HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Vol. 2, No. 2, (2018)

A Review of Cryptography Based on Key Dependent S-Box in 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 plays an important role in the block cipher algorithm. It can be used to encrypt and decrypt a key in a block cipher. Weaknesses in the substitution box (S-box) can lead to a cryptosystem which is easily broken. A key dependent S-box is needed to make cryptanalysis attacks are difficult to discover a key in a block cipher. In this paper, a key dependent S-box approach is reviewed to improve the security of a cryptosystem. The study found that, a key dependent S-box in a block cipher is more secure and efficient compare than the static S-box. With key-dependent S-box, attacker does not know what the S-box are used and make the system immune to linear and differential cryptanalysis. As a result, a new approach of key dependent S-box is enhanced to produce secure block cipher.

Keywords: confusion, diffusion, secure block cipher, dynamic, communication, security

1. Introduction

Since the development of network communications and technology is growing rapidly, cryptographic has become the most widely used technique to protect the secrecy of data. Cryptography plays an important role in secure communication systems. It becomes extremely useful in many applications such as wireless technology, online billing, e-business, secure log in, emails, etc. It is becoming necessary when sensitive data is being implemented over any insecure channel. Cryptography can be categorized as symmetric and asymmetric ciphers. A symmetric cipher also called "secret-key" and “private key” encryption, used the same key for encryption and decryption. Asymmetric key also called “public-key” encryption, used different key for encryption and decryption. It based on mathematics that are substantially slower than symmetric key cryptography algorithms. The symmetric key algorithm is faster in execution because of straightforward cryptographic transformations and can be pipelined to give better performance (Gutub & Khan, 2012). It consists of a basic building block of cryptographic primitives which are stream ciphers, block ciphers and hash functions. Thus, symmetric key algorithms are most commonly used for encryption and decryption. Generally, the S-box is a very important component of many block ciphers. Therefore, secure block cipher depends on the capability of S-boxes to protect the data from cryptanalysis attack. The processes of ascertain new and powerful S-boxes are of great concern in the field of cryptography. This paper is intended for reviewed a symmetric block cipher based on key dependent S-box.

The paper comprises three main sections. Section 2, contains an overview on S-Box in block ciphers. Section 3 explores and contrast between the standard AES S-Box and the dynamic S-Box with key dependent block cipher and Sections 4 summarizes and conclude the paper.

2. Overview on S-box in Block Ciphers

Block cipher can be defined as $E:\{0,1\}^{n_b} x\{0,1\}^{n_k} \rightarrow \{0,1\}^{n_b}$ as $C = E(P,k)$ where C is ciphertext computed from n_b-bit plaintext P and n_k-bit key k. An n_b- bit denote the block size and n_k -bit denote the key size. Block cipher consists of encryption and decryption process.

Encryption can be defined as:

$$E_k(p) = c \tag{1}$$

and decryption can be defined as:

$$E_k^{-1}(c) = P \tag{2}$$

Block cipher consists of S-box which is a nonlinear transformation which performs confusion of bits. An $n \times m$ S-box is a mapping from n input bits to m output bits, $S: \{0, 1\}^n \rightarrow \{0, 1\}^m$. Fundamentally, an S-box is a set of m single output Boolean functions combined in a fixed order. There are 2^n inputs and 2^m possible outputs for a $n \times m$ S-box. Generally, a $n \times m$ S-box, S, is represented as a matrix of size $2^{n \times m}$ for each m-bit entry. An $n \times m$ S-box is a bijective S-box where each input is mapped to a dissimilar output entry and all possible outputs are presented in the S-box It provides the cryptosystem with the confusion property described by Shannon (1949). In modern encryption algorithm a nonlinear transformation is essential and is proved to be a strong cryptographic primitive against linear and differential cryptanalysis (Hosseinkhani & Javadi, 2012). An example of a nonlinear transformation algorithm is Advanced Encryption Standard (AES). This standard specifies the Rijndael algorithm. It is widely used in cryptographic applications approved by the National Institute of Standards and Technology (NIST) in 2001. It was designed to handle additional block sizes and key lengths 128, 192 and 256 bits. In the Rijndael algorithm, S-box is the most important part because of the encryption algorithm. It requires the key to be the same length as the message to be encoded. Hence, it causes the most delay of the encryption algorithm. The AES block cipher consists of four stages which are sub bytes, shiftrows, mix columns and addround key as shown in Figure 1.

