CPK Cryptosystem and Identity Authentication

CPK公钥体制与标识鉴别

Xianghao Nan

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Xianghao Nan

CPK Cryptosystem
and
Identity Authentication

CPK公钥体制与标识鉴别

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

About the Author

Xianghao Nan

Dean, South China Information Security Institute

Doctorial Tutor, Information Engineering University, PLA

Part Time Professor, Institute of Computer Science and Technology, Peking University

Publications:

1. *Profile to Network Security Technologies*, 2003 (*Chinese*)
2. *Identity Authentication Based on CPK*, 2005 (*Chinese*)
3. *CPK Crypto-system and Cyber Security*, 2007 (*Chinese*)
4. *Cyber Seurity Technical Framework*, 2010 (*English*)

Forward

Providing trust in the face of anonymity is an impossibility. Since interactions on the Internet can easily be anonymous, it is imperative to find a digital authentication means that is reliable, simple to deploy, and simple to use. A method that will bring trust to the Internet and to the general population is critical. The CPK cryptosystem allows society to enjoy the benefits of eCommerce and individual privacy which is balanced with the social needs.

Anonymity, the ability to perform an act without identifying oneself, is not a new concept, but has been dramatically enhanced because of the Internet. Traditionally, the presence of an offender and a victim in the same location leaves behind physical evidence, and this evidence improves the ability of the police to identify and apprehend an offender. By comparison, the Internet has been shown to be a haven for offenders. Offenders can perform criminal acts at great distances that can transcend national boundaries in near perfect anonymity, making law enforcement dramatically more difficult.

Authentication is the natural defense of anonymity, it forms the foundation for trust by proving identity. Authentication can be used for authorization, privacy, and deterrence.

Authentication for authorization is necessary to access money in the bank or to know that the person who signed the document has the authority to commit for the organization.

Authentication for privacy is necessary to know that a conversation is private between two people. An email to your spouse should not be readable by someone who has attacked the Internet. This form of "direct encryption" has higher levels of trust if there is direct authentication by both parties.

Authentication for deterrence is necessary to be able to know who you interact with. Seeing the license of a car provides some assurance about who you are dealing with if something bad happens, there is a better chance of the police

being able to track down the offender.

Cryptographic Authentication attempts to provide this proof of identity from a distance using purely digital means. This is a difficult problem that transcends the mathematics of cryptography and moves into the philosophical issues of trust and the organizational basis of society.

In Whitfield Diffie 's and Martin Hellman 's 1976 paper " NEW DIRECTIONS IN CRYPTOGRAPHY" the authors introducing the concept of public key cryptography and digital signatures wrote. . .

- Authentication is at the heart of any system involving contracts and billing. Without it, business cannot function. Current electronic authentication systems cannot meet the need for a purely digital, unforgetable, message dependent signature. They provide protection against third party forgeries, but do not protect against disputes between transmitter and receiver.

Since that time, there have been many digital signature schemes proposed and some standardized. In general these are now described as traditional signature schemes that have been implemented as a directed graph of public keys which are signed by a more general key until the point that there is mutual trust.

Traditional digital authentication is tied to the individual. It requires a public key distribution scheme and lacks lawful intercept abilities.

If Alice needs to send an email to Bob, she must first get Bob 's public key from a repository, check the revoked key list, and authenticate this key to some root key that she trusts before she can send a message to Bob. This is a significant effort.

If Alice and Bob are conspirators in a crime, their communications cannot be investigated by law enforcement.

Identity based encryption provides simpler solutions to these problems. From Adi Shamir 's 1984 paper " IDENTITY BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES" he states:

- In this paper we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each

other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party.

Professor Shamir further states that...

- The scheme remains practical even on a nationwide scale with hundreds of key generation centers and millions of users, and it can be the basis for a new type of personal identification card which everyone can electronically sign checks, credit card slips, legal documents, and electronic mail.

One of the values of identity based encryption is the key generating centers can be operated by organizations who can naturally vouch for an individual's identity. For example, an university can vouch for a professor or a student, or a corporation can vouch for an employee.

