IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 5, Issue 1, Ver. III (Jan - Feb. 2015), PP 01-11
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Design and Analysis of Parallel AES Encryption and Decryption Algorithm for Multi Processor Arrays

A.Anusha[1], N.Samba Murthy[2]
[1]*PG Student, ECE Department, Gudlavalleru Engineering College, Gudlavalleru, India*
[2]*Assistant Professor, ECE Department, Gudlavalleru Engineering College, Gudlavalleru, India*
[1]anuece.anu@gmail.com,[2]sambanaga009@gmail.com

Abstract: *This paper presents information on AES Encryption and Decryption for multi processors. In this paper AES algorithm is used. The AES algorithm is a round based algorithm. The round based algorithm is used to provide security to the information. In AES algorithm there are different types of keys, they are 128,192 and 256 bits. These bits are used to encrypt and decrypt the information. In this paper 128bits are used. In this paper the main functional blocks are key generation, encryption and decryption. In order produce a new key sub byte, rotate word, round constant and add round key operations are used. In order to convert plain text to cipher message the sub bytes, shift rows, mix column and add round key operations are used. By doing these operations the cipher information is obtained. This cipher will be given to the decryption and it is the total reverse process of encryption. After completion of reverse process the outcome is original information.*

Index terms*- Advanced Encryption Standards, cipher, multi processor.*

I. Introduction

Encryption is the process of converting original message into cipher information by using key. In this process the information must be in the form of hexadecimal or integer format only. Decryption is the process of converting cipher information to original information by using same key. In decryption the format of message must be in Hexadecimal or integer. In this paper the advanced encryption standard algorithm technique uses the symmetric key that means private key. The main advantage of symmetric key is provide security to the data and reduces the area also. This types of private keys mainly used in ATM machines and software's also.

This paper mainly concentrates on developing suitable method for rapid and efficient way to perform hardware implementation for some applications to provide security to the information. To accomplish high security for a system the AES technique is used. Most of the users now a day's using wireless communication for fast sending and receiving the mails in less time and less cost. When this way of communication is going on, the unauthorized people who have the intension to know about the conversation will hack the information. The AES algorithm is used to provide security and hackers cannot hack the data even if they know the key and algorithm also. In this paper the sub bytes and inv sub bytes operation will be done word wise. By doing these operations reduce the area and increase the speed of the operation.

