Design And Implementation Of MAES Based On Pipeline Architecture Using Verilog

[1]Bhavani Mamilla, [2]Annapurna Ganji
[1]M.Tech Scholar, [2]Assistant Professor VJIT College, Hyderabad, India

Abstract - In the present paper, MAE S (Modified Advanced encryption Standard) is the light weight version of Advanced Encryption Standard (AES). MAES which consumes less energy than AES. Encryption and Decryption takes place in AES Algorithm. AES is mainly divided into three types , namely AES -128 and the key length is 10 rounds, AES -192 and the key length is 14 rounds, AES -256 and the key length is 14 rounds of operation. Here we are using 128 bits of cryptographic keys and 128 bits of plain text. Substitution box of AES is with 256 bits of combination but in MAES which is decreased to 16 bit of combination because the arithmetic operations are performed over the Galois Field (24). In AES the names of operations are Sub byte, Shift rows , Mix columns and Add round key. We need to perform 10 rounds of operation for Encryption and Decryption by connecting the registers to each round of operation, so that we can make the shortest delay when compared to AES.

Index Terms - Cryptography, Pipelined Architecture , Encryption , Decryption , Advanced Encryption Standard (AES).

I. INTRODUCTION

In present days as the civilization keeps on improving, Advancement in the electronics and communication is necessary. People are habituated to use the electronics for communication purpose while communicating with other don't know how to safe their information was and whether the information is receiving to receiver [1]. So Data Encryption Standard (DES) is one of the algorithm to protect the data from the unauthorized person. Here the decryption and encryption techniques takes place . In which DES uses the symmetric cryptography and encryption and decryption Block cipher algorithm is used. In DES the plain text range is 64 bit and the key size is 56 bit. So that DES has less capacity to secure the data because of the shortest key size [2]. To overcome this problem we are chosen the Advanced Encryption Standard (AES) same has the DES algorithm but the plain text and the key sizes are differ . AES is a symmetric block cipher chosen by the U.S government to protect the information and is implemented in software and hardware through out the world to encrypt the sensitive data. It was also easy to implement in hardware and software. AES which comprises three block ciphers AES-128 , AES-192 , AES-256 and which encrypts and decrypts the data in blocks of 128 bits , By using the cryptography keys which is of 128 with 10 rounds , 192 is of 12 rounds and 256 is of 14 rounds [3].

In AES Substitution Box has 256 bit of combinations were it is very complicated to do the arithmetic operation by using s-box and it is performed over the Galois Field (28) [4] . So that to reduce the arithmetic operations it is modified it to Modified Advanced Encryption Standard (MAES) . In MAES Substitutional Box reduced to 16 bit combination [5] . It is some what easy to do the arithmetic operations by using MAES s-box. It is a light weight version of AES which consumes less power and to calculate it takes less time than AES [6]. Here it has 4 stages they are namely called as Sub Byte , Shift Rows , Mix Column , Add Round Key . After performing every round with each stage according to the key size in the last round we does not perform the mix column operation because it doesn't produce the cipher text again the same cipher text is given to the input to decryption so that we can get the same message in the decryption output [1].

Joan Daemenand Vincent Rijmen urbanized a block cipher called Rijndael. In AES the span of each block and the key can be autonomously specified to be 128, 192, or 256 bits. The AES arrangement exploits data of 128 bits and same three key size alternatives. This 128 bit data can be divided into four operation blocks, which are represented as a square matrix of bytes. These operation blocks are copied into a state array. The state array is organized as a 4×4 matrix. The data is conceded through N rounds (N = 10, 12,14) for encryption.

These rounds are performed by the following transformations:

ByteSub transformation: In this process 128-bit block is replaced with another 128- bit block, for substitution purpose we use S-box.

Shiftrows transformation: In this process we leave the first row of data, perform once shift left on 2nd row, two times shift left on 3rd row and three times shift left on 4th row. It is a simple Permutation.

Mixcolumns transformation: Is a substitution; the bytes in the columns are linearly combined. The matrix multiplication is performed over the same GF (28) as used in the design of the S-box.

Addroundkey transformation: When working state and expanded key are XOR with each other, process is called Addround Key. All four layers expressed above (including key scheduling) have analogous converse methods. Procedure of encryption follows more than a few ladders. An initial addround key is applied. After this a round function is applied to the block. Each block consists of bytesub, shiftrows, mixcolumns and addroundkey transformation.

