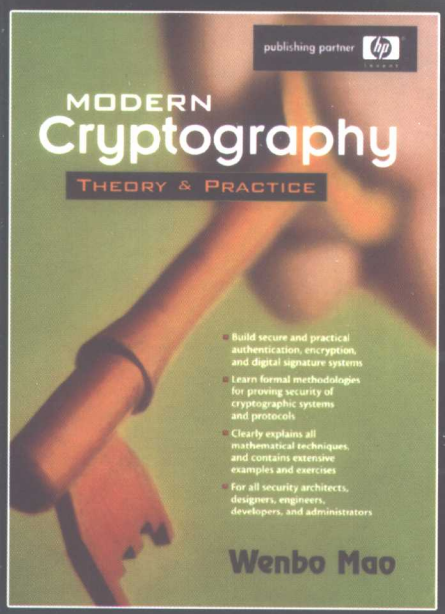
国外计算机科学教材系列

现代密码学理论与实践

Modern Cryptography: Theory and Practice



[英] Wenbo Mao 著
王继林 伍前红 等译
王育民 姜正涛 审校

PRENTICE HALL PTR
PHEI
電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

内容简介

很多密码方案与协议，特别是基于公钥密码体制的，有一些基础性或所谓的“教科书式密码”版本，这些版本往往是很多密码学教材所包含的内容。本书采用了一种不同的方式来介绍密码学——更加注重适于应用的密码学方面。它解释了那些“教科书式密码”版本仅适合于理想世界的原因，即数据是随机的、坏人的表现不会超越预先的假定。本书通过展示“教科书式密码”版本的方案、协议和系统在各种现实应用场合存在着很多攻击，来揭示“教科书式密码”版本在现实生活中的不适用性。本书有选择性地介绍了一些实用的密码方案、协议和系统，其中多数已成为了标准或事实上的标准，对其进行了详细的研究，解释了其工作原理，讨论了其实际应用，并且常会以建立安全性形式证明的方式来考察它们的强（实用）安全性。另外，本书还完整地给出了学习现代密码学所必备的理论基础知识。

本书可作为高学院校计算机专业研究生或高年级本科生的教材，也可供密码安全架构师、工程人员、开发人员以及管理人员参考。

版权贸易合同登记号　图字：01-2003-6231

图书在版编目（CIP）数据

现代密码学理论与实践/（英）毛文波著；王继林等译. -北京：电子工业出版社，2004.7
（国外计算机科学教材系列）
书名原文：Modern Cryptography: Theory and Practice
ISBN 7-5053-9925-X

Ⅰ.现...　Ⅱ.①毛...　②王...　Ⅲ.密码-理论-教材　Ⅳ. TN918.1

中国版本图书馆CIP数据核字（2004）第059006号

责任编辑：谭海平
印　　刷：北京智力达印刷有限公司
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
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：31.25　字数：800千字
印　　次：2004年7月第1次印刷
定　　价：49.00元

凡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。联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

序　言

2003年10月，本书英文版刚出版两个多月后，我收到西安电子科技大学（西电）王育民教授发来的电子邮件，说西安电子科技大学已着手本书的中文翻译工作。半年后的今天，高质量的全书中文译稿已摆在我面前！我非常感谢王老师及参加本书翻译的全体同仁们的辛勤工作，使本书能如此快地与中文读者见面！

应王老师之邀为中译本作序，我便想写上几句适宜于对我的中文读者们表达的我写此书之原动机。取决于密码算法及协议应用环境之敌意性，本书着重强调了应用（特别是商用）密码学研究与开发的几项原则：走标准化、公开性及在极端强化了的安全概念下获得形式可证安全的道路。这几项原则或许可以用孙子的名训“知己知彼，百战不殆”来概括。我想其中标准化、公开性可以解释为“知己”，而追求极端强化安全概念下的可证安全则是向着“知彼”的境界升华。若对孙子名训做更通俗点的诠释，则我认为在商用密码学上，我们可以说：“谁是我们的朋友，谁是我们的敌人，这个问题也是商用密码学的首要问题”。为了能与外部朋友们进行安全的商务交易，我们不可以没有算法的标准化；为了在极大程度上限制暗藏（特别是内部）的敌人，我们需要算法的公开性；而达到强安全概念下的可证明安全则为走标准化、公开性道路提供高信度的保障。

