A Survey on Various Dynamic S-box Implementation in Block Cipher Encryption Algorithm

Julia Juremi, Salasiah Sulaiman, Nurul Husna Mohd Saad, Jazrin Ramli
Faculty of Computing, Engineering & Technology
Asia Pacific University of Technology & Innovation
57000 Kuala Lumpur, Malaysia
julia.juremi@staffemail.apu.edu.my, salasiah@staffemail.apu.edu.my, nurul.husna@staffemail.apu.edu.my, jazrin86@gmail.com

***Abstract*—There are two types of s-boxes in block cipher algorithm; static s-box and dynamic s-box. Static s-box is defined as one particular same s-box will be used in each round of the block cipher whereas dynamic s-box is defined as different s-boxes will be used in each round depending on the way it been generated. This paper emphases mainly in various techniques of dynamic block cipher encryption algorithm that exists, and framing all the techniques together as a literature survey.**

***Index Terms*—AES, block cipher, confusion, dynamic s-box, encryption, randomness**

1. Introduction

Substitution box or s-box plays significant role in the block cipher algorithm. According to previous studies, there are few findings found to support the important role of the substitution box no matter in which design it was implemented. Mister & Carlisle (1996) wrote that much of the security of the block cipher based on the Feistel network depends on the properties of the substitution boxes (s-box) used in the round function and since the s-box also comprises the only nonlinear component of SPN, they are a crucial source of cryptographic strength. S-box is also said to be responsible for confusion in the encipherment process. The s-box substitution is the critical step in any block cipher system (EL-Ramly, El-Garf & Soliman, 2001).

Basically, there are two types of s-boxes; static s-box and dynamic s-box. Static s-box is defined as the particular same s-box will be used in each round of the block cipher whereas dynamic s-box is defined as different s-boxes will be used in each round depending on the way it been generated. According to Schneier et al. (1998), fixed s-box allows attackers to study the s-box component and find weak points. With dynamic s-box, attacker does not know which s-box is being used and hence there are many advantages such as defense against unknown attack and the complexity of the s-box constructed can increase the strength of the cipher. One way to generate dynamic s-box is by using key-dependent s-box method. The alteration and generation of the s-box for each round depends on the key and number of rounds. Ciphers with key-dependent s-box are in general more secure than fixed s-box. The dynamic structure of the s-box helps to increases the strength of the cipher (Elkamchouchi & Makar, 2004).

2. Symmetric Block Cipher Encryption

In symmetric key encryption, an identical key is use for both encryption and decryption process. This type of encryption is also known as secret key or one-key algorithm. Both sender and receiver should have a copy of the same key and the key is known as secret key. In a symmetric block cipher algorithm, the substitution box or s-box plays significant role. Figure 1 shows the encryption process of a block cipher symmetric key algorithm. According to previous studies, there are few findings found to support the important role of the substitution box no matter in which design it was implemented. S-box is also said to be responsible for confusion in the encipherment process.

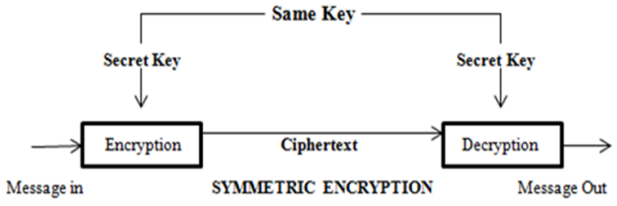

Figure 1: Symmetric Block Cipher Encryption

3. Dynamic Block Cipher

Although the static s-box in AES is still secured, various studies have attempted to modify the AES s-box to make it dynamic instead of static in order to increase the security of the algorithm. The shaded boxes shown in Figure 2 indicate the scope and the focus of the background survey in this paper. This section reviews some related studies of dynamic s-box in symmetric encryption technique back to before AES was implemented and up to recent establishment.

