Indian Journal of Science and Technology, *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/82302, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhanced MixColumn Design for AES Encryption

M. Vaidehi[1*] and B. Justus Rabi[2]

[1]Karpagam University, Coimbatore - 641021, Tamil Nadu, India; vaidehi.vlsi@gmail.com
[2]Shri Andal Alagar College of Engineering, Chennai - 603111, Tamil Nadu, India; bennisrobi@rediffmail.com

Abstract

The main aim of the current research work is to reduce the complexity path of AES (Advanced Encryption Standard) Encryption. Architecture of MixColumn transformation has been optimized in this research work. Traditional methods of MixColumn transformation methods has been realized and re-designed by reducing the redundant logical functions. Verilog Hardware Description Language (Verilog HDL) has been used to design the optimized MixColumn transformation of AES Encryption. Further optimized MixColumn design has been incorporated into AES Encryption with appropriate input points. Common Sub-expression Elimination (CSE) algorithm is used in developed AES Encryption algorithm. Proposed optimized MixColumn design offers 10.93% improvements in hardware slices, 13.6% improvements in LUTs and 1.19% improvements in delay consumption than traditional MixColumn design. Further proposed optimized MixColumn design has been incorporated into AES Encryption design. Further, proposed optimized MixColumn based AES Encryption design offers 4.75% improvements in silicon area, 4.56% reduction in power consumption than traditional MixColumn based AES Encryption. In future, proposed optimized MixColumn design will be useful in space and terrestrial applications for exhibiting secure transmissions.

Keywords: Advanced Encryption Algorithm, Common Sub-Expression Elimination, Optimized Inverse MixColumn, Verilog Hardware Description Language, Very Large Scale Integration (VLSI)

1. Introduction

In the growth of microchip based wireless communication applications such as 3G and 4G, low cost chip based secure algorithm is an essential part. Advanced Encryption Standard (AES) is one of the low cost hardware based crypto algorithm invented by National Institute of Standards and Technology (NIST) in 1997. This effective algorithm is invented by Rijndael which is used for encrypting and decrypting the 128, 196 and 256 input data bits. Very Scale Integration System (VLSI) is an effective tool for designing and fabricating the different types of automation and control system based applications. Less chip size utilization, improved speed of the processor and reducing the power consumption are the primary goal VLSI System design. Reducing the complexity in terms of fan-in and fan-out is the secondary goal of VLSI System design.

The major transmission steps of AES Encryption are Substitution Box (S-Box), Shift Rows, MixColumn and Add Round Key. Like that, reverse transformations such as Inverse Substitution Box (Inv S-Box), Inverse Shift Rows, Inverse MixColumn and Add Round Key are the major transmission steps of AES Decryption. All the transformations of encryption and decryption have the certain transformation for providing secure data transmission. When compared to logics involved in S-Box, Shift Rows and Add Round Key, transformation of MixColumn and Inverse MixColumn have most tedious path to provide secure data transmission. Hence, large endeavours have been taking concentrations on Inverse MixColumn transformation of AES Decryption. In[1,3,4] reduced Xtime multiplication has been designed. Further possibilities of improved structures have been identified in[4] with the help of reducing the redundant logical functions.

In this research work, Structure of MixColumn for AES Encryption has been realized to improve the hardware architecture of AES Encryption algorithm. Reducing the Common Sub-expression Elimination (CSE) technique has been used in this research work to minimize or

*Author for correspondence

reduce the hardware structure of MixColumn architecture. Further technique of enhanced Inverse MixColumn of[4] is used in decryption side. The main goal of the research work is to reduce the hardware Slices, Look up Tables (LUTs) and Power consumption of AES Encryption architecture. Design of Proposed Enhanced Encryption has been designed with the help of Verilog Hardware Description Language (Verilog HDL).

2. Related Works

A lot of research works have been suggested the different types of enhanced technique for improving the structure of Inverse MixColumn transformation of AES Decryption. Since other transformations except Inverse MixColumn have not the most arithmetic circuit like Multiplication, Correlation and Convolution. In[5] decomposition methods of Inverse MixColumn transformation have been explained. In those research works, gate level reduction of Inverse MixColumn transformation techniques has been introduced. Unlike normal multiplications, MixColumn and Inverse MixColumn multiplication transformation provide 'N' bit output for NxN multiplication. In[7] Xtime multiplication has been used for performing Inverse MixColumn multiplications. It gives high throughput and high speed for exhibiting the cipher data from plain data. Faulty analysis of AES encryption and decryption has been made in[6] with the help of hamming Error Detection and Correction (EDC) codes. The proposed structure of[6] gives the best VLSI performances in terms of lower power consumption and less area utilization as well as it is best fault detecting system for the space and terrestrial communication applications.

