ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 2

Parity Based Fault Detection Approach for the Low Power S-Box and Inverse S-Box

P.Jemima Anlet, M.Jagadeeswari

***Abstract*— Advanced Encryption Standard (AES) has been made as the first choice for many critical applications because of the high level of security and the fast hardware and software implementations, many of which are power and resource constrained and requires reliable and efficient hardware implementations. In addition to the efficiency requirements of the AES, it must be reliable against transient and permanent internal faults or malicious faults aiming at revealing the secret key. In this paper, parity-based fault detection architecture of the S-box and the Inverse S-box for designing high performance fault detection structures of the AES is presented. The proposed parity-based fault detection approach is based on the low-cost composite field implementations of the S-box and the inverse S-box. Instead of using look-up tables for the S-box (Inverse S-box) and its parity prediction, logical gate implementations based on the composite field are utilized and hence the area gets reduced. This parity-based fault detection scheme reaches the maximum fault coverage when compared to other methods of fault detection. The proposed fault detection of the S-box and the inverse S-box in this paper have the least area and power consumption compared to their counterparts with similar fault detection capabilities.**

***Index Terms*— AES, fault coverage, low power, parity based fault detection, parity prediction, S-box**

I. Introduction

The Advanced Encryption Standard (AES) has been accepted by NIST [12] as the symmetric key standard as a replacement for the previous standards because of its good characteristics in terms of security, cost, and efficient implementations for encryption and decryption of blocks of data. In encryption, under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may be configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. After 10 rounds, the ciphertext is generated where each encryption round (except for the final round) consists of four transformations. The four transformations of round of encryption is explained below.

Manuscript received April 7, 2012.

***P.Jemima Anlet**, M.E. VLSI Design, Sri Ramakrishna Engineering College, Coimbatore, India, Mobile No. 08220937683, (e-mail: jemimaanlet.p1988@gmail.com).*

***M.Jagadeeswari**, Professor & Head, M.E. VLSI Design, Sri Ramakrishna Engineering College, Coimbatore, India, Mobile No. 09486355965, (e-mail: jagadee_raj@rediffmail.com).*

The 128 bits of input (and output) of each transformation are considered as a four by four matrix, called state, whose entries are eight bits. Except for the last round, the first transformation in each round is the bytes substitution, called SubBytes, which is implemented by 16 S-boxes. ShiftRows is the second transformation in which the four bytes of the last three rows of the input state are cyclically shifted. The third transformation is Mixcolumns in which the columns are considered as polynomials over $GF(2^8)$ and multiplied by a fixed polynomial. The final transformation is AddRoundKey in which a roundkey is added to the input by 128 two-input XOR gates.

Among the transformations in the AES, the S-boxes in the encryption and the inverse S-boxes in the decryption are alone nonlinear. Fault detection in the AES hardware implementation is important inorder to make the standard robust to the internal and malicious faults. There exists various fault detection schemes for the AES hardware implementation. For fault detection of the encryption or decryption in AES redundant units may be used [1], [14], where algorithm-level, round-level and operation-level concurrent error detection for the AES is used. A number of fault detection schemes based on the error detecting codes, also exists. In [3] the fault detection is achieved using LUTs. The scheme presented in [2] uses memories. For high performance AES implementations, using ROMs may not be preferable. The proposed fault detection approach is only applied to the composite field S-box and inverse S-box. There exist a number of fault detection approaches which are specific to composite field S-boxes and inverse S-boxes. In the scheme of [17], the fault detection of the multiplicative inversion of the S-box is considered. In [4], predicted parities have been used for the multiplicative inversion of a specific S-box using composite field and polynomial basis. Furthermore, the transformation matrices are also considered. In [4], [5] and [6], the composite field S-boxes and inverse S-boxes (using polynomial basis) have been divided into sub-blocks and parity predictions are used for their fault detection.

In the schemes proposed in [7] and [9], all the search space of composite fields is considered for presenting optimum lightweight fault detection schemes. The scheme presented in [8] is for all the transformations in the AES encryption/decryption independent of the ways these transformations are implemented. Moreover, the scheme presented in [13] uses double-data-rate computation for counteracting the fault attacks. Additionally, a fault detection scheme based on the Hamming and Reed-Solomon codes for protecting the storage elements within the AES is proposed in [10].

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 2

It is also noted that, for the logic elements, the scheme in [2] and the use of the partial duplication of the most vulnerable elements are proposed in [10].

