IJRSET Volume 2, Issue 4 Pages: 32-42
ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

VLSI Based Minimized Composite S-Box and Inverse Mix Column for AES Encryption and Decryption

[1] J. Balamurugan, [2] Dr. E. Logashanmugam
[1] Research scholar, [2] Professor and Head,
[1] St. Peter's University, [2] Sathyabama University,
[1&2] Chennai, Tamilnadu, India.

Abstract:-

Advanced Encryption Standard (AES) is one of the best cryptography algorithms in secured data communication. Due to provide efficient security, AES consumes more hardware complexity and power consumption.

In addition, speed of the AES is low due to complexity in data flow path. Substitution Box (S-Box), Shift Rows, MixColumn multiplication and Add Round Key are the four fundamental steps in AES algorithm. Among those four steps, S-Box and Inverse MixColumn multiplication (decryption of MixColumn) are recognized as a high potential steps, because both S-Box and MixColumn multiplication consumes more hardware complexity and power consumption. In this paper, Enhanced Inverse MixColumn multiplications are used to reduce the hardware complexity of AES algorithm. In addition to enhanced Inverse MixColumn multiplications, architecture of composite S-Box is realized to minimize the hardware complexity of AES. Further minimized composite S-Box and enhanced Inverse MixColumn multiplication transformations are integrated into AES algorithm to increase the efficiency of AES in terms of less area utilization, high speed and low power consumption. Implementation of minimized AES composite S-Box and enhance inverse MixColumn transformations are done in the field of Very Large Scale Integration (VLSI).

Keywords: - Minimized Composite S-Box, Enhanced Inverse MixColumn transformation, Advanced Encryption Standard (AES), Reduced Xtime multiplication, Very Large Scale Integration (VLSI).

1. INTRODUCTION

In the perspective of technology growth, security also plays an important role. For instance, a mail delivery System and banking system has a large demand for best crypto algorithm. With ever increasing more mobile products, high speed and low on-chip area cryptography algorithms are necessary. Advanced Encryption Standard (AES) meets this requirement efficiently and this algorithm has been suggested by several endeavours to meet the best crypto mechanism. In AES encryption algorithm four types of transformations are suggested to encrypt the input data, these are

- Substitution Box (S-Box)
- Shift Rows () transformation
- MixColumn () transformation
- Add Round Key () transformation

Similarly, reverse processes are suggested in decryption side of AES transformation, these are

- Inverse Shift Rows (Inv Shift Rows ())
- Inverse S-Box (Inv S-Box)
- Inverse MixColumn (Inv MixColumn ())
- Add Round Key ()

Among those transformations, S-Box, Inv S-Box and Inv MixColumn transformations have more complexity than other transformation. Composite S-box has been suggested at the past, in which single circuit can control both S-Box and Inv S-Box transformations. Large endeavours have been designed the circuit of composite S-Box. The substitution table is generated by two processes named as Multiplicative Inverse (MI) and Affine transformation (AT). Most of the works uses the Look up Tables (LUTs) and Memories to process the S-Box of AES. But in [1], [5], [6] and [7], combinational logic circuits are used to provide the substitution table. This combinational circuit is based on both MI and AT techniques. In [1], Complementary Metal Oxide Semiconductor (CMOS) is used to design the combinational transformation is used to improve the performance of MixColumn transformation. Finally, both enhanced Inv MixColumn and minimized Composite S-Box are incorporated into AES encryption and decryption process.

2. AES ALGORITHM

AES is a Rijndael algorithm selected for data encryption standard by National Institute of Standards and Technology (NIST) in 1997. In general, it processes data blocks of fixed size using cipher keys of length 128, 196 and 256 bits. But, 128 bit AES are widely used for the design of encryption and decryption. Encryption of AES performs 4 types of transformation. (1) AES S-Box: Substitute the values which are derived from MI and AT transformation process. (2) AES Shift Rows (): Shift the Rows of bytes circularly in a certain principle [2]. (3) AES Inv MixColumn (): Multiplication is performed by a constant matrix [9]. (4) AES Add Round Key: N number of round can be performed in different word length of AES. For instance, N = 10 for AES 128 bit cipher keys, N = 12 for AES 196 bit cipher keys and N = 14 for AES 256 bit cipher keys. S-Box of AES is generated by taking MI of data input in the finite Galois Field GF (2^8) and it followed by an affine transformation. State bytes of the S-Box transformation results are shifted by Shift Rows transformation. Next to Shift Rows transformation, MixColumn transformation can be performed by making a multiplication with constant matrix. The constant matrix for MixColumn transformation is illustrated in equation (1).