In normal Inverse MixColumn multiplication, addition of "1B" with each transformation is performed for controlling the bit-width of MixColumn and Inverse MixColumn multiplication. In order to reduce the switching activities of "1B" value, Reduced Xtime multiplication based Inverse MixColumn transformation has been designed in[1,3,4]. Optimized Inverse MixColumn transformation has common shifter and common adder to produce the Inverse MixColumn transformation output. Further in[4], redundant operations have been identified to enhance the architecture of Inverse MixColumn transformation. In addition to these enhanced Inverse MixColumn transformation, Minimized Composite S-Box transformation has been designed in[4]. Finally FPGA implementation of AES Encryption and Decryption has been proposed in[8].

From above literature review, it is clear that, Enhanced and Optimized Inverse MixColumn transformation techniques are available for AES Decryption. Similarly, Minimized Composite S-Box transformation structure is available for the S-Box transformation operation. Hence, this research work identifies the possibilities of improving the MixColumn transformation for AES Encryption. For enhancing the structure of MixColumn transformation, Common Sub-expression Elimination (CSE) algorithm has been used.

3. AES Algorithm

AES Encryption and Decryption Processors are used to processes the data blocks of fixed size using cipher key of length 128, 196 and 256 bits. AES-128 bit cipher keys are widely used for encryption and decryption. In both encryption and decryption, four types of transformations have been used for producing the cipher data and plain data. Composite S-Box is used for performing both S-Box and Inverse S-Box. S-Box is generated by taking multiplicative inverse of data input in the finite Galois Field GF (2^8) and it followed by an affine transformation. The irreducible polynomial of data input is represented as follows:

$$\boldsymbol{m(x)}=x^8 + x^4 + x^3 + x+1 \quad (1)$$

Shift Rows transformation is used to shift the rows of state byte by one byte. MixColumn transformation is used to multiply the input state byte by a common state matrix. In MixColumn transformation, matrix multiplication can be performed over GF (2^8) with output of Shift Rows transformation. The matrix multiplication of MixColumn of AES is illustrated as follows,

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

Next to MixColumn, Add RoundKey function can be performed i.e., 10 rounds of transformations can be performed, since here AES-128 bit length is considered for both input and output. The generalized flow chart of AES encryption and decryption is analyzed in Figure 1.

In Decryption side of AES, reverse operations can be performed in specific order, i.e., first Inv Shift Rows transformation can be performed instead of Inv S-box. Next to Inv Shift Rows, Inv S-Box can be performed. The final round of the algorithm is similar to the standard one,

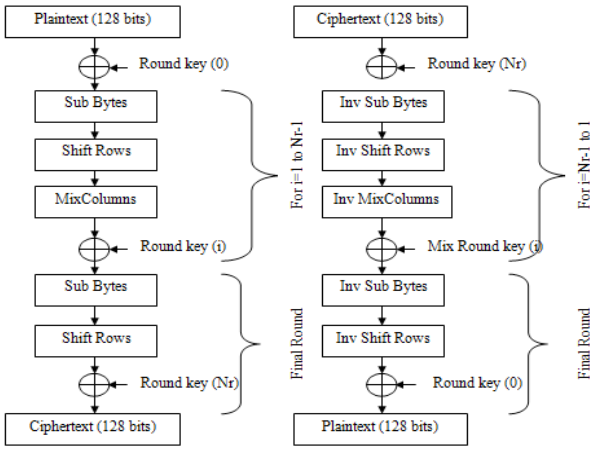


Figure 1. Generalized AES structure. **(a)** Encryption. **(b)** Decryption.

except that it does not have MixColumn operation. Matrix multiplication of Inv MixColumn of AES is illustrated as follows,

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

In[5], enhanced Inverse MixColumn design has been proposed. In this proposal, redundant logical functions are identified to reduce the most common hardware utilization. In this paper, Common Sub-expression Elimination (CSE) methods are used to improve the hardware architecture of MixColumn for the AES Encryption process.

