International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

AES-128 IMAGE CRYPTOGRAPHY AND ITS FPGA IMPLEMENTATION

Durgesh Kumar Gupta[1], Prof. Prashant Gupta[2]
Dept. - Electronics & Communication, Ideal institute of technology, Place – Ghaziabad (U.P.).

Abstract: This paper presents encryption and decryption of an image and their hardware implementation on FPGA. Advance encryption standard (AES) is an approved cryptography Algorithm that used in security of electronic data transaction. The design has been coded by Verilog hardware descriptive language. The algorithm was implemented in FPGA using QuestaSim, MATLAB, and Xilinx ISE software. In this cryptographic process 128 bit Plaintext and 128 bit initial key, as well as 128 bit output of Ciphertext are all divided into four 32 bit units respectively The aim this division is to reduced the latency and to increase Throughput of whole process. In this encryption there are 4 steps subbytes, shift rows, mix column and add round key. In fourth step we made computation and key generation simultaneously, so whole computation occurred in 10 rounds 10 clocks while in previous work both occurred in separate round and took 10 rounds but more clocks.

Keywords- AES, Verilog, Plaintext, Ciphertext, FPGA.

I. INTRODUCTION

In advance communication world to prevent data hacking was a large challenge in front of National Institute of standard and technology. Every day many users generate and interchange large amount of data in various field through internet, e-commerce and Networking [1, 8].With the continuous development of cryptographic technique, DES algorithm with 56-bit key length so the advance standard of DES algorithm is invented by NIST known by AES algorithm. In 1997 NIST made formal call for algorithm. In 1998 a group of fifteen candidate of AES algorithm is collected. These algorithm with were subjected to assessment process conducted by various group of cryptographic researchers all over the world. In august 2000, five algorithms out of 15 algorithms selected. They are Mars, RCE, Rijndael, Serpent and Towfish .these algorithm were Subjected further analysis finally NIST announced Rijndael algorithm was the winner. Our proposed work is an FPGA based design and implementation of 128 bit algorithm. This method gives very low latency and very high throughput. There are various AES algorithm based on key length like 128,192 and 256 bits [3] .They are performed in blocks of 128 bits. The hardware implementation of this algorithm provides high performance and low cost for specific application. FPGA implementation has much advantage over ASIC implementation. It provides faster hardware solution than ASIC.

II. DESIGN OF AES ALGORITHM

This algorithm composed of three main parts cipher, inverse cipher and key expansion.

(i) Cipher – This step converts data to an unintelligible form called Ciphertext.

(ii) Inverse cipher- It converts data back into its original form called plaintext. can easily break because of short Key length. This has very small number of different combination.

(iii) Key expansion- It generate a key schedule that used in cipher process and inverse cipher process

A. AES ENCRYPTION

It consists of steps. Which are given below?

(i) Sub bytes (ii) Shift rows

(iii) Mix column (iv) Add round key

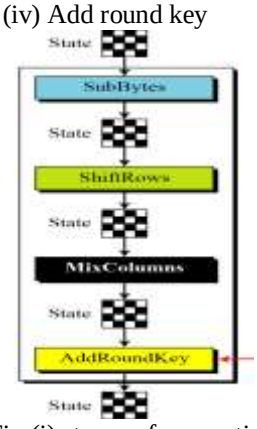


Fig (i) stages of encryption

(i) Sub bytes transformation- it is a on linear bytes substitution operating on each of the state bytes .The sub bytes transformation performed using a precalculated table consisting 16 rows and 16 columns. This table is also called S-box that contains 256 numbers (from 0 to 255) and their corresponding resulting values [3].

(ii) Shift rows transformation- In encryption process the rows of states are cyclically left shifted, according to value of number of row .But row 0 is not shifted, row 1 shifted one byte to left row 2 shifted two byte to left and row 3 shifted three byte to left [3].

