Design of Low Power Mixcolumn in Advanced Encryption Standard Algorithm

M. Anitha Christy[1], S. Sridevi Sathya Priya [2]

Abstract— the security data transmission algorithm in cryptography is Advanced Encryption Standard (AES). The operation mix column consumed more power in the algorithm. In this paper the power consumption of mix column is reduced in order to achive the total power consumption of AES. Using a simple exclusive OR gate that is XOR gate pass transistor logic, the power can be minimized when compare to the other methods of design the mixcolumn transformation. The design is implemented using the cadence Schematic Editor. The proposed methodology gives the low power as 3.996nW. The advantage of low power mixcolumn is playing an important role in today's security needs like RFID tags, smart cards.

Index Terms — Advanced Encryption Standard (AES), Cryptography, Encryption, low power, Mix Column architecture, Pass transistor logic.

1 INTRODUCTION

Cryptography is the art of hiding the information secret when transfers avoid the involvement of the third parties. Symmetric key is used when the both encryption and decryption keys are same. In same way the Asymmetric chiper key is known as both sender and receiver has the different kind of keys as for encryption and decryption respectively. The Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001 [1]. AES is a symmetric block cipher that is used to replace DES, Triple- DES algorithms for the wide range of application. The AES approach is stronger & faster than Triple-DES [2].

Cryptography is most often connected with scrambling plain text into cipher text (encryption) then back into its original form (decryption). The block size is same as 128bits in AES and key length is varies according to the number of rounds involved in the encryption or decryption.

The main concentration goes on the mixcolumn to reduce the overall power consumed. To reduce the power, AES Mixcolumn is converted into logical. It consists of only XOR operations. The two inputs XOR gate Pass Transistor is used. Pass transistor logic offers transistors less in count when compare to the conventional CMOS and also provide the greater power reduction.

1. M. Anitha Christy, Research Scholar

2. S. Sridevi Sathya Priya,

In Section II, we discuss the basic operations involved in AES and the detail about the power consumption of the each operation. Section III describes the design of the Mixcolumn. Section IV, explains about the comparison of our work results with the previously reported works, followed by conclusion in section V.

2 AES ALGORITHM

AES is a symmetric block cipher that is the same key is used for encrypting and decrypting the message and the pain text and the cipher text are in same size. In AES, the input state array has a key size which purely depends upon the round transformation. The number of rounds for 128, 192 and 256 are 10 rounds, 12 rounds, and 14 rounds respectively. Each round consists of few processing steps. Initially, the key expansion is used to derive the round key from the cipher key. First round involves AddRoundKey, SubBytes, ShiftRows, and MixColumns. One AddRoundKey is applied before the first round. The Mix Column transformation is missing in the last round. Fig.1. shows about the round involves in AES.

