J Med Syst (2016) 40: 257
DOI 10.1007/s10916-016-0622-2

Low Power S-Box Architecture for AES Algorithm using Programmable Second Order Reversible Cellular Automata: An Application to WBAN

Bhoopal Rao Gangadari[1] · Shaik Rafi Ahamed[1]

Received: 30 June 2016 / Accepted: 19 September 2016 / Published online: 8 October 2016

Abstract In this paper, we presented a novel approach of low energy consumption architecture of S-Box used in Advanced Encryption Standard (AES) algorithm using programmable second order reversible cellular automata (RCA^2). The architecture entails a low power implementation with minimal delay overhead and the performance of proposed RCA^2 based S-Box in terms of security is evaluated using the cryptographic properties such as nonlinearity, correlation immunity bias, strict avalanche criteria, entropy and also found that the proposed architecture is secure enough for cryptographic applications. Moreover, the proposed AES algorithm architecture simulation studies show that energy consumption of 68.726 nJ, power dissipation of 3.856 mW for 0.18-μm at 13.69 MHz and energy consumption of 29.408 nJ, power dissipation of 1.65 mW for 0.13-μm at 13.69 MHz. The proposed AES algorithm with RCA^2 based S-Box shows a reduction power consumption by 50 % and energy consumption by 5 % compared to best classical S-Box and composite field arithmetic based AES algorithm. Apart from that, it is also shown that RCA^2 based S-Boxes are dynamic in nature, invertible, low power dissipation compared to that of LUT based S-Box and hence suitable for Wireless Body Area Network (WBAN) applications.

Keywords Advanced encryption standard (AES) · Application specific integrated circuit (ASIC) · Substitution box (S-Box) · Programmable cellular automata (PCA) · Programmable second order reversible cellular automata (RCA^2) · Wireless body area network (WBAN)

Introduction

Information security plays a vital role in area of secure data transmission for WBAN applications. The cryptographic algorithms are generally based on secret key and public key systems. However a lot of emphasizes was made on the secret key systems which use a symmetric key on both the encryption as well as decryption. Moreover in 2001, Federal Information Processing Standard selected Rijndael algorithm for Advanced Encryption Standard (AES) as a replacement to Data Encryption Standard (DES) [1, 2]. The AES algorithm has been standardized and adopted in latest IEEE Standard 802.15.6 for Wireless Body Area Network (WBAN) application due to its performance and high security [3]. This algorithm also helps in ensuring enough security in applications like secure communication, RFID tags, WBAN, etc.

The AES algorithm was realized on hardware using pipelining, sub-pipelining and loop unrolling architecture in order to achieve maximum throughput. The implementation of AES algorithm with fully pipelined architecture for encryption process achieved a throughput of 30 to 70 Gbits/s on 0.18-μm CMOS ASIC technology [4]. Although, these architecture are efficient for few applications which

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Bhoopal Rao Gangadari
bhoopal@iitg.ernet.in

Shaik Rafi Ahamed
rafiahamed@iitg.ernet.in

[1] Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Guwahati- 781039, India

require high throughput. Moreover, these high throughput architecture hardware realizations utilize more area and high power consumption. Among these architectures, the hardware implementation of classical S-Box are traditionally designed using LUT and hence require large number of memory cells [5, 6] . In order to avoid unbreakable delay and enhance the speed of S-Box, these S-Box are also designed and implemented using composite field arithmetic, binary decision diagram (BDD) and T-Boxes. However, the composite field arithmetic involves in decomposition of Galois Field GF(2^8) to GF($(2^4)^2$) or GF($((2^2)^2)^2$) respectively using isomorphic mapping [7, 8]. The S-Box realizations using binary decision diagram (BDD) and T-Boxes achieved a throughput of 10 Gbps [9–11]. The literature works so far reported above mainly emphasized on reduction in hardware complexities and enhancement in throughput [12]. On the other hand, there is a need to develop alternative architecture of S-Box, which is sufficiently secure with that of standard AES S-Box, with lesser power dissipation and low energy consumption. Since the WBAN applications require a ultra low energy AES architecture to expand the lifetime of the battery [13, 14]. We proposed the dynamic RCA^2 based S-Box architecture, which colossally lessens power utilization, energy consumption contrasted with traditional LUT based S-Box. Moreover, to check the level of security for the proposed RCA^2 based S-Box, we additionally acquired cryptographic properties such as, nonlinearity, entropy, correlation immunity bias, balancedness property and strict avalanche criterion. It is also found that the proposed RCA^2 based S-Box gives comparable performance in terms of security with respect to LUT based S-Box.

In this paper, the concept of AES algorithm is revisited in Section "Concept of AES algorithm". The formulation of S-Box using programmable reversible cellular automata (RCA^2) is discussed in Section "Formulation of S-Box using 2^{nd} order reversible one dimensional cellular automata (RCA^2)". The proposed novel RCA^2 based S-Box and architecture is presented in Section "Proposed RCA^2 based S-Box". The comparative analysis of LUT based S-Box and RCA^2 based S-Box are evaluated using cryptographic properties with architecture implementation in Section "Security analysis of LUT based S-Box and RCA^2 based S-Box" and conclusion is reported in Section "Conclusion".

Concept of AES algorithm

The Advanced Encryption Standard is a symmetric block cipher with 128 bits secret key as recommended by the latest IEEE Standard 802.15.6 for Wireless Body Area Network (WBAN) application [3, 6, 15, 16]. The AES algorithm consists of four transformations namely the Substitution Bytes (S-Box), Shift Rows (SR), Mix Columns (MC) and Add Round Key (ARK) in order to generate cipher text over plain text [17]. The AES algorithm encryption process is shown in Fig. 1, the number rounds of transformation (N_r) is mathematically derived by $N_r = \frac{S_k}{32} + 6$, where S_k = key size. The latest IEEE standard 802.15.6 for Wireless Body Area Network (WBAN) application has recommended a secret key size of 128 bits for AES algorithm which results in 10 rounds of transformation. Out of these 10 rounds, first 9 rounds undergo four transformations S-Box, SR, MC and ARK, except the last 10 round have only three transformations S-Box, SR and ARK. The input bits are arranged in 4 × 4 matrix of bytes known as state array. Each column as well as row are known as a word (Fig. 2).

Substitution bytes

In S-Box transformation, each byte of input data is substituted with another byte using Look-Up-Table (LUT). These S-Boxes are computed by the multiplicative inverse of each element in the state using GF(2^8) with an irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$ and followed by an

