iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** II **Month of publication:** February 2017

DOI: http://doi.org/10.22214/ijraset.2017.2044

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Implementation of AES Algorithm and Improve Throughput

T. Sivaprakasam M.E (Ph.D.)[1], Dr. M. Ramasamy[2], M. Kuralarasan[3]
[1] *Assistant Professor, Dept of ECE, Sri Shakthi Institute of Engg and Tech, Coimbatore-641062, Tamilnadu*
[2], *Professor, Dept of ECE, KSR college of Engineering,Thiruchencode*
[3] *PG Scholar, ME VLSI Sri Shakthi Institute of Engg and Tech,Coimbatore-641062,Tamilnadu.*

Abstract: ***Now a days VLSI application speed and area reduction is very important one. In this paper implemented AES algorithm.AES represents an algorithm for advance encryption standard of different operation required in the steps of encryption and decryption. The proposed architecture is based on optimizing area in terms of reducing and improve throughput for design of AES algorithm in VHDL .this paper presents AES-128 bit algorithm design consist of 128 bit symmetric key and XILINX ISE 14.1 project used for synthesis and simulation of this proposed design***
Keyword: advance encryption algorithm (AES); VHDL; FPGA; encryption and decryption

I. INTRODUCTION

The internet plays an important role in day-to-day life. The people can transfer important data through the internet such as Email, banking transaction and online purchase. In order to get secured transaction, network security is essential. Network security is mostly achieved through the use of cryptography. Cryptography refers to the art and science of transforming the message to make them secure and immune to attacks. Different algorithms and protocols are used to protect the data. In this paper implement AES algorithm. AES is a cryptographic algorithm that is used to protect electronic data or information.AES is a symmetric algorithm which process 128bit stream in 10 rounds. It uses same key for encryption information. The AES algorithm input is applied, to perform number 10 rounds transformation and finally cipher is generated

II. AES (ADVANCED ENCRYPTION STANDARD)

AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys

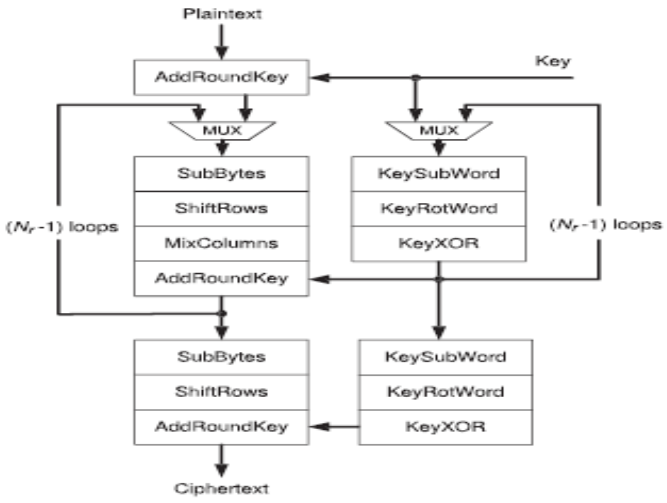


Figure 2.1 Block diagram of AES encryption

Each round in encryption process further follows some steps to complete each round till n. Each round possess four rounds
Subbytes
Shiftrows
Mixcolumn
Addroundkey

A. Substitution round

In this step, Sub-Bytes are byte-by-byte substituted during the forward encryption process.

B. Shift Rows

In this step, shifting the rows of the state array during the forward process(S-Box process)

C. Mix Column

Mix Columns for mixing up of the bytes in each column separately during the forward process.

D. Add Round Key

In this step, round key is added to the output of the previous step during the forward process. This step differs from others because of key size difference.

