Journal of Advanced Computing and Communication Technologies ***(ISSN:* 2347 - 2804*)***
Volume No. 5, Issue No. 2, April 2017

Security Strength Evaluation of Some Chaos Based Substitution-Boxes

By

Hamed D. AlSharari
College of Engineering, Aljouf University,
Sakaka, Aljouf, Kingdom of Saudi Arabia,
hamed_100@hotmail.com

ABSTRACT

Recently, handful amount of S-boxes, using the various methods such as affine transformations, gray coding, optimization, chaotic systems, etc, have been suggested. It is prudent to use cryptographically strong S-boxes for the design of powerful ciphers. In this paper, we sampled some widely used 8×8 S-boxes which are recently synthesized and security analysis and evaluation is executed to uncover the best candidate(s). The performance analysis is exercised against the crucial measures like nonlinearity, linear approximation probability, algebraic immunity, algebraic complexity, differential uniformity. These parameters are custom selected because their scores decide the security strength against cryptographic assaults like linear cryptanalysis, algebraic attacks, and differential cryptanalysis. The anticipated analysis in this work facilitates the cryptographers, designers, researchers to choose suitable candidate decided over many parameters and can be engaged in modern block encryption systems that solely rely on 8×8 S-box. Moreover, the analysis assists in articulating efficient S-boxes and to evaluate the attacks resistivity of their S-boxes.

General Terms

Security, Block Ciphers, Chaotic maps.

Keywords

Substitution-boxes, Nonlinearity, Linear cryptanalysis, Differential cryptanalysis, Algebraic attacks, Algebraic immunity.

1. INTRODUCTION

The protection of data during transmission through open channels has always been an indispensable part of secure communication and sharing. The data security issues are attracting increasing attention of researchers, scholars, academicians all over the world; this is due to the rapid and vast advancement in network communication and e-business innovation. The strength of data encryption systems binds back to properties of confusion and diffusion coined and explicated by Claude E. Shannon's in his seminal paper published in 1976 [1]. The property of confusion is fundamentally characterized as complicatedness of the liaison between the encryption key and output ciphertext. The diffusion is featured as the extent to which the impact of a bit of plaintext is spread all through the subsequent ciphertext. In developments of symmetric cryptosystems, the Shannon's confusion and diffusion properties are actualized by employing effective nonlinear transformations and mappings. The Substitution-Permutation Network is the famous and prominent architecture which are opted by most of the modern block symmetric systems [2]. The S-P network involves utilization of efficient substitution-boxes during substitution operation in their rounds that improves the substantial level of confusion and nonlinearity as an output of the cryptosystem. Thus, ample research has been dedicated to enhancing the quality and usage productivity of S-boxes in order to restrict cryptanalysis assaults that endeavor imperfect designs.

A cryptographic substitution-box is one-to-one mapping that nonlinearly transforms n-bit input data to m-bit output data. It is also be thought as a multi-input and multi-output Boolean function. Meaning that an 8×8 S-box consists of eight functions where each Boolean function takes 8-bit data as input and generates 1-bit as output, all eight functions collectively yields 8-bit output data. As a result, the performance features and characteristics meant for Boolean functions can be easily considered and extended to quantify the performance of the S-boxes. To date, most of the S-box work carried out is dedicated to the design of 8×8 S-boxes which is due to the success of AES block cipher and its S-box introduced by NIST in 2001 [3, 4]. Almost all of them were balanced and whose design primarily based on the concepts such as affine transformations, gray coding, poor mapping, optimization, chaotic systems, etc. Substitution-boxes are the merely nonlinear component and have a central role to play to decide the security strength of most modern block ciphers. The cryptographic features of S-boxes are of immense significance for the security of cipher systems. In particular, the S-boxes are vulnerable to two kinds of attacks namely, algebraic attack and side channel attack. In the former kind of attacks, the algebraic structure of S-boxes are targeted; while in the latter, the attackers use other measures such as its power consumption, electromagnetic radiation, timing attacks, etc, [5]. Two altogether different cryptanalyses to attack S-boxes have been suggested by Biham et. al. and M. Matsui known as: linear cryptanalysis and differential cryptanalysis [6, 7]. They showed that the S-boxes having low nonlinear nature and high input to output differential uniformity are susceptible to these two kinds of attacks. Therefore, it is prudent for S-boxes to have ample amount of resistivity against these types of attacks in addition of good nonlinearity to thwart linear attacks too. It has been observed in the recent studies that some of these attacks are actually practical on some weak S-boxes. The cryptographically good nature and

strength of these S-boxes is of utmost grandness and need to thwart various attacks.

