

## <<CPK公钥体制与标识鉴别>>

### 图书基本信息

书名：<<CPK公钥体制与标识鉴别>>

13位ISBN编号：9787121174858

10位ISBN编号：7121174855

出版时间：2012-7

出版时间：电子工业出版社

作者：南相浩

页数：316

字数：537000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<CPK公钥体制与标识鉴别>>

### 内容概要

本书讨论了未来“网际安全”的关键技术——基于标识鉴别的可信系统，也讨论了与此相关的自证性公钥体制、信任逻辑，以及信任逻辑在可信接入、可信计算、可信交易、可信物流、网络管理中的应用，以及在互联网和物联网构成的网际空间中建立互信的基本技术，也讨论了新一代信息安全的概念和下一代绿色网络安全的发展方向

# <<CPK公钥体制与标识鉴别>>

## 书籍目录

### Contents

#### Part One Authentication Technology

##### Chapter 1 Basic Concepts

- 1?1 Physical World and Digital World
- 1?2 A World with Order and without Order
- 1?3 Self-assured Proof and 3rd Party Proof
- 1?4 Certification Chain and Trust Chain
- 1?5 Centralized and Decentralized Management
- 1?6 Physical Signature and Digital Signature

##### Chapter 2 Authentication Logics

- 2?1 Belief Logic
    - 2?1?1 The Model
    - 2?1?2 The Formulae
    - 2?1?3 The Characteristics of Belief Logic
  - 2?2 Trust Logic
    - 2?2?1 Direct Trust
    - 2?2?2 Axiomatic Trust
    - 2?2?3 Inference Trust
    - 2?2?4 Behavior Based Trust
    - 2?2?5 Characteristics of Trust Logic
  - 2?3 Truth Logic
    - 2?3?1 The Needs of "Pre-proof"
    - 2?3?2 Entity Authenticity
    - 2?3?3 The Characteristics of Truth Logic
  - 2?4 Authentication Protocols
    - 2?4?1 Standard Protocol
    - 2?4?2 CPK Protocol
  - 2?5 Authentication Systems
    - 2?5?1 PKI Certification System
    - 2?5?2 CPK Authentication System
- ##### Chapter 3 Identity Authentication
- 3?1 Communication Identity Authentication
  - 3?2 Software Identity Authentication
  - 3?3 Electronic Tag Authentication
  - 3?4 Network Management
  - 3?5 Holistic Security
- #### Part Two Cryptosystems
- ##### Chapter 4 Combined Public Key (v6?0)
- 4?1 Introduction
  - 4?2 Mapping Functoin
  - 4?3 Computation of Keys
    - 4?3?1 Computation of Identity?key
    - 4?3?2 Computation of Separating?key
    - 4?3?3 Computation of General?key
    - 4?3?4 Computation of District?key

<<CPK公钥体制与标识鉴别>>

4?4Digital Signature and Key Delivery

4?4?1Digital Signature

4?4?2Key Delivery

4?5Security

4?6Conclusion

Chapter 5Cryptosystem and Authentication

5?1New Requirements for Cryptosystem

5?2Development of Cryptosystems

5?3Identity Authentication Schemes

5?3?1Identity Authentication with IBC

5?3?2Identity Authentication with CPK

5?3?3Identity Authentication with PKI

5?3?4Identity Authentication with IB?RSA

5?3?5Identity Authentication with mRSA

5?3?6Comparison of Schemes

5?4Key Delivery Schemes

5?4?1IBE Key Delivery

5?4?2CPK Key Delivery

5?4?3Other Key Delivery Schemes

5?4?4Performance Comparison

5?5Discussion on Trust Root

Chapter 6Bytes Encryption

6?1Coding Structure

6?1?1Permutation Table (disk)

6?1?2Substitution Table (subst)

