AN EFFICIENT IMPLEMENTATION OF AES IN FPGA

MONIGHA.A[1],YUVARAJ.G[2]

[1]*PG scholar, ECE Department, Vivekananda College of Engineering for Women*

[2]*Assistant Professor, ECE Department, Vivekananda College of Engineering for Women*

Abstract- Speed and area reduction are one of the major issues in VLSI applications. An implementation of the Advanced Encryption Standard (AES) algorithm is presented in this paper. The design uses looping method will reduce area and increase the speed .By using encrypted round for speed and pipelining ,isomorphic mapping method for area.This algorithm achieves efficiency and high throughput.

Keywords- Advanced Encryption Standard(AES) ,subbytes,mixcolumn,encrypted round

I.INTRODUCTION

Now-a-days security plays a vital role in eletronics world.The speed and area optimization is an important issue in today's electronics.The AES is a cryptographic algorithm that is used to protect electronic data or information. AES algorithm is a symmetric key used in that can encrypt and decrypt information.The AES algorithm input is applied,to perform number of rounds transformation and finally cipher is generated.

II.ADVANCED ENCRYPTION STANDARD

AES is a symmetric encrpyption alogrithm and it takes 128 bit data block as input and performs several rounds of transformation to generate output cipher text.The encryption process having four basic transformations are

1)Subbytes

2)Shiftrows

3)Mixcolumn

4)Addroundkey

2.1.Subbytes

This is one of the subtitution of bytes with help of SBOX

2.2.Shiftrows

During the operation,shifting the rows in that state array

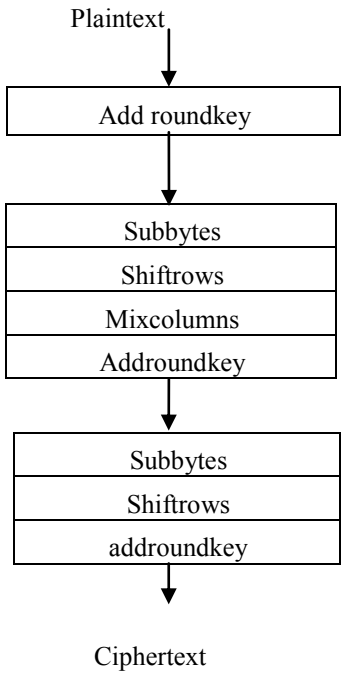


Figure 1. Block diagram of AES encryption

III. EXSITING WORK

3.1.One task one processor(OTOP)

Each task is performed in one processor and achieve low throughtput.To improve high

ISSN: 2278 – 909X

throughtput by using loop unrolling method in OTOP

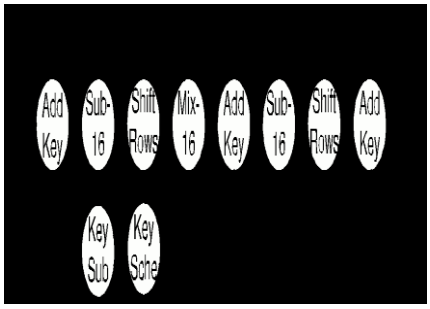


Figure..1. One-task One-processor

3.2. Loop-unrolled method

To enhance the AES cipher's throughput, we apply loop unrolling to the OTOP model**.**The loop unrolling breaks the dependency among different loops and allows the nine loops in the AES algorithm to operate on multi data blocks simultaneously

- **In parallel mixcolums:** Besides loop unrolling, way to increase the throughput of the OTOP model is to reduce the main loop's latency in the AES algorithm. In a single loop, the execution delay of MixColumns results in 60 percent of the total latency.
- **In Full parallelism:** AES implementation combines the Parallel-SubBytes MixColumns model and loop unrolling.

IV.RELATED TO EXISTING WORK

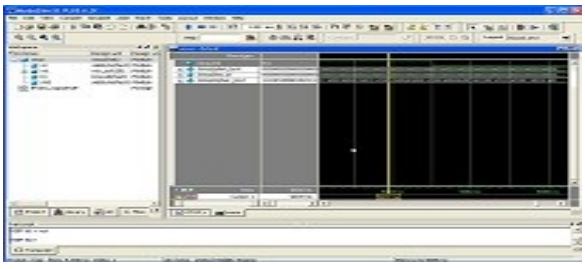


Figure 1:OTOP Simulation ouput

Figuure 2:Power Consumption of OTOP

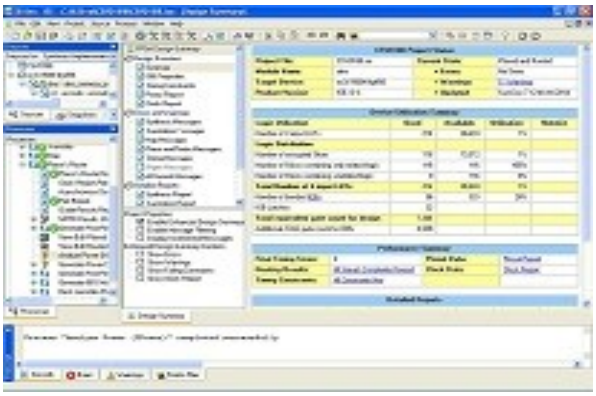


Figure 3:Area of OTOP

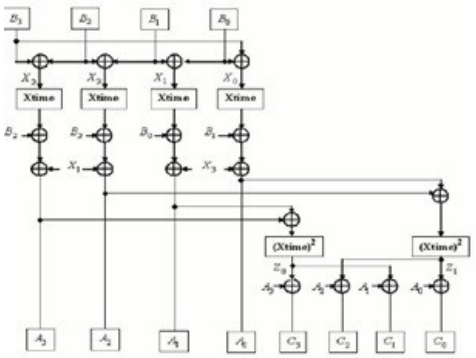
V. PROPOSED WORK

I did the changes in mixcolum, pipelining and key expansion system.In the mixcolum I have used bit level decomposition method, for pipelining I have used parallel pipelining and for key expansion system I have used encrypted round

5.1.Bit level decomposition

Mix column Methods based on X-time and decomposition bit level sharing techniques can be used for Integrated MC/IMC designs. Thus applying substructure sharing both to the computation with in a byte and between the bytes in a given column of the state, an efficient MC/IMC implementation architecture can be derived.

ISSN: 2278 – 909X



5.2.Parallel implementation of aes pipeline

Various architectures exist to realize the AES encryption/decryption algorithm. Among them, rolling and unrolling are the two basic architectures.

- The rolled AES pipeline uses a feedback structure where the data is iteratively transformed by round functions. This approach occupies small area, but achieves low throughput.
- In the unrolled AES pipeline, the round functions are pipelined furthermore.This best choice for implementation and gives maximum throughput area tradeoff.

5.3.Encrypted round

The encrypted round means the all the ten rounds are processed at a single round or at a time.

VII. RELATED TO PROPOSED WORK

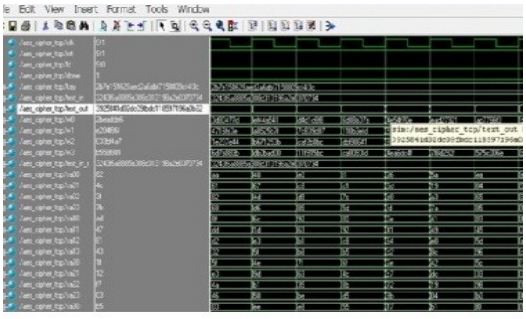


Figure 1:mixcolumn Simulation ouput

VII. CONCLUSION

The FPGA based parallel AES encryption for the core processor achieve the high speed and reduce the area compared to the existing system. The proposed work achieved the speed by using the encrypted round in the key expansion and the area optimization is achieved by using the AES parallel pipelining.

VIII. REFERENCES

[1]NIST,"Advanced Encryption Standard (AES),"hppt://csrc.nistgov/publications/fips/fips197, Nov. 2001

[2]S.Morioka and A.Satoh."A 10 gbps full AES Crypto Design with a Twisted BDD SboxArchitecture,"IEEE Trans.Very Large Scale Integration System,vol.12.no.7,pp.686-691,July

[3]Hodjat and I. Verbauwhede, "Area-Throughput Trade-Offs for Fully Pipeline30 to 70Gbits/s AES Processors," IEEE Trans.Computers, vol. 55, no. 4, pp. 366-372, Apr. 2006.

[4]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

[5]S.K.Mathew,F.Sheikh,M.Kounavis,S.Gueron,A. Agarwal,S.K.Hsu,H.Kaul,M.A.An ders and R.K.Krishnamurthy,"53 gbps Native GF(2^4) Composite Field AES Encrypt/Decrypt Accelerator for Content Protection in 45 nm High Performance Microprocessor."IEEE J.Solid State Circuits,vol.46,no.4,pp.767-776,Apr.2011

[6]Bin Liu, Student Member, IEEE, and Bevan M.Baas, Senior Member, IEEE "Parallel AES Encryption Engines for Many Core Processor Arrays" IEEE TRANSACTIONS ON COMPUTERS,vol.62,no.3,march 2013.

ISSN: 2278 – 909X

AUTHORS PROFILE

Ms.A.MONIGHA , Completed Under Graduate in Electronics and Communication Engineering from Mahendra Engineering College, Mallasamudram in 2013. She is currently pursuing master of engineering in Vlsi design in Vivekanandha College of Engineering for Women. Her area of interest includes Vlsi design and network

MR.G.YUVARAJ,received his Bachelors Degree in Electronics and Communication Engineering from K.S.R.College of Technology, Thiruchengode in 2004.He received his Master Degree in Applied Electronics from Kongu Engineering College, in 2008 .He is working as Assistant Professor in ECE in Vivekananda College of Engineering for Women. His area of interest is Vlsi Design and Low power Vlsi

ISSN: 2278 – 909X