These blocks are repeated N times, depending upon the length of the key applied. Same sequence of transformations is applied on decryption structure as which is applied in encryption structure. The transformations i.e. InvBytesub, InvShiftrows, Inv-Mix columns, and Addround key permit the type of key schedules to be matched for encryption and decryption Here it must be noted that the Mix Column reverse operation requires matrix elements.

II. DESIGN OF PIPELINED ARCHITECTURE

In the proposed method MAES pipeline registers are placed after round or after the operation. By placing the registers in the algorithm we can achieve high performance implementation both in encryption and decryption side. The fully expanded implementation for all ten rounds. The data generated in each in each individual round is utilized as an input data to the next round. Here placing the pipeline registers is the key of achieving better performance. Pipeline registers are basically used for intermediate data processing. We have different optimizations in our coding it may be delay optimization, we are choosing the technique which is used to reduce the delay in our previous delay.

I have let us considered from the previous delay is 4.28ns, if if have delay optimization techniques it may reduced to less than 4.28ns. We have several concepts to reduce the delay one of the technique is Pipelined architecture, in the name itself we can say that pipeline means it produce concurrent operation or parallel Execution .Let us take an example one statement will execute in different states based on following states, namely there are fetching, decoding, execution and write back. In fetching state it fetches the data from the external side, In decoding state it decodes what is the operation, In execution state it performs the operation, In write back state after the execution of statement it assigns the value to the output. Coming to our architecture MAES based pipeline architecture there are several ways to keep pipeline architecture it may take 2 stage or 3 stage pipeline according to our requirement. The proposed MAES delay is shown in the below diagram. Three key length alternatives 128, 192 or 256 bits and block length of 128 bits. We assume a key length of 128 bits, which is commonly implemented.

In Modified- AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mix column step and add the permutation step. Mix column gives better security but it takes large calculation that makes the encryption algorithm slow . The other three junctures remain unbothered as it is in the AES. A single 128-bit block is the input to the encryption and decryption algorithms. This block is a 4×4 square matrix consisting of 16 bytes. This block is divided into four operational blocks where we observe the data at either bytes or bit levels and the algorithm is designed to treat any combination of data and is flexible for key size of 128 bits. These four operational blocks represent one round of Modified-AES. There are 10 rounds for full encryption.