In this paper, we sampled some widely used S-boxes which are recently synthesized and security analysis and evaluation is executed. The performance measures such as nonlinearity, linear approximation probability, algebraic immunity, algebraic complexity, differential uniformity, and transparency order are quantified to carry out the analysis and study. These measures are associated with linear attacks, algebraic attacks, side-channel attacks, etc. The scores of these measures give the resistivity of the S-box under study against the attacks in some way or the other. The analysis carried out in this paper will help the designers and the researchers to choose suitable 8x8 S-box, which can be employed in modern block encryption algorithms which rely on the S-box. Apart from this, it will also help us in understanding what particular change in the design parameter of the S-boxes will leads to, which will help us in designing new S-boxes. So, it's very important to ensure that the design of the S-box should be robust for a good encryption algorithm. Hence, we analyze the strength and attack resistivity of some popular and recent 8x8 S-boxes. The analysis is focused on the quality of these S-boxes and to find the appropriate candidate for the design of block encryption systems.

The structure of the paper is prepared as follows: Section II describes in brief the different attacks on S-boxes. The security parameters selected for study are discussed in Section III. The strength evaluation of some popular S-boxes is explicated in Section IV. Section V draws the conclusion of the study.

2. ASSAULTS on S-BOXES

A strong encryption system should have considerably high resistivity to make different kind of cryptographic attacks infeasible. Following are the four prominent attacks that are applied by the cryptanalysts to break ciphers based substitution-boxes.

2.1 Linear Attack

As a fact, the substitution-boxes are the main informant of nonlinearity and thereby the confusion in a block ciphers. It is critical to comprehend the extent to which they can be proximated as linear equations [7]. With regards to linear cryptanalysis, for every input variable Xi having n-dimension of an S-box and for every output variable Yi of n-dimension of S-box. These variables Xi and Yi are not particularly independent from each other, because the likelihood of the output relies on upon the input is always exists. The aim of linear cryptanalysis is to discover the linear combination of Xi which is exactly as linear combination of Yi that is fulfilled by finite probability. For a perfect S-P network, such connections will be fulfilled precisely 50% of the ideal opportunity for any choice of Xi and Yi variables [5]. It should estimate and find that there exists some determination of linear combinations such that the chance of fulfilling the relation is not 0.5, if so then this bias from the relationship can be utilized in the attack.

2.2 Algebraic Attacks

The algebraic attacks consist of an intense class of attacks which may undermine block ciphers. The goal is to set up an arithmetic system of conditions and equations that are tested by the key values with an aim to solve them [8]. The purpose behind this is that it guarantees such scenario is of low degree, which is a fundamental for having the capacity to solve them. This raises the key issue of finding out if or not a given function has non-insignificant low degree. The lowest degree for which this happens is known as the algebraic immunity. Hence, it is sufficient for processing the algebraic immunity to probe regardless of whether an S-box has a measure of level of resistance against the algebraic attack. The algebraic complexity is regarded to gauge the susceptibility against such arithmetical assaults.

2.3 Differential Attack

The Differential cryptanalysis is a chosen plaintext attacks that endeavors to discover and misuse certain events of input and output differences and deviations in ciphers that takes place with high probabilities [10]. For a perfect block cipher having an efficient S-box, the likelihood that a specific output difference of $\Delta Y = Yi \oplus Yj$ will happen with an input difference of $\Delta X = Xi \oplus Xj$ is precisely $1/2^n$, where *n* indicates the bits in input X of S-box. The pair (ΔX, ΔY) is termed as a differential. By evaluating the output difference that take place with high probability, the relationship between the plaintext and input can be set up. These relationships are technically termed as differential trails [4]. The attacker can figure the key by counting the quantity of times a specified differential trail holds for a given key.

3. S-BOX PARAMETERS

In this section, the S-box parameters that are carefully selected for security strength evaluation of different substitution-boxes are discussed. The selection involves the parameters of nonlinearity, linear approximation probability, algebraic immunity, algebraic attack, transparency order, and differential uniformity.