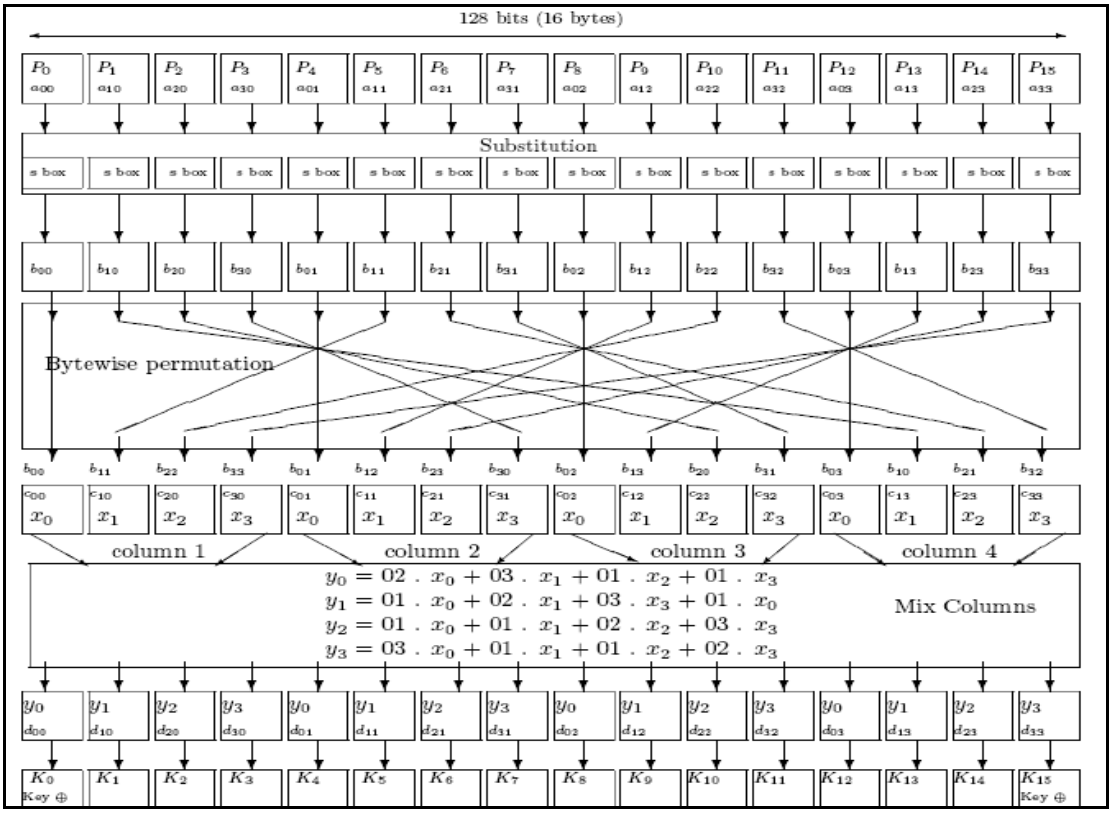

Figure 1. The Architecture of Rijndael S-box

Although the AES S-box is a standard block cipher nevertheless the component used in AES is fixed and not changeable. The key dependent algorithm should be generated to increase the cryptographic strength of the AES cipher system. Schneier (1996) found that S-box depend on key values are slower but more secure than independent ones. In addition, static or fixed S-box used the same S-box in each round. However, for key-dependent the S-box is changed depends on the key and the number of rounds. On the other hand, static S-box allows attacker to study S-box and easy to find a weak key compare than key dependent S-box approach where it makes an attacker difficulty to discover the key. Therefore, many researches were enhanced or renew the implementation of the S-box. Niemie & Machowski (2012) proposed the new symmetric cipher based on key-dependent S-boxes. The S-boxes with the Substitution Permutation Network served as a basic idea of key-dependent symmetric cipher. However, those keys are weak because they give the same substitution as S-boxes generated from shorter keys. If longer key lengths are used, more rounds are having so the whole encryption differs. A weak key is considered when there is at least one equivalent in shorter keys. Hence, probability to generate a weak key is very low.

