty of Engineering and Life Sciences, Universiti Selangor
nazran@unisel.edu.my

**Abstract:** Substitution box (S-box) plays an important role in block cipher to protect data from any threats. The need for secure cipher is ever-increasing to protect data in several ways to provide confidentiality, integrity and authentication. The data is encrypted to prevent unauthorized users from accessing the information. However, as stated in the National Strategy ICT Roadmap, security is one of the pressing needs and critical infrastructure in Malaysia. In addition, within the advancement of technology the design of cryptographic algorithm in block cipher is often enhanced to ensure that the information is secure. Therefore, this paper proposed the new S-box using the concept of Fibonacci number in nature to improve the security of block cipher algorithm. Result showed that the new proposed S-box using the Fibonacci number possessed good cryptographic properties.

**Keywords**: decryption, encryption, Fibonacci, golden ratio, substitution box

## 1. Introduction

Within the development of technology, the design of cryptography algorithm always enhanced to ensure that information is secure. Today ciphers are needed and deployed almost everywhere, the need of secure ciphers can be so crucial. Thus, the design of new S-box is an important concern in the creation of new and more secure cryptosystems. The design and characteristics of S-boxes in a block cipher are central measures of resistance against all adequately high nonlinearity (Datta, Bhowmik and Sinha, 2016). In 2001, the NIST was chosen Rijndael algorithm by Rijmen and Daemen as the Advanced Encryption Standard (AES). Since then, AES becomes the most widely used block ciphers in cryptographic applications. However, the cryptanalysis of the cryptographic strength of Rijndael has not stopped after the announcement and official publication of the AES (Chang, Lai & Yang, 2009; Karuvandan, Chellamuthu & Periyasamy, 2016; Huang & Mishra, 2017). Easttom (2012) stated that awareness of cryptographic backdoor would cause an organization have expressed an interest in modifying their AES implementation. Hence to protect the encrypted content against any type of attack, AES block needs to be improved and studied. According to Hussain et al. (2013) the strength of encryption depends on the ability of S-box in distorting the data; hence, the process of discovering new and powerful block ciphers is of great interest in the field of cryptography. Weaknesses in the S-box can lead to a cryptosystem which is easily broken (Mohamed et al., 2018). Thus, a study by Ruisanchez (2015) proposed a new algorithm to construct S-boxes over $GF(2^8)$ with branch number. Nevertheless, this method does not have fixed points and the nonlinearity values are acceptable. Moreover, there are no algebraic procedures that can give the preferred and complete set of properties for an S-box block cipher (Picek & Golub, 2014). Previous studies have showed that Fibonacci number can make secure communication from cryptanalysis attacks. According to Raphael & Sundaram (2012) Fibonacci numbers and Unicode symbol can make secure communication in cryptography and steganography. This technique will fulfil the requirements for communication such as capacity, security and robustness to secure data transmission over an open channel. Then, other studies prove that the performance of

encryption and decryption algorithm using Fibonacci number is faster than among symmetric algorithms (Tarle & Prajapati, 2012). Hence, this research is undertaken to propose an S-box based on Fibonacci number in nature as well as indicate the concepts that can be used within the symmetric block cipher. These numbers occur everywhere in nature, ranging from the leaf arrangement in plants, the structure of DNA as well as various proportions in human face and structure of sea shells. Therefore, understanding the role of the Fibonacci number is a key to increase the performance of block cipher in cryptosystems. The paper comprises six main sections. Section 2, contains an overview on Fibonacci number in natures, Section 3, review on Fibonacci sequence in cryptography, Sections 4 proposed the new S-box based on Fibonacci number, Sections 5 analysis of S-boxes and Section 6 concluded the paper.

## 2. Fibonacci numbers in Nature

The numbers of Fibonacci can be seen everywhere in nature. For example, the Fibonacci numbers have been encountered in plant morphogenesis as the phenomenon of phyllotaxis**.** The petals are often arranged in spiral patterns with delamination. From inside to outside, the numbers of petals are 21, 13, 8, 5, and 3 based on their size. Therefore, the basic biology of phyllotaxis is well documented and attempts made to provide an underlying mechanism as shown in Figure 1.

***Figure 1 : ThePhyllotaxis of Rose***

Similarly, the pattern of seeds within a sunflower follows the Fibonacci numbers or 1,1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144.In sunflowers, the spirals can be seen in the center are generated from the sequence as shown in Figure 2.

