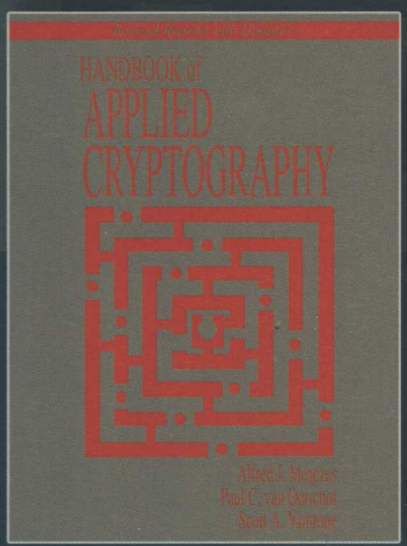
国外计算机科学教材系列

应用密码学手册

Handbook of Applied Cryptography



Alfred J. Menezes
[加] Paul C. van Oorschot 著
Scott A. Vanstone
胡 磊 王 鹏 等译

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

国外计算机科学教材系列

应用密码学手册

Handbook of Applied Cryptography

Alfred J. Menezes
[加] Paul C. van Oorschot 著
Scott A. Vanstone

胡 磊 王 鹏 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书是目前最优秀的密码学书籍之一。全书包含15章，内容覆盖了近20年来密码学发展的所有主要成就。除了通常密码学书籍都会讲到的对称密码、杂凑函数、公钥密码和签名、身份识别和密钥建立协议等内容外，本书首先提供了密码学的概貌，中间有三章专门讲述了公钥密码学的数学基础，最后两章给出了密码实现技巧和专利、标准等细节。这些内容对研究者和工程师们都是十分有用的。全书提供了丰富的密码学技术细节，包括200多个算法和协议、200多幅图表、1000多个定义、事实、实例、注释和评论。书末列举了1200多篇关于密码学的主要文献，并在各章中对其做了简要评述。

本书组织完美，表述清晰，适合密码学、计算机、通信、数学等领域的师生、专家和工程师们参考或作为教材使用。

版权贸易合同登记号　图字：01-2003-8825

图书在版编目（CIP）数据

应用密码学手册/（加）梅尼斯（Menezes, A. J.）等著；胡磊，王鹏等译. -北京：电子工业出版社，2005.6
（国外计算机科学教材系列）
书名原文：Handbook of Applied Cryptography
ISBN 7-121-01339-8

Ⅰ.应…　Ⅱ.①梅…　②胡…　③王…　Ⅲ.密码-理论-教材　Ⅳ.TN918.1

中国版本图书馆CIP数据核字（2005）第056339号

责任编辑：谭海平　　特约编辑：李玉龙
印　　刷：北京顺义兴华印刷厂
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：45.5　字数：1164千字
印　　次：2005年6月第1次印刷
定　　价：89.00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

译 者 序

从1976年公钥密码思想的发明和数据加密标准DES的问世算起，现代密码学已经走过了近三十年的发展历程。今天，密码学已成为信息技术中应用的重要学科，在信息安全领域中发挥着越来越重要的作用。现在国际上每年要举办数十个与密码学相关的学术会议，每年要发表大量的密码学研究论文。

回顾十几年前的情形则很不相同。那时，研究者没有现在这么多，全面介绍密码学知识的书籍也很少。不过，这种情况在20世纪90年代中期得到了很大改变。Schneier的*Applied Cryptography*以及Menezes，Oorschot和Vanstone的*Handbook of Applied Cryptography*即是当时出版的两本最权威、最有参考价值的密码学书籍。二者的内容都十分丰富，从基本的密码学概念到复杂的密码学协议，二者都涉及到密码学的许多方面，都属于百科全书式的宏篇巨著。但它们的不同之处也是十分明显的。Schneier的书虽然简要介绍了许多密码算法，但重点是叙述密码算法的应用——各式各样的密码协议，其中专门有一部分叙述真实世界中的密码学应用情况。该书非常适合于想了解密码学全貌的非专业人士，甚至为他们提供了一些算法的源代码。相比之下，Menezes，Oorschot和Vanstone的*Handbook of Applied Cryptography*则更适合于从事密码学研究和工程实现的专业人士，全书提供了丰富的密码学技术细节，包括200多个算法和协议、200多个图表、1000多个定义、事实、实例、注释和评论。这些细节对于学习和深入理解密码学是十分适宜的。书末还列举了1200多篇密码学主要文献，并在各章中对其做了简要评述。