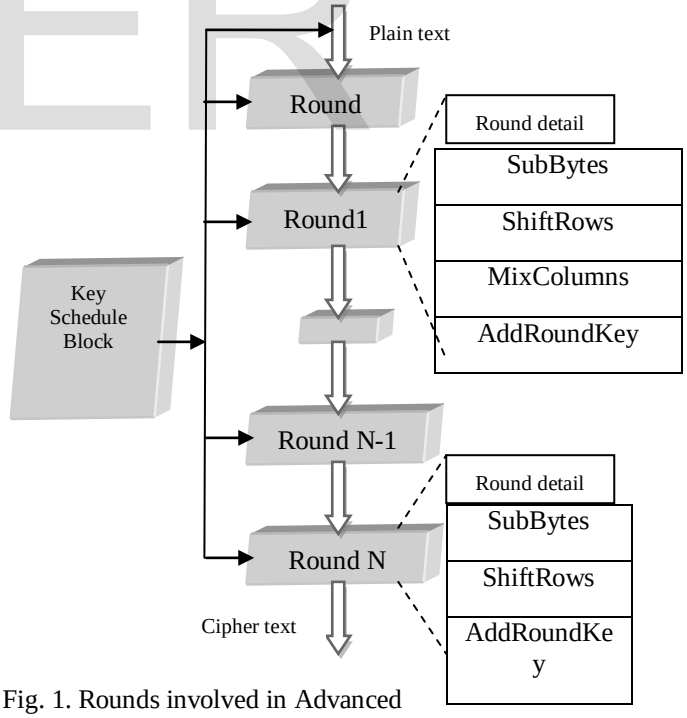

Fig. 1. Rounds involved in Advanced Encryption Standards

2.1 Subbytes:

Sub Byte is a simple substitution of the each bytes present in the state array using the S-Box. State array is the initial inputs contain 4x4 matrixes. S-box has the several possible ways in that the number can be arranged in order of all 256 8-bit values.

S-box can construct by the transformation of the values of polynomial Galois field GF (2^8) and the table for the S-box is fixed. Decryption requires the inverse of the table. Example for S-box for subbytes and inv subbytes transformation is mentioned in Fig. 2.

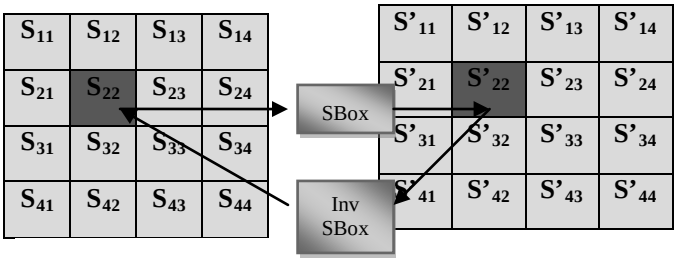

Fig. 2. Subbytes in AES.

2.2 Shift Rows:

As the name suggests, Shift Rows operates on each row of the state array. Right side rotation of the each row is giving the encryption value of shiftrows. The shifting details are:

1st Row rotated by 0 bytes (i.e., is not changed),

2nd Row rotated by 1 byte,

3rd Row rotated by 2 byte,

4th Row rotated by 3 byte.

Inverse Shift Rows involves rotating left instead of right.

2.3 MixColumns:

MixColumns is each column wise operation of the state array. Multiplication of matrix gives the new column. This is used to replace the old one. The Fig.3 represents in one column there are four bytes as an input and it gives the four corresponding outputs. Inverse MixColumns involves various constant matrixes to multiple the columns.

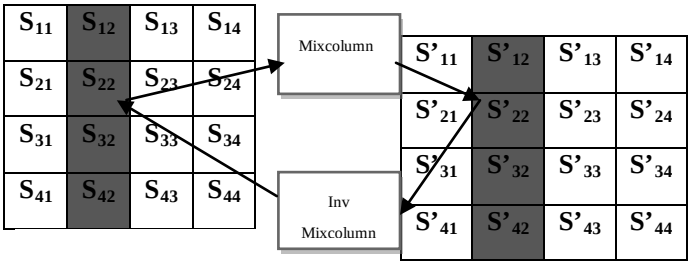

Fig. 3. Mixcolumn in AES.

2.4 AddRoundKey:

AddRoundKey is also called as XOR Round Key. It is a simple XOR operation between the state array and the appropriate round key value. This stage is involved once to start the round operations and also involved once per each round.

In last round, the MixColumns operation is not performed and only the Subbytes, Shift Rows, and AddRoundKey operations are done the low power logic style of the CMOS in AES plays a major part to consume the power. The power has divided into two types that are static power and the dynamic power. The problem in static is the increased leakage current due to decreasing the size of the transistor in CMOS logic. Dynamic power mostly depends upon the frequency of the operation. The main concept to reduce both the power is choosing the advanced technology to design the circuit which contributes the lower die area. This concept has considered the voltage supply, sub threshold voltage and scaling techniques taken into the account. In the concept of power the AES has been get the more concentration in the today's technique. In our design flow the usage of the pass transistor concept in the XOR logic is very useful approach to design the low power AES with a very less area.

