TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	iii
	LIST OF TABLES	xiiv
	LIST OF FIGURES	xv
	LIST OF SYMBOLS AND ABBREVIATIONS	xvii
1	**INTRODUCTION**	1
	1.1 GENERAL	1
	1.2 ENCRYPTION AND SECRECY	2
	1.3 OBJECTIVES OF CRYPTOGRAPHY	3
	1.4 CRYPTOGRAPHIC PROTOCOLS	4
	1.5 EVALUATING THE SECURITY OF A CRYPTOSYSTEM	5
	1.5.1 Computational Security	5
	1.5.2 Provable Security	5
	1.5.3 Unconditional Security	6
	1.6 DIGITAL SIGNATUARE SCHEMES	6
	1.7 DIGITAL CERTIFICATES	8
	1.8 ELLIPTIC CURVES	10
	1.8.1 Elliptic Curve Groups over Real Numbers	10
	1.8.2 Elliptic Curve Addition	11
	1.8.2.1 Adding two distinct points	12
	1.8.2.2 Adding the point P and –P	13

CHAPTER NO. **TITLE** **PAGE NO.**

1.8.2.3 Doubling the point P 13

1.9 MATHEMATICAL HARD PROBLEMS 15

1.9.1 Discrete Logarithm Problem 15

1.9.2 Elliptic Curve Discrete Logarithm Problem 17

1.9.3 Decision Diffie-Hellman Problem 17

1.9.4 Computational Diffie-Hellman Problem 17

1.9.5 Gap Diffie-Hellman Problem 17

1.10 LITERATURE SURVEY 17

1.11 OBJECTIVES OF THE WORK 23

1.12 THESIS ORGANIZATION 24

2 PROXY BLIND DISTRIBUTED DIGITAL SIGNATURE SCHEME 27

2.1 INTRODUCTION 27

2.2 MATHEMATICAL MODEL 29

2.3 DISTRIBUTION OF SECRET SHARES TO THE GROUP OF PROXY SERVERS BY B 31

2.3.1 Shamir's Secret Sharing Scheme 31

2.4 VERIFICATION FOR THE VALID SHARES BY THE INDIVIDUAL PROXY SERVERS 32

2.4.1 Feldman's Verifiable Secret Sharing Scheme 33

2.4.2 Generalization of Verifiable Secret Sharing Scheme 34

2.5 JOINT GENERATION OF KEYS BY THE GROUP OF SERVERS 35

CHAPTER NO.	TITLE	PAGE NO.
	2.6 GENERATION OF PROXY KEYS (PUBLIC KEY, SECRET KEY) BY B	36
	2.7 SIGNATURE GENERATION BY B	37
	2.8 SIGNATURE VERIFICATION BY C	38
	2.9 SECURITY ANALYSIS	39
	2.10 NUMERICAL RESULTS	41
	2.11 PERFORMANCE EVALUATION	42
	2.12 INFERENCE AND CONCLUSION	44
3	**IDENTITY BASED – PROXY BLIND DISTRIBUTED SIGNATURE SCHEME**	47
	3.1 INTRODUCTION	47
	3.2 BILINEAR PAIRINGS	49
	3.3 IDENTITY BASED SIGNATURE SCHEME	50
	3.4 MATHEMATICAL MODEL	52
	3.5 DISTRIBUTION AND RECONSTRUCTION OF SECRETS USING ELLIPTIC CURVES	53
	3.6 PRIVATE KEY SHARE DISTRIBUTIONS AND VERIFICATION FOR THE VALID SHARES BY THE INDIVIDUAL PROXY SERVERS	54
	3.7 JOINT GENERATION OF KEYS BY THE GROUP OF SERVERS	55
	3.8 COMMON PARAMETER GENERATION ALGORITHM	55
	3.9 PRIVATE KEY EXTRACTION ALGORITHM	56
	3.10 DISTRIBUTED SIGNATURE GENERATION ALGORITHM	56

