RESEARCH PAPER | Engineering | Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

Low Power and low Cmos Complexity Based Composite S-Box for Aes Encryption and Aes Decryption

KEYWORDS: Substitution-box (S- box), Advanced Encryption Standard (AES), Radio Frequency Identification (RFID), Data Encryption Standard (DES).

K. Sandyarani
Research scholar, Sathyabama University, India

Dr. P.Nirmal Kumar
Associate Professor, College of Engineering, Guindy, India

ABSTRACT *The substitution-box(s-box) is a basic component of symmetric key algorithms which performs substitution. This paper presents low power architecture for composite field arithmetic based Sub Bytes transformation (S-Box) used in Advanced Encryption Standard (AES) encryption. AES is more secure than Data Encryption Standard (DES). It supports large key sizes such as 128, 192 and 256 key sizes. AES is faster in both hardware and software. The S-box and Inverse S-box utilizes a low power 2-input XOR gate with only six devices to achieve a compact module implemented in 250nm IBM CMOS technology. In the proposed method, composite S-box is designed using Tanner 14.1i design tool. In order to reduce the hardware complexity and power consumption of AES Encryption and Decryption, Tanner design tool is preferred by the current research work. This design indicates power dissipation only around 0.0923µW using a 0.8v supply voltage and it is suitable for applications such as RFID tags and smart cards which require low power consumption with small silicon die.*

I.INTRODUCTION

The Advanced Encryption Standard (AES) was an accolade afforded to the Rijndael cipher, which was developed by Rijmen and Daemen by the National Institute of Standards and Technology (NIST) in 2000. Subsequently, there has been much interest in implementations of the AES. The AES algorithm is extremely flexible.AES has been widely used in a variety of applications ,such as secure communication systems, high-performance database servers, digital video or audio recorders, RFID tags, and smart cards.

The rapidly increasing demands for using internet and wireless communication have led to the development of efficient security algorithm and devices to protect the transmitted information over open channels. The Rijndael AES algorithm is a symmetric block cipher that processes data blocks of 128 bits organized as a 4×4 matrix of bytes called a state. A state is operated by Nr=10,12, or 14 rounds of transformations with key length K equal to 128, 192, or 256 bits ,respectively.

Four transformations including Sub Bytes (SB), Shift Rows (SR), Mix Columns (MC), and Add Round Key (ARK) are performed in the encryption process. The good properties of such S-boxes prevent penetrating in the cipher structure to perform successful attack. So, finding some simpler expression or approximation may be useful to overcome the design strength of S-boxes and the cipher.

The composite field arithmetic based implementation involves finding multiplicative inverse (MI) in GF (2^8) followed by affine transformation. As computation of MI in GF (2^8) is hardware intensive, the element in GF(2^8) is mapped to composite field of lower order using isomorphic mapping function. The composite field of order GF (2^4) or GF ((2^2)^2)^2) is used. The S-Box is at the core of any AES implementation and is considered a full complexity design consuming the major portion of the power and energy budget of the AES hardware.

This paper is focused on area-efficient low-voltage and low-power CMOS implementation of the S-Box or Inv S-Box. In the proposed method, the composite S-Box is designed using Tanner 14.1i design tool. In order to reduce the complexity and power consumption of AES encryption and decryption by using Tanner 14.1i design tool.

II. RELATED WORKS

A high–throughput low-cost AES processor has been briefly explained in [Chih-Pin Su, et al, 2003]. In this paper, propose an efficient hardware implementation of the Advanced Encryption Standard algorithm, with key expansion capability. Compared to the widely used table lookup technique, the proposed basis transformation technique reduces the hardware overhead of the S-Box by 64 percent. The simple error detection methods for hardware implementation of advanced encryption standard have been explained in [Chih-Hsu Yen and Bing-Fei Wu, 2006]. The proposed schemes have high fault coverage. In addition, the schemes proposed are scalable and symmetrical. The scalability makes these schemes suitable for an AES circuit implemented in 8-bit, 32-bit, or 128-bit architecture. Symmetry also benefits the implementation of the proposed schemes to achieve that the encryption process and decryption process can share the same error detection hardware.