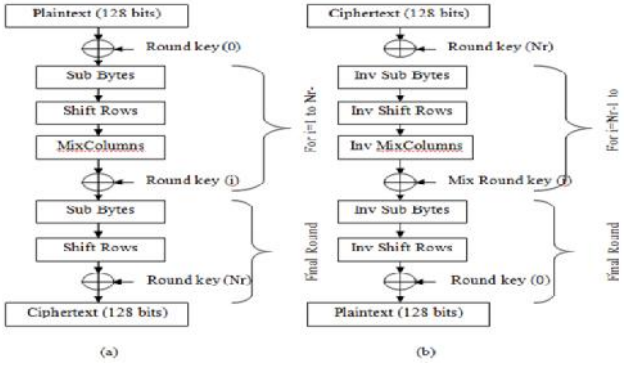

Figure: 1 Generalized AES structure (a)Encryption(b)Decryption.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 01 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 01 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad (1)$$

In Add Round Key transformation, 10 rounds of processes (above mentioned three transformations) can be performed, since here AES-128 bit length is considered for both encryption and decryption. Similar to encryption, decryption has reverse process of those mentioned four transformations such as Inv Shift Rows (), Inv S-Box (), Inv MixColumn (), and Add Round Key. The generalized AES flow for encryption and decryption is illustrated in fig. 1. Inv S-Box has same potential as S-Box transformation. But, Inv MixColumn transformation has more potential than MixColumn transformation. The constant matrix for Inv MixColumn transformation is illustrated in equation (2).

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad (2)$$

Since, from above analysis, it is clear that, S-Box and Inv MixColumn transformation processes consumes more hardware complexity and power consumption than other part of AES. Therefore to improve the architecture of AES and security, enhanced Inv MixColumn and minimized structure of S-Box/Inv S-Box are designed in this paper. Multiplexor of Composite S-Box controls the operation of both S-Box and Inv S-Box. When performing encryption operation, Multiplexor gives the control signal as 0 and it allows the input to the Multiplicative Inverse and Affine Transformation blocks sequentially to perform the S-Box transformation. Similarly, when performing decryption operation, Multiplexor gives the control signal as 1 and it allows the input to the Inv Affine Transformation and Multiplicative inverse blocks sequentially. Multiplicative Inverse (MI) unit require more hardware than other blocks. The block diagram of Multiplicative Inverse is illustrated in fig. 3.

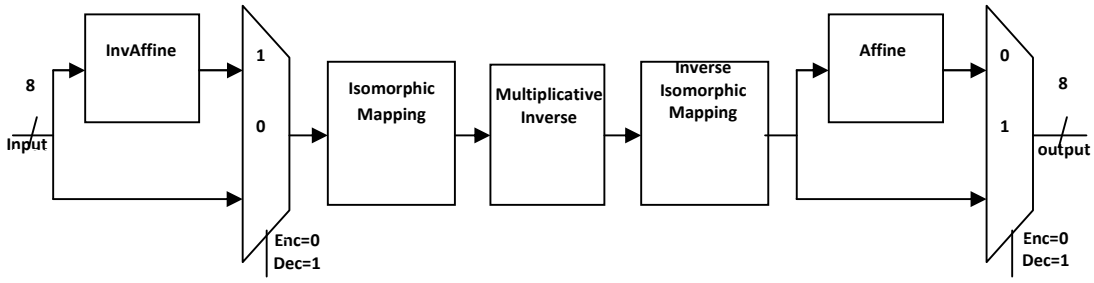

Figure: 2 Block diagram of Composite S-Box

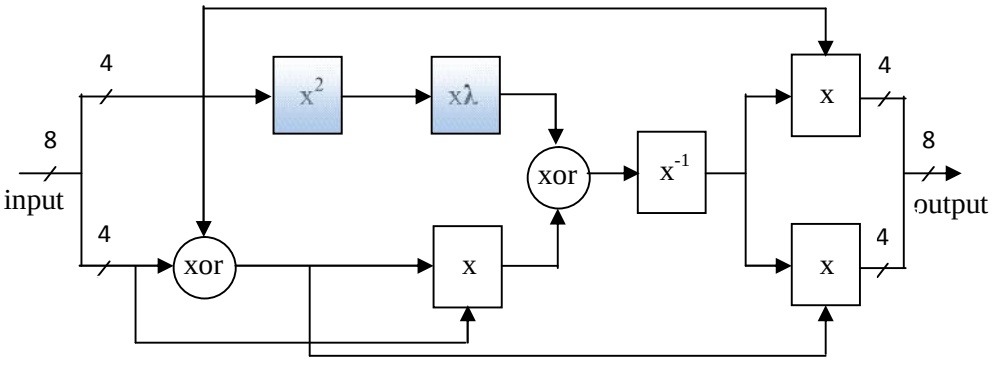

Figure: 3 Block diagram of Multiplicative Inverse

As per the diagram, input and output of MI unit has 8-bit word length. The intermediate operation for MI unit is shown in fig. 3. As per the rule, it requires inverse multiplication to compute the

multiplicative inverse of any input. Inverse multiplication is indicated as x^{-1}. Before performing the inverse multiplications, having some logical operations to be convert the data into a certain formation. These logic computations disturb the performance of MI in terms of VLSI concerns, i.e. requirement of less hardware complexity and lower power consumption. The block diagram of square of x (x^2) and Multiplication with constant (^{a}) is illustrated in fig. 4 and fig. 5 respectively.