CHAPTER NO.		TITLE	PAGE NO.
	3.11	VERIFICATION ALGORITHM	58
	3.12	SECURITY ANALYSIS	60
	3.13	NUMERICAL RESULTS	63
	3.14	PERFORMANCE EVALUATION	64
	3.15	INFERENCE AND CONCLUSION	66
4		**VERIFIABLE ENCRYPTION OF DIGITAL SIGNATURES**	68
	4.1	INTRODUCTION	68
	4.2	PROBLEM DEFINITION	69
	4.3	SOLUTION FOR CONTRACT SIGNING PROBLEM	71
	4.4	VERIFIABLE ENCRYPTION	72
	4.5	MATHEMATICAL MODEL	72
	4.6	ASSUMPTIONS FOR VERIFIABLE ECDSA SCHEME	74
	4.7	KEY GENERATION	74
	4.8	SIGNATURE GENERATION	75
	4.9	SIGNATURE VERIFICATION	76
	4.10	ECDSA INITIALIZATION	76
	4.11	PROTOCOL FOR OBTAINING SESSION KEY	77
	4.12	PROTOCOL FOR CONVINCING THE VERIFIER	78
	4.13	ARBITRATION BY TTP	80
	4.14	PERFORMANCE EVALUATION	81
	4.15	INFERENCE AND CONSLUSION	83

CHAPTER NO. TITLE PAGE NO.

5 THEFT-PROTECTED PROPRITARY CERTIFICATES 87

5.1 INTRODUCTION 87

5.2 PROPRIETARY CERTIFICATION PROCESS 89

5.3 ZERO-KNOWLEDGE PROOF SYSTEMS 91

5.3.1 Interactive Proof Systems 91

5.3.2 Interactive Proof Systems Requirements 92

5.4 CHAUM AND PEDERSEN SCHEME 93

5.5 MATHEMATICAL MODEL 94

5.6 VERIFIABLE ENCRYPTION SCHEME BASED ON ECDLP 95

5.6.1 Key Generation 95

5.6.2 Encryption Scheme 96

5.6.3 The Protocol 97

5.7 THEFT PROTECTED PROPRIETARY CERTIFICATES 99

5.7.1 Making Proprietary Certificate Theft Protected 100

5.8 COMPARISON BETWEEN ECDLP AND DLP 102

5.9 NUMERICAL EXAMPLE 102

5.10 PERFORMANCE EVALUATION 104

5.11 INFERENCE AND CONCLUSION 106

6 APPLICATIONS 109

6.1 INTRODUCTION 109

6.2 APPLICATION TO ELECTRONIC VOTING 109

CHAPTER NO.	TITLE	PAGE NO.
	6.3 APPLICATION TO HEALTH CARE INSURANCE SERVICE MANAGEMENT SYSTEM	111
	6.3.1 Claim Module	113
7	**CONCLUSION**	116
	REFERENCES	118
	LIST OF PUBLICATIONS	127
	VITAE	128

LIST OF TABLES

TABLE NO.	TITLE	PAGE NO.
1.1	Predicted sizes of problems that can be solved using the index calculus method	16
2.1	Shares distributed to each servers	41
2.2	Verification of secret shares	42
2.3	Performance evaluation of the proposed scheme	43
2.4	Comparison of time needed	44
3.1	Performance evaluation of the proposed scheme	65
3.2	Comparison of time needed	65
4.1	Performance evaluation of the proposed scheme	82
4.2	Comparison of time needed	82
5.1	Elliptic curve point set elements for $y^2 = x^3 - 10x - 8 (\mathrm{mod}\, 11)$	103
5.2	Repeated doubling of the point $B = (10,10)$	103
5.3	Numerical values for the variables in encryption scheme	103
5.4	Numerical values for the variables in protocol	104
5.5	Performance evaluation of the proposed scheme	105
5.6	Comparison of time needed	105