Memory-Free low-cost designs of Advanced Encryption Standard using common sub expression elimination for sub functions in transformations has been described in [Shen-Fu Hsiao, et al, 2006]. In this paper, they propose area-efficient Advanced Encryption Standard (AES) processor designs by applying a new common-sub expression-elimination (CSE) algorithm to the sub functions that realize the various transformations in AES encryption and decryption. The efficient method for simplifying and approximating the S-boxes based on power functions has been explained in [A.Farhadian and M.R Aref, 2009]. In recently proposed cipher algorithms, power functions over finite fields and specially inversion functions play an important role in the S-box design struc-

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

ture. The new systematic efficient method is introduced to cryptanalyse (to simplify and approximate) such S-boxes.

High –Speed AES encryptor with efficient merging techniques has been described in [Issam Hammad, et al, 2010]. This technique is implemented using composite field arithmetic byte substitution, where higher efficiency is achieved by merging and location rearrangement of different operations required in the steps of encryption. High speed S-box architecture for advanced encryption standard has been explained in [Rashmi Ramesh Rachh, et al, 2011]. The proposed design of S-box is shown to have the shortest critical path with moderate gate count requirement compared to the known composite field based S-box design.

Fault detection approach for the composite field S-Box and Inverse S-Box has been explained in [Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, 2011]. The high level of security and the fast hardware and software implementations of the Advanced Encryption standard have made it the first choice for many critical applications. Nevertheless, the transient and permanent internal faults or malicious faults aiming at revealing the secret key may reduce its reliability. Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis has been explained in [Massousd Masoumi and Mohammad Hadi Rezayati, 2014]. This method is based on randomization in composite field arithmetic which entails a low implementation cost while does not alter the algorithm, does not reduce the working frequency and keeps perfect compatibility with the published standard.

III. RIJNDAEL AES ALGORITHM

Rijndael AES algorithm consists of two parts, the data procedure and the key schedule. The data procedure is the main body of the encryption (decryption) and consists of four operations,(Inv)Sub Bytes, (Inv)Shift Rows, (Inv)Mix Column, and (Inv) AddRoundKey.Rijndael AES algorithm processes data blocks of fixed size using cipher keys of length 128,192 and 256bits. 128-bits AES Encryption has been widely used for encryption and decryption of AES. General data flow structure for 128 bit AES Encryption and Decryption is illustrated in fig. 1.

As shown in fig. 1, Final round of both AES Encryption and AES Decryption doesn't have Mix Column and Inv Mix Column transformation function respectively. It has 10 numbers of rounds for exhibiting cipher data from encryption process and plan data from decryption process.

3.1 Sub-Bytes Transformation ():

In Sub-Bytes transformation, substitution techniques are involved with the help of substitution tables (LUTs/ Memories/ROM). In general, Substitution box has been generated by two important transformation techniques.

Multiplicate Inverse (MI) Transformation: Taking MI for give input state bytes in Galois field GF (2^8).

Affine Transformation (AT): Taking Affine Transformation of MI outputs. In this operation XOR functions can be performed with in combined input bits itself.

Similarly, Inverse Sub-Bytes transformation performs inverse operation.

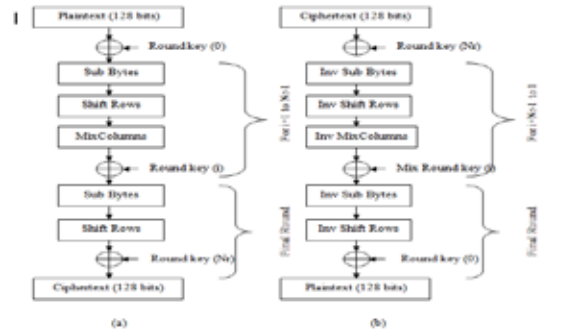

Fig.1 General Data Flow Structure for 128 bit AES (a) Encryption (b) Decryption

3.2 Shift Rows Transformation ():

$$\begin{bmatrix} s0 & s4 & s8 & s12 \\ s1 & s5 & s9 & s13 \\ s2 & s6 & s10 & s14 \\ s3 & s7 & s11 & s15 \end{bmatrix} \xrightarrow{\text{Shift Rows}} \begin{bmatrix} s0 & s4 & s8 & s12 \\ s5 & s9 & s13 & s1 \\ s10 & s14 & s2 & s6 \\ s15 & s3 & s7 & s11 \end{bmatrix}$$

The first row is unchanged, the second row is left circular shifted by one, the third row is by two and the last row is by three. Similarly, reverse process has been followed in Inv Shift Rows transformation.

