International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

# REVIEW ON DESIGN OF AES ALGORITHM USING FPGA

**Radhika D.Bajaj[1] , Dr. U.M. Gokhale[2]**

[1]M.Tech VLSI, Electronics and Telecommunication, GHRIETW, Nagpur,Maharashtra,India.

[2]Professor, Electronics and Telecommunication, GHRIETW, Nagpur,Maharashtra,India.

***Abstract:*** ***Increasing need of data protection in computer networks led to the development of several cryptographic algorithms hence sending data securely over a transmission link is critically important in many applications. AES represents an algorithm for Advanced Encryption Standard consisting of different operations required in the steps of encryption and decryption. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. This paper represents design of AES algorithm of 128 bit. The software Xilinx ISE project navigator is used for synthesis and simulation of these proposed algorithm purpose.***

***Key Words:*** AES, DES, Encryption, Decryption, Cryptography, FPGA, cipher text.

## 1. INTRODUCTION

Everyday millions of users generate and interchange large volumes of information in various fields such as medical reports, and bank services via Internet. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. Encryption is usually done just before sending data. To utilize the channel resources completely encryption algorithm must have a speed at least equivalent to data transmission speed. Achieving high throughput for encryption algorithm for a communication channel of high data rate is a challenging task. Encryption is a transformation technique to change one form of data called plain text to an unreadable form of data, called cipher text.

Initially DES (Data Encryption Standard) based encryption scheme was used in 1977 by FIPS (Federal Information Processing Standard). In DES data are encrypted in 64 bit block using 56 bit key. This scheme was considered as most secured scheme till 1998; because in 1998 EFF (Electronic Frontier Foundation) announced it developed DES cracker to crack code. Due to the short key length of DES it is replaced by the Rijndael algorithm which has became as a standard in the cryptography domain, known as Advanced Encryption Standard (AES).The AES was published by National Institute of Standards and Technology (NIST) in 2001. Later Rijndael algorithm was selected as AES algorithm.

## 2. REVIEW WORK

Below written is the analyzed review work on various researches done by the authors on AES and DES algorithms using FPGA. Here a brief study has been done on each paper that has been reviewed.

Nimmi Gupta presents the paper on DES encryption algorithm upto 4 round and used Xilinx software and implemented on Spartan 3 Modelsim. The two cryptographic techniques namely symmetric and asymmetric are briefly discussed and also DES encryption algorithm is explained thoroughly[1]. Sombir Singh, Sunil K Maakar, Dr. Sudesh Kumar planned their work on enhancing the security of DES algorithm using transposition technique of cryptography. If the transposition technique is used before the original DES algorithm then the intruder has to first break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm [2]. Mital Maheta presented the paper on Design and Simulation of AES algorithm. The RC6 algorithm is being explained and thereby implemented. In this paper the number of slices used is very less and design with minimum utilization is presented. This design offers minimum period of 13.345 ns (Maximum Frequency- 74.934MHz) [3]. Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani planned their work on the topic Efficient implementation of AES algorithm on FPGA in VHDL using Xilinx ISE 14.1 Project Navigator. The basic study of AES and its evolution from Rijndael algorithm is being described in this paper. The four transformation techniques of AES as well as

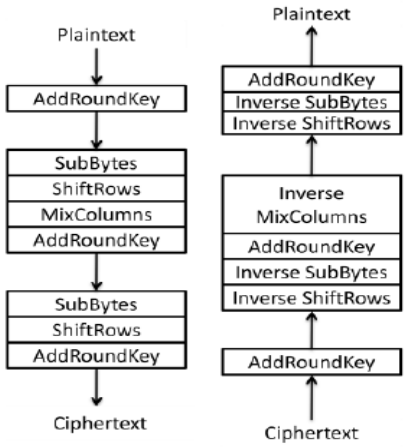
Encryption S-box and Decryption S-box are being explained in detail[4].

Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen has carried their work on FPGA implementation of AES based crypto processor using Xilinx ISE 14.4. The AES is integrated with a 32-bit general purpose 5-stage pipelined MIPS processor. In this paper, at the operating frequency of 553 MHz, the proposed design achieved the throughput of 58 Gbps, latency of 240 ns, and the minimum power consumption of 76 mw[6] . Abhijith.P.S, Mallika Srivastava, Aparna Mishra, Manish Goswami, B.R.Singh has studied in detail on AES encryption as well as decryption using Xilinx Virtex 5 FPGA. In this paper, the encryption unit takes 10 clock cycles to complete the operation. The maximum path delay of the design is 3.420ns resulting in a maximum frequency of operation as 292.403MHz. The throughput of the proposed encryption module is 3.74Gbps[7] . Manjesh.K.N, R K Karunavathi planned their work on High throughput implementation of AES algorithm using Xilinx ISE 9.2 Simulator and Synthesis is done by using RTL Compiler v11.2. In this paper the AES algorithm is encrypted and decrypted by using a single 128 bit block. At throughput frequency of 100 MHz clock, the Encryption block operates at an average frequency of 195 MHz for all pipelining stages and Decryption block operates at an average frequency of 226 MHz [9].

## *3. AES ALGORITHM*

The AES is basically a crypto graphical algorithm designed for the purpose of security. The NIST (National Institute of Standards and technology) issued a request for AES to replace DES in September 1997. The 15 candidate's algorithms were selected and a year later only 5 finalist were announced in August 1999.These five algorithms are MARS, RC6, Rijndael, Serpent and Twofish. The Rijndael algorithm, developed by Joan Daemen and Vincent Rijmen was selected as the winner of the AES development process in October 2000. The FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197(FIPS 197) specifies an algorithm called Advanced Encryption Standard (AES) in Nov-26-2001.

