

CPK

标识认证

Identity Authentication based on CPK

南湘浩 著

Name internet
Password *****



国防工业出版社

National Defense Industry Press

CPK 标识认证

Identity Authentication based on CPK

南湘浩 著



国防工业出版社

• 北京 •

图书在版编目(CIP)数据

CPK 标识认证/南湘浩著, —北京:国防
工业出版社, 2006. 10
ISBN 7-118-04310-9

I. C... II. 南... III. 计算机网络—安
全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2005)第 161051 号

※

国防工业出版社 出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100044)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 850×1168 1/32 印张 7 1/4 字数 181 千字

2006 年 10 月第 1 版第 1 次印刷 印数 1—4000 册 定价 35.00 元

(本书如有印装错误, 我社负责调换)

国防书店: (010)68428422

发行邮购: (010)68414474

发行传真: (010)68411535

发行业务: (010)68472764



南湘浩，解放军某部研究员；解放军信息工程大学兼职教授、博士生导师；北京大学计算机科学技术系兼职教授；中国计算机学会理事、信息保密专业委员会顾问；中国人民银行信息安全专家组成员；中国民生银行信息安全技术顾问。长期从事信息安全的理论研究。

曾获国家科技进步二等奖、三等奖及军队科技进步一等奖、二等奖。著有《网络安全技术概要》。

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分,又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展,加强社会主义物质文明和精神文明建设,培养优秀科技人才,确保国防科技优秀图书的出版,原国防科工委于1988年初决定每年拨出专款,设立国防科技图书出版基金,成立评审委员会,扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是:

1. 在国防科学技术领域中,学术水平高,内容有创见,在学科上居领先地位的基础科学理论图书;在工程技术理论方面有突破的应用科学专著。
2. 学术思想新颖,内容具体、实用,对国防科技和武器装备发展具有较大推动作用的专著;密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。
3. 有重要发展前景和有重大开拓使用价值,密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。
4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作,负责掌握出版基金的使用方向,评审受理的图书选题,决定资助的图书选题和资助金额,以及决定中断或取消资助等。经评审给予资助的图书,由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就,积累和传播科技知识的使命。在改革开放的新形势下,原国防科工委率先设立出版基金,扶持出版科技图书,这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物,是对出版工作的一项改革。因而,评审工作需要不断地摸索、认真地总结和及时地改进,这样,才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授,以及社会各界朋友的热情支持。

让我们携起手来,为祖国昌盛、科技腾飞、出版繁荣而共同奋斗!

国防科技图书出版基金
评审委员会

国防科技图书出版基金 第五届评审委员会组成人员

主任委员 刘成海

副主任委员 王 峰 张涵信 张又栋

秘 书 长 张又栋

副 秘 书 长 彭华良 蔡 镭

委 员 (按姓名笔画排序)

于景元 王小谟 甘茂治 刘世参

杨星豪 李德毅 吴有生 何新贵

佟玉民 宋家树 张立同 张鸿元

陈冀胜 周一宇 赵凤起 侯正明

常显奇 崔尔杰 韩祖南 傅惠民

舒长胜

前 言

随着网络发展和网上业务的发展,信息安全的内容也跟着发生变化和扩展。网络由封闭的计算机网络发展为开放的互联网络,业务由简单的数据通信,发展为以网上交易和事务处理为主要内容的新一代安全:网络世界安全(Syber Security)。交易(事务)的基本要求是可信性,为此,要构建可信认证系统为交易(事务)提供鉴别性证明、负责性证明等可信性证明。

在认证系统中最核心的问题是密钥管理问题,因为密钥不仅用于密钥交换,也用于数字签名;不仅提供鉴别性服务,也提供负责性服务,也可用来划定安全域,提供逻辑隔离技术手段。网络世界认证系统的密钥管理需要解决两个课题:一是密钥管理的规模化,二是基于标识的密钥分发。

组合公钥 CPK(Combined Public Key)算法,以很小的资源,生成大规模密钥,为认证系统的芯片化、代理化创造了条件。组化算法开创了密钥管理的新路,是解决规模化难题的必由之路。但是这种体制容易受到共谋攻击的威胁,因此私钥的保护成了新的关键课题。根据屈延文教授《软件行为学》理论,将代理和活性参数等技术引用到私钥的保护上,并开创了代理和密码技术相结合的新路。

