NEW HYBRID AES S-BOX ALGORITHM USING
CHAOTIC MAPS

Digest of paper

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 chaotic 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.
(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](image1)

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](image2)

**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 $\Delta Y$ (completeness);
3) Analysis of Hamming weights according to the bit position (Strong S-Box).

6. **RESULTS**

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

6.1 **The results of three tests of SAC**

![Plot of Hamming weight frequency for the four S-Boxes](image1)

![Plot of various differential values $\Delta Y$ for the four S-Boxes](image2)

![Plot of Hamming weights according to the bit position for the four S-Boxes](image3)

6.2. **Nonlinearity**

<table>
<thead>
<tr>
<th>AES S-Box</th>
<th>Dynamic S-Box</th>
<th>KSA and PRGA S-Box</th>
<th>KSA and PRGA with Henon chaotic map S-Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonlinearity</td>
<td>0.515</td>
<td>0.486</td>
<td>0.492</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.52</td>
</tr>
</tbody>
</table>
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