Towards the Generation of a Dynamic Key-Dependent S-Box to Enhance Security

[1] Grasha Jacob, [2] Dr. A. Murugan, [3]Irine Viola

[1]Research and Development Centre, Bharathiar University, Coimbatore – 641046, India, grasharanjit@gmail.com

[Assoc. Prof., Dept. of Computer Science, Rani Anna Govt College for Women, Tirunelveli]

[2] Assoc. Prof., Dept. of Computer Science, Dr. Ambedkar Govt Arts College, Chennai, India

[3]Assoc. Prof., Dept. of Computer Science, Womens Christian College, Nagercoil, India

E-mail: [1]grasharanjit@gmail.com

ABSTRACT

Secure transmission of message was the concern of early men. Several techniques have been developed ever since to assure that the message is understandable only by the sender and the receiver while it would be meaningless to others. In this century, cryptography has gained much significance. This paper proposes a scheme to generate a Dynamic Key-dependent S-Box for the SubBytes Transformation used in Cryptographic Techniques.

Keywords: *Hamming weight, Hamming Distance, confidentiality, Dynamic Key dependent S-Box*

1. INTRODUCTION

Today communication networks transfer enormous volume of data. Information related to healthcare, defense and business transactions are either confidential or private and warranting security has become more and more challenging as many communication channels are arbitrated by attackers. Cryptographic techniques allow the sender and receiver to communicate secretly by transforming a plain message into meaningless form and then retransforming that back to its original form. Confidentiality is the foremost objective of cryptography. Even though cryptographic systems warrant security to sensitive information, various methods evolve every now and then like mushroom to crack and crash the cryptographic systems. NSA-approved Data Encryption Standard published in 1977 gained quick worldwide adoption. However, DES was cracked with the advancement of technology in both hardware and software. The main disadvantage of DES was its short key length [2]. Hence it is highly indispensible to deliver and defend the confidentiality of sensitive and confidential information such as medical image data, pin numbers used in business transactions, defense information and personal data when stored in public databases or transmitted over networks of any kind. Several researchers were motivated to propose a variety of alternative designs concerning the security issue and the relatively slow operation of DES. The Advanced Encryption Standard published by NIST in December 2001 then became the standard encryption technique. In AES, the static S-Box denotes SubByte transformation and offers non linearity and confusion, created by multiplicative inverse and affine transformation.

Confusion and Diffusion are the nitty-gritties of any Cryptographic technique. Cryptographic techniques are mainly regarded as symmetric or asymmetric. The central part of any Symmetric key cryptographic technique is the S-Box, SubBytes transformation that offers the necessary confusion. They are used for concealing the relation between the plain text and the cipher text and are essentially non-linear mapping which take as input a certain number of bits and convert them into some number of bits. The number of bits at the input and output need not be equal. The security of systems using the S-boxes relies on a great deal on their proper selection.

2. DEFINITIONS

Definition 2.1 Hamming weight: The Hamming weight (H_w) of a binary vector V, is the number of 1's in V.

Definition 2.2 Hamming distance (H_d) between two binary vectors of equal length is the number of places for which the corresponding entries are different.

Definition 2.3 Key Dependent Dynamic S-Box function: A Key Dependent Dynamic S-Box is a mapping function,

$f:\{0,1\}^m \rightarrow \{0,1\}^n$,

that maps n bit input string X into n bit output string Y based on the codeword and has the following properties:

i. **Bijection**
ii. **Strict avalanche criterion**
iii. **Correlation-immunity**
iv. **Nonlinearity**
v. **Balance**

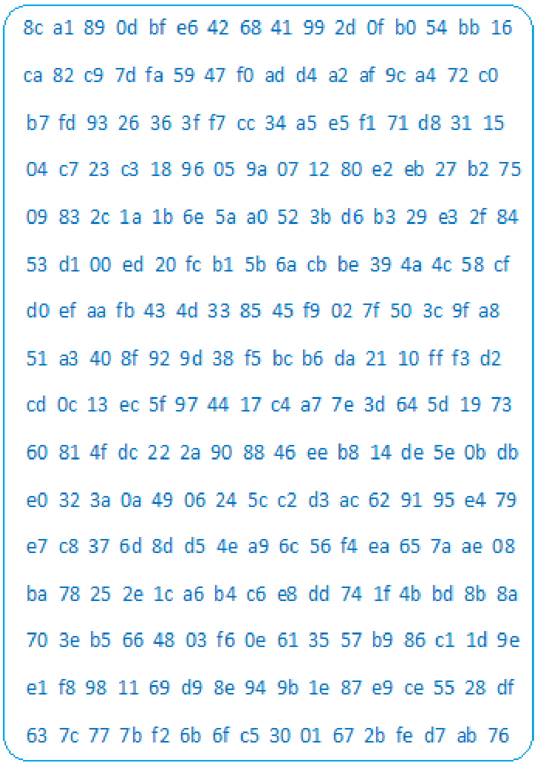
Definition 2.4 Bijection: A bijection (or bijective function or one-to-one correspondence) is a function between the elements of two sets, where every element of one set is paired with exactly one element of the other set, and every element of the other set is paired with exactly one element of the first set. A bijective function f: X → Y is a one to one and onto mapping of a set X to a set Y. A bijection from the set X to the set Y has an inverse function from Y to X.

Definition 2.5 Strict Avalanche Criterion: If a one bit change in the input results in at least 50 percent changes in the output bits, then there is Strict Avalanche criteria.

Definition 2.6 Correlation-immunity: If the output bits act independently from each other, then there is Correlation-immunity.

Definition 2.7 Nonlinearity: A function with its corresponding vector is said to be highly nonlinear when the resulting vector y_i from a function f_i has a high Hamming distance with all the linear vectors in the set of B_n.

Definition 2.8 Balanced: An S-box with n input bits and m output bits, m ≤ n, is balanced if each output occurs 2^{n-m} times. For the S-box to be balanced it should have the same number of 0's and 1's.



```
8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae 08
ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
```

Fig 1. Dynamic Key Dependent S-Box when the CodeWord is 11000001 (Key: F95B BAF3 656E FB64)

3. GENERATION OF DYNAMIC S-BOX

The Rijindael S-Box (used in AES) is generated by determining the multiplicative inverse for a given number in $GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$, Rijindael's finite field [8]. The multiplicative inverse is then transformed using the affine transformation.

In the proposed scheme, for generating the Dynamic key dependent S-Box, the AES S-Box is considered as the standard and used as the look-up table. For simplicity, in this paper, the keys and the Dynamic key dependent S-Box function are represented in hex. With the key dependent Dynamic S-Box function, each of the 256 possible byte values is being transformed to a different byte based upon the codeword generated from the key (a complete permutation). Every input gets changed, and all 256 possible elements are represented as the result of a change. Moreover, no two different bytes are mapped on to the same byte. Fig. 1 represents the Dynamic key dependent S-Box generated at runtime, when the key is A451B67290F7DE38.

```
DynamicS-Box(key)
Output :Dynamic S-Box

 1. codeword = Codeword_Generator(key)
 2. Z = Bin2dec(codeword) + 1
 3. Case Z of
        1 – 32 : do row transformation
        33-64 : do column transformation
        65-96: transpose of results obtained in case 1- 32
        97-128 : transpose of results obtained in case 33- 4
        129 – 160 : nibble exchange of results obtained in case 1- 32
        161 - 192 : nibble exchange of results obtained in case 32-64
        193 -224: transpose of results obtained in case 129- 160
        225 -256: transpose of results obtained in case 161-192
    EndCase
 4. Return Dynamic S-Box

End DynamicS-Box
```

3.1. Generation of Codeword:

The key used for encryption is considered to be 64 bits in length (eg., A451 B672 90F7 DE38). From the key, a codeword of 8 bits ($C_8C_7C_6C_5C_4C_3C_2C_1$) is generated at run-time based upon the Hamming Distance and Hamming Weight. The Dynamic key-dependent S-box generated at runtime based upon the codeword is non-linear in nature. For generating the codeword the following two assumptions are considered.

i. Each bit of the codeword calculates the parity (Hamming weight) for certain bits in the key.
ii. A parity bit is set to 1 if the total number of ones in the positions it checks is odd or 0 otherwise.

```
Codeword_Generator(key)
Output : codeword
 1. C8: check all the bits of the key(1-64)
 2. C7: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1,3,5,7,9,11,13,15,...)
 3. C6: check 2 bits, skip 2 bits, check 2 bits etc. (2,3,6,7,10,11,14,15,...)
 4. C5: check 4 bits, skip 4 bits, check 4 bits etc. (4,5,6,7,12,13,14,15,...)
 5. C4: check 8 bits, skip 8 bits, check 8 bits etc. (8-15,24-31,40-47,...)
 6. C3: check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc. (16-31,48-56)
 7. C2: check 32 bits, skip 32 bits, check 32 bits etc. (32-63)
 8. C1: check bit 1 and bit 64
 9. codeword=C8C7C6C5C4C3C2C1
```

End Codeword_Generator

The codewords for the keys A451 B672 90F7 DE38 and A451 B672 90F7 DE39 and 44D2 B6F6 B576 CB3D generated using the above procedure are 10111001, 00111100 and 11111111 respectively.

4. DESIGN ANALYSIS

The proposed scheme of dynamic key dependent S-Box is analyzed based on the five criteria for a good S-Box.

4.1. Bijection:

In the dynamic key dependent S-Box generated, there is a one-to-one and onto mapping from input vectors to output vectors as the input vectors and output vectors are isomorphic. Hence the property of Bijection holds good for the dynamic key dependent S-Box proposed.

4.2. Strict Avalanche Criterion

In the proposed work, slight changes in the input vector leads to a significant change in the output vector.

The codewords for the keys A451 B672 90F7 DE38 and A451 B672 90F7 DE39 (differ only in the least significant bit- ie., one bit change) are 10111001, 00111100 and hence significantly different Dynamic S-Boxes based on the codewords are generated. Hence there exists Strict Avalanche Criterion in the dynamic key dependent S-Box proposed and it is complete.

4.3. Correlation Immunity:

In the proposed dynamic key dependent S-Box scheme, the S-box values are not known initially and this increases its main strength, as both linear and differential cryptanalyses require known S-boxes. The dynamic key dependent S-Box generated has high Correlation-immunity, as the output bits act independently from each other.

4.4. Non-Linear Mapping:

As the dynamic key dependent S-Boxes are generated from the key in sufficiently random fashion based upon the codeword, each S-box possesses fairly high nonlinearity and has a high probability of being complete.

4.5. Balance:

If there are equal number of zeros and ones in the S-Box generated, then the dynamic key dependent S-box generated is balanced. The condition for balance can be proved by the principle of induction.

Let P(n) denote the number of zeros(ones) in the different combinations.

When n = 1, the bit can be either 0 or 1.
$P(1)$ = Number of zeros = Number of ones = 1.

When n = 2, the combinations are 00, 01, 10 and 11.
$P(2)$ = Number of zeros = Number of ones = $(2^n)/2 + 2 * P(1) = 4/2 + 2*1 = 4$.

When n = 3, the combinations are 000,001,010,011,100,101,110,111
$P(3)$ = Number of zeros = Number of ones = $(2^n)/2 + 2 * P(2) = 8/2 + 2*4 = 12$.

$P(4) = (2^n)/2 + 2 * P(3) = 8 + 24 = 32$

Assume P(k) is true for n = k.
$P(k) = (2^k)/2 + 2 * P(k-1)$

To prove P(k+1) is true.
$P(k+1) = (2^k+1)/2 + 2 * P(k)$

If p(k) is true, then p(k+1) is true.
Hence by the principle of mathematical induction, P(n) is true for all n $\in$ N.

Therefore, when n=8, P(k) = (2^8)/2 + 2 * P(7) = 1024.
Number of zeros = number of ones = 1024 indicating that the dynamic key dependent S-box generated is balanced.

Thus the proposed scheme for the generation of dynamic key dependent S-Box satisfies all the criteria for a good S-Box.

5. CONCLUSION

. The proposed dynamic key dependent S-Box coding when incorporated with other cryptographic techniques will support in higher degree of security. The proposed scheme is simple, easy to implement, difficult to guess and can be adopted to enhance security and thereby resist internet-borne attacks.

REFERENCES

[1] W. Diffie, E.M. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard". Computer, 10 (6): 74–84, June 1977

[2] E. Biham, A. Shamir, "Differential Cryptanalysis of DES like Cryptosystems", Journal of Cryptology 4 (1): 3–72, (1991)

[3] B. H. Westlund,. "NIST reports measurable success of Advanced Encryption Standard". Journal of Research of the National Institute of Standards and Technology, (2002)

[4] G.N. Krishnamurthy, V. Ramaswamy, “Making AES Stronger: AES with Key Dependent S-Box”, IJCSNS International Journal of Computer Science and Network Security, vol.8, pp. 388-398 (2008).

[5] N. R. Wagner, “The Laws of Cryptography: Advanced Encryption Standard: S-Boxes”

[6] K. Kazlauskas, J. K. Kazlauskas, “Key-Dependent S-Box Generation in AES Block Cipher System” Journal Informatica, vol 20(1): 23-34, (2009)

[7] K. Khoo, Chu-Wee Lim, Guang Gong, “Highly Nonlinear Balanced Sboxes with Improved Bound on Unrestricted and Generalized Nonlinearity”, Applicable Algebra in Engineering, Communication and Computing, vol 19(4), 323-338 (2008)

[8] en.wikipedia.org/wiki/Rijndael_S-box