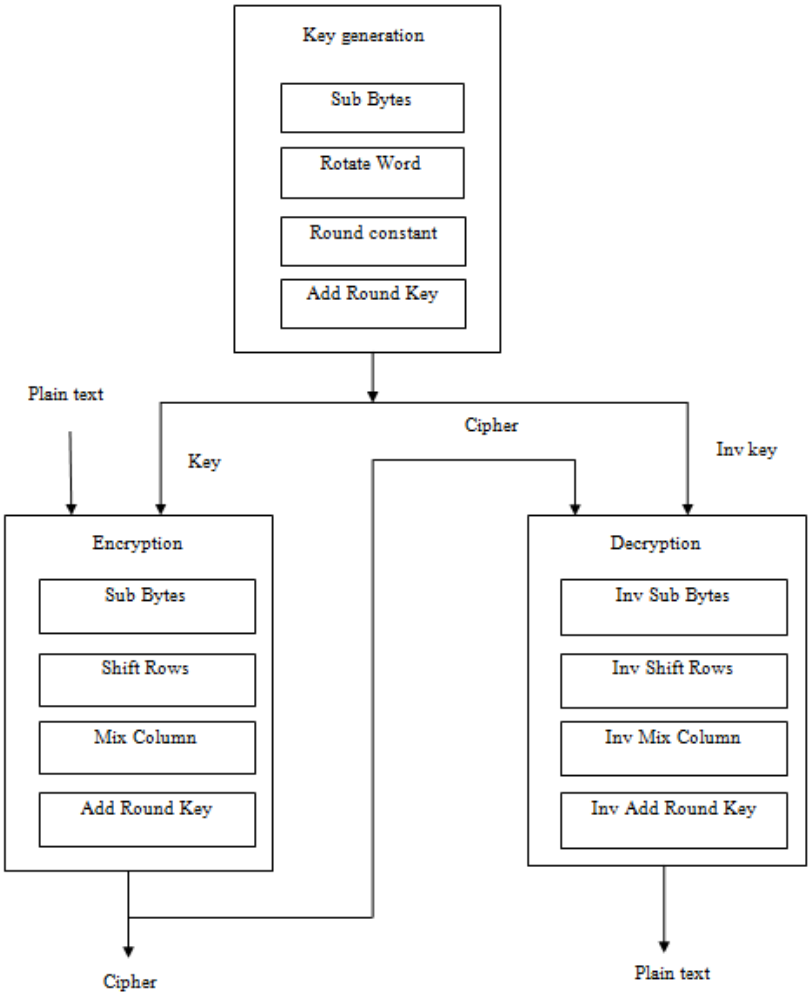


Fig1. Block Diagram Of AES

There are mainly 3 types of operations in advanced encryption standard algorithm. They are key generation; encryption and decryption.

II. Key Generation

The key generation processes the data block of fixed size i.e. 128 bits using cipher key length of 128,192 and 256 bits. The number of operations will be depending on number of bits. By using different type of bits it has some constant rounds of operation. For 128 bits it has 10 rounds of operations. By rounds of operations, it provides security because by doing this types operation they cannot hack the data. The below table [1] shows the number of keys and number of rounds for particular bits.

Table 1: key generation

No. of bits	128 bits	192 bits	256 bits
No. of keys	10 keys	12 keys	14 keys
No. of rounds	10 rounds	12 rounds	14 rounds

For 128 bits (which we r using here) there are fixed 10 rounds. For getting 10 keys we have to done some operations. They are sub bytes, rotate word, round constant and add round key operations.

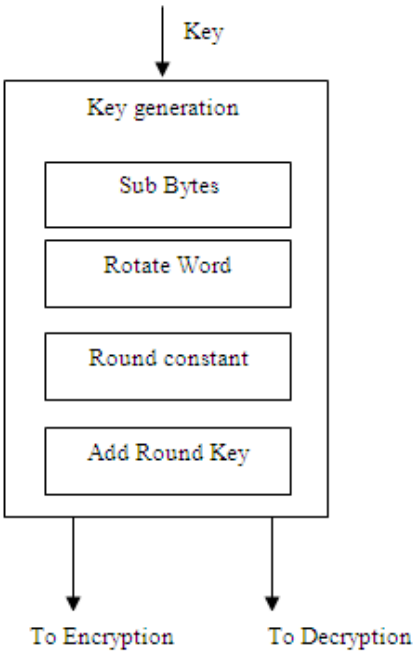


Fig2. Block diagram of key generation

2.1 Sub bytes operation

The sub bytes operations will be done word wise. This is non-linear substitution technique. It works on every byte of the state independently. By using S-box table, it will operate. The S-box table is developed on 2 transformation techniques. They are

2.1.1 Take the replica of Rijndael's conditions.

2.1.2 Apply a non-regular technique that is already implemented on Rijndael technique.

The predefined values of substitution table is used here. Every bytes of the state is compared with the value in the equal positioned value in S-box.

