数学与现代科学技术丛书 7

可证明安全算法与协议

张 华 温巧燕 金正平 著

科学出版社

数学与现代科学技术丛书 7

可证明安全算法与协议

张 华 温巧燕 金正平 著

科学出版社
北京

内 容 简 介

近年来，可证明安全算法与协议是信息安全、密码学等研究领域的重要问题之一. 本书以作者及其课题组在该领域多年来的研究成果为主体，结合国内外学者的代表性成果，系统论述了可证明安全密码算法与协议的设计与分析，详细介绍了该研究方向的发展情况，并提出一些与之紧密相关的新研究课题.

全书分四部分，共 17 章. 第一部分(第 1~3 章)系统介绍了密码算法和协议设计中的基础知识；第二部分(第 4~6 章)论述了可证明安全的加密体制；第三部分(第 7~12 章)对数字签名进行了深入研究；第四部分(第 13~17 章)阐述了可证明安全的密钥协商协议及其应用.

本书既可作为对可证明安全算法与协议感兴趣的读者的入门教材，也可作为可证明安全理论研究工作者的参考用书，同时适合密码学、信息安全、数学、计算机及相关学科的高年级本科生、研究生、教师和科研人员阅读参考.

图书在版编目(CIP)数据

可证明安全算法与协议/张华，温巧燕，金正平著. —北京：科学出版社，2012

(数学与现代科学技术丛书; 7)

ISBN 978-7-03-033540-1

Ⅰ. ①可… Ⅱ. ①张… ②温… ③金… Ⅲ. ①密码算法 ②密码协议 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2012) 第 022865 号

责任编辑：王丽平 房 阳 / 责任校对：李 影

责任印制：钱玉芬 / 封面设计：陈 敬

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2012 年 3 月第 一 版 开本: B5(720×1000)

2012 年 3 月第一次印刷 印张: 33 3/4

字数: 656 000

定价: 98.00 元

(如有印装质量问题，我社负责调换)

《数学与现代科学技术丛书》序

当代数学在向纵深发展的同时，被空前广泛地应用于几乎一切领域. 一方面，它与其他学科交汇，形成了许许多多交叉学科(例如，信息科学、计算机科学、系统科学、数学物理、数学化学、生物数学、数学语言学、数量经济学、金融数学、复杂性科学、科学计算等)；另一方面，它又被应用于高新技术的开发(例如，信息安全、信息传输、图像处理、语音识别、网络、海量数据处理、网页搜索、遥测遥感、交通管理、医疗诊断、手术方案、药物检验、商业广告等方面)，成为一些高新技术的核心. 应用数学的这种发展趋势急剧地扩展了数学的疆界，也深刻地改变了数学的面貌.

中国的经济正在迅猛发展，其中的科技含量也与日俱增. 为了提高自主创新能力，我国已经有不少数学工作者投身于这类应用数学的研究中，还有更多的数学工作者则正在密切关注这方面的进展，看好它的前景. 愈来愈多的人希望了解这类应用数学的现状，寻找入门之径.

《数学与现代科学技术丛书》是力图反映这个发展趋势的一套应用数学丛书，它将较全面地向我国读者介绍当今数学在现代科学技术各个领域中应用的状况，通过必要的准备知识，逐步把读者引向相关的研究前沿.

从事交叉学科研究和高新技术开发的应用数学家，除了要精通所需的数学知识外，还必须深入了解其所研究问题的来龙去脉. “建模”是应用数学研究实际问题的关键. 这也是一门数学艺术：从复杂的实际问题中抽象出关键的“量的关系”，使得既能反映出问题的基本特征，又能用现阶段的数学工具加以处理. 有鉴于此，这套丛书的一个特点就是：不但要介绍有关的数学理论和方法，还必须介绍问题的来源与背景、数学建模以及如何运用数学工具来解决实际问题.

本丛书适用于数学及相关专业的大学生和研究生，以及与数学有关的各专业科技工作者.

张恭庆

2009 年 11 月

前　言

随着全球信息化程度的日益提高，信息安全问题已经由个人、团体的隐私与机密保护问题上升为国家的战略性问题. 密码算法和协议是解决网络安全问题最直接、最有效的手段之一，是构建安全信息系统的基本要素. 在计算机网络和通信系统中，通信各方通过采用密码算法和协议实现消息加密、密钥分配、身份与消息认证、行为不可否认和安全电子交易等功能.