CPK 认证系统将认证协议扩充为四个主要协议:主体可信认证协议、客体可信认证协议、内容可信认证协议、行为可信认证协议。主体认证包括身份认证在内的标识认证,并实现了多标识认证系统,为一卡通的实际应用提供了很好的技术基础。

经五年多的研究,CPK 算法和认证系统得到了很大改善。在研究过程中先后得到了屈延文教授、陈华平教授、裴定一教授、周

仲义院士、陆浪如教授、利益发博士、管海明高工、沈昌祥院士、蔡吉人院士、何德全院士、吕述望教授、吴世忠博士、安晓龙高工、杜虹研究员等人的鼓励和帮助,北京大学信息安全实验室陈钟教授、唐文博士、博士生关志、陈瑞川、郭文嘉承担了后期的主要开发和研制任务,完成了芯片化、代理化,付出了辛勤的劳动,这里一并表示由衷的谢意。

QNS北京工作室、北京大学信息安全实验室、广东省科技厅、广东省信息产业厅、广东省信息安全产业基地、北京握奇公司、北京密海公司、武汉瑞达公司、武汉大学、北京市科委、北京信息安全产业基地、北京易恒信公司、中兴微电子公司等有关单位,为CPK认证系统的芯片化、代理化、产业化的实现,给予了支持和帮助,作出了很大努力,现已研制出CPKbiult-in芯片和DEMO系统,为实现规模化生产打下了良好基础。

作者

2005年7月北京

目 录

第 1 章 基本概念	1
1.1 新一代安全	1
1.2 物理世界和网络世界	8
1.3 无序世界和有序世界	9
1.4 手写签名和数字签名	10
1.5 生物特征和逻辑特征	13
1.6 自身证明和第三方证明	13
1.7 对称密码和非对称密码	14
1.8 加密算法和鉴别算法	15
1.9 身份鉴别和标识鉴别	16
1.10 CA 证书和 ID 证书	17
1.11 证书链和信任链	18
1.12 强制型和自主型策略	19
1.13 集中式管理和分散式管理	21
1.14 CPK 和 PKI 认证系统	22
第 2 章 认证系统的架构	24
2.1 概况	24
2.2 认证体系	25
2.3 认证网络	31
2.4 密钥管理	35
第 3 章 密钥管理算法	47
3.1 IBE 加密算法	47
3.2 ECC 组合公钥算法	50

3.3	其他密钥组合算法	62
第4章	ID 证书	71
4.1	ID 证书构成	71
4.2	证书体	71
4.3	变量体	73
4.4	证书组成形式	78
第5章	认证协议	81
5.1	基于 ID 证书的主体鉴别协议	81
5.2	基于第三方的主体鉴别协议	83
5.3	数字签名协议	85
5.4	密钥交换协议	86
5.5	口令验证与更换协议	86
5.6	加密协议	88
第6章	运行格式	90
6.1	格式定义	90
6.2	注释	91
6.3	运行特点	92
第7章	电子办公认证系统	94
7.1	电子邮件认证系统	94
7.2	办公手机认证系统	99
第8章	电子银行认证系统	106
8.1	电子银行证书	106
8.2	取款认证流程	109
8.3	转账认证流程	115
8.4	电子票据认证系统	118
第9章	CSK 算法的应用	122
9.1	客户证书	122
9.2	中心证书	123
9.3	中心密钥矩阵的存储	123
第10章	LPK 算法的应用	125

10.1	改造 PKI 的必要性	125
10.2	改造 PKI 的可行性	126
10.3	具体实现方法	127
第 11 章	行为的评分	130
11.1	鉴别行为树	130
11.2	主体鉴别与评分	131
11.3	客体鉴别与评分	132
11.4	行为鉴别与评分	132
11.5	评分汇总与信任体系的建立	133
第 12 章	证书发行机制	135
12.1	密钥管理机构	135
12.2	行政管理	140
第 13 章	美军 CAC 卡	144
13.1	标识管理的目标	144
13.2	CAC 卡的内容	145
13.3	系统构成	145
13.4	CAC 卡的发行过程	147
13.5	过去的 ID 卡和现在 CAC 卡的不同	148
13.6	CAC 卡的启示	149
第 14 章	CPK 基础部件	151
14.1	CPK 功能模块和协议模块	151
14.2	CPK ID 证书	161
第 15 章	CPK 基础应用	168
15.1	CPK 标签防伪	168
15.2	CPK 可信计算	175
15.3	CPK 可信连接	178
15.4	CPK 认证网关	185
15.5	CPK 数字版权	188
15.6	CPK 电子印章	192
第 16 章	基于 CPK 的标识认证	202