3.1 Nonlinearity

An 8×8 S-box consists of eight Boolean functions, each one maps from Galois field $GF(2^8)$ to GF(2). The nonlinearity of an S-box can be evaluated by finding the nonlinearity of all its components functions. For a Boolean function *f(x),* it is accounted as the minimum distance of it to all respective affine functions. The set of affine functions for *f(x)* includes all its functions which are linear and corresponding complements of them. It is mandatory for cryptographically potent S-boxes to have a high nonlinearity score as S-box having poor nonlinearities tend to show weak resistance to linear cryptanalysis and related approximation attacks. The measure nonlinearity NL_f for a function *f(x)* is determined as [11]:

$$NL_f = 2^{n-1}(1 - 2^{-n} \max | S_{\langle f \rangle}(w) |)$$

$$S_{\langle f \rangle}(w) = \sum_{w \in GF(2^n)} (-1)^{f(x) \oplus x.w}$$

Where, $S_{<f>}(w)$ is the Walsh spectrum of *f(x)* and *x.w* denotes the dot-product of x and w. To thwart the linear cryptanalysis, all the Boolean functions of the employed S-box should provide pretty large nonlinearity scores, or the S-box should provide a high score of average nonlinearity.

3.2 LP

The linear probability (LP) is termed as the maximum value of the deviation of an event. The parity of the input bits selected by the mask Γx is equal to the parity of the output bits selected by the mask Γy. A linear probability of probability bias of an S-box is computed as [12]:

$$LAP = \max_{\Gamma x, \Gamma y \neq 0 y} \left(\frac{\#\{x \in X \mid x \bullet \Gamma x = f(x) \bullet \Gamma x\}}{2^n} \right)$$

Where, Γx and Γy are input and output masks, respectively; X is the set of all possible inputs variables; and 2^n is the number of its elements. The maximum linear approximation probability corresponding to an S-box should be as low as possible to not to leakage any information for the attacker that makes the linear cryptanalysis easier and feasible.

3.3 Differential Uniformity

Differential cryptanalysis, originally introduced by Biham and Shamir, is concerned with exploiting of imbalance on the input/output distribution to attack S-boxes. The S-boxes resistance to differential assaults can be done if the eXOR value of an output has equal uniformity with the Exclusive-OR value of the respective input [6]. If the substitution-box is lying in input and output likelihood distribution, the S-box is able to resist the differential cryptanalysis. A strong S-box should hold as low as possible the largest value of differential uniformity (DU). The differential uniformity for a component Boolean function *f(x)* is quantified as:

$$DU_f = \max_{\Delta x \neq 0, \Delta y} \left(\#\{x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\} \right)$$

Where X is the set of all possible input values with 2^n (n = 8 for 8x8 S-box) as the number of its total elements. It also one of the practical attacks that have been successfully utilized to break the DES bock ciphers. The maximum score of the differential uniformity in an 8x8 S-box should be as low enough to resist the differential cryptanalysis and prevailing attack procedure.

3.4 Algebraic Immunity

The algebraic immunity of an S-box is a measure of the complexity of general algebraic attacks. It depends on the count and kind of linearly independent multivariate equations it satisfies [13]. The AI of a Boolean function f is the minimum value of d such that f or $f + 1$ admits a function g of degree d such that $f \times g = 0$ [14]. Algebraic immunity is aspired to evaluate Boolean resistive strengths to attacks that takes into account the annihilators, which are used to deduce a multivariate equation in the output of the function that have a sufficiently low degree to solve them proficiently. Utilizing low-degree annihilators, it is conceivable to diminish the level of a Boolean function in system of multivariate conditions to a small enough value such that the system of equations relating the Boolean function and state bits of a cryptosystem can be solved in a reasonable amount of time [5]. The AI metrics denotes the resistance of an S-box, used in block ciphers, against the algebraic attacks and inversely the effectiveness of the XSL attack on a particular S-box. The procedure of computing the algebraic immunity is explained in [13]. A high score of algebraic immunity is desired to complicate the algebraic attacks on S-box. Meaning, an S-Box having high algebraic immunity will be better.

