



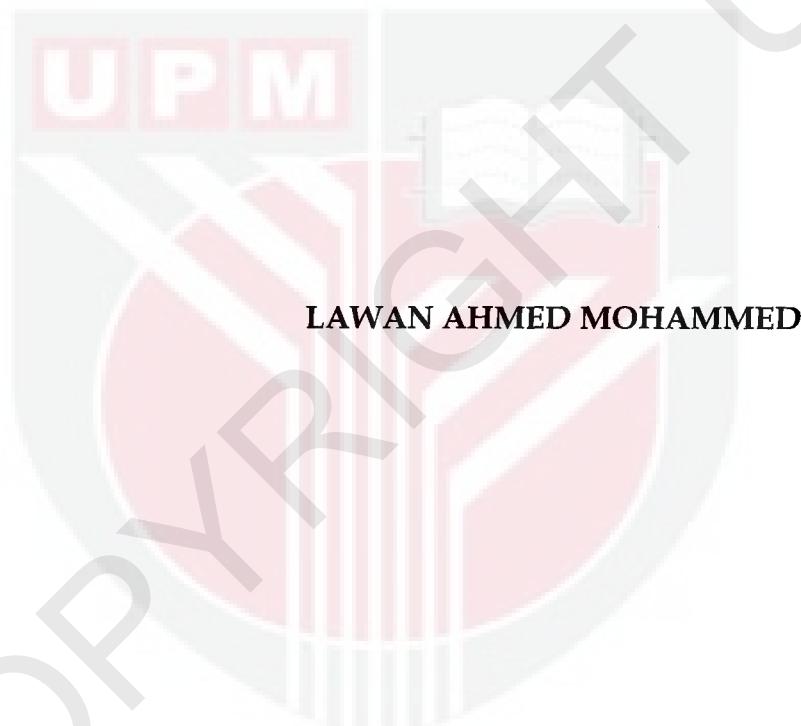
**UNIVERSITI PUTRA MALAYSIA**

**ENHANCEMENT OF SECURITY ARCHITECTURE FOR  
SMARTCARD-BASED AUTHENTICATION PROTOCOLS**

**LAWAN AHMED MOHAMMED.**

**FK 2004 47**

ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-  
BASED AUTHENTICATION PROTOCOLS