可证明安全性理论与技术是一种安全可靠的密码分析方法，它在适当的模型下，把高层的密码算法和协议的复杂安全性归约为底层的极微本原的简单安全性. 它又是一种科学而高效的密码设计方法：其模块化的设计思路使得密码算法和协议的设计人员不再拘泥于极为困难的极微本原的设计，而是直接以极微本原为工具，以形式化的安全性定义为参照，再结合具体的模型来设计密码算法和协议，从而大大提高了设计效率.

加密体制、数字签名和密钥协商是密码算法和协议的核心内容. 加密体制为保证信息的机密性提供了重要的技术手段. 根据密钥的特点，可将加密体制分为对称密钥体制和非对称密钥体制两种. 一般来说，对称密钥体制具有计算量少、效率高等优点，而非对称密钥体制具有无需预共享密钥的优势. 因此，两类加密体制的研究都取得了长足的发展. 与非对称密钥体制的思想类似，数字签名技术利用公私钥对实现了对消息的完整性认证、消息发送者身份的认证和不可抵赖性等功能. 数字签名的研究是密码技术发展的重要分支之一，受到学术界与产业界的广泛关注. 在此基础上，为满足实现需求的特殊功能，各种具有特殊功能的数字签名方案 (如盲签名、代理签名、签密等) 也相继出现，目前已取得了一系列的研究成果. 密钥协商协议允许通信的双方或多方在一个不安全的开放网络上联合建立秘密密钥，是实现保密通信的重要技术手段之一. 安全高效的密钥协商协议可用于构建安全、复杂、高层的安全协议，与数字签名等密码技术结合可以形成具有广泛应用价值的密码算法，在密钥管理、数据安全、保密通信以及各种电子商务中具有不可低估的应用价值. 关于密钥协商协议的设计与分析研究也得到了蓬勃发展，适用于不同应用场景需求的密钥协商协议不断涌现.

近年来，可证明安全密码算法和协议的研究一直很活跃，出现了一系列的学术论文和博士、硕士学位论文，取得了丰硕的研究成果和较显著的发展. 但从目前的研究情况看，可证明安全密码算法和协议的许多问题还值得进一步研究.

本书旨在系统论述现代密码学中可证明安全密码算法和协议，以作者及其课题

组多年的研究成果为重点, 汇集了国内外学者在这方面的重要研究成果. 对相关领域的理论工作者、研究生以及高年级本科生的专业课题研究有一定的参考价值.

全书共分四部分. 第一部分重点论述了可证明安全理论以及密码算法和协议的基础理论. 第二部分对加密体制进行了研究, 除了介绍经典的加密算法外, 重点介绍了典型的可证明安全加密体制. 第三部分重点介绍了一系列可证明安全的数字签名及具有特殊功能的数字签名方案. 第四部分重点介绍了可证明安全的密钥协商协议及其应用. 作为专著, 本书集中论述了课题组及国内外的相关成果, 对密码学基础知识只做简单的介绍, 感兴趣的读者可参考其他相关书籍.

作者对课题组成员李文敏博士、郭瑞博士、孙海燕博士、徐洁硕士、张敏硕士等给予的密切配合, 以及北京邮电大学网络与交换技术国家重点实验室网络安全研究中心全体老师和学生的支持表示感谢. 本书第二部分由郭瑞博士协助完成, 第四部分由李文敏博士、孙海燕博士协助完成, 再次向他们深表谢意.

最后, 本书的出版得到了以下项目的资助: 国家自然科学基金项目 (编号: 60873191, 60821001, 60903152)、中央高校基本科研业务费专项资金资助项目 (编号: BUPT2011YB01, BUPT2011RC0505, BUPT2011RCZJ15) 等, 在此特别表示感谢.

由于作者水平有限, 时间仓促, 书中不妥之处在所难免, 恳请读者指正.

作　者

2011 年 6 月于北京

目　　录

第二部分　加 密 体 制

第三部分 数 字 签 名

第四部分　密 钥 协 商

第一部分　基础知识