Area optimized in storage area network using Novel Mix column Transformation in Masked AES

Mrs.S.Anitha[#1,] Ms.M.Suganya[#2]
[#1]*Assistant professor,* [#2]*P.G.Scholar, II M.E.VLSI Design*
[#1,#2]*Department of Electronics and Communication Engineering,*
[#1,#2]*Avinashilingam Institute for Home Science and Higher Education for Women-University*
Coimbatore, India

Abstract:

Advanced Encryption Standard was implemented in cryptographic techniques like Data Encryption Standard and Triple Data Encryption Standard. Advanced Encryption Standard is more secure and faster than conventional techniques. Advanced Encryption Standard are used to map the input values from GF(2^8) to GF(2^4) at the beginning of the operation and map the result back from GF(2^4) to GF(2^8) at the end of the operation, which reduces area resources. But further area reduction is possible by implementing a novel technique in mix column.

Keywords: **Data Encryption Standard (DES),Triple Data Encryption Standard (3DES)**

I. INTRODUCTION

Cryptography is a kind of processing techniques which is closely related to the disciplines of cryptology. It is a method of storing and transmitting data in a particular format such that only intended person can read it. The main objective of encryption is to scramble the plaintext (readable form) in to ciphertext(unreadable form). In decryption, the scrambled data is converted back to plaintext. Correct decryption key is necessary to recover the original contents. The function of key is to undo the work of encryption algorithm. Encryption/Decryption is mostly important in Wireless communication, because wireless circuits are easier to hack than their hard-wired counterparts. Encryption/Decryption is a good idea when carrying out any kind of sensitive data such as online purchase using credit card, and discussion of a company secret between different organizations. If the cipher is stronger then it will be more harder for unauthorized people to hack it. In order to maintain the secrecy and to minimize fraud, the strong encryption is required as a potential vehicle by which third parties can't hack any of the information. Encryption is used in all mode of applications such as files and digital transfer, Here two different cryptographic techniques such DES and 3DES were followed.

A.DES and 3DES

Data Encryption Standard (DES) is a well known cipher. DES has been applied in software and in all kind of banks over many years. During the design phase, National Security Agency(NSA) was consulted and warned that some trapdoor might be possible in DES. The weak point of DES is key size of about 56bit. In 1998 the Electronic Frontier Foundation (EFF) found a special computer called Deep Crack Machine, it could decrypt a DES within a average time of 4.5days.In order to overcome these constraints, another technique called 3DES was adopted. In 3DES the key size is simply extended to three times in succession with three different keys. The key size is about 168 bits almost beyond the reach of brute force attacks which is used by the EFF DES cracker, but 3DES is very slow especially in software, hence DES and 3DES does not fulfil the requirements of a modern algorithm. To overcome all these limitations another technique has been adopted called Advanced Encryption Standard (AES).

II. EXISTING METHOD

In 1997, National institute of standards and technology (NIST) expected new candidates to overcome the aging of Data Encryption Standard (DES).NIST declared that Rijindael as the proposed

AES and was submitted by Joan Daemen and Vincent Rijmen.AES is considered as a strong cipher consists of 128-bit block size. It allows for three different key lengths 128,192 or 256 bits. Encryption consists of 10 rounds for 128-bit keys,12 rounds for 192-bit keys, and 14 rounds for 256 bit keys, except for the last round remaining all other rounds are identical. Masked AES constituted S-box over GF(2^8) has two 8-bit input and output for storing large area. It is large enough to be fit in to any field programmable gate array. To make feasible implementation the only possible way is to transform the AES from GF(2^8) to GF(2^4).Hence the entire process like masked mix column ,masked shift rows, masked add round key is performed mainly over GF(2^4),finally the output values are transformed from GF(2^4) to GF(2^8).