4. Traditional Mixcolumn Design

MixColumn transformation has been performed after the Shift Rows transformation in AES Encryption. In this transformation logical state byte multiplication has been performed for providing security. In MixColumn transformation, state byte multiplication can be performed over GF (2^8) with Shift Rows transformation. As shown in Equation (2), MixColumn transformation has multiplication with 02, 03 and 01. Mostly shifters and adders are used to provide the multiplication of 02, 03 and 01. Reduced Xtime multiplication has not been developed yet for MixColumn transmissions. In[5], reduced Xtime multiplications has been developed for 09, 0D, 0B and 0E. Reduced Xtime calculation of 09, 0B, 0D and 0E has shifter and state bytes of respective coefficients. By taking exclusive of specific bits itself, MixColumn transformation functions have been performed.

Similar approaches have been already proposed in MixColumn transformation of AES Encryption. However, it should not reduce the hardware complexity effectively, since same kind of hardware resources have been utilized more than once.

In order to overcome this problem, common sub-expressions (same hardware utilizations) are to be identified and eliminated. Design of enhanced MixColumn has been proposed in this research work.

5. Enhanced MixColumn Design

In this proposed work, common sub-expressions of MixColumn transformation has been identified and eliminated to further reduce the hardware complexity of AES Encryption. The procedure for designing an Enhanced MixColumn transformation of AES Encryption has been demonstrated as follows:

From Equation (2), it can possible to write as,

$$s'_{0,c} = (\{02\} * s_{0,c}) \otimes (\{03\} * s_{1,c}) \otimes (\{01\} * s_{2,c}) \otimes (\{01\} * s_{3,c}) \quad (4)$$

$$s'_{1,c} = (\{01\} * s_{0,c}) \otimes (\{02\} * s_{1,c}) \otimes (\{03\} * s_{2,c}) \otimes (\{01\} * s_{3,c}) \quad (5)$$

$$s'_{2,c} = (\{01\} * s_{0,c}) \otimes (\{01\} * s_{1,c}) \otimes (\{02\} * s_{2,c}) \otimes (\{03\} * s_{3,c}) \quad (6)$$

$$s'_{3,c} = (\{03\} * s_{0,c}) \otimes (\{01\} * s_{1,c}) \otimes (\{01\} * s_{2,c}) \otimes (\{02\} * s_{3,c}) \quad (7)$$

Further, Equation (4) to (7), can be simplified as,

$$s'_{0,c} = \lfloor \{02\} * s_{0,c} \rfloor \otimes \lfloor (\{02\} * s_{1,c}) \otimes s_{1,c} \rfloor \otimes \lfloor s_{2,c} \rfloor \otimes \lfloor s_{3,c} \rfloor \quad (8)$$

$$s'_{1,c} = \lfloor s_{0,c} \rfloor \otimes \lfloor \{02\} * s_{1,c} \rfloor \otimes \lfloor (\{02\} * s_{2,c}) \otimes s_{2,c} \rfloor \otimes \lfloor s_{3,c} \rfloor \quad (9)$$

$$s'_{2,c} = \lfloor s_{0,c} \rfloor \otimes \lfloor s_{1,c} \rfloor \otimes \lfloor \{02\} * s_{2,c} \rfloor \otimes \lfloor (\{02\} * s_{3,c}) \otimes s_{3,c} \rfloor \quad (10)$$

$$s'_{3,c} = \lfloor (\{02\} * s_{0,c}) \otimes s_{0,c} \rfloor \lfloor s_{1,c} \rfloor \otimes \lfloor s_{2,c} \rfloor \otimes \lfloor s_{3,c} \rfloor \quad (11)$$