3. Related Works

Low power AES design is benefited for many of the applications like smart cards, security sensor nodes and radio frequency identification (RFID) tags. The pipelining architecture, clock duration can be short a single 3 input XOR gate delay, with high throughput but it consumes more power. The different type of implementation of the encryption algorithm AES under VHDL language in FPGA for the mixcolumn is discussing in [3].

4. Design Overview

Designing of Mixcolumn with lower power consumption is possible through the implementation of pass transistor logic. The mix columns theory is calculated using this formula:

$$\begin{bmatrix} R0 \\ R1 \\ R2 \\ R3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} A0 \\ A1 \\ A2 \\ A3 \end{bmatrix}$$

Where R0, R1, R2 and R3 are the results after the transformation. A0 – A3 can be obtaining from the matrix after the data undergoes substitution process in the S-Boxes. We will now discuss the forward mixcolumn transformation. The forward mix column transformation, called MixColumns, and operates on each column individually. Each byte is mapped into a new value that is a function of all four bytes in the column. The transformation can be defined as the following matrix multiplication on State.

02	03	01	01		S00	S01	S02	S03
01	02	03	01	*	S10	S11	S12	S13
01	01	02	03		S20	S21	S22	S23
03	01	01	02		S30	S31	S32	S33

=

S00'	S01'	S02'	S03'
S10'	S11'	S12'	S13'
S20'	S21'	S22'	S23'
S30'	S31'	S32'	S33'

Each element in the product matrix is the sum of products of elements of one row and one column. In this case, multiplications and additions are performed in GF(2^8).

The following is the example of MixColumns;

87	F2	4D	97	=>	47	40	A3	4C
6E	4C	90	EC		37	D4	70	9F
46	E7	4A	C3		94	E4	3A	42
A6	8C	D8	95		ED	A5	A6	BC

1st column of the result is obtained by:

{02}{87}+{03}{6E}+{46}+{A6} = {47}
{87}+{02}{6E}+{03}{46}+{A6} = {37}
{87}+{6E}+{02}{46}+{03}{A6} = {94}
{03}{87}+{6E}+{46}+{02}{A6} = {ED}

For example the 1st equation, we have

{02}{87}=(0000 0010)(1000 0111)=
$x(x^7 + x^2 + x+1)$
$=(x^8 + x^3 + x^2 +x) \bmod (x^8 + x^4 + x^3 +x+1)$
$= x^4 + x^2 +1$
(0001 0101)={15}
{03}{6E}=(00000011)(01101110)=
$(x+1) (x^6 + x^5 + x^3 + x^2 +x)$
$(x^7 + x^5 + x^4 +x)$
(1011 0010) = {B2}
{02}{87}+{03}{6E}+{46}+{A6}={15}+{B2}+{46}+{A6}=
(0001 0101)+
(1011 0010)+
(0100 0110)+
(1010 0110)=
(0100 0111)={47}

Then therefore, the x time block can be implemented by 3-XOR gates with the pass transistor logic of XOR gates. As shown in Fig. 4. Mixcolumn transformation.