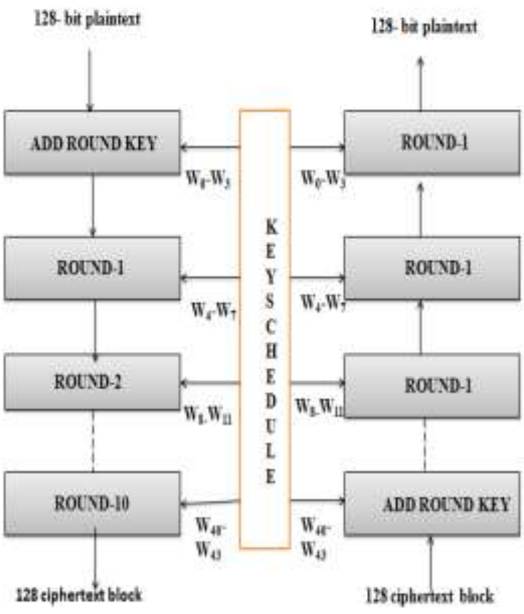


Fig1:Structure of AES for 128 bit

Fig1, the given input to the add round key is 128bit plaintext. Here W_0-W_3 is a key XORed with plaintext, then the result from the add round key is followed by the remaining rounds. For 128 bit plaintext,AES consists of 10 rounds.

Each round consists of four stages as shown in Fig2

- Substitute bytes
- Shift Rows
- Mix Columns
- Add round key

1. Sub Byte transformation(S box substitution):S-box is a first stage used to provide non linearity and confusion, which is constructed by multiplicative inverse.

2. Shift Row: It performs rotation which is used to provide inter-column diffusion, where the bytes in the last three rows of the states are cyclically shifted. Main goal is to scramble the data

3. Mix Column: Manipulations are used to provide inter-byte diffusion where each column vector is multiplied by a fixed matrix. The bytes will be treated as polynomials rather than numbers

4. AddRoundKey: Last stage in the process is a round key where bytes XORed with each of the state, hence the round key byte provides confusion

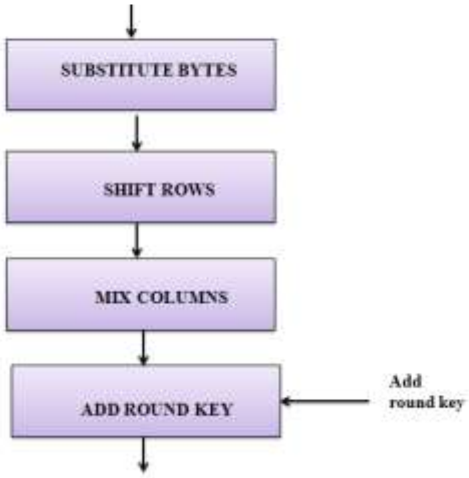


Fig2:One round of encryption

A.Substitute bytes:

Fig3 depicts the block diagram of sub bytes. In this step lookup table is used to make a replacement for a given byte in the input state array. Lookup table entries are created by using multiplicative inverse. Substitute bytes are mainly used to scramble the data in order to avoid the correlations. For example, byte {95}, the leftmost byte specified as row and the rightmost byte specified as column

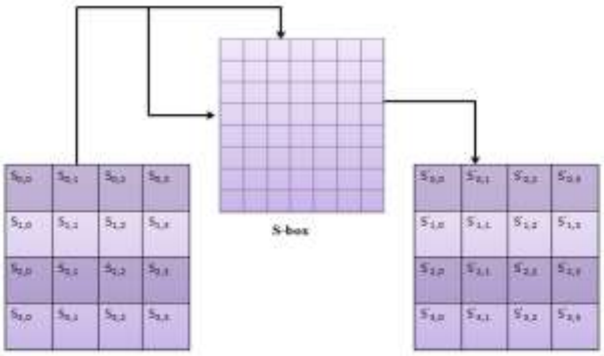


Fig3:Substitute bytes

B.Shift row Transformation:

Fig4 depicts a shift row transformation.For encryption, the rows are rearranged during the forward process. Goal of transformation is to scramble the data order. Shift row transformation consists of

- First row of the state array is not shifting
- Alter the second row by one byte to the left circularly
- Alter the third row by two bytes to the left circularly
- Alter the last row by three bytes to the left circularly

For the decryption, inverse shift rows performs the circular shifts in the opposite direction.