毛文波

2004年3月于西安

译 者 序

随着人类进入信息化社会，信息安全已成为人们在信息空间中生存与发展的重要保证条件，著名未来学家托夫勒曾说过，在信息时代“谁掌握了信息，控制了网络，谁就将拥有整个世界”。因此，密码学和信息安全技术在最近二十多年来，越来越受到人们的重视，特别是“911”事件以来，信息安全业已成为各国政府和有关部门、企业、机构的重要议事内容。

现代密码学形成于20世纪70年代，其重要标志有两个，一是美国制定并于1977年1月15日批准公布了公用数据加密标准(DES, Data Encryption Standard)；二是公钥密码体制的诞生。这两个事件在密码学史上具有里程碑意义。

DES的出现有两方面的意义，一是算法的标准化，二是密码算法的公开化。标准化的重要性容易为人们所认识，人类在20世纪学到的一件最重要的经验就是技术进步中标准化的作用。标准化提供产品的互操作性，对生产厂家和使用者都提供了极大的方便，大大降低了成本和提高了推广应用的速度，极大地促进了生产率的提高和技术进步。在密码和安全技术普遍用于实际通信网的过程中，密码算法的标准化是一项非常重要的工作。标准化可以实现规定的安全水平，具有兼容性，在保障安全的互连互通中起关键作用；标准化有利于降低成本、训练操作人员和技术的推广使用。因此各国政府有关部门和国际标准化组织都大力开展标准化的研究和制定工作。

首先我们来看密码算法的标准化问题。支持现代人生存的重要基础设施之一是国家信息基础设施，即NII。在NII中建设国家信息安全基础设施(NISII)具有极其重要的意义，它是保障人民、国家、企业和个人能够在信息空间中生存的重要条件，是发展电子商务的基础。而公用密码算法和安全协议标准又是NISII的一个重要组成部分。没有密码算法和安全协议的支持，就无法建立信息空间中的信赖性，就不能支持信息空间中的仲裁机构、保护个人隐私和个人数据的安全保密。作为现代人也就无法在信息空间中生存。如欧盟就出资33亿欧元来制定NESSIE(New European Schemes for Signatures, Integrity, and Encryption，新的欧洲数字签名、完整性和加密方案)。

公用密码算法的标准要不要公开？长期以来，这一直是一个有争议的论题。虽然早在100多年以前，1883年荷兰密码学家A.Kerchoff(1835～1903)就给出了密码学的一个基本原则：密码的安全必须完全寓于密钥之中。尽管密码学家们大都同意这一看法，但直到制定DES时才首次认真地遵循这一原则。这一做法适应信息化社会发展的需要，是完全正确的。但是，1984年9月美国总统里根签署了145号国家安全决策令(NSDD)，命令NSA着手发展新的加密标准，并且规定算法不再公开，认为算法公开不利于美国国家的安全。到1993年4月，克林顿政府公布了一项建议的加密技术标准，称做密钥托管加密标准(EES, Escrowed Encryption Standard)。EES不仅算法保密，而且每个芯片中的单元(或用户)密钥也在政府完全控制之下。在密码发展史上，DES确定了发展公用标准算法的模式，而EES的制定路线却与DES的背道而驰。EES在美国引起很大争论，由于它对美国公民的隐私权造成威胁而遭到多方面的反对。1995年5月AT&T贝尔实验室的M.Blaze博士在PC机上用45分钟时间使SKIPJACK的LEAF协议失败，伪造ID码获得成功。虽然NSA声称已弥补，但丧失了公众对此体制的信心。1995年7月美国政府宣布放弃用EES来加密数据，重新回到制定DES标准立场，这一耗资几亿美元的计划基本上遭到失败。

1997年1月2日美国NIST着手进行AES(Advanced Encryption Standard)的研究，成立了标准工作室。1997年4月15日讨论了AES的评估标准，开始在世界范围内征集AES的建议算法。1998年8