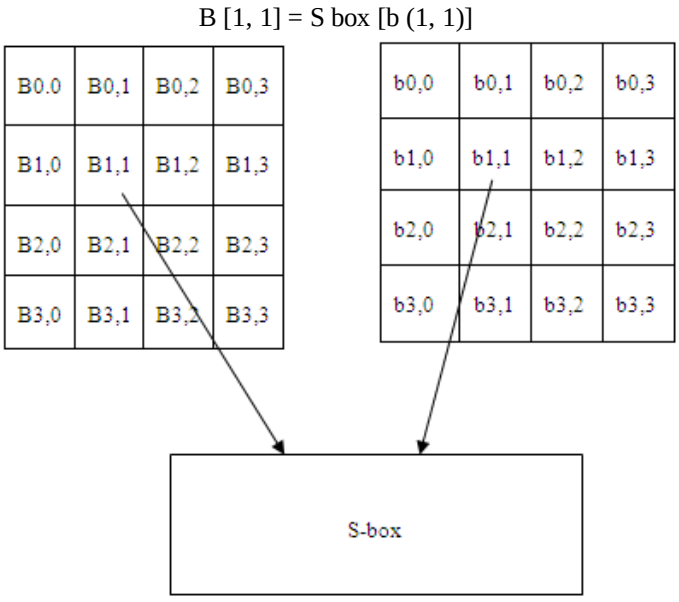


Fig 2.1 Sub bytes operation

2.2 Rotate word operatio

Rotate word performs a one byte circular rotate left.

Rot word [A8 A7 A6 A5] = [A5 A8 A7 A6]

2.3 Round constant operation

The round constant operation is different for each step.

3b	38	ae	07
8e	ab	f9	cf
14	d4	14	3f
19	b6	99	4cZ

In the example take either one column or row
07 cf 3f 4c
Then rotate the equation
Cf 3f 4c 07
Now put these values through the AES s-box (component wise)
8a 75 29 c5
This is the operation for round1.Now we need the round constant operation. Add round one to the s-box output

8a $\oplus$ 01 = 8b

75 $\oplus$ 00 = 75

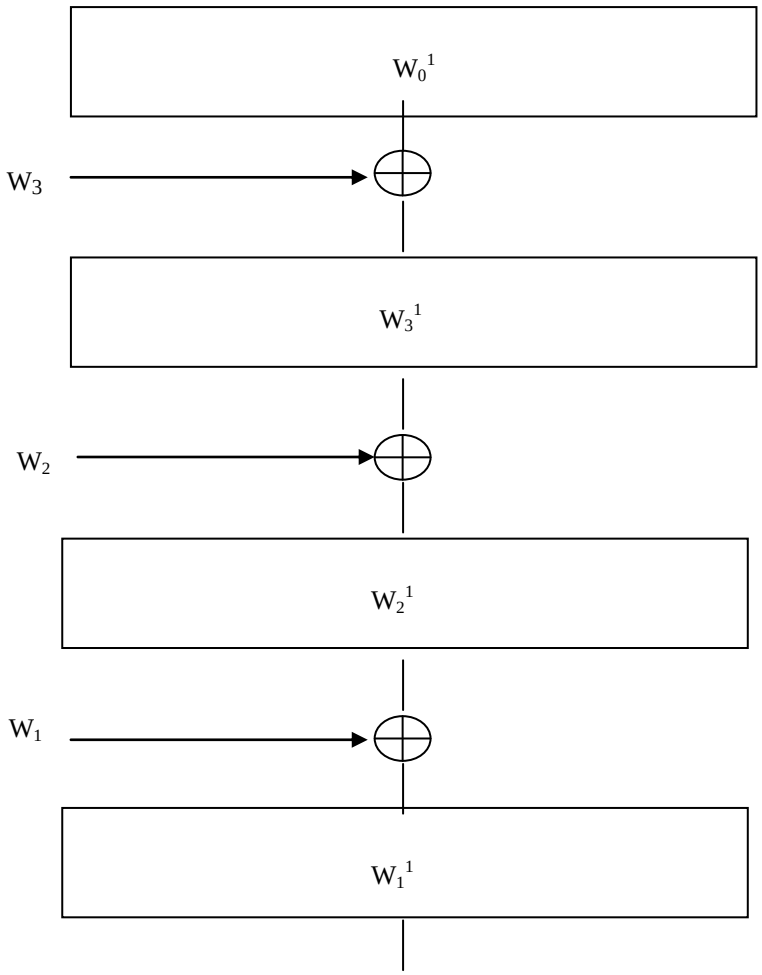
29 $\oplus$ 00 = 29

C5 $\oplus$ 00 = c5

This is the operation for round constant 1. These are the operations for key generation.