All the S-boxes (respectively the inverse S-boxes) occupy much of the total AES encryption (respectively decryption) area and their power consumption is around three fourths of that of the entire AES [16]. LUTs can be utilized for the AES S-boxes and inverse S-boxes in hardware implementation. In this paper, the low-area implementation of the S-boxes and the inverse S-boxes using composite fields is focused. Moreover, the low-power S-box (respectively inverse S-box) presented in [16] uses composite fields. This paper involves the following

- The S-box and the inverse S-box has been designed to obtain low power and low area.
- Inorder to increase the error coverage, new formulations for the five predicted parities of the three blocks of the S-box (respectively the inverse S-box) has been obtained. The actual parity is obtained from the blocks using XOR gates. The predicted parity is compared with the actual parity. The error gets indicated using the error indication flag.
- The proposed fault detection scheme is simulated and maximum error coverage is obtained compared to existing methods.

It is shown that the power and area of the proposed technique is least compared to the schemes that have the same fault detection capabilities.

II. S-Box and Inverse S-Box in Composite Field

In this section, the S-box and the inverse S-box operations and their composite-field realizations are described. The S-box and the Inverse S-box are nonlinear operations which take 8-bit inputs and generate 8-bit outputs. In the S-box, the irreducible polynomial of $p(x) = x^8 + x^4 + x^3 + x + 1$ is used to construct the binary field $GF(2^8)$. Let $X = \sum_{i=0}^{7} x_i \alpha^i \in GF(2^8)$ and $Y = \sum_{i=0}^{7} y_i \alpha^i \in GF(2^8)$ be the input and the output of the S-box, respectively, where α is a root of $p(x)$, i.e. $p(\alpha)=0$. Then, the S-box consists of the multiplicative inversion, i.e., $X^{-1} \in GF(2^8)$, followed by an affine transformation. Moreover, let $Y \in GF(2^8)$ and $X \in GF(2^8)$ be the input and the output of the Inverse S-box, respectively. Then, the Inverse S-box consists of an inverse affine transformation followed by the multiplicative inversion. The composite fields can be represented using normal basis or polynomial basis. For the S-box using polynomial basis, the transformation matrix ψ transforms a field element X in the binary field $GF(2^8)$ to the corresponding representation in the composite fields $GF(2^8)$ / $GF(2^4)$. It is noted that the result of $X = \eta_h u + \eta_l$ is obtained using the irreducible polynomial $u^2 + \tau u + \upsilon$. The multiplicative inversion consists of composite field multiplications, additions and an inversion in the sub-field $GF(2^4)$ over $GF(2) / x^4 + x + 1$.

The decomposition can be further applied to represent $GF(2^4)$ as a linear polynomial over $GF(2^2)$ and then $GF(2)$ using the irreducible polynomial $\upsilon^2+\Omega\upsilon+\varphi$ and w^2+w+1, respectively. As a result, it is understood that the implementation of the multiplicative inversion can be performed using the field represented by $GF((2^4)^2)$ or the field represented by $GF(((2^2)^2)^2)$. For calculating the multiplicative inversion, the most efficient choice is to let $\Omega = \tau = 1$ in the above irreducible polynomials. Then, the multiplicative inversion of the S-box using polynomial basis is given by,

$$(\eta_h u + \eta_l)^{-1} = [((\eta h + \eta_l) + \eta_h^2 \upsilon)^{-1} \eta_h] u + ((\eta h + \eta_l) + \eta_h^2 \upsilon)^{-1} (\eta_h + \eta_l) \quad (1)$$

It is noted that η can be replaced with σ to obtain the multiplicative for the Inverse S-box.

III. Proposed S-box and Inverse S-Box and its Power Optimization

The structure of the S-box and the inverse S-box in composite field is shown in the Fig.1. The S-box and the inverse S-box has been divided into 3 blocks as shown in the Fig.1. The transformation matrix converts the 8-bit binary input to the elements in the composite field, $GF(2^8)$. The Lambda-Squarer represents the squaring in the composite field $GF(2^4)$ followed by the multiplication with the irreducible polynomial $u^2+u+\upsilon$. The multiplication and inversion in Fig.1 indicates the multiplication and inversion operation in the composite field $GF(2^4)$ respectively. The outputs of the three blocks for S-box are represented as below.

$B1 = \gamma\ (\gamma')$
$B2 = \theta\ (\theta')$
$B3 = Y(X)$

The letters in parenthesis indicate the outputs of the inverse S-box.