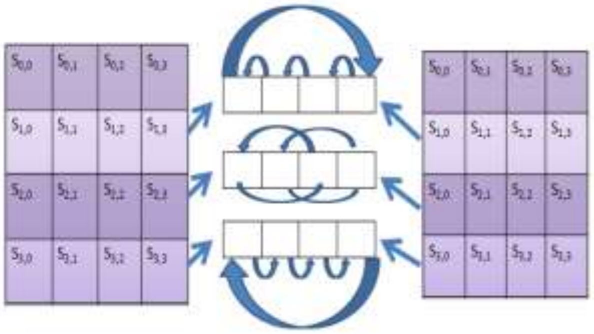


Fig4:Shift Rows

C.Mixcolumns

Fig5 each column is individually operated. Each byte in a column is mapped in to a new value.

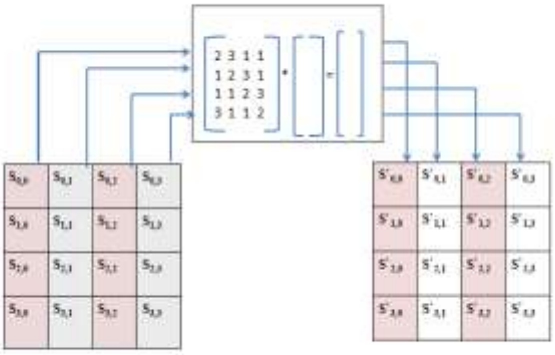


Fig5:MixColumns

Each column on the left most matrix is multiplied with constant matrix and the obtained value is stated to right side. Now the right side matrix is considered as new state matrix for the following steps. Here additions involved are meant to be XOR operations.

As a result of this multiplication, the four bytes in a column are replaced by the following equations as (i) [1] & [2]

$S'_{0,c} = (\{02\} \,.\, S_{0,c}) \oplus (\{03\}.S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$

$S'_{1,c} = S_{0,c} \oplus (\{02\} \,.\, S_{1,c}) \oplus (\{03\}.S_{2,c}) \oplus S_{3,c}$

$S'_{2,c} = S_{0,c} \oplus S_{1,c} \oplus (\{02\} \,.\, S_{2,c}) \oplus (\{03\}.S_{3,c})$

$S'_{3,c} = (\{03\} \,.\, S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\}.S_{3,c})$ (i)

D. Add round key:

Fig6 depicts add round key, executes one column at a time and adds a round key word with each column of the state matrix. Key Expansion process is necessary to generate the round keys for each round. Each round has its own round key that is deduced from the original 128-bit encryption key. The sub keys are derived from the original key by XORing with previous columns. For columns that are in multiples of four, the process involves round constant addition and substitute bytes. The deciphering is therefore the reverse order of the ciphering process

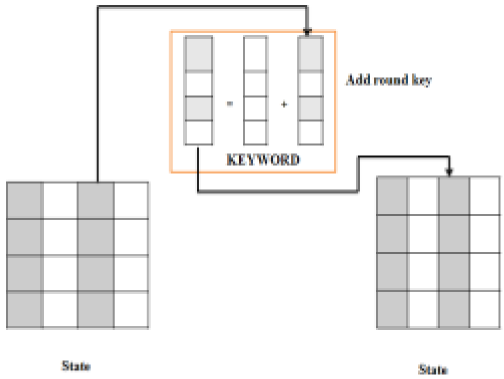


Fig6:Add round key

The first column of the encryption key consists of four bytes representing the word w_0,next column consist of another four bytes representing the word w_1 and so on.

$$\begin{pmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{pmatrix}$$

$$\Downarrow$$

$$[\; W_0\; W_1\; W_2\; W_3 \;] \qquad \text{(ii)}$$

This algorithm expands the words up to 44 word key. Remaining 40 words of the key schedule are used for the forthcoming rounds.