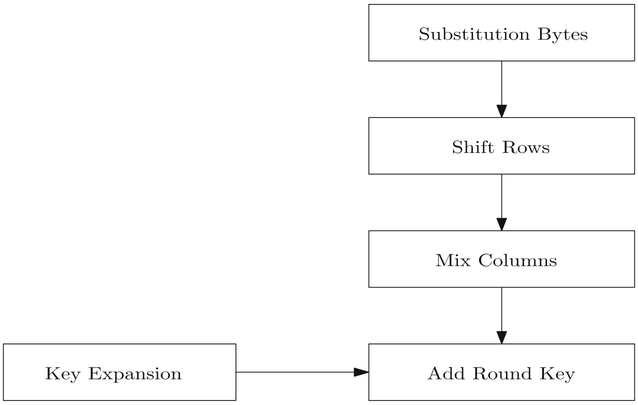

Fig. 1 Encryption process of each round

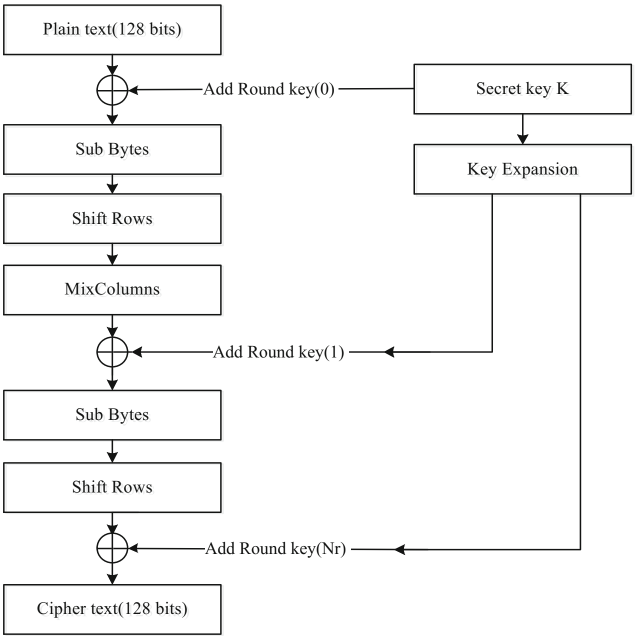

Fig. 2 A block diagram of AES Encryption

affine transformation. Traditionally, the classical S-Box are implemented using memory cells which can store the 256 possible values in 8 × 8 array of bits. However, the input data is 128 bit so the total number of 16 LUT based S-Box used in the AES algorithm hence there is increase in hardware area and power consumption. The LUT based S-Box in hexadecimal form is shown in Table 1. For example, if the input data is 'd4', then the substituted value of S-Box from the Table 1. is determined by the intersection of 'd' row and '4' column which results in '48'.

Shift rows

The SR transformation is attained by shifting of elements by one byte in order to create diffusion in cipher text. In SR transformation, the bytes in the first row remain unchanged whereas the second, third and fourth row are shifted to the left by 1, 2, 3 bytes respectively.

Mix columns

This MC transformation is used for attaining diffusion in the block cipher and a column operation, where each column is expressed as a four term polynomial over GF(2^8) field and multiplied by fixed polynomial $A(x) = (03H)x^3 + (01H)x^2 + (01H)x + (02H)$ with modulo x^4+1. Mathematically, this operations are written in matrix form as follows:

$$S^1(x) = A(x) \otimes S(x). \tag{1}$$

$$\begin{bmatrix} S^1_{0,C} \\ S^1_{1,C} \\ S^1_{2,C} \\ S^1_{3,C} \end{bmatrix} = \begin{bmatrix} 02H & 03H & 01H & 01H \\ 01H & 02H & 03H & 01H \\ 01H & 01H & 02H & 03H \\ 03H & 01H & 01H & 02H \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix} \tag{2}$$

where $0 \leq C < 4$.

Add round key

In ARK transformation, the ARK cipher keys are generated in the key expansion phase by using bitwise XOR operation. A total of $4(N_r + 1)$ words are generated in the key expansion block. Each ARK $(i) = (w_{4i},\ w_{4i+1},\ w_{4i+2},\ w_{4i+3})$, where $i = 0\ to\ N_r$. Initially, the first ARK is the initial 128 bits secret key and the subsequent round keys are calculated using SubWord, RotWord and Rcon. SubWord means nonlinear transformation of each byte of key using S-Box. The Rotation Word (RotWord) is a cyclic left shift of each byte in a word by one byte. Rcon is an array of constant words and the left most byte in word is non-zero.

Formulation of S-Box using 2^{nd} order reversible one dimensional cellular automata (RCA^2)

As S-Box is responsible for the amount of confusion introduced in the plain text, an efficient S-Box design makes the system immune to cryptographic attacks. So, in this paper, we proposed a efficient S-Box architecture using programmable second order reversible one dimensional cellular automata (RCA^2). The basic function of S-Box is to transform 8 bits input to another 8 bits secret data using predefined Look-Up-Table (LUT). The truth table of S-Box is basically a function $f : B^n \rightarrow B^m$. For encryption of 128 bits plain text, a total number of 16 LUT based S-Boxes are utilized in AES algorithm therefore the LUT based S-Box architecture utilize more area, high energy consumption and these S-Boxes are more prone to differential cryptanalysis due to rigid architecture [18]. Hence, LUT based S-Box architectures is no more suitable for WBAN applications. Apart from this, in order to meet the requirements of WBAN application, there is a demand to develop a cryptographic algorithm which is highly secure, lesser area and low energy consumption [19]. However, to overcome the limitation of classical S-Box, we proposed the architecture of S-Box using second order reversible one dimensional cellular automata (RCA^2) which requires lesser area and low energy consumption [20].

The basic structure of CA is shown in Fig. 3, consist a groups of cells with a finite size of length from K_0 to K_7

Table 1 LUT based S-Box

y																	
x		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fd	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

which evolve at discrete time steps using deterministic rule with each cell can store one of the two states 0 and 1. If the right most and left most (extreme) cells of this finite size CA are considered to be adjacent each other, then the CA is called as periodic boundary CA. The one dimensional periodic boundary CA evolves with different neighborhood configurations of elementary CA [21]. Each elementary CA consists of central cell i which is surrounded by neighborhood cells of a defined radius r, therefore the total number of cells in elementary CA is given as $n_s = 2r + 1$, including central cell i. We considered $r = 1$, which results in the total number of possible different neighborhood configurations of elementary CA are $L = 2^{n_s}$ with K_{i-1}^t, K_i^t, K_{i+1}^t cells, where $i = 0$ to 7. The next state of central cell K_i^{t+1} at time $(t + 1)$ depends on the current state of central cell K_i^t and also neighborhood K_{i+1}^t, K_{i-1}^t cells respectively at time t with a deterministic rule of function f_r. Mathematically, K_i^{t+1} can be expressed as

$$K_i^{t+1} = f_r(K_{i-1}^t, K_i^t, K_{i+1}^t) \tag{3}$$

The decimal form representation of deterministic rules f_r is shown in Table 2 and the total number of CA rules considered are $2^L = 256$. The CA is dynamic in nature as the output pattern evolve depending on the deterministic rule moreover the rule can also be updated at discrete time step t.

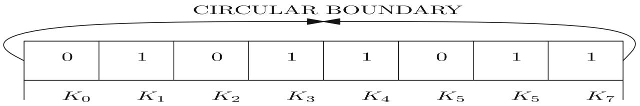

Fig. 3 Lattice of Cellular Automata

A CA is said to be 1^{st} order one dimensional (1-D) CA, if the next configuration K_i^{t+1} is the function of defined rule and present neighborhood configuration K_{i-1}^t, K_i^t, K_{i+1}^t cells. The reversibility of one dimensional (1-D) CA system of a given length in which each output state is based on rules and the output can be realized using Boolean function [22]. If the function is invertible then the rule is reversible which is a desired property in cryptography.