**DOCTOR OF PHILOSOPHY  
UNIVERSITI PUTRA MALAYSIA**

**June, 2004**



**ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-  
BASED AUTHENTICATION PROTOCOLS**

**By**

**LAWAN AHMED MOHAMMED**

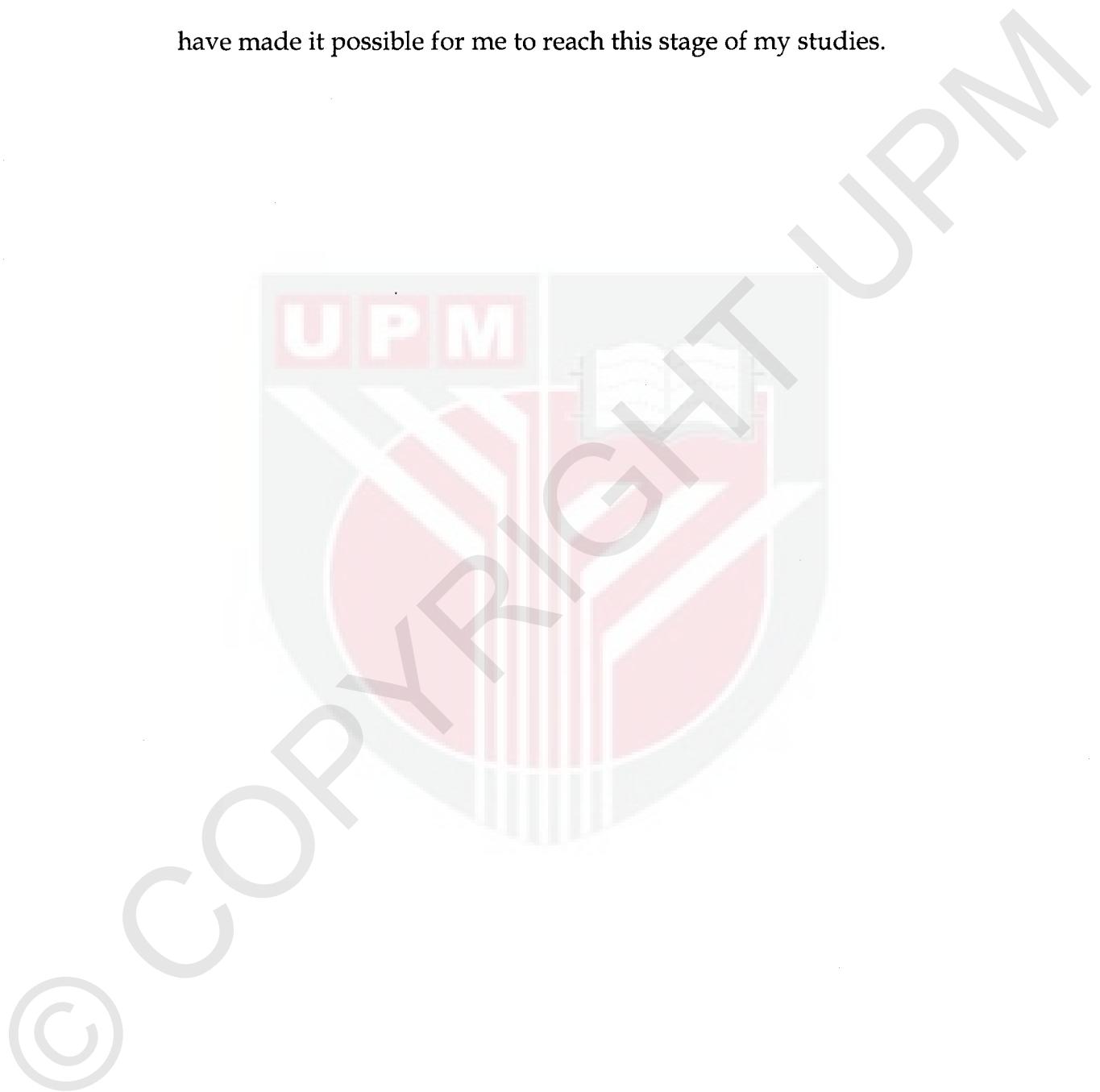
**Thesis Submitted to the School of Graduate Studies,  
Universiti Putra Malaysia, in Fulfilment of the  
Requirements for the Degree of Doctor of Philosophy**

**June, 2004**



## **DEDICATION**

This thesis is dedicated to my parents whose selfless sacrifices and dedications have made it possible for me to reach this stage of my studies.



Abstract of thesis presented to the Senate of the Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

**ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-BASED AUTHENTICATION PROTOCOLS**

By

**LAWAN AHMED MOHAMMED**

June, 2004

**Chairman: Associate Professor Haji. Dr. Abdul Rahman Ramli, Ph.D.**

**Faculty: Engineering**

Currently computer systems and software used by the average user offer less security due to rapid growth of vulnerability techniques. This dissertation presents an approach to increase the level of security provided to users when interacting with otherwise unsafe applications and computing systems. It provides a general framework for constructing and analyzing authentication protocols in realistic models of communication networks. This framework provides a sound formalization for the authentication problem and suggests simple and attractive design principles for general authentication protocols. The general approach uses trusted devices (specifically smartcards) to provide an

area of secure processing and storage. The key element in this approach is a modular treatment of the authentication problem in cryptographic protocols; this applies to the definition of security, to the design of the protocols, and to their analysis. The definitions are drawn from previous ideas and formalizations and incorporate several aspects that were previously overlooked. To identify the best cryptographic algorithm suitable for smartcard applications, the dissertation also investigates the implementation of Elliptic Curve encryption techniques and presents performance comparisons based on similar techniques. The findings discovered that the proposed Elliptic Curve Cryptographic (ECC) method provides greater efficiency than similar method in terms of computational speed.

Specifically, several aspects of authentication protocols were studied, and new definitions of this problem were presented in various settings depending on the underlying network. Further, the thesis shows how to systematically transform solutions that work in a model of idealized authenticated communications into solutions that are secure in the realistic setting of wired communication channels such as access control, and online transactions involving contact communication schemes.

