

## TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	<b>DECLARATION</b>	ii
	<b>DEDICATION</b>	iii
	<b>ACKNOWLEDGEMENTS</b>	iv
	<b>ABSTRACT</b>	v
	<b>ABSTRAK</b>	vi
	<b>TABLE OF CONTENTS</b>	vii
	<b>LIST OF TABLES</b>	xi
	<b>LIST OF FIGURES</b>	xiii
	<b>LIST OF ABBREVIATIONS</b>	xvii
	<b>LIST OF APPENDICES</b>	xix
<b>1</b>	<b>INTRODUCTION</b>	
	1.1 Background and Motivation	1
	1.2 Research Objectives	3
	1.3 Scope of Work	4
	1.4 Overview of Research Methodology	4
	1.5 Research Contribution	6
	1.6 Thesis Organization	6
<b>2</b>	<b>LITERATURE REVIEW AND BACKGROUND</b>	
	2.1 Previous Work	8
	2.2 Hardware Accelerator in Embedded System on Chip Design	12
	2.3 Tightly Coupled Hardware in Nios II Platform	14

<b>3</b>	<b>THEORY AND ALGORITHM ELLIPTIC CURVE CRYPTOGRAPHY</b>	
3.1	Cryptography in Data Security	19
3.2	Elliptic Curve Cryptography – An Introduction	20
3.3	Theory of Finite Fields	23
3.4	Finite Field Arithmetic	25
	3.4.1 Field Addition	26
	3.4.2 Field Multiplication	26
	3.4.3 Field Squaring	29
	3.4.4 Field Inversion	30
3.5	Elliptic Curve Arithmetic over $F_2^m$	33
3.6	Montgomery Point Multiplication in Projective Coordinate	36
3.7	Elliptic Curve Scheme	38
	3.7.1 ECDH Key Agreement Algorithm	38
	3.7.2 Elliptic Curve Digital Signature Algorithm (ECDSA)	40
	3.7.3 EC-AES Hybrid Encryption Algorithm	41
3.8	Summary	42
<b>4</b>	<b>DESIGN OF ECC HARDWARE ACCELERATOR</b>	
4.1	ECC Domain Parameter	43
4.2	ECC System Design Exploration	44
4.3	Design of ECC Processor	48
	4.3.1 ECC Field Arithmetic Level Coprorocessor (LC-F)	48
	4.3.2 ECC Point Arithmetic Level Coprorocessor (LC-P)	53
4.4	Design of ECC TC-hardware	55
	4.4.1 ECC Field Arithmetic Level TC- hardware (TC-F)	55
	4.4.2 ECC Point Arithmetic Level TC- hardware (TC-P)	60
4.5	Summary	62

<b>5</b>	<b>ECC BASED HYBRID ENCRYPTION AND DIGITAL SIGNATURE CRYPTOSYSTEMS</b>	
5.1	Elliptic Curve Cryptosystem Scheme	63
5.2	Embedded Software Development of ECHEDSC	66
5.3	Hardware Development of of ECC-based Security Scheme	68
5.3.1	Elliptic Curve Cryptography TC- Hardware Custom Instruction	69
5.3.2	SHA -1 Hash Function Coprocessor	71
5.3.3	Modular Arithmetic Processor (MAP)	75
5.3.4	AES	78
5.3.5	Pseudo Random Number Generator	81
5.4	Summary	82
<b>6</b>	<b>DESIGN VERIFICATION, TEST AND PERFORMANCE ANALYSIS</b>	
6.1	Tests Consideration	83
6.2	Test Verification of ECC Hardware Accelerator	84
6.2.1	Test Verification of ECC Field Arithmetic Level Hardware Accelerator	84
6.2.2	Test Verification of ECC Point Arithmetic Level Hardware Accelerator	86
6.3	Resource Utilization	88
6.4	ECC Hardware Performance	90
6.4.1	Performance in Field Arithmetic Level	91
6.4.2	Performance in Point Arithmetic Level	92
6.4.3	Performance Comparison of ECC Arithmetic Level	93
6.5	Benchmarking	94
6.6	Tests in Elliptic Curve Cryptosystem	95
6.6.1	SHA-1 Verification Test	95
6.6.2	AES-256 Verification Test	96