月 20～22 日经评审选定并公布了 15 个候选算法。1999 年 8 月经评审筛选出 5 个算法，2000 年 10 月 2 日最后确定了以比利时两位密码学家 Proton World International 公司的 Joan Daemen 博士和 Katholeke 大学电机工程系的 Vincent Rijmen 博士所设计的 Rijdeal 算法作为 AES 的标准算法。

方针、政策的正确制定非常关键，它应当符合社会发展的需要，能代表先进的社会生产力，这样才能推动事物的发展。由 DES 到 EES，再到 AES 的曲折历史告诉我们，制定信息化社会所需的公用密码算法标准的正确途径是公开地进行，一是算法要公开，二是方案要公开征集和公开评价。只有这样才能使密码算法的使用者相信用它能够保护自己的隐私和数据的安全、保证他能够在信息空间中公平地参加各类活动而不会遭受欺诈。也只有这样才能使所制定的密码算法标准能够经受住各种攻击，达到所需的安全性。

毛博士在其书的 1.2.6 节中所做有关“民用的密码研究应该采用公开的途径”的论述，是非常正确和重要的。

并非所有人都同意这种看法。有人认为，密码是一把双刃剑，既可以为我所用，也可以为敌所用。应当努力研究和发展密码的可控性理论和技术，以防范我们的密码为敌所用和滥用。这的确是一个重要和值得研究的问题。但是这决不是公用密码不应公开的根据。我们知道，EES 的初衷就是想用它来对付恐怖分子、贩毒集团等犯罪分子，只要这类人采用 EES 的保密终端进行通信，就可以对他们实施实时监听。试想，这些人会如此之傻地跳进为他们设好的陷阱吗？难道他们不会用自行设计的密码来保护他们的关键数据？所以说 EES 不能实现他们预想的目的，倒是成为监听好人通信的工具了。

作为公用密码算法标准 EES 是失败了，但它在密码发展史上也有成功之处。EES 发展了密码可控性理论与技术，大大推进了密钥托管和密钥恢复技术的发展，这类技术在电子商务和电子政务等方面有重要用途。我们在应用密码的各种技术时，一定要分析清楚所在的环境，有些适用于像 Intranet 和 Extranet 环境，有些更适用于 Internet 环境。

其次，我们来看现代密码学赖以发展的环境问题。我们知道，20 世纪 70 年代以前的密码学，包括香农所创建的保密通信的信息理论，讨论的基本问题是抗击被动攻击者对密文的截收和分析。只要设计出在理论和实际上让密码分析者难以破译的密码算法，就能保证信息的安全性。而现代密码学的应用环境是开放的网络环境，除了要对付被动攻击者外，还必须对付开放网络环境中的各种主动攻击者。

如何对付主动攻击者，特别是如何对付那些刁钻的主动攻击者，是现代密码学中最具挑战性的问题。这类攻击者不仅很好地掌握了密码学和信息安全技术方面的知识，而且智商不低，能够充分利用开放网络环境所提供的资源来获取所需的信息，对他们所感兴趣的系统实施攻击。他们不仅会利用密码算法上的各种弱点，而且还能利用协议设计和使用中的各种缺陷。

毛博士在他的书中全力以赴论述如何对付刁钻的主动攻击者。这不仅涉及“教科书式密码”的内容，还要用到现代密码学的一些新理论，特别是安全性的形式证明理论。这本书的重要特色就是全面而又深刻、严谨而又通俗地论述了现代密码学这一极为重要而又很前沿的问题。当今，任何密码算法、协议的设计和相应标准的制定，都不能回避可证明安全性，都必须通过这一理论的严格检验。

毛博士的书以一种全新的方式介绍密码学，首先深刻揭示“教科书式密码”的不安全性和弱点，阐明它们不适于实际应用的理由；而后引入如何将一个密码算法或协议的“原型”改造成为一个能实际用于开放网络环境的安全方案，并给出这类方案安全性的形式证明。书中对于“理想世界”和“现实世界”、“两类攻击者”、“教科书式密码”和“非教科书式或适于应用的密码学”、“密码原