Then, Juremi, Mahmod, & Sulaiman (2012) proposed a new approach for designing key dependent AES algorithms. The encryption and decryption process of this new design resembles the original AES, but the original AES consists of four stages while in this new design, it consists of five stages as shown in Figure 2. The key-dependent S-box changes in each round based on the key and number of rounds. The results show that the enhancement on the original AES does not violate the security of the cipher. However, in terms of performance and speed, the studied has not been sufficiently addressed and widely investigated.

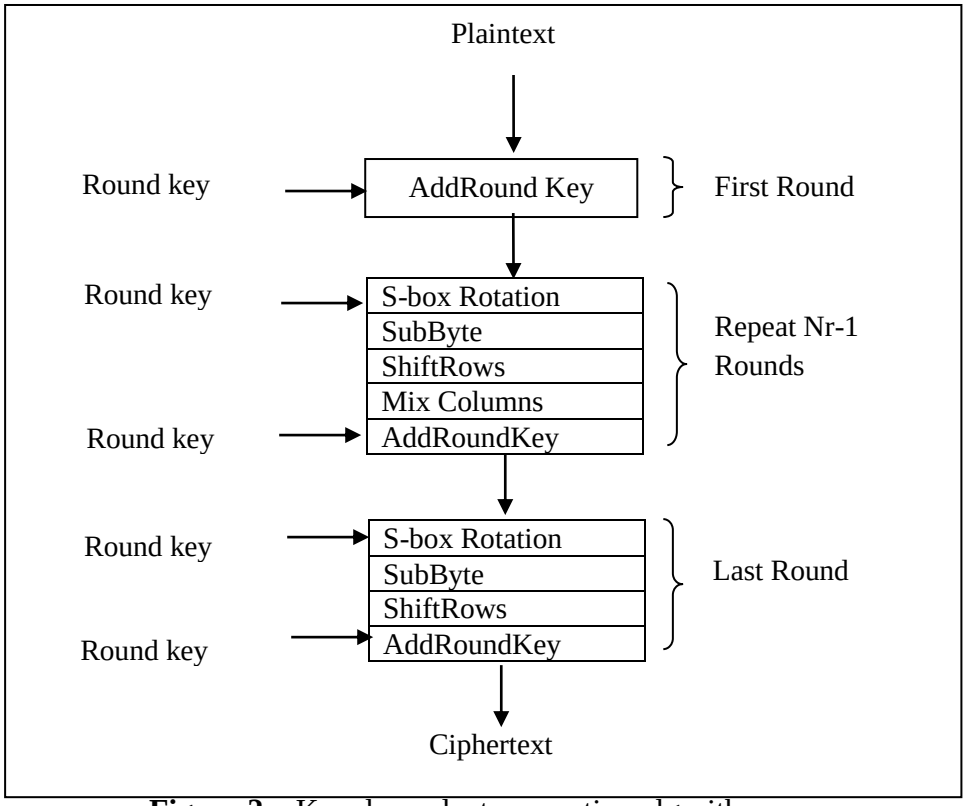

Figure 2. Key dependent encryption algorithm

Hosseinkhani & Javadi (2012) used the cipher key to generate dynamic S-box that is changed with every changing of the cipher key. The quality of this algorithm test by changing only two bits of cipher key to generate new S-box. This algorithm will lead generating more secure block ciphers to solve the problem of the fixed structure of S-box and increase the security level of the AES block cipher system. The main advantage of this algorithm is that many S-boxes can be generated by changing cipher key.

Stoianov & Altimirski (2012) found that in order to meet the requirements, new substitution matrices should be identified in the algorithm depending on the parameters or values of keys. Meanwhile, these S-boxes should have characteristics identical or better than those used in the standard AES. New substitution matrices were developed by XOR operation with choosing byte from the key and existing AES S-box. The result was analyzed and shows that the characteristics of the new 256 S-boxes are identical. The weakness of this study is it will not lead to a deterioration of stability of AES to linear and differential cryptanalysis.