III. EXISTING METHOD

The AES algorithm has 4 phases that execute the process in sequential manner. The encryption process is achieved by processing plain text and key for initial and 9rounds, same decryption is takes place but in reverse Manner. A 4x4 state is formed in each round and particular length data is introduced in it for encryption process. The 10, 12, 12 rounds are there for 128, 192,256 bits in length respectively. Initially a key expansion process is used to expand the basic 16 byte key into 11 arrays of total
44 word. Due to this the 16 byte key is converted into 176 byte ie 44words which are further used for 11 rounds. AES is basically a recent cryptographic security algorithm, and in our proposed structure we uses basically symmetrical structure of 128 bit ie 11 round process. Out of these 11 rounds 1 round is used for initialization purpose and remaining 10 are used for AES actual process. There are mainly two logical steps for key expansion based on either the key is multiple of 4 or it is not multiple of 4. Once the key is expanded same key is used for encryption and decryption process to achieve symmetric AES structure

Bits	Key Length	Block Size	Number of Rounds
128	4	4	10
192	6	4	12
256	8	4	14

AES Rounds with Key length

The each round consist of total 4 phases used for
Formation of cipher text as an output of the respective step and that output feeded as input for next successive round. The overall process is same for next 10 round till Formation of cipher text is completed, but for all these rounds keys are differ that are derived from words (as Output of key expansion unit) from wO to w43.

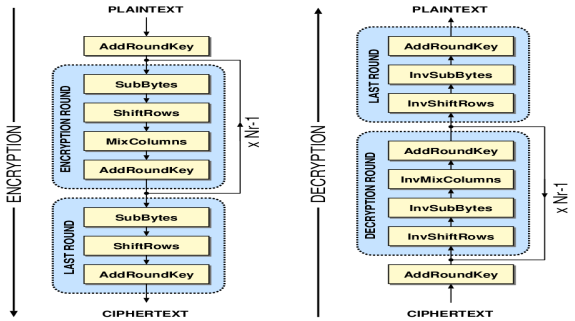


Figure 3.1 Block diagram of AES encryption and decryption process

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

As initially 11 arrays are formed out of that 1 use for
Initialization process and from that array key expansion is done. Thus the keys formed total W43 which are used further for next 10 rounds. Each round uses 4 word key along with plaintext/cipher text.

VHDL

We have used VHDL in order to design the hardware Elements, which will be run-time reconfigured. Some Important features of VHDL are: it is one of the most used HDL, it has a large and flexible syntax which allows to describe a circuit by using different abstraction levels
(Structural, data flow, or hardware behavior), it is possible to indicate low- level constraints (like place-and-route constraints), etc. All these features have motivated us to use VHDL.

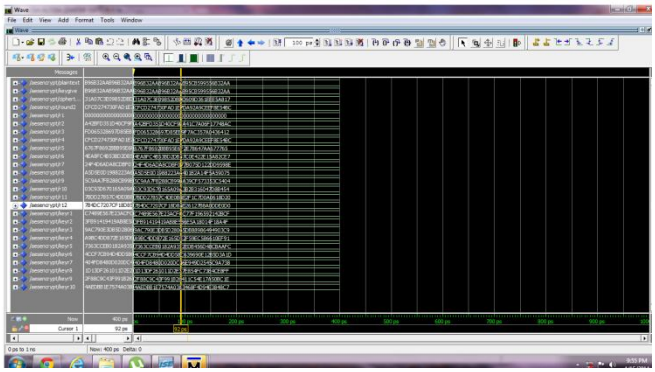


Figure 3.2modelsim simulation result

IV. PROPOSED SYSTEM

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

V. EXPERIMENTAL SETUP

A. 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

B. 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

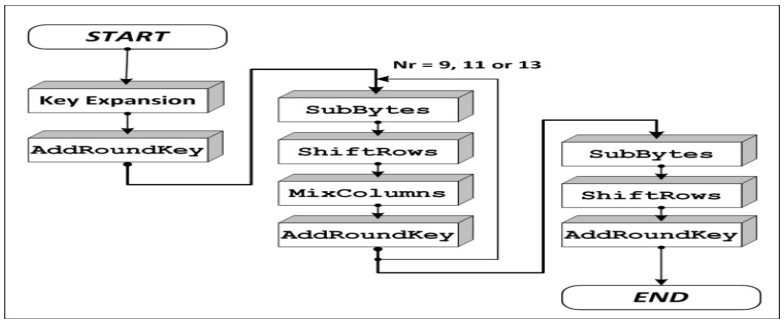
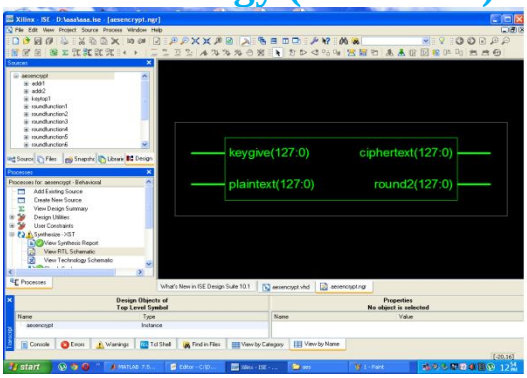