3.5 Algebraic Complexity

Algebraic complexity is counted as the number of terms appearing in the algebraic expression of an S-box. Algebraic expression can be calculated using Lagrange interpolation of an S-box, but it has to be done in Galois field GF(2^8). The algebraic complexity of an S-box is the number of non-zero coefficients of terms in the corresponding linearized polynomial. Daemen and Rijmen pointed out that a function in finite galois field onto itself is expressible as a linear polynomial [3]. In fact, given a tabular form of the function, it is possible to generate the Lagrange polynomial and then simplify to have algebraic expression. AES and similar S-boxes S-boxes are based of power (inverse) mappings of the form x^d for exponents d. In case of AES proposal, Fermat's Little Theorem provides that d = 254 = -1 in galois field GF(2^8) [15]. The power mapping used in AES S-box is followed by the affine transformation. The algebraic complexity for AES S-box is just 9. The researchers consider that this score is too low and may render varieties of interpolation attacks fertile [16]. As such, there has been ample work carried out to improve the algebraic complexity to higher values. The method to apply Lagrangian interpolation to find algebraic complexity of an S-box is detailed in [17].

In this study, a number of recent 8x8 S-boxes have been collected, the selected set has S-boxes that are designed by employing different concepts and primitives such as power mapping techniques, affine transformation, number theoretic approaches, chaos, etc and investigated in [20-29]. Most of them are popular that have been extensively cited and referred in the literature for S-boxes synthesis and study. These S-boxes are analyzed and assessed against the following performance measures pertinent to the strength of S-boxes. The performance measures include average nonlinearity NL (denotes the mean of nonlinearity scores of all 8 Boolean functions inherent to the S-box under consideration, higher score is appreciated), linear approximation probability (maximum value is reported for the analysis, it is preferable to have the maximum score of LAP as low as possible), algebraic immunity AI and algebraic complexity AC (an S-box should have high scores of algebraic immunity and algebraic complexity as well), and differential uniformity (lower score of maximum values of DU is appraised). The scores of security parameters for selected 8x8 substitution-boxes are carefully computed by using their refereed algorithms and procedures available in the literature are listed conjointly in Table I. The comparison study has the findings which are discussed subsequently.

It is evident from the study that the algebraic immunity alone cannot be considered as a good parameter for commenting on the resistivity against the algebraic attacks. For that matter, the algebraic complexity has a significance as well to compare S-boxes over resistivity to algebraic attacks. There exists some sort of direct relationship between the non-linearity and transparency order.

The study unveils that the S-box in Ref. [29] tend to show excellent nonlinearity scores of 112 along with lowest achievable LAP of 16/256 = 0.0625 for 8x8 S-boxes. Thereby, it can be claimed that these three S-boxes has the ability to resist the linear cryptanalysis as they provide sufficiently enough nonlinearity structure to the block ciphers. In this regard, the S-box in Ref. [34] offers lowest nonlinearity score of 99.5 and S-box in Ref. [36] shows the poorest LAP score of 160/256 = 0.625 among all S-boxes in the set.

As far as analysis against the differential cryptanalysis is concern, the performance through differential uniformity is portrayed in Table 1. Again, the S-box in Ref. [29] has DU = 4, thereby offers splendid resistance to the differential cryptanalysis. However, the S08 and S09 failed to provide sufficient susceptibility unlike the other S-boxes of the set. The resistivity of S-boxes under consideration have somewhat similar tendency to handle the algebraic attacks. Almost all S-boxes (except in Ref. [33] for AI and S01 for AC) provide decent potentiality against algebraic attacks. Deciding over all performance measures, the S-boxes in decreasing order in

Ref. [29] → in Ref. [30] tends to exhibits the best features and appeared as best among the others of the set. However, depending upon the use cases we can choose one of the S-box from our observations, for instance if we are shipping a hardware which uses algorithms like AES for encryption. Similarly, if we are to use AES implementation on the software, where there is no possibility of SCA attacks, it will be better to choose S-boxes which are resilient toward algebraic attacks. But in all cases, we must try to make sure that the S-box chosen always satisfies basic properties up to higher extend as possible.

TABLE I. COMPARISON OF SECURITY STRENGTHS OF SOME 8×8 S-BOXES

S-Box	NL	LP	AI	AC	DU
Ref. [29]	112	0.0625	4	255	4
Ref. [30]	108	0.1406	4	255	10
Ref. [31]	103.75	0.0625	4	255	10
Ref. [32]	102.75	0.1328	4	254	12
Ref. [33]	104	0.1250	3	253	32
Ref. [34]	99.5	0.1328	4	254	72
Ref. [35]	104	0.1328	4	253	64
Ref. [36]	105.25	0.6250	4	255	10
Ref. [37]	107	0.1484	4	255	10
Ref. [38]	105.25	0.1328	4	254	10
Ref. [39]	100	0.1796	3	253	16

As a future work, there is a great scope of research in finding an optimal S-box particular for higher input-output bits. For instances, considering an 8x8 S-box, mathematically 256! different bijective S-boxes are possible. It is computationally infeasible to evaluate all such possibilities and finding out the optimal S-box(es) out of the total 256! cases. So, it raises a direction for finding optimal or sub-optimal S-boxes, if one can develop an approach which decides the optimal S-box by giving some weightage to each of the properties. This will be certainly beneficial for picking up the optimal S-box when we could develop S-boxes dynamically.