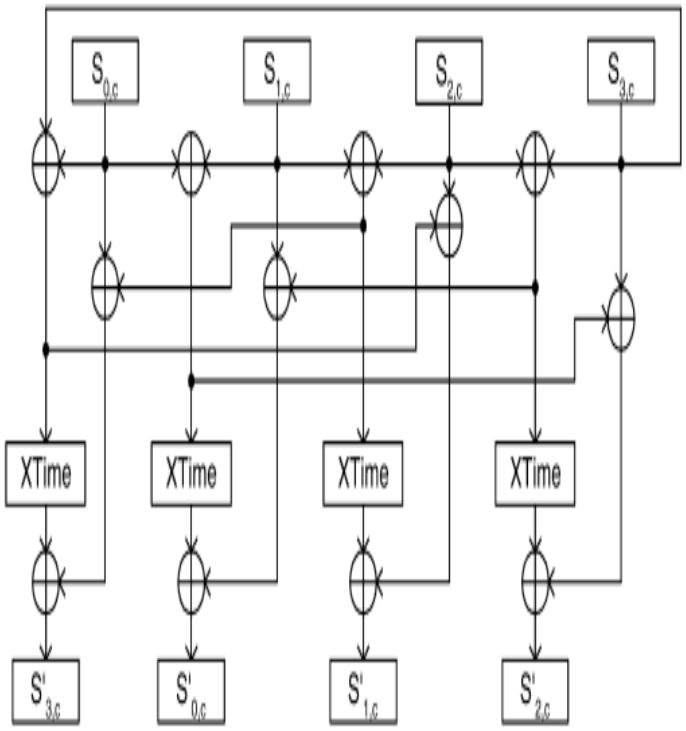

Fig. 4. Mixcolumn transformation

Similarly, in the Inv Mix Columns architecture is implemented by the logic Xor gate as shown in fig.5.

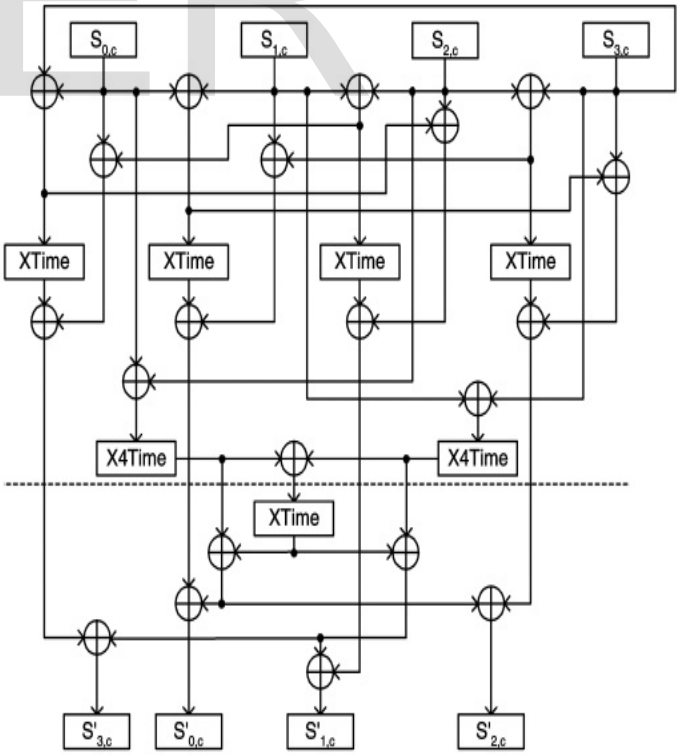

Fig. 5. Inv Mixcolumn transformation

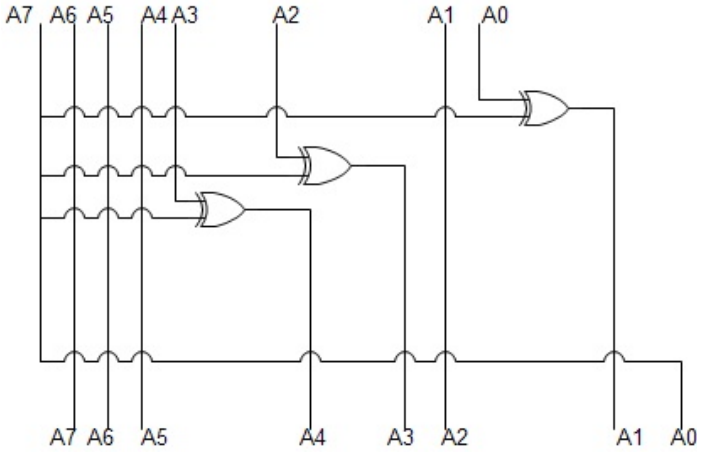

Fig. 6. Diagram of X Time using XOR gate.

