Proceedings of the 33rd International Conference on Information Technologies (InfoTech-2019)
19-20 September 2019, Bulgaria

NEW HYBRID AES S-BOX ALGORITHM USING CHAOTIC MAPS

***Digest of paper*[1]**

Amira S. El Batouty, Hania H. Farag, Mohamed-Amr A. Mokhtar, and El-Sayed A-M. El-Badawy

Department of Electronics, Faculty of Electronic Engineering
University of Alexandria
amislh@yahoo.com, hania11@yahoo.com, amromokhtar61@gmail.com, sbadawy@ieee.org
Egypt

Abstract: Methods of security need to be improved to face new techniques of data stealing. The substitution table is the core of the block ciphers encryption and its good design increases the encryption algorithm security. This paper proposes two algorithms to generate modified S-Boxes; the key and plaintext dependent S-Box using RC4 algorithm and using RC4 chaotic algorithm. This paper aims to demonstrate the efficiency of the proposed S-Boxes compared to the existing AES and Dynamic S-Boxes.
Key words: Encryption, Henon chaotic map RC4, S-Box, security**.**

1. INTRODUCTION

Cryptography is one of the most important fields of information and data security. The Substitution Box (S-Box) is the only nonlinear component assuring the confusion property of the conventional block ciphers such as the Advanced Encryption Standard (AES). The strength of this algorithm depends on a design of strong S-Box. In this paper we propose two new methods to generate S-Boxes: key and plain dependent S-Box using RC4 algorithm and using RC4 algorithm, and key and plain dependent S-Box using RC4 chaotic algorithm.

2. S-BOXES

AES S-Box is constructed as follows:
(1) Initialize the S-Box with the byte values in ascending order row by row.

[1] The full paper is proposed for including in the IEEE Xplore Digital Library

(2) Map each byte in the S-Box to its multiplicative inverse in the finite field GF (2^8).

(3) Apply the affine transformation to each bit of each byte in the S-Box.

The **Dynamic S-Box** is a key dependent S-Box [12] which depends on RC4 key scheduling algorithm [6].

3. RC4

RC4, is a kind of stream cipher based on nonlinear data table changes, often used in real-time communications. The RC4 Algorithm contains two parts: Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA).

4. THE PROPOSED S-BOXES

4.1. The key and plaintext dependent S-Box using RC4 algorithm. The proposed method uses the two main parts of the RC4 encryption algorithm to generate a strong S-Box, and then performs the affine transformation of the produced value.

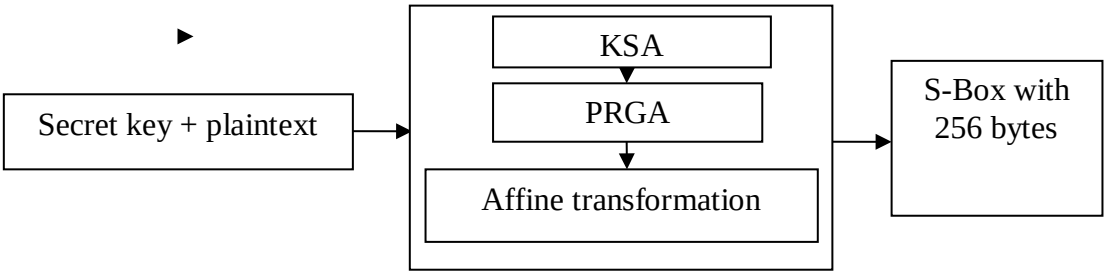

Fig 1 Block diagram for the key and plaintext dependent S-Box using RC4 algorithm

4.2. The key and plaintext dependent S-Box using RC4 Chaotic algorithm. In [8], RC4 encryption was implemented using Henon chaotic map to decrease time consumption. Henon map [14] has go.

