ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

An Efficient VLSI Architecture for Data Encryption Using AES Algorithm and Its FPGA Implementation

Akarsh B G[1], Darshan K S[2], Dheeraj Shridhar Harikant[3], Girichandra M Tarikeri[4], Akalpita Kulkarni[5]

U.G Student, Department of Electronics and Communication, Dr.AIT, Bengaluru , India[1]

U.G Student, Department of Electronics and Communication, Dr.AIT, Bengaluru , India[2]

U.G Student, Department of Electronics and Communication, Dr.AIT, Bengaluru , India[3]

U.G Student, Department of Electronics and Communication, Dr.AIT, Bengaluru , India[4]

Associate Professor, Department of Electronics and Communication, Dr.AIT, Bengaluru, India[5]

ABSTRACT: To accomplish the objective of secure correspondence, cryptography is one of the best fundamental activity. The more well known and broadly received symmetric encryption calculation prone to be experienced now a days is AES (Advanced Encryption Standard) calculation .It is found no less than 6 times quicker than old AES calculation. AES is an iterative as opposed to Feistel Cipher. It depends on substitution stage organize. Parallelization idea utilizes different assets to take care of substantial and complex issue. Throughput is increased by sub-pipelining and by number of different pipelining stages.

KEYWORDS: Cryptography, pipelining, AES-algorithm, Fiestel cipher, FPGA.

I. INTRODUCTION

Cryptography is presumably the most vital part of interchanges security, and it is an essential building square of PC security. It empowers us to store delicate data or transmit it crosswise over unreliable systems, with the goal that unapproved people can't read it. The direness of secure trade of advanced information brought about vast amounts of various crypto calculations that are assessed based on throughput, speed of task, and territory requirements. Every calculation performs different substitutions and change on unique information by utilizing a key. Contingent on the key, there are fundamentally two sorts of cryptographic calculations: symmetric and lopsided calculations. Symmetric frameworks, for example, Data Encryption Standard (DES), 3DES, and AES utilize an indistinguishable key for both encode the message and unscramble the figure content (scrambled plaintext). The AES appreciates gigantic notoriety in light of the fact that the preferences represent themselves The AES is utilized as a part of request to ensure information against unapproved get to and to encode this. The cryptographic procedure key of changing lengths is used for this reason. This is assigned AES-128, AES-192 or AES-256 relying upon the length. This technique for encryption of an information is thought to be especially secure and viable. It is utilized as a part of various conventions and transmission advances, for instance the WPA2 assurance of WiFi systems uses the Advanced Encryption Standard and similarly the SSH or IPsec Standard. With Voice-over-IP innovation (VoIP), the AES procedure is often utilized as a part of request to secure client and flagging data. Today, the AES is for all time incorporated into the equipment of numerous gadgets. This empowers more quick and powerful encryption and decoding than would be conceivable with unadulterated. For instance this encryption standard is unreservedly usable, brings about no permit expenses and isn't liable to patent limitations. Added to this come moderately low stockpiling and equipment prerequisites. The encryption calculation is uncomplicated and exquisite in programming, and is easy to actualize.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

II. RELATED WORK

. Hardware and software implementation of the AES algorithm is one of the most important area to attractive researches to do a research on it. In recent years a number of research papers have been publishing on AES algorithm to provide much more complexity and comparing the performance between the popular encryption algorithms to encrypt and decrypt data. In [6] Lu, etal proposed a new architecture method to reduce the complexity architecture of Cryptography and Network Security 2017 AES algorithm when it is implementing on the hardware such as mobile phone, PDAS and smart card etc. This method has consisted of integrating the AES encrypted and the AES decrypted to provide a perfect functional AES crypto-engine. To do that they focused on some important features of AES especially (Inv)SubBytes and (Inv)Mixcolumn module. A study in [9] has conducted on different secret key algorithms to identify which algorithm can be provided the best performance to encrypt and decrypt data. To do that there was conducted on four common algorithms such as Blowfish, AES, DES and 3DES. In this paper to evaluate these algorithm contents and sizes of encrypting input files were changed and two different platforms were used to test these algorithms such as P-II 266 MHz and P-4 2.4 GHz. According to the results Blowfish has the ability to provide the best performance compared to other algorithms and AES has a better performance than 3DES and DES. It also provide that 3DES 1/3 throughput of DES. In [10] provides the performance evaluation of symmetric encryption algorithms. This paper was conducted on six different common algorithms like AES, DES, 3DES, RC2, Blowfish and RC6. To compare among these algorithms different settings were performed on each algorithm such as different data types, different size of data block, different key sizes, battery power consumption and different speed for encryption and decryption data. Under these situations there was not found significant deference when the data types were based on hexadecimal encoding or 64 encoding and there is no difference when using audio, video, text or documents. According to the results Blowfish can provide better performance compared to other algorithms when the packed size was changing, followed by RC6. On the other hand, they found that DES has high performance compared to 3DES algorithm. To time consumption RC2 provided the worst performance over all algorithms. Whereas AES has better performance than three common algorithms RC2, DES and 3DES. However, it is clear from the results when the size of key was increasing, it needs more battery and time consumption.

