A Project Report on

Advanced Encryption Standard Implemented on FPGA

Submitted in the Partial Fulfillment of the Requirements
For the Award of

Bachelor of Technology
in
Electronics & Communication Engineering

By

Himanshu Kumar

Kritika Kirthalaya

Rohit Prakash

Under the guidance of

Dr. Shweta Tripathi

Assistant Professor

Department of Electronics & Communication Engineering

Motilal Nehru National Institute of Technology Allahabad

Allahabad –211004, India

Department of Electronics & Communication Engineering

Motilal Nehru National Institute of Technology Allahabad

Allahabad –211004, India

CERTIFICATE

This is to certify that the work contained in the thesis titled **"Advanced Encryption Standard Implemented on FPGA"** submitted by **Himanshu Kumar(20105014),Kritika Kirthalaya(20105013)** and **Rohit Prakash(20105022)** in the partial fulfillment of the requirement for the award of Bachelor of Technology in Electronics and Communication Engineering to the Electronics and Communication Engineering Department, Motilal Nehru National Institute of Technology, Allahabad, is a bonafide work of the students carried out under my supervision.

Date:

Place:

Dr. Shewta Tripathi

Assistant Professor

ECE Department

MNNIT, Allahabad

Acknowledgement

It is a great privilege for us to express our deep sense of gratitude to our guide, Assistant Professor Dr. Shweta Tripathi of Electronics and Communication Engineering Department, MNNIT for her stimulating guidance and profound assistance .We shall always cherish our association with her for her constant encouragement and freedom to thought and action that she rendered to us throughout the project.

We also feel a great pleasure to thank all the staff members of the department for their cooperation which led to the successful completion of our project work.

Finally, we deem it a great pleasure to thank one and all whose valuable suggestion and in time cooperation helped us to carry out this project successfully.

We are also thankful to our friends and colleagues for their support.

Abstract

AES is the new encryption standard. In this project, we implement a very efficient pipelined hardware implementation of AES-128 cipher. It has a throughput of more than 500Mega bit per second. Besides, improving the encryption throughput, the pipeline can be taken advantage of if the number of rounds (currently 10) must increase for security reasons.

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

List of Figures

- Fig. 2.1 State array input and output…….4
- Fig. 2.2 Matrix for subbyte……6
- Fig. 2.3 S-BOX…….…….6
- Fig. 2.4 Shift rows…….…….8
- Fig. 2.5 Mix Column operates on the State……...9
- Fig. 2.6 InvshiftRows cyclically shifts…….……12
- Fig. 2.7 Matrix Multiplication…….……..13
- Fig. 2.8 Equation for InvMix Column……..14
- Fig. 3.1 Basic component in Mix Columns component…….17
- Fig. 3.2 Architecture of the multicomponent……....17
- Fig. 3.3 Description of operation xtime…….....18
- Fig. 3.4 2 stage pipelined AES 128 bit cipher block diagram…..……...….19
- Fig. 3.5 2 stage pipelined AES 128 bit inverse cipher…….…..18
- Fig. 3.6 Block Diagram for key expansion routine……19
- Fig. 3.7 Block Diagram for inverse key expansion……..……..19

List of Tables

- Table 2.1 S-BOX…….…7
- Table 2.2 Inverse S-BOX……12

Table of Content

Certificate ii
Acknowledgement iii
Abstract iv
List of Figures v

Chapter 1: Introduction

1.1: Introduction ……1

1.2: Need for Data Encryption……...…...2

Chapter 2: AES Encryption Algorithm

2.1: The state Representation…….....3

2.2: The Cipher…….……4

2.3: Inverse Cipher……..……10

Chapter 3: Implementation Issues

3.1: Architecture of Basic Components……...14

3.2: Pipelining…….….17

3.3: Key Expansion and Invkey Expansion…….18

3.4: Memory and input output…….19

3.5: Key Length Requirement……..20

Chapter 4: Conclusion

4.1: Conclusion……..……...21

4.2: Future scope……..…….....22

Appendix A: Cipher key Examples.....23

Appendix 2: Interfacing….…….28

References…….32