Performance Analysis of AES Cryptographic Algorithm

1Abhishek Kumar Sinha
4th Sem., M. Tech, Dept. of ECE
The Oxford College of Engineering
Bengaluru, India

2Jayaraj N
Asst. Prof, Dept. of ECE
The Oxford College of Engineering
Bengaluru, India

Abstract—Cryptographic algorithm are needed for network security. This paper presents the technique of Advanced Encryption Standard (AES) focuses on Confidentiality. AES algorithm uses Rijndael encryption and decryption process. Higher performance is achieved by throughput of 4.28 Gbps and maximum frequency of 334.5 Mhz. Simulation and Synthesis is done on Modelsim and Xilinx. The design is implemented on Xilinx-Virtex5 Field Programmable Gate Array (FPGA).

Keywords — AES, Confidentiality, Rijndael, Encryption, Decryption, Simulation, Performance, FPGA

I. INTRODUCTION

Cryptographic algorithms assure information protection across the network communication with high security. As the abundant information is increasing, there is a need for cryptographic algorithms. It protects from hackers, crackers and spying networks. The cryptographic algorithm satisfies security service such as confidentiality, authentication and availability. Confidentiality is defined as the denial of information disclosure to the unauthorized users. It emphasize on encryption. The example is Biometric. Authentication ensures genuine data with trust assurance of data. Example is fingerprint. Availability is the available of resource whenever it is in need. E-mail, E-commerce and internet transactions are the important applications of cryptography.

The process of transforming information into the secret information with the help of key is known as encryption which is available at transmitter. Encryption employs confidentiality. Transformation of secret data into original data with the help of key is decryption process which is available at receiver. Advanced Encryption Standard (AES) and RSA are several types of cryptographic encryption-decryption algorithms. Those are symmetric and asymmetric algorithm. RSA and AES algorithms are asymmetric and symmetric algorithm respectively. FIPS 197 (2002) gives specification on notations and convention, mathematical preliminaries, algorithmic specification and implementation issues of AES algorithm [4]. Xinmiao Zhang et al (2002) have presented various approaches in AES for efficient hardware implementation. Two classes are categorized for optimization methods which are architectural optimization and algorithmic optimization. In architectural optimization, the strength of pipelining, loop unrolling and sub-pipelining are exploited. Loop unrolling architecture can achieve a slight speedup with significantly increased area. Resource sharing issues are discussed for both encryptor and decryptor are needed to be implemented in small area [3]. Abhijith.P.S (2013) have presented and proposed a different approach to increase speed by utilizing lesser resources by mapping all four Logical functions of AES to LUTs, ROMs and Block RAMs available in FPGA which serves as the best high speed encryption algorithm with less area utilization and can be embedded with other larger designs as well [1].

Hardware implementation provides better security. Reconfigurable devices such as FPGAs are preferred over Application Specific Integrated Circuits (ASICs) due to the properties such as low cost, high performance, reprogramming and experiment testing.

This paper presents AES algorithm using a proposed system which provides information confidentiality for high security. This algorithm coding is written in Verilog whereas ModelSim is used for simulation, Xilinx is used for synthesis and implementation is done on Virtex-5 FPGA. The proposed system is applicable in VISA, secured cloud computing and cryptographic protocols.

This paper consists of various sections which are as follows: Section 2 discusses theory; Section 3 deals with proposed system. Simulation result is given in Section 4. Application and conclusion are provided in Section 5 and Section 6.

II. THEORY

AES algorithm was introduced by National Institute of Standards and Technology (NIST) as standard electronic protection describes about encryption and decryption processing and its specification is given in Federal Information Processing Standards (FIPS 197). Joan Daemen and Vincent Rijmen have founded the AES algorithm which uses Rijndael technique in the purpose of hiding and displaying the message. Fig. 1 shows 128 bit of input message with 128 bit of key giving 128 bit of output message.

![AES encryption/decryption process](image)

Fig. 1. AES encryption/decryption process

Four operations for Rijndael encryption/decryption process are as follows:
III. PROPOSED SYSTEM

A method for AES algorithm having minimal resources is employed. Here the block diagram and algorithm are described.