If the Boolean function is not one on one, then a value in the range set can map to many value in domain set, which in the process of decryption the plain text is not retrieved from the the cipher text. We observed that the 1^{st} order one dimensional cellular automata only 6 rules are reversible. Moreover to overcome the limitations, we proposed 2^{nd} order one dimensional cellular automata (RCA^2) in which there are 64 reversible rules and the mapping of Boolean function is one on one. The structure of RCA^2 is slightly different as that of 1^{st} order one dimensional cellular automata, the results obtained with 1^{st} order one dimensional CA is XORed with the previous value of the central cell i at time step $t - 1$ in order to achieve the new configuration of RCA^2 at a time step $t + 1$. The next configuration of central C_i^{t+1} for RCA^2 at $t + 1$ depends not only on present cell C_i^t but also on the previous cell C_i^{t-1}, as shown in Fig. 4. Mathematically, the RCA^2 is represented by

$$C_i^{t+1} = (C_i^t \oplus C_i^{t-1}) \tag{4}$$

Table 2 Truth table for Rule 90 and 75

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
	111	110	101	100	011	010	001	000	
Rule 57	0	0	1	1	1	0	0	1	Decimal 57
Rule 99	0	1	1	0	0	0	1	1	Decimal 99

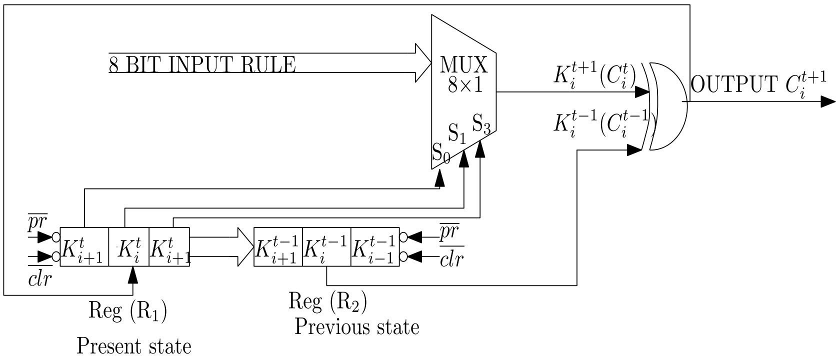

Fig. 4 Basic cell structure of RCA^2

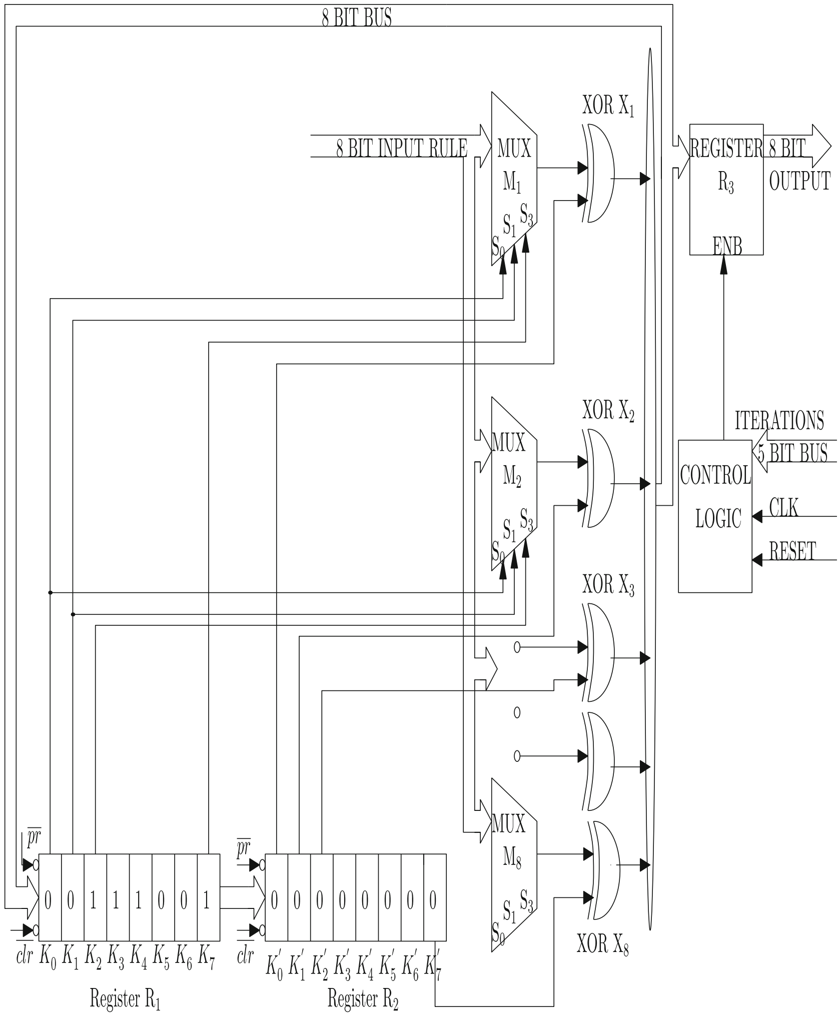

Fig. 5 RCA^2 based 8 × 8 S-Box architecture

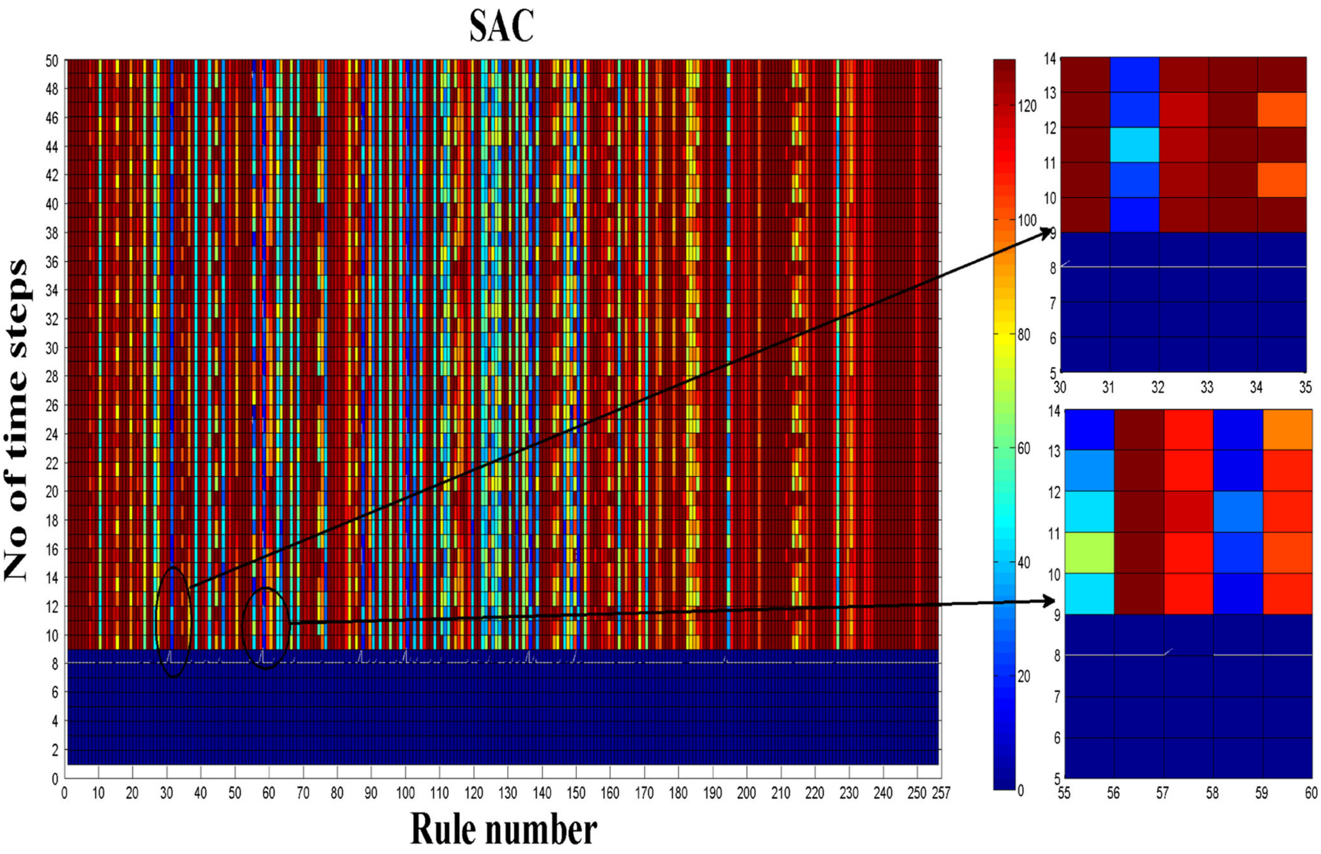

Fig. 6 Values for Strict Avalanche Criteria of RCA^2 based S-Box

where $(C_i^t, C_i^{t-1}) = (K_i^{t+1}, K_i^{t-1})$ respectively at discrete time step $t+1$ and $t-1$.