***Figure 2 : Pattern of Sunflower Seeds***

Besides, Fibonacci numbers are often found in animal patterns. In 1202, Bonacci (Pomeraz, 1970) introduced the concept of Fibonacci sequence to describe the patterns of reproduction in populations of rabbits. A beautiful appearance of Fibonacci sequences is seen in the shape of shells of snails and sea shells. A cross-section of a nautilus shell shows the spiral curve of the shell and the internal chambers that the animal using it adds on as it grows. This spiral follows a precise mathematical pattern based on the Fibonacci sequences as shown in Figure 3.

***Figure 3: Nautilus Shell***

Furthermore, the unique of this mathematical sequence in nature, has led many researchers to investigate that it embodies some kind of human body. In 1973, Littler identified that by making a clenched fist, Fibonacci's spiral can be approximated in Figure 4.

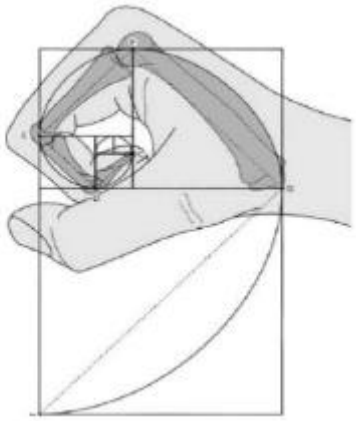


***Figure 4: Flexor and Extensor Movement of the Human Hand***

The flexor and extensor movement of the primary fingers approximate the golden spiral. A spiral would have to be created based upon the relationship between the metacarpophalangeal and interphalanges of the digits. Hamilton and Dunsmuir (2002) investigated that the phalangeal length ratio data obtained from their subjects compared to those that were almost arbitrarily as proposed by Littler. In fact, comparable and approximated the Fibonacci value of (φ) is 1.618. The results of the study indicate that the length measurement for the fourth digit (little finger) that follows the initial values of a Fibonacci sequence of 0, 1, 1, 2 represented by y, y, and 2y. Hence, the data from their study supported Littler's initial proposal of a clenched fist approximating the dimensions of the golden spiral. In 2011, Ashrafian and Athanasiou found that the structure of the coronary arterial tree follows a Fibonacci distribution. They stated that the Fibonacci number theory is useful in developing an innovative bio mathematical model of the coronary system as well as

new techniques in cardiac arterial. Then in 2013, Yetkin et al. reported a new finding where the golden ratio of Phi (φ) 1.618, exists within the cardiac cycle of the human heart beat. It is known that the time periods for the systolic and diastolic phases vary with the method of measurement. However, Persaud and O'Leary (2015) points out that the lack of statistical and well documented empirical data, accurate representations of the golden spiral could not be readily determined. Studied by Hutchison & Hutchison (2010) presented the functional lengths of the phalanges of the little finger actually do follow a Fibonacci sequence and that the functional lengths of the index, long, and ring fingers follow a mathematical relative of the Fibonacci numbers. The Fibonacci numbers also can be seen in the DNA. Robertson (2001) proves that the order of replication of DNA in cells also appears based on the Fibonacci sequence. Then Perez (2015) found that the organization of nucleic acid bases in the DNA sequence has an order (called the DNA SUPRA code) that follows Fibonacci numbers. Therefore, Fibonacci numbers are special and can be seen all over the world in every living thing.

## 3 Fibonacci number in Cryptography

The Fibonacci number is an emerging area in cryptography. It works with the code represented in the picture because each integer *n* can be represented by a sum of non-consecutive Fibonacci numbers to encrypt and decrypt the message. The adaptability of the previous equation comes from the flexibility of the value of *n*; by giving *n* be a different value for each set of encryptions, it makes the code more difficult to decipher (Yeates, 2013). In order to begin the encryption of a number, it is crucial to know the initial *n*-value. In sequence-based cryptography, all numbers that are to be encrypted must be successfully translated into another set of values. Elfard (2013) presented the theoretical and practical applications of Fibonacci sequence used in cryptography based on linear Fibonacci forms. Then, Khadri, Samanta and Paul (2014) proposed a new approach for the secure communication using Fibonacci numbers. For example, every ASCII value is added one by one with Fibonacci sequence such as JOB DONE of J→67, O→ 72, B→59, SPACE → 37, D → 61, N → 71, E → 62. In these studies, data encryption is carried out by combining the original data with Fibonacci numbers to obtain a ciphertext that is non-understandable to any intruder which give a higher-level security to the message being hacked. Then, Agarwal et al. (2015) used the Fibonacci sequence for encryption data based on the Raphael & Sundaram (2012) proposed method. These studies applied this method for text to image encryption and image shuffling using Fibonacci sequence. Nevertheless, there is no experimental test is performed to indicate the security of the system. Studied by Gonsalves, Bhat and Tangod (2017) used a similar method to perform an experiment between Fibonacci cryptography and RSA encryption and decryption. From the experiment, comparison has been made between Fibonacci cryptography and RSA. The result obtained from the experiment is compared in Table 1. The result shows that the performance for the Fibonacci cryptography is faster than the RSA algorithm.