The implementation complexities of different blocks of the S-box and the Inverse S-box and those for their predicted parities are dependent on the choice of the coefficients $\upsilon \in GF(2^4)$ and $\varphi \in GF(2^2)$ in the irreducible polynomials $u^2 + u + \upsilon$ and $v^2 + v + \varphi$ used for the composite fields. The goal in the following is to find $\upsilon \in GF(2^4)$ and $\varphi \in GF(2^2)$ for the composite fields $GF(((2^2)^2)^2)$ and $\upsilon \in GF(2^4)$ for the composite fields $GF((2^4)^2)$ so that the area complexity of the entire fault detection implementations becomes optimum. According to [19], 16 the possible combinations for $\upsilon \in GF(2^4)$ and $\varphi \in GF(2^2)$ exist. Moreover, for the composite fields $GF((2^4)^2)$, the possible choices for υ making the polynomial $x^2 + x + \upsilon$ irreducible has been exhaustively searched and found. Some single faults may lead to even number of erroneous bits in the output of the blocks in Fig. 1. Then, the parity-based fault detection scheme will not be able to detect such faults if one uses the predicted parity of the corresponding block.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 2

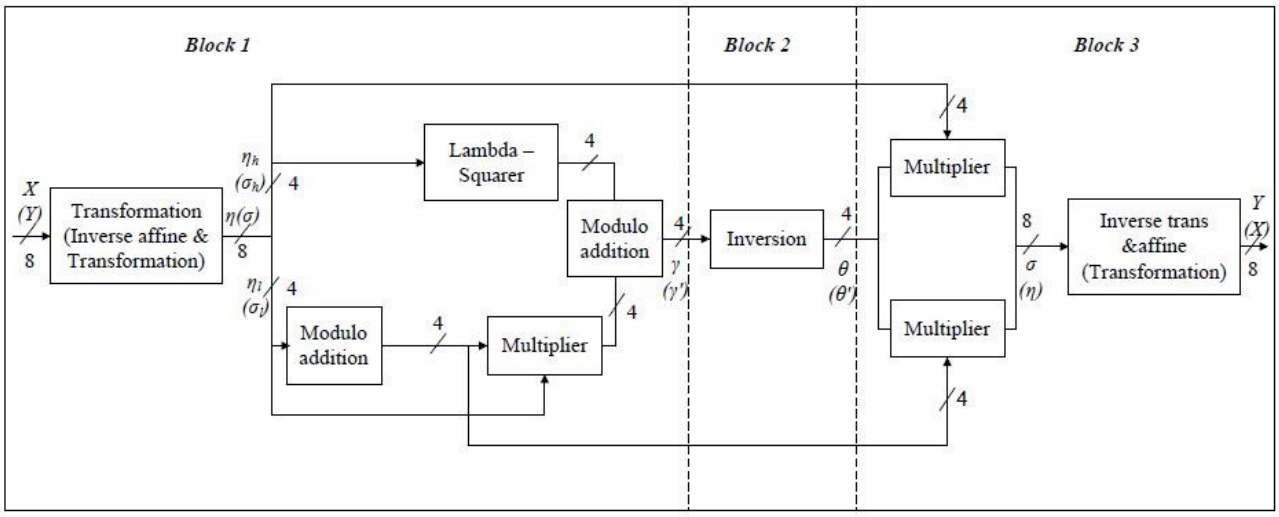

Fig. 1 Structure of the S-Box and the Inverse S-Box Using Composite Field Arithmetic

Thus, in order to detect all single faults in each block using the parity prediction scheme, each block of the S-box is modified so that all single faults lead to odd number of errors in the output. To do so, the following remark for each block is applied.

Remark1: Consider a circuit which only consists of XOR (and XNOR) gates and the number of paths from each gate to the output bits is odd. Then, the number of erroneous bits will be odd for each single fault occurred in that circuit.

For the purpose of reaching low-power architecture with acceptable hardware complexity, it is suggested in [16] that the structures are partitioned into three blocks as in Fig. 2. Then, the logic gates within each of these blocks are implemented using two-level logics consisting of the arrays of ANDs and XORs. Although this method increases the area of the composite field implementation, it reduces the power consumption significantly [16].

The AND-XOR structure of each block shown in Fig. 2 results in minimum number of transitions and thus low-power consumption is achieved. This is because the AND array has 50 percent propagation probability of signal transitions.