Algorithm 1 RCA^2 with 256 rules

```
$K \leftarrow 0$;
$K^t \leftarrow D$;
$INPUT \leftarrow f_r$;
$INPUT \leftarrow NOI$;
loop $r \leftarrow 1$ to $256$
        for $t \leq NOI$ do
          if $Rule(r) == f_r$ then
            for $i \leftarrow K_0$ to $K_7$ do
              $K_i^{t+1} \leftarrow f_r(K_{i-1}^t, K_i^t, K_{i+1}^t)$
                assign $(C_i^t = K_i^{t+1}), (C_i^{t-1} = K_i^{t-1})$
                $C_i^{t+1} \leftarrow (C_i^t \oplus C_i^{t-1})$
            end for
          end if
        end for
end loop
```

The functioning of RCA^2 based S-Box with 256 number of different rules is shown in Algorithm 1. The initial 8 bit input data stacked on the array of registers through D, NOI means the number of iterations from 1 to 50 at discrete time steps and K_0 to K_7 is defined as the size of the lattice. Hence, RCA^2 algorithm there exists 2^8 possible random initial states which are taken into consideration. However, the 8 bit random initial states of RCA^2 evolves using different 256 deterministic rule and number of iterations which are considered from time step 1 to 50. There exist a relationship between time step t and group of CA cells K_0 to K_7 in a lattice as the diversification in output is high if the time step is greater than size of the lattice.

Proposed RCA^2 based S-Box

The S-Box of AES algorithm in cryptography provide confusion in the cipher text and hence plays an important role in AES algorithm. The conventional LUT based S-Box architecture uses a large number of memory cells which eventually consumes more power. Moreover, the secret information from the existing AES algorithm architecture can be revealed using power analysis attacks [18].

In order to overcome these limitations, we proposed a RCA^2 based architecture for S-Box with low energy

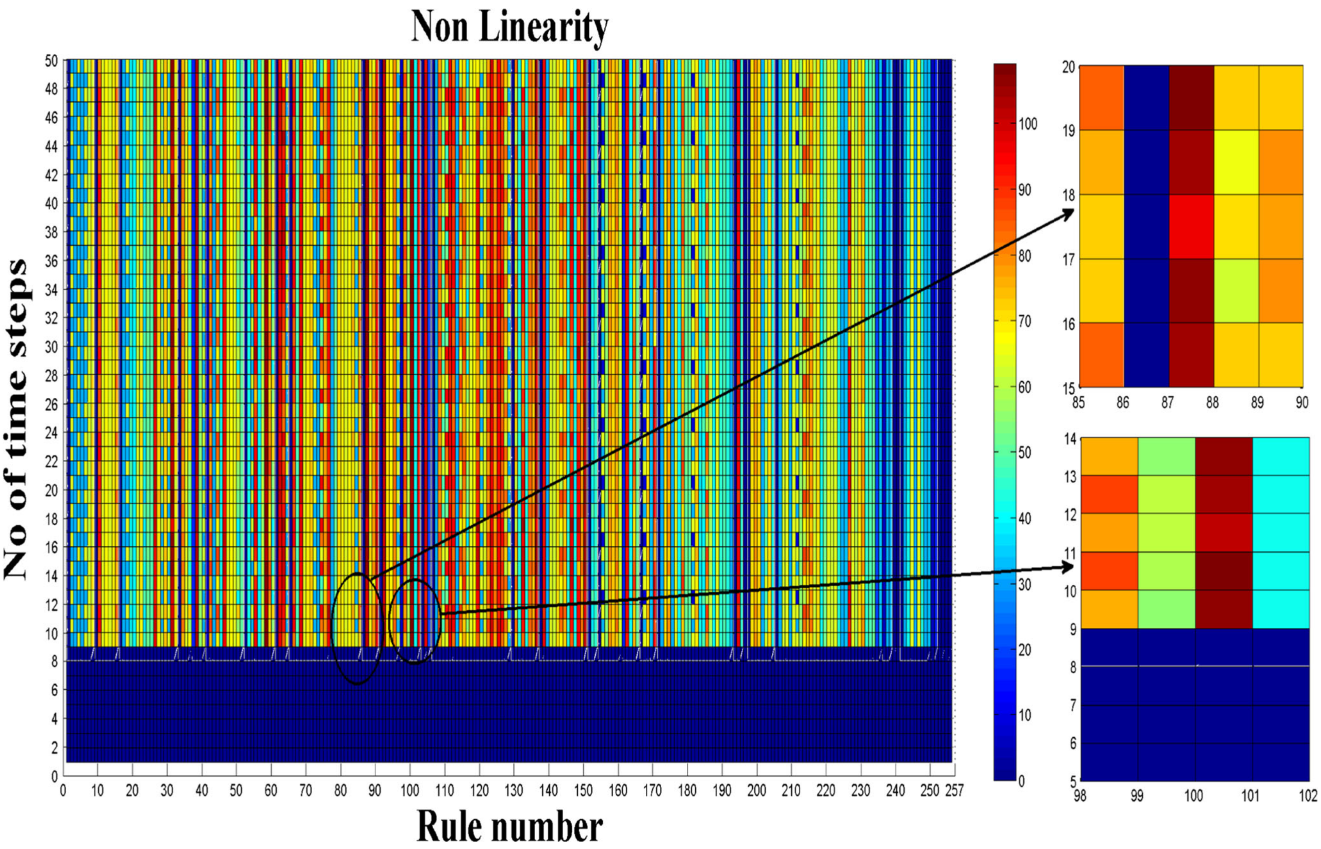

Fig. 7 Value for Non Linearity of RCA^2 based S-Box

consumption and dynamic in nature. Unlike the conventional LUT based S-Box, the proposed RCA^2 S-Box is dynamic in nature because of the fact that the output of the S-Box is a function of input rule which can be programmed. The basic function of RCA^2 based S-Box is to transform 8 bits input data to another secret data which is achieved using a combinational logic as shown in Fig. 4.

The initial 3 bits are loaded into the register R_1, R_2 using preset and clear signals. The output of C_i^{t+1} depends on the current state of cell C_i^t and previous state of cell C_i^{t-1}, where as $K_i^{t+1} = C_i^t$ and $K_i^{t-1} = C_i^{t-1}$ as depicted in Fig. 4.

The switches of multiplexer are activated and deactivated according to the control signals K_{i-1}^t, K_i^t, K_{i+1}^t and the output of multiplexer is mapped according to the stored 8 bits rule in the register.

The output of the proposed basic RCA^2 structure is one bit with given 8 bit input rule as shown in Fig. 4. In order to implement the S-Box which operates on 8 bits, eight such basic cells shown in Fig. 4 needs to be inter connected.

