AES S-Box Construction using One Dimensional Cellular Automata Rules

K. J. Jegadish Kumar
Assistant Professor, SSN College of Engineering, Kalavakkam, Tamil Nadu, India;

V. Karthick
PG Scholar, SSN College of Engineering, Kalavakkam, Tamil Nadu, India;

ABSTRACT
S-Box is the only non-linear component in Advanced Encryption Standard(AES) which determine its strength. The Look-Up Table based S-Box of conventional AES occupies large storage space, reduced throughput and consumes more power. This article presents the design of an S-Box based on Reversible Cellular Automata function that reduces the implementation cost. Further, Cellular Automata functions are derived from various rules that are non-linear and S-Box properties are discussed briefly in this paper. With this approach, the time consumption for the AES S-Box is considerably decreased without compromising the non-linearity of conventional S-Box.

Keywords
AES, Substitution Box (S-Box), Cellular Automata(CA), One Dimensional(1-D) CA.

1. INTRODUCTION
Cryptography plays an important role in securing data transmission against various attacks. In 2001,the National Institute of Standards and Technology(NIST) established a symmetric key encryption algorithm called AES to provide higher security than Data Encryption Standard(DES).The security level of any encryption algorithm relies on the key size. Hence AES, that operates on variant key sizes of 128, 192, 256 bits is said to be more secure than DES having the key size of 56 bits. The AES is an iterative algorithm composed of a number of rounds 10, 12, 14 depending on the key size of 128, 192, and 256 respectively. A round consists of four stages named SubByte, ShiftRow, MixColumn and AddRoundKey. However, the final round is constituted withstages as previous rounds except the MixColumn [1].

The Substitution Box(S-Box) is the core part in AES algorithm that defines the non-linearity of the entire algorithm. This S-box is created based on finite field arithmetic operation which involves multiplicative inverse and affine transformation. The conventional S-Box used in AES is LUT based that need large memory storage and consumes more power [2]. Hence, the implementation cost will be more when using the conventional LUT based S-Box. To overcome the setback in the LUT based design, the Cellular Automata based S-Box design for AES is proposed.

The Cellular Automata is a collection of cells on a grid that changes its state through a number of discrete time steps according to a set of rules based on the states of neighboring cells. The state of current cell and its neighboring cells combined called as neighborhood states. Neighborhood radius r is defined as the number of neighbor cells to either side of the central cell. Neighborhood state l is defined as $l = 2r + 1$. For one-dimensional (1-D) CA, when the radius r=1 then the neighborhood state $l = 3$.Then, the total number of neighborhood states $K = 2^l$ and the number of rules is $R = 2^k$ (when k =8, R = 256) [3].

Reversible Cellular Automata (RCA) is defined as the high order CA in which the future (C_x^{t+1}) states of the grid of cells (C_x) are calculated using the present (C_x^t) and past (C_x^{t-1}) configuration of the cells. Generally, second order CA is used to construct local transition rule function. A second order local transition rule function is defined in equation (1) as

$$C_x^{t+1} = f(C_x^t, C_x^{t-1}) \quad (1)$$

2. RELATED WORKS
Satohet al. proposed a compact hardware architecture of AES S-Box with the introduction of a new composite field of GF($((2^2)^2)^2$). The author claimed that the efficient throughput of the algorithm can be boosted using the parallel feature of Substitution Permutation Network(SPN) [4]. Rohiem et al. proposed a new S-Box for AES Using Chaotic Map. The author presented a Couple Chaotic System based Pseudo Random Bit Generator(CCS-PRBG) and the output sequences are tested using NIST tests for randomness to ensure cryptographic property. The chaotic key dependent S-Box satisfies the Strict Avalanche Criterion (SAC) [5].Sakamura et al. proposed a work for the study of linear cryptanalysis on AES cipher and proved that linear cryptanalysis method on AES getting failed after three rounds [6]. Farhadian et al. proposed a new efficient method to cryptanalysis the S-Boxes. In this paper RBO(Reducing By Order) method was introduced to produce a systematic and efficient technique to simplify and approximate the S-Boxes based on the power and inversion function [7].