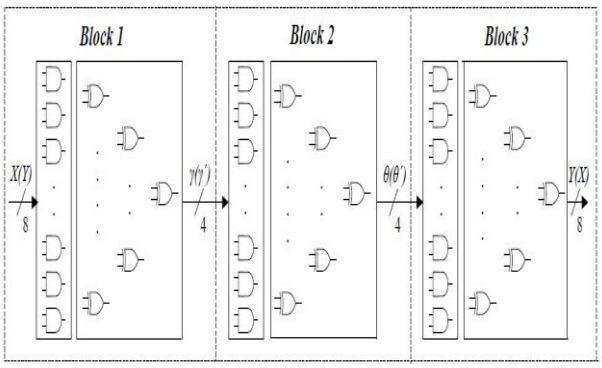

Fig. 2 Proposed Low Power Architecture for S-box and Inverse S-box

As seen in Figs. 1 and 2, for block 1, a field element X for the S-box (Y for the inverse S-box) in the binary field $GF(2^8)$ is converted to the corresponding representation in the composite field $GF(2^8)$ / $GF(((2^2)^2)^2)$. The output of block 1 is then obtained as $\gamma \in GF(2^4)$ and $\gamma' \in GF(2^4)$ for the inverse S-box. The output of block 2 is obtained as $\theta \in GF(2^4)$ for the S-box and $\theta' \in GF(2^4)$ for the inverse S-box. Eventually, using the irreducible polynomials $u^2+u+\upsilon$ and $v^2 + v + \varphi$, the output of the S-box, i.e., Y and X for the inverse S-box, is obtained after conversion from the composite field $GF(2^8)$ / $GF(((2^2)^2)^2)$ to the binary field $GF(2^8)$.

IV. Parity Based Fault Detection

In the parity based fault detection schemes, the parity of a block is predicted and compared with the actual parity of the block. The result is the error indication flag of the corresponding block which alarms the detected faults. In the presented parity-based fault detection scheme, we divide the structures of the S-box and the inverse S-box using polynomial basis into 3 blocks as shown in Fig. 1 so that it can also be used for the low-power structures presented in [16]. It can be seen that, in the S-box and inverse S-box presented in Fig. 1, blocks 1 and 3 occupy around 86 percent of the area of the entire operations [18]. Therefore, these two blocks are more susceptible to the internal faults and more prone to fault attacks. Hence, two bits predicted parities for each of these two blocks is proposed. Furthermore, one predicted parity is used for block 2. The details of the proposed scheme are presented below.

A. S-Box

In the proposed technique, five predicted parities are derived for three blocks of the S-box. Then, by comparing these with the five actual parities, five error indication flags are obtained.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 2

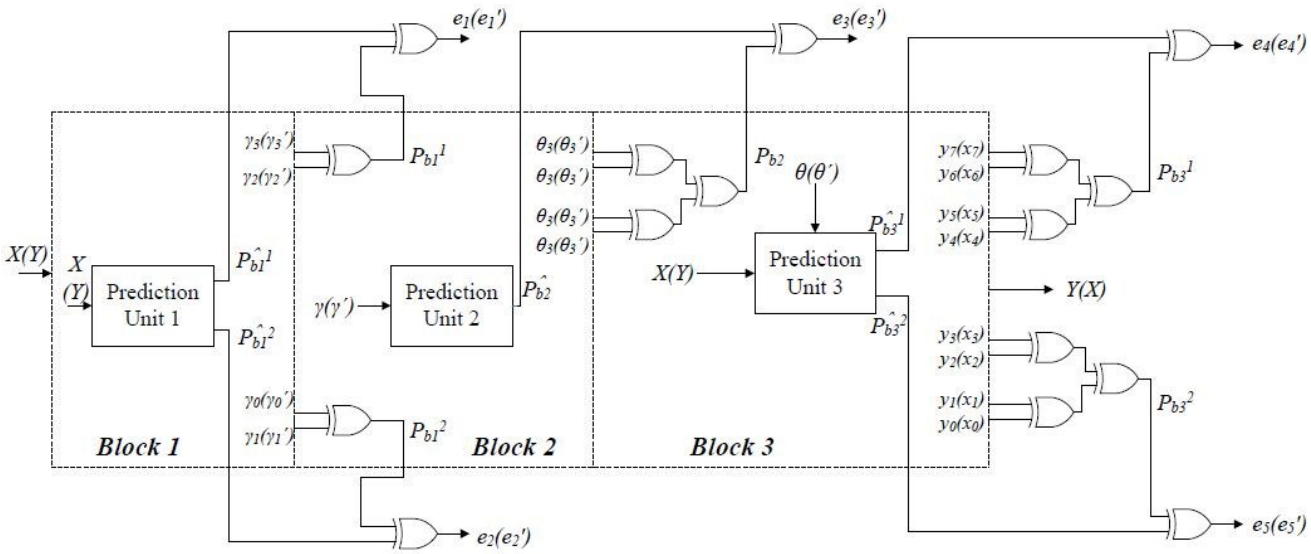

Fig. 3 Proposed Parity based fault detection structure of the low power S-box and the Inverse S-box