本书内容组织得很完美，文字的表达也很清晰。由于内容多，翻译工作量大，其中肯定有不少错误和不准确的地方，欢迎读者批评指正。参加翻译和校对的同志有胡磊、李学俊、曾祥勇、聂旭云、鲁力、汪维家、张培清、李剑宇、周知远、彭建芬、张龙、方根溪、申艳光等，最后由胡磊统稿。

序　言

R.L.Rivest

当时间临近20世纪末时，我们十分清晰地看到正在进行的信息处理和电信革命将持续充满活力地迈进21世纪。在信息空间中，利用大量的数字信息，我们相互影响，进行交易，传递爱的信息、数字现金和秘密合作文件。我们的个人和经济生活越来越依赖于我们用这样无形的信鸽传播远程信息的能力，而在过去，我们是通过面对面会议、纸面文件和实在的握手来做到这一点的。遗憾的是，使得我们可以远程合作的技术魔力是建立在这样一个事实上的：任何信息都是通过"0,1"序列来传播的。当每一个音节被人造卫星反射并传遍整个大陆时，我们如何才能实现私人谈话呢？一家银行如何才能知道比尔·盖茨的确通过他在斐济的便携式电脑委托了一笔转到另一家银行的100亿美元转账呢？幸运的是，密码学的魔力数学为我们提供了帮助。密码学提供了保持信息秘密性、确定信息未被篡改、确定谁制作了信息片段的技术。

密码学是如此地美妙，因为它如此紧密地联系了理论与实践，而如今密码学的实际应用正是我们的信息社会广泛使用和最为关键的一部分。在理论基础上设计的信息保护协议一年以后就会出现在产品和标准文件中。相反地，新的理论发展有时意味着去年提出的方案有先前未曾预料到的弱点。虽然理论发展得非常迅猛，然而真正可保证的不多；许多方案的安全性依赖于(看似真实的)未被证明的猜测。理论工作精炼和改进了实践，而实践挑战和激发了理论工作。当一个系统"被攻破"时，我们的知识就得到了提高，而下一年的系统将改进以弥补这个缺陷(这使人想起银行金库的设计者和他们的敌手之间长期而复杂的斗争)。

密码学是如此地迷人，还因为它具有与游戏一样的对抗特性。一位好的密码学家在他/她思考问题时会迅速地来回改变角色，从攻击者到防御者然后再回来。就像下象棋一样，必须考虑一系列自己的走子和对手的走子，直到理解了当前的形势。与象棋选手不同的是，密码学家还必须考虑敌手可能试图破坏规则或干扰期望的所有方法(她度量我的计算时间有关系吗？她的"随机数"不是1有关系吗？)。

本书是密码学领域的一本重要著作。它是已有技术的一本严密的百科全书，强调那些(相信是)既安全又有实际用途的技术。本书按照内在逻辑，描述了大部分重要的密码工具，这些工具是实现安全密码系统、解释现有系统的很多密码原理和协议所必需的。本书覆盖从低层的考虑如随机数生成器和高效模指数算法，到中层的技术如公钥签名方案，再到高层的课题如零知识协议。本书优秀的组织和风格使得它不仅可作为一本完备的自成体系的指南，而且还可作为一本不可缺少的案头参考书。

