TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
ALU	-	Arithmetic Logic Unit
ASIC	-	Application Specific Integrated Circuit
ASIP	-	Application Specific Instruction set Processor
CPU	-	Central Processing Unit
DLP	-	Discrete Logarithm Problem
DSA	-	Digital Signature Algorithm
ECC	-	Elliptic Curve Cryptography
EC-AES-		Elliptic Curve – Advance Encryption Standard
ECDLP-		Elliptic Curve Discrete Logarithm Problem
ECDSA-		Elliptic Curve Digital Signature Algorithm
ECDSC-		Elliptic Curve Digital Signature Cryptosystem
ECP	-	Elliptic Curve Processor Core
FPGA	-	Field Programmable Gate Array
GUI	-	Graphic User Interface
GPPs	-	General Purpose Processor
HDL	-	Hardware Description Language
I/O	-	Input/Output
IOWR	-	I/O Write
IORD	-	I/O Read
IDE	-	Integrated Development Environment
IC	-	Integrated Circuit
IFP	-	Integer Factorization Problem
IEEE	-	Institute of Electrical and Electronics Engineers
IP	-	Intellectual Property
JTAG	-	Joint Action Test Group
LC	-	Logic Cell

LCH	-	Loosely Coupled Hardware
LE	-	Logic Element
LSD	-	Least Significant Digit
LUT	-	Lookup Table
MAP	-	Modular Arithmetic Processor
MUX	-	Multiplexer
PIO	-	Parallel Input/Out
PKI	-	Public-Key Infrastructure
RAM	-	Random Access Memory
RSA	-	Rivest, Shamir, Adleman
RTL	-	Register-Transfer-Level
SDK	-	Software Development Kit
SHA-1	-	Secure Hash Algorithm
SoC	-	System-on-Chip
SOPC	-	System-on-a-Programmable-Chip
TCH	-	Tightly-Coupled Hardware
UART	-	Universal Asynchronous Receiver/Transmitter
UTM	-	Universiti Teknologi Malaysia
VHDL	-	Very High Speed Integrated Circuit Hardware Description Language

LIST OF APPENDICES