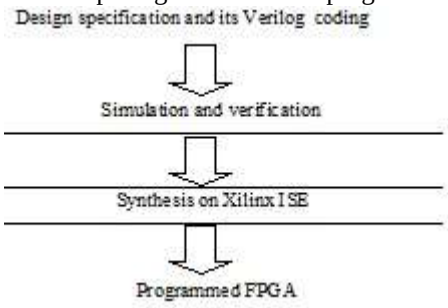
(iii)Mix columns transformation- In this column transformation the columns of the states are consider as polynomial over gross field(GF) 2^8 and multiplied by modulo x^4 +1 with a fixed polynomial c(x) ={01}x^3+{01}x^2+{01}x+{02}.In decryption the whole process is identical since XOR own inverse, with reverse key. It designed to be as simple as possible. A form of VERNAM cipher on expended key requires other stages for complexity and security [7].

(iv) Add round key - In this process a round key is added to

the states resulted from the operation of mix column Transformation by a simple bit wise XOR operation [5]. The round key of each round is derived from main key using key expansion algorithm. The encryption /decryption algorithm needs eleven 128 bits round key [10].While first round key [0] is main key

B. Design Flow chart

There are 4 design steps in AES. In first we made Verilog coding of whole process. In second step we simulate the coding and verify it. In next step we synthesize the whole process. In last step we generate FPGA program.



C. AES decryption

Decryption is a reverse process of encryption. It has also 4 steps like encryption process. The sequence of these steps becomes reverse. In this process cipher text is used with add round key, inverse mix columns, inverse shift rows, and inverse sub bytes respectively [2].

D. Table of result

This table shows comparison of both results of previous work and updated work of whole AES-128 process.

Works	Encryption		Decryption	
	No. of clocks	Throughput	No. of clocks	Throughput
Previous	13	1054Mbps	25	615Mbps
Current	10	1814Mbps	10	1586Mbps