The architecture for the 'x time' is clearly explained in the fig.6.

5. Simulated Results And Comparison Of The Proposed Method

The implementation of the mixcolumn using XOR gate is designed to achieve the maximum low power. Fig. 10 shows the designed circuit diagram for the XOR. The pass transistor logic is used for the minimal power consumption and achieves the less number of transistors in count.The operation of XOR gate is that explained as if the one of the input is low and another is high then the output will be high, if both the input is low or high then the output is low.

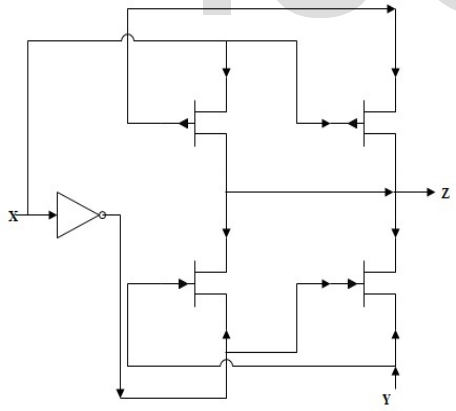

Fig. 7. XOR gate using pass transistor logic.

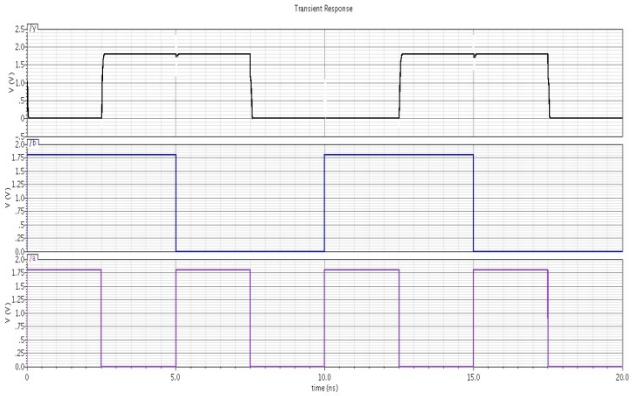

Fig. 8. Simulation results for the XOR gate using pass transistor logic.

Our proposed XOR gates constructed by the use of six pass transistors which reduce the count of large transistor circuit. To enable the low voltage operation this circuit is designed. All the required component blocks of the AES been implemented using XOR pass transistor logic gates and the outputs verified. Table I. can say about the comparisons between the previous methodologies and the proposed methodology.

6. Conclusion

The work is done for the mixcolumn in AES. The logic style used here is that the source or drain side of the transistor is connected to the input instead of the voltage supply and the ground. So the proposed system clearly describes us that this pass transistor XOR architecture reduces the total power consumption of the mixcolumn Architecture improves in the lower power consumption.

References

[1] Yogesh Kumar, Rajiv Munjal, Harsh Sharma "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[2] Manoj Sharma.T, Thilagavathy.R," Performance Analysis of Advanced Encryption Standard for Low Power and Area Applications", Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).

[3] Sliman Arrag, Abdellatif Hamdoun , Abderrahim Tragha and Salah eddine Khamlich ," Design and Implementation A differentArchitectures of mixcolumn in FPGA".

[4] Hua Li Zac Friggstad," An Efficient Architecture for the AES MixColumns Operation"pg.no.4637- 4640, IEEE-2005.

[5] J.Balamurugan , Dr.E.Logashanmugam,"Design of Efficient AES using modified mix-column architecture", International

Journal Of Technology And Engineering Science [IJTES] Vol 1(7), pp1054-1059, October 2013.

[6] P. Noo-intara, S. Chantarawong, and S. Choomchuay," Architectures for MixColumn Transform for the AES", pg.no. 153-156 , ICEP 2004, Phuket, Thailand.

[7] Richa Sharma, Purnima Gehlot, S. R. Biradar," VHDL Implementation of AES-128", UACEE International Journal of Advances in Electronics Engineering – IJAEE Volume 3 : Issue 2,05 June 2013.