Implementation of Advanced Encryption Standard on FPGA

Rashmi R. Patil,
Department. Of Electronics and Telecommunication, MITCOE, PUNE,

Prof. V. V. Shete
Department. Of Electronics and Telecommunication, MITCOE, PUNE,

Abstract

Speed and the area are the major limitations of embedded systems. There are number of Encryption standards available for Encryption and Decryption. These standards are analysed with different input block sizes and keys. In this paper a comparison of Advanced Encryption Standard with other algorithms like DES, TRIPLE DES, BLOWFISH, RC2 are discussed. The comparison of parameter average encryption decryption time and the throughput of Advanced Encryption standard with above algorithms are discussed. The AES provides high throughput with minimum encryption decryption time.

1. Introduction

For the information security there are many encryption algorithm are available. They are classified into private (symmetric) and public (asymmetric) keys encryption. In the symmetric key, encryption only one key is used for both encryption and decryption. Before the information transmission the key should be distributed. Anyone can decrypt the data if the key is weak. If a longer key is used it is hard to break the information than smaller key. In the asymmetric key encryption, there are two keys, private key and public key. The public key is used for encryption and private key is used for decryption. There is no need of key distribution in asymmetric key algorithm before transmission.

2. Related Work

The commonly used symmetric encryption algorithms are DES, 3DES, RC2, BLOWFISH The Data Encryption standard Technique uses 64 bits of block ciphers that is, at a time 64 bit of data is encrypted. This uses number of rounds where each of the rounds contains exclusive OR, bit shuffling, non-linear substitutions (use of s-box)[13]. The triple Data Encryption Standard is applied three times to the each data block. The 3DES technique gives simple way of key size increment to protect the data without designing a new algorithm for higher security. The RC2 (Rivest cipher) technique is a variable key size technique which has 64 bit block cipher which uses 18 rounds [4]. Two fish technique is a 128 bit symmetric block cipher. It can accept the variable length of the key up to the 256 bits. It contains 16 rounds [16]. The AES is the successor of DES. It is a standard symmetric encryption algorithm. AES accepts keys of 128, 192 or 256 bits. AES uses 128-bit blocks and is efficient in both software and hardware. A block cipher is a box which encrypts block, which is a 128-bit chunk of data. When AES encrypt a data which may be longer than 128 bits, the data is divided into blocks, and the method used for making the split is called the mode of operation. The native mode (simple split) is called ECB.

3. Case Study – AES

The AES is a standard symmetric encryption algorithm, which accepts the keys 128, 192, 256 bits, with 128 bits of blocks. The AES is used for protecting the electronic data. The AES is advantageous in both the hardware & software.

The “BLOCK” is the 128 bit chunks of the data with AES and a block cipher is a box which encrypts “blocks”. When the more than 128 bits message is encrypted, it is split into blocks, and the way in which

splitting is done is called mode of operation and simply split message is called ECB.
The AES is a symmetric block cipher. In this same key is used for encrypting and decrypting the data. AES uses the round operations where four transformations are used in the round operations for generating the cipher text from the plain text substituting bytes, shifting rows, mixing columns and adding the round keys [5].

4. Overview of the design

In the standard AES algorithm there are four steps as written above in the normal rounds. It works on 128 bits of cipher text. There are ten rounds except for the last consisting of four steps. The 128 bit input is divided into 16 bytes of 8 bits. Matrix of 4 X 4 is arranged for this. The 'Confusion' and 'diffusion' design method is used for first three functions of the AES rounds. The encryption is done by the fourth function. The concept of the confusion and diffusion is by Claude Shannon in his paper 'Communication theory of secrecy systems.' The plain text patterns are distributed in the cipher text is called diffusion and the relation between the plain text and cipher text is not easily understood is called as confusion.

The AES is associated with 'the state 'that is 'Intermediate cipher'. AES divides the 128 bit plain text to the 16 bytes blocks that are 128 bits. These 16 bytes are arranged in to 4 X 4 matrix or state array. Then it performs four operations, in each of the round [13].

1) Sub bytes: It gives confusion by processing each byte through an S-box. The S-box is a substitution table; using this table one byte is substituted by another byte.
2) Shift rows: The diffusion is added by shift row step. In this mixing of the data within rows is done as shown below. Row 3, row 2, row 1, row 0 are shifted by 3 bytes, 2 bytes, 1 byte and zero or no shift respectively.
3) Mix columns: It mixes the data within the columns and provides the diffusion. By the finite field mathematics 4 byte numbers are transformed to another 4 byte number.
4) Add row key: Within this step, the actual encryption is done. In this step each byte in the state is XORed with the subkey. The 'key expansion' design gives the sub keys [3].