The proposed architectural design of 8 × 8 array RCA^2 based S-Box is implemented using logic gates, multiplexers and registers as shown in Fig. 5. The initial 8 bits of RCA^2 array will be loaded into register R_1 using preset and clear signals. The bits in the register R_1 will be applied as control signals to 8:1 MUX (M_1-M_8) in circular fashion whose input is an 8 bit rule. First 3 bits R_7, R_0 and R_1 will act as a control signals to M_1, R_0, R_1 and R_2 to M_2 and the last MUX M_8 the control signal are R_6, R_7 and R_0. The register R_2 is used to store the previous value of bits K_0 to K_7 as K_0^1 to K_7^1. The previous bit K_0^1 is XORed with the output of MUX M_1, K_1^1 is XORed with output of MUX M_2 and the last bit K_7^1 is XORed with output of MUX M_8. The MUXs produces the output according to the Table 2. The outputs bits produced by the XOR gate will be used as a RCA^2 array bits in subsequent iterations.

The control logic has a 6 bit up counter and a comparator. If the count value of counter is equal to the number of iteration in time step, then the output of the control logic circuit goes high to enable the register (R_3). The latency incurred in computing the S-Box depends upon the number of iterations defined in the RCA^2. However, on the other side, the ASIC implementation of RCA^2 based S-Box architecture shown in Fig. 5 utilizes few logic elements compared to that of LUT based S-Box [23]. As a result, RCA^2 based S-Box architecture consumes less power and require small

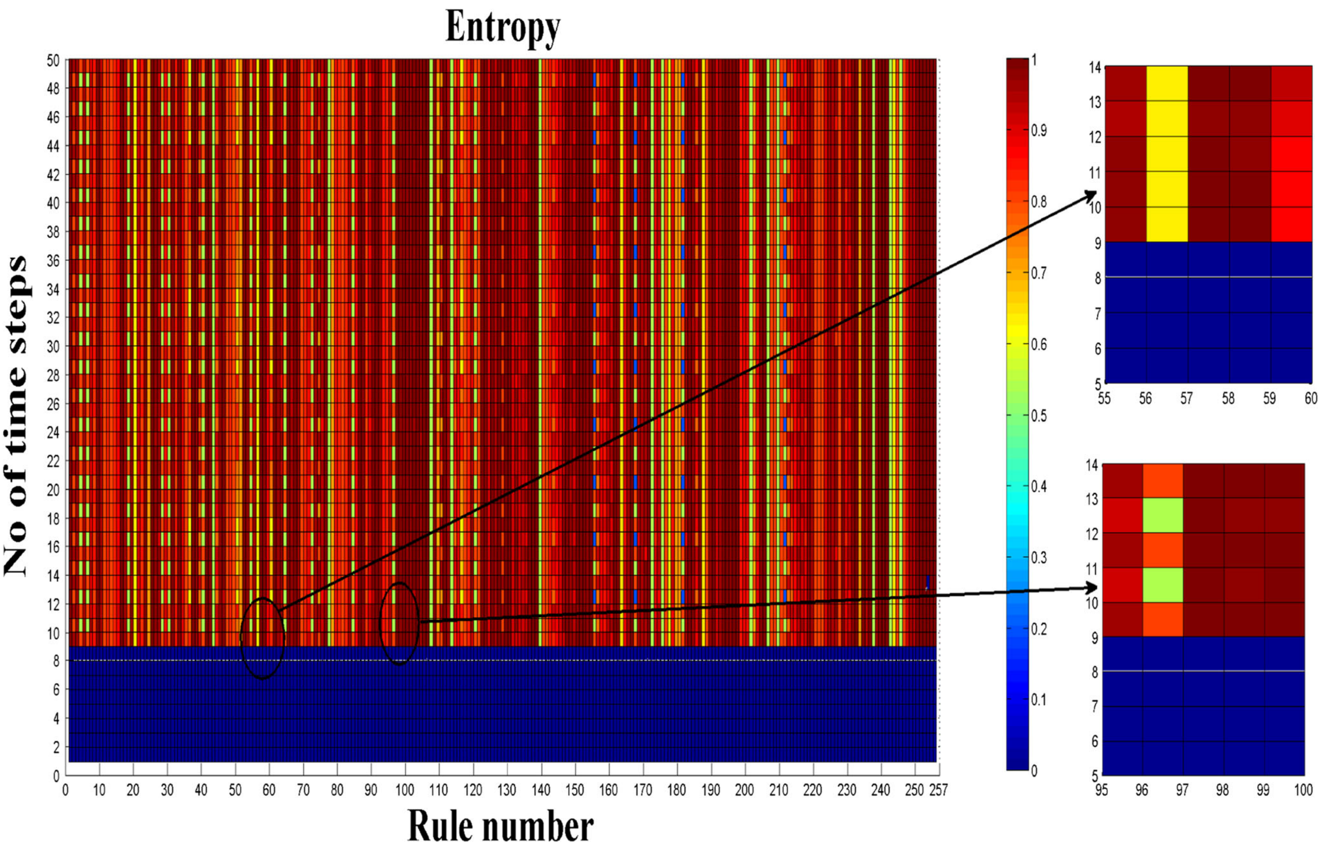

Fig. 8 Values for Entropy of RCA^2 based S-Box

chip area and hence this hardware realization is much suitable for WBAN applications. The process overhead incurred in order to compute (number of time steps) for proposed RCA^2 based S-Box depends upon the specified number of iterations. As WBAN application deal with a low frequency biomedical signals, the process overhead incurred will not effect the overall performance of the system.

Security analysis of LUT based S-Box and RCA^2 based S-Box

In order to analyze the security aspects, the output bits obtained by the proposed RCA^2 based S-Box architecture as described in Section "Proposed RCA^2 based S-Box", are taken as inputs bits to the MATLAB system which computes cryptographic properties. The functioning of S-Box is to map 8 input bits to 8 output bits using predefined table known as Look-Up-Table (LUT) μ : GF(B^n) → GF(B^n) [24].

In cryptography, the Boolean function used to encrypt the plain data must be diverse and mapping from input to output should be one on one, so as to provide enough security and proper decryption [24]. In order to analyze the S-Box using cryptographic properties the 2^8 output bits are transformed into a single output bit using Boolean function $f_i : B^n \rightarrow B$, where $i \in [1, m]$. In a S-Box, $\mu : B^n \rightarrow B^m$ and hence there exists m number of function $\mu = \{f_1, f_2, \cdots\cdot f_m\}$, The truth table in polarity form is written as follows: $f_k(x)=(-1)^{f(x)}$.

$$f_\beta(x) = (\alpha_1 f_1(x) \oplus \alpha_2 f_2(x) \oplus \alpha_3 f_3(x) \ldots \oplus \alpha_m f_m(x)) \quad (5)$$

f_β is a Boolean function of the linear combination of m functions $f_i(x)$, $i \leq m$, where $\alpha_i \in B^m$ are coefficient of the linear function. The security analysis was carried out using S-Box values obtained from the proposed RCA^2 architecture. The values obtained by using cryptographic properties are plotted in Figs. 6, 7, 8 and 9. The level of security of S-Box is observed using the cryptographic properties, namely, the correlation immunity bias, strict avalanche criteria, nonlinearity and entropy. If an S-Box satisfies these cryptographic properties then the S-Box is cryptographically secure against cryptanalysis. The symbolic representation of the cryptographic properties are presented in Table 3. We considered the size of RCA^2 lattice to be 8 bits, number of RCA^2 rules are 256 and the RCA^2 lattice is iteratively executed for 9 to 50 discrete time steps with 256 different RCA^2 rules. The results obtained using the proposed RCA^2 technique are compared with that of conventional S-Box in Table 4.

