Volume 7, Issue 1, January 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Modified AES S-Box Based on Determinant Matrix Algorithm

Julia Juremi*, Ramlan Mahmod, Zuriati Ahmad Zukarnain, Sharifah Md. Yasin
Faculty of Computer Science & Information Technology, Universiti Putra Malaysia,
43400 UPM, Serdang, Selangor, Malaysia

Abstract—There are many researches in designing and enhancing Rijndael, since it has been chosen as AES. The S-box is the only nonlinear part in the symmetric encryption algorithms and it defines the performance of AES. In this paper, we propose a new stage named as DeterminantRotation (DR) in modifying and generates different S-box for each round by implementing determinant matrix calculation in rotating the position of AES S-box to be used in the SubBytes transformation. The randomness test and the avalanche test were performed on the output produced in order to prove the security of the new proposed algorithm. The result of the tests shows that the proposed algorithm in the new extra stage has good randomness as well as proven to be secured.

Keywords— block cipher, algorithm, AES, determinant, rotation, randomness, avalanche

I. INTRODUCTION

Cryptography and encryption technique is one of the most proficient approaches employed in order to secure and protect the non-secure channels from attackers. Since Rijndael block cipher or AES (Advanced Standard Encryption) has been announced and adopted by the US government to be used widely as a standard encryption algorithm, there are many other encryption algorithms being develop to fulfil the requirement of secure block cipher. AES is a very robust algorithm that has shown resistance towards many cryptographic attacks so far. It is a symmetric block cipher that can process 128 bits of data blocks using 128, 192 or 256 bits of cryptographic keys. Basically, the block cipher consists of a sequence of identical rounds with each of the round operating under a round key computed from the key.

Numerous efforts have been done in redesigning and reconstructing the AES algorithm in order to improve its performance. There are many methods used by researchers in the design and modification of AES block cipher in order to enhance the security of the algorithm as in [3], [4], [5], [7] and some including merging the AES block cipher with other models from various fields, such as in [1] [2] [8] and [9]. Since the AES original S-box has been designed and tested thoroughly for linear and differential attack, attempt on substituting the original S-box without detailed analysis may violate the security of AES original design. This paper introduces a new approach, DeterminantRotation (*DR*) in modifying and generates different AES S-box each round by implementing determinant matrix calculation in rotating the position of AES S-box to be used in the SubBytes transformation. The aim of this paper is to modify the original AES S-box in terms of the position of state for each round and to generate different S-box to be used in each round without risking the security properties of a block cipher algorithm.

II. BLOCK CIPHER

In AES, a block of plaintext will be XORed with the initial key and go through the round transformation which comprise of four transformation processes which are SubBytes, ShiftRows, MixColumns and AddRoundKey [19]. It uses a 4x4 byte array known as the state in each cycle of the encryption and decryption process. Generally the block cipher consists of three elements: plaintext *P*, key *K* as input, and ciphertext *C* as output. The encryption and decryption process are denoted as Ek, and Dk respectively. The mathematic represent of the cryprosystem is as follows:

$$\forall\, k \in \mathrm{K}\ \exists\ Ek \text{ and } Dk : Dk(Ek(s))=\mathrm{s}\ \forall\ \mathrm{s} \in P$$

The S-box is the main non-linear transformation in an encryption algorithm which replaces a set of input bits with a different set of bits known as its output bits. If S-Box denoted by: πsb then:

$$\pi sb\text{: } \{0,1\}n \longrightarrow \{0,1\}n$$

where *n* represent the number of input and out bits for S-box.