Another studied by Nayaka and Biradar (2013) proposed a method for constructing 128 bits cryptographic key dependent S-Box, P-Box transposition and round key or sub key based on prime key. The proposed S-Box passes the avalanche, bit independence tests and randomness tests which are important features for strong S-box. SPN block cipher encryption algorithms which simultaneously use key based S-box, P-box, transposition and key expansion for block ciphers. The advantages of this scheme are:

i) Frequent cipher flow change based on key guarantees that can change the flow of ciphers immediately and easily by changing key alone.

ii) Key based cipher flow change prevents information from being concentrated under a single overall flow, which would be a primary attack target. This prevents the opposing attack budget from concentrating on a single algorithm flow.

iii) Frequent key based cipher flow changes support the continued creation and use of new ciphers, which the enemy must then identify, obtain, analyze and break. Thus, cryptanalysis will take longer time.

The operation of a cipher usually depends on the use of an encryption key. The key may be any auxiliary information added to the cipher to produce certain outputs. Block ciphers consist of static and dynamic S-box. In 2001, El-Ramly, El-Garf & Soliman were proposed a new approach to build up dynamic change S-boxes based on the Latin square S-box. The secret key of the length 128 bits is used to generate new Latin square S-box. This approach will solve the problem of the fixed structure S-boxes and consequently will increase the security level of the block cipher system. However, Wu , Noonan & Agaian (2011) stated that the main question of dynamic S-boxes is how to generate them with satisfactory properties. This is because the harder it is to discover the key, it shows that the more secure of the S-boxes mechanism. According to Anderson (2008) there are three things need to be done to make such a design secure: the cipher needs to be "wide" enough; the cipher needs to have enough rounds and the S-boxes need to be suitably chosen.

This study found that, many researchers proposed a new design for key dependent S-box in order to increase the security level of the AES block cipher. The security strength of all these ciphers depends on the nonlinearity properties to protect from cryptanalysis attack. In addition, it is very difficult and complex to use the traditional methods of mathematical to construct the S-box with good performance (Xiangyang, 2010). The dynamic S-box is needed to make cryptanalysis is difficult to discover the key in a block cipher. The dynamic or dependent key algorithm should be generated to increase the cryptographic strength of block cipher system. Thus more dynamic and key dependent S-box will increase the complexity and make the differential and linear cryptanalysis more difficult to attack the block cipher.

3 Comparison between AES S-box and Key Dependent S-boxes

Based on the previous studies the standard AES S-box should be improved in order to protect from cryptanalysis attack. Hence, Arrag et al. (2013) expanded and modified the structure of the AES S-Box. They used basic operations of the AES and implemented in Cyclone II Device by using VHDL Language. The encryption process based on subBytes, shiftflows, mixColumns and AddRoundKey. The result shows that; 256 substitutions have been obtained. The master key and dynamic SBOXxor key are used. Hence, the new substitution matrices have been developed by XOR. The disadvantages of this research are it consumes a little extra time and more logic elements. It also will not lead to a deterioration of the stability of the AES linear cryptanalysis and differential.

Then, Mahmoud et al. (2013) proposed the dynamic AES-128 with key dependent S-box based on permutes or rearrange the standard S-box under control of AES secret key is as shown in Table 1. This proposed algorithm leads to increase the complexity and makes the differential and linear cryptanalysis more difficult.

Table 1. Key Dependent S-box Steps

Steps	Corresponding sequence (hexadecimal form)
Secret key	B9B5ED7585C8B15D7454ED271AA3A3A3
Initial state	C0155C55ADF95E8C
PN sequence	0B5AFCEC075DF07DBFEE5CFA9B8D2F52
Permutation sequence	B2EF119982954120CBBAB1DD812E8CF1
S_1 before arrangement	B2EF119982954120
S_1 after arrangement	B2EF198540367ACD
S_2 before arrangement	CBBAB1DD812E8CF1
S_2 after arrangement	CBA1D82EF0345679

From Table 2, the both key dependent S-boxes are modified the AES S-box based on ByteSub using XOR operation in ShiftRow transformations. These studies presented that a new approach to generate a dynamic AES with key dependent S-boxes. It was established any change of the secret key; the structure of the S-box will be changed essentially. These studies also evaluated the performance of standard AES and the result showed that the dynamic AES is faster than standard AES. Moreover, the key dependent S-boxes are more secure and efficient compared than standard AES. However, the weakness of both key dependent S-boxes can be improved based on the features of complexity and the time complexity.

Table 2 shows the comparison between the AES S-Box and the key dependent S-boxes.