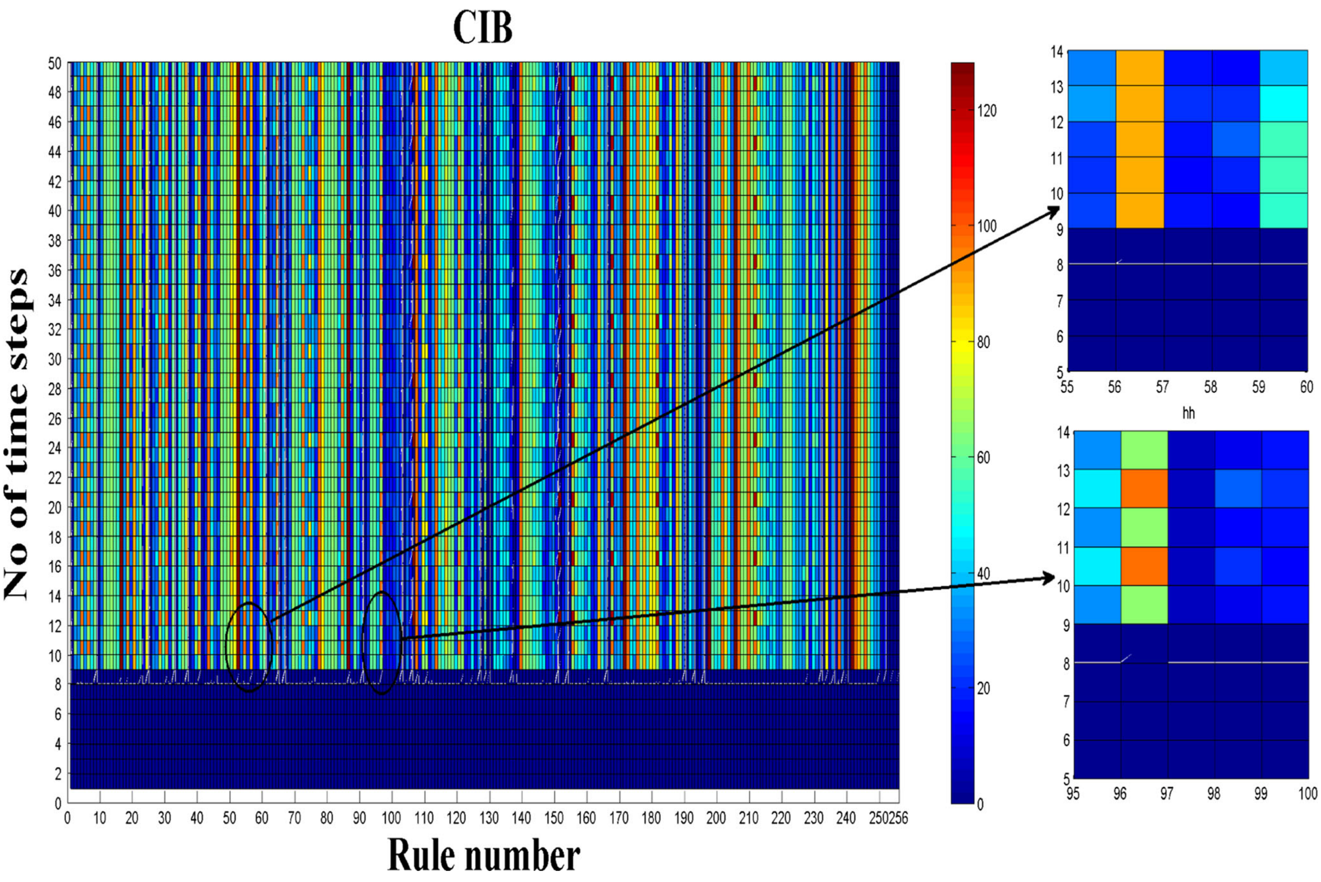

Fig. 9 Value for Correlation Immunity Bias of RCA^2 based S-Box

Strict avalanche criteria(Υ_S)

Strict avalanche criteria states that, if one input bit changes in a Boolean function, then half of the output bits should be changed [25]. For a Boolean function, if f is to satisfy SAC the following condition, $f(x) \oplus f(x \oplus \alpha)$ should be balanced, where the Hamming weight of a is 1 and SAC is represented by Υ_S.

$$dSAC_f = max_{1 \le i \le n} |2^{n-1} - \sum_{x \in B^n} f(x) \oplus f(x \oplus c_i^n)| \quad (6)$$

B^n consists of all the possible input in the n variable function which is basically 2^n different inputs c_i^n consisting of all the element in B^n whose Hamming weight is 1 .

$$\Upsilon_S = max(SAC_\mu) \quad (7)$$

If the observed value of SAC is less for a cipher, then the cipher is more difficult to cryptanalysis. We infer that the value of SAC for RCA^2 S-Box are 16 for rule number 30, 57, 99, 135 as shown in Fig. 6 and Table 4, which is comparable with that of standard LUT S-Box as shown in Table 4. Moreover, we found that 31.0323 % out of 256 CA rules had comparable SAC value of 16. The best values obtained for SAC is 14 in case of rule 31 and rule 58 which are emphasize in Fig. 6.

Entropy(H_S)

This property provides us the amount of information in the input bits, when output bit are already known [26]. If the function is $f : B^n \rightarrow B$, then the entropy function can be defined by H_S.

$$H(P_i) = P_i \, log_2 \frac{1}{P_i} + (1 - P_i) \, log_2 \frac{1}{1 - P_i} \quad (8)$$

Table 3 Symbolic representation

Cryptographic property	Notation
Strict Avalanche Criteria(SAC)	Υ_S
Entropy	H_S
Non Linearity	$\Re_S$
Correlation Immunity Bias (CIB)	$\Phi_S(l)$

Table 4 Cryptographic Properties values for RCA^2 based S-Box

Rule No	Time Step	NL	Entropy	CIB	SAC
30	15	100	0.9887	16	16
31	9	102	0.9887	16	14
57	9	106	0.9914	14	16
58	9	106	0.9914	14	14
86	10	100	0.9887	16	16
87	19	109	0.9947	11	16
99	9	106	0.9914	14	16
100	10	108	0.9857	18	18
135	13	100	0.9857	18	16
149	46	100	0.9887	16	16
Hussain et al.	NA	105	NP	NP	16
[27]		96	NP	NP	10
Clark et al.	NA	90	NP	19	44
[28]		100	NP	24	48
Millan et al.	NA	80	NP	NP	16
[29]			NP	NP	18
Nedjah et al.	NA	70	NP	NP	NP
[30]		102	NP	NP	NP
Standard	Polynomial				
AES S-Box	$x^8 + x^4 + x^3 + x + 1$	112	0.9887	16	14

*NA means not applicable

*NP means not provided

where P_i is fraction of ones in the output. The $(i, j)^{th}$ input/output bit to bit entropy $H(\frac{x_i}{\mu_j})$ is computed.

$$H = min[H(\frac{x_i}{\mu_j})] \quad [i \in \{1, n\}, j \in \{1, m\}] \tag{9}$$

$$H_S = min(H_\mu) \tag{10}$$

where $H(x_i/\mu_j)$ is the entropy corresponding to the probability $P(x_i/\mu_j)$ If the value of entropy is high for a observed cipher, then the cipher is difficult for cryptanalysis. The best values are achieved at rule number 30, 57, 86, 99, 135, 149 are presented in Table 4. We also found for RCA^2 based S-Box that 26.0323 % out of 256 CA rules had better entropy value than AES with standard LUT based S-Box entropy values. The entropy plots best value obtained at rule 57 is 0.9914 and rule 99 is 0.9914 are highlighted in Fig. 8.