$$W_{0,}\, W_{1,}\, W_{2,}\, W_{3}\, ,\dots\dots\dots\dots\, W_{43} \qquad \text{(iii)}$$

Key expansion is quite difficult part, it sense each column of four words and decides upon the next column of the four words.W_0,W_1,W_2,W_3 is the round key for the initial round, similarly W_4,W_5,W_6,W_7 is the round key for round 1 and so on

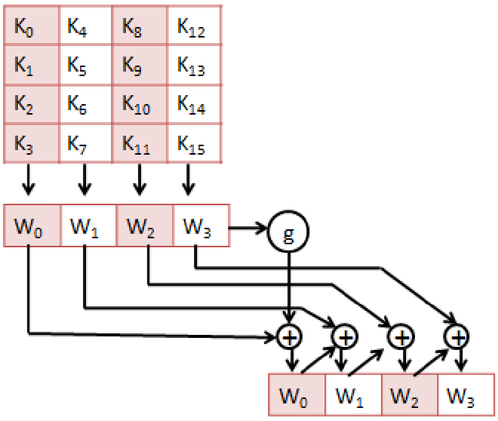


Fig7:Key Expansion

In fig7 XOR'ing the first word of the key with the value that is being returned from a function g() takes place at the last word of the previous grouping function. g() function comprises the following three steps

- Rot Word
- Sub Word
- R Con

Rot word takes four byte as input word $[a_0,a_1,a_2,a_3]$ and it manipulates the cyclic permutation and get the result as$[a_0,a_1,a_2,a_3]$. Sub word () it consider four byte word and applies the S-box(substitute bytes)to produce an output word. XORing the bytes obtained from the previous steps is known as round constant. In round constant first three rightmost bytes are always zero.

The round constant for the ith round is denoted Rcon[i].Since, by specification, the three right most[4] bytes of the round constant are zero, The left hand side of the expression stands for the Rcon[i] = (RC[i], 0x00, 0x00, 0x00)round constant to be used in the ith round. The right hand side of the equation says that the rightmost three bytes of the round constant are zero. The addition of the round constants is for the purpose of destroying any symmetries that may have been introduced by the other steps in the key expansion algorithm.

III. XTIME CIRCUIT:

In the conventional masked AES architecture, complex mix column is used. It comprises of 8 multipliers and 11 adder operators. If number of adders and multipliers are large, then system becomes more complex and introduces delay in the process. Complexity in system area leads to delay in execution process. In order to overcome the above drawbacks AES mix column is proposed to get less area and delay than the existing mix column. In this new scenario the architecture of mix column is reduced using X-time circuit. Proposed mix column comprises of 12 adders and 4 xtime circuit. To reduce the circuit complexity in the conventional mix column, the X-time circuit is introduced instead of using multiplier.

IV.PROPOSED METHOD

A. For Encryption

Instead of multiplying each column with constant Matrix and to avoid the Polynomial Co-efficient calculation, the preferable technique is to use Novel Mixcolumn, with a fixed coefficient Architecture.

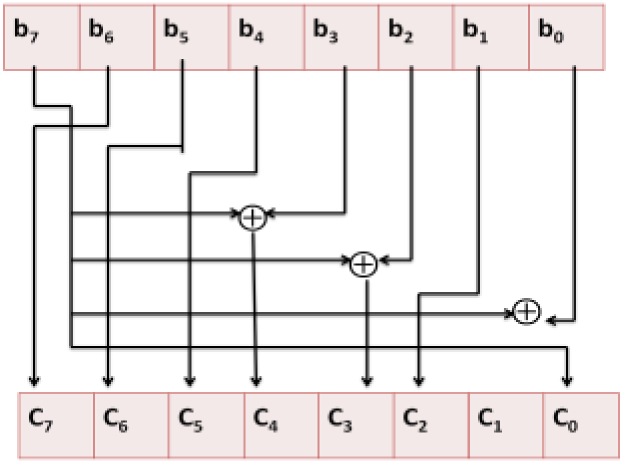


Fig8:Fixed Coefficient for value (02)[7]