From Equation (8) to (11), it is clear that multiplication of source signals with {02} and {03} are redundantly used for the calculation of MixColumn transformation. These common resources are represented as follows,

$$c1_{02} = \{02\} * s_{0,c} \quad (12)$$

$$c2_{02} = \{02\} * s_{1,c} \quad (13)$$

$$c3_{02} = \{02\} * s_{2,c} \quad (14)$$

$$c4_{02} = \{02\} * s_{3,c} \quad (15)$$

The hardware complexity of MixColumn transformation can be absolutely reduced, when utilizing the common resources to all numerical calculation of MixColumn transformation. Further Equation (8) to (11) can be simplified as,

$$s'_{0,c} = [c1_{02}] \otimes [c2_{02} \otimes s_{1,c}] \otimes [s_{2,c}] \otimes [s_{3,c}] \quad (16)$$

$$s'_{1,c} = [s_{0,c}] [c2_{02}] \otimes [c3_{02} \otimes s_{2,c}] \otimes [s_{3,c}] \quad (17)$$

$$s'_{2,c} = [s_{0,c}] \otimes [s_{1,c}] \otimes [c3_{02}] \otimes [c4_{02} \otimes s_{3,c}] \quad (18)$$

$$s'_{3,c} = [c1_{02} \otimes s_{0,c}] \otimes [s_{1,c}] \otimes [s_{2,c}] \otimes [s_{3,c}] \quad (19)$$

From Equation (16) to (19), it is clear that coefficient of MixColumn transformation based multiplications is reduced effectively and hence the speed of MixColumn transformation can be increased successfully. Only multiplication of {02} is estimated manually and the remaining coefficients use the same hardware resources for the further multiplication. The proposed model of Enhanced AES Encryption structures have been illustrated in Figure 2. When compared to traditional architecture, proposed architecture reduces more than 5 gates for performing MixColumn transformation based multiplication.

6. Simulation Results and Performance Evaluations

Proposed Enhanced and Traditional MixColumn based AES Encryption methods have been designed by using Verilog Hardware Description Language (Verilog HDL). Simulation result of Proposed Enhanced MixColumn based AES Encryption has been evaluated by using ModelSim 6.3c and Synthesis results have been estimated by using Xilinx 10.1i (Family-Virtex 4, Devices-XC4VLX25/XC4VLX15, Package- FF668 and Speed: -12) design tool. The simulation result of traditional and proposed Enhanced MixColumn has been illustrated in Figure 3 and Figure 4 respectively. Further, traditional and proposed Enhanced MixColumn transformation has been integrated into AES Encryption process. Simulation result of Proposed MixColumn transformation based AES Encryption has been illustrated in Figure 5. As shown in Figure 5, 128-bit input data "1234567890abcdef1234567890abcdef" is given in hexadecimal format. Encrypted output obtained as "7838e4e0a0876581f7fde709c2f5ad6c" in hexadecimal format. Simulation result of AES Decryption has been illustrated in Figure 6. In Figure 6, encrypted data is given to decryption side as input and output obtained as "1234567890abcdef1234567890abcdef". Further Register Transfer Logic (RTL) view of both traditional and proposed Enhanced MixColumn based AES Encryption process has been illustrated in Figure 7 and Figure 8 respectively.

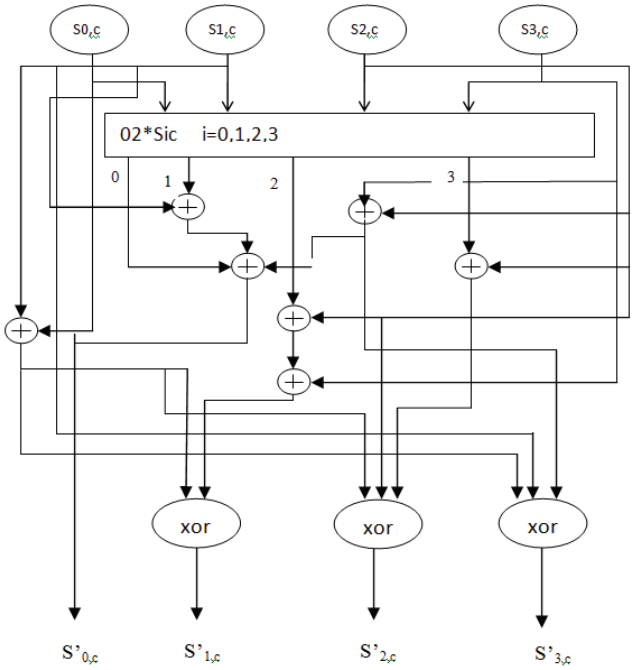


Figure 2. Proposed Model of Enhanced MixColumn Transformation.