型”和“实用密码方案”、安全协议等的论述是十分精辟的，需要认真体会。因此，本书对于密码和信息安全技术专业的学生以及从事这方面的工作者来说是一本不可多得、值得认真研读的好书。

有关安全性可证明理论，Goldreich 的“Fundations of Crytography”是应当提及的，但这是一本严格而数学化的书，适合于那些有很好数学基础而且要认真研究这一理论的读者。

三十年前，要想找一本密码方面的书并不容易。最近二十多年来，特别是最近十年来，已出版了数以百计的密码学和信息安全技术的书。其中，中文书也已不下百本。这一方面是由于信息安全问题的重要性，另一方面也是由于借助于计算机来编写一本书已不是什么难事。但要写一本有特色、有存在价值的书就绝非易事。我想，当我们读过毛博士这本书以后，就会知道我们为什么要翻译和出版它了。

毛博士能写这样的书与他的经历是分不开的。这里向读者简要介绍毛博士的有关信息。毛博士于 1982 年 7 月获复旦大学应用数学学士学位；1987 年 1 月获北京航空航天大学计算机科学硕士学位；1993 年 7 月获英国格拉斯哥 Strathclyde 大学计算机科学博士学位；1992 年到 1994 年在英国曼彻斯特大学做博士后研究，与 C. Boyd 博士对密码协议和协议形式的分析进行深入研究，做出了贡献。曾在澳大利亚 Technology 学院、Issac Newton Institute 及布里斯托尔大学做访问研究。1994 年 11 月加入 HP 公司做高级技术成员，在英国的布里斯托尔研究实验室的可信赖系统实验室，参加了多项重要的电子商务系统和信息安全系统的设计和开发工作，其中包括欧盟的 CASENET 计划的 HP 部分的领导工作。在密码算法、协议的设计和分析方面进行了广泛而深入的研究，做出了优异成绩。他在重要国际会议和杂志上发表了多篇论文，曾获 IEE 的 The Hartree 奖，是 IEEE、BCS 和 IACR 会员，澳大利亚昆士兰、布里斯托尔、伦敦等大学客座研究员。多个有关密码和信息安全重要国际会议的程序委员会成员和有关杂志的密码和信息安全方面专辑的编辑或顾问组成员。自 2000 年 4 月至今任 HP 公司总工程师、技术领导。

毛博士正在撰写“Cryptographic Protocol”一书，我们期待它早日问世。

参加本书翻译的八位博士生，他们对于所分担部分的内容都比较熟悉，与他们博士论文的研究方向比较接近。翻译的初稿，先两两一组相互校对，然后由姜正涛做仔细的初校，最后由我做全面的校对，有些部分进行了多回合的商榷和订正。各部分分工如下：王继林译前言、目录、图的列表、第 1 章、第 2 章，伍前红译第 4 章、第 18 章、第 19 章、第 20 章，庞辽军译第 3 章、第 10 章，郝艳华译第 5 章、第 7 章，姜正涛译第 6 章、第 8 章，张键红译第 9 章、第 13 章，田海波译第 11 章、第 12 章，陈原译第 14 章、第 15 章、第 16 章、第 17 章。名词索引的初稿由伍前红和王继林译出。他们都认真、负责和按时完成了任务。姜正涛付出最多，他连续工作了三个多月，寒假也在工作；他的英语水平高，汉语语言表达能力强；他工作认真、细心，负责，出色地完成了校对任务。没有这八位同学的努力和合作，就不可能把这本书及时献给中文读者。

毛博士曾仔细地阅读了中译本的初稿，提出不少修改意见，在此表示衷心的感谢！

感谢电子工业出版社在我们翻译本书时所给予的协助和支持，以及编辑们的辛勤工作！

我们衷心希望这本书的中文版能在我国的密码和信息安全技术领域发挥它应有的作用。虽然我们做了努力，但有些地方的译文未必能正确表达出原书的意思，甚至会有错误。敬请读者批评和指正。

西安电子科技大学　王育民

ymwang@xidian.edu.cn

2004 年 3 月 18 日

前　言

我们的社会已经进入了一个崭新时代，传统的商务活动、事务处理以及政府服务已经或越来越多地将要通过开放的计算机和通信网，如 Internet，特别是基于万维网的工具来实施和提供。对在世界各个角落的人来说，在线工作有着“随时可得”的巨大优点。下面是一些可以或即将可以在线完成的事例：