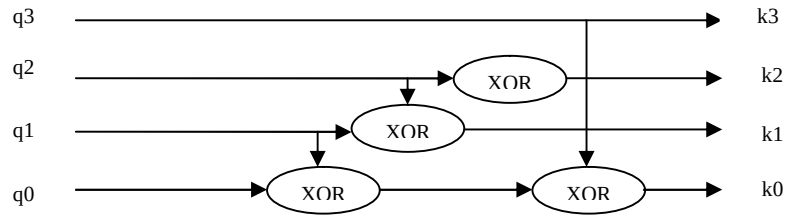

Fig. 4 Multiplication of X^2

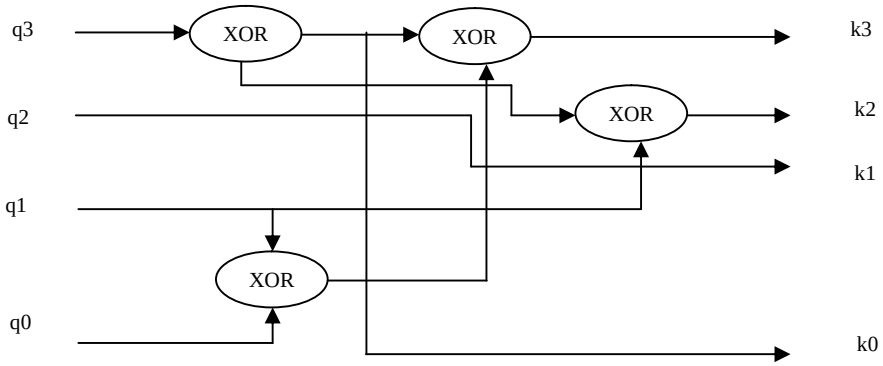

Figure: 4 Multiplication of X^a

Multiplication of X^2 require the 4 number of XOR gates and Multiplication of X^a requires the 4 number of XOR gates to produce the sufficient information which suited for inverse multiplication. Hence, 8 number of logic gates are required to produce the sufficient data for inverse multiplication. This multiplicative inverse block serves for both encryption and decryption.

4. PROPOSED COMPOSITE AES S-BOX

Composite AES S-Box for both AES encryption and AES decryption is represented in fig. 3. In that architecture, Multiplicative Inverse unit is recognized as a high potential for more hardware complexity. MI architecture consists of multiplication of X^2 and multiplication of X^a. The architecture of both X^2 and X^a is illustrated in fig. 4 and fig. 5 respectively. In this proposed model, redundant operation of both multiplication of X^2 and multiplication of X^a are identified to further reduce the hardware complexity of Composite S-Box. Redundant operations of multiplications are identified through following equations.

Let as input of multiplication X^2 as q3, q2, q1 and q0. Similarly, corresponding output of multiplication of X^2 as k3, k2, k1 and k0 respectively. These should be derived with the help of fig. 4. Equation representation (3) to (6) gives the output of multiplication of X^2

$$k3 = q3 \tag{3}$$

$$k2 = q3 \oplus q2 \tag{4}$$

$$k1 = q2 \oplus q1 \tag{5}$$

$$k0 = q3 \oplus q1 \oplus q0 \quad (6)$$

Similarly, let as input of multiplication X^a as q3, q2, q1 and q0, corresponding output of multiplication of X^a as K3, K2, K1 and K0 respectively. These should be derived with the help of fig. 5. Equation representation (7) to (10) gives the output of multiplication of X^a .

$$K3 = q0 \oplus q1 \oplus q2 \oplus q3 \quad (7)$$

$$K2 = q1 \oplus q3 \quad (8)$$

$$K1 = q2 \quad (9)$$

$$K0 = q2 \oplus q3 \quad (10)$$

In our proposed work, we combine these two multiplications and get the minimized circuit which is obtained by following simplifications. From equation (7) and equation (3) to (6), we can also write,

$$K3 = q0 \oplus q1 \oplus q3 \oplus q2 \oplus q1 \oplus q2 \oplus q3 \oplus q3$$

We know that, A XOR A = 0. Hence, we get,

$$K3 = q0 \oplus q3 \quad (11)$$

From equation (8) and equation (3) to (6), we can also write,

$$K2 = q1 \oplus q2 \oplus q3 \quad (12)$$

From equation (9) and equation (3) to (6), we can also write,

$$K1 = q2 \oplus q3 \quad (13)$$

From equation (10) and equation (3) to (6), we can also write,

$K0 = q2 \oplus q3 \oplus q3$ Hence, we get,

$$K0 = q2 \quad (14)$$

From equation (12) and equation (13), a common factor $q2 \oplus q3$ can be repeated. Hence, we can reuse the same resource for both of the place.

Let $h = q2 \oplus q3$ Therefore finally, we get,

$$K3 = q0 \oplus q3 \quad (15)$$

$$K2 = q1 \oplus h \quad (16)$$

$$K1 = h \quad (17)$$

$$K0 = q2 \quad (18)$$

Equation (15) to equation (18) represents the proposed equations for minimized Composite S-Box. The architecture of combined both multiplication of X^2 and multiplication of X^a is illustrated in fig. 6. The proposed combined multiplication uses only three XOR gates to produce sufficient data suited for inverse multiplication operation.

