

# Identity Authentication

Technical Basis of Cyber Security

## 标识鉴别

——网际安全技术基础

Nan Xiang - Hao



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

# Identity Authentication

Technical Basis of Cyber Security

16 15 13 10

ISBN 978-1-7256-0000-0

© 2020 Taylor & Francis

**Taylor & Francis**

Taylor & Francis Group

# Identity Authentication

Technical Basis of Cyber Security

标识鉴别——网际安全技术基础

Nan Xiang-Hao

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

## Abstract

The latest version of CPK (v6.0) is realized on chip. The CPK-chip carries CPK-cryptosystem to a new stage of development. The chip not only has the function of signature and verification, but also has the function of encryption and decryption without any outside support. CPK can solve the hard problem of scaled identity authentication, minimizing the threat of attack (cloud computing, quantum computing and collusion). CPK can advance the authentication logic from "belief logic" and "trust logic" to "truth logic". The truth logic is the foundation of constructing authenticated (trusted) connecting, computing, transaction, logistics, counter-forgery, and so on.

Readers benefited from this book will be researchers and professors, experts and students, engineers and policy makers, and all others who are interested in cyber security.

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有,侵权必究。

### 图书在版编目(CIP)数据

标识鉴别: 网际安全技术基础: 英文/南相浩著. —北京: 电子工业出版社, 2011.6  
ISBN 978-7-121-13479-1

I. ①标… II. ①南… III. ①计算机网络-安全技术-英文 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 084551 号

责任编辑: 赵 平

印 刷: 三河市鑫金马印装有限公司  
装 订:

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编: 100036

开 本: 720 × 1000 1/16 印张: 17.75 字数: 452 千字

印 次: 2011 年 6 月第 1 次印刷

印 数: 1 500 册 定价: 88.00 元

凡所购买电子工业出版社的图书, 如有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 [zltz@phei.com.cn](mailto:zltz@phei.com.cn), 盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

服务热线: (010) 88258888。

## About the Author

NAN Xiang-Hao: Dean, South China Information Security Institute, visiting professor of Information Engineering University and 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 Security 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 mathe-

matics 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, unforgettable, 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

## 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 Huaping, 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 differ-

ent 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 signature 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.

Author  
In Beijing, Sep. 2009

# 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 3 <sup>rd</sup> Party Proof | 4  |
| 1.4       | Certification Chain and Trust Chain                | 7  |
| 1.5       | Centralized and Decentralized Management           | 8  |
| 1.6       | Physical Signature and Digital Signature           | 9  |
| Chapter 2 | Authentication Logics                              | 13 |
| 2.1       | Belief Logic                                       | 14 |
| 2.1.1     | The Model                                          | 14 |
| 2.1.2     | The Formulae                                       | 14 |
| 2.1.3     | The Characteristics of Belief Logic                | 15 |
| 2.2       | Trust Logic                                        | 15 |
| 2.2.1     | Direct Trust                                       | 15 |
| 2.2.2     | Axiomatic Trust                                    | 16 |
| 2.2.3     | Inference Trust                                    | 16 |
| 2.2.4     | Behavior Based Trust                               | 17 |
| 2.2.5     | Characteristics of Trust Logic                     | 18 |
| 2.3       | Truth Logic                                        | 19 |
| 2.3.1     | The Needs of Truth Logic                           | 19 |
| 2.3.2     | Entity Authenticity                                | 19 |
| 2.3.3     | The Characteristics of Truth Logic                 | 22 |
| 2.4       | Authentication Protocols                           | 23 |
| 2.4.1     | Standard Protocol                                  | 23 |
| 2.4.2     | CPK Protocol                                       | 24 |
| 2.5       | Authentication Systems                             | 25 |
| 2.5.1     | PKI Certification System                           | 26 |

|                  |                                             |           |
|------------------|---------------------------------------------|-----------|
| 2. 5. 2          | CPK Authentication System .....             | 27        |
| <b>Chapter 3</b> | <b>Identity Authentication .....</b>        | <b>29</b> |
| 3. 1             | Communication Identity Authentication ..... | 29        |
| 3. 2             | Software Identity Authentication .....      | 31        |
| 3. 3             | Electronic Tag Authentication .....         | 32        |
| 3. 4             | Network Management .....                    | 33        |
| 3. 5             | Holistic Security .....                     | 34        |