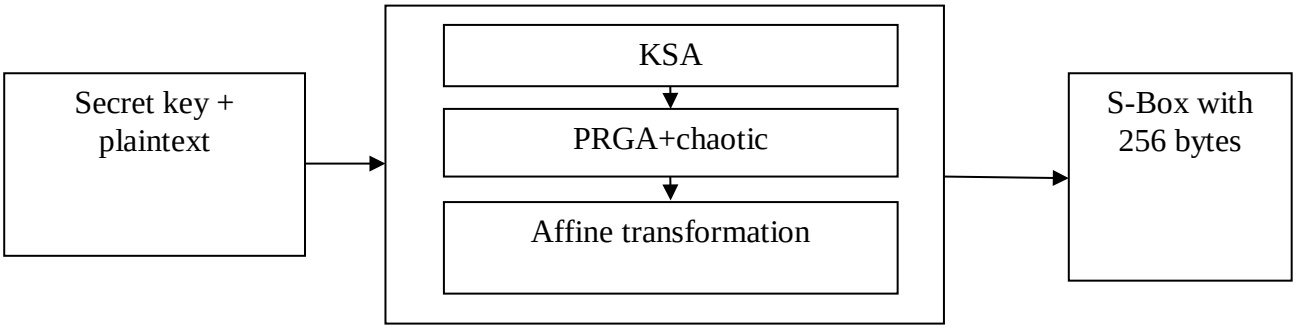

Fig. 2 Block diagram for the key and plaintext dependent S-Box using RC4 chaotic algorithm

5. SECURITY ANALYSES

5.1. Nonlinearity. Nonlinearity means that the probability of the numbers of bits inverted from the input to the output is 0.5 [15].

5.2. Strict Avalanche Criterion. An S-Box is said to satisfy SAC, if when one input bit of the S-Box changes, it changes each output bit with probability of one half. Three analysis methods for strict avalanche criteria (SAC) are used for testing

1) Analysis of the frequency of various Hamming weights (Avalanche effect);

2) Analysis of the frequency of various differential values ΔY (completeness);

3) Analysis of Hamming weights according to the bit position (Strong S-Box).

6. RESULTS

he simulations were achieved by using C++ program with 200 trails number with key T = "0123456789ABCDEF", and plain text = {00,11,22,33,44,55,66,77,88,99, AA,BB,CC,DD,EE,FF}.