Identity based encryption also provides a deterrence against the abuse of trust. In practice, a key generated by a corporation has the valuable side effect of allowing policing by that corporation of an individual's use of that key.

The CPK algorithm represents a great step forward in identity based encryption. It creates a simple to understand, easy to implement, and easy to deploy system that provides all the benefits that these visionaries imagined for public key and identity based cryptosystems.

This book delivers a complete analysis of what Identity, Authentication and Trust mean in a digital age. It shows how CPK can meet the challenges of the Internet to make it a safer place.

This book may not result in world peace, but it can provide a roadmap to calm the chaos which exists on the Internet today.

James P. Hughes
Palo Alto, CA, USA

Note: The forward was written for the book of "Identity Authentication". In this new book, the forward was reused because the contents of the old book was not changed except the newly added Part Eleven.

Preface

A report submitted by the US President 's Information Technology Advisory Committee (PITAC) in 2005, entitled *Cyber Security—A Crisis of Prioritization*, marked the arrival of a new era of cyber security (cyber world). If the main task of "information security" was a passive prevention that consists mainly of plugging and patching, the main task of "cyber security" is active management that consists mainly of building a trusting (authenticating) system. It is a new mission. In the past, since there were no proper evidence-showing and verifying systems, information security can only adopt the principle of "mutual trust", or based on the presumption that the subject was trustworthy. However, cyber security is totally different. It is established on the basis of "mutual suspicion", not allowing authentication or verification under presumption.

Such changes of main task and basic principles first affect basic theory of security. All the security protocols and standards adopting the principle of "mutual trust" in the past shall be reconsidered with "mutual suspicion", for example, communication protocols and standards, computing protocols and standards. This will surely lead to a revolutionary change.

At the EU crypt'2007 annual meeting, James Hughes (executive chairman of Crypt '04) and Guan Zhi (Ph. D student of Peking University) delivered a presentation on identity-based Combined Public Key (CPK) system. The authoritative experts attending the meeting affirmed that CPK system is novel. Identity-based system represents new development trend of modern cryptosystem, and attracts attention from cryptography community around the world. CPK Cryptosystem has attracted great attention from China 's top leaders, and also has received substantial support from the administrations of Guangdong Science and Technology Department and Beijing Municipal Science and Technology Commission. Researchers/Professors Zhou Zhong-yi, Chen Hua-ping, Lü Shu-wang, Zhai Qi-bing, Li Yi-fa and Doctors Tang Wen, Guan Zhi, Chen

Yu, Tian Wen-chun, Zheng Xu have involved in this CPK project.

Another important progress is that a theory of authentication logic is established based on identity authentication, to promote the conventional belief logic and trust logic to truth logic. The truth logic based on identity authentication is different from the belief logic based on data authentication. The truth logic consisted of identity of entity authentication and body of entity authentication, can conduct "pre-proof". That is, identity authentication can be conducted before the body event occurs, so as to effectively prevent illegal events from happening. Large scale authentication technology is the core technology to establishing a secure world. CPK system can solve such international puzzle well.

Solutions in the main fields of trusting (authenticating) system in the book are introduced. Such fields include a number of problems which cannot be solved in the past but easily dealt with now, for instance: illegal communication access, illegal software running, seal authentication systems, etc. From examples of application, readers can find that due to the core issue of identity authentication has been solved, a number of difficult problems that was impossible to solve in the past can be easily tackled. Thus, "identity authentication" is the "silver bullet" of cyber security, which will lead to the solution of all other problems. This is the base of a holistic solution of trusting (authenticating) system. In the process of researching, Communication expert Sun Yu, Computer expert Qu Yan-wen, IT expert James Hughes and sci&tech information expert Zhao Jian-guo offered useful suggestions.

At the beginning of 2009, U. S. government has released some documents related with cyber security. The documents have stressed three points: Addressing system in internet, identity authentication and secure software engineering. The address is the identity of communication. It tells us the identity management, including identity definition and identity authentication, will be the basic techniques of future cyber security. How to define identity is an important subject but beyond this book. However, we have enough experience in defining identity in real life such as the mailing address, phone number, bank account

number, and so on. This is the reason why we stand for real name system. From the rules of identity definition in real life we may draw an important conclusion: in authenticating system, identity must have special meaning and the meaning must be commonly recognized. It is obvious that, the address is defined randomly and only explained by special DNS in existing IPv4 and IPv6 protocols. It is unfortunate that the protocols go against above mentioned basic rules. This is the reason why we took "identity authentication" and addressing system as core task of cyber security.