2.4 Add round key operation

Every byte of the value is directly added with the key. The below figure shows the operation of add round key



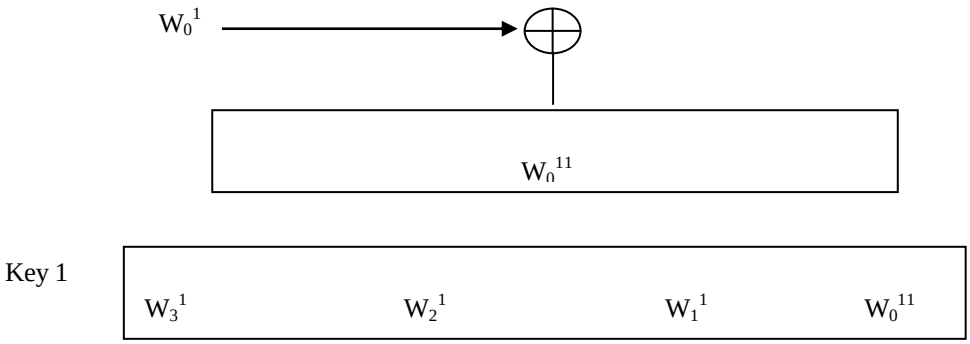


Fig 2.2 Add round key operation

This is the operation for key 1.Repeat the above steps up to 10 rounds for every round will get one key total 10 keys because this technique using 128bits. For 128 bits it has 10 rounds of operation for each round it will get one new key.

III. Encryption

It is defined as converting original message to cipher message.

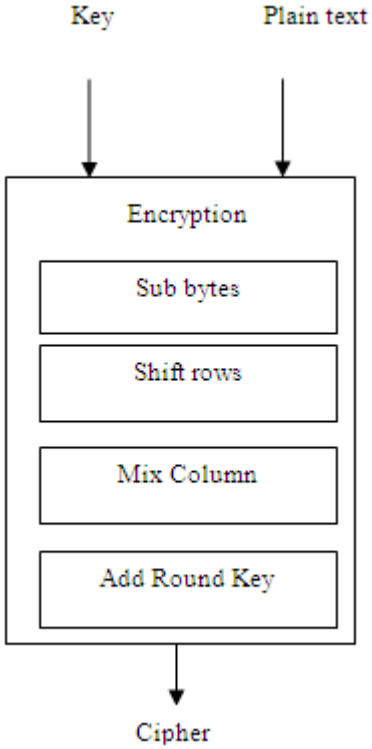


Fig3. Block diagram of Encryption

There are mainly 4 types of operations in encryption. They are

3.1 Sub bytes operation

The sub bytes operations will be done word wise. This is non-linear substitution technique. It works on every byte of the state independently. By using substitution table it will operate. The substitution table is developed on 2 transformation techniques. They are

3.1.1 Take the replica of Rijndael's conditions.

3.1.2 Apply a non-regular technique that is already implemented on Rijndael technique.

The predefined values of substitution table is used here. Every bytes of the state is compared with the value in the equal positioned value in s-box.

B [1, 1] = S box [b (1, 1)]