3.3 Mix Column Transformation ():

In Mix Column transformation, state bytes treated as a four-term polynomial. The columns are considered as polynomials over GF (2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial. Similarly, in Inv Mix Column transformation, reverse process has been followed (i.e.) state bytes are multiplied with another fixed polynomials.

3.4 Add Round Key Transformation ():

In the Add Round Key transformation, a Round Key is added to the state by a simple bitwise XOR operation. Each Round Key consists of Nb words. Those Nb words are added into the columns of the state.

IV. DESIGN OF AES COMPOSITE S-BOX

In Rijndael AES algorithm. Substitute Box (S-Box) is the first step of encryption operation. In S-Box transformation, Substitution bytes are used to replace the state bytes. The symbolic block diagram of Sub Bytes transformation is shown in fig. 2. The substitution table has been generated by performing two functions on input state bytes. They are (1) Multiplicative Inverse and (2) Affine Transformation. In MI unit, inverse multiplication has been performed with the help of digital logics and affine transformation has been performed by taking exclusive operation MI outputs with 63. Block diagram of composite S-Box is shown in fig. 3, which performs both Sub-Bytes and Inv Sub-Bytes transformation by switching combinational logics using multiplexers. To make a compact AES implementations composite field inversions are extended to GF $(((2^2)^2)^2)$ from GF (2^8). This approach is used to reduce the chip size to design. The column vector of the input state matrix first goes into isomorphic transformation from GF (2^8) into the composite field GF $(((2^2)^2)^2)$ followed by inversion in composite field and inverse isomorphic transformation. Finally, an affine transformation is carried out to create the cipher data.

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

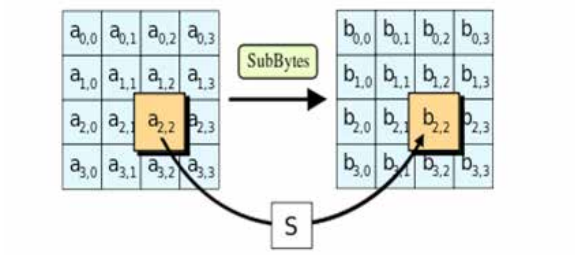

Fig. 2 Block diagram of Sub Bytes Transformation

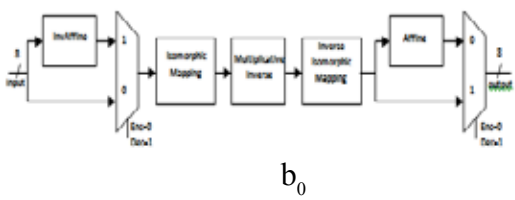

Fig. 3 Block diagram of composite S-Box

In S-Box Transformation, Isomorphic Mapping function (q) has performed initially on the input State Bytes (b). Secondly, Inverse Multiplication (q') has been performed on isomorphic output data. Then inverse isomorphic mapping function (b') has been performed on q'. At the end, affine transformation function (b'') has been carried out by inverse isomorphic functions. Generally, the affine transformation (AT) function involves the multiplication with 63.

In Inv S-Box Transformation, inv Affine Transformation (q') function has performed initially on the given input bytes (q''). Secondly, Multiplicative Inverse function (q) has performed on IAT outputs. Finally, inverse isomorphic mapping function has been performed on MI outputs to reconstruct the original input State-Bytes.

The state matrix representation of Affine and inverse Affine transformation techniques is demonstrated as follows,

$$[\mathrm{AT}(b')] = \begin{bmatrix} b_o'' \\ b_1'' \\ b_2'' \\ b_3'' \\ b_4'' \\ b_5'' \\ b_6'' \\ b_7'' \end{bmatrix} = \begin{bmatrix} \overline{b_0' \wedge b_4' \wedge b_5' \wedge b_6' \wedge b_7'} \\ \overline{b_0' \wedge b_1' \wedge b_5' \wedge b_6' \wedge b_7'} \\ b_0' \wedge b_1' \wedge b_2' \wedge b_6' \wedge b_7' \\ b_0' \wedge b_1' \wedge b_2' \wedge b_3' \wedge b_7' \\ b_0' \wedge b_1' \wedge b_2' \wedge b_3' \wedge b_7' \\ \overline{b_1' \wedge b_2' \wedge b_3' \wedge b_4' \wedge b_5'} \\ \overline{b_2' \wedge b_3' \wedge b_4' \wedge b_5' \wedge b_6'} \\ b_3' \wedge b_4' \wedge b_5' \wedge b_6' \wedge b_7' \end{bmatrix} \quad (1)$$