***Table 1 Performance Comparison between RSA and Fibonacci Cryptography***

| File Size (kb) | RSA (Sec) | Fibonacci (Sec) |
|---|---|---|
| 10 | 56 | 0.656 |
| 14 | 62 | 2.271 |

| | | |
|---|---|---|
| 20 | 68 | 3.722 |
| 24 | 74 | 5.174 |
| 30 | 82 | 7.965 |

Then, Quazi, Maddikar & Tangod (2017) proposed an algorithm to improve the email security and minimizing the threat of intrusion using Fibonacci sequence encryption. The study stated that the proposed system is better, secure and efficient from all the traditional system, but no analysis is carried out to prove the statement. Ahmad et al. (2018) demonstrated that the Playfair algorithm for encryption and modified it by using Fibonacci sequence. The modified algorithm starts by generating the random key of a fixed length then generate the next six terms of the Fibonacci input. These studies have shown that the use of Fibonacci sequences and random keys provide significant security for shared communication. According to Mohamed et al. (2015) the simplicity and beauty of Fibonacci sequence have been motivated to develop matrix cryptosystems which are useful in digital communications. For example, a new approach for the secure transmission of information via the communication channel was obtained using Fibonacci Q-matrix with a key concept of variability in symmetric key algorithm (Prajapat, Jain & Thakur, 2012). Then, Paul & Mandal (2013) proposed a novel symmetric key cryptographic technique at bit level. It based on spiral matrix concept along clock-wise direction starting from (1,1). The technique is called as Spiral Matrix Based Bit Orientation Technique (SMBBOT). During the encryption process a session – based key is generated for one time in a transmission session to ensure security form SMBBOT. Mohamed et al. (2018) applied a concept of Fibonacci number and prime factor to improve AES S-box in cryptography. As a conclusion, Fibonacci number is very interesting technique could be applied to improve and enhance the security of any cipher.

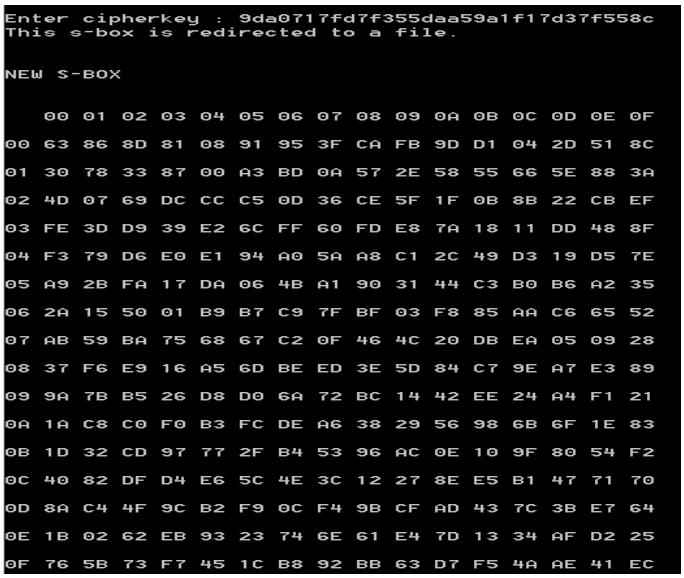
## 4 Proposed new S-box using Fibonacci Number

S-box mapping based on the substitution unit: $m$ x $n$, where $m$ and $n$ is not necessarily the same bit word which is $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$ . In other words, the input to an S-box could be $m$-bit word and the output can be $n$-bit word. It is a bijective S-box represented as a matrix of size $2^{8 \times 8}$. The proposed S-box is designed based on the following steps :

i) The multiplicative inverse in the finite field GF($2^8$) was taken and the element {00} was mapped to itself.
ii) The affine transformation was applied (over GF($2^8$)).
iii) Each byte in the S-box was assumed to comprise 8 bits labelled [$x_7$, $x_6$, $x_5$, $x_4$, $x_3$, $x_2$, $x_1$, $x_0$].
iv) XOR with the constant value {63} or {01100011} which is a byte of $C_i$.
v) Then XOR with the Fibonacci sequence.