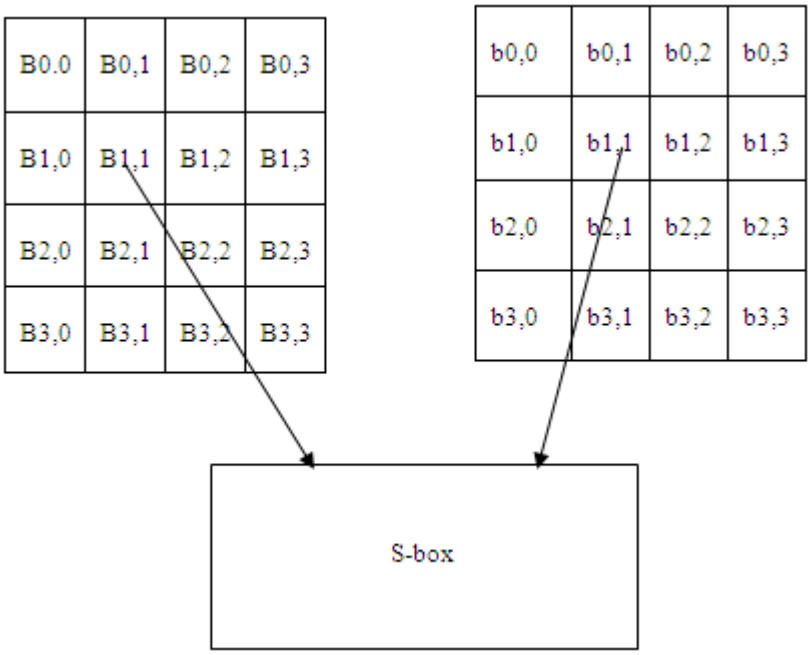


Fig 3.1 sub bytes operation

3.2 Shift rows

The shift rows operations were done with the shifting rows cyclically either right or left.

3.2.1 In first row there is no change.

3.2.2 In second row shift cyclically by one position either left side or right side

3.2.3 In third row shift cyclically by two positions.

3.2.4 In fourth row shift cyclically by three positions.

No change	D0 D1 D2 D3	D0 D1 D2 D3
1st shift	D4 D5 D6 D7	D5 D6 D7 D4
2nd shift	D8 D9 D10 D11	D10 D11 D8 D9
3rd shift	D12 D13 D14 D15	D15 D12 D13 D14

3.3 Mix column operation

In mix column operation each column of the state array is considered as a multiplicative term. In mix column operation the 4*4 matrix is multiplied with the constant matrix. In mix column operation, there are only 9 rounds (1 to 9). There is no 10th round for mix column operation. For 10^{th} round, the shift rows operation is directly given to the add round key operation because there is no 10^{th} round for mix column.

3.4 Add round key operation

Every byte of the value is directly added with the key. The operation between mix column output with key 1 to 9 rounds only.

IV. Decryption

It is defined as the converting cipher message to original message. The decryption is the total reverse operation of the encryption.

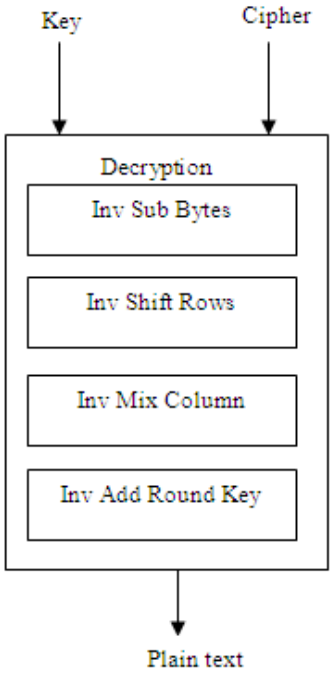


Fig4. Block diagram of Decryption

There are mainly 4 types of operations in decryption. They are

4.1 Inv sub bytes operation

The inv sub bytes operations will be done word wise. This is non-linear substitution technique. It works on every byte of the state independently. It operates by using inverse substitution table. The inverse substitution table is develops on 2 transformation techniques. They are

4.1.1 Take the replica of Rijndael's finite field.

4.1.2 Apply a non-regular technique that is already implemented on Rijndael technique.

$$B [1, 1] = S \text{ box } [b (1, 1)]$$

The predefined values of substitution table is used here. Every bytes of the state is compared with the value in the equal positioned value in the inverse s-box.