3. S-BOX DESIGN
S-Box is the basic component of a cipher system. It Substitutes a given value of the input into another value as output. It can have the different number of inputs and outputs (m-bit input word and n-bit output word) [8].

There are two different types of design approaches:

1. Look Up Table (LUT) based

   In the LUT based design, fixed table are normally used in which for each value of ‘m’ bit word an alternate value of ‘n’ bit word is pre-defined. (Ex: S-Boxes in AES, DES).

2. Function-based

   In the function-based design, the functions are defined such that

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

3.1Proposed RCA based S-Box

The proposed S-Box design is based on Reversible Cellular Automata (RCA) function [9]. The RCA based S-Box is constructed in the following way,

- Generate a constant matrix with the initial constant value as $\{63\}_H$.
- Then apply the RCA function based on the rule to the constant matrix and the state matrix (input to the S-Box).

The proposed approach is depicted in matrix form as in equation (2):

$$\begin{pmatrix} n_{0,0} & n_{0,1} & n_{0,2} & n_{0,3} \\ n_{1,0} & n_{1,1} & n_{1,2} & n_{1,3} \\ n_{2,0} & n_{2,1} & n_{2,2} & n_{2,3} \\ n_{3,0} & n_{3,1} & n_{3,2} & n_{3,3} \end{pmatrix} = f \left(\begin{bmatrix} m_{0,0} & m_{0,1} & m_{0,2} & m_{0,3} \\ m_{1,0} & m_{1,1} & m_{1,2} & m_{1,3} \\ m_{2,0} & m_{2,1} & m_{2,2} & m_{2,3} \\ m_{3,0} & m_{3,1} & m_{3,2} & m_{3,3} \end{bmatrix}, \begin{bmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{bmatrix} \right) \quad (2)$$

where $\hat{m}$ - Input state matrix to S-Box with values in Hexadecimal

$\hat{n}$ - Output state matrix of S-Box with values in Hexadecimal

$\hat{c}$ - Constant matrix in Hex with values in Hexadecimal

f - RCA function

The RCA function for Rule-30, Rule-45, and Rule-229 is mathematically defined as in equations (3), (4) and (5).

$$n_i(t) = [c_i(t) \vee c_{i+1}(t) \oplus c_{i-1}(t)] \oplus m_i(t) \quad (3)$$

$$n_i(t) = [c_i(t) \bullet c_{i+1}(t) \oplus c_{i-1}(t) \oplus c_{i+1}(t) \oplus 1] \oplus m_i(t) \quad (4)$$

$$n_i(t) = [c_{i-1}(t) \bullet c_i(t) \bullet c_{i+1}(t) \oplus c_{i-1}(t) \bullet c_i(t) \oplus c_{i-1}(t) \oplus c_{i+1}(t) \oplus 1] \oplus m_i(t) \quad (5)$$

where the symbols $\bullet, \vee, \oplus$ represents AND,OR,XOR operation respectively.

3.1.1 Algorithm to construct the constant matrix

Step 1: Consider the initial constant value as $\{63\}_H$.

Step 2: Apply one bit cyclic left shift to the initial constant.

Step 3:Store the resulting constant in column wise and again apply the cyclic left shift to the new constant.

Step 4:Repeat step 1 to step 3 until the 4×4 constant matrix is generated.

The resultant constant matrix generated is given below

$$\begin{bmatrix} 63 & 36 & 63 & 36 \\ C6 & 6C & C6 & 6C \\ 8D & D8 & 8D & D8 \\ 1B & B1 & 1B & B1 \end{bmatrix}$$

3.2 Cryptographic Properties

The robustness of a cryptographic system depends on its underlying elements. Boolean functions are the most widely used element in various cryptographic systems. The balancedness, non-linearity, algebraic degree, correlation immunity, randomness are the cryptographic properties that are analyzed to determine cryptographically strong update rule functions in 1-D Cellular Automata.

3.2.1 Balancedness

An n-variable Boolean function f is balanced if the hamming weight of the function's binary truth table is equal to 2^{n-1}. In other words, the function is said to be balanced if 0's and 1's are evenly distributed in its binary truth table [10].