在记录密码学这个快速发展领域的状态方面，作者难以置信地提供了最新的、无错误的、全面的内容。事实上，很多章节，如杂凑函数和密钥建立协议两章，在内容和统一表述上都开辟了新天地。在权衡内容全面覆盖和单项内容穷尽对待方面，作者选择了简单、直接而有效的描述，使得每个单项内容可以和它的重要细节、注意事项及与其他内容的比较一起进行解释。

虽然撰写本书的动机出于实际应用，但作者在书中包含了大量的数学基础及相关理论的讨论，这使得本书对于研究者和学生与对于实践者一样有意义。本质的数学技术和必需的概念在书中描述得很清晰，当然，还有说明性的例子。富有洞察力的历史注释和详尽的参考书目使得本书是通往密码学殿堂的极好基石(我非常惊喜地发现附录中有 CRYPTO 和 EUROCRYPT 会议的完整论文书目)。

我很高兴被邀请为这本书作序，并祝贺作者完成了本书，我要告诉读者，你们正在阅读该领域发展的一个里程碑。

Ronald L. Rivest
麻省理工学院电子工程与计算机科学系 Webster 讲席教授
1996 年 6 月

前　言

本书的目的是作为专业密码学家的参考书，提供当前专业人士最感兴趣的技术和算法，以及提供动机和背景资料。本书还为学生和老师提供了学习密码学的广泛资源。此外，论述上的一丝不苟、覆盖面广、大量的参考书目，使得本书对于专业研究是一本重要的参考书。

我们的目标是充分吸收具有产业价值的现有密码学知识，使得本书成为从事实际应用的工程师、从事学术研究的计算机科学家和数学家的图书，同时也成为激发非专业人士学习密码学欲望的一本容易得到的、自成体系的完备图书。这样一个任务超越了下列任何一项所覆盖的范围：研究论文，很自然地，这些论文是集中在很窄的课题上，用的是非常专业化（常常不标准）的术语；调查报告，这类文章通常是在很高层次上陈述至多一小部分的专业课题；大部分书籍，由于作者缺乏实际经验或是不熟悉研究文献资料或是两者皆有，这些书籍不能胜任本书的任务。我们的目的是详细描述密码学中的一些领域，这些领域是我们在自己的产业实践中发现为最有实用价值的，同时本书还保留了足够正式的方法，适合作为那些主要兴趣是进一步研究的人员的参考书，而且为学生和其他的初学者提供坚实的基础。

纵览每一章，我们强调的是密码学各个不同方面的联系。背景节出现在大部分章中，对于随后的技术提供了框架和全貌。算法的计算机源代码（如 C 代码）有意舍去了，为的是用足够的细节来专门叙述算法，以指导实现而无须参看二手资料。我们相信这种描述方法能使读者更好地理解算法是如何正确地工作的，与此同时，避免用当前流行的各种程序语言来描述与实现相关的低层算法结构（某些读者总是不熟悉）。

本书着重描绘了什么是由现有的简单猜想出发（通过数学评论）建立起来的事实。为了突出项目的应用特性，书中大多数情形下的正确性的严格证明均被省去；然而，每一章后面注释一节中的参考给出了那些结果的来源或推荐来源。注释一节同时提供了一些未在正文中阐述的各种其他技术的信息（十分详细），而且也是一篇研究活动和理论结果的报告；参考文献再一次告诉读者，若要进一步研究一些特定问题，可以到哪里去查找文献。毫无疑问，很多结果（包括某些研究领域）本书并未关注到，或是完全由于空间不够而被整体略去；我们事先对这些省略表示道歉，并且希望那些有意义但被省去的部分能够引起人们的注意。

为了提供跨越基础动机到具体实现的一个完整的密码学处理，考虑思考的层次是很有用的，这个层次包括从概念上的思想和终端用户服务到完整实际实现所必需的工具。表 1 描述了本书的整个组织层次结构。相应地，图 1 说明了这些层次在各章中的体现方式，以及它们的内部依赖关系。