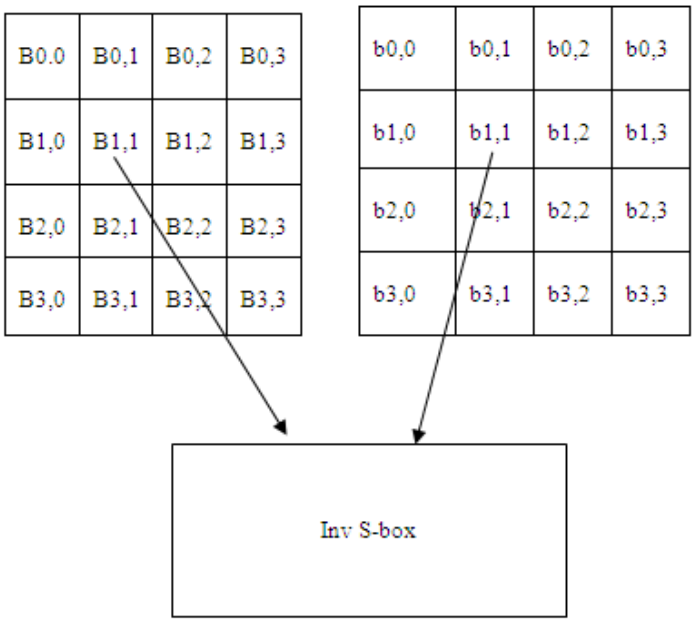


Fig. 4.1 sub bytes operation

4.2 Inv shift rows operation

The inv shift rows operations were done with the shifting rows cyclically right. The inv shift rows operation is same as the shift rows operation.

4.2.1 In first row there is no change.

4.2.2 In second row shift cyclically by one position either left side or right.

4.2.3 In third row shift cyclically by two positions.

4.2.4 In fourth row shift cyclically by three positions.

No change	D0 D1 D2 D3	D0 D1 D2 D3
1st shift	D4 D5 D6 D7	D5 D6 D7 D4
2nd shift	D8 D9 D10 D11	D10 D11 D8 D9
3rd shift	D12 D13 D14 D15	D15 D12 D13 D14

4.3 Inv mix column operation

In inv mix column operation each column of the state array is considered as a multiplicative term. In inv mix column operation the 4*4 matrix is multiplied with the constant matrix and we get same dimensional matrix. In first round there is no inv mix column operation.

4.4 Inv add round key

Every byte of the value is directly added with the key. The key must be in reverse order i.e. 10 to 1 for decryption

Applications:

1. It is used in online banking.
2. ATM machines and social networking also.
3. It is also used in business purpose also.

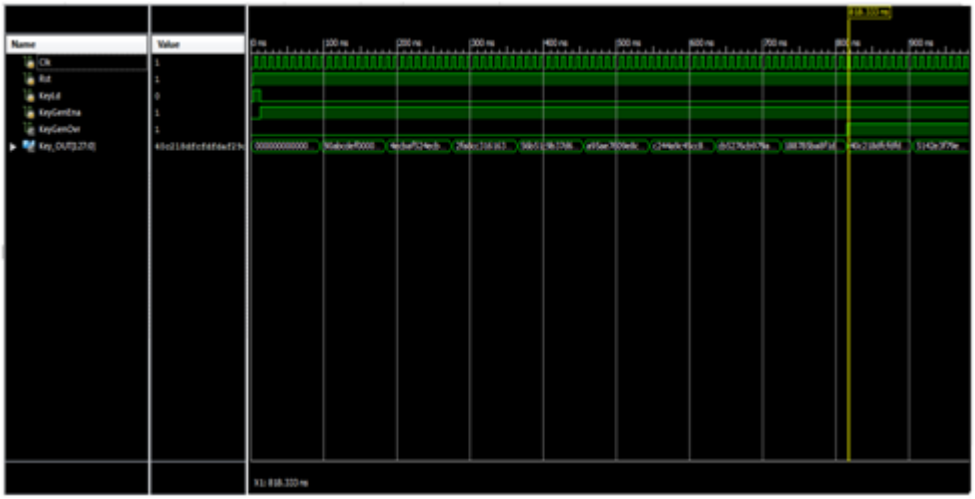


Fig 2.3 Timing diagram for key generation

After key generation is enabled and reset is high and key load is loaded, then the keys are produced.