3.2.2 Non-linearity

The non-linearity(N_f) of a function f is the minimum of the hamming distances(H_d) between f and any affine function (l) as given in equation (6):

$$N_f = \min\{H_d(f,l)\} \quad (6)$$

The non-linearity of an affine function is zero, and the non-linearity of balanced Boolean functions must be below the upper bound [10]as given in equation (7):

$$N_f \leq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} - 2, & n \text{ is even} \\ \left\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \right\rfloor, & n \text{ is odd} \end{cases} \quad (7)$$

3.2.3 Algebraic Degree

The number of variables in the highest product term with non-zero coefficients is the algebraic degree. To measure the degree of a function, first represent it in its Algebraic Normal Form (ANF). The ANF of a Boolean function is the XOR sum of some selected input bits. Thus, strong cryptosystem relies on

the function with higher algebraic degree [11]. For an example, consider the function $f = x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_3 \oplus 1$, the algebraic degree is 3.

3.2.4 Correlation Immunity

The correlation Immunity of a Boolean function is a measure of the degree to which its outputs are uncorrelated with some subset of its inputs. Specifically, a Boolean function is said to be correlation-immune of order m if every subset of m or fewer variables in $x_1, x_2, \ldots x_n$ is statistically independent of the value of $f(x_1, x_2, \ldots, x_n)$.

A function $f : F_2^n \rightarrow F_2$ is k-th order correlation immune if for any independent n binary random variables $X_0 ..... X_{n-1}$, the random variable $Z = f(X_0, ..., X_{n-1})$ is independent from any random vector $(X_{i_{11}}, ..., X_{i_{1k}})$ with $0 \leq i_1 < .... < i_k < n$. In cryptography, a Boolean function with low order correlation immunity is more susceptible to a correlation attack than a function with correlation immunity of high order [12].

4. EXPERIMENTAL ANALYSIS

The conventional AES S-Box and proposed RCA based S-Box design is coded in MATLAB R2014a software and simulated using commercial computer system. The specification of the system used is Intel® Core ™ i5- 3470 @ 3.2 GHz, installed memory of 4.00 GB RAM and 64-bit Microsoft windows OS for the experimental analysis. The balancedness, non-linearity, correlation immunity properties of the proposed S-Box is analyzed and compared with the existing S-Box. Eight sample test vectors of 128-Bit are taken for the experimental analysis.