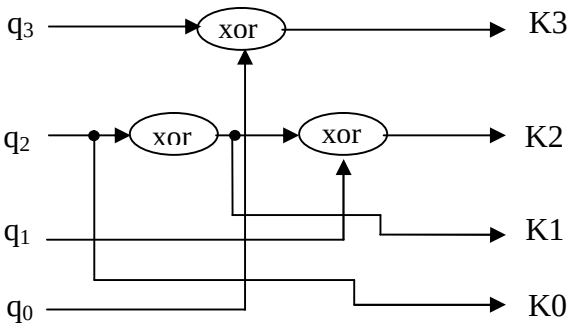

Figure: 5 Proposed reduced structure of combined both multiplication of X^2 and multiplication of X^a

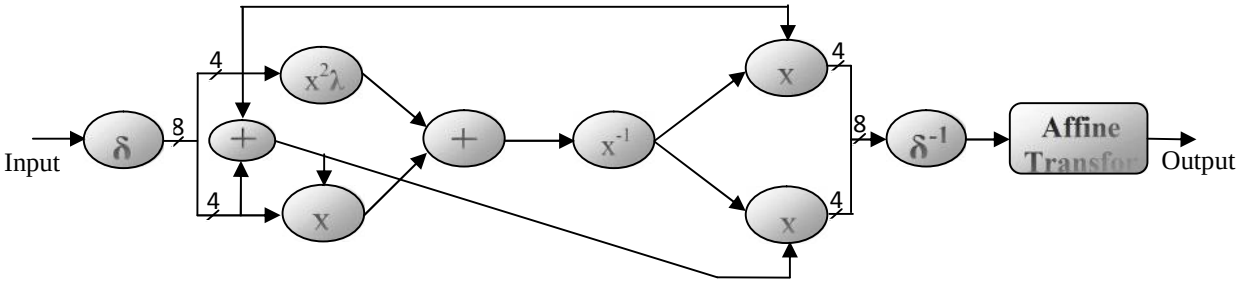

Figure: 6 Block diagram of Proposed Composite S-Box

It reduces the five XOR gates when compared to the traditional multiplication structures. Further, this structure is incorporated into Multiplicative Inverse Block of Composite S-Box to reduce the hardware complexity and power consumption of AES encryption and decryption process. The block diagram of proposed Composite S-Box is illustrated in fig. 7.

5. ENHANCED INVERSE MIXCOLUMN TRANSFORMATION

In addition to minimized Composite S-Box, enhanced Inv MixColumn transformation is used in this paper. Enhanced Inv MixColumn multiplication is developed in [9] by using redundant multiplication elements. For an Inv MixColumn transformation, multiplication of state byte input with 09, 0d, 0b and 0e are performed concurrently. In enhanced Inv MixColumn multiplication, only multiplication of 09, 04 and 02 are be determined manually. For further evaluation these resource are utilized effectively, since all the multiplications uses maximum of those resources only. The architecture of enhanced Inv MixColumn multiplication for AES decryption is illustrated in fig. 8. While reusing the existing resources for other operations, hardware complexity can be reduced successfully. Hence, it is clear that enhanced Inv MixColumn provides the better solution for AES decryption than traditional types of Inv MixColumn multiplication. Numbers 1, 2, 3 and 4 of fig. 8 represent the reusing the resources of $s_{o,c}$, $s_{1,c}$, $s_{2,c}$ and $s_{3,c}$ respectively.