## **Part Two Cryptosystems**

|                  |                                              |           |
|------------------|----------------------------------------------|-----------|
| <b>Chapter 4</b> | <b>Combined Public Key (v6. 0) .....</b>     | <b>38</b> |
| 4. 1             | Introduction .....                           | 38        |
| 4. 2             | Mapping Function .....                       | 39        |
| 4. 3             | Computation of Keys .....                    | 39        |
| 4. 3. 1          | Computation of Identity-Key .....            | 39        |
| 4. 3. 2          | Computation of Separating-key .....          | 40        |
| 4. 3. 3          | Computation of General-key .....             | 40        |
| 4. 3. 4          | Computation of District-key .....            | 40        |
| 4. 4             | Digital Signature and Key Delivery .....     | 41        |
| 4. 4. 1          | Digital Signature .....                      | 41        |
| 4. 4. 2          | Key Delivery .....                           | 41        |
| 4. 5             | Security .....                               | 42        |
|                  | Conclusion .....                             | 42        |
| <b>Chapter 5</b> | <b>Cryptosystem and Authentication .....</b> | <b>43</b> |
| 5. 1             | New Requirements for Cryptosystem .....      | 43        |
| 5. 2             | Development of Cryptosystems .....           | 44        |
| 5. 3             | Identity Authentication Schemes .....        | 45        |
| 5. 3. 1          | Identity Authentication with IBC .....       | 45        |
| 5. 3. 2          | Identity Authentication with CPK .....       | 46        |
| 5. 3. 3          | Identity Authentication with PKI .....       | 47        |
| 5. 3. 4          | Identity Authentication with IB-RSA .....    | 48        |
| 5. 3. 5          | Identity Authentication with mRSA .....      | 48        |
| 5. 3. 6          | Comparison of Schemes .....                  | 49        |
| 5. 4             | Key Delivery Schemes .....                   | 49        |
| 5. 4. 1          | IBE Key Delivery .....                       | 49        |

|                  |                                    |           |
|------------------|------------------------------------|-----------|
| 5. 4. 2          | CPK Key Delivery .....             | 50        |
| 5. 4. 3          | Other Key Delivery Schemes .....   | 51        |
| 5. 4. 4          | Performance Comparison .....       | 52        |
| 5. 5             | Related Discussions .....          | 52        |
| 5. 5. 1          | Discussion on Trust Root .....     | 52        |
| 5. 5. 2          | Discussion on Quantum Attack ..... | 53        |
| <b>Chapter 6</b> | <b>Bytes Encryption .....</b>      | <b>55</b> |
| 6. 1             | Coding Structure .....             | 55        |
| 6. 1. 1          | Permutation Table ( disk) .....    | 55        |
| 6. 1. 2          | Substitution Table ( subst) .....  | 56        |
| 6. 1. 3          | Key Structure .....                | 57        |
| 6. 2             | Working Flow .....                 | 58        |
| 6. 2. 1          | Given Conditions .....             | 58        |
| 6. 2. 2          | Key Derivation .....               | 59        |
| 6. 2. 3          | Data Expansion .....               | 59        |
| 6. 2. 4          | Compound of Data and Key .....     | 59        |
| 6. 2. 5          | Left Shift Accumulation .....      | 60        |
| 6. 2. 6          | Permutation .....                  | 60        |
| 6. 2. 7          | Right Shift Accumulation .....     | 60        |
| 6. 2. 8          | Data Concentration .....           | 60        |
| 6. 2. 9          | Single Substitution .....          | 61        |
| 6. 2. 10         | Compound of Data and Key .....     | 61        |
| 6. 3             | Security Analysis .....            | 61        |

### **Part Three CPK System**

|                  |                                          |           |
|------------------|------------------------------------------|-----------|
| <b>Chapter 7</b> | <b>CPK Key Management .....</b>          | <b>64</b> |
| 7. 1             | CPK Key Distribution .....               | 64        |
| 7. 1. 1          | Authentication Network .....             | 64        |
| 7. 1. 2          | Communication Key .....                  | 65        |
| 7. 1. 3          | Classification of Keys .....             | 65        |
| 7. 2             | CPK Signature .....                      | 66        |
| 7. 2. 1          | Digital Signature and Verification ..... | 66        |
| 7. 2. 2          | Signature Format .....                   | 67        |
| 7. 3             | CPK Key Delivery .....                   | 67        |

|                  |                                   |           |
|------------------|-----------------------------------|-----------|
| 7.4              | CPK Data Encryption .....         | 68        |
| 7.5              | Key Protection .....              | 68        |
| 7.5.1            | Password Verification .....       | 69        |
| 7.5.2            | Password Change .....             | 69        |
| <b>Chapter 8</b> | <b>CPK-chip Design .....</b>      | <b>70</b> |
| 8.1              | Background .....                  | 70        |
| 8.2              | Main Technology .....             | 70        |
| 8.3              | Chip Structure .....              | 72        |
| 8.4              | Main Functions .....              | 75        |
| 8.4.1            | Digital Signature .....           | 75        |
| 8.4.2            | Data Encryption .....             | 76        |
| <b>Chapter 9</b> | <b>CPK ID-card .....</b>          | <b>78</b> |
| 9.1              | Background .....                  | 78        |
| 9.2              | ID-card Structure .....           | 79        |
| 9.2.1            | The Part of Main Body .....       | 80        |
| 9.2.2            | The Part of Variables .....       | 80        |
| 9.3              | ID-card Data Format .....         | 81        |
| 9.4              | ID-card Management .....          | 83        |
| 9.4.1            | Administrative Organization ..... | 83        |
| 9.4.2            | Application for ID-card .....     | 84        |
| 9.4.3            | Registration Department .....     | 85        |
| 9.4.4            | Production Department .....       | 86        |
| 9.4.5            | Issuing Department .....          | 88        |