The work of cyber security is in progress of developing on its track and has yielded some important results. For example, a new type of network router is designed with real name communication system. The address is the real location that bounded with the signuture code, so it can prohibit any unauthorized connection. Meanwhile code signing has been developed rapidly as main part of software security.

CPK cryptosystem, identity authentication and truth logic is introduced in this book as the basic theory and technology. The construction of secure world needs a joint effort of all nations because we have a common enemy: that is the "terrorist software". I sincerely wish that this book can satisfy the demands of readers, facilitate transition of information security from network security to cyber security.

This book is rewritten on the base of *Cyber Security Technical Framework—Trusting System Based on Identity Authentication*, where Chapters 2, 4, 6 are rewritten and Chapter 26 is added; and all the terms of "trusted" and "trusting" are replaced by "authenticated" and "authenticating" respectively.

In these two years, we have made some important progresses in public key cryptosystem and RFID design. The new progresses are added to the new book as Part Eleven.

Author
In Beijing. Sep. 2009
Revised, Nov. 2011.

Contents

Part One Authentication Technology

Chapter 1 Basic Concepts 2
1.1 Physical World and Digital World 2
1.2 A World with Order and without Order 3
1.3 Self-assured Proof and 3rd Party Proof 5
1.4 Certification Chain and Trust Chain 7
1.5 Centralized and Decentralized Management 8
1.6 Physical Signature and Digital Signature 10
Chapter 2 Authentication Logics 14
2.1 Belief Logic 15
2.1.1 The Model 15
2.1.2 The Formulae 16
2.1.3 The Characteristics of Belief Logic 16
2.2 Trust Logic 17
2.2.1 Direct Trust 17
2.2.2 Axiomatic Trust 17
2.2.3 Inference Trust 18
2.2.4 Behavior Based Trust 19
2.2.5 Characteristics of Trust Logic 20
2.3 Truth Logic 20
2.3.1 The Needs of "Pre-proof" 20
2.3.2 Entity Authenticity 21
2.3.3 The Characteristics of Truth Logic 24
2.4 Authentication Protocols 25
2.4.1 Standard Protocol 25
2.4.2 CPK Protocol 26

2.5 Authentication Systems ····· 28
2.5.1 PKI Certification System ····· 28
2.5.2 CPK Authentication System ····· 30
Chapter 3 Identity Authentication ····· 32
3.1 Communication Identity Authentication ····· 33
3.2 Software Identity Authentication ····· 34
3.3 Electronic Tag Authentication ····· 36
3.4 Network Management ····· 37
3.5 Holistic Security ····· 38

Part Two Cryptosystems

Chapter 4 Combined Public Key (v6.0) ····· 42
4.1 Introduction ····· 42
4.2 Mapping Functoin ····· 43
4.3 Computation of Keys ····· 43
4.3.1 Computation of Identity-key ····· 43
4.3.2 Computation of Separating-key ····· 44
4.3.3 Computation of General-key ····· 44
4.3.4 Computation of District-key ····· 44
4.4 Digital Signature and Key Delivery ····· 45
4.4.1 Digital Signature ····· 45
4.4.2 Key Delivery ····· 46
4.5 Security ····· 46
4.6 Conclusion ····· 47
Chapter 5 Cryptosystem and Authentication ····· 48
5.1 New Requirements for Cryptosystem ····· 48
5.2 Development of Cryptosystems ····· 49
5.3 Identity Authentication Schemes ····· 50
5.3.1 Identity Authentication with IBC ····· 50
5.3.2 Identity Authentication with CPK ····· 51
5.3.3 Identity Authentication with PKI ····· 52
5.3.4 Identity Authentication with IB-RSA ····· 53