表 2 列出了这本书的所有章节，还列出了所有章节的主要作者，读者若有意评论某个章节，则应该和他们联系。每一章都是一个主要课题的自成体系的处理。然而就整体来说，每一章都经过了精心设计，补充了相关的定义、术语和概念，从而使之成为一个整体。更进一步，基本上没有贯穿各章的重复资料；相反，在相关的地方提供了贯穿各章之间的相应参考。

表 1　应用密码学的层次

信息安全目标	
机密性	
数据完整性	
认证(实体和数据源)	
不可抵赖性	
密码函数	
加密	第 6 章、第 7 章、第 8 章
消息认证和数据完整性技术	第 9 章
身份识别/实体认证技术	第 10 章
数字签名	第 11 章
密码构造模块	
流密码	第 6 章
分组密码(对称密钥)	第 7 章
公钥加密	第 8 章
单向杂凑函数(无密钥的)	第 9 章
消息认证码	第 9 章
签名方案(公钥,对称密钥)	第 11 章
部件	
公钥参数生成	第 4 章
伪随机比特生成器	第 5 章
离散算术的有效算法	第 14 章
基础	
密码学介绍	第 1 章
数学背景	第 2 章
复杂度和基础问题的分析	第 3 章
基础设施技术和商用方面	
密钥建立协议	第 12 章
密钥安装和密钥管理	第 13 章
密码专利	第 15 章
密码标准	第 15 章

虽然本书并没有刻意安排按顺序从头至尾阅读,但这样安排材料会有一些优点。这个项目的"手册"特性激发的两个主要目标是,允许容易得到独立的结果和允许容易参考结果与算法(如用做讨论或随后交叉参考)。为了易于得到和参考结果,所有项都被分类而且很大程度上都编了号,即下列诸项在每一章内被连续编号:*定义*、*实例*、*事实*、*注释*、*评论*、*算法*、*协议*和*机制*。用更传统的处理,*事实*通常等同于命题、引理或定理。我们用编了号的*注释*来阐述附加的技术点,而编了号的*评论*等同于非技术的(常常是非严格的)评论、观察和观点。*算法*、*协议*和*机制*指的是那些有一系列步骤的技术。*实例*、*注释*和*评论*一般都由插入的总结性标题开始,这样可使得读者很快地确定这部分内容的特性,因而可以确定是否应该阅读。使用数目较多的小节也是为了突出手册的特性和方便快速地找到想要的结果。

考虑利用章节划分主题领域,我们使用的是称之为*功能性组织*的方法(基于针对最终用户兴趣的功能)。例如,所有与实体认证有关的项目都放在同一章中。另一个可选的划分方法是

可称为学术组织的方法,在这种方法下,所有的基于零知识概念(包括实体认证协议和签名方案的一个共同子集)都可能放在同一章中。我们相信功能性组织的方法对于实际工作者更为便利,他们更感兴趣的是选择得到一个实体认证协议(见第 10 章)或是一个签名方案(见第 11 章),而不是寻求一个未指定最终目的的零知识协议。