$$[\mathrm{IAT}(q'')] = \begin{bmatrix} q_o'' \\ q_1'' \\ q_2'' \\ q_3'' \\ q_4'' \\ q_5'' \\ q_6'' \\ q_7'' \end{bmatrix} = \begin{bmatrix} \overline{q_2'' \wedge q_5'' \wedge q_7''} \\ q_0'' \wedge q_3'' \wedge q_6'' \\ \overline{q_1'' \wedge q_4'' \wedge q_7''} \\ q_0'' \wedge q_2'' \wedge q_5'' \\ q_1'' \wedge q_3'' \wedge q_6'' \\ q_2'' \wedge q_4'' \wedge q_7'' \\ q_0'' \wedge q_3'' \wedge q_5'' \\ q_1'' \wedge q_4'' \wedge q_6'' \end{bmatrix} \quad (2)$$

Similarly, state matrix transformation of Isomorphic and Inverse Isomorphic transformation is demonstrated as follows,

$$[\mathrm{ISO}(b)] = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} * \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \quad (3)$$

$$[\mathrm{ISO}(b)] = \begin{bmatrix} b_0 \wedge b_2 \\ b_1 \wedge b_6 \wedge b_7 \\ b_2 \wedge b_3 \wedge b_5 \wedge b_7 \\ b_2 \wedge b_5 \\ b_1 \wedge b_3 \wedge b_6 \wedge b_7 \\ b_1 \wedge b_4 \wedge b_5 \wedge b_6 \\ b_1 \wedge b_2 \wedge b_3 \wedge b_4 \wedge b_5 \wedge b_6 \\ b_5 \wedge b_7 \end{bmatrix} \quad (4)$$

$$[\mathrm{ISO}^{-1}(b)] = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \end{bmatrix} \quad (5)$$

$$[\mathrm{ISO}^{-1}(b)] = \begin{bmatrix} q_0 \wedge q_1 \wedge q_2 \wedge q_3 \wedge q_6 \\ q_4 \wedge q_7 \\ q_1 \wedge q_3 \wedge q_5 \wedge q_7 \\ q_1 \wedge q_3 \\ q_1 \wedge q_5 \wedge q_7 \\ q_1 \wedge q_2 \wedge q_2 \wedge q_5 \wedge q_6 \\ q_2 \wedge q_3 \wedge q_4 \wedge q_5 \wedge q_6 \\ q_1 \wedge q_2 \wedge q_2 \wedge q_5 \wedge q_6 \wedge q_7 \end{bmatrix} \quad (6)$$

The block diagram of Multiplicative Inverse (MI) unit is illustrated in fig.4. It performs the inverse operation of input x(i.e.1/x). It consists of mathematical block xλ and x^2 are shown in fig. 5 and fig. 6 respectively.

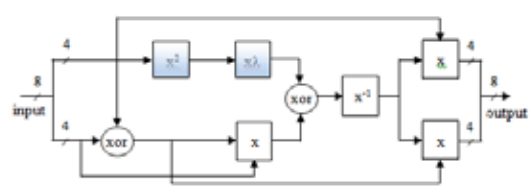

Fig .4 Block diagram of Multiplicative Inverse

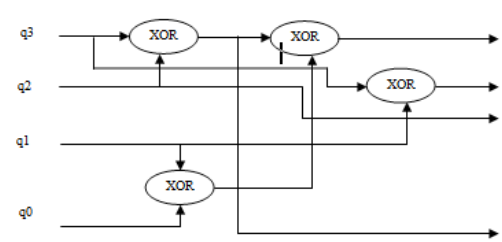

Fig .5 Multiplication of xλ

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

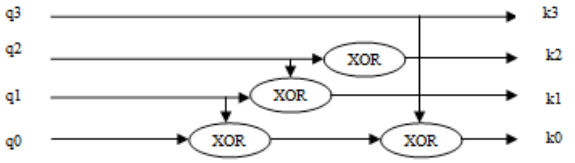

Fig .6 Multiplication of x^2

Finally, the multiplexer circuit is used to select S-Box/ Inv S-Box outputs based on the select line. Hence, this S-Box circuit is referred as Composite S-Box. Instead of using direct Look Up Tables (LUTs), this Composite S-Box gives more advantage in terms of less chip utilization, lower delay and power consumptions.