AES has advantages as it provides combination of security, performance, efficiency and flexibility. For any security system Key size is very important, it determines the strength of security, area optimization and power consumption. As AES is derived from Rijndael it is also called as Rijndael in cryptography to protect sensitive data by converting it into unintelligible form called as a cipher text means coded text.




**(a) Encryption process (b) Decryption process**

Fig.1. AES Encryption/Decryption process

The AES algorithm is a symmetric block cipher that can encrypt as well as decrypt information. Encryption converts data into an unreadable form known as cipher-text. Encryption of the cipher-text converts the data back into its original readable form, which is called plain-text.AES as well as most encryption algorithms, are reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order.

The AES algorithm operates on bytes, which makes it simpler to implement and describe. The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption which is the symmetric type of cryptography. The data block length is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. In addition, the AES algorithm is also an iterative algorithm.

For encryption, each round consists of the following four steps:
1) Sub bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key.
For decryption, each round consists of the following four steps:
1) Inverse shift rows, 2) Inverse bytes, 3) Add round key, and 4) Inverse mix columns.

### *3.1 Sub Bytes:*

The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits. The goal of the substitution step is to reduce the correlation between the input bits and the output bits at the byte level. The bit scrambling part of the substitution step ensures that the substitution cannot be described in the form of evaluating a simple mathematical function.

### 3.2 Shift Row:

The Shift Row transformation consists of (i) not shifting the first row of the state array at all; (ii) circularly shifting the second row by one byte to the left; (iii) circularly shifting the third row by two bytes to the left; and (iv) circularly shifting the last row by three bytes to the left. Recall again that the input block is written column-wise.

### 3.3 Mix Column:

The Mix Column transformation replaces each byte of a column by a function of all the bytes in the same column. More precisely, each byte in a column is replaced by two times that byte, plus three times the next byte, plus the byte that comes next, plus the byte that follows.

### 3.4 Add Round Key:

Each round has its own round key that is derived from the original 128-bit encryption key .One of the four steps of each round, for both encryption and decryption, involves XOR ing of the round key with the state array. The AES Key Expansion algorithm is used to derive the 128- bit round key for each round from the original 128-bit encryption key.

Decryption is exactly reverse of encryption which inverses round transformations to compute out the original plain text of an encrypted cipher text in reverse order. The round transformation of decryption uses the functions Add Round Key, Inv Mix Columns, Inv Shift Rows, and Inv Sub Bytes successively. Add Round Key is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order. Inv Mix Columns needs a different constant polynomial than Mix Columns does. Inv Shift Rows rotates the bytes to the right instead of to the left. Inv Sub Bytes reverses the S-Box look-up table by an inverse transformation followed by the same inversion over which is used for encryption.

## 4. PROPOSED WORK

The figure below is the unit block diagram showing AES encryption as well as decryption process. The Key generation module is the most important component of this algorithm. We are therefore designing 128 bit AES.

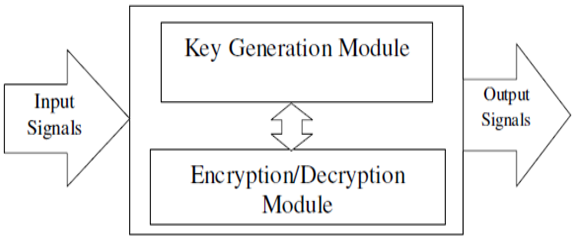



Fig 2. AES Encryption and Decryption Unit Block Diagram

Encryption algorithm is being used by military and government over a last couple of decades for securing communication. The main purpose of encryption is to hide data from unauthorized usage. Thus AES-128 algorithm for encryption and decryption will be designed and synthesized on Xilinx ISE project navigator using Verilog. The various performance parameters of the design like throughput, latency, area, power, etc will be calculated and compared with the previous work.

## REFERENCES

[1] Nimmi Gupta “Implementation of Optimized DES Encryption Algorithm upto 4 Round on Spartan 3”, International Journal of Computer Technology and Electronics Engineering , Volume 2 , Issue 1,Jan 2012.

[2] Sombir Singh, Sunil K Maakar, Dr. Sudesh Kumar “Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[3] Mital Maheta ”Design and simulation of AES algorithm- Encryption using VHDL”, International Journal of Engineering Development and Research Volume 2, Issue 1, 2014.

[4] Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani “Efficient Implementation of AES Algorithm on FPGA”,Progress In Science in Engineering Research Journal, 2014, ISSN 2347-6680pp.170-175.

[5] Ashwini R. Tonde and Akshay P. Dhande“ Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA”, International

Journal of Current Engineering and Technology ,Volume 4,No.2 ,April 2014.

[6] Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen "FPGA Implementation of AES-based Crypto Processor",*IEEE* 2013.

[7] Abhijith.P.S, MallikaSrivastava, Aparna Mishra, Manish Goswami, B.R.Singh "High Performance Hardware Implementation of AES Using Minimal Resources", *IEEE International Conference* on Intelligent Systems and Signal Processing (ISSP),2013.

[8] K. Soumya, G. Shyam Kishore "Design and Implementation of Rijndael Encryption Algorithm Based on FPGA",International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 9, September 2013,pp.120-127.

[9] Manjesh.K.N, R K Karunavathi"Secured High throughput implementation of AES Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 1193-1198.

[10] Ohyoung Song, Jiho Kim "Compact Design of the Advanced Encryption Standard Algorithm for IEEE 802.15.4 Devices", Journal of Electrical Engineering & Technology, Vol. 6, No. 3, pp. 418-422,2011.