> 银行业务、账单支付、家中购物、股票交易、拍卖、税收、赌博、小额支付(例如按下载支付)、电子身份、对医药记录的在线访问、虚拟保密网、安全数据存档与恢复、文件的挂号递送、敏感文件的公平交换、公平合同签署、时戳、公正、选举、广告、授权、订票、交互式游戏、数字图书馆、数字权限管理、盗版追踪等。

只有在开放网络能提供安全通信的条件下，上述诱人的商务活动、事务处理以及服务才能实现。而要保证在开放网络中通信的安全性，一个有效的解决办法就是利用密码技术。加密、数字签名、基于口令的用户认证是实现安全通信的一些最基本的密码技术。但是，正如我们将在本书中多次看到的那样，即使是最基本的密码技术，在应用中也存在令人惊讶的难以捉摸和严重的安全性问题。而且对很多像上一段所列出的“想像的”应用来说，这些基本的密码技术是不够的。

越来越复杂的电子商务、事务处理和服务形式[①]，对在开放的网络中实现安全通信的需求正迅速增加。对能够进行设计、开发、分析和维护信息安全系统和密码协议的信息安全方面的专业人员的需求量正日益增大。这些专业人员可能是从 IT 系统的管理员、信息安全工程师和有安全要求的软/硬件系统产品的开发人员，直到密码学家。

在过去的几年里，作者作为在英国布里斯托尔 Hewlett-Pachard 实验室信息安全与密码系统方面的一名技术顾问，已经注意到了对信息安全人员需求的持续增长和现有专业人员明显短缺这一失调现象。结果，很多在密码或信息安全方面缺少适当训练的面向应用的工程师，由于应用的需要，不得不“挽起袖子”成了安全系统或密码协议的设计者或者开发者。尽管这是不争的事实，但要设计密码系统和协议，即便对密码学专家来说，也不是件容易的事。

作者的工作性质允许他有机会审查很多信息安全系统和密码协议，其中有一些就是由“挽袖子”工程师所提出和设计的，而且是用在一些重要的实用上。在很多场合，作者看到了这些系统中存在有所谓的“教科书式密码”的特征，这是把很多密码学教科书中一般都介绍的密码算法直接拿来应用的结果。利用基本的公钥加密算法(如 RSA)直接对口令(一个不大的秘密数)进行加密就是“教科书式密码”的一个典型例子。教科书式密码以“不可忽略的概率”在重要应用场合下的出现引起了作者的担心。看来，教科书式密码的一般危害，尚没有被那些针对重要现实应用来设计和开发信息安全系统的许多人所意识到。

---

① Gartner Group 预计，欧盟的 B2B 和 B2C 电子商务税收在 2004 年将以 0.7 的概率达到 2.6 万亿美元，是 2000 年的 28 倍[5]。eMarketer[105]也报告，美国金融机构在 2002 年因电子身份问题被窃的损失为 140 亿美元，并预计每年将会以 29% 的速度增加。

考虑到对信息安全专业人才的大量需求，并相信专业人才的密码学知识不能仅囿于教科书式密码学，作者写了这本“非教科书式密码学”教材。本书致力于：

- 在强调“非教科书式”的情况下，广泛介绍有关密码算法、方案和协议。
- 通过展示对这类系统的大量攻击和总结典型的攻击技术，来说明“教科书式密码”的不安全性。
- 通过对标准的关注，为密码系统和协议的设计、分析与实施提供原理和指导原则。
- 研究严格建立密码系统和协议的强而实用安全性表示的形式化技术和方法。
- 为希望系统了解这一领域的读者精心选取学习现代密码学必备的理论素材。