Table 2. Comparison between AES S-Box and Key Dependent S-boxes

	AES S-Box	Key dependent S-Boxes	
		Arrag, et. al. (2013)	Mahmoud et. al. (2013)
Block length	128-bits	256-bits	128-bits
Key Length	128-192-256 bits	256 bits	128-192-256 bits
Number of Rounds	For key length 128-bit. 10 Rounds	For key length 128-bit. 10 Rounds	For key length 128-bit: 10/12/14
Round Function	Composed of 4 transformation ByteSub using SBOX, Shift Row, Mix Column, AddRoundKey	Transformations: ByteSub using SBOXxor key Shift Row, Mix Column, AddRound-Key	Transformations: ByteSub using SBOXxor key Shift Row, Mix Column, AddRoundKey
SBOX	Fixed	initial Key Dependent	Permutes or rearrange the standard S-Box based on random sequence
Key Expansion	Use the master key and static SBOX	Use the master key and Dynamic SBOXxor key	Use to generate an initial key of a pseudo random(PN)
Performance	2.963207	Consumes little extra time	2.960076

4 Conclusion

S-box is the most critical step in any block cipher system. The strong and secure S-box is needed to protect a key in a block cipher. The key should be difficult to discover in order to show that the more secure of the S-boxes mechanism. This study found that a key dependent S-box are more strength against linear and differential cryptanalysis comparable than the static S-box. Through the key dependent S-box and XOR's together with an involution structure, it can be efficiently implemented on various platforms. Besides that, with a key dependent S-box the security margin of the cipher is increased the strength of the cipher. As a result, a thorough understanding of key dependent S-box will help us to develop better ways to protect valuable information as technology becomes faster and more efficient.

5 References

Anderson, R. J. (2010). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

Arrag, S., Hamdoun, A., Tragha, A., & Khamlich, S. E. (2013). IMPLEMENTATION OF STRONGER AES BY USING DYNAMIC S-BOX DEPENDENT OF MASTER KEY. *Journal of Theoretical & Applied Information Technology*, *53*(2).

El-Ramly, S. H., El-Garf, T., & Soliman, A. H. (2001). Dynamic generation of S-boxes in block cipher systems. In *Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National* (Vol. 2, pp. 389-397). IEEE.

El-Sheikh, H. M., El-Mohsen, O. A., Elgarf, S. T., & Zekry, A. (2012). A new approach for designing key-dependent S-box defined over GF (24) in AES. *International Journal of Computer Theory and Engineering*, *4*(2), 158.

Gutub, A. A. A., & Khan, F. A. A. (2012, November). Hybrid crypto hardware utilizing symmetric-key and public-key cryptosystems. In *Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on*(pp. 116-121). IEEE.

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), 19-28.

Juremi, J., Mahmod, R., & Sulaiman, S. (2012, June). A proposal for improving AES S-box with rotation and key-dependent. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 38-42). IEEE.

Mahmoud, E. M., Abd, A., Hafez, E., & Elgarf, T. A. (2013). Dynamic AES-128 with key-dependent S- box. International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 1, January-February 2013, pp.1662-1670.

Nayaka, R. J., & Biradar, R. C. (2013, June). Key based S-box selection and key expansion algorithm for substitution-permutation network cryptography. In *Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy (AICERA/ICMiCR), 2013 Annual International Conference on* (pp. 1-6). IEEE.

Niemiec, M., & Machowski, L. (2012, October). A new symmetric block cipher based on key-dependent S-boxes. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on* (pp. 474-478). IEEE.

Schneier, B. (2007). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, *28*(4), 656-715.

Stoianov, N., & Altimirski, E. (2012). A new approach of generating key-dependent S-BOXes in AES. *Technical University of Sofia, INDECT project team.*

Wu, Y., Noonan, J. P., & Agaian, S. (2011, October). Dynamic and implicit latin square doubly stochastic s-boxes with reversibility. In *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on* (pp. 3358-3364). IEEE.

Xiangyang, X. (2010, May). The block cipher for construction of S-boxes based on particle swarm optimization. In *Networking and Digital Society (ICNDS), 2010 2nd International Conference on* (Vol. 1, pp. 612-615). IEEE.

Zhang, R., & Chen, L. (2008, June). A block cipher using key-dependent S-box and P-boxes. In *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on* (pp. 1463-1468). IEEE.