Fig8 consists of 8bits,each bit is shifted and is xor-ed with any one of the bit values based on the structure and it shows the following Operations

{02}*b(x)=(b7)+(b0+b7)x+(b1)x2+(b2+b7)x3+(b3+ b7)x4 + (b4)x5 + (b5)x6 + (b6)x7 (iv)

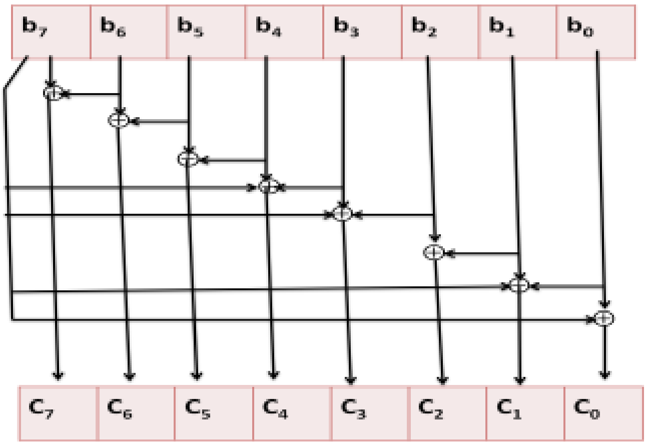


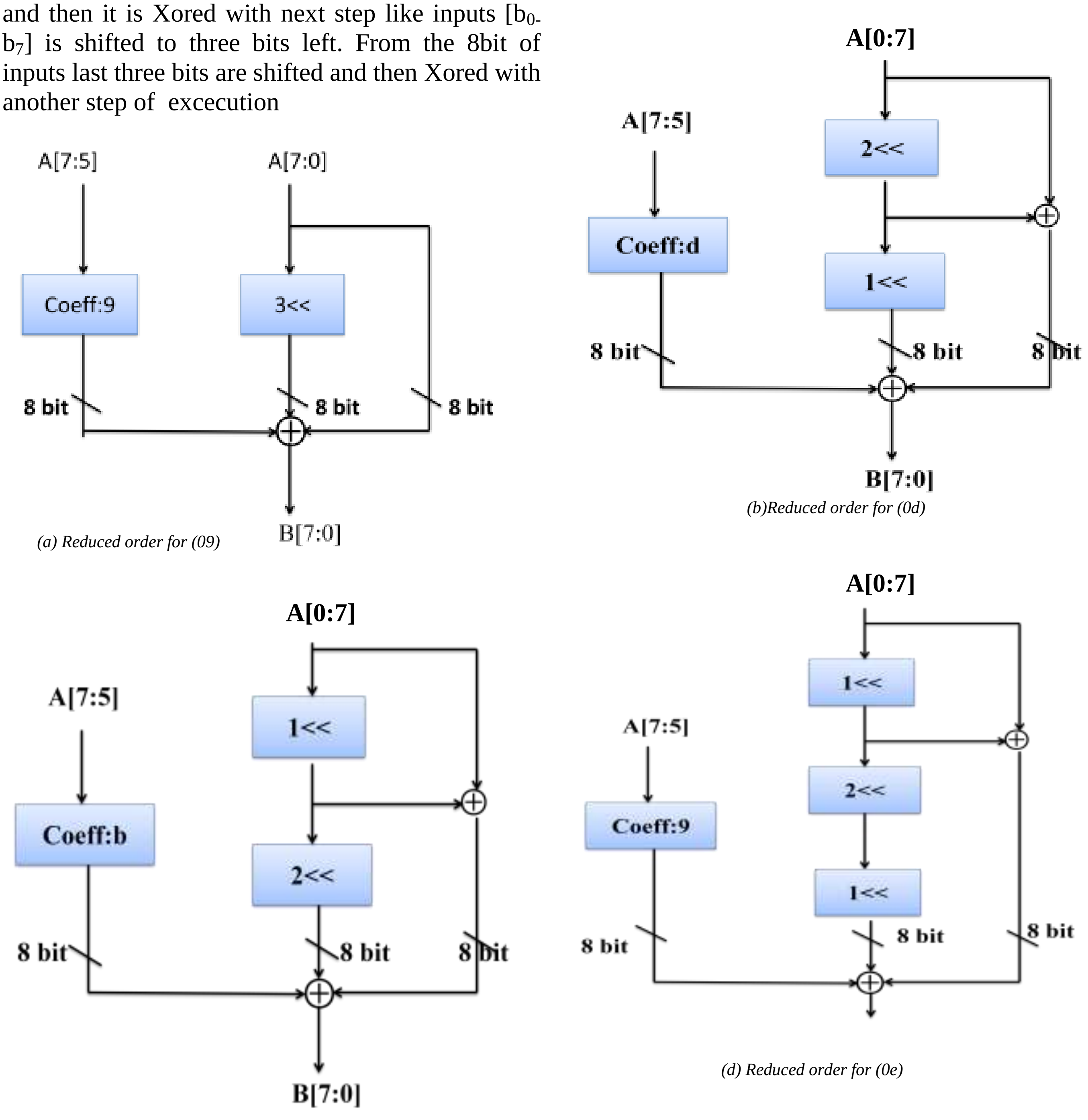
Fig 9 Fixed Coefficient for value (03)