6?1?3Key Structure

6?2Working Flow

6?2?1Given Conditions

6?2?2Key Derivation

6?2?3Data Expansion

6?2?4Compound of Data and Key

6?2?5Left Shift Accumulation

6?2?6Permutation

6?2?7Right Shift Accumulation

6?2?8Data Concentration

6?2?9Single Substitution

6?2?10Compound of Data and Key

6?3Security Analysis

Part ThreeCPK System

Chapter 7CPK Key Management

7?1CPK Key Distribution

7?1?1Authentication Network

7?1?2Communication Key

7?1?3Classification of Keys

7?2CPK Signature

7?2?1Digital Signature and Verification

7?2?2Signature Format

<<CPK公钥体制与标识鉴别>>

- 7?3CPK Key Delivery
- 7?4CPK Data Encryption
- 7?5Key Protection
- 7?5?1Password Verification
- 7?5?2Password Change
- Chapter 8CPK?chip Design
- 8?1Background
- 8?2Main Technology
- 8?3Chip Structure
- 8?4Main Functions
- 8?4?1Digital Signature
- 8?4?2Data Encryption
- Chapter 9CPK ID?card
- 9?1Background
- 9?2ID?card Structure
- 9?2?1The Part of Main Body
- 9?2?2The Part of Variables
- 9?3ID?card Data Format
- 9?4ID?card Management
- 9?4?1Administrative Organization
- 9?4?2Application for ID?card
- 9?4?3Registration Department
- 9?4?4Production Department
- 9?4?5Issuing Department
- Part FourSoftware Authentication
- Chapter 10Software ID Authentication
- 10?1Technical Background
- 10?2Main Technology
- 10?3Signing Module
- 10?4Verifying Module
- 10?5The Feature of Code Signing
- Chapter 11Windows Code Authentication
- 11?1Introduction
- 11?2PE File
- 11?3Mini?filter
- 11?3?1NT I/O Subsystem
- 11?3?2File Filter Driving
- 11?3?3Mini?filter
- 11?4Code Authentication of Windows
- 11?4?1The System Framework
- 11?4?2Characteristics Collecting
- 11?5Conclusion
- Chapter 12Linux Code Authentication
- 12?1General Description
- 12?2ELF File
- 12?3Linux Security Module (LSM) Framework
- 12?4Implementation

<<CPK公钥体制与标识鉴别>>

Part Five Communication Authentication

Chapter 13 Phone Authentication

13?1 Main Technologies

13?2 Connecting Procedure

13?3 Data Encryption

13?4 Data Decryption

Chapter 14 SSL Communication Authentication

14?1 Layers of Communication

14?2 Secure Socket Layer (SSL)

14?3 Authenticated Socket Layer (ASL)

14?4 ASL Working Principle

14?5 ASL Address Authentication

14?6 Comparison

Chapter 15 Router Communication Authentication

15?1 Principle of Router

15?2 Requirements of Authenticated Connection

15?3 Fundamental Technology

15?4 Origin Address Authentication

15?5 Encryption Function

15?5?1 Encryption Process

15?5?2 Decryption Process

15?6 Requirement of Header Format

15?7 Computing Environment

15?7?1 Evidence of Software Code

15?7?2 Authentication of Software Code

15?8 Conclusion

Part Six?Commerce Authentication

Chapter 16e?Bank Authentication

16?1 Background

16?2 Counter Business

16?3 Business Layer

16?4 Basic Technology

16?5 Business at ATM

16?6 Communication Between ATM and Portal

16?7 The Advantages

Chapter 17e?Bill Authentication

17?1 Bill Authentication Network

17?2 Main Technologies

17?3 Application for Bills

17?4 Circulation of Bills

17?5 Verification of Check

Part Seven Logistics Authentication

Chapter 18e?Tag Authentication

18?1 Background

18?2 Main Technology

18?3 Embodiment ( )

18?4 Embodiment ( )

<<CPK公钥体制与标识鉴别>>

Chapter 19 The Design of Mywallet(v1.0)