本书范围

在过去的30年里，现代密码学的研究可谓突飞猛进，其研究领域非常广泛和深入。本书集中讨论一个方面的问题：对以其强安全性能明确建立起来的实用密码方案和协议进行介绍。

本书分为6部分：

第一部分 这一部分共有两章内容(第1章，第2章)，是本书和密码学与信息安全的入门性介绍。其中第1章以解决一个微妙的通信问题为开场白，来阐述密码学的效用。本章将给出一个在电话上实现公平掷币的简单密码协议(本书的第一个协议)并对其进行讨论。然后对要研究领域的文化和“贸易”进行介绍。第2章使用一系列的简单认证协议，来表明该领域的一个不幸的事实：缺陷处处存在。

作为入门性介绍，这一部分是为想进入该领域的新手写的。

第二部分 这一部分介绍学习本书必备的数学背景知识，它包含4章内容(第3章～第6章)。只想“知其然”，即了解如何使用实用密码方案和协议的读者，可以跳过这一部分而基本上不影响大多数后续章节的阅读。要想知道“所以然”，即为什么这些方案和协议具有强安全性的读者将会发现，这里给出的数学背景知识是足够的。当我们揭示方案和协议的工作原理，指出其中的一些方案和协议是不安全的，或者论述别的协议和方案是安全的时候，我们就能在这里找到相应的理论根据。

这一部分也可作为学习现代密码学理论基础的系统背景知识。

第三部分 这部分也有4章内容(第7章～第10章)，介绍提供保密和数据完整性保护最基本的密码算法和技术。其中第7章是对称加密方案，第8章是非对称加密技术，第9章讨论的是，在数据是随机的理想条件下，利用基本通用的非对称密码函数所拥有的一个重要的安全特性。最后的第10章是数据完整性技术。

由于这里介绍的是最基本的方案和技术，其中多数属于“教科书式密码”，因而是不安全的。在介绍这些方案的同时，也给出不少相应的攻击，并明确阐述了告诫注释。对于那些不想对实用密码和它们的强安全性概念做深入研究的实际工作人员，教科书式密码部分也仍会就教科书式密码的不安全性向他们提出明确的预警信号。

第四部分 这部分有3章内容(第11章～第13章)，介绍应用密码学和信息安全中一个重要的概念——认证。这些章节的研究范围很广，第11章介绍技术背景、原理、一系列的基础协议和标准，以及常规的攻击技术和防护措施。第12章是对四个著名的认证协议系统在现实应用案例的研究。第13章介绍特别适合于开放系统的有关最新技术。

企业中信息安全系统的管理者、安全产品的软/硬件开发商们将会发现这一部分对他们是非常有用的。

第五部分 这部分有4章内容(第14章～第17章),对公钥密码技术(加密、签名和签密)的强(实用)安全性概念进行严格的形式化处理,并给出认证协议的形式化分析方法。第14章介绍强安全性概念的形式化定义,接着的两章是和第三部分教科书式密码方案相对的实用密码方案,具有形式化建立起(即明确推理)的强安全性。最后,第17章对在第四部分尚未进行分析的认证协议,给出其形式化的分析方法和技术。

第六部分 这是本书的最后一部分,包括两个技术章节(第18章～第19章)和一个简短的评述(第20章)。其主要的技术章节,第18章,介绍了一类被称为零知识协议的密码协议。这类协议能提供一种重要的安全性业务,它为"想像中"的各种电子商务和事务处理应用所必需,在对所声明的内容保持严格保密性的情况下,对一个秘密数所宣称的性质进行证实(例如,符合商业上的需求)。这部分要引入零知识协议,说明了在各种现实应用中对特定安全性需求的多样性。这种多样性超越了机密性、完整性、认证和不可否认性。在本书的最后一个技术章节(第19章)中,我们将解决本书一开始介绍的协议中的遗留问题——实现"通过电话公平掷币"。最后的实现协议不但在效率上适宜实用,而且也明确地建立起了强安全性。

不用说,对每一个实用密码协议或方案的描述,都是要先给出与之相应的教科书式密码不适用的原因。我们总是以给出相应存在的攻击来说明原因,就相应的攻击而言,这些方案和协议往往存在某些微妙之处。另外,一个实用密码协议和方案的描述,也必是以其所宣称的必须包含的强(实用)安全性成立的分析来结束。因而,本书一些部分不可避免地要包含有数学和逻辑推理、为明示和对付攻击所需的归纳和变换。