III.METHODOLOGY

The basic VLSI architecture of the four transformations in AES is modified in the aspect of increasing the throughput and reliability. The overall throughput is increased by applying the pipelining register as shown in Figure 1. Register is used at the end of each round and further the architecture speed has been increased by introducing sub-pipelining technique . In between each transformation in that round a register is kept to speed up the execution process. The two areas of pipeline computer designs are Instruction Pipeline and Arithmetic Pipeline. Pipelining the instructions helps to increase instruction throughput by performing multiple instructions in parallel. Therefore it allows faster CPU throughput at a given clock cycle. The time needed between moving an instruction one stage down the pipeline and the ideal time per instruction on the pipeline will be increased. Some of the issues in pipelining technique are, data dependency problems which occur when the instruction depend on the previous instruction output. Resource conflict will occur in memory when two segments want to access it at the same time. The third problem is due to branch instructions. Equation 1, 2 and 3 helps to find the speedup of the architecture.

Speedup = non-pipeline / pipeline..... (1)
Where,
pipelined = (k +n-1)*tp.....(2)
non- pipelined =n*k*tp ..... (3)

Where, ‘k’ is the number of segments, ‘tp’ is the time consumed for a block and ‘n’ is the number of tasks.
Multiprocessor implementation takes advantage of increasing the encryption throughput of the hardware pipelining. In this work we have tried to further increase the throughput of the algorithm by sub-pipelining architecture. Increase the blocks of data that are executed in parallel in order to increase the throughput. This could be achieved by duplicating the round function hardware and placing the intermediate registers in between the rounds. The design will output a 128-

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

bit block of cipher text data at each clock cycle. The architecture of this sub-pipelining method requires more hardware resources when compared to a loop unrolling architecture.

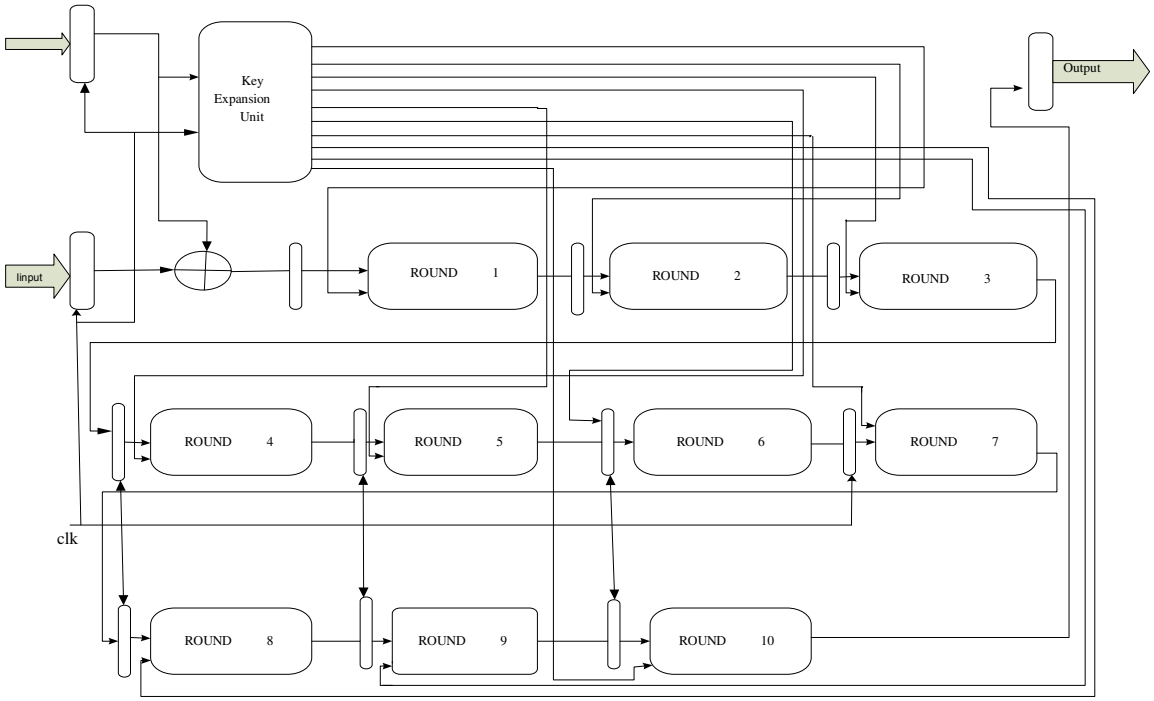

Figure 1.Optimized Pipelining Architecture

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round, the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

1. Substitute bytes

Each input byte of the State matrix is freely supplanted by another byte from a look-up table called S-box. The AES, S-box is a 256-entry table made out of two transformations: First each input byte is supplanted with its multiplicative inverse in $GF(2^8)$[1] with the element {00} being mapped onto itself followed by an affine transformation over $GF(2^8)$. For decryption, inverse S-box is obtained by applying inverse affine transformation followed by multiplicative inversion in $GF(2^8)$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

.