Table 2 shows the proposed S-box design using the Fibonacci number. When a new cipher key is entered, the S-box and the inverse S-box is generated as shown in Table 3.

***Table 2 Proposed S-box***

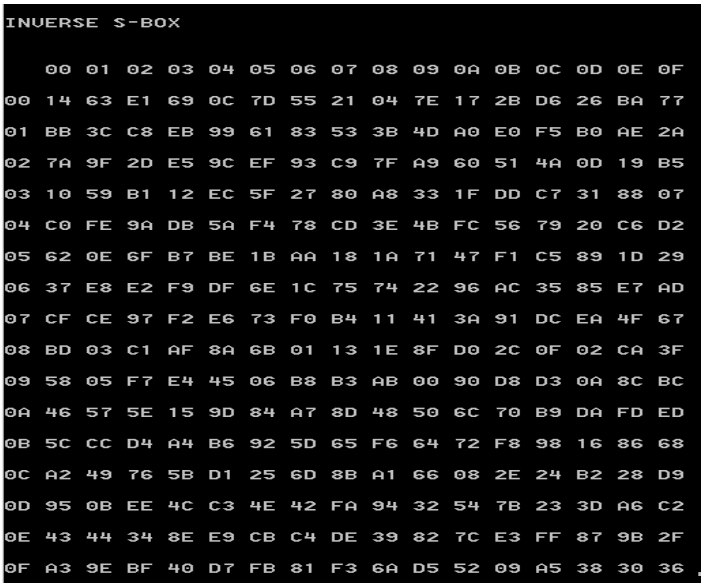


```
Enter cipherkey : 9da0717fd7f355daa59a1f17d37f558c
This s-box is redirected to a file.

NEW S-BOX

    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 63 86 8D 81 08 91 95 3F CA FB 9D D1 04 2D 51 8C
01 30 78 33 87 00 A3 BD 0A 57 2E 58 55 66 5E 88 3A
02 4D 07 69 DC CC C5 0D 36 CE 5F 1F 0B 8B 22 CB EF
03 FE 3D D9 39 E2 6C FF 60 FD E8 7A 18 11 DD 48 8F
04 F3 79 D6 E0 E1 94 A0 5A A8 C1 2C 49 D3 19 D5 7E
05 A9 2B FA 17 DA 06 4B A1 90 31 44 C3 B0 B6 A2 35
06 2A 15 50 01 B9 B7 C9 7F BF 03 F8 85 AA C6 65 52
07 AB 59 BA 75 68 67 C2 0F 46 4C 20 DB EA 05 09 28
08 37 F6 E9 16 A5 6D BE ED 3E 5D 84 C7 9E A7 E3 89
09 9A 7B B5 26 D8 D0 6A 72 BC 14 42 EE 24 A4 F1 21
0A 1A C8 C0 F0 B3 FC DE A6 38 29 56 98 6B 6F 1E 83
0B 1D 32 CD 97 77 2F B4 53 96 AC 0E 10 9F 80 54 F2
0C 40 82 DF D4 E6 5C 4E 3C 12 27 8E E5 B1 47 71 70
0D 8A C4 4F 9C B2 F9 0C F4 9B CF AD 43 7C 3B E7 64
0E 1B 02 62 EB 93 23 74 6E 61 E4 7D 13 34 AF D2 25
0F 76 5B 73 F7 45 1C B8 92 BB 63 D7 F5 4A AE 41 EC
```