6.6.3	MAP-233 Verification Test	96
6.7	ECDSA and ECAES-Hybrid Encryption Test	97
6.7.1	ECDSA Verification Test	98
6.7.2	EC-AES Hybrid Encryption Verification Test	101
6.7.3	Timing Performance	103
6.8	Tests in Demonstration Application Prototype	104
6.8.1	Demonstration Application System View	104
6.8.2	e-Cheque GUI Application Test	105
6.10	Summary	107
<b>7</b>	<b>CONCLUSIONS</b>	
7.1	Concluding Remarks	108
7.2	Future Work	110
	<b>REFERENCES</b>	111
	Appendices A – E	117 - 141

## LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Custom Instruction Types, Application and Hardware Ports (Altera,2008)	16
3.1	ECC and RSA comparison	22
4.1	Types of ECC hardware	47
4.2	Field multiplier coprocessor instruction	51
4.3	Field squarer coprocessor instruction custom instruction	53
4.4	Field multiplier TC-hardware custom instruction	58
4.5	Field squarer TC-hardware custom instruction	59
5.1	Instruction Format of 233-bit ECC TC-Hardware Custom Instruction	70
5.2	Instruction Format of SHA-1	73
5.3	Instruction Format of MAP	76
5.4	Instruction Format of AES	80
6.1	Resources Utilization for Field Multiplier	89
6.2	Resources Utilization for Field Squarer	89
6.3	Resources Utilization for Point Arithmetic Level	89
6.4	Resources Utilization for Point and Field Arithmetic Level	90
6.5	Execution times of 163-bit ECC field arithmetic level	91
6.6	Execution times of 193-bit ECC field arithmetic level	91

6.7	Execution times of 233-bit ECC field arithmetic level	91
6.8	Execution times of 163-bit ECC point arithmetic level	92
6.9	Execution times of 193-bit ECC point arithmetic level	92
6.10	Execution times of 233-bit ECC point arithmetic level	92
6.11	Execution times of Point Multiplication operation for TC-hardware architecture in Point and Field Arithmetic Level	93
6.12	Execution times of Point Addition operation for TC-hardware architecture in Point and Field Arithmetic Level	93
6.13	Benchmarking result with other existing ECC TC-H implementations	94
6.14	Resource Utilization of Each Module in EC-Based Cryptosystems	98
6.15	Timing Performance of 233-bit EC-based Embedded Crypto system	103
7.1	Specifications of the ECC Tightly Coupled Hardware with Custom Instruction	109

## LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	System Design Flow	5
2.1	Nios II TC-hardware custom instruction	11
2.2	Hardware/Software coprocessor system bus communication	13
2.3	Tightly Coupled hardware and Coprocessor architecture	13
2.4	Architecture of Nios II processor (Altera, 2008)	14
2.5	Block Diagram of a Nios II Custom Instruction Logic (Altera, 2008)	15
2.6	Extended Custom Instruction with Swap Operations	17
3.1	Design Hierarchy of Elliptic Curve Cryptography	22
3.2	Geometric Description of Point Addition (a) and Point Doubling (b) on Elliptic Curve	34
4.1	Hierarchy of ECC	44
4.2	Hardware/Software partitioning in field arithmetic level	45
4.3	Hardware/Software partitioning in point arithmetic level	45
4.4	(a) ECC coprocessor architecture. (b) ECC TC-hardware architecture.	46
4.5	(a) Coprocessor interface and (b) TC-hardware interface	46
4.6	Functional diagram of ECC with field arithmetic coprocessor	48
4.7	Field multiplier coprocessor architecture (LC-F)	49
4.8	Behavioral flow chart of field multiplier coprocessor	50