V. PROPOSED ENHANCED AES COMPOSITE S-BOX USING TANNER

In this paper, Composite AES S-Box is designed using Tanner 14.1i design tool. To reduce the complexity and power consumption of AES encryption and decryption. The architecture of Composite S-Box has different kinds of blocks like Affine Transformation (AT), Inverse Affine Transformation (IAT), Isomorphic Mapping (ISO), Inverse Isomorphic Mapping (Inv ISO) and Multiplicative Inverse (MI) for performing inverse multiplication of input. Each and Every block has digital logics to support the function of inverse multiplication. Redundant logic function of each and every block has identified with the help of Boolean logic expressions.

Equation (1) establishes the Affine Transformation techniques. In this equation, there are four Redundant logic functions are identified.

Redundant Function_AT1 =b'_6 ^ b'_7; Redundant Function_AT2 = b'4 ^ b'5; Redundant Function_ AT3 =b'_0 ^ b'_1; Redundant Function_AT4 =b'_2 ^ b'_3.

Hence, equation of Affine Transformations can be reduced as follows,

AT[0] = ~ (b'_0 ^ Redundant Function_AT2 ^ Redundant Function_AT1);AT[1] = ~(Redundant Function_AT3 ^b'_5 ^ Redundant Function_AT1); AT[2] = Redundant Function_AT3 ^ b'_2 ^ Redundant Function_AT1; AT[3] = Redundant Function_AT3 ^ Redundant Function_AT4 ^ b'_7; AT[4] = Redundant Function_AT3 ^ Redundant Function_AT4 ^b'_4;AT[5] = ~ (b'_1 ^ Redundant Function_AT4 ^ Redundant Function _AT4 ^ Redundant Function_AT2); AT[6] = ~(Redundant Function_AT4 ^ Redundant Function_AT2 ^ b'_6); AT[7] = b'_3 ^ Redundant Function_AT2 ^ Redundant Function_AT1.

When compared to traditional AT technique, 12 gates are reduced in proposed Enhanced AT techniques. The circuit diagram of AT technique is shown in fig. 7. Similarly, Redundant Functions of Inverse Affine Transformation techniques are identified from equation (2) as follows,

Redundant Function_IAT1 =q'_2 ^ q'_5; Redundant Function_IAT2 =q'_3 ^ q'_6; Redundant Function_IAT3 =q'_4 ^ q'_7.

Hence, equations of Inverse Affine Transformation can be reduced as follows,

IAT [0] = ~ (Redundant Function_IAT1 ^ q'_7); IAT [1] = q'_0 ^ Redundant Function_IAT2; IAT [2] = ~(q'_1 ^ Redundant Function_IAT3); IAT [3] = q'_0 ^ Redundant Function_IAT1; IAT [4] =q'_1 ^ Redundant Function_IAT2; IAT [5] = q'_2 ^ Redundant Function_IAT3; IAT [6] = q'_0 ^ q'_3 ^ q'_5; IAT [7] = q'_1 ^ q'_4 ^ q'_6.