As with all software development, good design and engineering practices are important for software quality. Rather than thinking of security as an add-on

feature to software systems, security should be designed into the system from the earliest stages of requirements gathering through development, testing, integration, and deployment. In view of this, a new approach for dealing with this problem in an object-oriented approach is presented. Some practical illustrations were analyzed based on the *Unified Modeling Language* (UML) as it applies to modeling authentication/access control schemes in online transactions. In particular, important issues such as how smartcard applications can be modeled using UML techniques and how UML can be used to sketch the operations for implementing a secure access using smartcard has been addressed.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia bagi mendapatkan ijazah Doktor Falsafah

**SUATU KAJIAN DAN PEMANTAPAN SENIBINA KESELAMATAN UNTUK  
PROTOKOL PENGESAHAN BERASASKAN KAD PINTAR**

Oleh

**LAWAN AHMED MOHAMMED**

Jun, 2004

Pengerusi: Profesor Madya Prof. Haji. Abdul Rahman Ramli, Ph.D.

Fakulti: Kejuruteraan

Sistem komputer dan perisian yang digunakan oleh pengguna kini mempunyai ciri keselamatan yang semakin tumpul disebabkan peningkatan dalam teknik-teknik pendedahan dalam ciri keselamatan (*vulnerability techniques*). Disertasi ini cuba mengengahkan satu kaedah untuk meningkatkan tahap keselemanan untuk pengguna apabila berinteraksi dengan aplikasi dan sistem komputer yang kurang selamat. Ia juga memberikan satu garis panduan untuk membina dan menganalisa protokol pengesahan di dalam model rangkaian komunikasi yang realistik. Garis panduan memberikan satu susun atur yang rapi bagi permasalahan pengesahan dan mencadangkan prinsip rekabentuk yang mudah

dan menarik untuk protokol pengesahan umum. Kaedah umum menggunakan peranti yang dipercayai (khususnya kad pintar) untuk memberikan kawasan selamat bayi elemen utama di dalam kaedah ini ialah dengan menggunakan rawatan modular terhadap permasalahan pengesahan dalam protokol kriptografi. Kaedah ini juga diterapkan kepada definisi keselamatan hingga ke kepada rekabentuk protokol dan analisis protokol tersebut. Definisi yang dimaksudkan telah di ambil dari idea-idea dan perancangan terdahulu dan melibatkan beberapa aspek yang sebelum ini telah diabaikan. Untuk mengenal pasti algoritma kriptografi yang terbaik sesuai untuk aplikasi kad pintar, disertasi ini juga mengkaji perlaksanaan teknik enkripsi '*Elliptic Curve Cryptography*' (ECC), dan membuat perbandingan berdasarkan pada teknik-teknik yang serupa. Penemuan yang dijumpai bahawa ECC yang dicadangkan memberikan kecekapan yang lebih tinggi berbanding kaedah ECC yang serupa.

Khususnya, beberapa aspek protokol pengesahan telah di kaji dan penakrifan baru bagi masalah ini telah dibentangkan dalam pelbagai persekitaran bergantung kepada rangkaian asasnya. Selanjutnya, tesis ini menunjukkan bagaimana untuk menukar secara sistematik penyelesaian yang berfungsi di dalam model komunikasi disahkan yang unggul, kepada penyelesaian yang selamat dalam persekitaran saluran komunikasi yang realistik seperti di dalam sistem kawalan laluan, dan urusniaga dalam talian yang melibatkan skema-skema komunikasi secara terus.

Sebagaimana dalam pembangunan perisian, rekabentuk dan amalan kejuruteraan yang baik adalah penting bagi memastikan kualiti perisian. Daripada memikirkan ciri keselamatan sebagai satu ciri tambahan kepada sistem perisian, ciri-ciri keselamatan sepatutnya diterapkan ke dalam sistem dari peringkat permulaan pengumpulan keperluan sehingga tahap pembangunan, ujian, integrasi dan perlaksanaan. Dengan ini, satu pendekatan baru bagi menangani masalah ini dengan menggunakan pendekatan berorientasikan objek diunjurkan. Beberapa contoh praktik telah dianalisa berdasarkan kepada '*Unified Modeling Language (UML)*' seperti mana ia dilaksanakan kepada model pengesahan/skema kawalan laluan di dalam urusniaga melalui Internet. Secara khususnya, perhatian dapat diberikan kepada isu-isu penting seperti bagaimana aplikasi kad pintar dapat dilaksanakan menggunakan teknik UML dan bagaimana UML dapat digunakan untuk melakarkan operasi bagi melaksanakan laluan selamat berasaskan kad pintar .