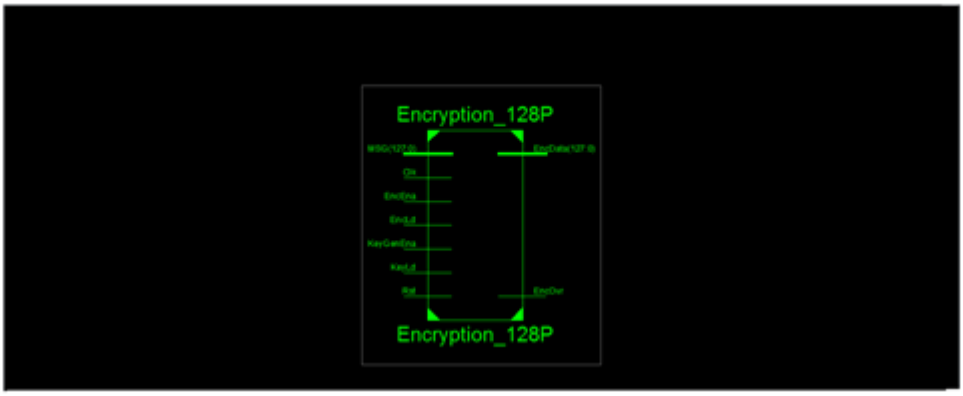


Fig 3.2 RTL schematic for Encryption

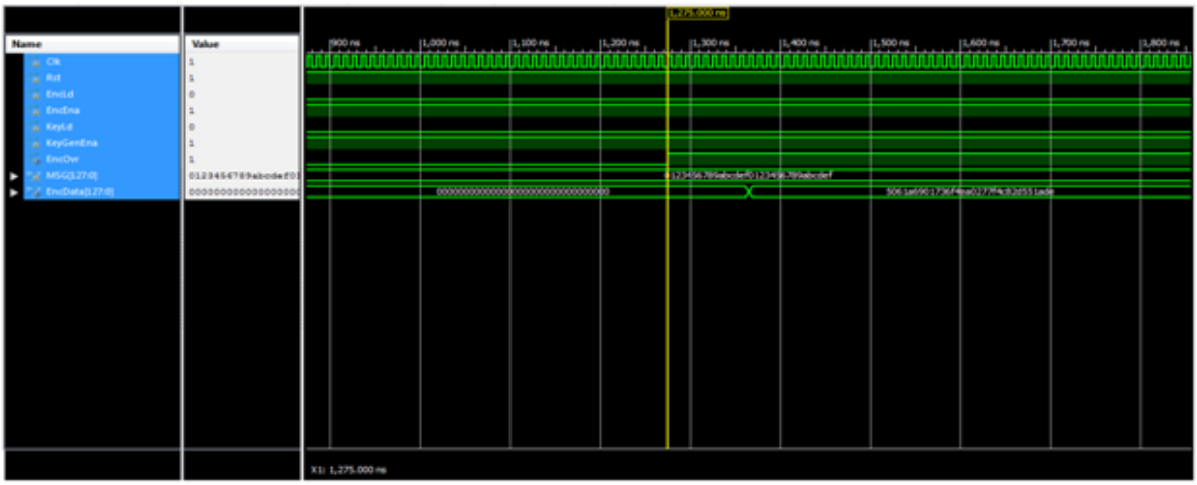


Fig 3.2 Timing diagram for Encryption

After reset and key generation enabled encryptions starts. As encryption ends, encryption over signal is high indicating that message is converted into encrypted information