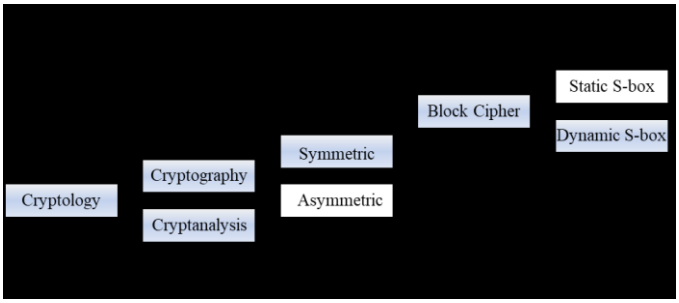

Figure 2: Dynamic S-box in Block Cipher Encryption

One of the earliest block cipher encryption to implement different s-box is Khufu. It is a 64-bit block cipher design by Merkle (1991). It was developed based on Feistel structure with 16 rounds by default (other multiple of eight between 8 and 64 are allowed) and uses key size of 512 bits. At the start and end of the algorithm, extra key material is XORed with the block.

Each set of eight rounds is termed as an octet and a different s-box is used in each octet. In a round, the least significant byte of half of the block is passed into the 8×32-bit s-box and the s-box output will then combined using the XOR operation with the other 32-bit half. The left half is then rotated to bring a new byte into position, and the halves are swapped. Most of the key material is used to construct the cipher's s-boxes. Khufu was used for bulk encryption of large amounts of data.

Blowfish algorithm designed by Schneier (1993) has a 64-bit block size and a key length between 32 bits to 448 bits. It was designed as a fast, free alternative to existing algorithm. It is a 16 round Feistel cipher and has four dynamic s-boxes. Each round consists of a key-dependent permutation, and a key-and data-dependent substitution. All operations are XORs and additions on 32-bit words. Later in the year of 1998, Schneier et al. (1998) came out with Twofish block cipher. It is a Feistel network with 16 rounds and slightly modified using 1-bit rotations. The round function acts on 128-bit block cipher with four key-dependent 8x8 s-boxes. Twofish's distinctive features are the use of pre-computed key-dependent s-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent s-boxes).

In more recent years, more and more block cipher is designed to be dynamic. DSDP is a block cipher with a block length of 128 bits proposed by Zhang & Chen (2008). The DSDP cipher engages the Feistel structure with efficient byte wise operation for fast speed implementation. A key-dependent s-box and eight key-dependent p-boxes is introduced into the algorithm, so the internal structure of this algorithm is hided so as to resist the existing shortcut attacks, such as linear and differential cryptanalysis.

Wang et al. (2009) introduces block cipher with dynamic s-boxes based on tent maps. They analysed the difference trait of the tent map and presents method for generating s-boxes based on iterating the tent map. Different s-boxes were used to encrypt the plaintext block. There are 32 rounds of substitution and left cyclic shift is implemented in order to obtain the cipher blocks. They improve the security of the cryptosystem by using a cipher feedback and by altering the state value of the tent map, which leads to the confusion and diffusion properties of the cryptosystem.

In the year of 2010, Zaibi et al. (2010) proposed the construction of dynamic s-box by using chaotic maps. The dynamic chaotic s-box enhances the security of the block ciphers based on the combination of two chaotic maps: one and three dimensional piecewise linear maps. The NIST test package is used to verify the randomness of those maps. The results from the security analysis displays that the dynamic s-boxes based on two chaotic maps have the lowest linear approximation probability and also an equiprobable input/output distribution.

Szaban & Seredynski (2011) came out with new and more sophisticated classes of s-boxes, in particular dynamic ones. They proposed a method in designing a dynamic cellular automata (CA)-based s-boxes. The results show that the proposed s-boxes have high quality cryptographic properties (high non-linearity and balance, also low autocorrelation and distance to fulfil the strict avalanche criterion). The proposed s-boxes also provide a dynamic flexible structure, fully functionally method based on cellular automata.

Hosseinkhani & Javadi (2012) then introduced a new algorithm that dynamically generates s-box from cipher key in only two steps. The first step is to generate a primary s-box using the same procedure used in the previous algorithm (AES). The second step is to swap the values in the rows with the values in the columns of primary s-box. This routine uses cipher key as input and then dynamically generates s-box from the cipher key by using shift columns, shift row and shift account.