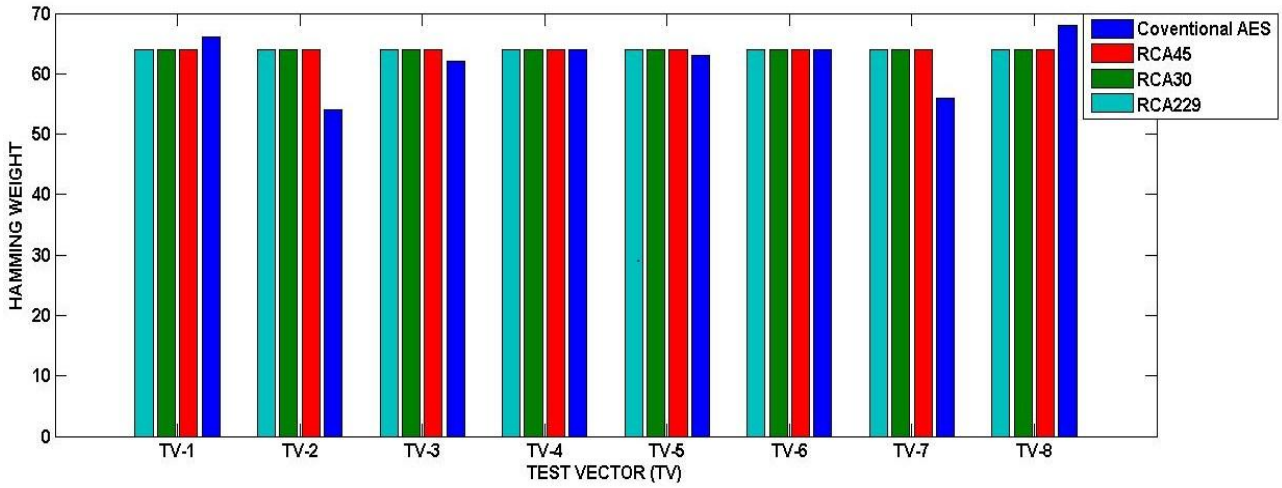

Figure 1: Balanced property analysis

The rule-based S-Box is more balanced than the LUT based S-Box. In figure1, the balancedness test on both the S-Boxes is analyzed by evaluating the hamming weight of the conventional LUT based S-Box for the input test vector {00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F}$_H$. The evaluated value is $\{66\}_d$ for the conventional AES S-Box while, for RCA rule-30, RCA rule-45 and RCA rule-229 based S-Box is $\{64\}_d$. It is observed from the table 1 and 2 that the balancedness in terms of hamming weight for the conventional S-Box is varied depending on the input test vectors. On the other hand, the RCA based S-Box gives the constant hamming weight of$\{64\}_d$ for all the input test vectors.

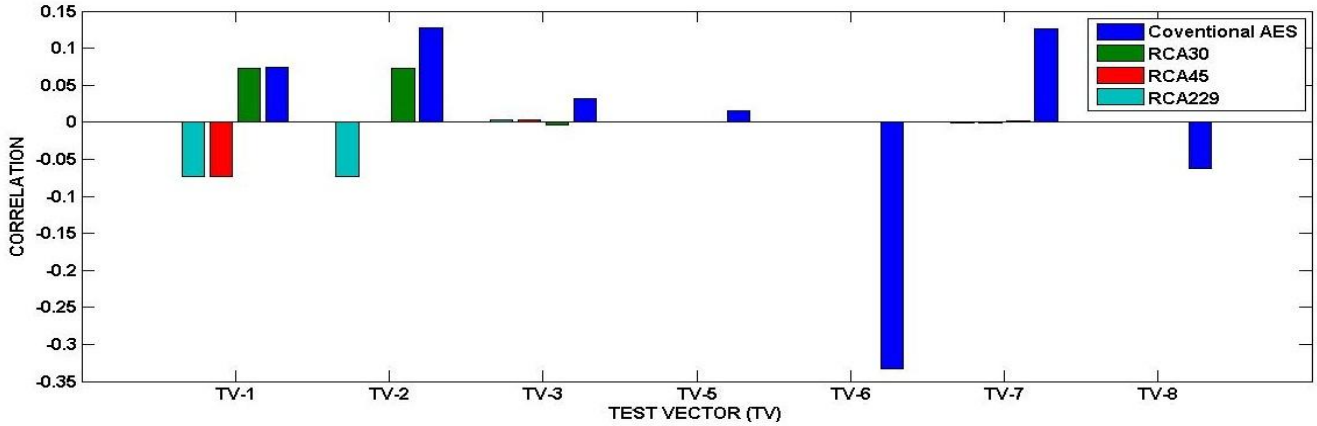

Figure 2: Correlation Immunity analysis

The correlation immunity of the conventional LUT based S-Box and RCA rule-based S-Box is calculated for various input test vector is shown figure 2. As an example, for the input test vector of 128-bit {01 12 23 34 45 56 67 78 89 9A AB BC CD DE EF F0}$_H$, the evaluated correlation value for conventional AES S-Box is 0.0156, while for RCA rule-30, RCA rule-45, RCA rule-229 based S-Box is 0. Hence, the correlation between the input and output of this RCA rule-based approach reaches more or less zero.