III. PROPERTIES OF DETERMINANTS

The determinant is a value in linear algebra that can be computed from the elements of a square matrix. The determinant of a matrix J, denoted det(J), detJ , or $|J|$ and can be viewed as the scaling factor of the transformation described by the matrix. In the case of a 2 × 2 matrix, the specific formula for the determinant:

$$|J| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \text{ad-bc}$$

Equally, suppose we have a 4 × 4 matrix *J*, and we want the specific formula for its determinant |*J*|:

$$|J| = \begin{vmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{vmatrix} = \mathrm{a}\begin{vmatrix} e & f \\ h & i \end{vmatrix} - \mathrm{b}\begin{vmatrix} d & f \\ g & i \end{vmatrix} + \mathrm{c}\begin{vmatrix} d & e \\ g & h \end{vmatrix} - \mathrm{d}\begin{vmatrix} b & c \\ h & i \end{vmatrix}$$

A matrix is often used to signify the coefficients in a system of linear equations where determinants can be used to resolve those equations. The determinant of a square matrix J is denoted by “det J” or $|J|$. The determinant is a real number, it can be a negative number and it can only exists for square matrices {*2x2, 3x3, …, nxn*}[11]. The determinant of matrix will be zero if an entire row is zero, or two rows or columns are equal, or a row or column is a constant multiple of another row or column. The inverse of a matrix will exist only if the determinant is not zero. A square matrix *J* has an inverse if the determinant if $|J| \neq 0$. The so-called invertible matrix theorem is major result in linear algebra which associates the existence of a matrix inverse with a number of other equivalent properties. A matrix possessing an inverse is called non-singular, or invertible. An immediate consequence of the result is the following important theorem.

Theorem A: Let *J* be an *nxn* matrix. If *J* has a row of zeros then $|J| = 0$.

Theorem B: An *n x n* matrix *J* is invertible if and only if $|J| \neq 0$.

Theorem C: If *J* is invertible, then $|J^{-1}| = \frac{1}{|J|}$ [12].

IV. PROPOSED METHOD

Static S-box means the same S-box will be used in each round. Fixed S-box permits attackers to study the S-box and find frail points, while changing the S-box for each round will makes it tougher for attacker to do any offline analysis of an attack of one particular set of S-boxes [6]. However, overall performance in terms of security and speed has not been sufficiently addressed and widely investigated [13].

In our research, an additional stage known as DeterminantRotation, denoted DR, is introduced at the beginning of each round function to rotate the S-box. A fixed 128-bit block of plaintext, P and an initial key, K of size 128 bits will be inputted to the block cipher algorithm. Both P and K (in Hex) are placed into a square array with four rows and four columns as (4x4) matrix named as state. P and the K will be XORed with each other producing a new input state. Next, the values in the new input state are converted to decimal number before performing the computation of determinant matrices on the input state. The determinant value calculated will then be used to rotate the original AES S-box position.

The result of the rotation process will generate ten modified determinant S-box, for 10 rounds which is obtained by the inspiration of the determinant matrix calculation. The DR will then be used in the substitution transformation SubByte, SB. The remaining four stages ShiftRow SR, MixColumn MC and AddRoundKey ARK are unchanged as it is in AES. After the final stage of transformation, the state is copied to an output matrix as C. Fig. 1 shows the new proposed stage in AES block cipher.

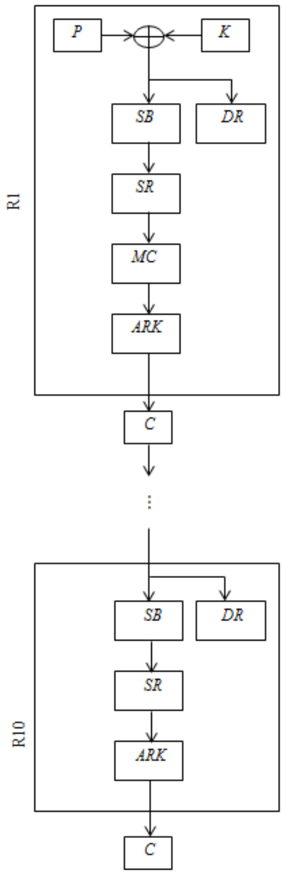

Fig. 1 New proposed stage in AES block cipher

The randomness of the output produced at the end of the transformation will be tested through the NIST Statistical Test Suite [10] to ensure the randomness and security of the proposed algorithm. Fig. 2 illustrates the process of DR in generating a new S-box for one round.