AES Decryption: The functions used for decryption of the data are add round key, and the inverse key function, Inverse shift rows, Inverse subbytes and Inverse Mix Columns.

The Add round key function only XOR's the state with the subkeys. It doesn't require any inverse function. It encrypts when it is applied one time and decrypts when applied again [3].

5. Experimental design

For this experiment, the Intel (R) ™ i3-2350M CPU @ 2.30 GHz processor was used. The file sizes varying from 355KB to 7.14 MB were encrypted by the CPU. The time taken for converting the plain text to cipher text is the Encryption time. This time is used to calculate the encryption throughput; this is nothing but the speed of the encryption [1].

The encrypted blocks per cycle = Throughput.

Throughput = clock frequency * 128 bits.

The high load on the CPU is considered as the more CPU time required for the encryption. The clock cycles of the CPU are showing the energy consumption of the CPU i.e. energy consumed per cycle [2].

A comparison between algorithms is discussed for different input block sizes, considering their encryption time. Also the throughputs with different packet sizes are discussed. As shown in the table below AES has high throughput as compared with 3DES, DES, RC2 etc. The average time required for the encryption & decryption with the different packet sizes is compared. From this, it is seen that AES is better than other algorithms (3DES, DES, RC2). Then per slice throughput is calculated [1].

No. of CLB slices used = Throughput per slice.

A study of power consumption for the different key sizes for the AES is discussed. As discussed above the AES gives high throughput with minimum encryption time [3].

6. Hardware implementation of AES

For the implementation of AES, Reconfigurable Hardware is used. The coding of the architecture is done in the VHDL language. The architecture is implemented on the FPGA board of the device family SPARTAN –III.

Device family – SPARTAN – III

Tools used – XILINX ISE 9.1i

Device XC3S400-4PQ208

Board - SPARTAN-III DSP proto board (Model-MXS3FK-004-DSP)

The AES of 128 bit length is used also key of 128 bits is used. The control signals are INVERSE IN, LOAD IN, RST IN, START IN, UNLOAD IN and BUSY OUT. The input data is processed using the key and the cipher text or the plain text is available on DATA OUT terminal. The module of key expansion is the same for encryption & decryption [14].

7. Synthesis results

Table 1. Device utilization summary

Devices used	Usage of devices	Percentage
Number of Slices	458 out of 4656	9
Number of Slice Flip Flops	192 out of 9312	2
Number of 4 input LUTs	851 out of 9312	9
Number used as logic	803	-
Number used as Shift registers	48	-
Number of IOs	31	-
Number of bonded IOBs	30 out of 158	18
Number of GCLKs	1 out of 24	4

7.1 Timing Summary

Speed Grade: -5
Minimum period: 9.659ns (Maximum Frequency: 103.535MHz)
Minimum input arrival time before clock: 6.949ns
Maximum output required time after clock: 6.458ns
Timing constraint: Default period analysis for Clock 'clk'

Clock period: 9.659ns (frequency: 103.535MHz)

Total number of paths / destination ports: 119547 / 408

Delay: 9.659ns

7.2 Design Summary:

T1 Project Status

Project File:	t1.ise	Current State:	Placed and Routed
Module Name:	aes	• Errors:	No Errors
Target Device:	xc3s500e-5pq208	• Warnings:	12 Warnings (5 new, 0 filtered)
Product Version:	ISE 9.2i	• Updated:	Thu 18. Jul 22:09:58 2013

T1 Partition Summary

No partition information was found.

Device Utilization Summary

Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	176	9,312	1%	
Number of 4 input LUTs	802	9,312	8%	
Logic Distribution				
Number of occupied Slices	569	4,656	12%	
Number of Slices containing only related logic	569	569	100%	
Number of Slices containing unrelated logic	0	569	0%	
Total Number of 4 input LUTs	850	9,312	9%	
Number used as logic	802			
Number used as Shift registers	48			
Number of bonded IOBs	30	158	18%	
IOB Flip Flops	16			

Figure 1. Design summary

8. Simulation results

The translate, map and place and route of the code is done on XILINX-project Navigator, ISE9.1i. In the simulation result it is seen that all the 16 bytes of outputs are observed in terms of 8bits of chunks. We have forced MIT-COE as an input to the design.