## **ACKNOWLEDGMENTS**

First of all I would like to thank All Mighty Allah for everything (Alhamdulillah). I am extremely grateful to my supervisor Associate Professor Haji AbdulRahman Ramli for the technical, financial and moral support he provided throughout my study. He has opened my mind to research in the field of computer and network security. I am also very grateful to the other members of the dissertation committee - Professor Mohamad Daud and Dr V. Prakash for their support and feedback in many ways. I had the opportunity to work with them and it has helped my research work immensely. Further, I would like to acknowledge Professor Mohamad Daud for his financial support.

Several people have helped and supported me in writing this dissertation. I would like to acknowledge Abdulkarim Mohd and Salisu Garba for their contribution in processing and delivering the thesis to the authority concern while I was away. Special thank goes to Mohammad Fadzilli for his efforts and comments especially in translating the abstract. Many thanks to all my lab mates who contributed in one way or the other toward successful completion of the thesis. Last but not least, I would like to thank my parents and my wife for being patient with me and for their encouragement during my studies.

Thanks everyone!  
Lawan Ahmed.

## TABLE OF CONTENTS

	Page
DEDICATION	ii
ABSTRACT	iii
ABSTRAK	ix
AKNOWLEDGEMENTS	vii
DECLARATION	x
LISTS OF TABLES	xvi
LISTS OF FIGURES	xviii
GLOSSARY OF TERMS	xxii
 <b>CHAPTER</b>	
I      INTRODUCTION	1
II     REVIEW OF SMARTCARDS AND AUTHENTICATION PROTOCOLS	12
Introduction To Smart Cards	12
Type of Smart Cards	13
Physical structures	15
Using Smart Card as Security Devices	17
Security Issues	18
Terminal Problems	18
Cryptographic Co-processors Cards	20
Considerations for Choosing Cryptosystems	27
Elliptic Curve Cryptosystem	32
Elliptic Curve Over $F_{2^m}$	34
Categorization of Finite Fields $F_q$	37
Defining EC Additions	38
Elliptic Curve and Discrete Logarithm Problems	48
Analysis of Encryption Algorithms	50
ECC in Comparison	51
Analog to DSA and ElGamal Schemes	55
Security Analysis of Elliptic Curves	58
A survey of Authentication Protocols	62
Arbitrary Authentifications	66
The Needham-Schroeder Protocols	66
The Kerberos Authentication Protocols	70
Direct Authentifications	76
X.509 Recommendation	77
Diffie Hellman Exchange	79

Cryptographic Protocols	80
Symmetric Key Protocol	81
Public Key Protocol	82
Attacks on Protocols	83
Attacks on Public Key	88
Attacks on Secret Key	89
Entity Authentication Tools	91
Password Based Authentication	91
Biometrics Based Authentication	93
A Comparison	96
Smart Card Based Authentication Protocols - State-of-Art	99
Conclusion	105
 III MATERIALS AND METHODS	107
Development Environment	107
Smartcard Platform and Specification	109
Debugging Environment	111
Security Issues	115
Security Commands	115
Implementation Process for ECC Algorithm	122
Cryptographic Plug-in Libraries	131
Elliptic Curve Domain Parameters	134
Conformance Specifications	135
Methodology for Choosing curves	137
System Implementation Overview	142
Scalar Multiplication	144
System Analysis and Design	145
Unified Modelling language (UML)	146
Systems Analysis	149
Systems Design	156
Conclusion	162
 IV RESULTS AND VERIFICATION	163
System Model Overview	163
Application Environment	167
Online Learning Systems	168
Implementation Example	171
ECC Implementation for the Proposed System	182
Pre-Computation Algorithm	183
Performance Analysis	187
Performance Evaluation	190
Numerical Test for Data Transfer	191
Benefits of the Proposed ECC Scheme	196