In the year of 2013, Mahmoud et al. (2013) proposed a dynamic s-box based on byte permutation of the standard s-box. Linear Feedback Shift Register (LFSR) was used to generate random sequences. The AES key is used to generate an initial state of LFSR by dividing it into two parts and placing an XOR between these parts. The results can be used as the initial value of LFSR. The output from the generator is XORed with the key. The repeated values are discarded, and then the missing numbers are added to the 62 sequence to ensure that all s-box indexes are mapped. These numbers are used to rearrange columns and rows on the standard s-box.

Alabaichi, Mahmod & Ahmad (2014) then came out with an enhanced version of Blowfish Algorithm based on cylindrical coordinate system in the year of 2014. This algorithm implements a new function (F-Function) into a Cylindrical Coordinate System (CCS). The F-Function is known as Cylindrical Coordinate System with Dynamic Permutation Box (CCSDPB) and the enhanced algorithm is known as the RAF. In the RAF design, a dynamic 3D s-box, a dynamic p-Box, and an F-Function were designed and implemented. The NIST statistical test shown the output tested through this algorithm is random and proven to be secured.

Zhang, Zhao & Wang (2014) presented an image encryption based on dynamic s-boxes, in which the s-boxes are constructed by chaotic systems. An external 256-bit key and the last pixel of plain image are used to generate the parameters and initial states of the chaotic systems for the first s-box. The plain image is divided into groups in which the pixels are substituted by S-boxes and in order to smash the correlation of adjacent pixels the image is grouped in four directions. After encrypting previous group, the initial states of chaotic systems are altered by encrypted image pixels and the s-box for the next group is generated. This algorithm scheme make it resistance towards differential attacks and chosen plain-text attacks. Moreover, since in total they only need to construct less than 50 s-boxes, the progress time is reduced. Superiority in speed and security

is analyzed by applying the algorithm on 256-grey images and the results show a good randomness effect.

Al-Wattar et al. (2015) and Liu et al. (2016) proposed dynamic encryption method based on DNA approach. The new approach proposed by Al-Wattar et al. (2015), is a DNA based block cipher algorithm was proposed where the substitution and permutation functions use some of the DNA processes and techniques to improve the design of the block cipher by creating a new key-dependent s-boxes, key-dependent shift rows and key-dependent mix columns for the round transformations. A year after that, Liu et al. (2016) introduced a combination of dynamic s-boxes and chaotic system to develop a new image encryption scheme. The diffusion layer is based on DNA operations unlike the traditional diffusion methods. The diffusion of the pixel values of the image is by using the dynamic s-boxes composed of DNA sequences and were constructed using logistic map. Both research works were inspired by DNA properties and were used in constructing a block cipher algorithm. The results of the security test showed the proposed functions are able to provide both confusion and diffusion to the whole cipher.

In the year of 2017, Belazi et al. (2017) proposed two efficient cryptosystem schemes in the form of permutation–substitution based on chaotic systems. Dynamic s-boxes are generated using the keys in chaotic map. A colour encryption scheme based on chaotic maps and s-boxes in the form of permutation–substitution network is also presented. The analysis shows the efficiency of the proposed schemes and provides good implementation in cryptographic applications.

Another dynamic block cipher based on chaotic map were proposed by Ahmad & Chopra (2017) where it encrypts images based on the chaos, substitution boxes, nonlinear transformation in galois field and latin square. Initially, the dynamic s-boxes are generated using Fisher Yates shuffle method and piece wise linear chaotic map. The algorithm utilizes advantages of keyed Latin square and transformation to substitute highly correlated digital images and yield encrypted image with valued performance. The chaotic behavior is achieved using logistic map which is used to select one of thousand s-boxes and also decides the row and column of selected s-box. The selected s-box value is transformed using nonlinear transformation. Along with the keyed Latin square generated using a 256 bit external key, used to substitute secretly plain image pixels in cipher block chaining mode. To further strengthen the security of algorithm, round operation are applied to obtain final ciphered image. The security analyses prove the proposed algorithms effectiveness in providing high security to digital media

4. Security Analysis

Security is important in evaluation and comprises features such as soundness of its mathematical basis, randomness of the output, resistance of the algorithm towards cryptanalysis and relative security. The most basic properties expected from cryptographic primitives such as block ciphers are indistinguishability from random mapping (Al-Wattar et al. 2015) (Doganaksoy et al., 2010) (Sulak et al., 2010) (Juremi et al., 2017). Therefore, the outputs of the algorithm must at least be tested through the statistical randomness tests.