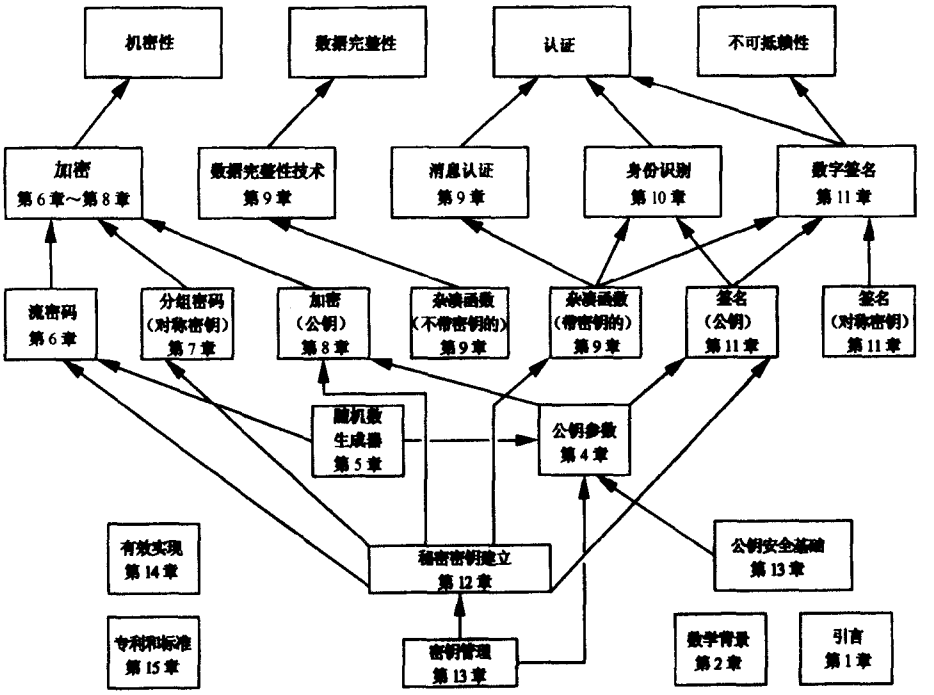


图 1　本书的路线图

表 2　每一章的主要作者

章	主要作者		
	AJM	PVO	SAV
1. 密码学概述	*	*	*
2. 数学背景	*		
3. 数论相关问题	*		
4. 公钥参数	*	*	
5. 伪随机比特和序列	*		
6. 流密码	*		
7. 分组密码		*	
8. 公钥加密	*		
9. 杂凑函数和数据完整性		*	
10. 身份识别和实体认证		*	
11. 数字签名			*
12. 密钥建立协议		*	
13. 密钥管理技术		*	
14. 有效实现			*
15. 专利和标准		*	
— 总体组织	*	*	

在本书的最后，我们提供了一个论文列表，该列表包含了至今为止的每一届 Crypto，Eurocrypt，Asiacrypt/Auscrypt 和快速软件加密会议的论文，以及发表在密码学杂志（*Journal of Cryptology*）上第 1 卷到第 9 卷的所有论文目录。这些列表以及参考书目中所列出来的文章在本书正文中至少引用了一次。几乎所有的参考文献都已验证了它们的确切标题、卷以及页数等。最后作者做了一个大范围的索引。索引开头是符号列表。

我们的目的不是介绍新的技术和协议，而是有选择地描述从当前公开文献中可得到的技术。这种文献的合集是时时都需要的。事实上，很多书籍都没有像本书第 7 章、第 8 章和第 11 章那样举例说明过去 15 年来该领域的惊人发展历程（实际上，这些章节与第 1 章一起可认为是一个介绍性的课程）。第 2 章、第 3 章提供的数学背景很难在同一册书中找到，而且被大部分的密码学图书忽略了。第 4 章关于公钥参数的生成和第 14 章关于有效实现方面的资料仅为一些小团体的专家所知，而且仅能在一些零星的文献中找到，在以前的书中很难见到一般性的文本。第 5 章、第 6 章中的伪随机数生成器和流密码也常常被其他图书忽略（很多书完全集中在分组密码上），或那些图书仅从理论的观点来处理伪随机数生成器和流密码。杂凑函数（第 9 章）和身份识别协议（第 10 章）仅在最近作为一些专门课题被深入研究。第 12 章的密钥建立协议很难在当前的主流课题的合集上找到。第 13 章中的密钥管理技术通常不会引起密码学家太多兴趣，但它在实际中是非常重要的。关于密码学专利和密码学标准的简明总结，我们放在了第 15 章。