***Table 3 Inverse S-box***



```
INVERSE S-BOX

    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 14 63 E1 69 0C 7D 55 21 04 7E 17 2B D6 26 BA 77
01 BB 3C C8 EB 99 61 83 53 3B 4D A0 E0 F5 B0 AE 2A
02 7A 9F 2D E5 9C EF 93 C9 7F A9 60 51 4A 0D 19 B5
03 10 59 B1 12 EC 5F 27 80 A8 33 1F DD C7 31 88 07
04 C0 FE 9A DB 5A F4 78 CD 3E 4B FC 56 79 20 C6 D2
05 62 0E 6F B7 BE 1B AA 18 1A 71 47 F1 C5 89 1D 29
06 37 E8 E2 F9 DF 6E 1C 75 74 22 96 AC 35 85 E7 AD
07 CF CE 97 F2 E6 73 F0 B4 11 41 3A 91 DC EA 4F 67
08 BD 03 C1 AF 8A 6B 01 13 1E 8F D0 2C 0F 02 CA 3F
09 58 05 F7 E4 45 06 B8 B3 AB 00 90 D8 D3 0A 8C BC
0A 46 57 5E 15 9D 84 A7 8D 48 50 6C 70 B9 DA FD ED
0B 5C CC D4 A4 B6 92 5D 65 F6 64 72 F8 98 16 86 68
0C A2 49 76 5B D1 25 6D 8B A1 66 08 2E 24 B2 28 D9
0D 95 0B EE 4C C3 4E 42 FA 94 32 54 7B 23 3D A6 C2
0E 43 44 34 8E E9 CB C4 DE 39 82 7C E3 FF 87 9B 2F
0F A3 9E BF 40 D7 FB 81 F3 6A D5 52 09 A5 38 30 36
```

## 5 Analysis of S-boxes

This paper discusses the analysis of the proposed S-box algorithm. The purpose is to ensure that the S-box is secure and efficient based on the confusion and diffusion properties. According to Hussien et al. (2013), once the S-box is designed, it is important to analyse the properties displayed by them. The experiments were conducted on Ubuntu 16.04LTS operating system to test the cryptographic properties of S-boxes which are based on SET tool box. Comparison is made between the standard AES S-box and the proposed S-box. Table 4 shows the result of proposed S-box while Table 5 shows the result of AES S-box. Based on the balance properties, the both S-boxes are balanced because its truth table has equal number 0s and 1s. For the nonlinearity properties the both S-boxes show that the value is 112. It means that the both S-boxes achieved the optimal value to resist linear cryptanalysis attack. For correlation immunity, the value for both S-boxes is zero. That means there is no correlation exists between input and output bits. For algebraic degree properties the result of

proposed S-box (value is 8) is better than AES S-box (value is 7). For algebraic immunity, both S-boxes show that the value is 4 means that both S-boxes is secure from algebraic attack. For robustness to differential cryptanalysis, the proposed S-box algorithm (0.981) was seen to have higher resistance to DPA attacks compared than the AES S-box (0.984). The SNR (DPA) valued of the proposed S-box algorithm (9.8) was higher than the AES S-box (9.6). Thus, the proposed S-box has better resistance to DPA attacks in terms of SNR (DPA). The SNR (DPA) valued of the proposed S-box (10.140) was higher than the AES S-box (9.6). Hence, the proposed S-box has better resistance to DPA attacks in terms of SNR (DPA). The last cryptographic property is confusion coefficient. From the results, the proposed S-box has a confusion coefficient variance of 0.093474 compared to the AES S-box, which is 0.1113. Hence, it was seen that the proposed S-box indicated a low confusion coefficient value to make it harder for the side-channel attacks to attack the S-box.