Fig9 represents Fixed coefficient for value (03) consists of 8 bits, each bit is shifted and Xored with consecutive value to scramble the data. The calculations are

{03}*b(x)=(b0+b7)+(m0+m1+m7)x+(m1+m2)x2+(m2+m3+m7)x3+(m3+m4+m7)x4+(m4+m5)x5+(m5+m6)x6+(m6+m7)x7 (v)

B. For Decryption

In conventional technique, Decryption it consumes more area, delay power and more computation work .To come out from this problem, Inverse Mix-Columns unit is redesigned using optimised structures which excecute shifting operations directly than XOR. Number of Shifting and XOR operation is reduced in projected Inverse Mix-Columns structure. Hence reduced Inverse Mix-Columns presents less area, than conventional X-Time based AES decryption process. In Fig10 a Reduced Xtime for 09,0b,0d,0e value is represented. Here it consists of 8bits as inputs[b0:b7] and the last three bits[b5:b7] are considered to make some modifications based on equations are $T_{7=}0$, $T_{6=}b_7$, $T_{5=}b_6 \oplus b_7$, $T_{4=}$ $b_5 \oplus b_6$, $T_{3=}$ $b_5 \oplus b_{7,} T_{2=}T_5$, $T_{1=}T_4$, $T_{0=}b_{5,}$for (09) value similarly there is formula for 0b,0d,0e conditions, and then it is Xored with next step like inputs [b$_0$-b$_7$] is shifted to three bits left. From the 8bit of inputs last three bits are shifted and then Xored with another step of excecution



(a) Reduced order for (09)

(b)Reduced order for (0d)

(c) Reduced order for (0e)

(d) Reduced order for (0e)

Fig10:Reduced Structure for 09,0b,0d,0e

Here, only 3XOR operations are required for every step of 09, 0b, 0d and 0e structures. Hence it is called as reduced Xtimeunit. In this paper, a novel Inverse MixColumns of 09,0b,0d and oe are performed using reduced Inverse MixColumns. Then this Inverse Mix Columns based on reduced Xtime is incorporated into AES 128-bits cryptography operations process for high security, smaller chip size, high speed and low power utilizations than the conventional Xtime based AES 128-bits