III. BLOCK DIAGRAM OF PIPELINE ARCHITECTURE

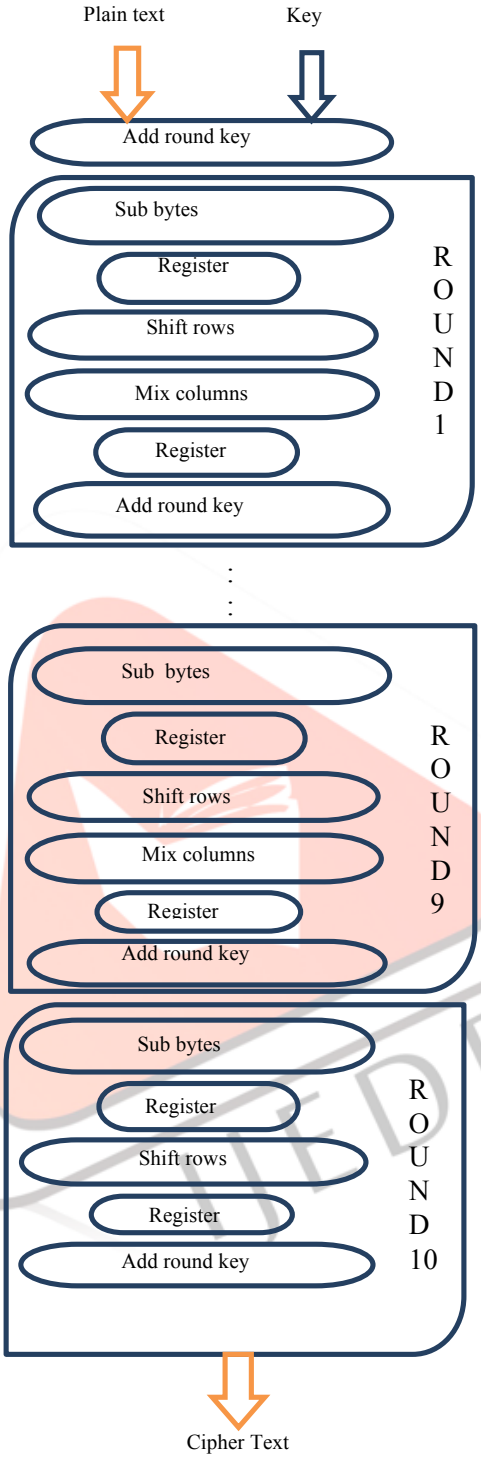

Fig.1. MAES using pipeline

IV. RESULTS AND DISCUSSION

For testing the algorithm we use a very simple code that checks the efficiency of algorithm. This test shows that the modified-AES algorithm is much better than AES algorithm. In this tutorial we have tested several files and in order to check that how fast the Modified-AES algorithm than the real AES. To test the algorithm we take sixteen byte text compare the calculated elapsed time of both the Modified-AES with Advanced Encryption Standard (AES). In the below diagram input which is nothing but a plain text of 128 bit and key is also a 128 bit and out temp is a cipher text and the main output is a decryption output which is same as plain text which is given as input to the encryption . The proposed method is design by using Xilinx ISE 14.5.

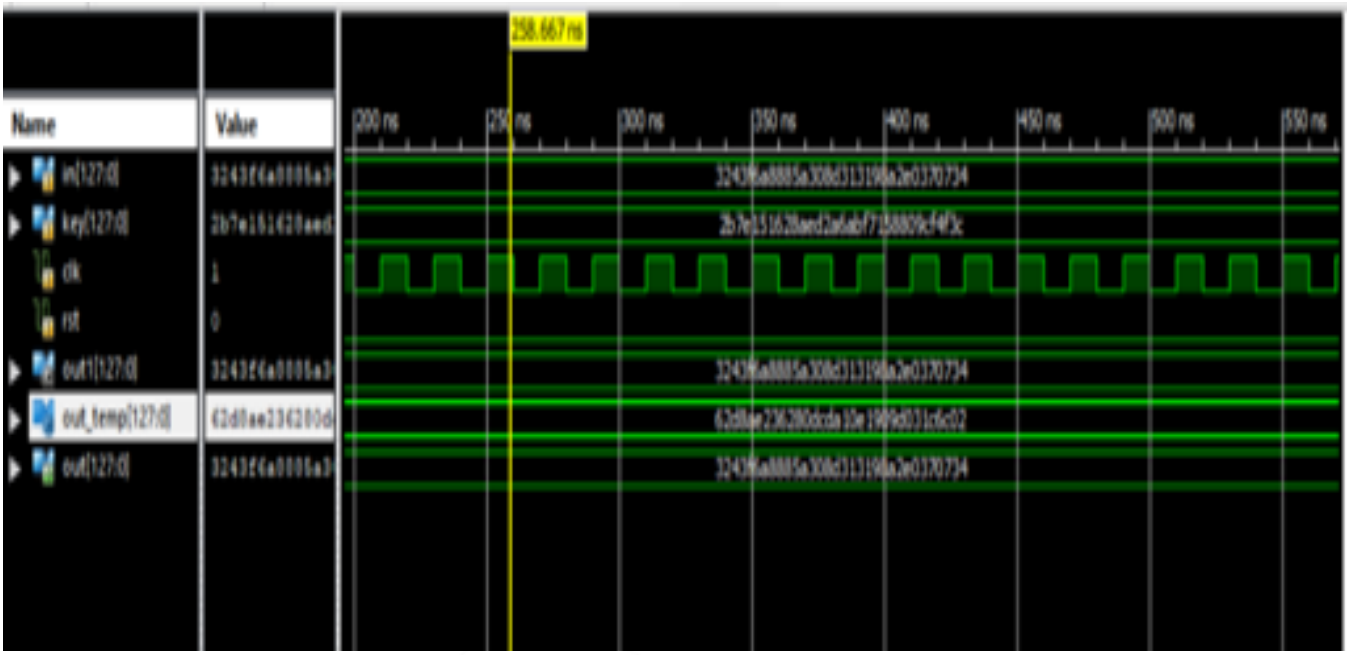

Fig.2. Simulation of encryption and decryption

Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and ShiftRows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry indicates a specific position of a numbered input bit may also consist of 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242th bit of the 256-bit block is in first position, the 226th is in second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. For the full decryption of Modified-AES algorithm the transformation processes are, Inv-Bytesub, Inv-Shiftrows, Inv-Permutation, and the Addroundkey, which are performed in 10 rounds as it is in the encryption process.