All five flags should be zero for the error free computations. The proposed fault detection scheme for the S-box is shown in Fig. 3. As seen in this figure, for block 1, two predicted parities, i.e., $\hat{P}_{b1}{}^1$ and $\hat{P}_{b1}{}^2$, are obtained using the Prediction Unit 1. As seen from Fig. 3, the predicted parity of the second block, $\hat{P}_{b2}$ is obtained by the Prediction Unit 2. Also, for block 3, two predicted parities, i.e., $\hat{P}_{b3}{}^1$ and $\hat{P}_{b3}{}^2$, are derived using the Prediction Unit 3.

The derivations of the actual parities are also shown in Fig.3. As seen from Fig. 3, two actual parities for the two most and the least significant bits of γ, i.e., $P_{b1}{}^1 = \sum_{i=2}^{3} \gamma_i$ and $P_{b1}{}^2 = \sum_{i=0}^{1} \gamma_i$, have been derived from the output of block 1 using two trees of XOR gates. Similarly, as shown in Fig. 3, the two actual parities for block 3 are obtained from the output of block 3 for the four most and least significant bits of Y, i.e., $P_{b3}{}^1 = \sum_{i=4}^{7} y_i$ and $P_{b3}{}^2 = \sum_{i=0}^{3} y_i$. In addition, an actual parity is obtained for block 2 as $P_{b2} = \sum_{i=0}^{3} \theta_i$. Then, as shown in Fig. 3, by comparing the predicted and actual parities, the error indication flags of three blocks, i.e., *e1-e5*, are obtained.

The following lemma is used from [18] for the multiplication in $GF((2^2)^2)$ used in blocks 1 and 3. Then, using this lemma, the predicted parities for the S-box in Fig. 3 are derived.

Lemma 1: Let $U = (u_3, u_2, u_1, u_0)$ and $V = (v_3, v_2, v_1, v_0)$ be the inputs of a multiplier in $GF((2^2)^2)$. Then, the result of multiplication, i.e., $Z = UV$, is

$$z_3 = u_3 (v_3 + v_2 + v_1 + v_0) + u_2 (v_3 + v_1) + u_1 (v_3 + v_2) + u_0 v_3$$
$$z_2 = u_3 (v_3 + v_1) + u_2 (v_2 + v_0) + u_1 v_3 + u_0 v_2$$
$$z_1 = u_3 v_2 + u_2 (v_3 + v_2) + u_1 (v_1 + v_0) + u_0 v_1$$
$$z_0 = u_3 (v_3 + v_2) + u_2 v_3 + u_1 v_1 + u_0 v_0$$

Using Lemma 1, we present the formulations for these five predicted parities in the following theorem.

Theorem 1: Let $X \in GF(2^8)$ be the input of the S-box. Then, the five predicted parities of the three blocks of the S-box in Fig. 3, i.e., $\hat{P}_{b1}{}^1$, $\hat{P}_{b1}{}^2$, $\hat{P}_{b2}$, $\hat{P}_{b3}{}^1$, $\hat{P}_{b3}{}^2$ are obtained as follows:

$$\hat{P}_{b1}{}^1 = x_7 (D + x_5) + x_4 B + x_3 (B + x_4) + x_0 D + x_1 x_2 \quad (2)$$
$$\hat{P}_{b1}{}^2 = x_7 (G + x_6) + x_4 I + x_1 (C + E) + x_2 \vee x_5 + P_x \quad (3)$$
$$\hat{P}_{b2} = (\overline{\gamma_2} \vee \gamma_1)\, \gamma_0 + (\gamma_1 + \gamma_0)\, \gamma_3 \quad (4)$$
$$\hat{P}_{b3}{}^1 = \theta_3 H + \theta_2 (G + x_7) + \theta_1 (J + C) + \theta_0 J \quad (5)$$
$$\hat{P}_{b3}{}^2 = \theta_3 (C + x_0) + \theta_2 (H + x_3) + \theta_1 (I + x_7) + \theta_0 (A + x_2) \quad (6)$$

where $x_1 + x_6 = A$, $x_5 + A = B$, $x_3 + x_2 = C$, $P_x + H = D$, $x_0 + x_6 = E$, $x_2 + x_5 = F$, $F + x_4 = G$, $x_0 + x_7 = H$, $B + C = I$, $E + F = J$. Furthermore, "+" and $\vee$ represent the modulo-2 addition using an XOR gate and the OR operation, respectively. Moreover, $P_x = \sum_{i=0}^{7} x_i$. The proof for the predicted parities is given in [11].