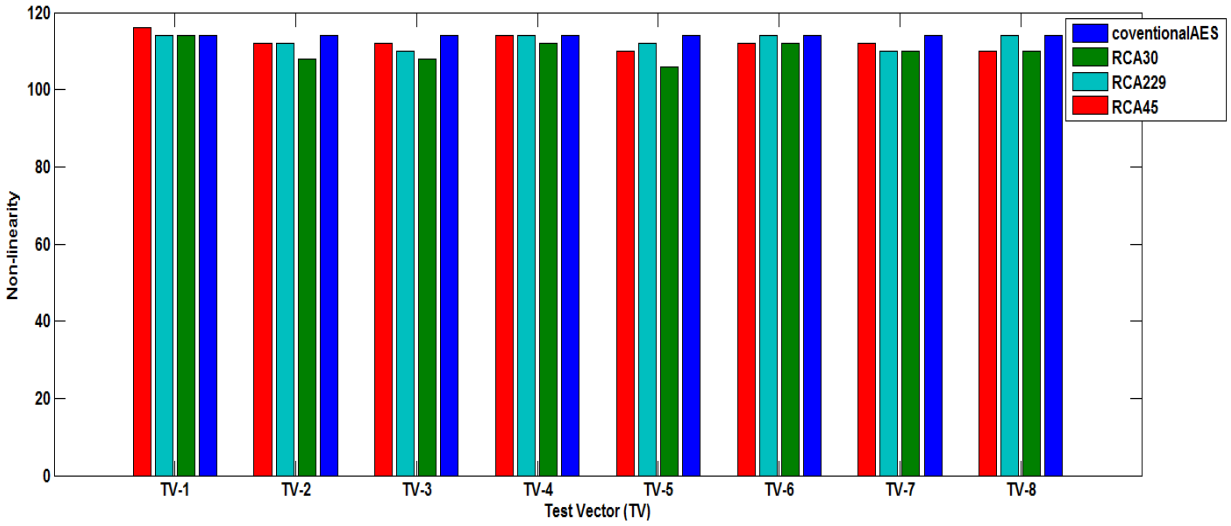

Figure 3: Non-linearity Test results

The non-linearity value of the conventional LUT based S-Box and RCA rule-based S-Box is calculated for various input test vectors are shown in figure 3. As an example, for the input test vector of 128-bit {01 12 23 34 45 56 67 78 89 9A AB BC CD DE EF F0}$_H$, the evaluated non-linearity value for conventional AES S-Box is {114}$_d$, while for RCA rule-30, RCA rule-45 and RCA rule-229 based S-Box is {106}$_d$, {110}$_d$, {112}$_d$ respectively. Hence, the non-linearity of the proposed S-Box reaches the value almost equal to non-linearity provided by the conventional S-Box.