In these paper the main outcome is delay , when compared to MAES delay it is decreased 80% of delay by adding the pipeline architecture in this method it is shown in below diagram.

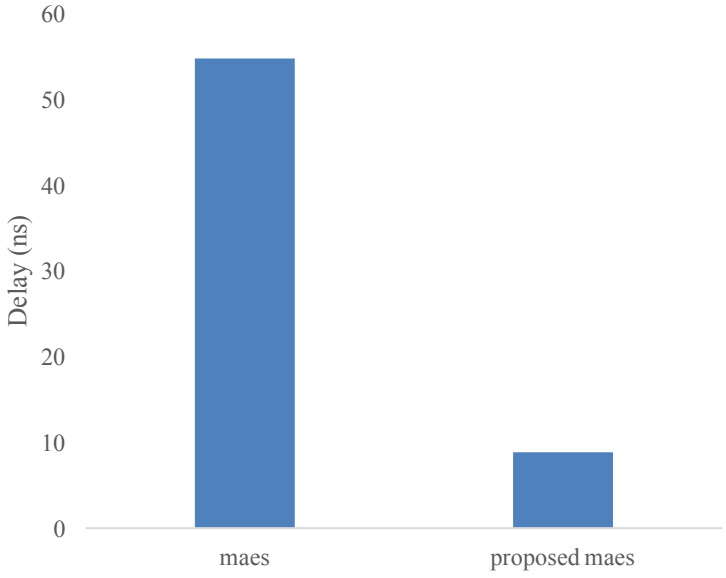

Fig.3. Delay comparison between MAES and Proposed MAES

V. CONCLUSION

In modified AES algorithm having 20% optimization in delay, In normal proposed MAES has 54.7ns , whereas in pipelined architecture it has 8.85ns. So that we have reduced the delay by using this method. Usually lightweight encryption algorithms are very attractive for multimedia applications. Luckily we have achieved through our research a fast lightweight encryption algorithm to secure our multimedia data from unauthorized access. For the security of multimedia data, we have proposed an encryption algorithm that is based on AES using symmetric key encryption algorithm. In version of security analysis and experimental results our proposed encryption scheme is fast and on the other hand it provides good security and adds very less

overhead on the data . Theoretical analysis and experimental results of the achievement makes it very suitable for high rate and less overhead on the data. For all these compensation it is suitable for any large scale text and image transfer.

REFERENCES

[1] Umalaxmi sawant, Prof .Kishore wane "Analysis of the effective advanced encryption standard algorithm" IJARCCE vol. 5, issue 3, March 2016.
[2] Indumathi saikumar "Data Encryption Standard" IRJET vol. 04, issue 3,March 2017.
[3] Pravin kawle , avinash hiwase , Gautam badge, ekant tekam, Rahul kalbande "Modified Advanced encryption" IJSCE vol. 04, issue1, March 2014.
[4] A.Sriram , godugu shiva Kumar " Fully pipelined high throughput VLSI architecture for MAES Algorithm" IJournals vol. 03 issue 10, October 2015.
[5] Lejla batina , Amitabh das, Baris ege , Tolga yalcm "Dietary Recommendations for Light weight Block ciphers".
[6] Shubhangi V. Funde , Dr. D. v. padole "Design of Advanced Encryption Standard Algorithm Using Xilinx Project Navigator, ISE 13.1". IJERGS vol.03, issue 2, 2015.
[7] Shtewi, A.M."An Efficient Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2.
[8] ShashiMehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2,Issue 2, June 2011 pp.192-192.
[9] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3.
[10] Behrouzan A. Forouzan (2010), Cryptography & Network Security, TMH Publisher, ISBN: 9780070660465.
[11] Bruce Schneier (2009), Applied Cryptography, John Wiley & Sons Publisher, ISBN:9780471117094.
[12] Wanican Julian Okello , Qingling Liu, Faizan Ali Siddiqui1 , Chaozhu Zhang "A Survey of the current state of lightweight cryptography for internet of things".IEEE Trans. 978-1-5090-59577/17/$31.00.
[13] Verbauwhede, I., Schaumont, P., and Kuo, H.: 'Design and performance testing of a 2.29 Gb/s Rijndael processor', IEEE J. Solid-S.Circ., 2003, pp. 569–572.
[14] Mangard, S., Aigner, M., and Dominikus, S.: 'A highly regular and scalable AES hardware architecture', IEEE Trans. Comput., 2003, 52 (4), pp.483–491