2. Shift rows

This stage (known as Shift Rows) is appeared in figure 2. This is a straight forward stage.It consists of following steps:
i. The first row of state isn't altered.
ii. The second row elements are moved 1 bytes to one side in a round way.
iii. The third row elements are moved 2 bytes to one side in a round way.
iv. The fourth row elements are moved 3 bytes to one side in a round way.

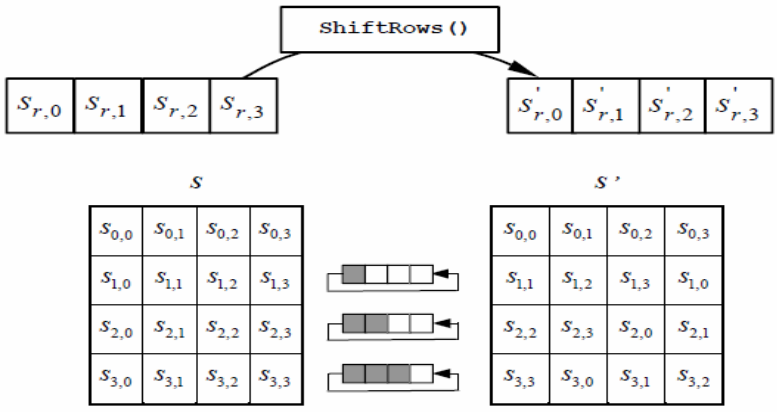

Fig 2.Shift rows

3. Mix columns

Mix column transformation is done by operating on column individually. Each column of the state matrix is multiplied with the standard GF matrix. The new element in the output matrix of mix column is obtained by sum of products of one row and one column.

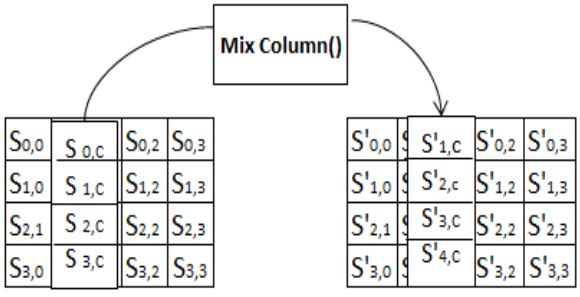

Fig 3. Mixed column

4. Add round key transformation

In this stage (known as Add Round Key) the 128 bits of state are bit wise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a state column and single word of the round key. The change is as basic as conceivable which helps in efficiency.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

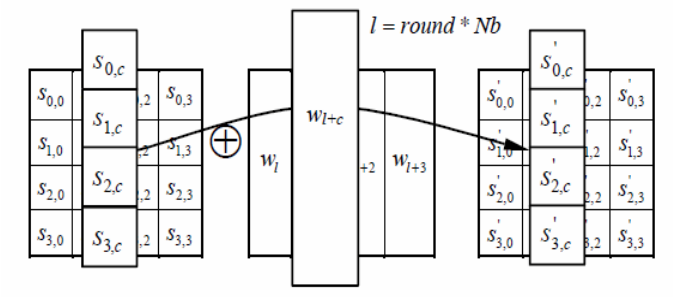

Fig 4. Add round key

5. AES key expansion

The AES algorithm requires four words of round keys for each encryption round. That is total of 4*(Nr + 1) round keys considering the initial set of keys required for the first Add Round Key transformation. All the round keys are derived from the cipher key itself. The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 4 words. Each round uses 4 of these words. Each word contains 32 bytes which means each sub-key is 128 bits long.

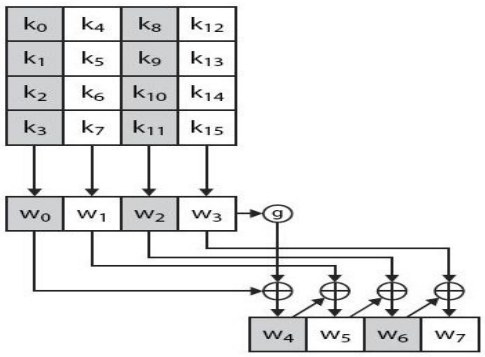

Fig 5. AES Key Expansion

IV.SIMULATION RESULTS

Inputs and Outputs Details are as follows:

The Plaintext given is = [3243f6a888a308d313198a2e0370734]H

The Cipher key is = [2b7e151628aed2a6abf7158809cf4f3c]H

The Cipher text generated is = [3925841d02dc09fbdc118597196a0b32]H

Simulated Waveforms for AES Encryption of 128 bit data which includes encrypt_out, plain_text, cipher_text and clock.