V.SIMULATION RESULT

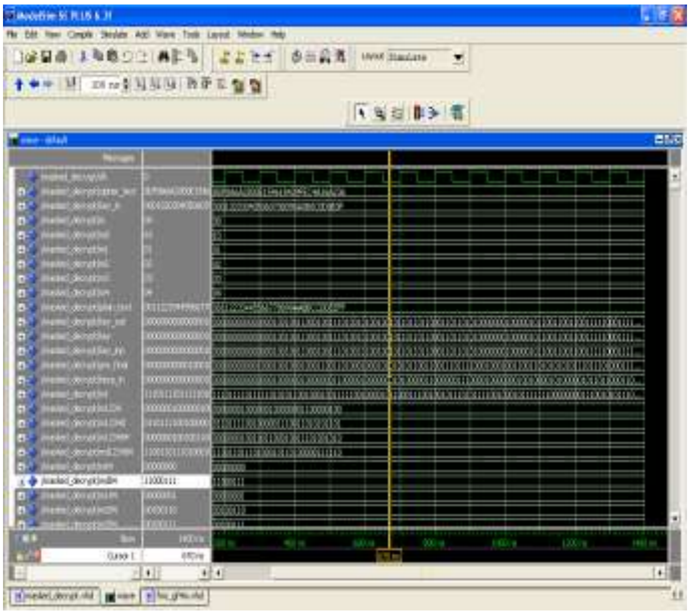


Fig 11 proposed Encryption

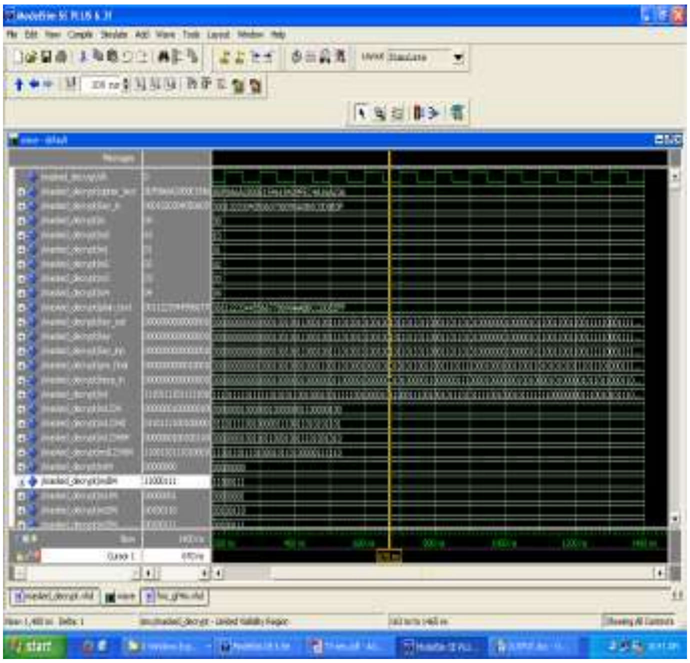


Fig 12 proposed decryption

	Existing Area	Proposed Area
Mix column	509	354
InverseMix column	676	440

Table.1 Comparison Table

Fig 11 & 12 represents proposed encryption and Decryption result. The performances of proposed AES with reduced Xtime over existing AES with regular Xtime are analyzed.

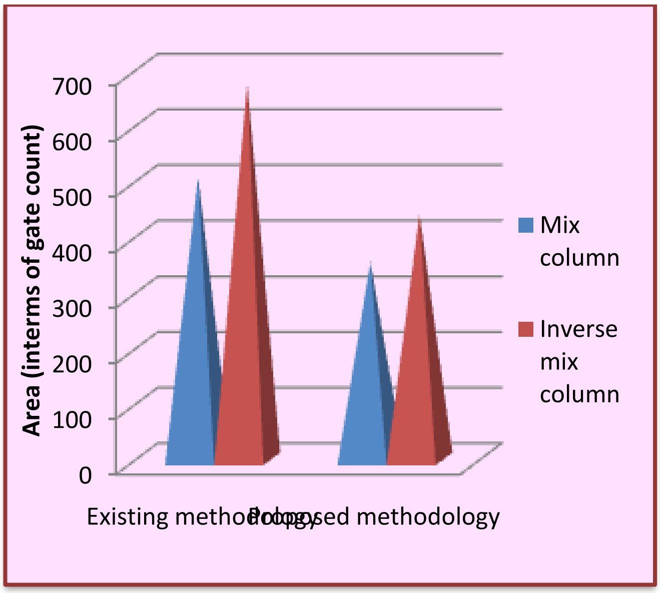


Fig 13AES Report

In Fig11 shows AES report, the Area consumption in case of existing AES Mix Column, number of slices occupied in existing AES is 509, which is improved to 354 using Fixed Co-efficient Mix Column structure, similarly in inversed mix column number of slices occupied in existing AES is 676 which is improved to 440 using Reduced Order Structure for 09,0b,0e,0d proposed AES with reduced inverse MixColumns based on Shrunk Xtime unit.