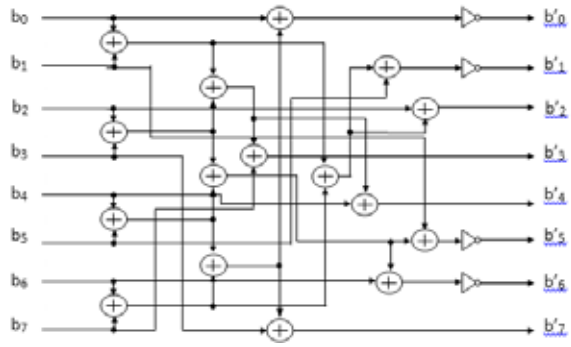

Fig.7 Circuit diagram of proposed Enhanced AT Technique

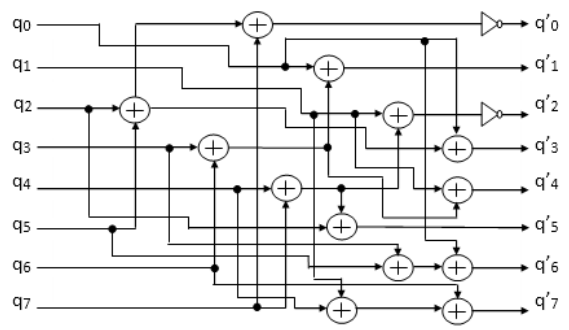

Fig. 8 Circuit diagram of proposed Enhanced IAT Technique

When compared to traditional IAT technique, 3 gates are reduced in proposed Enhanced IAT technique. The circuit diagram of proposed Enhanced IAT technique is shown in fig. 8. Equation (4) establishes the Isomorphic Mapping Transformation. In this equation, there are five redundant functions are identified.

Redundant Function_ISO2 = b_6 ^ b_7; Redundant Function_ISO3 = b_5 ^ b_7; Redundant Function_ISO3 = b_2 ^ b_5; Redundant Function_ISO4 = b_1 ^ b_3; Redundant Function_ ISO5 = b_4 ^ b_6.

Hence, equations of Isomorphic Transformation can be reduced as follows,

ISO [0] =b_0 ^ b_2; ISO [1] = b_1 ^ Redundant Function_ISO1; ISO [2] = b_2 ^ b_3 ^ Redundant Function_ISO2; ISO [3] = Redundant Function_ISO2; ISO [4] = Redundant Function_ISO4 ^ Redundant Function_ISO1; ISO [5] = b_1 ^ b_5 ^ Redundant Function_ ISO5; ISO [6] = Redundant Function_ISO3 ^ Redundant Function_ ISO5; ISO [7] =Redundant Function_ ISO2.

When compared to traditional ISO technique, 5 gates are reduced in proposed Enhanced ISO technique. The circuit diagram of proposed Enhanced ISO technique is shown in fig. 9 . Similarly, redundant functions of Inverse Isomorphic Transformation are identified from equation (6) as follows,

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

Redundant Function_InvISO1 = q_1 ^ q_3; Redundant Function_InvISO2 =q_5 ^ q_6; Redundant Function_InvISO3 =q_7 ^ q_5.

Hence, equations of Inverse Isomorphic Transformation can be reduced as follows,

Inv ISO [0] = q_0 ^ Redundant Function_ISO1 ^ Redundant Function2; Inv ISO [1] = q_7 ^ q_5; Inv ISO [2] = Redundant Function_InvISO1 ^ Redundant Function_InvISO3; Inv ISO[3] = Redundant Function_ InvISO1;Inv ISO [4]= q_1 ^ Redundant Function_InvISO3; Inv ISO [5] = q_2 ^ Redundant Function_InvISO1 ^ Redundant Function_InvISO2; Inv ISO[6] =q_2 ^ q_3 ^ q_4 Redundant Function_InvISO2; Inv ISO [7] = q_2 ^q_7 ^ Redundant Function_InvISO1 ^ Redundant Functiom_InvISO2.

When compared to traditional Inv ISO technique, 8 gates are reduced in proposed Enhanced Inverse ISO technique. The circuit diagram of proposed Enhanced Inverse ISO technique is shown in fig. 10. In addition, the circuits of multiplication of xλ and x^2 are realized and re-designed by eliminating the unwanted redundant functions. Hence a new architecture has been proposed for Inverse Multiplication unit. The circuit diagram of Enhanced combined multiplication of xλ and x is shown in fig.11 by using following expressions,