Non linearity($\Re_S$)

The non linearity of a Boolean function is the minimum distance from the function to the set of affine functions and non linearity is represented by $\Re_S$.

$$N_f = min[d(f, g)], \ where \ g \in A_n \tag{11}$$

where A_n is the set of all the affine function.

$$d(f, g) = 2^{n-1} - 2^{-1}(\langle \eta, \beta \rangle) \tag{12}$$

where η, β represent the binary sequence of f, g respectively and $\langle \eta, \beta \rangle$ define the scalar product of sequence ?, Hence, for a function $f : B^n \rightarrow B$

$$N_f = 2^{n-1} - 2^{-1}[max(\langle \eta, \beta_j \rangle)] \tag{13}$$

where β_j belongs to sequence of all linear function.

$$\Re_S = min(N_\mu) \tag{14}$$

If the value of non linearity is high for a cipher, then the cipher is secure enough against cryptanalysis. We observed that the value of non linearity is high for rule 57, 99 and also observed that 6.098 % out of 256 CA rules has higher values of non linearity as shown in Fig. 7. The maximum value of non linearity attained was 109 in case of RCA^2 based S-Box as shown in Table 4. The best value obtained for non linearity at rule 87 and rule 100 are highlighted in Fig. 7.

Correlation immunity bias($\Phi_S(l)$)

A Boolean function is said to satisfy correlation immunity bias of order l, if it is statistically independent of combination of any l input bits. Mathematically, if l input bits are

Table 5 Hardware results of Proposed AES algorithm with RCA^2 based S-Box

AES	Tech	Gates	Power (mW)	Frequency (MHz)	Clock cycles	Energy (nJ)
Kim [31]	0.25μm	4000	0.02	0.1	870	174
Eslami [32]	0.18μm	NP	7.55	13.56	248	138
Manoj [33]	0.18μm	NP	0.0512	1	500	25.60
Kaps [34]	0.13μm	4070	0.0238	0.5	534	24.56
Proposed AES algorithm	0.18μm	4830	3.856	13.69	244	68.726
Proposed AES algorithm	0.13μm	4120	1.65	13.69	244	29.408

*NP means not provided

fixed then we can get ${}^nC_l 2^l$ g functions. So for $f : B^n \rightarrow B$, the CIB is represented as $\Phi_S(l)$.

$$CIB_f(m) = max|2^m * W(g_j) - W(f)| \qquad (15)$$

where $W(g_j)$belongs to Hamming weight of all the possible function keeping m bits in the function f fixed. $W(f)$ corresponds to the Hamming weight of function f.

$$\Phi_S(l) = max(CIB_\mu) \qquad (16)$$

If the CIB value is less for a observed cipher, then the cipher is secure enough against cryptanalysis. We observed that the best value of CIB at rule number 57, 99, 169 are presented in Table 4. The CIB plots of best value obtained at rule 57 and rule 99 are highlighted in Fig. 9. The best observed values is 14 at rule 99 and rule 57, for 36.3548 % out of 256 RCA^2 rules had better value of CIB, as shown in Fig. 9.

Moreover, we observed the results obtained for 256 number of rules for RCA^2 and the values of non linearity, CIB, entropy and SAC for all the 62 reversible rules of RCA^2 have better values. The value of SAC, CIB, non linearity and entropy of 2^{nd} order 1-D Cellular Automata along with few reversible rules are shown in Table 4. The RCA^2 based S-Boxes are flexible, dynamic in nature and more resistant to differential cryptanalysis as these provide enough level of security compared to that of LUT based S-Box. The observed values of nonlinearity, correlation immunity bias, strict avalanche criterion and entropy of standard LUT based S-Box for AES algorithm and our proposed RCA^2 S-Box with that of the existing works are shown in Table 4 [27–30].

Architectural design

In order to validate the proposed architecture, AES algorithm with RCA^2 based S-Box is implemented using verilog, verified on FPGA board and synthesized with Cadence RTL compiler. The proposed architecture is operated at different clock frequency with 0.18-μm technology (core voltage of 1.62 V) and 0.13-μm technology (core voltage of 1.08 V) under worst-case conditions. The total time consumed to encrypt 128 bits of plain text is calculated by $Latency = Clockcycles \times Timeperiod$. The performance of AES with RCA^2 based S-Box are reported in Table 5 in terms of gate count, power dissipation, energy consumption and operating frequency. However, our proposed RCA^2 based S-Box realization, the number of iterations were considered are 20 clock cycles to compute the RCA^2 S-Box, whereas, the total time taken to encrypt 128 bit plain text by AES with RCA^2 S-Box are 244 clock cycles.

Number of gates utilized for LUT based S-Box and Composite Field Arithmetic based S-Box realizations was 696, 294 respectively with 0.11-μm [35], while, the proposed dynamic RCA^2 S-Box realizations the number of gates utilized are 124, 136 using 0.18-μm and 0.13-μm technology libraries. Sumio et al. [10] presented low power S-Box architecture which consumes power of 29 μW at 10 MHz using 130-μm CMOS technology, where as our proposed RCA^2 S-Box operated at 10 MHz using 130-μm CMOS technology consumes power of 14 μW. It is easily seen that our proposed S-Box consumes 51 % less power compared to the existing work [33]. The work reported in [32] needs power consumption of 7.55 mW for encryption with 0.18-μm technology operated at 13.56 MHz frequency while our proposed work of AES with RCA^2 based S-Box if operated at 13.69 MHz clock frequency, power consumption of 3.856 mW for encryption and energy consumption of 68.726 nJ, which is 50 % less compared to Eslami et al. [32]. The ASIC implementation of AES algorithm using Composite Field Arithmetic based S-Box uses 500 clock cycles to complete 128 bits of cipher text, operating at 1 MHz frequency with 51.20 μW of power dissipation and energy consumption of 25.60 nJ using 180-μm CMOS technology library [33]. Our proposed RCA^2 S-Box architecture with AES algorithm when operated at 1 MHz clock consumes power of 104.08 μW and energy consumption of 25.396 nJ, it is clear that there is slight decrease in energy consumption compared with Manoj et al. [33]. Our proposed RCA^2 S-Box with AES algorithm operating at 1 MHz frequency shows an reduction in energy consumption compared with Kaps et al. [34] It is clear from Table 5 that the proposed RCA^2 based S-Box out performs in terms of power dissipation and energy consumption compared with existing works [10, 32–35].

Conclusion

In this paper, we proposed a RCA^2 based S-Box realization for AES algorithm to overcome the limitations of classical S-Box used in standard AES algorithm. The proposed RCA^2 S-Box with AES algorithm architecture is evaluated through simulation and synthesis using CMOS technology library. Unlike the design in [10, 31–34], the proposed architecture require few logic elements, hence there is reduction in power and energy consumption. The level of security for LUT based conventional S-Box and RCA^2 based S-Box was evaluated using cryptographic properties. However, we have achieved a comparable performance in terms of security for the proposed RCA^2 with that of conventional S-Box used in AES using cryptographic properties. The proposed architecture was synthesized usin Cadence RTL compiler to evaluate area, power and frequency of operation. The maximum operating frequency achieved is 496 MHz for 180-μm 130-μm and 646 MHz for 130-μm technology. Therefore, it has been observed that AES with RCA^2 based S-Box is an ultra low power and low energy consumption encryption algorithm and hence suitable for WBAN applications.