V.CONCLUSION

Fixed coefficient Technique is applied in the Mix column process to reduce the area than the conventional techniques, similarly for inverse mix column Reduced 09, 0b, 0d and 0e Technique is used and is designed using shrunk Xtime. These shrunk Xtime is applied in the inverse MixColumns process to analyze the performance. After applying the shrunk Xtime in Inverse MixColumns further reduction in the area is achieved. The proposed AES with reduced Mix column and Inverse Mix Columns offers more product than the conventional AES process. This AES can be used in high security applications such as satellite communication techniques, Net Banking and ATM. The proposed Inverse MixColumns with reduced Xtime unit is best to use in Applied Predictive Technologies product. Fixed coefficient and reduced shrunk technique is coded using VHDL and simulated using modelsim. Synthesis Report can be analysed using Xilinx ISE 9.1 software

Reference

[1] Design of "High Speed AES-128 using Novel Mix Column Transformation and Subbytes" by K.Sandyarani,Dr.p.Nirmal Kumar Journal of Computer Apllications Volume VII, Issue 2, 2014

[2] Incorparation of Reduced 09,0B,0D and 0E Structures Into Inverse MixColumns For AES-128 TechniquesJournal of Theoretical and Applied Information Technology 10th December 2014. Vol.70 No.1 © 2005 - 2014 JATIT & LLS. All rights reserved

[3] Design and Implementation a different Architecture of Mixcolumn in FPGA Department of Electronics and treatment of information university hassan ii mohammedia, Casablanca, Morocco

[4] The Advanced Encryption Standard(AES):The Successor of DES, Dr Reinhard Wobst

[5] Design of High Speed and Low area Masked AES using Complexity Reduced Mix-Column Architecture, IJCSEC-International Journal of Computer Science and Engineering Communications, Vol.2 Issue.3, May 2014. ISSN: 23478586,J.Balamurugan1,Dr.E.Logashanmugam2Research Scholar1, Professor and Head2, St.Peter's University1, Sathyabama University2, TN, India

[5] A VHDL Implementation of the Advanced Encryption Standard-Rijndael Algorithm by Rajender Manteena,Wilfrido Moreno,Ph.D.James Leffew,ph.d.Wei Qian,Ph.d March 23,2004

[6]Image Cipher Technique for Covert and Low Bandwidth Channels Sangeeta Solanki1, A.K.Vats1, Shikha Maan1 (Corresponding Author: Sangeeta Solanki) School of computer engg & IT. Shobhit University, Meerut, U.P.

[7]FPGA implementations of advanced encryptionstandard: a survey shylashree.n1, nagarjun bhat2 and v. shridhar31research scholar (r.n.s.i.t),in e.c.e, at pesce, mandya, karnataka, india 2student, b.e (4th semester), dept of ece, rnsit 3professor, in e.c.e, at p.e.s.c.e, mandya, karnataka, india

[8]lightweight mix columns implementation for aes, computer systems department computer systems department information system department faculty of computer and information science ain shams university abbasiaa, cairo

[9] International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 183-188 The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012) Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key

[10]Evaluation of Countermeasures Implementations Based on Boolean Masking to Thwart Side-Channel Attacks Houssem Maghrebi, Jean-Luc Danger, Florent Flament, Sylvain Guilley, Laurent Sauvage
D´epartement COMELEC Institut TELECOM, TELECOM ParisTech, CNRS LTCI (UMR 5141), 46 rue Barrault, 75 634 Paris Cedex, France.