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
1.1	Graph of the elliptic curve $y^2 = x^3 - 4x + 0.67$	11
1.2	Elliptic curve point addition	12
1.3	Adding P and –P	13
1.4	Doubling the point P	14
1.5	Doubling the point P with 2P=o	15
2.1	Proxy blind distributed signature scheme	30
2.2	Comparison of the time needed for the proposed scheme with Schnorr's scheme	45
3.1	Comparison of the overall process with Zhang's scheme	66
4.1	Initialization phase	77
4.2	Overall verifiable encryption scheme	81
4.3	Key generation process	83
4.4	Signature generation process	84
4.5	Signature verification process	84
4.6	Alice's computation	85
4.7	Bob's computation	85
4.8	Comparison of security levels of ECC and RSA	86
5.1	Overview of issuing proprietary certificates	89
5.2	Verifiable encryption scheme for certification process	99

FIGURE NO.	TITLE	PAGE NO.
5.3	A new approach to avoid penalizing accidental sharing	101
5.4	Key generation process	106
5.5	Encryption process	107
5.6	Prover's computation	107
5.7	Verifier's computation	108
6.1	Proxy blind distributed signature scheme use in polling station based internet voting scheme	110
6.2	Identity based proxy blind distributed signature scheme fitted to health care insurance claim module	114

LIST OF SYMBOLS AND ABBREVIATIONS

SYMBOLS

$O(n)$	-	Big-O notation
cf	-	Cofactor, $cf = \#E / n$
$a \| b$	-	Concatenation of strings a and b
sk	-	Decryption key / Secret key
$Cert_A$	-	Digital certificate of the entity A
$Cert_{T:A}$	-	Digital certificate of the entity A issued by the entity T
E	-	Elliptic curve point set
pk	-	Encryption key/Public key
$E_k(m)$	-	Encryption of the message m using the key k
F_q	-	Finite field with q elements
g, h	-	Generators of the set Z_n^*
$H(.)$	-	Hash function $H : \{0,1\}^* \rightarrow Z_q^*$
$H_1(.)$	-	Hash function $H_1 : \{0,1\}^* \rightarrow E_l^*$
$\bar{x}$	-	Integer representation of the x-coordinates of $R(x, y)$
$H_{hk}(.)$	-	Keyed hash function that uses a key hk
L	-	Label, having bit string of arbitrary length
m	-	Message or Plaintext
$\#E$	-	Order of the set E
O	-	Point at infinity, which acts an indenity element in E
$G = (x_G, y_G)$	-	Point in E of prime order n
p^1, q^1, p, q	-	Prime numbers

Z_n^*	-	Prime residue class group modulo n, $Z_n^* := \{x \in Z_n \mid x$ is a unit in $Z_n\}$. An element which has a multiplicative inverse is called units.
$a \bmod n$	-	Remainder of a modulo n
$[a]$	-	Residue class of $a \bmod n$, $[a] := \{x \in Z \mid x \equiv a \bmod n\}$
Z_n	-	Residue class ring modulo n, $Z_n = \{[a] \mid a \in Z\} = \{0,1,2,..n-1\}$
$\{0,1\}^*$	-	Set of bit strings of arbitrary length
Z	-	Set of integers
$sign_{sk}(m)$	-	Signing function operated under the secret key sk
E_l^*	-	Subset of E having element of order l
$veri_{pk}(s,m)$	-	Verification function which use the private key pk

ABBREVIATIONS

AES	-	Advanced Encryption Standard
CA	-	Certificate Authority
CDHP	-	Computational Diffie-Hellman Problem
DDHP	-	Decision Diffie-Hellman Problem
DES	-	Data Encryption Standard
DLP	-	Discrete Logarithm Problem
DSA	-	Digital Signature Algorithm
ECC	-	Elliptic Curve Cryptosystem
ECDLP	-	Elliptic Curve Discrete Logarithm Problem
ECDSA	-	Elliptic Curve Digital Signature Algorithm
ECMQV	-	Elliptic Curve Menezes-Qu-Vanstone Protocol
IDEA	-	International Data Encryption Algorithm

KDF	-	Key Derivation Function
MAC	-	Message Authentication Code
PKI	-	Public Key Infrastructure
RSA	-	Rivest Shamir Adleman Algorithm
TTP	-	Trusted Third Party