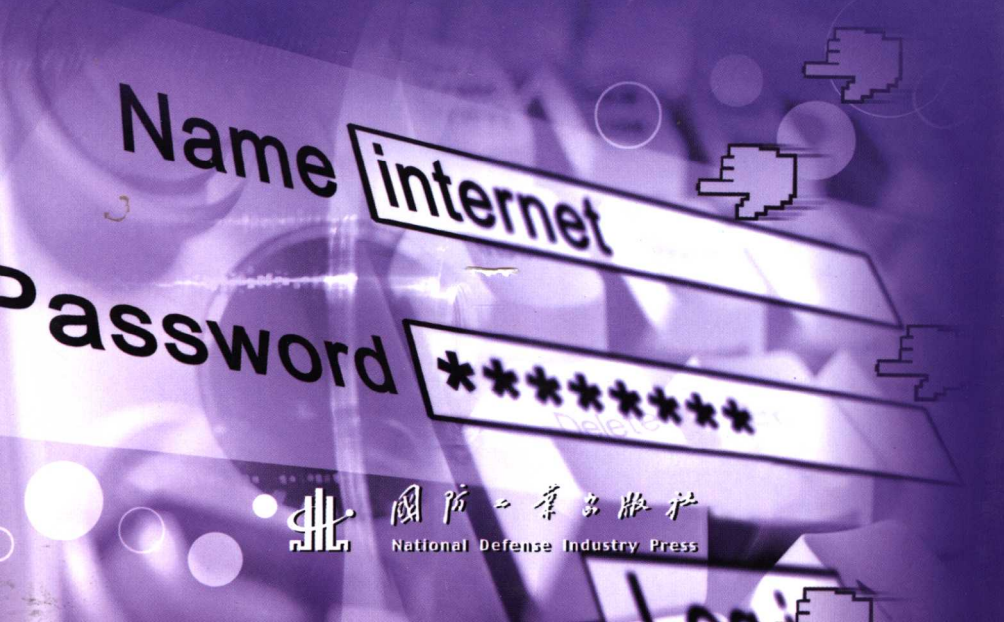
# CPK
# 标识认证

Identity Authentication based on CPK

南湘浩 著




國防工業出版社
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** 7¼ **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

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。组合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、郭文嘉承当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

# Contents