References

1. National Institute of Standards and Technology: FIPS PUB 46-3: Data Encryption Standard (DES). super-sedes FIPS 46-2, 1999.
2. Advanced Encryption Standard (AES): Federal Information Processing Standards Publication 197 Std., 2001.
3. IEEE Standard for Local and metropolitan area networks− Part 15.6: Wireless Body Area Networks, Std.
4. Hodjat, A., and Verbauwhede, I., Area-throughput trade−offs for fully pipelined 30 to 70 Gbits/s AES processors. *IEEE Trans. Comput.* 55(4):366–372, 2006.
5. Kuo, H., and Verbauwhede, I., Architectural optimization for a 1.82Gbits/sec VLSI implementation of the AES rijndael algorithm. In: Cryptographic Hardware and Embedded Sys- tems CHES 2001, ser. Lecture Notes in Computer Science, Vol. 2162, pp. 51–64. Berlin: Springer, 2001.
6. Li, H., Efficient and flexible architecture for AES. *IEE Proc. Circ. Devices Syst.* 153(6):533–538, 2006.
7. Zhang, X., and Parhi, K., High−speed VLSI architectures for the AES algorithm. *IEEE Trans. Very Large Scale Integrat. (VLSI) Syst.* 12(9):957–967, 2004.
8. Zhang, X., and Parhi, K.K., On the optimum constructions of composite field for the AES algorithm. *IEEE Trans. Circ. Syst. II: Express Briefs* 53(10):1153–1157, 2006.
9. Morioka, S., and Satoh, A., A 10−Gbps full−AES crypto design with a twisted BDD S−Box architecture. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* 12(7):686–691, 2004.
10. Morioka, S., and Satoh, A., An optimized S−Box circuit architecture for low power AES design. In: Cryptographic Hardware and Embedded Systems − CHES 2002, ser. Lecture Notes in Computer Science, Vol. 2523, pp. 172–186. Berlin: Springer, 2003.
11. Shastry, P., Somani, N., Gadre, A., Vispute, B., and Su- taone, M.: Rolled architecture based implementation of AES using T−Box. In: *IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 626-630, 2012.
12. Kapoor, H., Rao, G., Arshi, S., and Trivedi, G., A security framework for NoC using authenticated encryption and session keys. *Circ. Syst. Signal Process* 32(6):2605–2622, 2013.
13. Selimis, G., Huang, L., Massle, F., Tsekoura, I., Ashouei, M., Catthoor, F., Huisken, J., Stuyt, J., Dolmans, G., Penders, J., and De Groot, H., A lightweight security scheme for wireless body area networks: Design, energy evaluation and proposed microprocessor design. *J. Med. Syst.* 35(5):1289–1298, 2011.
14. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., and Kwak, K.S., A comprehensive survey of wireless body area networks. *Comprehen. Survey Wireless Body Area Netw.* 36(3):1065–1094, 2012.
15. Al Ameen, M., Liu, J., and Kwak, K., Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.* 36(1):93–101, 2012.
16. Hu, C., Zhang, N., Li, H., Cheng, X., and Liao, X., Body area network security: A fuzzy attribute-based signcryption scheme. *IEEE J. Select. Areas Commun.* 31(9):37–46, 2013.
17. Bahrak, B., and Aref, M.R., Impossible differential attack on seven-round aes-128. *IET Inf. Secur.* 2(2):28–32, 2008.
18. Bechtsoudis, A., and Sklavos, N.: Side channel attacks cryptanalysis against block ciphers based on FPGA devices. In: *2010 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 460–461, 2006.
19. Zaidan, B.B., Haiqi, A., Zaidan, A.A., Abdulnabi, M., Kiah, M.L.M., and Muzamel, H., A security framework for nationwide health information exchange based on telehealth strategy. *J. Med. Syst.* 39(5):1–19, 2015.
20. Szaban, M., Nowacki, J., Drabik, A., Seredynski, F., and Bouvry, P., Application of cellular automata in symmetric key cryptography. In: Advances in Information Technology, ser. Communications in Computer and Information Science, Vol. 114, pp. 154–163. Berlin: Springer, 2010.
21. Nandi, S., Kar, B., and Pal Chaudhuri, P., Theory and applications of cellular automata in cryptography. *IEEE Trans. Comput.* 43(12):1346–1357, 1994.
22. *A New Kind of Science*. Champaign, Ilinois, US, United States: Wolfram Media Inc., 2002.
23. Kumar, S., Sharma, V., and Mahapatra, K.: An improved VLSI architecture of S-box for AES encryption. In: *2013 International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 753–756, 2013.
24. Rothaus, O., On bent functions. *J. Comb. Theory, Series A* 20(3):300–305, 1976.
25. Webster, A., and Tavares, S., On the design of S-Boxes. In: Williams, H. (Ed.) Advances in Cryptology CRYPTO 85 Proceedings, ser. Lecture Notes in Computer Science, Vol. 218, pp. 523–534. Berlin: Springer, 1986.
26. Adams, C., and Tavares, S., good S-Boxes are easy to find. In: Advances in Cryptology 'CRYPTO' Proceedings, ser. Lecture

Notes in Computer Science, Vol. 435, pp. 612–615. New York: Springer, 1990.

27. Hussain, I., Shah, T., Gondal, M.A., and Khan, W.A., Construction of cryptographically strong 8x8 S-boxes 1. *World Appl. Sci. J.* 13(11):2389–2395, 2011.
28. Clark, J.A., Jacob, J.L., and Stepney, S., The design of S– boxes by simulated annealing. *New Gen. Comput.* 23(3):219–231, 2005.
29. Millan, W., How to improve the nonlinearity of bijective S-Boxes. In: Proceedings of the Third Australasian Conference on Information Security and Privacy, ser. ACISP '98, pp. 181–192. London: Springer–Verlag, 1998.
30. Nedjah, N., and Mourelle, L.d.M., Designing substitution boxes for secure ciphers. *Int. J. Innov. Comput. Appl.* 1(1):86–91, 2007.
31. Kim, M., Ryou, J., Choi, Y., and Jun, S., Low power AES hardware architecture for radio frequency identification. In: Advances in Information and Computer Security, ser. Lecture Notes in Computer Science, Vol. 4266, pp. 353–363. Berlin: Springer, 2006.
32. Eslami, Y., Sheikholeslami, A., Gulak, P., Masui, S., and Mukaida, K., An area–efficient universal cryptography processor for smart cards. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* 44(1):43–56, 2006.
33. Sharma, T., and Thilagavathy, R.: Performance analysis of advanced encryption standard for low power and area applications. In: *2013 IEEE Conference on Information Communication Technologies (ICT),*, pp. 967–972, 2013.
34. Kaps, J.-P., and Sunar, B., Energy comparison of AES and SHA–1 for ubiquitous computing. In: Emerging Directions in Embedded and Ubiquitous Computing, ser. Lecture Notes in Computer Science, Vol. 4097, pp. 372–381. Berlin: Springer, 2006.
35. Satoh, A., Morioka, S., Takano, K., and Munetoh, S., A compact Rijndael hardware architecture with S–Box optimization. In: Advances in Cryptology ASIACRYPT 2001, Vol. 2248, pp. 239–254.