在大多数情形（带有历史性的例外）下，对于那些现在已知的不安全的算法，我们选择忽略它们的专门细节，因为大部分这样的技术是没有实际意义的。本质上，囊括在本书中的算法已经由独立的实现验证了它们的正确性，确认了指定的测试向量。

致谢

没有我们的同仁的鼎力帮助，这本书是不可能完成的。他们花费时间阅读了无休止的草稿，确保了技术上的正确性，并且建设性地反馈了无数的建议。特别是我们的顾问编辑为我们提出了无价的建议，仅通过本书无法就他们提出的这些建议一一对他们表示感谢。我们要特别感谢顾问编辑中的如下各位：

Mihir Bellare	Don Coppersmith	Dorothy Denning	Walter Fumy
Burt Kaliski	Peter Landrock	Arjen Lenstra	Ueli Maurer
Chris Mitchell	Tatsuaki Okamoto	Bart Preneel	Ron Rivest
Gus Simmons	Miles Smid	Jacques Stern	Mike Wiener
Yacov Yacobi			

另外，我们还要感谢所有为改进本书质量而提供了高质量的反馈和指导的人们。他们是：

Carlisle Adams	Rich Ankney	Tom Berson	Simon Blackburn
Ian Blake	Antoon Bosselaers	Colin Boyd	Jørgen Brandt
Mike Burmester	Ed Dawson	Peter de Rooij	Yvo Desmedt
Whit Diffie	Hans Dobbertin	Carl Ellison	Luis Encinas
Warwick Ford	Amparo Fuster	Shuhong Gao	Will Gilbert
Marc Girault	Jovan Golić	Dieter Gollmann	Li Gong

Carrie Grant	Blake Greenlee	Helen Gustafson	Darrel Hankerson
Anwar Hasan	Don Johnson	Mike Just	Andy Klapper
Lars Knudsen	Neal Koblitz	Çetin Koç	Judy Koeller
Evangelos Kranakis	David Kravitz	Hugo Krawczyk	Xuejia Lai
Charles Lam	Alan Ling	S. Mike Matyas	Willi Meier
Serge Mister	Peter Montgomery	Mike Mosca	Tim Moses
Volker Müller	David Naccache	James Nechvatal	Kaisa Nyberg
Andrew Odlyzko	Richard Outerbridge	Walter Penzhorn	Birgit Pfitzmann
Kevin Phelps	Leon Pintsov	Fred Piper	Carl Pomerance
Matt Robshaw	Peter Rodney	Phil Rogaway	Rainer Rueppel
Mahmoud Salmasizadeh	Roger Schlafly	Jeff Shallit	Jon Sorenson
Doug Stinson	Andrea Vanstone	Serge Vaudenay	Klaus Vedder
Jerry Veeh	Fausto Vitini	Lisa Yin	Robert Zuccherato

我们向那些由于疏忽而未在上表中列出姓名的人表示道歉。特别感谢 Carrie Grant, Darrel Hankerson, Judy Koeller, Charles Lam 和 Andrea Vanstone。他们的努力工作极大地提高了本书的质量,真的很高兴能和他们一起工作。还要感谢 CRC 出版社的工作人员,包括 Tia Atchison, Gary Bennett, Susie Carlisle, Nora Konopka, Mary Kugler, Amy Morrell, Tim Pletscher, Bob Stern 和 Wayne Yuhasz。第二位作者还要感谢他在 Nortel Secure Networks (Bell-Northern Research)的同事对本书的贡献,他们中的许多已在上表中提及,但要特别感谢 Brian O'Higgins 的鼓励与支持。第三位作者还要感谢自然科学与工程研究理事会(Natural Sciences and Engineering Research Council)的支持。

当然,我们会为本书所有存在的错误负责。若读者能指出错误、遗漏的参考文献或错误的结果并与我们联系,我们将十分感谢。我们希望本书能推动该领域的进一步发展,希望我们所做的工作能在其中起到一小部分作用。

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone

目　录