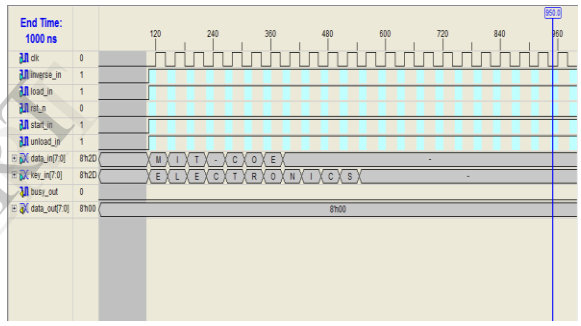

Figure 2. Input data and key given

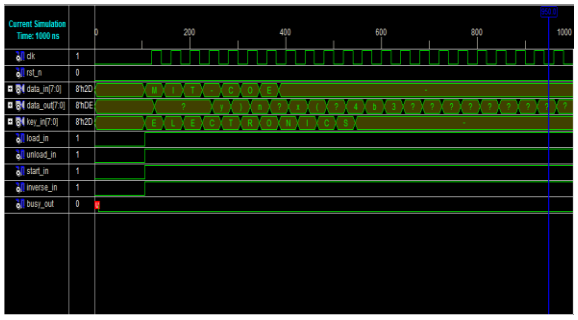

Figure 3. Output for given input

8.1 Inputs and outputs at various steps

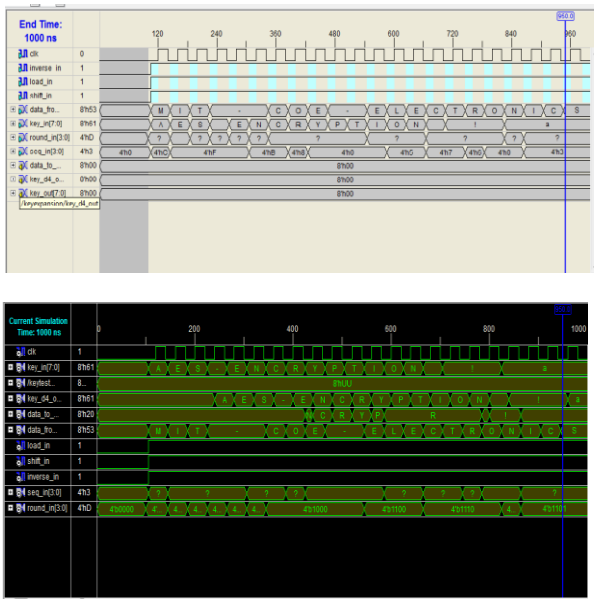

Figure 4. Key test-given input and simulation output

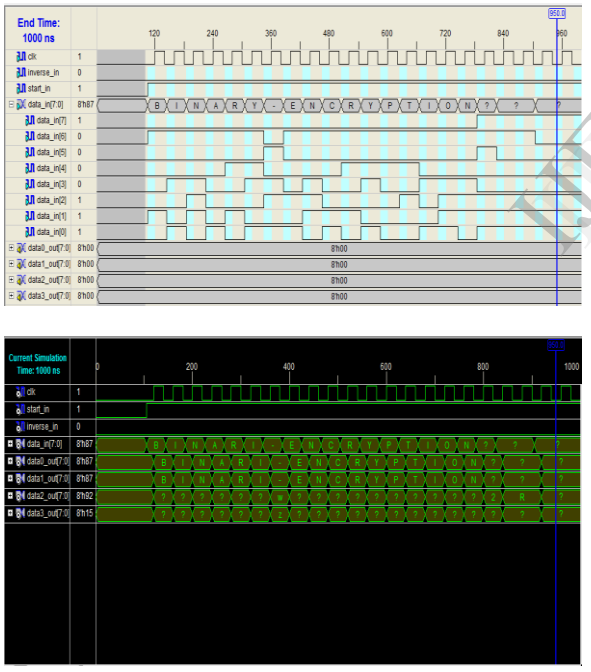

Figure 5. Mix columns test- given input and simulation output

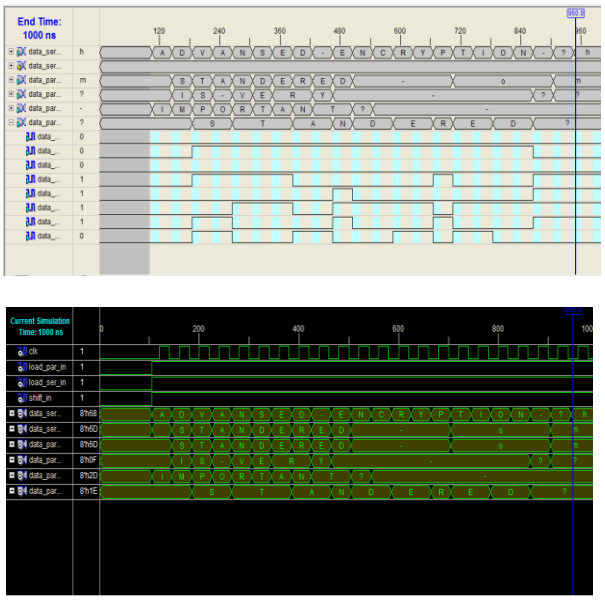

Figure 6. Byte permutation test- given input and simulated output

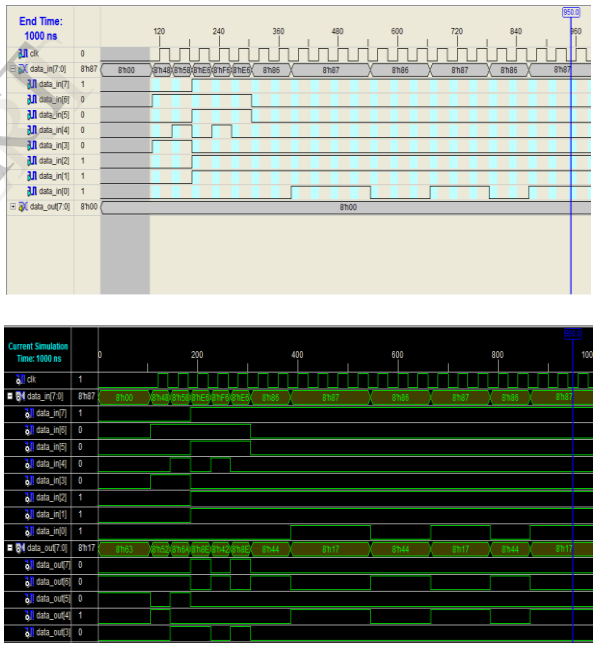

Figure 7. S1 box test- given input and simulated output

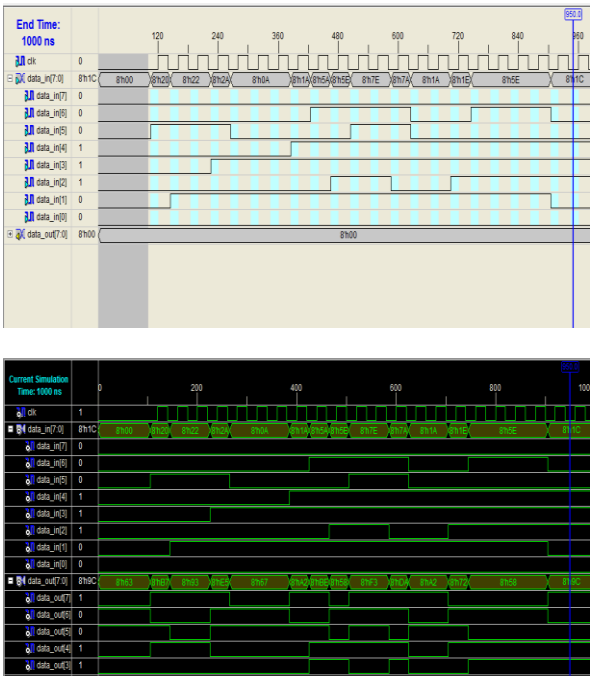

Figure 8. S2 box test- given input and simulated output

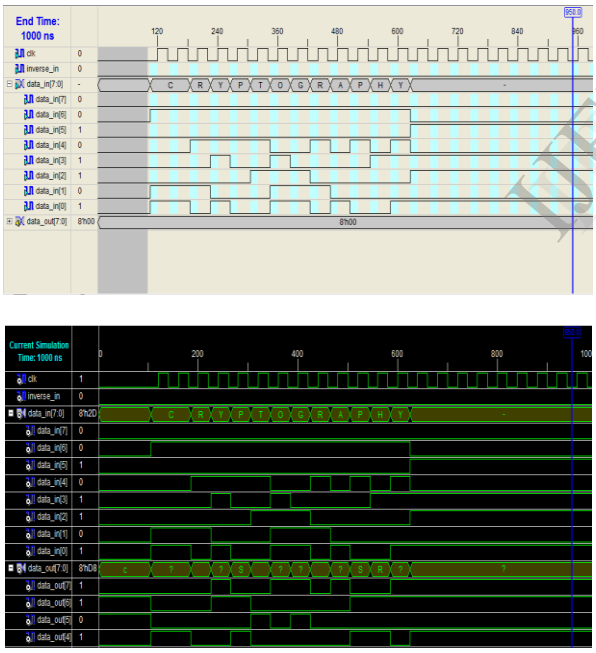

Figure 9. Sub byte test- given input and simulated output

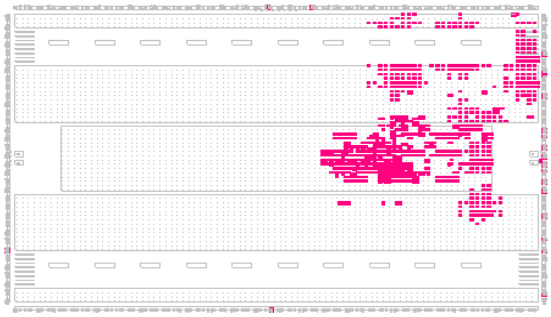

Figure 10. Floor plan of the design

9. Conclusion

The comparisons of Advanced Encryption Standard with the other standards are discussed. Also the importance of AES with the variety of input block sizes, their average encryption decryption time and throughput are discussed. Upon comparison it is determined that AES gives high throughput. AES is taken for case study. AES-128 is implemented on FPGA board. The synthesis and simulation results are shown.