***Table 4 Analysis of Proposed S-box***

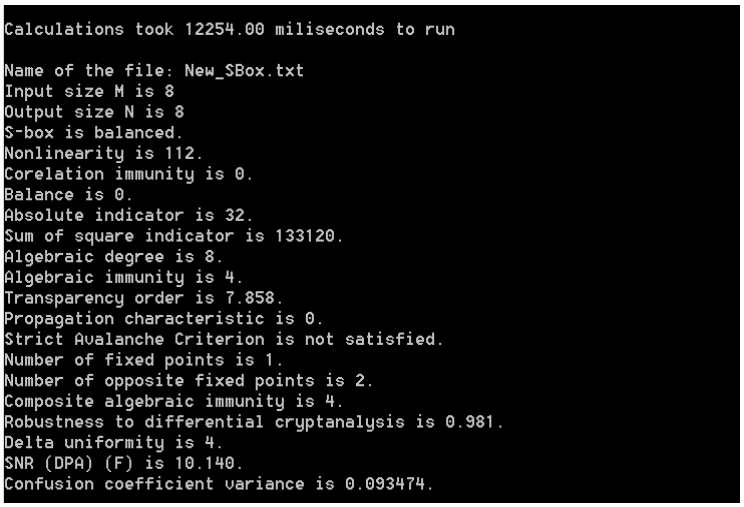



***Table 5 Analysis of AES S-box***

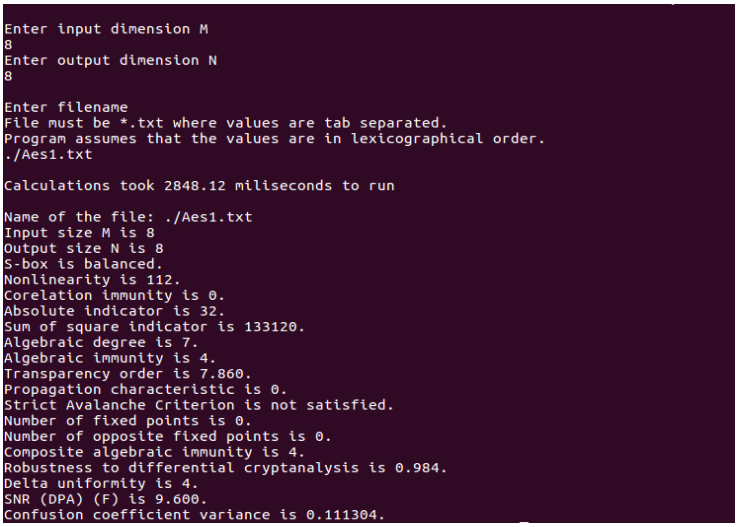



Table 6 shows the comparison between proposed S-box and AES S-box. As a conclusion, in the proposed S-box, the result of balance =0, nonlinearity =112, correlation immunity =0, and algebraic immunity =4 is similar to AES S-box. Besides, the proposed S-box has good

cryptographic properties for algebraic degree, transparency order, robustness to differential cryptanalysis, SNR(DPA) and confusion coefficient than the AES S-box. Therefore, it is important for every S-box to be evaluated based on cryptographic properties to resist linear attack, differential attack, algebraic attack and side channel attack.

***Table 6 Comparison between proposed S-box and AES S-box***

| **Cryptographic properties** | **AES S-box** | **Proposed S-box Algorithm** | **Good Cryptographic Properties** |
|---|---|---|---|
| Balance | 0 | 0 | No exploitable bias |
| Nonlinearity | 112 | 112 | High |
| Correlation immunity | 0 | 0 | Low |
| Algebraic degree | 7 | 8 | High |
| Algebraic immunity | 4 | 4 | Low |
| Transparency order | 7.860 | 7.858 | Low |
| Propagation Characteristic | 0 | 0 | Low |
| Fixed (Fp) and Opposite Fixed Points (OFp) | 0,0 | 1,0 | Low |
| Robustness to differential cryptanalysis | 0.984 | 0.981 | Low |
| Signal to noise ratio (SNR) Differential Power Analysis | 9.600 | 10.140 | High |
| Confusion coefficient | 0.111 | 0.0934 | Low |

## 6 Conclusion

The Fibonacci numbers are natural numbering system appropriate for the development of each living thing. Thus, the security of encryption and decryption will be improved with Fibonacci number so that it can withstand any attack of cryptanalysis. This paper clearly revealed that by using the Fibonacci number, the security in S-box block cipher can be improved. The experiments have shown that the new proposed S-box fulfilled the confusion and diffusion properties as described by Shannon (1949). The experimental results indicate that the proposed S-box has a high quality of cryptography properties. Therefore, the Fibonacci number have made the proposed S-box to have more resistant to linear cryptanalysis attacks, differential cryptanalysis and algebraic attack. As a result, this

approach had increased the security level of S-box to achieve high quality cryptography properties. It can be concluded that understanding the role of the Fibonacci number is a key to increase data security in cipher.

## 7 References

Ashrafian, H., & Athanasiou, T. (2011). Fibonacci series and coronary anatomy. Heart, Lung and Circulation, 20(7), 483-484.

Chang, C.C., Lai, Y.W. & Yang J.H. (2009) An efficient authenticated encryption scheme based on elliptic curve cryptosystem for broadcast environments." ICIC Express Letters. 4(1)( pp.95-100).

