DEVELOPMENT OF INTERFACING CIRCUIT FOR TRIPLE DATA ENCRYPTION STANDARD (3DES) USING VERILOG FOR FPGA IMPLEMENTATION

Industrial Project Thesis is presented in partial fulfillment for the award of the Bachelor of the Electrical Engineering (Honors)
UNIVERSITI TEKNOLOGI MARA

NOR AIZEE MASYITAH BINTI KAMAL BAHRIN
UNIVERSITI TEKNOLOGI MARA
Faculty of Electrical Engineering
40450 Shah Alam, Selangor

ACKNOWLEDGEMENT

First and foremost, I would like to thank The Almighty Allah s.w.t. If it were not for his blessing, I would never have the chance to complete this project.

I would also like to express my deepest appreciation to my ever supportive supervisor, Assoc. Prof. Zulkifli Abd. Majid for his suggestion, moral support and patience throughout of this project. His advices and comments were indeed significant.

I would also like to thank Mr. Azman Baharom, Mr. Farid Zainal Abidin and Mr. Mohd Rezal Md. Amin from SyMMid for their invaluable guidance and help. My next gratitude would go to Selangor Human Resource Development Centre (SHRDC) for providing the facilities and for my team project for their strong support and commitment to complete this project successfully.

I would also like to express my utmost gratitude to all who have been involved directly or indirectly. I would also like to expand my thanks to my beloved parents and family for their moral support throughout my project.

May Almighty Allah s.w.t bless and reward all of them for their generosity.

ABSTRACT

This report presents the development of interfacing circuit for Triple Data Encryption Standard (3DES) that is being designed using Verilog HDL for Field Programmable Gate Array (FPGA) implementation. The purpose of this project is to design the interfacing circuit that can minimize the input/output port pins of the 3DES from about 300 pins to 44 pins that is suited for standard packaging available in the market. The port pins allow the 3DES to communicate with outside world. Xilinx ISE™ 7.1i software is utilized to create Verilog HDL code and synthesize. The result of simulation was carrying out by ModelSim XE III 6.0a.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

This thesis presents a design of an interfacing circuit for Triple Data Encryption Standard (3DES). The task of this interfacing circuit is to reduce the input and output port pins of the 3DES from 298 pins to only 44 pins by using register as the main concept. All the circuit components were designed using Verilog HDL under Xilinx environment.

1.1.1 Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard or 3DES is a block cipher formed from the Data Encryption Standard (DES) cipher by running it three times. It is a cryptosystem which can carry encrypt or decrypt data using a single secret key [1]. Encryption is the process of converting data to a code called cipher [2]. This cipher code is a secret code that is impossible to read. Decryption is the reversed process of encryption where the cipher is coded back to the plaintext.

It is used in computer system or network to provide cryptographic protection or information security to binary coded data [3]. Banking system is one the most important user of 3DES for electronic financial transactions because of it security conscious application. There are a variety applications that used 3DES including secure communications, secure video surveillance systems and encrypted data storage [4].

The revolution of 3DES from DES is primarily due to DES key cracking in only 24 hours by someone with a special chip.