Table 1 illustrates the comparison result of traditional and proposed Enhanced MixColumn transformation design. Proposed Enhanced MixColumn transformation offers 10.93% reduction in Slices, 13.6% reduction in LUTs and 1.19% reduction in delay consumption than traditional MixColumn transformation architecture of AES Encryption. Comparison of both traditional and pro-

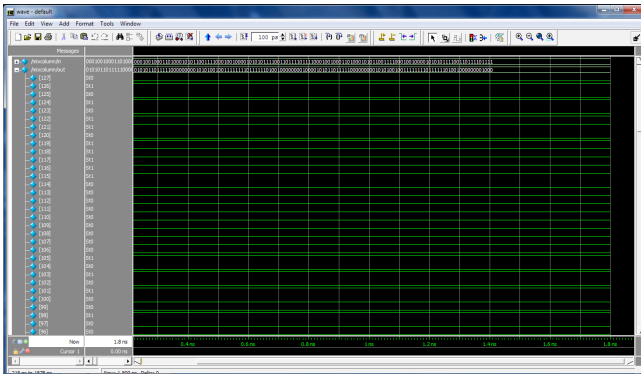


Figure 3. Simulation result of traditional MixColumn architecture.

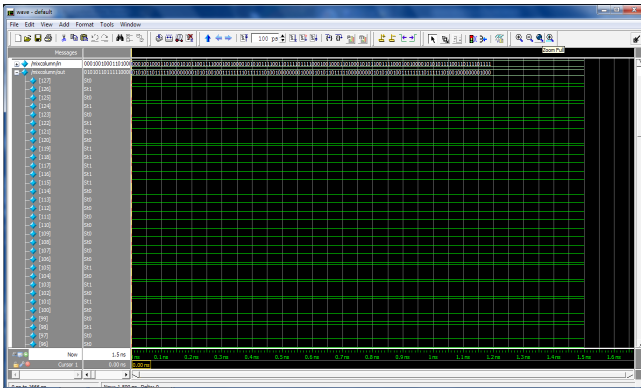


Figure 4. Simulation result of Proposed MixColumn architecture.

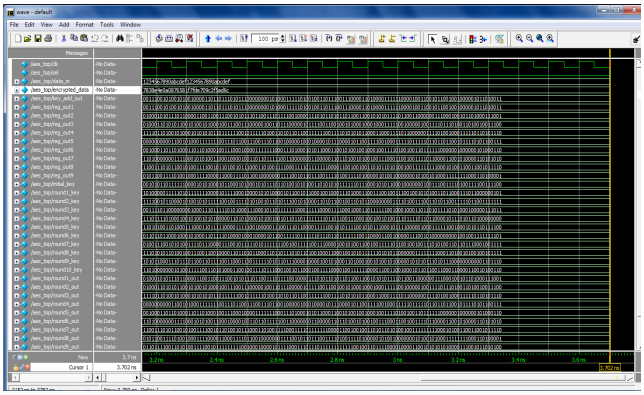


Figure 5. Simulation result of Proposed MixColumn based AES Encryption.

posed Enhanced MixColumn transformation function has been graphically illustrated in Figure 9. Further proposed enhanced MixColumn transformation technique is integrated into AES Encryption algorithm for increasing the performances of AES Encryption in terms

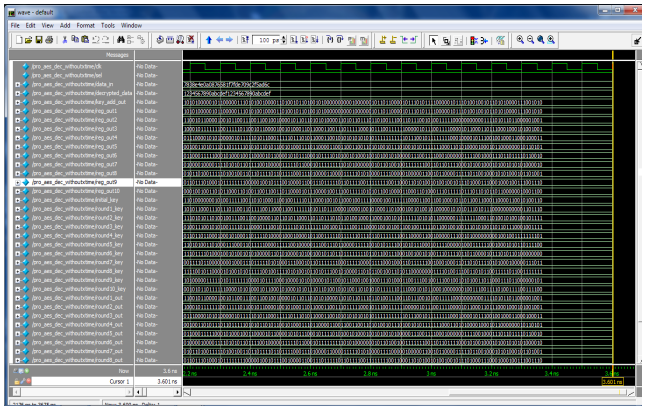


Figure 6. Simulation result of AES Decryption result.