B. Inverse S-Box

As seen in Fig. 3, similar to the S-box, for blocks 1-3 of the inverse S-box, five predicted parities are derived using the parity prediction units. This is also depicted in Fig. 3. It is noted that the notations for the inverse S-box are denoted by parentheses to be contrasted from those for the S-box. Additionally, similar to the S-box, the actual parities of the three blocks for the inverse S-box are derived using XOR trees. The actual parities blocks 1 and 3 are obtained as follows $P_{b1}{}^1 = \sum_{i=2}^{3} \gamma'_i$ and $P_{b1}{}^2 = \sum_{i=0}^{1} \gamma'_i$ for block 1 and $P_{b3}{}^1 = \sum_{i=4}^{7} x_i$ and $P_{b3}{}^2 = \sum_{i=0}^{3} x_i$ for block 3. Also for block 2 the actual parity is calculated as $P_{b2} = \sum_{i=0}^{3} \theta'_i$. Then, as seen in Fig. 3, by comparing the predicted and actual parities, five error indication flags of three blocks, i.e., *e1' − e5'*, are obtained.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 2

Using Lemma 1 and considering Theorem 1, the formulations for the five predicted parities of the inverse S-box for the three blocks shown in Fig. 3 is obtained as follows.

Theorem 2: Let $Y \in GF(2^8)$ be the input of the inverse S-box. The five predicted parities of the three blocks of the inverse S-box in Fig. 3 are obtained as follows:

$$\hat{P}_{b1}^{1} = y_0 e + y_5 (y_4 + y_3 + a) + y_2 b + y_7 y_4 + \bar{b} \quad (7)$$

$$\hat{P}_{b1}^{2} = y_1 (y_7 + y_5 + h) + y_2 a + y_3 (y_5 + y_4) + y_5 h + y_0 + e \quad (8)$$

$$\hat{P}_{b2} = (\overline{\gamma_2}' \vee \gamma_1') \gamma_0' + (\gamma_1' + \gamma_0') \gamma_3' \quad (9)$$

$$\hat{P}_{b3}^{1} = \theta_3' \bar{f} + \theta_2' (\overline{P_y} + d + y_7) + \theta_1' (\bar{c} + y_7 + y_4) + \theta_0' (\bar{a} + y_4 + y_2) \quad (10)$$

$$\hat{P}_{b3}^{2} = \theta_3' (y_1 + d) + \theta_2' (y_0 + g) + \theta_1' (y_6 + g) + \theta_0' (y_1 + f) \quad (11)$$

where $y_6 + y_7 = a$, $y_1 + a = b$, $y_1 + y_2 = c$, $y_3 + y_6 = d$, $c + d = e$, $P_y + y_4 + y_6 = g$, *and* $y_4 + y_0 = h$. Furthermore, "+" and $\vee$ represent the modulo-2 addition using an XOR gate and the OR operation, respectively. Also, $P_y = \sum_{i=0}^{7} y_i$. The proof of the parity prediction is in [11].

C. Error Indication

In order to develop a fault detection structure, the predicted parity can be compared with the actual parity in order to obtain the error indication flag of the corresponding block. By ORing five indication flags of five blocks, the error indication of the entire S-box is obtained [15].

V. Simulation Results

First the S-box and the Inverse S-box are constructed using logic gates for low power and fault detection. Then, single Struck-At-Faults have been introduced to the S-box and the Inverse S-box and the corresponding output simulation is obtained. After that the circuit is tested for multiple Struck-At-Faults. Xilinx ISE is used as the simulation tool. The target device used is Spartan 3A. Finally, the error coverage has been calculated from the obtained results. The design is also simulated for power, delay and area calculations. From the simulation result the following is inferred.

A. Low Area and Low Power

From the synthesis report, the number of LUTs and slices needed to design the S-box and the Inverse S-box is calculated. Table I gives the comparison of the number of LUTs and slices used for the design of S-box and Inverse S-box using various techniques.