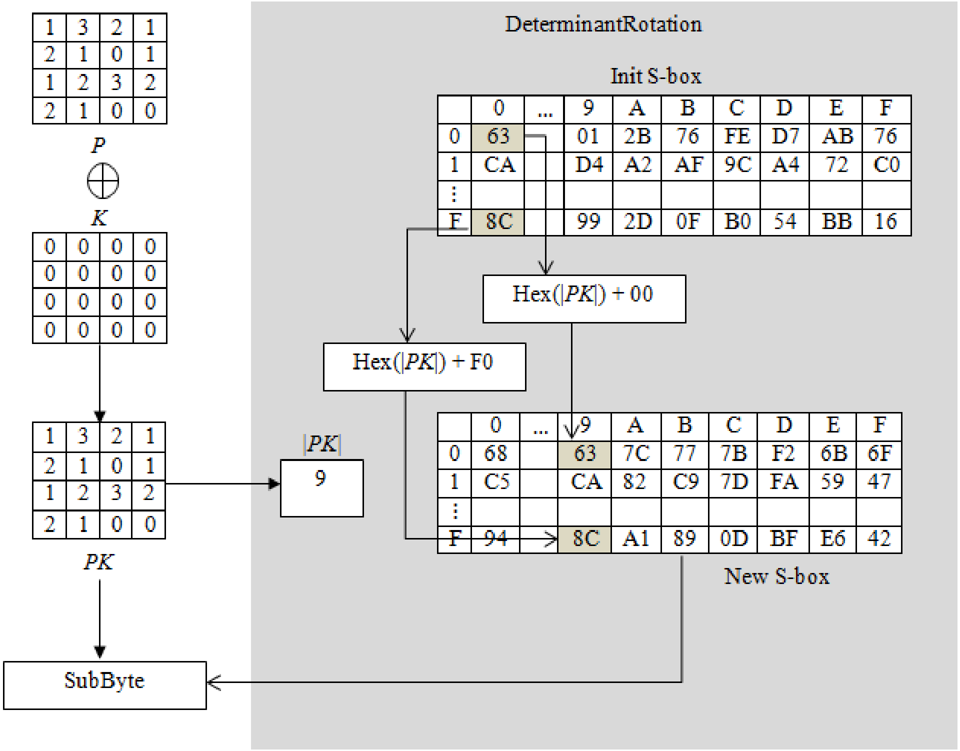

Fig. 2 DeterminantRotation used in rotation of S-box position

In the *DR* stage, the values in the input state *PK* are converted to decimal number and the determinant of the 4x4 state will be calculated to produce |*PK*|. |*PK*| will then be used to rotate the value in the original S-box generating a new position for the S-box. The input state *PK* will then be substituted with the new modified S-box and the next stage of round transformation will be continued as usual. For example, in Figure 2, |*PK*| = 9. Since 9 is a positive value, the initial S-box will be rotated nine times to the right, producing a new position as described in New S-box. However, since *P* and *K* are randomly generated, the determinant may produce a negative number. If |*PK*| is negative, then the S-box will be rotated |*PK*| times to the left. On the off chance that |*PK*| = 0, a new *K* will be generated and the process *P* ⊕ *K* will be repeated to obtain a new *PK*. The reason of discarding |*PK*| = 0 is so that the inverse process of the S-box can be done since the inverse of a matrix can only exists if the determinant ≠ 0. In the case of |*PK*| > 255, then |*PK*| will be mod with 256. This is because since the maximum size of the initial S-box is 16x16 state array, having a, for example |*PK*| = 300, would mean rotating the original S-box to the same position once plus the additional 44 times to the right. Thus to avoid wasting time on the unnecessary rotation, |*PK*| that is bigger than 255 will be mod by 256, ensuring that the S-box is rotated based on the remainder only. If the remainder is evaluated to 0, then this would mean no rotation process needed on that round and the SubByte operation will be performed on the initial S-box.