实用密码学并不是一个轻易驾驭或者稍稍读读就能掌握的论题。尽管如此,本书并不是一本仅为专业密码学家所感兴趣的高深研究课题的书。这里所介绍的东西对密码学家来说都是已知的和相当基本的。作者相信,在有充足的解释、实例、足够的数学背景知识和参考材料的情况下,这些东西完全能被非专业人士理解。

本书针对的读者对象为:

- 已经或即将完成计算机、信息科学、应用数学第一学位课程并计划从事信息安全行业的学生。对他们来说,本书可以作为应用密码学的高级教程。
- 在高科技公司从事信息安全系统设计和开发的安全工程师。如果我们说在科学研究计划中,教科书式密码所产生的危害不是很大的话,至多是出现一种令人尴尬的场面,那么在信息安全产品中使用教科书式密码将会造成严重损失。因此对这类读者来说,了解教科书式密码在现实中的不适用性是非常必要的。而且,这类读者应该对隐藏在实用方案和协议下的安全原理有很好的理解,以便能正确地使用这些方案和原理。第II部分所给出的自足的数学基础材料使得本书很适合这类读者自学。
- 对企业信息安全系统管理人员或者生产安全产品的软/硬件开发商这类读者来说,第I部分是简单而基本的文化和"商务"方面的培训教程,第III部分和第IV部分是一个适当裁减的密码学和信息安全知识集。这三部分包含有很多基本的密码方案和协议,以

及很多对应的攻击方法和防护措施。这些攻击方法和防护措施能被大多数读者理解，不需要有所谓理论基础的负担。

- 对于刚开始从事密码学或计算机安全方面研究的博士生这类读者来说，将会欣赏一本能包含强安全性概念的形式化处理并对其进行适当和详细解释的书感兴趣。本书将能帮助他们快速深入地进入这一浩瀚的研究领域。对这类人员来说，第 II、IV、V 和 VI 部分构成了一个适当深度的文献综述材料，这将能引导他们找到更进一步的文献，并能帮助他们明确自己的研究课题。
- 本书的适当取舍（如第 1 章、第 2 章、第 3 章和第 6 章）也可以组成适合计算机、信息科学和应用数学大学高年级学生学习用的应用密码学教程。

致谢

非常感谢 Feng Bao、Colin Boyd、Steven Galbraith、Dieter Gollmann、Keith Harrison、Marcus Leech、Helger Lipmaa、Hoi-Kwong Lo、Javier Lopez、John Malone-lee、Cary Meltzer、Christian Paquin、Kenny Paterson、David Pointcheval、Vincent Rijmen、Nigel Smart、David Soldera、Paul van Oorschot、Serge Vaudenay 和 Stefek Zaba。他们花费了大量时间校阅有关章节或全书，并提供了非常有价值的评论、批评和建议，使得本书更加完善。

本书还得益于向下列人士的请教：Mihir Bellare、Jan Camenisch、Neil Dunbar、Yair Frankel、Shai Halevi、Antoine Joux、Marc Joye、Chalie Kaufman、Adrian Kent、Hugo Krawczyk、Catherine Meadows、Bill Munro、Phong Nguyen、Radia Perlman、Marco Ricca、Ronald Rivest、Steve Schneider、Victor Shoup、Igor Shparlinski 和 Moti Yung。

作者还要感谢 Prientice-Hall PTR 的 Jill Harry 和 HP Professional Books 的 Susan Wright，他们鼓励并引导我写作了本书，并在我漫长的写作中提供了技术帮助，感谢 Prientice-Hall PTR 的 Jennifer Blackwell、Robin Carroll、Brenda Mulligan、Justin Somma 和 Mary Sudul 以及 HP Professional Books 的 Walter Bruce 和 Pat Pekary。

还要感谢我在布里斯托尔 Hewlett-packard 实验室的同事们在技术、修辞和管理方面给予的支持，他们是 David Ball、Rachard Cardwell、Liqun Chen、Lan Cole、Gareth Jones、Stephen Pearson 和 Martin Sadler。

作者于英国布里斯托尔

2003 年 5 月

目　录