5.3.5 Identity Authentication with mRSA ····· 54
5.3.6 Comparison of Schemes ····· 54
5.4 Key Delivery Schemes ····· 55
5.4.1 IBE Key Delivery ····· 55
5.4.2 CPK Key Delivery ····· 56
5.4.3 Other Key Delivery Schemes ····· 56
5.4.4 Performance Comparison ····· 57
5.5 Discussion on Trust Root ····· 58
Chapter 6 Bytes Encryption ····· 60
6.1 Coding Structure ····· 60
6.1.1 Permutation Table (disk) ····· 60
6.1.2 Substitution Table (subst) ····· 61
6.1.3 Key Structure ····· 62
6.2 Working Flow ····· 63
6.2.1 Given Conditions ····· 63
6.2.2 Key Derivation ····· 64
6.2.3 Data Expansion ····· 64
6.2.4 Compound of Data and Key ····· 64
6.2.5 Left Shift Accumulation ····· 65
6.2.6 Permutation ····· 65
6.2.7 Right Shift Accumulation ····· 65
6.2.8 Data Concentration ····· 66
6.2.9 Single Substitution ····· 66
6.2.10 Compound of Data and Key ····· 66
6.3 Security Analysis ····· 67

Part Three CPK System

Chapter 7 CPK Key Management ····· 70
7.1 CPK Key Distribution ····· 70
7.1.1 Authentication Network ····· 70
7.1.2 Communication Key ····· 71
7.1.3 Classification of Keys ····· 71

7.2 CPK Signature ····· 72
7.2.1 Digital Signature and Verification ····· 72
7.2.2 Signature Format ····· 73
7.3 CPK Key Delivery ····· 73
7.4 CPK Data Encryption ····· 74
7.5 Key Protection ····· 75
7.5.1 Password Verification ····· 75
7.5.2 Password Change ····· 76
Chapter 8 CPK-chip Design ····· 77
8.1 Background ····· 77
8.2 Main Technology ····· 77
8.3 Chip Structure ····· 79
8.4 Main Functions ····· 82
8.4.1 Digital Signature ····· 82
8.4.2 Data Encryption ····· 84
Chapter 9 CPK ID-card ····· 86
9.1 Background ····· 86
9.2 ID-card Structure ····· 88
9.2.1 The Part of Main Body ····· 88
9.2.2 The Part of Variables ····· 88
9.3 ID-card Data Format ····· 89
9.4 ID-card Management ····· 92
9.4.1 Administrative Organization ····· 92
9.4.2 Application for ID-card ····· 93
9.4.3 Registration Department ····· 94
9.4.4 Production Department ····· 95
9.4.5 Issuing Department ····· 97

Part Four Software Authentication

Chapter 10 Software ID Authentication ····· 100
10.1 Technical Background ····· 100
10.2 Main Technology ····· 101

10.3 Signing Module ····· 102
10.4 Verifying Module ····· 104
10.5 The Feature of Code Signing ····· 105
Chapter 11 Windows Code Authentication ····· 107
11.1 Introduction ····· 107
11.2 PE File ····· 107
11.3 Mini-filter ····· 108
11.3.1 NT I/O Subsystem ····· 108
11.3.2 File Filter Driving ····· 110
11.3.3 Mini-filter ····· 110
11.4 Code Authentication of Windows ····· 111
11.4.1 The System Framework ····· 111
11.4.2 Characteristics Collecting ····· 112
11.5 Conclusion ····· 112
Chapter 12 Linux Code Authentication ····· 113
12.1 General Description ····· 113
12.2 ELF File ····· 113
12.3 Linux Security Module (LSM) Framework ····· 114
12.4 Implementation ····· 115

Part Five Communication Authentication

Chapter 13 Phone Authentication ····· 118
13.1 Main Technologies ····· 118
13.2 Connecting Procedure ····· 119
13.3 Data Encryption ····· 120
13.4 Data Decryption ····· 121
Chapter 14 SSL Communication Authentication ····· 123
14.1 Layers of Communication ····· 123
14.2 Secure Socket Layer (SSL) ····· 124
14.3 Authenticated Socket Layer (ASL) ····· 127
14.4 ASL Working Principle ····· 128
14.5 ASL Address Authentication ····· 130