The randomness of the outputs can be evaluated using the pseudorandom number generator (PRNG) statistical test suite which consists of several subtests. During AES competition, statistical testing of the candidates was done by Soto (1999). Randomness test has been conducted in various research work including Soto & Bassham (2000), Fahmy et al. (2005), Katos (2005), Limin, Dengguo & Yongbin (2008), Chen, Feng & Fan (2009), Zhou et al. (2009), Sulak et al. (2010), Ariffin et al. (2012), Alabaichi, Mahmod & Ahmad (2014) and Zakaria (2017).

5. Conclusions

This paper presented the literature review and background study on various dynamic s-box implementation in block cipher encryption algorithm. Basic explanation on symmetric encryption algorithm narrowed down to the construction of dynamic s-box in substitution function of block cipher algorithm is discussed. Background study on various works on AES based block ciphers and other block cipher models are reviewed and discussed. Those encryption techniques are studied and analyzed in terms of the randomness of the output produced. As the conclusion, the implementation of dynamic s-box in various field and approach are proven to produce random output and each approach is unique in its own way, which might be suitable for different software or hardware applications.

References

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. (2015) A new DNA based approach of generating key-dependent mix column transformation. International Journal of Computer Networks & Communications. 7(2). p. 93-102.

Ahmad, M., & Chopra, A. (2017) Chaotic dynamic s boxes based substitution approach for digital images. arXiv preprint: arXiv:1709.07620. [Online] Available from: https://arvix.org/abs/1709.07620. [Accessed: 25 June 2018].

Alabaichi, A., Mahmod, R., & Ahmad, F. (2014) Randomness analysis of 128 bits Blowfish block cipher on ECB mode. International Journal of Computer Science and Information Security (IJCSIS). 11(10). p. 8-21.

Ariffin, S., Mahmod, R., Jaafar, A., Rezal, M. & Ariffin, K. (2012) *An immune system-inspired byte permutation function to improve confusion performance of round transformation in symmetric encryption scheme.* In Computer Science and its Applications (CSA 2012). Jeju, Korea: Springer, Dordrecht. p. 339-351.

Belazi, A., El-Latif, A. A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Journal of Optics and Lasers in Engineering. 88. p. 37-50.

Chen, H., Feng, D., & Fan, L. (2009) New statistical test on block ciphers. Jisuanji Xuebao/Chinese Journal of Computers. 32(4). p. 595-601.

Doganaksoy, A., Ege, B., Koçak, O., & Sulak, F. (2010) Cryptographic randomness testing of block ciphers and hash functions. IACR Cryptology ePrint Archive. 564. p. 1-12.

El-Ramly, S.H., El-Garf, T. & Soliman, A.H., (2001) *Dynamic generation of s-boxes in block cipher systems.* In Proceedings of the

Eighteenth National Radio Science Conference (NRSC'2001). Mansoura, Egypt, Egypt. p. 389-397.

Elkamchouchi, H. M. & Makar, M. A. (2004) *Kamkar symmetric block cipher*. In Proceedings of the Twenty-First National Radio Science Conference (NRSC'2004). Cairo, Egypt, Egypt. p. C1-1.

Fahmy, A., Shaarawy, M., El-Hadad, K., Salama, G., & Hassanain, K. (2005) *A proposal for a key-dependent AES*. In 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications. Tunisia: SETIT. p. 1-7.

Hosseinkhani, R., & Javadi, H. H. S. (2012) *Using cipher key to generate dynamic s-box in AES cipher system*. International Journal of Computer Science and Security (IJCSS). 6(1). p. 19-28.