10. References

[1] D. S. Abdul. Elminaam,"Performance Evaluation of Symmetric Encryption Algorithms", *Communications of the IBIMA* Volume 8, 2009 ISSN: 1943-7765 pp.58-63.

[2] Srinivasa Rao D,Sushma Rani N, Ch.Panchamukesh and S.Neelima "Analyzing The Superlative Symmetric Cryptographic Encryption Algorithm (ASCEA)", Journal of Global Research in Computer Science, Volume 2, No. 7,ISSN-2229-371X, July 2011 pp.101-105.

[3] 'Advanced Encryption Standard' Eric Conrad

[4] Vibha Verma, Mr. Avinash Dhole "Analysis of comparison between Single Encryption (Advance Encryption Scheme (AES)) and Multicrypt Encryption Scheme" International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153, pp.1-4

[5] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,pp. 137-139.

[6] P. Chodowiec and K.Gaj, "Very compact FPGA implementation of the AES algorithm." in CHES, ser. Lecture Notes in Computer Science, C. D.Walter, C¸ . K. Koc¸, and C. Paar, Eds., vol. 2779. Springer, 2003, pp.319–333.

[7] Daemen J. and Rijmen V. "The design of Rijndael: AES – The Advanced Encryption Standard," Springer-Verlag, ISBN 3-540-42580-2, 2002, pp. 1-45.

[8] T. Wollinger and C. Paar, , W. Rosenstiel and P. Lysaght, Eds., "Security aspects of FPGAs in cryptographic applications," in New Algorithms, Architectures, and

Applications for Reconfigurable Computing. Norwell, MA: Kluwer, 2004.
[9]W. Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .
[10] Wayne Wolf "FPGA-Based System Design" Prentice Hall, 2009
[11] Atul Kahate "Cryptography and network security", Tata McGraw-Hill, 2008
[12]http://csrc.nist.gov/publications/fips/fips463/flips463.pdf.
[13]http://wwwmath.ucdenver.edu/~wcherowi/courses/m540/des.pdf
[14]www.design-reuse.com/.../fpga-implementation-of-aes-encryption-and-d...
[15]https://users.cs.jmu.edu/.../TwofishEncryptionAlgorithm-by-Horatiu-P
[16]www.support.intel.com/support/performancetools
[17] www.chameleonsystems.com
[18]www.castinc.com/ipcores/encryption/aesp/index.html
[19]FIPS197.URL:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[20]AES Fact Sheet. URL: http://csrc.nist.gov/CryptoToolkit/aes/aesfact.htm