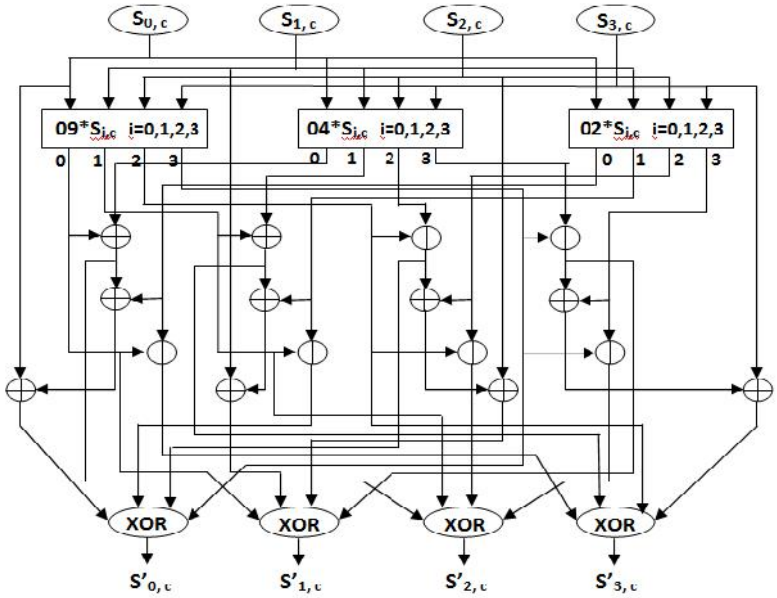

Figure: 7 Enhanced Inv MixColumn Multiplication

6. RESULTS AND DISCUSSION

Verilog Hardware Description Language (Verilog HDL) is used in this paper for the design of Minimized Composite S-Box and Enhanced Inv MixColumn. The simulation results of minimized Composite S-Box and enhanced Inv MixColumn of AES encryption and AES decryption are validated by ModelSim 6.3C and Synthesis results are evaluated by using Xilinx 10.1i (Family-Virtex 4, Devices-XC4VLX15/XCVLX25, Package-FF668 and Speed:-12) design tool. The simulation result of AES encryption is demonstrated in fig. 9. Encryption of 128-bits data is obtained in fig. 8 though four transformations (Minimized Composite S-Box, Shift Rows, MixColumn and Add Round Key). For instance, 128-bit data input is considered as 85fc3432abcd53210be0ac125ccdb110 in hexadecimal format. Encrypted data obtained in simulation result is 9ba71628a7ee25e0416a7354a15b1321 in hexadecimal format, which is illustrated in fig. 8. Similarly, the simulation result of AES decryption is illustrated in fig. 10. In decryption process, encrypted data, (i.e.) 9ba71628a7ee25e0416a7354a15b1321 is given as input. It reconstructs the original input (i.e.) 85fc3432abcd53210be0ac125ccdb110 through proposed Minimized Composite AES S-Box and Enhanced Inv MixColumn. The performances of Traditional Composite S-Box and Proposed Minimized Composite S-Box is analyzed and compared in table 1.

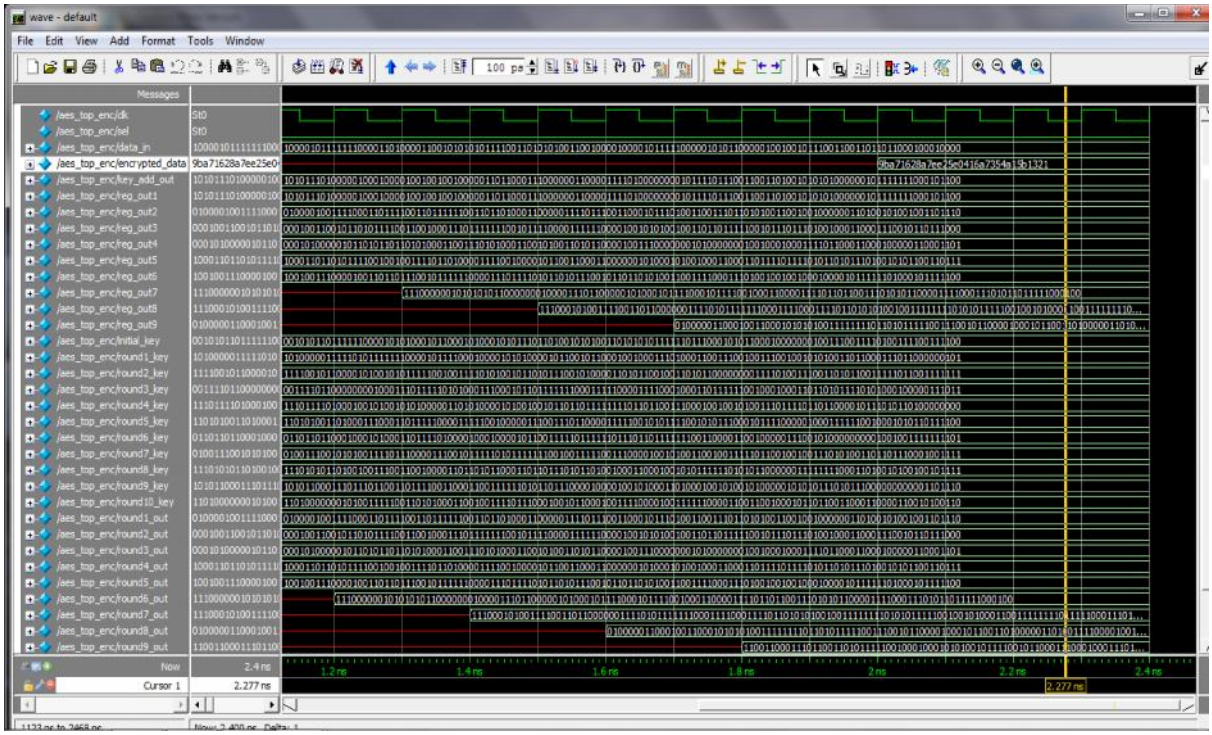

Figure: 8 Simulation result of Encryption by using Minimized Composite S-Box and Enhanced Inv Mix Column

From table 1, it is clear that proposed Minimized Composite S-Box offers 8.53% reduction Slices, 9.79% reduction of LUT, 37.66% reduction of delay and 6.15% reduction of power consumption than traditional Composite S-Box. The performance of table 1 is graphically illustrated in fig. 11. Further proposed Minimized Composite S-Box and enhanced Inv MixColumn transformations are incorporated into encryption and decryption of AES algorithm. The

comparison of traditional AES encryption and Proposed Minimized Composite S-Box based AES encryption is demonstrated in table 2. Their Performances are graphically illustrated in fig. 12. From table 2, it is clear that proposed Minimized Composited S-Box based AES Encryption offers 6.86% reduction of Slices, 6.27% reduction of LUTs, 12.68% reduction of delay and 7.35% reduction of power consumption than traditional AES Encryption. The comparison of traditional AES decryption and Proposed Minimized Composite S-Box & Enhanced Inv MixColumn based AES decryption is demonstrated in table 3. Their performances are graphically illustrated in fig. 13. From Table 3, it is clear that Proposed Minimized Composite S-Box & Enhanced Inv MixColumn based AES Decryption offers 17.15% reduction of Slices, 17.55% reduction of LUT, 3.97% reduction of delay consumption and 1.25% reduction of power consumption than traditional AES Decryption.