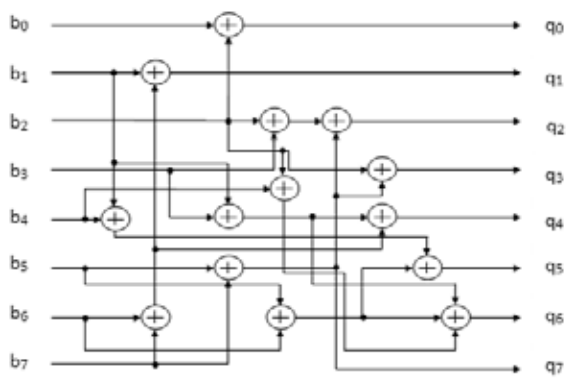

Fig. 9 Circuit diagram of proposed Enhanced ISO Technique

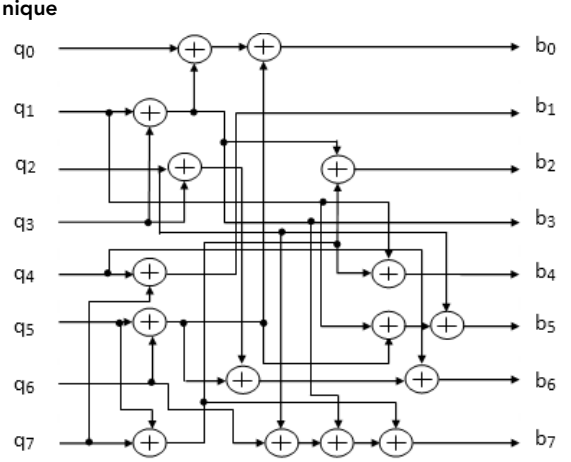

Fig. 10 Circuit diagram of proposed Enhanced Inverse ISO Technique

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

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

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

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

Where,

$$h = q2 \oplus q3$$

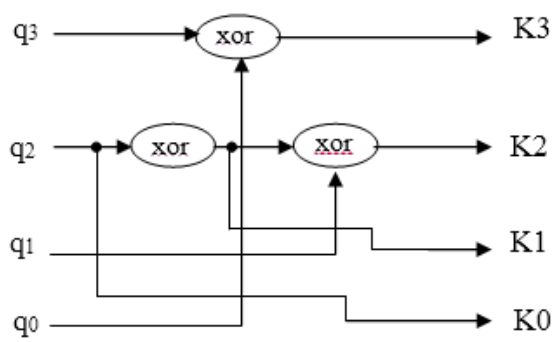

Fig. 11 Circuit diagram of proposed combined multiplication of xλ and x^2

VI. RESULTS AND DISCUSSION

Design of Enhanced AT, IAT, and ISO, Inverse ISO and combined Multiplication of xλ and x^2 are designed through Back End Tanner Electronic Design Automation (EDA) v14.1i tool. The schematic RTL (Register Transfer Logic) views of proposed Enhanced AES Composite S-Box techniques are validated by using Tanner 14.1i design tool. In this research work, 128 bit AES is considered for realizing the proposed Enhanced techniques of Composite S-Box. The Schematic RTL view of proposed Enhanced Composite S-box based 128- bit AES Encryption using Tanner is shown in fig. 12. Composite S-Box and Inv S-Box are designed using Tanner to reduce the complexity and power consumption.

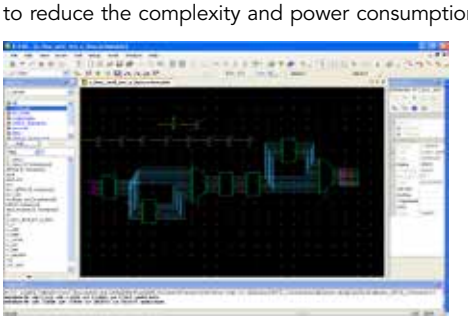

Fig. 12 Schematic RTL View of Proposed Enhanced Composite S-Box based 128 bit AES Encryption using Tanner

Volume : 5 | Issue : 10 | October 2015 | ISSN - 2249-555X

The Schematic result of proposed Enhanced AES Composite S-Box and Inv S- box using Tanner is shown in Fig.13 and Fig.14. The Proposed Enhanced AES Composite S-Box and Inv S-Box using backend Tanner EDA v14.1 design tool .By using Tanner, it will reduce the complexity and power consumption and also improves the performance of AES Encryption and Decryption.

