International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 6, pp 30-32, June-2019

AES-256 Algorithm using FPGA

[1]Sayali Ingle, [2]Neha Lohikpure, [3]Rupali Shinde, [4]S.C.Wagaj

[1,2,3]Student, Department of Electronics and Telecommunication, J.S.P.M's Rajarshi Shahu College of Engineering, Pune, India
[4]Assistant Professor, Department of Electronics and Telecommunication, J.S.P.M's Rajarshi Shahu College of Engineering, Pune, India

***Abstract* – The rapid increase in the technology has brought up a requirement for more security. This has led to the development of one most secure algorithm for network security called AES algorithm using 256 Bits on FPGA. Advanced Encryption Standard Algorithm (AES) a National Institute of Standards and Technology specifications is an approved cryptographic algorithm that can be used for securing electronic data. Reprogrammable devices such as Field Programmable Arrays (FPGA) are highly attractive option for hardware implementation of cryptographic algorithm AES as they offer a quicker and more customizable solutions. This paper proposes an efficient FPGA implementation of advanced encryption standards (AES). The coding for encryption is done in VHDL language. To implement AES Rijndael algorithm on FPGA offers a better performance than any other cryptographic algorithms. This implementation is covered with other works to show the efficiency. The design uses an iterative looping approach with block and key size of 256 bits, lookup table implementation of S-box. This gives low complexity architecture and easily achieves low latency as well as high throughput.**

Keywords: Encryption, Decryption, FPGA, AES.

I. INTRODUCTION

Today, the transmission of large amount of Data through Internet is playing the important role in various fields. Increasing the utilization of web and remote correspondence requires the safety efforts to secure the information transmission through open channel by the client. Sometimes there might be the possibility that the data transmitted through open channel from sender to receiver. So, to protect these different techniques and method have been using by private and public sectors. To fulfill this AES(Advanced Encryption Algorithm) was an introduced by NIST (National Institute of Standards and Technology) in December 2001. Due to the power consumption and power attack AES algorithms and standards come as a replacement for DES. The AES algorithm has many applications such as a storage cards, ATM (Automated Teller Machine), cell phones, advanced video recorders and monetary exchanges, PC etc. Programming and equipment executions are some potential problems in AES calculation. In VLSI based processor implementation, for doing each round operation separate the procedure speed also. For the AES application in installed frameworks and smart cards, the region is constrained and for the media transmission the speed in the scope of GBPS is fundamental. AES algorithm is implemented using FPGA (Field Programmable Gate Array). For the encryption process total 14 rounds take place for 256 bits while for 128 bits 10 rounds takes place.

Field Programmable Gate Arrays (FPGA) are semiconductor devices that are based around a matrix of configurable logic blocks (CLBs) connected via programmable interconnects. FPGA can be reprogrammed to desired applications or functionality requirements after manufacturing. This feature distinguishes FPGAs from Application Specific Integrated Circuits (ASICs), which are custom manufactured for specific design tasks. Although one-time programmable (OTP) FPGAs are available, the dominant types are SRAM based which can be reprogrammed as the design evolves.

a) Algorithm flowchart

DECRYPTION

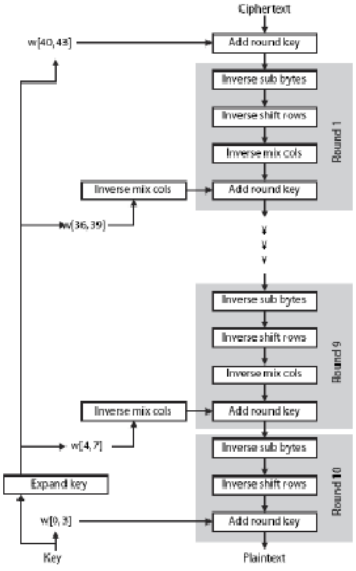

Figure 1: Decryption Flowchart

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 6, pp 30-32, June-2019

ENCRYPTION

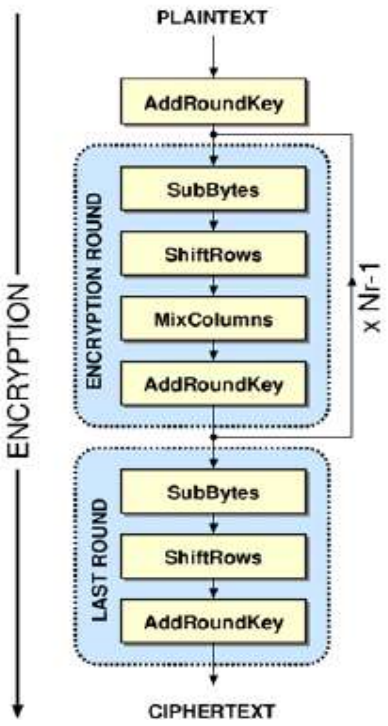

Figure 2: Encryption Flowchart

II. LITERATURE SURVEY

Wang Wei, Chen jie, Xu Fei "Efficient FPGA implementation of the Advanced Encryption"

This paper introduced the mathematical principle, encryption process and logical structure of Advanced Encryption Standard algorithm. The data can be secured by using the method AES algorithm. The purpose of AES algorithm is to improve the system computing speed, parallel processing methods were used and the pipelining. AES encryption algorithm uses a specific key to secure the data. The AES is a Federal Information Processing Standard (FIPS).