V. EVALUATION CRITERIA

I. Randomness Test

The first evaluation is to measure the randomness of the output generated by the proposed algorithm. NIST Statistical Test Suite is used in order to evaluate the randomness of the output. It is one of the security testing tools that are used to evaluate the confusion and diffusion properties for the new encryption system, according to [14]. The test judges if the production of undoubted algorithms under test conditions shows features that suggest that the outputs are randomly generated. The values of the 128 bit plaintext and 128 bit key were based on data generated using the pseudo-random bit generator. According to [14], as a minimum, 128 sequences with 1,000,000 bits for each sequence should be used for an NIST test suite. This paper uses 146 sequences of length 1,000,064 bits per sequence in length, which were tested and plotted in the laboratory experiments' action as a random plaintext with random keys of 128 bits. The tested ciphertext for the experiments is the output of round 1, 2 and 3 of the modified S-box. The entire randomness testing relied upon the use of the NIST Statistical Test Suite, which comprises 15 tests. Most of the 15 tests have one p-value; however, some of the tests have more than one P-value. Table I shows the breakdown of the 15 statistical tests applied during the experiment. Every P-value matches to the function of a random statistical test on a distinct block and this block is a binary sequence [15]. The significant level α used for analysis of its value = 0.01, as proposed by NIST, for the study of P-values gained from a variety of statistical tests. Depending on the p-value the following states can be concluded:

1) The sequence is shown to be completely non-random if a p-value = 0.
2) The sequence is shown to be non-random if a p-value <0.01.
3) The sequence is shown to be random if a p-value ≥0.01.
4) The sequence is shown to be perfect-random if a p-value =1.

Table I: 15 Statistical Tests Conducted During Experimentation

Number of Test ID	**Type of NIST Statistical Test**	**Number of P-value**
1	Frequency	1
2	Frequency Within a Block	1
3	Runs	1
4	Longest-Run-of-Ones in a Block	1
5	Binary Matrix Rank	1
6	Discrete Fourier Transform (Spectral)	1
7	Non-overlapping Template Matching	1
8	Overlapping Template Matching	1
9	Maurer's "Universal Statistical"	1
10	Linear Complexity	1
11 - 12	Serial	2
13	Approximate Entropy	1
14 - 15	Cumulative Sums (Cusums)	2
16 - 23	Random Excursions	8
24 -41	Random Excursions Variant	18

Given the empirical results for a particular statistical test, the proportion of the sequences that passed will be calculated. In this experiment, 146 binary sequences 1,000,064 bits were tested, s = 146, α = 0.01 (the significance level). The range of acceptable proportions acceptable is determined using the confidence interval defined:

$$P\alpha = (1 - \alpha) \pm 3\sqrt{((\alpha\,(1- \alpha))/146)} = 0.96530$$

where P = 1 – α, and s is the sample size. The proportion of the sequences that exceeded a particular statistical test should rest above the proportion value Pα. According to [17][18], the Frequency Test, Frequency Test Within Block an Run Test are most associated to SAC test in examining the randomness and avalanche effect for ciphertext. Fig. 3 shows the result of the Frequency Test for round 3 of the modified S-box block cipher. For the Frequency Test, it was reported that 143 out of 146 sequences exhibits p-values greater than 0.01 with proportion of 0.979 in round 3 indicating that the block cipher passes the Frequency Test. The Frequency Within Block Test shows that 144 out of 146 sequences recorded p-values greater than 0.01 for round 3 indicating that the block cipher passes the Frequency Within Block Test with the proportion of 0.986 and the result is demonstrate in Fig. 4. The Runs Tests results for the modified S-box shows that in round 3, 145 out of 146 sequences recorded p values greater than 0.01, indicating the modified S-box block cipher pass the Runs Tests with proportion of 0.993 and the result is demonstrate in Fig. 5. All of the results show the modified rotated S-box provides good randomness to the output which proves to fulfil the security requirement.

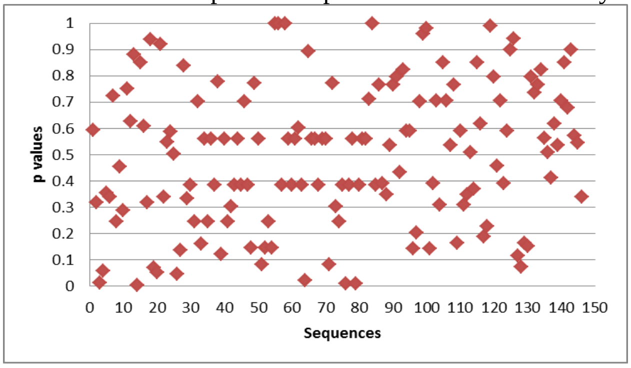

Fig. 3 Frequency Test of Modified S-box using DeterminantRotation for Round 1

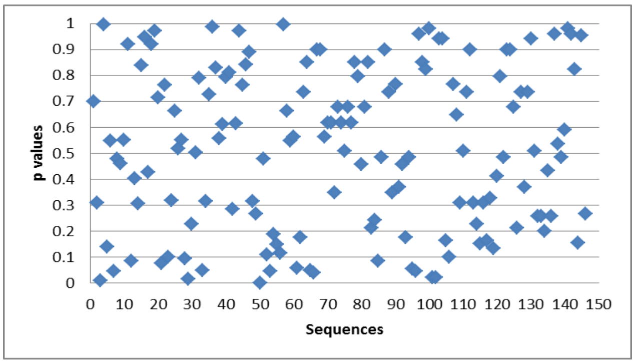

Fig. 4 Frequency Within Block Test of Modified S-box using DeterminantRotation for Round 2

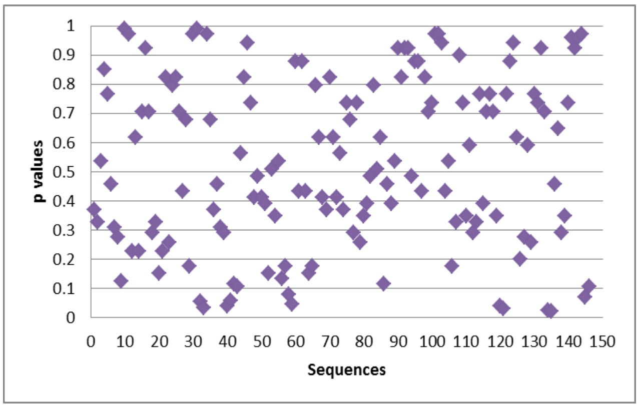

Fig 5 Runs Test of Modified S-box using DeterminantRotation for Round 3

The high p-value of the Frequency Test is a major indicator of the proposed algorithm and considered as one of the important measures of the security of block cipher algorithm. Fig. 6 shows the result of the randomness test gathered for the modified S-box block cipher at round 3.

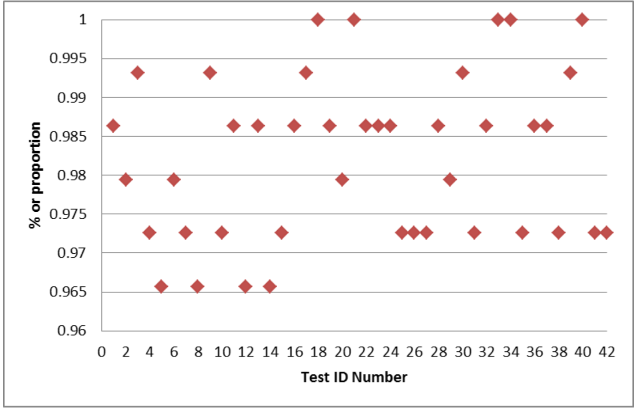

Fig. 6 Randomness Test Result for the modified S-box block cipher at round 3

II. Key Sensitivity Test

Key sensitivity test is to identify the rate if a bit changes between the original ciphertext and the changing ciphertext with one digit key difference. 128 data sets were tested each of them consists of 32 sequences (128 bits per sequence). The result of the test is tabulated in Table II. Fig. 7 shows plot of the difference between the point location of key changed and the bit error rate. It shows that the values of bit differ between two ciphertexts of every sequence of key lie within range of 0.5 or 50%. The result indicates that a single bit change on input causes changes on approximately half of the output bits. It justifies the high sensitivity of ciphertext to the key. The result of the test is tabulated in Table II and Fig. 7 shows the difference between the point location of key changed and the bit error rate.

III. Correlation coefficient

Correlation coefficient is a number between -1 and 1 which measures the degree to which two variables are linearly related. The correlation is 1 in the case of an increasing linear relationship, −1 in the case of a decreasing linear relationship, and some value in between in all other cases, indicating the degree of linear dependence between the variables [16]. If the variables are independent then the correlation is 0. The experiment examined all functions of the modified S-box. The analysis is shown in Fig. 8, where the correlation value for round 1, 2 and 3 for each sequence is recorded. Figure shows that most of the correlation value, at different rounds during the modified S-box algorithm implementation is near to 0, which indicate a strong positive or negative non-linear relationship. From the results of the analysis, it can be concluded that the modified S-box shows an increased confusion performance between the plaintext and the ciphertext.

Table II: Number of Bit Error and Bit Error Rate of Key

Point location changed	Key	Differ bits	Ratio
1	1234567890123456	260	0.507813
2	1234567890123056	284	0.554688
3	1234567890120456	271	0.529297
4	1234567890103456	237	0.462891
5	1234567890023456	257	0.501953
6	1234567891123456	255	0.498047

7	1234567800123456	267	0.521484
8	1234567090123456	240	0.468750
9	1234560890123456	243	0.474609
10	1234507890123456	254	0.496094
11	1234067890123456	255	0.498047
12	1230567890123456	279	0.544922
13	1204567890123456	245	0.478516
14	1034567890123456	237	0.462891
15	0234567890123456	252	0.492188