The encrypt_out is done by using plain text of 128 bits as inputs and by using cipher key of 128 bits.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

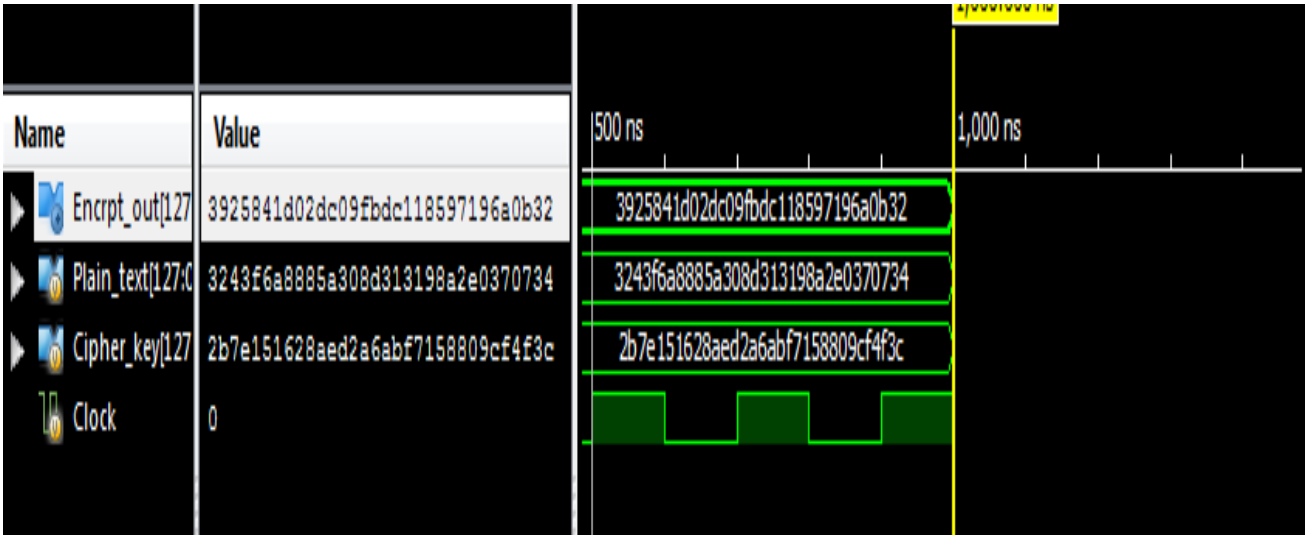

Figure 5.Simulation Results

V. CONCLUSION

In the VLSI architecture , AES is altered with a specific end goal to expand the speed ,throughput, and reliability. Speed is expanded atleast twice of existing design and also throughput. Furthermore a RTL code utilizing Verilog has been planned with pipelining structures for a better latency and throughput. Further work includes the realization of full encryptor or decryptor core as well as possible improvements of designs performance figures by using different optimization technique.

REFERENCES

[1] Marko Mali, Franc Novak and Anton Biasizzo"Hardware Implementation of AES Algorithm" –Journal of ELECTRICAL ENGINEERING, Vol. 56, No. 9-10, 2005,265-269.
[2] BehrouzA.ForouzanandDebdeepMukhopadhyay"CryptographyandNetworkSecurity" (2ndedition).
[3] L. Thulasimani , "A Single Chip Design and Implementation of AES -128/192/256 Encryption Algorithms"- International Journal of Engineering Science and Technology, Vol. 2(5), 2010,1052-1059.
[4] Nation Institute of Standards and Technology (NIST), Data Encryption Standard (DES), National Technical Information Service, Sprinfgield, VA 22161, Oct.1999.
[5] J. Daemen and V. Rijmen, "AES Proposal: Rijndael", AES Algorithm Submission, September 3,1999.
[6] Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285).
[7] K.GajandP.Chodowiec,ComparisonofthehardwareperformanceoftheAEScandidates using reconfigurable hardware, in The Third AES Candidates Conference, printed by the National Institute of Standards and Technology.
[8] W.Stallings, Network Security Essential Applications and Standards, New Jersey Pearson, Education,2000.
[9] Nadeem, H (2006). A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, (pp. 84-89).
[10] Diaa, S., E, Hatem M. A. K., & Mohiy M. H. (2010, May) Evaluating the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, Vol.10, No.3, (pp.213-219)