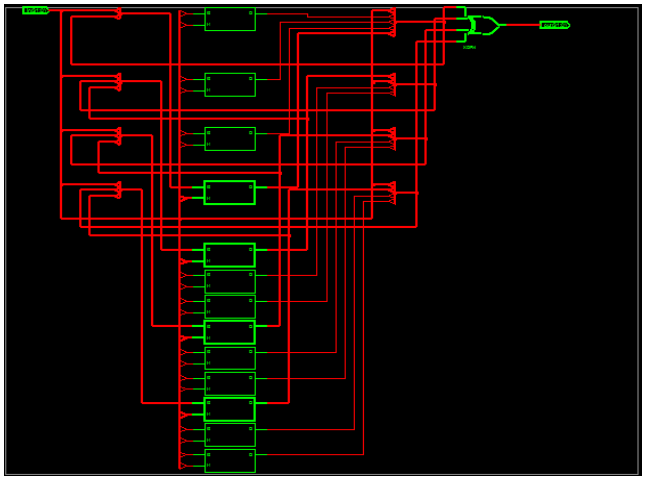


Figure 7. RTL View for traditional MixColumn transformation.

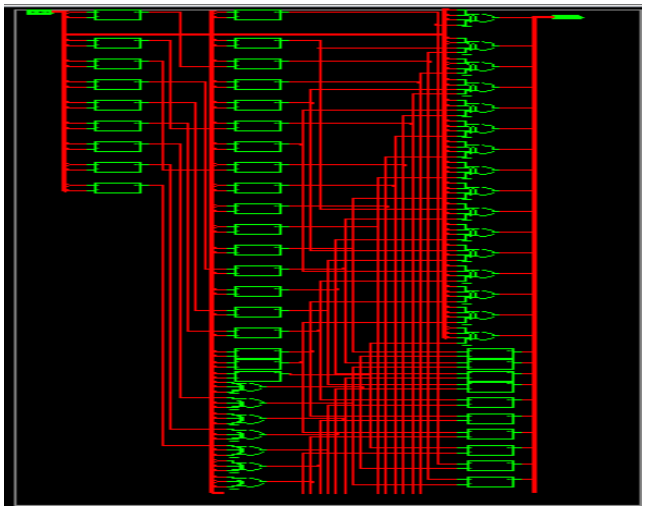


Figure 8. RTL View for proposed Enhanced MixColumn transformation.

Table 1. Comparison of performances of traditional and Proposed Enhanced MixColumn transformation

Types/Parameters	Slices	LUTs	Delay (ns)
Traditional MixColumn transformation	128	250	5.682
Proposed Enhanced MixColumn transformation	114	216	5.614

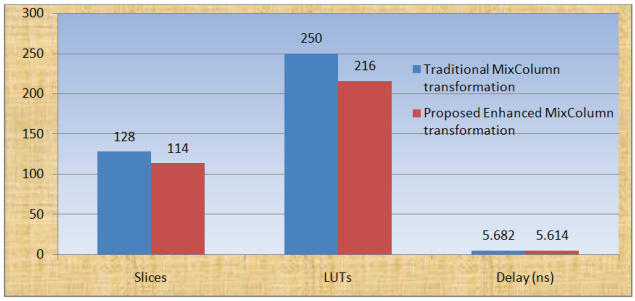


Figure 9. Comparison of traditional and Proposed Enhanced MixColumn transformation.

X axis : Methods (Traditional MixColumn Transformation and Proposed Enhanced MixColumn Transformation).
Y axis : Slices & LUTs (1 unit = 50), Delay (1 unit = 50ns).

Table 2. Comparison of Performances of traditional MixColumn transformation based AES Encryption and Proposed Enhanced MixColumn transformation based AES Encryption

Types/Parameters	Slices	LUTs	Power (nW)
Traditional MixColumn transformation based AES Encryption	8928	16880	6.775
Proposed Enhanced MixColumn transformation based AES Encryption	8884	16077	6.466

of VLSI crucial factors. Comparison of performances of traditional MixColumn transformation based AES Encryption and proposed enhanced MixColumn transformation based AES Encryption has been analyzed and compared in Table 2. It shows that, Proposed Enhanced MixColumn transformation based AES Encryption offers 4.75% reduction in area and 4.56% reduction in power consumption than traditional MixColumn based AES Encryption. Comparison of both traditional and Proposed Enhanced MixColumn transformation based AES Encryption has been graphically illustrated in Figure 10.