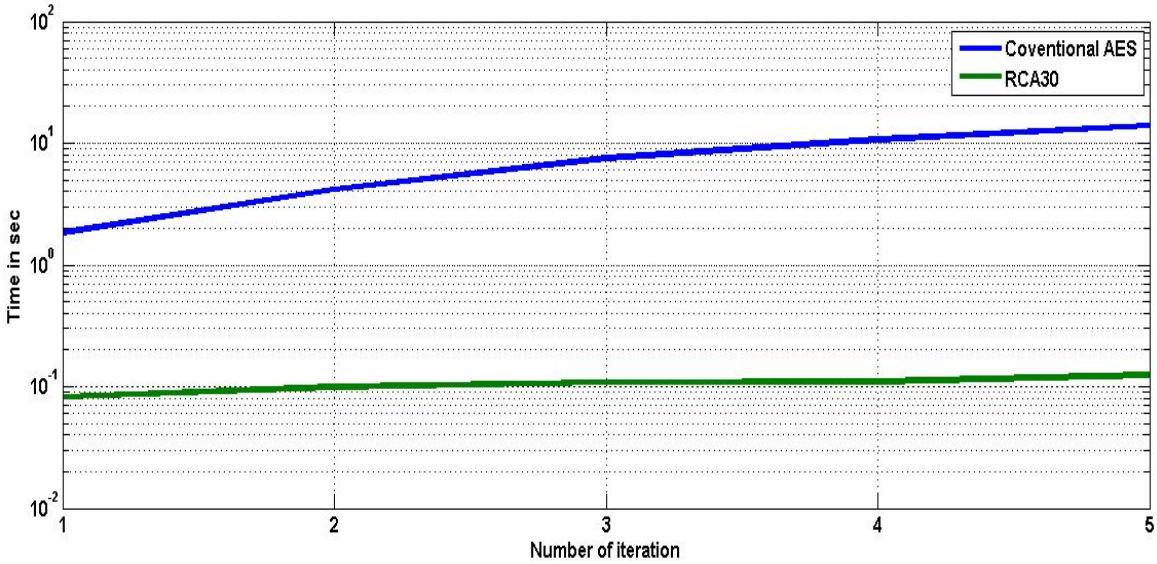

Figure 4: Computational Time analysis of S-Box

Figure 4 shows the Computational time analysis on both the LUT based and RCA rule-based S-Boxes are simulated. The time taken for computation of conventional LUT based S-Box is 0.9724 seconds, while for the RCA rule-30, RCA rule-45, RCA rule-229 based S-Box is 0.0303, 0.0316, 0.0310 seconds respectively. Hence, the proposed S-Box is a time optimized S-Box compared to the existing LUT based S-box.

5. CONCLUSION

This paper has proposed an RCA rule-based function for AES S-Box design. The proposed S-Box is designed by selecting different RCA rules that are highly non-linear and random in nature. From the experimental analysis, the S-Box designed using RCA rule-30 gave better performance than the other rules and conventional AES S-Box. Obviously, the time taken to produce an S-Box is found to be reduced while using the RCA rule-based approach. Further work will be carried out to test the proposed S-Box against the linear and differential cryptanalysis attacks.

6. REFERENCES

[1] Daemen, J., Rijmen, V. 2002."The design of Rijndael: AES-the advanced encryption standard", Information Security and Cryptography, Springer-Verlag,pp.238.

[2] Webster, A. F., Tavares, S. E. 1986."On the Design of S-Boxes", In Proceedings of Advances in Cryptology-CRYPTO '85. Lecture Notes in Computer Science, Vol. 218, Springer-Verlag,pp. 523-534.

[3] Blackburn, S., Murphy, S., Paterson, K. 1997."Comments on Theory and Application of Cellular Automata in Cryptography",IEEE Transactions on Computers, Vol. 46, No. 5, pp. 637-638.

[4] Satoh, A., Morioka, S., Takano, K., Munetoh, S. 2001."A Compact Rijndael Hardware Architecture with S-Box Optimization", In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Springer-Verlag, pp. 239-254.

[5] Rohiem, A. E., Elagooz, S., Dahshan, H. 2005."A Novel Approach for Designing the S-Box of Advanced Encryption Standard Algorithm(AES) Using Chaotic Map", In Proceedings of the Twenty second National Radio Science Conference, pp. 455-464.

[6] Sakamura, K., Dong, W. X., Ishikawa, H. 2004."A Study on Linear Cryptanalysis of AES Cipher", Journal of the Faculty of Environmental Science and Technology, Vol. 9, No. 1, pp. 19-26.

[7] Farhadian, A., Aref, MR. 2009. "Efficient method for simplifying and approximating the S-boxes based on power functions", In Proceedings of CSCW Companion, pp. 114-118.

[8] Szaban, M.,Seredynski,F. 2012."Dynamic Cellular Automata-Based S-Boxes", In Proceedings of Computer Aided Systems Theory-EUROCAST '11. Lecture Notes in Computer Science, Vol. 6927, Springer-Verlag, pp. 184-191.

[9] Jegadish Kumar, K. J., Chenna Kesava Reddy, K., Salivahanan, S. 2011."Novel and Efficient Cellular Automata based Symmetric Key Encryption Algorithm for Wireless Sensor Networks", International Journal of Computer Applications (IJCA), Vol. 13, No. 4, pp. 30–37.

[10] Jamil, N., Mahmood, R., Zaba, M. R., Zukarnaen, Z. A., Udzir, N. I. 2011."An Observation of Cryptographic Properties of 256 One-Dimensional Cellular Automata Rules", In Proceedings of ICIEIS, Springer-Verlag, pp. 409-420.

[11] Carlet, C., Dalai, D. K., Gupta, K. C., Maitra, S. 2006. "Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction", IEEE Transactions on Information Theory, Vol. 52, No. 7, pp. 3105-3121.

[12] Camion, P., Carlet, C., Charpin, P., Sendrier, N. 1992."On correlation-immune functions",In Proceedings of Advances in Cryptology-CRYPTO '91.Lecture Notes in Computer Science, Vol. 576, Springer-Verlag, pp. 86–100.