4.9	Macro C of field multiplier coprocessor	50
4.10	Field squarer coprocessor hardware architecture (LC-F)	51
4.11	Behavioral flow chart of field squarer coprocessor	52
4.12	Macro C of field squarer coprocessor	52
4.13	ECC point arithmetic TC-hardware custom instruction	53
4.14	ECC coprocessor hardware architecture	54
4.15	Flow chart of Write read and Fetch operation	54
4.16	Read/Write operation in ECC coprocessor	55
4.17	The functional diagram of field arithmetic TC-hardware architecture	56
4.18	The Field multiplier TC-hardware architecture (TCF)	56
4.19	Behavioral flow chart of field multiplier TC-hardware	57
4.20	Macro C of field multiplier custom instruction	57
4.21	Field squarer TC-hardware architecture (TC-F)	58
4.22	Behavioral Flow Chart of Field Squarer TC-hardware	59
4.23	Macro C of field squarer custom instruction	59
4.24	The behavioral flowchart of ECC point arithmetic operation	60
4.25	ECC point arithmetic TC-hardware custom instruction	61
4.26	ECC TC-hardware architecture (TC-P)	61
4.27	Flow chart of Write read and Fetch operation in TC-hardware	62
4.28	Read/Write operation	62
5.1	ECC-based Security Scheme	64
5.2	ECDSA Scheme	64
5.3	EC-AES Scheme	65
5.4	Top-level Block Diagram of the Hardware Evaluation System	65



5.5	Software functional architecture of ECC-based Security Scheme	66
5.6	ECDSA and ECAES Software functional architecture of embedded device driver	68
5.7	233-bit ECC-TC-hardware custom instruction functional diagram	69
5.8	Behavioral flowchart of ECC	69
5.9	233-bit ECC TC-Hardware Custom Instruction (TC-P)	70
5.10	ECC Status word format	70
5.11	Functional diagram of ECC-TC Hardware device driver	71
5.12	Functional block diagram of SHA-1 LC-hardware coprocessor	72
5.13	Behavioral flowchart of SHA-1	72
5.14	SHA-1 Control Word Format	73
5.15	SHA-1 Signal Word Format	74
5.16	SHA-1 Device Driver Hierarchy	74
5.17	Functional Block Diagram of MAP 233 LC-hardware Coprocessor	75
5.18	Behavioral Flowchart of MAP 233 LC-hardware Coprocessor	76
5.19	MAP Control Word Format	77
5.20	MAP Status word format	77
5.21	Structural hierarchy of the MAP 233 device driver	78
5.22	Functional block diagram of AES LC-hardware Coprocessor	79
5.23	Flowchart of the AES coprocessor	79
5.24	AES control word format	80
5.25	AES Status word format	81
5.26	The hierarchy of AES device driver	81
5.27	Functional Diagram of PRNG233	82

6.1	ECDH Key Agreement test verification of 163-bit Field Multiplier and Field Squarer	84
6.2	An ECDH Key Agreement test verification of 193-bit Field Multiplier and Field Squarer	85
6.3	An ECDH Key Agreement test verification of 233-bit Field Multiplier and Field Squarer	86
6.4	An ECDH Key Agreement test verification of 233-bit ECC point arithmetic level hardware accelerator	87
6.5	An ECDH Key Agreement test verification of 233-bit ECC point arithmetic level hardware accelerator	88
6.6	SHA-1 Hardware Test Output on Nios II EDS Terminal Window	95
6.7	AES-256 Hardware Test Output on Nios II EDS	96
6.8	MAP 233 Hardware Test Output on Nios II EDS Terminal Windows	97
6.9	ECDSA Key Pair Generation	99
6.10	ECDSA Signature Generation	100
6.11	ECDSA Verification Generation	101
6.12	EC-AES Encryption Generation	102
6.13	EC-AES Decryption Generation	103
6.14	Demonstration Application Prototypes – System View	104
6.15	e-Cheque Format in Application Demonstration Prototype	105
6.16	Main GUI of e-Cheque Application (signing and encrypting)	106
6.17	Main GUI of e-Cheque Application (decrypting and verifying)	107

## 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**

<b>APPENDIX</b>	<b>TITLE</b>	<b>PAGE</b>
A	Recommended ECC Domain Parameter and Functional Blok Diagram of ECC core	117
B	Point Multiplication and Point Addition Implementation in Finite Field Arithmetic	124
C	Verilog and VHDL Code for Field Arithmetic Level and Point Arithmetic Level Hardware Accelerator	127
D	Test Vector	135
E	Publication	139