TABLE I
Comparison of LUTs and Slices

	No. of 4-input LUTs	No. of Slices
LUT based S-box	250	158
LUT based Inverse S-box	250	158
Composite S-box	83	43
Composite Inverse S-box	73	38
Proposed low power S-box	**87**	**46**
Proposed low power Inverse S-box	**84**	**44**

From the Table I the number of LUTs and Slices used for low power S-box and Inverse S-box is slightly higher than the composite field S-box, but less when compared to S-box based on LUTs.

Table II illustrates the comparison results based on simulation in terms of power.

TABLE II
Comparison of Power

Technique	Power (mW)
LUT based S-box	56
LUT based Inverse S-box	56
Composite S-box	44
Composite Inverse S-box	46
Low power S-box	**28**
Low power Inverse S-box	**29**

From the table it is seen that the power of the proposed low power S-box is the least compared to other techniques.

The comparison result for delay is shown in Table III. From the table it is inferred that the delay is increased. But the power delay product for the low power S-box and Inverse S-box is better when compared to other techniques and is shown in Table IV.

TABLE III
Comparison of Delay

Technique	Delay (ns)		
	Gate Delay	Net Delay	Total Delay
LUT based S-box	4.612	3.653	8.256
LUT based Inverse S-box	4.612	3.653	8.256
Composite S-box	9.143	7.725	16.868
Composite Inverse S-box	8.500	7.566	16.066
Proposed low power S-box	**8.485**	**6.830**	**15.313**
Proposed low power Inverse S-box	**8.224**	**6.968**	**15.192**

TABLE IV
Comparison of Power –Delay Product

Technique	Power-Delay Product
LUT based S-box	462.336
LUT based Inverse S-box	462.336
Composite S-box	742.192
Composite Inverse S-box	739.036
Proposed low power S-box	**428.764**
Proposed low power Inverse S-box	**440.568**

B. Fault Detection

The proposed architecture for the S-box and Inverse S-box is able to find all the single Struck-At faults. Faults are injected randomly on the input and output nodes of the logic gates. In the case of multiple Struck-At faults in S-box, 50 multiple SA faults have been injected and 49 faults have been identified.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 2

At the maximum, 20 nodes have been made faulty for a single multiple SA fault. In the Inverse S-box out of the 50 multiple SA faults injected 48 faults have been identified. The error coverage is given in table V.

TABLE V
ERROR COVERAGE

Faults	Error Coverage
Single SA fault in S-box	100%
Multiple SA fault in S-box	98%
Single SA fault in Inverse S-box	100%
Multiple SA fault in the inverse S-box	96%

From the above simulation results, it has been found that the error coverage is approximately 97%. The total area cost of the proposed fault detection scheme in the S-box and inverse S-box is much less than the scheme based on LUTs. Also, low power is achieved in the proposed method with a slight increase in delay when compared to LUTs.

VI. CONCLUSION

In this paper, low power S-box and the Inverse S-box has been designed. Parity based fault detection scheme for the low power S-box and the Inverse S-box is presented inorder to find the faults in the hardware implementation of the S-box and the Inverse S-box. Instead of using the look-up table approach for the implementation of the S-box and its parity prediction, the composite field arithmetic with logical gates is used. Using exhaustive searches, the least complexity S-boxes and Inverse S-boxes as well as their fault detection circuits is found. Simulation results show that very high error coverage for the presented scheme is obtained when compared to other fault detection schemes like those based on LUTs and redundant units. Also low power and low area is achieved when compared to previous methods.

ACKNOWLEDGMENT

The authors thank the Management and Principal of Sri Ramakrishna Engineering College, Coimbatore for providing excellent computing facilities and encouragement.

REFERENCES

[1] H. Yen and B. F. Wu, "Simple error detection methods for hardware implementation of advanced encryption standard," *IEEE Trans. Computers*, vol. 55, no. 6, pp. 720-731, June 2006.

[2] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," *IEEE Trans. Computers*, vol. 52, no. 4, pp. 492–505, Apr. 2003.

[3] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri and V. Piuri, "A parity code based fault detection for an implementation of the advanced encryption standard," *Proc. of IEEE Int'l Symp., Defect and Fault Tolerance in VLSI Systems (DFT '02)*, pp. 51-59, Nov. 2002.

[4] M. Mozaffari Kermani and A. Reyhani-Masoleh, "Parity Prediction of S-box for AES," *In Proc. of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2006)*, pp. 2357-2360, May 2006.