19.1 Two Kinds of Authentication Concept

19.2 System Configuration

19.3 Tag Structure

19.3.1 Structure of Data Region

19.3.2 Structure of Control Region

19.4 Tag Data Generation and Authentication

19.4.1 KMC

19.4.2 Enterprise

19.4.3 Writer and Reader

19.5 Protocol Design

19.6 Conclusion

Part Eight Stored File Authentication

Chapter 20 Storage Authentication

20.1 Security Requirements

20.2 Basic Technology

20.3 File Uploading Protocol

20.4 File Downloading Protocol

20.5 Data Storing

20.5.1 Establishment of Key File

20.5.2 Storage of Key File

20.5.3 Documental Database Encryption

20.5.4 Relational Database Encryption

Chapter 21 Secure File Box

21.1 Background

21.2 System Framework

21.3 Features of the System

21.4 System Implementation

Chapter 22 Classification Seal Authentication

22.1 Background Technology

22.2 Main Technologies

22.3 Working Flow

22.4 Embodiment

22.5 Explanation

Part Nine Moving Data Authentication

Chapter 23 e-Mail Authentication

23.1 Main Technologies

23.2 Sending Process

23.3 Receiving Process

Chapter 24 Digital Right Authentication

24.1 Technical Background

24.2 Main Technologies

24.3 Manufacturer's Digital Right

24.4 Enterprise's Right of Operation

24.5 Client's Right of Usage

Part Ten Network Authentication

Chapter 25 Pass Authentication

<<CPK公钥体制与标识鉴别>>

- 25?1Background
- 25?2Working Principles
- 25?3The Diagram of Gate?guard
- 25?4Gate?guard for Individual PC
- 25?5Guarding Policy
- Chapter 26Address Authentication
  - 26?1Background
  - 26?2Main Problems
  - 26?3Technical Approach
    - 26?3?1CPK Cryptosystem
    - 26?3?2New Routing Protocol
    - 26?3?3Computing Environment
  - 26?4New Prototype of Router
- Part ElevenNew Progress
- Chapter 27Measures against Exhaustion Attack
  - 27?1Exhausting Capability
  - 27?2Basic Analysis
  - 27?3Main Objectives
  - 27?4Technical Approach
  - 27?5Module Design
- Chapter 28CPK Cryptosystem
  - 28?1Introduction
  - 28?2Identity?key
  - 28?3Separating?key
  - 28?4Compound?key
  - 28?5Public and Private Network Key
  - 28?6Digital Signature Protocol
  - 28?7Key Delivery Protocol
  - 28?8Security
  - 28?9Summary
- Chapter 29On?line Key Distribution Protocol
- Chapter 30The Design of Mywallet (v2?0)
  - Abstract
    - 30?1Technical Requirements
      - 30?1?1Two Kinds of Authentication Concept
      - 30?1?2Two Kinds of Authentication Networks
      - 30?1?3Two Kinds of Business Requirements
    - 30?2System Structure
      - 30?2?1Key Distribution
      - 30?2?2Data Structure
      - 30?2?3Controller Structure
    - 30?3Protocol Design
      - 30?3?1Authentication Protocol
      - 30?3?2Decryption and Verification Protocol
      - 30?3?3Encryption and Signature Protocol
  - Summary
- PostscriptFrom Information Security to Gyber Security



<<CPK公钥体制与标识鉴别>>

Appendices

Appendix A

Walk Out of Mysterious "Black Chamber"

Appendix B

Identity Authentication Opening a New Land for Information

Security

Appendix C

Searching for Safe "Silver Bullet"

Appendix D

"Electronic?ID Card" Attracts International Attention

Appendix E

CPK System Goes to the World

Appendix F

Identity Authentication Based on CPK System

Appendix G

CPK Cryptosystem

References

Glossary

Technical Terms

Symbols

## 章节摘录

版权页：插图： Development and spread of horizontally structured networking and end to end transmission technology such as store-forward communication and packet switching raise many new issues to the authentication system. The issues can be summarized as follows: scalability of proof and immediacy of verification in digital signature. Different domains and classifications were defined in the networks in the past but now the horizontal management i.e. the management over the Grid authentication network has become the new trends. To meet the new requirement it must be supported by new technology and theory.

### 7.1.2 Communication Key

Since the authentication network is a grid network with no center, and the modern communication is individualized and end to end communication, on the open public network (such as Internet, telephone network), it is redundant to divide the network or data into function domains (e.g. longitudinal multi-layered division, horizontal internal-external network division), and to divide personnel and data into different classifications (except for private network). Despite all that, in view of the actual situation of coexistence of private network and public network, it is acceptable to remain function domain division of keys and registration classification of personnel. Communication key is a main parameter variable that ensures communication between the communicating parties. The keys are divided into symmetric keys and asymmetric keys.

- 1) Symmetric Key: A common key shared by both communicating parties.
- 2) Asymmetric Key: The decryption key is owned by the designated party.

### 7.1.3 Classification of Keys

In generally, there is no need to define different classifications for the communication network and computer facilities in public network. It is the same as above mentioned authentication network. But if the keys are used in file management then files may be classified different levels to realize different encryption. The keys are classified by roles and domain. Role is divided into

- 1) System administrator
- 2) Senior employees
- 3) Mid-level employees
- 4) General employees
- 5) Customers

Domain is divided into

- 1) Global domain
- 2) District domain

Different keys are distributed to different classes and domain for enabling different access control.

## <<CPK公钥体制与标识鉴别>>

### 编辑推荐

《CPK公钥体制与标识鉴别(英文)》讨论了新一代信息安全的概念和下一代绿色网络安全的发展方向，[《CPK公钥体制与标识鉴别\(英文\)》](#)适合网络技术方面的教授和研究人员做为参考文件，也适合学生，工程师和全部对网络技术感兴趣的人士阅读。

<<CPK公钥体制与标识鉴别>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>