4. CONCLUSION

In this communication, the security strength evaluation of some widely used 8×8 S-boxes which are recently synthesized is studied to uncover the optimal candidate(s). The strength comparison is done through measures like nonlinearity, linear approximation probability, algebraic immunity, algebraic complexity, and differential uniformity. These parameters are directly or indirectly decide the security strength of S-boxes against cryptographic assaults like linear cryptanalysis, algebraic attacks, and differential cryptanalysis. The analysis highlighted few practical findings and suggested optimal/sub-optimal S-box(es) based on the study. The anticipated analysis in this work facilitates the cryptographers, designers, researchers to choose suitable S-boxes decided over many parameters that can be applied in modern block encryption systems for desired confusion and diffusion of plaintext data.

5. REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems", Bell Systems Technical Journal, vol. 28, no. 4, pp. 656-715, 1949.

[2] M. Ahmad, S. Alam, "A Novel Approach for Efficient S-Box Design Using Multiple High-Dimensional Chaos." International Conference on Advanced Computing & Communication Technologies, pp. 95-99, 2014.

[3] Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[4] J. Daemen, V. Rijmen, The design of Rijndael: AES – the Advanced Encryption Standard, Information Security and Cryptography, Springer, 2002.

[5] C. A. Wood, "Large Substitution Boxes with Efficient Combinational Implementations", M.S. Thesis, Rochester Institute of Technology, 2013.

[6] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology, vol 4, no. 1, pp. 3-72, 1991.

[7] M. Matsui, "Linear Cryptanalysis Method of DES Cipher", Advances in Cryptology: EuroCrypt-1993 Proceedings, Lecture Notes in Computer Science, vol. 765, pp. 386-397, 1994.

[8] J.H. Cheon, D. H. Lee, "Resistance of S-Boxes against Algebraic Attacks", Lecture Notes in Computer Science vol. 3017, pp. 83–93, 2004.

[9] K. P. Stjepan, "Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes", INDOCRYPT-2014, Lecture Notes in Computer Science, vol. 8885, pp 374-390, 2014.

[10] D. R. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC, 2005.

[11] T. Cusick, P. Stanica, Cryptographic boolean functions and applications, Elsevier, 2009.

[12] F. Özkaynak, A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system", Physics Letters A, vol. 374,no. 36, pp. 3733–3738, 2010.

[13] F. Didier, J.P. Tillich, "Computing the algebraic immunity efficiently", International Workshop on Fast Software Encryption, Lecture Notes in Computer Science, vol. 4047, pp. 359-374, 2006.

[14] F. Armknecht, C. Claude, G. Philippe, K. Simon, M. Willi. R. Olivier, "Efficient computation of algebraic immunity for algebraic and fast algebraic attacks", Advances in Cryptology – EUROCRYPT-2006, Lecture Notes in Computer Science, vol. 4004, pp. 147-164, 2006.

[15] J. Liu, B. Wai, X. Cheng, X. Wang, "An AES S-box to increase complexity and cryptographic analysis", 19th International Conference on Advanced Information Networking and Applications, vol. 1, pp. 724–728, 2005.

[16] J. Cui, L. Huang, H. Zhong, C. Chang, W. Yang, "An improved AES S-Box and its performance analysis", International Journal of Innovative Computing, Information and Control, vol. 7, no. 5, pp. 2291-2302, 2011.

[17] C. Cid, S. Murphy, M. Robshaw, "Computational and algebraic aspects of the advanced encryption standard", Seventh International Workshop on Computer Algebra in Scientific Computing, vol. 2004, pp. 1-11, 2004.

[18] E. Prou, "DPA Attacks and S-Boxes", Proceedings of FSE-2005, Lecture Notes in Computer Science, vol. 3557, pp 424-441, 2005.