[5] M. Mozaffari Kermani and A. Reyhani-Masoleh, "Parity-based fault detection architecture of S-box for advanced encryption standard," *In Proc. of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT 2006)*, pp. 572-580, Oct. 2006.

[6] M. Mozaffari Kermani, "Fault Detection Schemes for High Performance VLSI Implementations of the Advanced Encryption Standard," *M.E.Sc. Thesis*, Department of Electrical and Computer Engineering, The University of Western Ontario, London,Ontario, Canada, April 2007.

[7] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A Lightweight Concurrent Fault Detection Scheme for the AES S-boxes Using Normal Basis," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '08), pp. 113-129, Aug. 2008

[8] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard," IEEE Trans. Computers, vol. 59, no. 5, pp. 608-622, May 2010.

[9] Mentens, N. Batina, L. Preneel, B. and Verbauwhede, I. "A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-box", Proc. CT-RSA, pp. 323–333, 2005

[10] Moratelli, F. Ghellar, E. Cota, and M. Lubaszewski, "A Fault- Tolerant DFA-Resistant AES Core," Proc. IEEE Int'l Symp. Circuits and Systems (ISCAS '08), pp. 244-247, May 2008.

[11] Mozaffari-Kermani, M. and Reyhani-Masoleh, A. "A Low-Power High-Performance Concurrent Fault Detection Approach for the Composite Field S-Box and Inverse S-Box", IEEE transactions on computers, vol. 60, no. 9, September 2011, pp. 1327-1340, September 2011.

[12] National Institute of Standards and Technologies, Announcing the Advanced Encryption Standard (AES) FIPS 197, Nov. 2001

[13] P. Maistri and R. Leveugle, "Double-Data-Rate Computation as a Countermeasure against Fault Analysis," IEEE Trans. Computers, vol. 57, no.11, pp. 1528-1539, Nov. 2008.

[14] R. Karri, K. Wu, P. Mishra, and K. Yongkook, "Fault-based Side-Channel Cryptanalysis Tolerant Rijndael Symmetric Block Cipher Architecture," *Proc. IEEE Int'l Symp. Defect and Fault Tolerance in VLSI Systems (DFT '01)*, pp. 418-426, Oct.2001

[15] Reyhani-Masoleh, A. and Hasan, M.A. (2006) 'Fault Detection Architectures for Field Multiplication Using Polynomial Bases', IEEE Trans. on Computers, Vol. No.55, no. 9, pp. 1089-1103.

[16] S. Morioka and A. Satoh, "An Optimized S-Box Circuit Architecture for Low Power AES Design," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '02), pp. 172-186, Aug. 2002.

[17] S.Y. Wu and H.T. Yen, "On the S-Box Architectures with Concurrent Error Detection for the Advanced Encryption Standard", *IEICE Trans. On Fundamentals of Electronics, Communications and Computer Sciences*, vol. E89-A, no. 10, pp.2583-2588, Oct. 2006

[18] Satoh, A. Morioka, S. Takano, K. and Munetoh, S. "A Compact Rijndael Hardware Architecture with S-box Optimization", Proc. ASIACRYPT 2001, Gold Coast, Australia, pp. 239-254.

[19] Zhang, X. and Parhi, K.K. (2006) "On the Optimum Constructions of Composite Field for the AES Algorithm", *IEEE Trans. Circuits Syst. II, Exp. Briefs*, Vol. No. 53, no. 10, pp. 1153–1157.

P.Jemima Anlet received her B.E. degree in Electronics and Communication Engineering at V.P.M.M. Engineering College for Women, Srivilliputhur, India in the year 2010. She is currently pursuing her M.E. degree in VLSI Design at Sri Ramakrishna Engineering College, Coimbatore, India. Her area of research interest includes Cryptography, Computer Networks and VLSI Testing.

M.Jagadeeswari received her B.E Electronics and Communication Engineering from Government College of Technology, Coimbatore and ME (Applied Electronics) from P.S.G College of Technology, Coimbatore in the year 1992 and 1999 respectively. She has completed her Ph.D from Anna University, Chennai, India in 2010. She is presently working as Professor and head in the department of Electronics and Communication Engineering (PG) at Sri Ramakrishna Engineering College, Coimbatore, India. She has published more than 25 research papers in the National & International Journals/ Conferences. Her research interests are VLSI design, Hardware Software co-design, Computer architecture and Genetic algorithms.