Security Analysis	198
Access Control Models	200
Subject-Object Based Access Control	201
Role-Based Access Control	201
Improving Role-Based Access Control	204
Security Analysis	208
Conclusion	209
<b>V APPLICATION AREAS</b>	<b>210</b>
Generalized Smart Card Authentication Scheme	210
Improving Time Stamp	214
Signature Verification	217
Security Analysis	217
Protocol Based on One-Way Hash Function and Biometrics	218
Algorithm for ATM Authentication	222
Current ATM Practice	224
Proposed ATM Authentication Protocols	225
Trusted User Protocol	226
Partially Trusted Terminal Protocol	228
Untrusted User and Terminal Protocol	231
Security Analysis	233
Consideration for MyKad	234
Security Mechanisms in MyKad	235
Areas of Possible Attack in MyKad	237
Conclusion	246
<b>VI CONCLUSIONS AND RECOMMENDATIONS</b>	<b>247</b>
Recommendations	247
Recommendation for Future Studies	250
Summary of Contributions	253
Conclusion	254
<b>BIBLIOGRAPHY</b>	<b>255</b>
<b>APPENDICES</b>	<b>270</b>
<b>BIODATA OF THE AUTHOR</b>	<b>307</b>

## List of Tables

<b>Table</b>		<b>Page</b>
2.0	Projection of Cryptographic Co-processor Available in 2000	26
2.1	Key Sizes Strength Comparison	51
2.2	Performance Evaluation	52
2.3	System's Parameters and Key	54
2.4	Signature Sizes on Long Messages	54
2.5	Size of Encrypted 100-bit Messages	55
2.6	Requirements Comparison	57
2.7	Smart Card Processing Time for RSA Algorithm	61
2.8	Smart Card Processing Time for DSA Signature	62
2.9	Smart Card Processing Time for ECC Signature	62
3.0	APDU Command and Response for ECC 161	121
3.1	Plug-in Libraries	132
3.2	Scheme Specification	136
3.3	Primitive Specification	136
3.4	Additional Technique Specification	136
3.5	Order of SuperSingular EC Over $F_{2^m}$ for Odd Number	139
3.6	Order of SuperSingular EC Over $F_{2^m}$ for Even Number	139
3.7	Non-SuperSingular Curves Over $F_{2^5}$	141
3.8	Some Non-SuperSingular Curves Over $F_{2^{155}}$	142
3.9	Candidates for Cryptosystems based on $F_{2^m}$	142

4.0	Parameter Requirement	183
4.1	Performance Analysis	188
4.2	General ATR Formulation	194
4.3	ATR-ETU Numerical Value	194
4.4	BWT Numerical Value	195
4.5	CWT Numerical Value	195
4.6	ATR Transmission Speed	196
5.0	Communication Rate and Storage Capacity	240
5.1	Requirements Bytes for Biometrics	244
5.2	Comparison between Smart Card and Biometrics	245

## LIST OF FIGURES

<b>Figure</b>		<b>Page</b>
2.0	Architecture of Memory Cards	14
2.1	Contact Smart Card	16
2.2	Contactless Smart Card	16
2.3	Plug-in Card	16
2.4	Time of Cryptographic Operations in Siemens Chip	23
2.5	Time of Cryptographic Operations in Phillips Chip	23
2.6	Time of Cryptographic Operations in Thomson's Chip	24
2.7	Average Time for Cryptographic Operations	25
2.8	Classification for Cryptographic Techniques in Smartcard	27
2.9	Graphical Representations of EC Points	36
2.10	Intersection Point on EC	39
2.11	Addition of two Points on EC	41
2.12	Doubling of Points on EC	43
2.13	Addition of P and $-P$ in EC	44
2.14	Discrete Logarithm in EC Over Real Numbers	49
2.15	Comparison of Security Levels	53
2.16	Needham_Schroeder Protocol	67
2.17	Kerberos Authentication Dialog	71
2.18	X.509 Certificate Format	78
3.0	Basic Card and Balance Reader	108

