INTEGRATION AND SYNTHESIZE OF TRIPLE DES USING SYNOPSYS DESIGN COMPILER TARGETING FOR ASIC IMPLEMENTATION

NOORDALILA SYAIRAH BINTI OMAR

FACULTY OF ELECTRICAL ENGINEERING
UNIVERSITI TEKNOLOGI MARA
MALAYSIA

ACKNOWLEDGEMENT

In the name of ALLAH

Most Gracious Most Merciful

This project would not been possible without the help of a number of people, either directly or indirectly.

First, I would like to express my greatest appreciation to my project supervisor, Assoc. Prof. Zulkifli bin Abd. Majid for his continuous guidance and valuable opinions throughout my project.

Special thanks to Encik Azman Baharom, Encik Farid Zainal Abidin and Encik Mohd. Rezal Md. Amin from SyMMid Corporation for their assistance and willingness in sharing their knowledge in IC design as well as guiding us throughout this project and Management of SHRDC for their great helps, providing us tools and training courses to realize our project.

Finally, special thanks also go for my team project for their strong support and commitment to make this project successfully complete, my family, colleagues and others, either directly or indirectly for their help, inspiration and support throughout my studies in UiTM.

ABSTRACT

This paper presents a project that integrates and synthesize the Verilog Hardware Description Language (HDL) of the Triple Data Encryption System (DES) using Synopsys Design Compiler targeting for ASIC implementation using TSMC 0.25μm technology library. The target is to check on timing analysis whether it met the time constraints or not, and to find out the critical path that leads to the delay of the circuit, then a gate level netlist is generated as to proceed to the next step of the design flow which is the placement and routing, for further ASIC implementation.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

The Data Encryption Standard (DES) was developed by an IBM team around 1974 and adopted as the USA national standard in 1977. Triple DES (3DES) is a minor variation of this standard. It is three times slower than regular DES but can be billions of times more secure if used properly. Triple DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. Therefore, Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES [3].

DES is a block cipher. It acts on a fixed-length block of plaintext and converts it into a block of ciphertext of the same size by using the secret key. In DES, the block size for plaintext is 64 bits. The length of the key is also 64 bits but 8 bits are used for parity. Hence the effective key length is only 56 bits. In Triple DES, we apply three stages of DES with a seperate key for each stage. So the key length in Triple DES is 168 bits.

Encryption is the process of converting data to a secret code called cipher that is impossible to read without the appropriate knowledge and key. Triple DES is a cryptosystem which can encrypt and decrypt data using a single secret key [1]. Triple DES has three standard 56 bit keys and 64 bits of data as input and generates a 64 bit encrypted or decrypted result. Today, the standard packaging ports available in the market is not enough for Triple DES implementation.