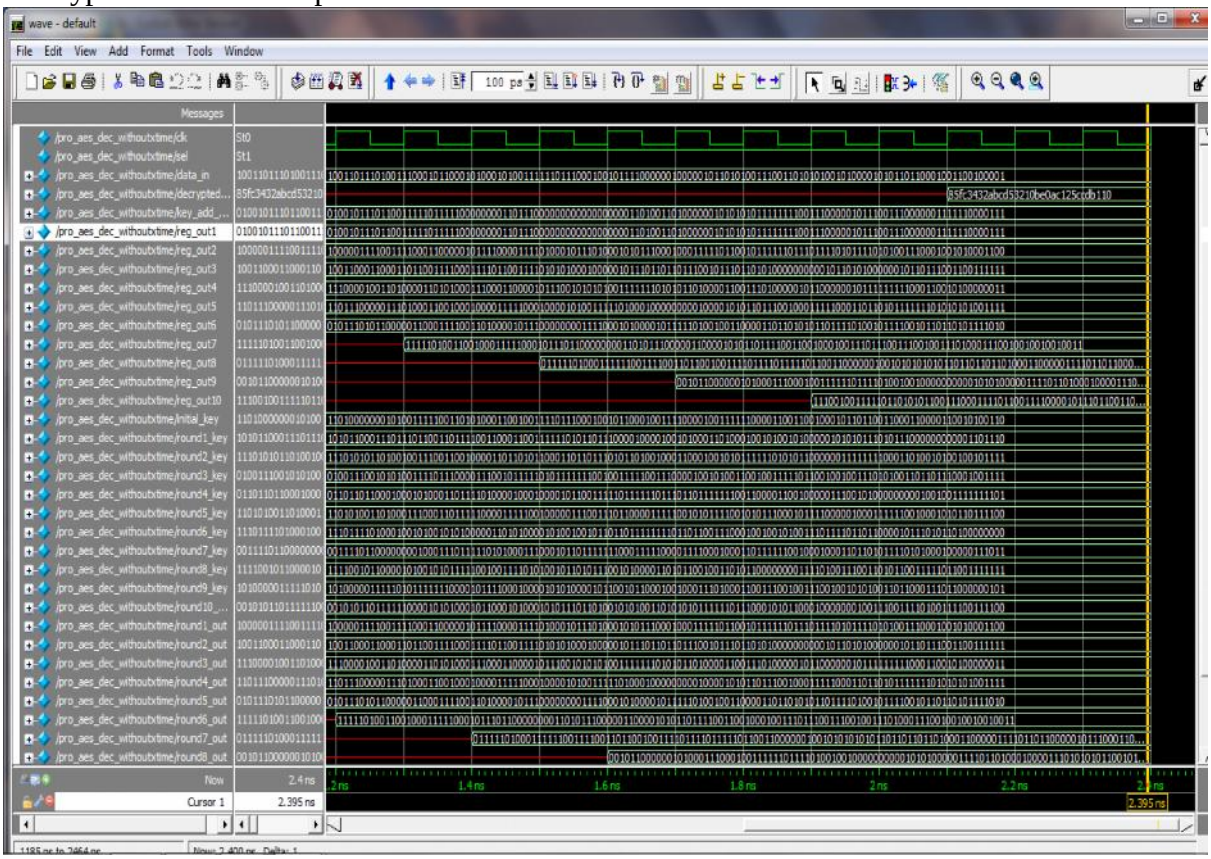

Figure: 9 Simulation result of Decryption by using Minimized Composite S-Box and Enhanced Inv MixColumn

Types	Slices	LUT	Delay(ns)	Power(mW)
Traditional Composite S-Box	47	91	8.260	601
Proposed Minimized Composite S-Box	43	83	5.149	564

Table: 1 Comparison of Traditional Composite S-Box and Proposed Minimized Composite S-Box

Types	Slices	LUT	Delay(ps)	Frequency (MHz)	Power(mW)
Traditional AES Encryption	8576	16,041	8170	122.393	6511
Proposed Minimized Composite S-Box based AES Encryption	7987	15,035	7134	140.176	6032

Table: 2 Comparison of Traditional Encryption and Proposed Minimized Composite S-Box based AES Encryption