A. Amaar, I. Ashour and M. Shiple "Implementation of Advanced Encryption Standard (AES) on FPGA"

This paper presented a compact implementation of Advanced Encryption Standard (AES) using different devices of FPGA technology. In AES algorithm the data is transmitted to FPGA with the help of MATLAB. The AES algorithm is implemented on FPGA with hardware in loop. FPGA Artix 7Nexys 4 kit is used to implement the algorithm and the configuration of algorithm is done with the help of software development kit in Xilinx ISE design suit.

Shelke R.B., Patil A.P., Dr. Patil S.B."VLSI Based Implementation of Single Round AES Algorithm"

VLSI based implementation of single round of AES algorithm is presented in this paper. The AES algorithm is capable of using keys of 128, 192 and 256 bits, in this paper 128-bit key length with single round is implemented. VHDL is used as the hardware description language. The software used is Xilinx ISE design suit 13.2 the tools primarily used is the Xilinx ISE and ISim for simulation, synthesis and implementation. Some results are verified using test bench.

P. Aatheeswaran, Dr. R. SureshBabu "FPGA CAN BE IMPLEMENTED BY USING ADVANCED ENCRYPTION STANDARD ALGORITHM"

Iimplementation of AES encryption and decryption standard using 128-bit key is mainly focused in this paper. Input plaintext of 128 bit and output cipher text of 128 bit is shown. Encryption coverts to an unintelligible form cipher text and decrypting the data from cipher text back to its original form called plain text. The AES is an iterative algorithm. Two different architectures of AES, namely iterative and concurrent have been implemented in Xilinx FPGA.

III. RESULTS AND DISCUSSIONS

The problem security is solved with the help of AES-256 encryption and decryption algorithm using FPGA. The data is sent in the coded form for more security purpose and only the authorized person can access this data that provides more security to this system. Additional to this its speed of processing is also very fast as compared to that of other algorithms.

IV. CONCLUSION

We have understood the concept of Network security, need of AES algorithm and the basic approach of AES algorithm that we have found in the literature and references. The basic unit of AES algorithm process is a byte and this algorithm is based on Substitution Permutation network it means it has series of linked mathematical operations. We have described the AES algorithm process and explained our methodology and how exactly we are going to implement the algorithm.

REFERENCES

[1] Hoang Trang and Nguyen Van (2012), "An efficient FPGA implementation of the advanced encryption" Standard algorithm IEEE 978-1-4673-0309-5/12.

[2] Pritamkumar N. Khose, Prof. Vrushali G. Raut "Implementation of AES Algorithm on FPGA for low Area Consumption"2015 International conference on Pervasive Computing (ICPC).

ISSN (online): 2581-3048
Volume 3, Issue 6, pp 30-32, June-2019

[3] Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani "EFFICIENT IMPLEMENTATION OF AES ALGORITHM ON FPGA" International Conference on Communication and Signal Processing, April 3-5, 2014, India.

[4] Chen-Hasing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu "AN Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems" IEEE TRANSACTIONS, VOL. 18 NO. 4, April 2010.

[5] Bin L iu, Student Member, IEEE, and Bevan M. Baas, Senior Member, IEEE "Parallel AES Encryption Engines for Many Core Processors Arrays "IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3, MARCH 2013.

[6] Tim Good, Student Member, IEEE, and Mohammed Benaissa, "very Small FPGA Application-Specific Instruction Processor for AES" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, VOL. 53, N.7, JULY 2006.

AUTHOR'S BIOGRAPHIES

Miss. Sayali S. Ingle
Student, Department of Electronics and Telecommunication J.S.P.M's Rajarshi Shahu College of Engineering, Pune, India

Miss. Neha D. Lohikpure
Student, Department of Electronics and Telecommunication J.S.P.M's Rajarshi Shahu College of Engineering, Pune, India

Miss. Rupali Shinde
Student, Department of Electronics and Telecommunication J.S.P.M's Rajarshi Shahu College of Engineering, Pune, India

MR. S. C. Wagaj
Assistant Professor, Department of Electronics and Telecommunication, J.S.P.M's Rajarshi Shahu College of Engineering, Pune, India

Citation of this article:

Sayali Ingle, Neha Lohikpure, Rupali Shinde, S.C.Wagaj, "AES-256 Algorithm using FPGA" Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET)*, Volume 3, Issue 6, pp 30-32, June 2019.