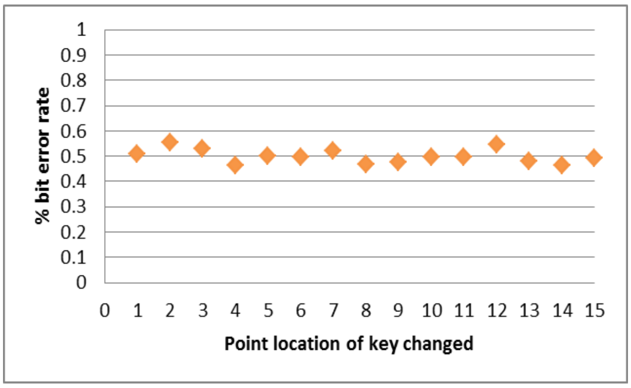

Fig. 7 Key Sensitivity Analysis

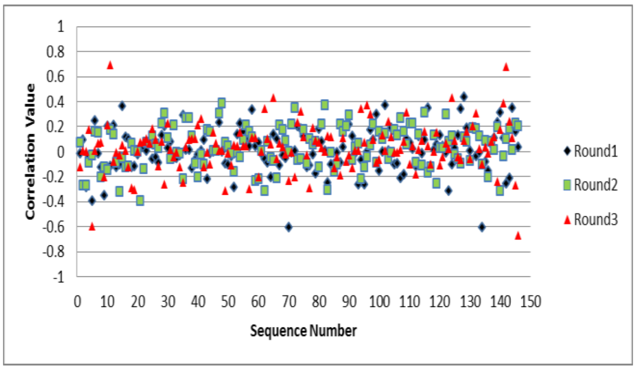

Fig. 8 Correlation test results on modified S-box

VI. CONCLUSION

This paper introduced a new method DeterminantRotation (DR) in modifying and generates different AES S-box each round by implementing determinant matrix calculation in rotating the position of AES S-box to be used in the SubByte transformation. This new approach will not challenge the security of the original AES algorithm by keeping all the mathematical criteria of AES remain unaffected. The performance of this proposed approach is tested and it has been proven that a simple mathematical operation could be implemented and used in the encryption algorithm like AES. For the security analysis purpose, the randomness test, the key sensitivity test and the correlation for the modified S-box has been done. The results of the experiments and analysis show that the modified S-box has successfully passed several demanding security analysis. Hence, it can be concluded that the modified S-box is a secure algorithm and can be used to produce random output. This research still requires many further investigations which include analysis on the security of modified S-box and cryptanalysis attack on the new algorithm as part of the evaluation test. The result of the cryptanalysis attack is hoped to help in allowing its subversion or evasion.

REFERENCES

[1] Ariffin et al., “Symmetric encryption algorithm inspired by randomness and non-linearity of immune systems,” *International Journal of Natural Computing Research*, 3(1), pp. 56-72, January-March 2012.

[2] G. Tang, *et al.*, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 23, pp. 413-419, 2005.

[3] M. T. Tran, *et al.*, "Gray S-box for advanced encryption standard," in *Computational Intelligence and Security, 2008. CIS'08. International Conference on*, 2008, p. 253-258.

[4] D. Canright and L. Batina, "A very compact “perfectly masked” S-box for AES," in *Applied Cryptography and Network Security*, 2008, p. 446-459.

[5] G. Krishnamurthy and 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.

[6] H. M. El-Sheikh, *et al.*, "A new approach for designing key-dependent S-Box defined over GF (2^4) in AES," *International Journal of Computer Theory and Engineering,* vol. 4, No. 2, April 2012.

[7] A. Janadi and D. Anas Tarah, "AES immunity enhancement against algebraic attacks by using dynamic S-Boxes," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, 2008, p. 1-6.

[8] G. Zaibi, *et al.*, "A new design of dynamic S-Box based on two chaotic maps," in *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference*, 2010, p. 1-6.

[9] Al-Wattar et.al., "A new DNA-based S-Box" in *International Journal of Engineering & Technology IJET-IJENS*, Vol:15 No:04.

[10] L. E. Bassham III, *et al.*, "SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," 2010.

[11] Szidarovszky and Molnar, *Introduction to Matrix Theory with applications to business and economics,* Series on Concrete and Applicable Mathematics, Vol.3., World Scientific, 2001.

[12] Lipschutz, S., *Invertible Matrices, Schaum's Outline of Theory and Problems of Linear Algebra*, 2nd ed.,New York:McGraw-Hill, p 44-45, 1991.

[13] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," in *Selected Areas in Cryptography*, p. 103-111, 2001.

[14] J. Soto and L. Bassham, "Randomness testing of the advanced encryption standard finalist candidates," DTIC Document, 2000.

[15] A. Rukhin, *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," DTIC Document, 2001.

[16] Mahmoud et al., "Dynamic AES-128 with key-dependent S-box*," International Journal of Engineering Research and Applications (IJERA)*, Vol. 3, Issue 1, pp.1662-1670, January -February 2013.

[17] Doganaksoy, A., Ege, B., Koçak, O., & Sulak, F., "Cryptographic randomness testing of block ciphers and hash functions," *IACR Cryptology ePrint Archive*, 564, 2010.

[18] J. Daemen, and V. Rijmen, "The block cipher Rijndael," in Proceedings of the Third International Conference on smart card Research and Applications, CARDIS'98, 1820, p. 277-284, Berlin: Springer, 2000.