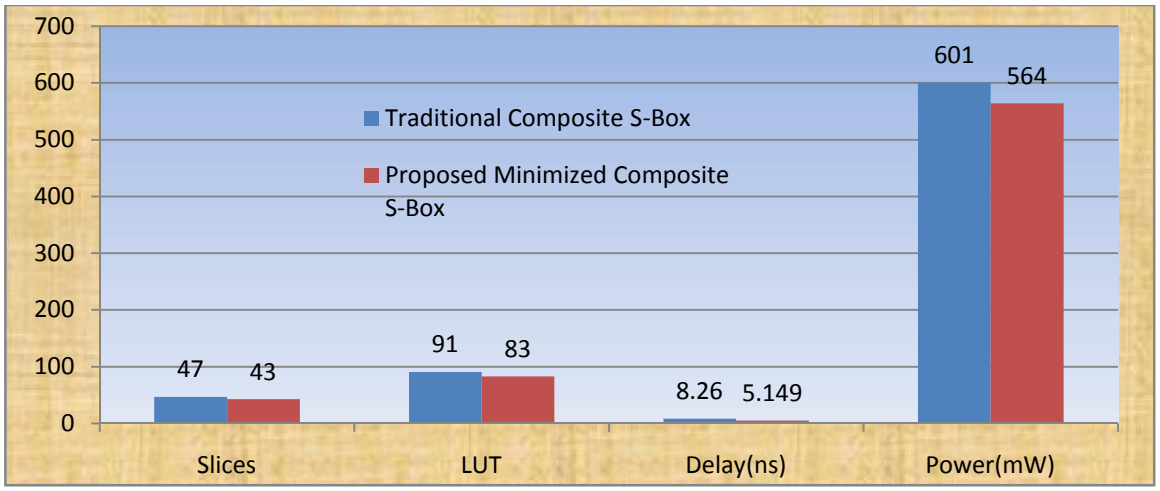

Figure: 10 Performances of Traditional Composite S-Box and Proposed Minimized Composite S-Box

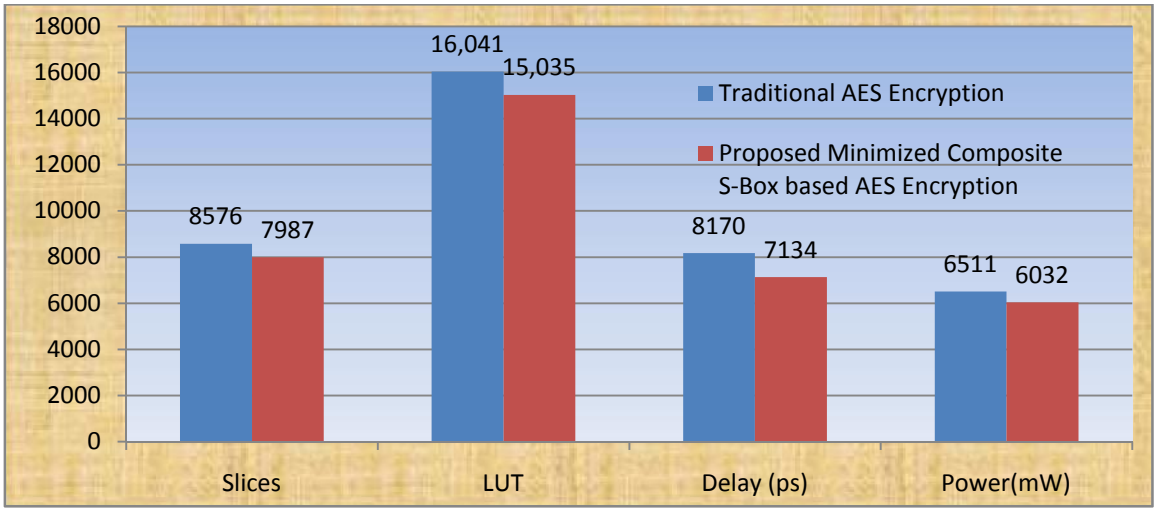

Figure: 11 Performances of Traditional AES Encryption and Proposed Minimized Composite S-Box based AES Encryption

Types	Slices	LUT	Delay(ps)	Frequency(MHz)	Power(mW)
Traditional AES Decryption	10,307	19,035	7042	142.002	6554
Proposed Minimized Composite S-Box & Enhanced Inv MixColumn based AES Decryption	8539	15,693	6762	147.886	6472

Table: 3 Comparison of Traditional Decryption and Proposed Minimized Composite S-Box & Enhanced Inv MixColumn based AES Decryption