3.1	ZC-Basic Source Text Editor	112
3.2	Execution Environment	113
3.3	Card Downloading Process	114
3.4	Key Generation Console	116
3.5	Command APDU Structure	119
3.6	Response APDU Structure	120
3.7	Key Generation Class Diagram	125
3.8	Certificate Generation Class Diagram	143
3.9	General Use Case Diagram	152
3.10	Access Information Use Case Diagram	153
3.11	Package of Actors	154
3.12	Analysis Level Class Diagram	155
3.13	Sequence Diagram Depicting Card and Password	157
3.14	Prototype Illustrating Access to H.Secure Data	158
3.15	Design Level Class Diagram	160
3.16	Authentication Class Diagram for Staffs Access	161
3.17	Authentication Class Diagram for Students	161
3.18	Class Diagram for the System's Security Manager	162
4.0	Smartcard Personalization Process	164
4.1	Smartcard Initialization Process	164
4.2	CyberMouse Smartcard Reader	165

4.3	CyberMouse Installation	167
4.4	General System Architecture	172
4.5	Security Main Page	173
4.6	Login Applet	174
4.7	Lsecure Main Page	174
4.8	Access Control Terminal	175
4.9	Change PIN Dialog	176
4.10	Encryption Main Page	177
4.11a	Generating Symmetric Keys	177
4.11b	Secret Key Scheme	178
4.12a	RSA Scheme	179
4.12b	Encryption Based on Auto Key Generation	179
4.13	Saving Dialog	180
4.14	Saving to PC	180
4.12c	RSA Decryption Process	181
4.15	ECC Implementation on Smartcard	186
4.16	Signature Verification	187
4.17a	Key Generation - 10 Random Numbers	189
4.17b	Key Generation - 20 Random Numbers	189
4.17c	Key Generation - 30 Random Numbers	189
4.17d	Key Generation - 40 Random Numbers	190
4.18	Comparison Analysis	191

4.19	ATR Procedure	192
4.20	ATR Simulation	193
4.21	Subject_Object Based Access Control	201
4.22	Role Based Access control	202
4.23	Remote User Authentication Protocol	207
5.0	Simple Terminal Authentication Process	240
5.1	User Authentication Process	244
5.2	User and Terminal Authentication Process	245

## GLOSSARY OF TERMS

ACLU	American Civil Liberties Union
ATR	Answer to Reset
BBS	Blum-Blum-Shub
BWT	Block Waiting Time
CA	Certification Authorities
CRT	Chinese Remainder Theorem
CWT	Character Waiting Time
COSng	Next Generation Smartcard Operating Systems
CDMF	Commercial Data Masking Facility
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DNS	Domain Name System
ECC	Elliptic Curve Cryptosystem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECKAS-DH	Elliptic Curve Key Agreement Scheme ( Diffie-Hellman)
ECSSA	Elliptic Curve Signature Scheme
ECSVDP-DH	EC Secret Value Derivation Primitive (Diffie-Hellman)
ECSP-NR	Elliptic Curve Signature Primitive, Nyberg-Rueppel
ECVP-NR	Elliptic Curve Verification Primitive, Nyberg-Rueppel
EMSA	Encoding Method for Signatures with Appendix
ECDSA	Elliptic Curve Digital Signature Algorithm
ECES	Elliptic Curve Encryption Scheme
ETU	Element Time Unit
FAR	False Acceptance Rate
FRR	False Rejection Rate
GSM	Global System for Mobile Communication
GUI	Graphical User interface
IDEA	International Data Encryption Algorithm
ICC	Integrated Circuit Card
KDF	Key Derivation Function
LCG	Linear Congruential Generators
LFSR	Linear Feedback Shift Register
MAC	Message Authentication Code
MEPS	Malaysian Electronic Payment Systems
MISC	Miscellaneous procedures
MOV	Menezes-Okamoto-Vanstone
NBS	National Bureau of Standard
NTP	Network Time Protocol
ODL	Online Distance Learning
PCBC	Propagating CipherBlock Chaining
PGP	Pretty Good Privacy

PRNG	Pseudo-random number generator
RBAC	Role based access control
RSA	Rivest-Shamir-Adleman Algorithm
SHA-1	Secure Hash Algorithm, Version1
SG-LFSR	Shrinking Generator Linear Feedback Shift Register
SSL	Secure Sockets Layer
STS	Station-to-Station Protocol
SNMP	Simple Network Management Protocol
RNG	Random number generation
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Server
TGT	Ticket-Granting Ticket
TTP	Trusted Third Party
UML	Unified Modeling Language