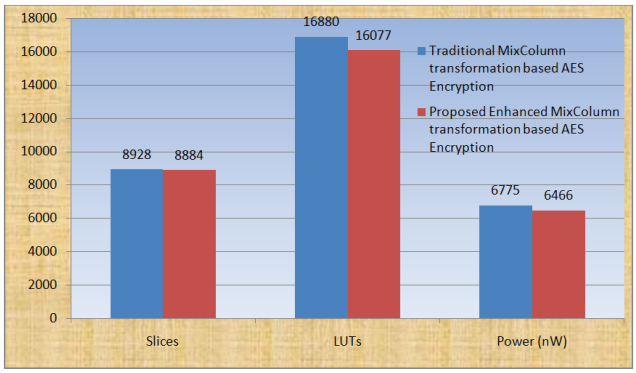


Figure 10. Comparison of traditional and Proposed Enhanced MixColumn transformation based AES Encryption.

X axis : Methods (Traditional MixColumn Transformation based AES Encryption and Proposed Enhanced MixColumn Transformation based AES Encryption).
Y axis : Slices & LUTs (1 unit = 2000), Power (1 unit = 2000mW).

7. Conclusion

In this paper, Common Sub-expression Elimination (CSE) technique has been used to design the Enhanced MixColumn transformation for AES Encryption. VLSI is the current hot domain area in the integrating multi-application in the minimized chip. The main goal of this research work is to reduce the hardware complexity and power consumption of AES Encryption. In order to increase the performances of AES Encryption, MixColumn transformation has been considered to reduce the complexity of hardware structure. The remaining structure of AES Encryption except MixColumn transformation has the simplest path to transmit the data for providing cipher data from plain data. Hence, CSE algorithm has been used in this research work to eliminate the most redundant path of AES MixColumn transformation. Proposed Enhanced MixColumn transformation offers 10.93% reduction in Slices, 13.6% reduction in LUTs and 1.19% reduction in delay consumption than traditional MixColumn transformation architecture of AES Encryption. Similarly, Proposed Enhanced MixColumn transformation based AES Encryption offers 4.75% reduction in area and 4.56% reduction in power consumption than traditional MixColumn based AES Encryption. In future, proposed structure will be used in space and terrestrial communication based application for providing security with the help of minimum cost based AES hardware architecture.

8. References

1. Anitha S, Suganya M. Area optimized in storage area network using novel MixColumn transformation in masked AES. IJETT. 2015 Feb; 20(6):275–82.
2. Balamurugan J, Logashanmugam E. VLSI based minimized composite S-Box and invere MixColumn for AES encryption and decryption. IJRSET. 2015; 13(8):32–42.
3. Balamurugan J, Logashanmugam E. Design of a high speed and area efficient optimized MixColumn for AES. IJAER. 2015; 2(4):32–42.
4. Balamurugan J, Logashanmugam E. Enhanced inverse MixColumn design for AES decryption. EJSR. 2015 Jul; 133(3):358–68.
5. Fischer V, Drutarovsky M, Chodowiec P, Gramain F. InvMixColumns decomposition and multilevel resource sharing in AES implementations. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2015; 13(8):989–92.
6. Jishamol TK, Rahimunnisa K. Low power and low area design for advanced encryption standard and fault detection scheme for secret communications. IEEE International Conference on Communications and Signal Processing; 2013 Apr 3-5. p. 743–7.
7. Lala K, Kumar A, Kumar A. Enhanced throughput AES encryption. IJECSE. 2012; 1(4):2132–7.
8. Priya S, Kumar KP, Sivamangai NM, Rejula V. FPGA implementation of efficient AES encryption. IEEE International Conference on Innovations in Information, Embedded and Communication Systems; 2015. p. 1–4.
9. Baek S-S, Won Y-S, Han D-K, Ryou J-C. The effect of eight-shuffling AES implementations techniques against side channel analysis. Indian Journal of Science and Technology. 2015; 8(15).
10. Sharma TM, Thilagavathy R. Performance analysis of advanced encryption standard for low power and area applications. IEEE Conference on Information and Communication Technologies; 2013 Apr 11-12. p. 967–72.