[19] M. Ahmad, "Cryptanalysis of chaos based secure satellite imagery cryptosystem", In International Conference on Contemporary Computing, pp. 81-91, 2011.

[20] P.K. Sharma, M. Ahmad and P.M. Khan, "Cryptanalysis of image encryption algorithm based on pixel shuffling and chaotic S-box transformation", International Symposium on Security in Computing and Communication, pp. 173-181, 2014.

[21] O.P. Verma, M. Nizam and M. Ahmad, "Modified multi-chaotic systems that are based on pixel shuffle for image encryption", Journal of Information Processing Systems, vol. 9, no. 2, pp. 271-286, 2013.

[22] M. Ahmad, P.M. Khan, and M.Z. Ansari, "A simple and efficient key-dependent S-box design using fisher-yates shuffle technique,", International Conference on Security in Computer Networks and Distributed Systems, pp. 540-550, 2014.

[23] M. Ahmad, N. Mittal, P. Garg and M.M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos", Perspectives in Science, vol. 8, pp. 465-468, 2016.

[24] M. Ahmad and M. Malik, "Design of chaotic neural network based method for cryptographic substitution box", International Conference on Electrical, Electronics, and Optimization Techniques, pp. 864-868, 2016.

[25] M. Ahmad, Hitesh Chugh, Avish Goel, and Prateek Singla, "A chaos based method for efficient cryptographic S-box design." In International Symposium on Security in Computing and Communication, pp. 130-137. Springer Berlin Heidelberg, 2013.

[26] M. Ahmad, F. Ahmad, Z. Nasim, Z. Bano and S. Zafar, "Designing chaos based strong substitution box." International Conference on Contemporary Computing, pp. 97-100, 2015.

[27] M. Ahmad, D.R. Rizvi and Z. Ahmad, "PWLCM-Based Random Search for Strong Substitution-Box Design", International Conference on Computer and Communication Technologies, pp. 471-478. 2016.

[28] L. Cui, Y. Cao, "A new S-box structure named Affine-Power-Affine", International Journal of Innovative Computing, Information and Control, vol. 3, no. 3, pp. 751-759, 2007.

[29] M.T. Tran, D.K. Bui, A.D. Duong, "Gray S-box for advanced encryption standard", International Conference on Computational Intelligence and Security, vol. 1, pp. 253-258, 2008.

[30] Y. Wang, K.K. Wong, C. Li, Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm", Physics Letters A, vol. 376, no. 6, pp. 827-833, 2012.

[31] M. Dara, K. Manochehri, "A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key", World Applied Sciences Journal, vol. 28, no. 12, pp. 2003-2009, 2013.

[32] Peng, Jun, et al. "A Novel Method for Designing Dynamical Key-Dependent S-Boxes based on Hyperchaotic System." International Journal of Advancements in Computing Technology, vol. 28, no. 12, pp. 2003-2009, 2013.

[33] I. Hussain, T. Shah, M.A. Gondal, W.A. Khan, "Construction of cryptographically strong 8× 8 S-boxes", World Applied Sciences Journal vol. 13, no. 11, pp. 2389-2395, 2011.

[34] E.S. Abuelyman, A.A.S. Alsehibani, "An optimized implementation of the S-Box using residue of prime numbers", International Journal of Computer Science and Network Security, vol. 8, no. 4, pp. 304-309, 2008.

[35] I. Hussain, T. Shah, M.A. Gondal, M. Khan, W.A. Khan, "Construction of new S-box using a linear fractional transformation." World Applied Science Journal, vol. 14, no. 12, pp. 1779-1785, 2011.

[36] A. H. Alkhaldi, I. Hussain, M.A. Gondal, "A novel design for the construction of safe S-boxes based on TDERC sequence", Alexandria Engineering Journal, vol. 54, no. 1, pp. 65-69, 2015.

[37] M. Ahmad, D. Bhatia, Y. Hassan. "A Novel Ant Colony Optimization Based Scheme for Substitution Box Design", Procedia Computer Science, vol. 57, pp. 572-580, 2015.

[38] M. Ahmad, H. Haleem, P. M. Khan. "A new chaotic substitution box design for block ciphers." International Conference on Signal Processing and Integrated Networks, pp. 255-258, 2014.

[39] M. Khan, T. Shah and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption", Neural Computation and Applications, vol 27, no. 3, pp. 677-685, 2016.