16.1	标识认证算法的形成	202
16.2	标识认证与网络秩序	203
16.3	标识认证与可信交易	204
附件 A	PMT 算法	208
附件 B	ATM 机的新旧兼容方案	210
参考文献		214

Contents

Chapter 1 Basic Concepts	1
1.1 The New Generation Security	1
1.2 Physical World and Cyber World	8
1.3 Ordered World and Disordered World	9
1.4 Written Signature and Digital Signature	10
1.5 Physical Feature and Logical Feature	13
1.6 Shelf-Certification and Certification by Third Party	13
1.7 Symmetric or Asymmetric Algorithm	14
1.8 Algorithms for Encryption and Authentication	15
1.9 Authentication of Identities	16
1.10 CA Certificate and ID Certificate	17
1.11 Certificate Chain and Trust Chain	18
1.12 Security Policy or Assurance Policy	19
1.13 Centralized and Decentralized Management	21
1.14 CPK-based and PKI-based Certification System	22
Chapter 2 Profile to Certification System	24
2.1 Introduction	24
2.2 Certification Mechanism	25
2.3 Certification Network	31
2.4 Key Management	35
Chapter 3 Algorithm for Key Management	47
3.1 IBE Encryption Algorithm	47

3.2	ECC Combined Public Key Algorithm	50
3.3	Related Algorithms for Key Management	62
Chapter 4	ID Certificate	71
4.1	Composition of Certificate	71
4.2	Portion of Main Body	71
4.3	Portion of Variables	73
4.4	Certificate Models	78
Chapter 5	Authentication Protocols	81
5.1	Subject Authentication Based on ID	81
5.2	Subject Authentication Based on Third Party	83
5.3	Digital Signature Protocols	85
5.4	Key Exchange Protocols	86
5.5	Password Verification and Updating Protocols ...	86
5.6	Encrypting Protocols	88
Chapter 6	Transmitting Formula	90
6.1	Definition of Formula	90
6.2	Notes	91
6.3	Features of Operation	92
Chapter 7	e-Office Certification System	94
7.1	e-Mail Certification System	94
7.2	Hand Phone Certification System	99
Chapter 8	e-Bank Certification System	106
8.1	e-Bank Certificate	106
8.2	Procedure of Withdraw	109
8.3	Procedure of Transfer	115
8.4	Certificate for e-Cheque	118
Chapter 9	Application of CSK Algorithm	122
9.1	Certificate for Client	122
9.2	Certificate for Center	123
9.3	Storage of Key-Matrix in Center	123

Chapter 10	Application of LPK Algorithm	125
10.1	Necessity of PKI Reform	125
10.2	Feasibility of PKI Reform	126
10.3	Method of PKI Reform	127
Chapter 11	Behavior Evaluation	130
11.1	Authentication Behavior Tree	130
11.2	Subject Authentication and Evaluation	131
11.3	Object Authentication and Evaluation	132
11.4	Behavior Authentication and Evaluation	132
11.5	Scores and Establishment of Trust System	133
Chapter 12	Certificate Issuing Scheme	135
12.1	Key Management Agency	135
12.2	Administration	140
Chapter 13	U. S. DoD CAC System	144
13.1	Aim of ID Management	144
13.2	Composition of Card	145
13.3	Structure of CAC System	145
13.4	Process of Card Issuance	147
13.5	Difference from Old Card	148
13.6	Enlightenment	149
Chapter 14	CPK Basic Components	151
14.1	CPK Modules of Functions and Protocols	151
14.2	CPK ID Certificate	161
Chapter 15	CPK Basic Application	168
15.1	CPK e-Label Protection against Forgery	168
15.2	CPK Trusted Computing	175
15.3	CPK Trusted Connecting	178
15.4	CPK Authenticating Gateway	185
15.5	CPK Digital Right	188
15.6	CPK e-Seal Stamping	192

Chapter16 Identity Certification Based on CPK	202
16.1 The rise of Identity Certification Algorithm ...	202
16.2 Identity Certification and Cyber Order	203
16.3 Identity Certification and Trusted Transaction	204
Appendix A PTM Algorithm	208
Appendix B All-Inclusive Scheme	210
References	214