6.1 The results of three tests of SAC

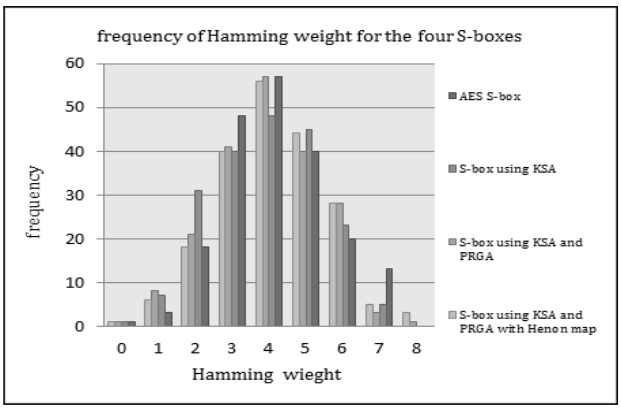

Fig. 3 Frequency of Hamming weight for the four S-Boxes

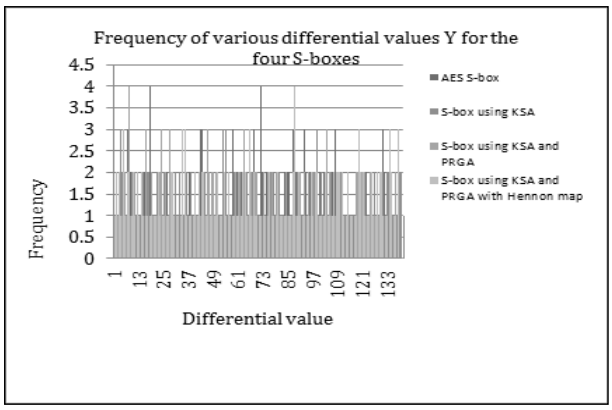

Fig. 4 Frequency of various differential values ΔY for the four S-Boxes

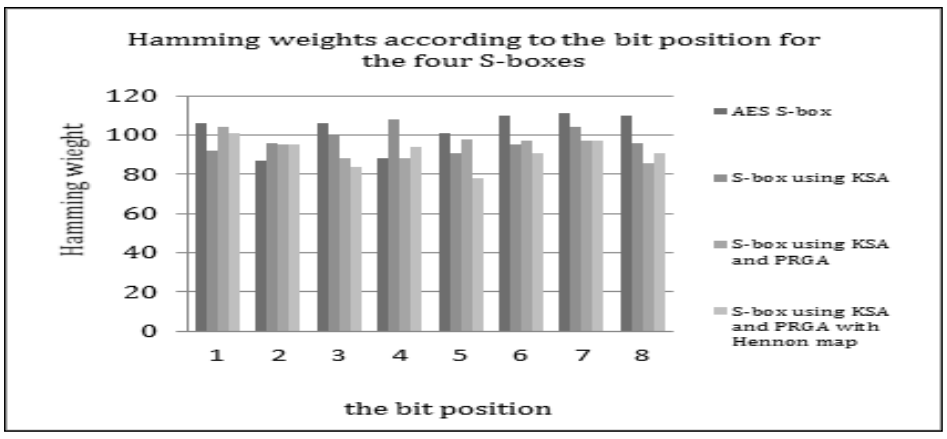

Fig. 5 Hamming weights according to the bit position for the four S-Boxes

6.2. Nonlinearity

Table 1 the nonlinearity for the four S-boxes

	AES S-Box	*Dynamic S-Box*	*KSA and PRGA S-Box*	*KSA and PRGA with Henon chaotic map S-Box*
Nonlinearity	*0.515*	*0. 486*	*0.492*	*0.52*

7. CONCLUSIONS

The security of any symmetric algorithm depends on the security its S-Box. This paper proposes two methods to generate new secured S-Boxes. The results show that the key and plaintext dependent S-Box using RC4 chaotic algorithm generates the best S-Box because it depends on affine transformation to ensure confusion and diffusion and depends on Henon chaotic map to ensure the complexity and ergodicity.

REFERENCES

[1] W. Stallings. *Cryptography and Network Security*. Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2009

[2] C. Shannon. *Communication Theory of Secrecy Systems.* Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64, 1998.

[3] A. F Webster and S .E. Travares. *On The Design of S-Boxes.* Queen's University. Kingston, Springer-verlag ,Canada 1998 .

[4] The Mathworks: Galois Field Computations. ttp://www.mathworks-.com/Access/help-desk/help /toolBox/comm./tutor3.shtml, Communications ToolBox, 2001.

[5] F. Fahmy and G. Salama. *A proposal for Key-dependant AES.* 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SETIT), TUNISIA March 2005.

[6] I. Abd-ElGhafar, A. Rohiem, A. Diaa, F. Mohammed. *Generation of AES Key Dependent S-Boxes using RC4 Algorithm.* 13th international conference on AEROSPACE SCIENCES & AVIATION TECHNOLOGY, ASAT-13,May 26-28,2009 .

[7] Razi Hosseinkhani & H. Haj Seyyed Javadi. *Using Cipher Key to Generate Dynamic S-Box in AES Cipher System.* international journal of computer science and security(IJCSS),volume (6):issue(1):2012.

[8] Yuan MEI, Yonghe JIANG. *Secure RFID System Based on RC4 Chaotic Algorithm*. Journal of Computational Information Systems 9: 5 (2013) 2083–2091

[9] Brian Whitley. *Implementing the RC4 Algorithm*. Computer Science 3 - CSI 3050 Term Paper,April 2004.

[10] Bhavana Agrawal, Himani Agrawal. *Implementation of AES and RSA Using Chaos System.* International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 ISSN 2229-5518.

[11] Phyu Phyu Mar, Khin Maung Latt. *New Analysis Methods on Strict Avalanche Criterion of SBoxes.* World Academy of Science, Engineering and Technology International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering Vol:2, No:12, 2008.

[12] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS. *Key-Dependent S-Box Generation in AES Block Cipher System.* INFORMATICA, 2009, Institute of Mathematics and Informatics, Vilnius Vol. 20, No. 1, 23–34 23 2009.

[13] Balajee Maram K , J M Gnanasekar. *Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output.* TEM J. 2016; 5:67–75.

[14] Haoran Wen, *A review of the H´enon map and its physical interpretations.* School of Physics Georgia Institute of Technology, Atlanta, GA 30332-0430, U.S.A (Dated: April 21, 2014).

[15] Pedro Miguel Sosa. *Calculating Nonlinearity of Boolean Functions with Walsh-Hadamard Transform.* UCSB, Santa Barbara, CA – USA April 23, 2016.