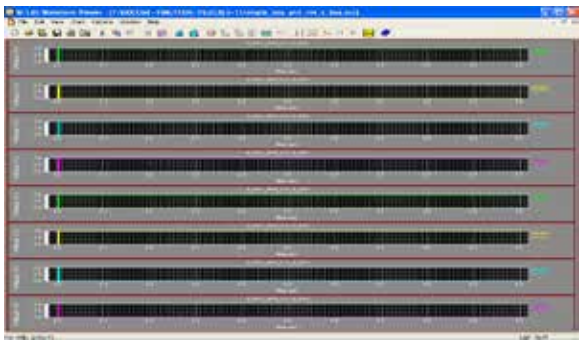

Fig .13 Schematic result of Proposed Enhanced AES Composite S-Box using Tanner

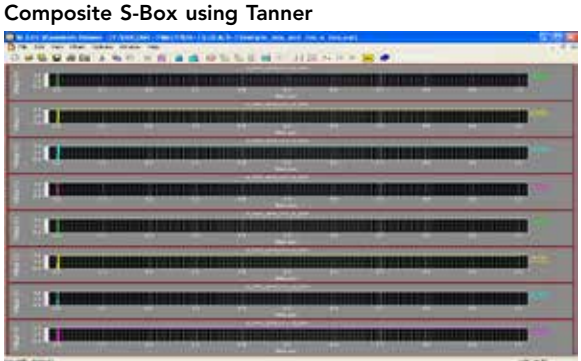

Fig. 14 Schematic result of Proposed Enhanced AES Composite Inv S-Box using Tanner

VII. CONCLUSION

In this paper, Enhanced AES Composite S-Box is designed using Tanner through Very Large Scale Integration (VLSI) System design environment. Less area utilization, high speed and lower power consumption are the main key Factors in VLSI System design environment. Therefore, the main goal of this research work is to reduce the complexity and power consumption of AES Encryption and Decryption process using Tanner. The Enhanced Affine Transformation, Enhanced Inverse Affine Transformation, Enhanced Isomorphic Mapping, Enhanced Inverse Isomorphic Mapping and combined multiplication of $x\lambda$ and x^2 are proposed in this research work. Further, Enhanced all techniques are integrated in Composite S-Box. This design indicates power dissipation only around 0.0923µW using a 0.8v supply voltage.The S-Box and Inverse S-Box utilizes a low power 2-input XOR gate with only six devices to achieve a compact module implemented in 250nm IBM CMOS technology. In future, proposed Enhanced Composite S-Box based AES Encryption and Decryption standard will be absolutely used in different types of wireless cryptography based applications for implementing with less hardware and high speed.

REFERENCE

[1] Chin-pin su, Tsung- Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu, (2003) "A High-Throughput Low-Cost AES Processor", IEEE Communications Magazine, pp: 86 -91. [2] Chin-Hsu Yen and Bing-Fei Wu, (2006) "Simple Error Detection Methods For Hardware Implementation of Advanced Encryption Standard", IEEE Transactions on Computers, Vol.55, No.6, pp: 720-731. [3] Shen-Fu Hsiao,Ming-chihChen and Chia-Shin Tu,(2006) "Memory-Free Low-Cost Designs Of Advanced Encryption Standard using Common Sub expression Elimination for Sub functions in Transformations", IEEE Transactions on Circuits and Systems-I: Regular Papers, Vol. 53,No.3,pp: 615-626. [4] A.Farhadian, M.R. Aref, (2009)" Efficient Method for Simplifying and Approximating the S-Boxes based on Power Functions", The Institution of Engineering and Technology, Vol.3, Iss. 3, pp: 114-118. [5] Issam Hammad, Kamal El-Sankary and Ezz El-Masry, (2010)" High-Speed AES Encryptor with Efficient Merging Techniques", IEEE Embedded Systems Letters, Vol.2, No.3,pp:67-71. [6] Rashmi Ramesh Rachh, P.V.Anandamohan and B.S.Anami,(2011)" High Speed S-Box Architecture for Advanced Encryption Standard", IEEE Conference ,pp:1-6. [7] Mehran mozaffari-Kermani, Arash Reyhani-Masoleh, (2011)" 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, pp:1327-1340. [8] Massoud Masoumi and Mohammad Hadi Rezayati, (2014)," Novel Approach to Protect Advanced Encryption Standard Algorithm Implementation against Differential Electromagnetic and Power Analysis", IEEE Transactions on Information Forensics and Security,pp:1-10.