## **Part Four Code Authentication**

|                   |                                          |           |
|-------------------|------------------------------------------|-----------|
| <b>Chapter 10</b> | <b>Software ID Authentication .....</b>  | <b>90</b> |
| 10.1              | Technical Background .....               | 90        |
| 10.2              | Main Technology .....                    | 91        |
| 10.3              | Signing Module .....                     | 92        |
| 10.4              | Verifying Module .....                   | 93        |
| 10.5              | The Feature of Code Signing .....        | 95        |
| <b>Chapter 11</b> | <b>Windows Code Authentication .....</b> | <b>97</b> |
| 11.1              | Introduction .....                       | 97        |
| 11.2              | PE File .....                            | 97        |

|            |                                             |     |
|------------|---------------------------------------------|-----|
| 11.3       | Mini-filter .....                           | 98  |
| 11.3.1     | NT I/O Subsystem .....                      | 98  |
| 11.3.2     | File Filter Driving .....                   | 99  |
| 11.3.3     | Mini-filter .....                           | 100 |
| 11.4       | Code Authentication of Windows .....        | 101 |
| 11.4.1     | The System Framework .....                  | 101 |
| 11.4.2     | Characteristics Collecting .....            | 101 |
| 11.5       | Conclusion .....                            | 101 |
| Chapter 12 | Linux Code Authentication .....             | 102 |
| 12.1       | General Description .....                   | 102 |
| 12.2       | ELF File .....                              | 102 |
| 12.3       | Linux Security Module (LSM) Framework ..... | 103 |
| 12.4       | Implementation .....                        | 104 |

## **Part Five Communication Authentication**

|            |                                                |     |
|------------|------------------------------------------------|-----|
| Chapter 13 | Phone Authentication .....                     | 108 |
| 13.1       | Main Technologies .....                        | 108 |
| 13.2       | Connecting Procedure .....                     | 109 |
| 13.3       | Data Encryption .....                          | 110 |
| 13.4       | Data Decryption .....                          | 111 |
| Chapter 14 | SSL Communication Authentication .....         | 112 |
| 14.1       | Layers of Communication .....                  | 112 |
| 14.2       | Secure Socket Layer (SSL) .....                | 113 |
| 14.3       | Authenticated Socket Layer (ASL) .....         | 115 |
| 14.4       | TSL Working Principle .....                    | 116 |
| 14.5       | ASL Address Authentication .....               | 118 |
| 14.6       | Comparison .....                               | 120 |
| Chapter 15 | Router Communication Authentication .....      | 121 |
| 15.1       | Principle of Router .....                      | 122 |
| 15.2       | Requirements of Authenticated Connection ..... | 123 |
| 15.3       | Fundamental Technology .....                   | 124 |
| 15.4       | Origin Address Authentication .....            | 125 |
| 15.5       | Encryption Function .....                      | 127 |
| 15.5.1     | Encryption Process .....                       | 128 |

|            |                                       |     |
|------------|---------------------------------------|-----|
| 15.5.2     | Decryption Process .....              | 128 |
| 15.6       | Requirement of Header Format .....    | 128 |
| 15.7       | Computing Environment .....           | 129 |
| 15.7.1     | Evidence of Software Code .....       | 129 |
| 15.7.2     | Authentication of Software Code ..... | 129 |
| Conclusion | .....                                 | 130 |

## **Part Six e-Commerce Authentication**

|            |                                            |     |
|------------|--------------------------------------------|-----|
| Chapter 16 | e-Bank Authentication .....                | 132 |
| 16.1       | Background .....                           | 132 |
| 16.2       | Counter Business .....                     | 133 |
| 16.3       | Business Layer .....                       | 134 |
| 16.4       | Basic Technology .....                     | 135 |
| 16.5       | Business at ATM .....                      | 136 |
| 16.6       | Communication Between ATM and Portal ..... | 137 |
| 16.7       | The Advantages .....                       | 138 |
| Chapter 17 | e-Bill Authentication .....                | 140 |
| 17.1       | Bill Authentication Network .....          | 140 |
| 17.2       | Main Technologies .....                    | 141 |
| 17.3       | Application for Bills .....                | 141 |
| 17.4       | Circulation of Bills .....                 | 142 |
| 17.5       | Verification of Check .....                | 143 |

## **Part Seven Logistics Authentication**

|            |                                           |     |
|------------|-------------------------------------------|-----|
| Chapter 18 | e-Tag Authentication .....                | 146 |
| 18.1       | Background .....                          | 146 |
| 18.2       | Main Technology .....                     | 147 |
| 18.3       | Embodiment ( I ) .....                    | 148 |
| 18.4       | Embodiment ( II ) .....                   | 150 |
| Chapter 19 | e-Wallet Authentication .....             | 151 |
| 19.1       | Two Kinds of Authentication Concept ..... | 151 |
| 19.2       | System Configuration .....                | 153 |
| 19.3       | Tag Structure .....                       | 154 |
| 19.3.1     | Structure of Data Region .....            | 154 |