14.6 Comparison ····· 132
Chapter 15 Router Communication Authentication ····· 134
15.1 Principle of Router ····· 135
15.2 Requirements of Authenticated Connection ····· 136
15.3 Fundamental Technology ····· 137
15.4 Origin Address Authentication ····· 138
15.5 Encryption Function ····· 141
15.5.1 Encryption Process ····· 142
15.5.2 Decryption Process ····· 142
15.6 Requirement of Header Format ····· 142
15.7 Computing Environment ····· 143
15.7.1 Evidence of Software Code ····· 143
15.7.2 Authentication of Software Code ····· 143
15.8 Conclusion ····· 144

Part Six e-Commerce Authentication

Chapter 16 e-Bank Authentication ····· 146
16.1 Background ····· 146
16.2 Counter Business ····· 147
16.3 Business Layer ····· 148
16.4 Basic Technology ····· 149
16.5 Business at ATM ····· 151
16.6 Communication Between ATM and Portal ····· 151
16.7 The Advantages ····· 153
Chapter 17 e-Bill Authentication ····· 155
17.1 Bill Authentication Network ····· 155
17.2 Main Technologies ····· 156
17.3 Application for Bills ····· 156
17.4 Circulation of Bills ····· 158
17.5 Verification of Check ····· 158

Part Seven Logistics Authentication

Chapter 18 e-Tag Authentication ····· 162

18.1 Background ····· 162
18.2 Main Technology ····· 163
18.3 Embodiment (Ⅰ) ····· 165
18.4 Embodiment (Ⅱ) ····· 166
Chapter 19 The Design of Mywallet(v1.0) ····· 168
19.1 Two Kinds of Authentication Concept ····· 168
19.2 System Configuration ····· 170
19.3 Tag Structure ····· 171
19.3.1 Structure of Data Region ····· 171
19.3.2 Structure of Control Region ····· 172
19.4 Tag Data Generation and Authentication ····· 172
19.4.1 KMC ····· 173
19.4.2 Enterprise ····· 173
19.4.3 Writer and Reader ····· 173
19.5 Protocol Design ····· 174
19.6 Conclusion ····· 175

Part Eight Stored File Authentication

Chapter 20 Storage Authentication ····· 178
20.1 Security Requirements ····· 178
20.2 Basic Technology ····· 179
20.3 File Uploading Protocol ····· 180
20.4 File Downloading Protocol ····· 181
20.5 Data Storing ····· 182
20.5.1 Establishment of Key File ····· 183
20.5.2 Storage of Key File ····· 183
20.5.3 Documental Database Encryption ····· 184
20.5.4 Relational Database Encryption ····· 185
Chapter 21 Secure File Box ····· 187
21.1 Background ····· 187
21.2 System Framework ····· 188
21.3 Features of the System ····· 189

21.4 System Implementation ····· 190
Chapter 22 Classification Seal Authentication ····· 193
22.1 Background Technology ····· 193
22.2 Main Technologies ····· 194
22.3 Working Flow ····· 196
22.4 Embodiment ····· 197
22.5 Explanation ····· 198

Part Nine Moving Data Authentication

Chapter 23 e-Mail Authentication ····· 206
23.1 Main Technologies ····· 206
23.2 Sending Process ····· 208
23.3 Receiving Process ····· 208
Chapter 24 Digital Right Authentication ····· 210
24.1 Technical Background ····· 210
24.2 Main Technologies ····· 211
24.3 Manufacturer's Digital Right ····· 212
24.4 Enterprise's Right of Operation ····· 213
24.5 Client's Right of Usage ····· 215

Part Ten Network Authentication

Chapter 25 Pass Authentication ····· 218
25.1 Background ····· 218
25.2 Working Principles ····· 219
25.3 The Diagram of Gate-guard ····· 220
25.4 Gate-guard for Individual PC ····· 223
25.5 Guarding Policy ····· 224
Chapter 26 Address Authentication ····· 225
26.1 Background ····· 225
26.2 Main Problems ····· 226
26.3 Technical Approach ····· 226
26.3.1 CPK Cryptosystem ····· 226