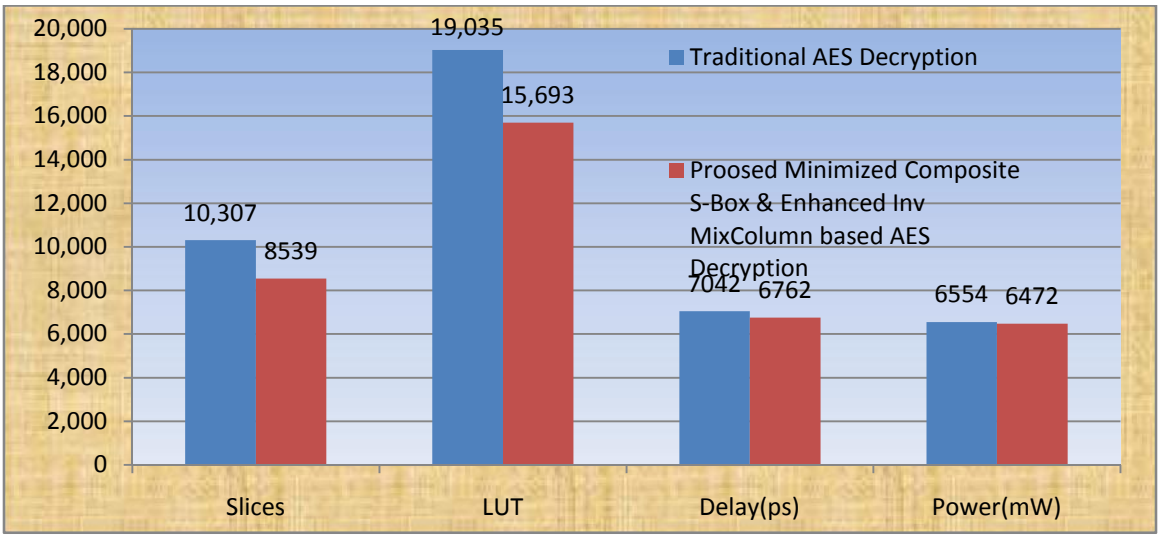

Figure: 12 Performance of Traditional AES Decryption and Proposed Minimized Composite S-Box & Enhanced Inv MixColumn based AES Decryption

CONCLUSION

In this paper, design of Minimized Composite S-Box and Enhanced Inv MixColumn transformation was done by using Verilog HDL. Proposed designs are implemented in Very Large Scale Integration (VLSI) System design environment. Low power consumption, high speed and less area utilization are the main key factors in VLSI System design environment. Hence, proposed model aims to reduce the hardware complexity, Power consumption and improve the speed of the System. Redundant operations cause poor performances in terms of hardware complexity in any combinational path. Hence, in this paper, redundant logic functions of Composite S-Box and Inv MixColumn transformations are identified and eliminated. Common resources of Composite S-Box and Inv MixColumn Transformations are designed once and it should be shared for entire combinational path. Proposed Minimized Composite S-Box offers 8.53% reduction Slices, 9.79% reduction of LUT, 37.66% reduction of delay and 6.15% reduction of power consumption than traditional Composite S-Box. Further Proposed Composite S-Box and Enhanced Inv MixColumn transformations are integrated into AES encryption and AES decryption process respectively. Proposed Minimized Composited S-Box based AES Encryption offers 6.86% reduction of Slices, 6.27% reduction of LUTs, 12.68% reduction of delay and 7.35% reduction of

power consumption than traditional AES Encryption. Similarly, Proposed Minimized Composite S-Box & Enhanced Inv MixColumn based AES Decryption offers 17.15% reduction of Slices, 17.55% reduction of LUT, 3.97% reduction of delay consumption and 1.25% reduction of power consumption than traditional AES Decryption.

REFERENCES

[1] K. Munusamy, C. Senthilpari, and D. C. Kho, "A low power hardware implementation of S-Box for Advanced Encryption Standard" In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2014 11th International Conference on (pp. 1-6). IEEE.

[2] M. Anitha Christy, S. Sridevi Sathya Priya, N. M. Siva Mangai, and P. Karthigaikumar, "Design and implementation of low power Advanced Encryption Standard S-Box using pass transistor XOR-AND logic" In Electronics and Communication Systems (ICECS), 2014 International Conference on (pp. 1-7). IEEE.

[3] M. Senthil Kumar and S. Rajalakshmi, "Incorporation of Wave Pipelined Techniques into Composite S-Box and AES Architectures" Research Journal of Applied Sciences, Engineering and Technology (RJASET), Vol. 8, No. 15, pp: 1717-1723, 2014.

[4] M. Senthil Kumar, and S. Rajalakshmi, "Incorporation of Reduced 09, 0B, 0D and 0E Structures into Inverse MixColumns for AES 128 Algorithm" Journal of Theoretical and Applied Information Technology (JTAIT), Vol. 70, No. 1, pp: 112-120, 2014.

[5] N. Ahmad, and S. R. Hasan, "Low-power compact composite field AES S-Box/Inv S-Box design in 65nm CMOS using Novel XOR Gate". Integration,the VLSI journal, Vol. 46, Issue. 4, pp: 333-344, 2013.

[6] N. Shanthini, P. Rajasekar and H. Mangalam, "Design of low power S-Box in Architecture Level using GF" International Journal of Engineering Research and General Science (IJERGS), Vol. 2, Issue. 3, pp: 268-276, 2014.

[7] R. Thillaikkarasi and K. Vaishnavi, "Optimum Composite Field S-Boxes Aimed at AES" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Vol. 3, Issue. 1, pp: 1-5, 2014.

[8] S. Anitha, and M. Suganya, "Area optimized in storage area network using Novel Mix column Transformation in Masked AES" International Journal of Engineering Trends and Technology (IJETT), Vol. 20, No. 6, pp: 275-282, 2015.

[9] J. Balamurugan and E. Logashanmugam, "Enhanced Inverse MixColumn Design for AES Decryption" accepted for publication in Middle East Journal of Scientific Research (MEJSR), June, 2015.

[10] Zhao Wang, Xiao Zhang, Sitao Wang, Zhisong Hao and Zhiming Zheng, "Application of the Composite Field in the Design of an Improved AES S-Box Based on Inversion" The Third International Conference on Communications, Computation, Networks and Technologies, pp: 23-29, 2014.