A. Block diagram

![AES cryptographic system](image1)

Fig. 2. AES cryptographic system

The proposed system consists of encryptor, decryptor, secret key and xor logic at transmitter section and receiver section over a network channel as shown in Fig. 2. At transmitter section, user 1 sends a message in the form of cipher by encryption across the channel to the receiver section. User 2 receives the original message by decrypting the cipher into inverse cipher. The secret key is used in the system. The message across the channel is accessible to user 2.

B. Algorithm

- Initialize the input message.
- Applying AES encryption algorithm to the input message.
- Encrypted message is passed through a medium known as channel.
- Retrieval of original message is obtained by AES decryption algorithm.

C. AES Encryption Algorithm

- 128-bit input message and 128-bit key \((k_{0,e})\) is added.
- The four operations from s-box, shift rows, mix columns and add round key is performed in sequential way.
- Repeat for 10 rounds. At last round mix columns operation is not performed.
- 128-bit cipher or encrypted message is obtained at last round i.e. 10th round.

D. AES Decryption Algorithm

- 128-bit cipher and 128-bit of key \((k_{0,d})\) is added
- The four operations from inverse shift rows, inverse s-box, inverse mix columns and inverse add round key is performed in sequential way.
- Key schedule from \(k_{10,e} = k_{0,d} \ldots k_{0,e} = k_{10,d}\). Repeat for 10 rounds. At last round mix columns operation is not performed.
- 128-bit inverse cipher or initial message is obtained at last round i.e. 10th round.

IV. SIMULATION RESULT

The simulation of Verilog code for AES encryption and decryption is obtained on ModelSim 6.3. The synthesis is done on Xilinx 12.2. Virtex-5 FPGA is used for implementation. AES encryption and decryption simulation result is shown in Fig. 3. Fig. 4 presents the Technology Schematic for AES proposed system.
Table I presents the device utilization summary for 5vlx110ff1136-

**TABLE I.** SLICE LOGIC UTILIZATION

<table>
<thead>
<tr>
<th></th>
<th>Number of Slice Registers</th>
<th>128 out of 69120</th>
<th>1%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of slice LUTs</td>
<td>1028 out of 69120</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>Number used as logic</td>
<td>1028 out of 69120</td>
<td>1%</td>
</tr>
</tbody>
</table>

In the proposed design encryption and decryption unit takes 10 clock cycles for completion. The maximum path delay for the design is 2.99ns and generating 334.45 MHz of maximum frequency. The throughput of encryption and decryption section is 4.28 Gbps which is given by Equation 3.

\[
\text{Throughput} = \frac{b_l(128) \times f_M(334.45)}{c_O(10)}
\]  

Here \(b_l\) represents number of input bits, \(f_M\) gives maximum clock frequency and \(c_O\) indicates number of cycles per output. Table II presents the comparison result with other reference for different AES architecture.

**TABLE II.** COMPARISON

<table>
<thead>
<tr>
<th>Design</th>
<th>Delay (ns)</th>
<th>Max. frequency (MHz)</th>
<th>Throughput (Gbps)</th>
<th>Regs</th>
<th>LUTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Design</td>
<td>2.99</td>
<td>334.45</td>
<td>4.28</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Abhijith.P.S[1]</td>
<td>3.42</td>
<td>292.40</td>
<td>3.74</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>M. Goswami[2]</td>
<td>4.25</td>
<td>235.29</td>
<td>2.73</td>
<td>1%</td>
<td>.7%</td>
</tr>
<tr>
<td>W. Wei, C.jie[5]</td>
<td>4.97</td>
<td>201.2</td>
<td>2.57</td>
<td>Not Available</td>
<td></td>
</tr>
</tbody>
</table>

**VI. CONCLUSION**

In this paper the proposed system uses integration of AES which ensures confidentiality across the network and it is implemented on Virtex5 FPGA. The obtained simulation suggests the system maintains confidentiality. The throughput computed is 4.28 Gbps with optimized area resulted in high performance. It can be further used in HTML 6.

**ACKNOWLEDGEMENT**

I would like to thank my guide Jayaraj N of The Oxford College of Engineering Bangalore for supporting the study.

**REFERENCES**