Juremi, J., Mahmod, R., Zukarnain, Z. A., & Md. Yasin, S. (2017) Modified AES S-Box Based on Determinant Matrix Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper. 7(1). p. 110-116.

Katos, V. (2005) A randomness test for block ciphers. Applied mathematics and computation. 162(1). P. 29-35.

Limin, F., Dengguo, F., & Yongbin, Z. (2008) A fuzzy-based randomness evaluation model for block cipher. Journal of Computer Research and Development. 45(12). p. 2095-2101.

Liu, Y., Wang, J., Fan, J., & Gong, L. (2016) Image encryption algorithm based on chaotic system and dynamic s-boxes composed of DNA sequences. An International Journal of Multimedia Tools and Applications. 75(8). p. 4363-4382.

Mahmoud, E. M., Abdelhalim, Z., El Hafez, A. A., & Elgarf, A. T. (2013) Enhancing channel coding using AES block cipher. International Journal of Computer Applications. 61(6). P. 28-33.

Merkle, R.C. (1991) *Fast software encryption functions*. In Proceeding of the Advances in Cryptology-CRYPTO '90. Santa Barbara, California: Springer-Verlag. p. 476–501.

Mister, S. & Carlisle, A., (1996) *Practical s-box design*. In Workshop Record of the Workshop on Selected Areas in Cryptography (SAC' 96). Queen's University, Kingston, Ontario. p. 61–76. [Online] Available from: CiteSeerX Portal. [Accessed: 03rd July 2018].

Schneier, B. (1993) *Description of a new variable-length key, 64-bit block cipher (Blowfish)*. In International Conference on Fast Software Encryption. Cambridge, U.K: Springer. p. 191-204.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. & Ferguson, N. (1998) Twofish: A 128-bit block cipher. AES submission - NIST AES Proposal. [Online] Available from: http://www.nist.gov/aes. [Accessed: 25 June 2018].

Soto, J. (1999) Randomness testing of the AES candidate algorithms. NISTIR 6390. [Online] Available from: https://csrc.nist.gov/publications/detail/nistir/6390/final. [Accessed: 25 June 2018].

Soto, J., & Bassham, L. (2000) Randomness testing of the advanced encryption standard finalist candidates. NISTIR 6483. [Online] Available from: https://csrc.nist.gov/publications/detail/nistir/6483/final. [Accessed: 25 June 2018].

Sulak, F., Doganaksoy, A., Ege, B., & Koak, O. (2010) *Evaluation of randomness test results for short sequences*. In International Conference on Sequences and Their Applications (SETA 2010). Paris, France: Springer. p. 309-319.

Szaban, M., & Seredynski, F. (2011) *Dynamic cellular automata-based S-boxes*. In International Conference on Computer Aided Systems Theory-EUROCAST 2011. Las Palmas de Gran Canaria, Spain: Springer. p. 184-191.

Wang, Y., Wong, K.-W., Liao, X., & Xiang, T. (2009) A block cipher with dynamic s-boxes based on tent map. Communications in Nonlinear Science and Numerical Simulation. 14(7). p. 3089-3099.

Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., & Samet, M. (2010) *A new design of dynamic s-box based on two chaotic maps*. In IEEE/ACS International Conference of Computer Systems and Applications (AICCSA 2010). Hammamet, Tunisia: IEEE. p. 1-6.

Zakaria, N. H. (2017) A block cipher based on genetic algorithm. PhD Thesis. Universiti Putra Malaysia. Serdang, Malaysia.

Zhang, R., & Chen, L. (2008) *A block cipher using key-dependent s-box and p-boxes*. In Industrial Electronics (ISIE 2008). Cambridge, UK: IEEE International Symposium. p. 1463-1468.

Zhang, X., Zhao, Z., & Wang, J. (2014) Chaotic image encryption based on circular substitution box and key stream buffer. Journal of Signal Processing: Image Communication. 29(8). p. 902-913.

Zhou, Q., Liao, X., Wong, K., Hu, Y., and Xiao, D. (2009). True random number generator based on mouse movement and chaotic hash function. Information Sciences. 179(19). p. 3442-3450.