E. SIMULATION RESULTS

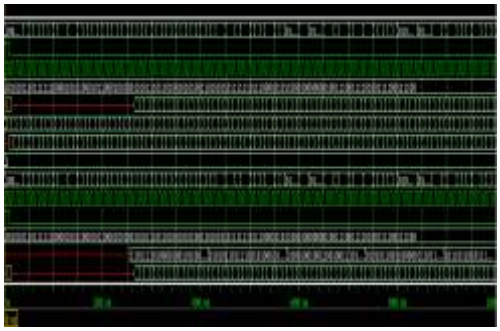


Fig (2) Simulation wave diagram of Encryption

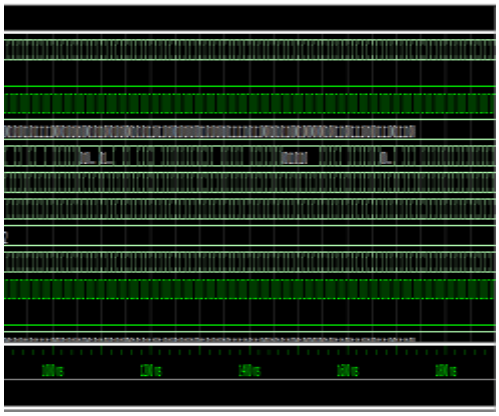


Fig (3) simulation wave diagram of decryption

Fig (4) Input image

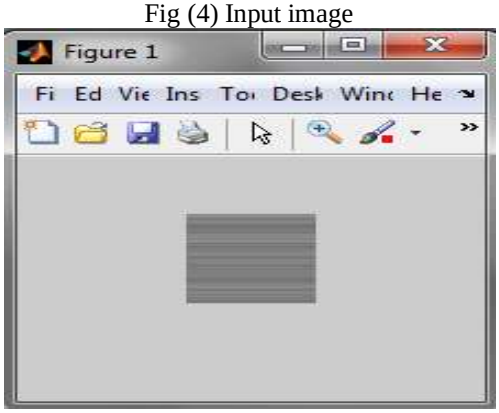


Fig (5) Encrypted image

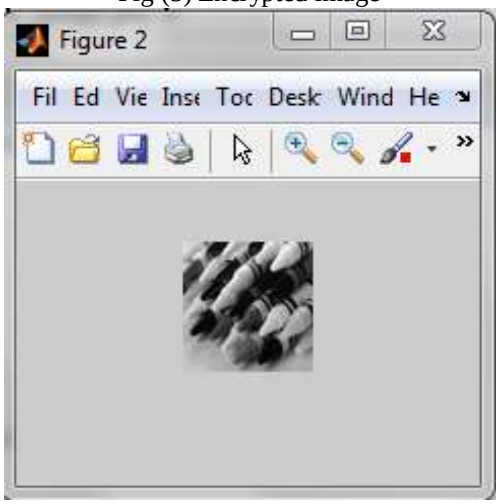


Fig (6) output image

F. Synthesis results

Here we describe device family which used in synthesis process. And time has taken in per clock.

(1)Timing Summary of Encryption
Minimum period: 4.410ns (Max freq: 226.76MHz)
Minimum input arrival time before clock: 4.047ns
Maximum output required time after clock: 0.659ns
Maximum combinational path delay: No path founding

(2) Device summary of encryption
Selected Device: 6vcx75tff484-2
Number of Slice Registers: 538 out of 93120 0%
Number of Slice LUTs: 1922 out of 46560 4%
Number used as Logic: 1922 out of 46560 4%
Slice Logic Distribution: Number of LUT Flip Flop pairs used: 1937
Number with an unused Flip Flop: 1399 out of 1937 72%
Number with an unused LUT: 15 out of 1937 0%
Number of fully used LUT-FF pairs: 523 out of 1937 27%
Number of unique control sets: 6
IO Utilization:
Number of IOs: 146
Number of bonded IOBs: 146 out of 240 60%

(3) Device summary of decryption
Selected Device:
6vcx75tff484-2
Slice Logic Utilization:
Number of Slice Registers: 1819 out of 93120 1%
Number of Slice LUTs: 6509 out of 46560 13%
Number used as Logic: 6509 out of 46560 13%
Slice Logic Distribution:
Number of LUT Flip Flop pairs used: 6591
Number with an unused Flip Flop: 4772 out of 6591 72%
Number with an unused LUT: 82 out of 6591 1%
Number of fully used LUT-FF pairs: 1737 out of 6591 26%
Number of unique control sets: 6
IO Utilization:
Number of IOs: 146
Number of bonded IOBs: 146 out of 240 60%

(4) Time summary of Decryption
Minimum period: 5.044ns (Max freq; 198.250MHz)
Minimum input arrival time before clock: 26.786ns
Maximum output required time after clock: 0.659ns
Maximum combinational path delay: No path found

III. CONCLUSION

The AES 128 bit algorithm has been efficiently implemented using different software. In this algorithm there are 128 bit key lengths with 128 bit block size .The design is coded using Verilog Hardware descriptive language and synthesis is done by Questa Sim software. Varification of coding is done by Xilinx ISE simulator. Hardware implementation of this algorithm provides high speed and low cost for specific application.

REFERENCES

[1] International conference on computer communication and informatics (ICCCI-2014), Jan 03-05-2014 Coimbatore, India.
[2] The first international conference of Electrical, Communication, Computer, Power and control Engineering ICECCPCE 13 Dec 2013.
[3] IEEE Global conference on wireless computing and networking in 2013 (GCWCN).
[4] International conference on computing Electronics and Electrical Technologies in 2012 (ICCEET).
[5] International conference on computer science and application in 2013.
[6] International journal of advance research in computer and communication Engineering Vol.3 issue 1 Jan 2014.
[7] International journal of Computational Engineering Research (ijceronline.com) Vol.2 7 Nov 2012.
[8] International journal of computer science and mobile computing volume2, 4April2013