Figure 5.1 Block diagram of AES encryption

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



. Figure 5.2 simulation result for AES encryption

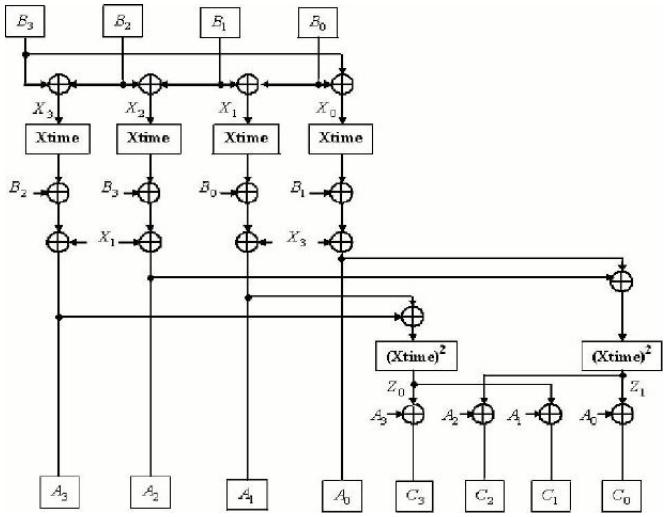


Figure 5.3bit level decomposition

The proposed architectures for MC/IMC transformation in AES has been simulated and validated by ISE 10.1 simulator and implemented on a Xilinx Virtex II Pro FPGA programmable platform using XC2VP30-5ff896 device.
Bit-level output expressions and placement attributes. Detailed analysis shows that arch-I combined MC/IMC design based on byte level sharing is the most optimum in size and delay analytically and arch-II separate MC/IMC design based on bit level sharing and FPGA structure is the most optimum in terms of resources on the selected device with placement attributes leading to a increase in throughput of the resulting AES Hardware.