Fig 4.2 RTL schematic for Decryption

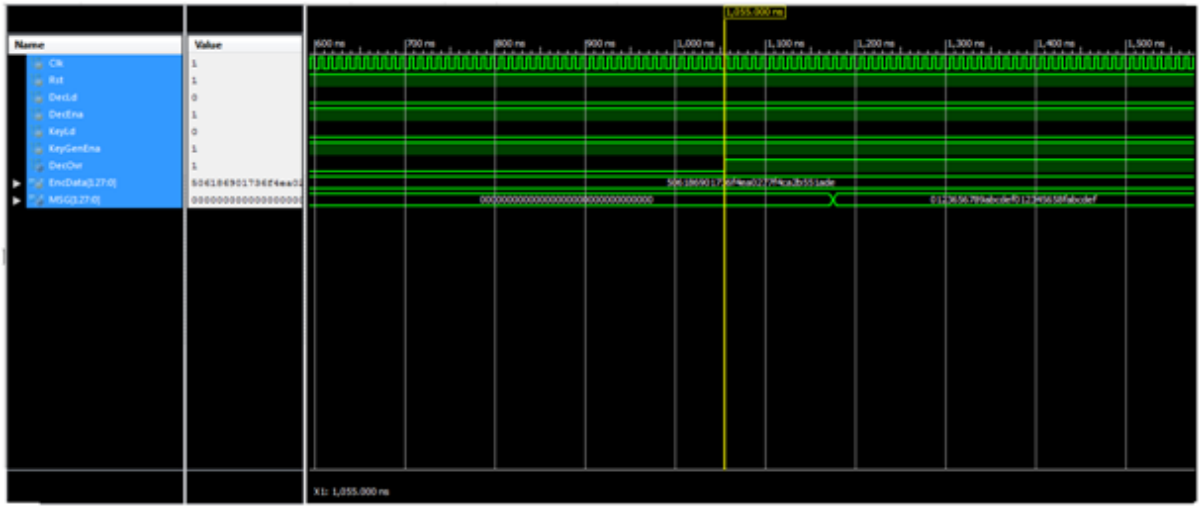


Fig 4.3 Timing diagram for Decryption

After reset and key generation enabled decryptions starts. As decryption ends, decryption over signal is high indicating that message is converted into original information

V. Analysis report:

	Encryption	Decryption
No .of Slices	717	717
No. of flip-flops	682	682
No. of 4 I/p LUT's	1076	1075
No. of IOB's	263	263
No. of CLK's	1	1
Total Delay	5.014ns	5.014ns

Table2. Analysis report for encryption and decryption

VI. Conclusion

Xilinx is very helpful tool for software and hardware. By using this technique we can provide security to information. By using AES we can reduce the area and reduction of cost will lead to the reduction of overall production cost and 100% security of data. The future scope of this project is further to extend up to 256 bits efficiently and successfully by using the same techniques.

Acknowledgement

I am glad to express my deep sense of gratitude to, Mr. N.Samba Murthy, Assistant Professor of Electronics and Communication Engineering, for his guidance and cooperation in completing this project. Through this, I want to convey my sincere thanks to him for his inspiring assistance during my project. I express my heartfelt gratitude and deep indebtedness to the beloved Head of the Department, Dr. M.KAMARAJU, for his great help and encouragement in completion of my project. I also express my gratitude to our principal Dr. P.NAGESWARA REDDY, for his encouragement and facilities provided for my project. I thank one and all who have rendered help to us directly or indirectly in the completion of this work.

References

[1]. Bin Liu and Bevan M. Baas "Parallel AES Encryption Engines for Many-Core Processor Arrays" IEEE Transactions on computer, VOL. 62, NO. 3, MARCH 2013.
[2]. A. Still maker, "Exploration of Technology Scaling of CMOS Circuits from 180 nm to 22 nm Using PTM Models in HSPICE, "Technical report, UC Davis, June 2011.
[3]. J. Granado-Criado, M. Vega-Rodriguez, J. Sanchez-Perez, and J. Gomez-Pulido, "A New Methodology to Implement the AES Algorithm Using Partial and Dynamic Reconfiguration," Integration, the VLSI J., vol. 43, no. 1, pp. 72-80, 2010.
[4]. S. Gueron, "Intel Advanced Encryption Standard (AES) Instructions Set," Jan. 2010.
[5]. Z. Yu and B.M. Baas, "A Low-Area Multi-Link Interconnect Architecture for GALS Chip Multiprocessors," IEEE Trans. Very Large Scale Integration (VLSI) Systems, vol. 18, no. 5, pp. 750-762, May 2010.
[6]. M. Butler, "AMD Bulldozer Core—A New Approach to Multithreaded Compute Performance for Maximum Efficiency and Throughput," Proc. IEEE Hot Chips Symp High-Performance Chips (Hot Chips '10), Aug. 2010.