Datta, A., Bhowmik, D., & Sinha, S. (2017). A Novel Scheme for Analyzing Confusion Characteristics of Block Ciphers. In Proceedings of the First International Conference on Intelligent Computing and Communication, pp. 635-642. Springer, Singapore.

Easttom, C. (2016). Modern Cryptography: Applied Mathematics for Encryption and Information Security. McGraw-Hill Education.

Elfard, S. S. (2013) Cryptography Based on the Linear Fibonacci Forms. University Bulletin – Issue no.15 – Vol . 2.

Hamilton, R. & Dunsmuir, R.A.(2002) Radiographic assessment of the relative lengths of the bones of the fingers of the human hand. J Hand Surg Br.27: 546-548.

Huang, Y., & Mishra, P. (2017). Trace Buffer Attack On The AES Cipher. Journal of Hardware And Systems Security, 1(1), 68-84.

Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2013). A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Computing and Applications, 22(6), 1085-1093.

Hutchison, A. L., & Hutchison, R. L. (2010). Fibonacci, Littler, and the hand: a brief review. Hand, 5(4), 364-368.

Karuvandan, V., Chellamuthu, S., & Periyasamy, S. (2016). Cryptanalysis of AES-128 and AES-256 block ciphers using lorenz information measure. Int. Arab J. Inf. Technol., 13(6B), 1054-1060.

Littler, J.W. (1973) On The Adaptability of Man's Hand (With Reference To The Equiangular Curve). Hand. 5: 187-191

Mohamed, K., Ali, F. H. H. M., Ariffin, S., Zakaria, N.H. & Pauzi, M. N. M (2018). An Improved AES S-box Based on Fibonacci Numbers and Prime Factor. In International Journal of Network Security, 20(6): pp. 1206-1214.

Mohamed, K., Hj. Mohd Ali, F. H., Ariffin, S., & Mohammed Pauzi, M. N. (2018). A Review of Cryptography Based on Key Dependent S-Box in Block Cipher. *Selangor Science & Technology Review (SeSTeR)*, *2*(2), 1-8. Retrieved from http://sester.journals.unisel.edu.my/ojs/index.php/sester/article/view/32

Mohamed, M. H., Mahdy, Y. B., & Shaban, W. A. E. W. (2015). Confidential Algorithm for Golden Cryptography Using Haar Wavelet. arXiv preprint arXiv:1501.03617.

Paul, M., & Mandal, J. K. (2013). A Novel Symmetric Key Cryptographic Technique At Bit Level Based On Spiral Matrix Concept. arXiv preprint arXiv:1305.0807.

Perez, J. C. (2015). Deciphering Hidden DNA Meta-Codes-The Great Unification & Master Code of Biology. Journal of Glycomics & Lipidomics, 5(2), 1.

Persaud, D., & O'Leary, J. P. (2015). Fibonacci Series, Golden Proportions, and the Human Biology.

Picek, S., & Golub, M. (2014). On Using Genetic Algorithms for Intrinsic Side-Channel Resistance: The Case of AES S-Box Categories and Subject Descriptors. CS2, January 20 2014, Vienna, Austria Copyright 2014 ACM

Pomeraz, V. (1970). Leonardo of Pisa. James Joyce Quarterly, 7(2), 148-150.

Prajapat, S., Jain, A., & Thakur, R. S. (2012). A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix. IJCCT, 3(3), pp.54-57.

Raphael, A. J., & Sundaram, V. (2012). Secured communication through fibonacci numbers and unicode symbols. *International Journal of Scientific & Engineering Research*, *3*(4), 2229-5518.

Robertson, D. S. (2001). Cellular configuration of DNA and cell division. Medical hypotheses, 57(3), 344-353.

Ruisanchez, P.C. (2015). A New Algorithm To Construct S-Boxes With High Diffusion. International Journal Of Soft Computing, Mathematics and Control (IJSCMC),Vol. 4, No. 3.

Shannon, C.E. (1949). Communication Theory of Secrecy Systems, Bell Sysit. Tech 5.28, pp.656-715

Tarle, B. S., & Prajapati, G. L. (2011). On the information security using Fibonacci series. In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (pp. 791-797). ACM.

Yetkin, G., Sivri, N., Yalta, K., & Yetkin, E. (2013). Golden Ratio Is Beating in Our Heart. International journal of cardiology, 168(5), 4926-4927.