VI. SIMULATION CIRCUIT

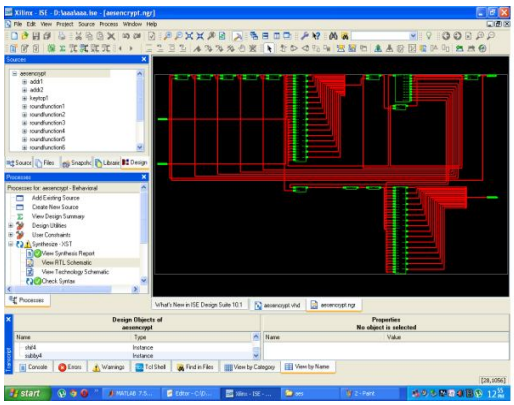


Figure 6.1simulation result

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

VII. EXPERIMENTAL RESULTS

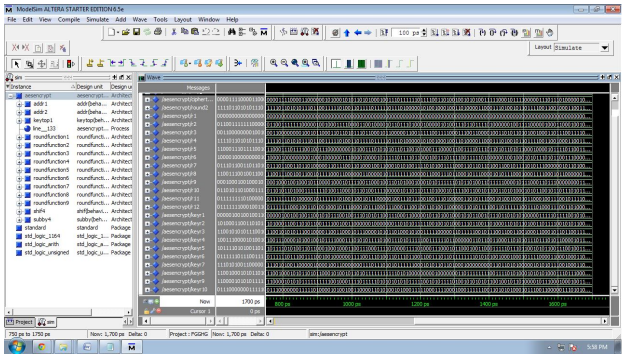


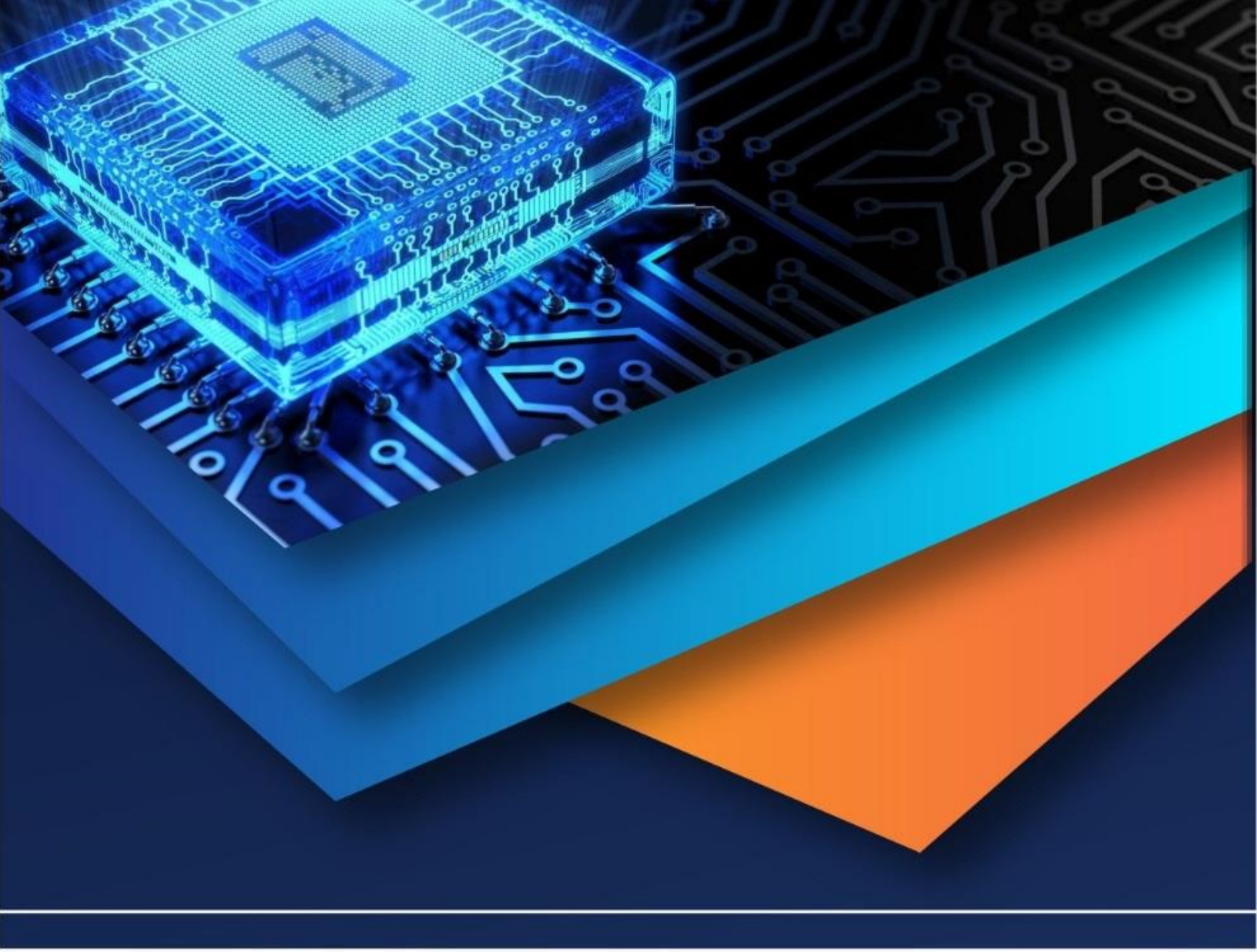
Figure 7.1 modelsim result AES algorithm

VIII. 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.

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 Sbox Architecture,"IEEE Trans.Very Large Scale Integration System, vol.12.no.7,pp.686-691, Jul
[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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY