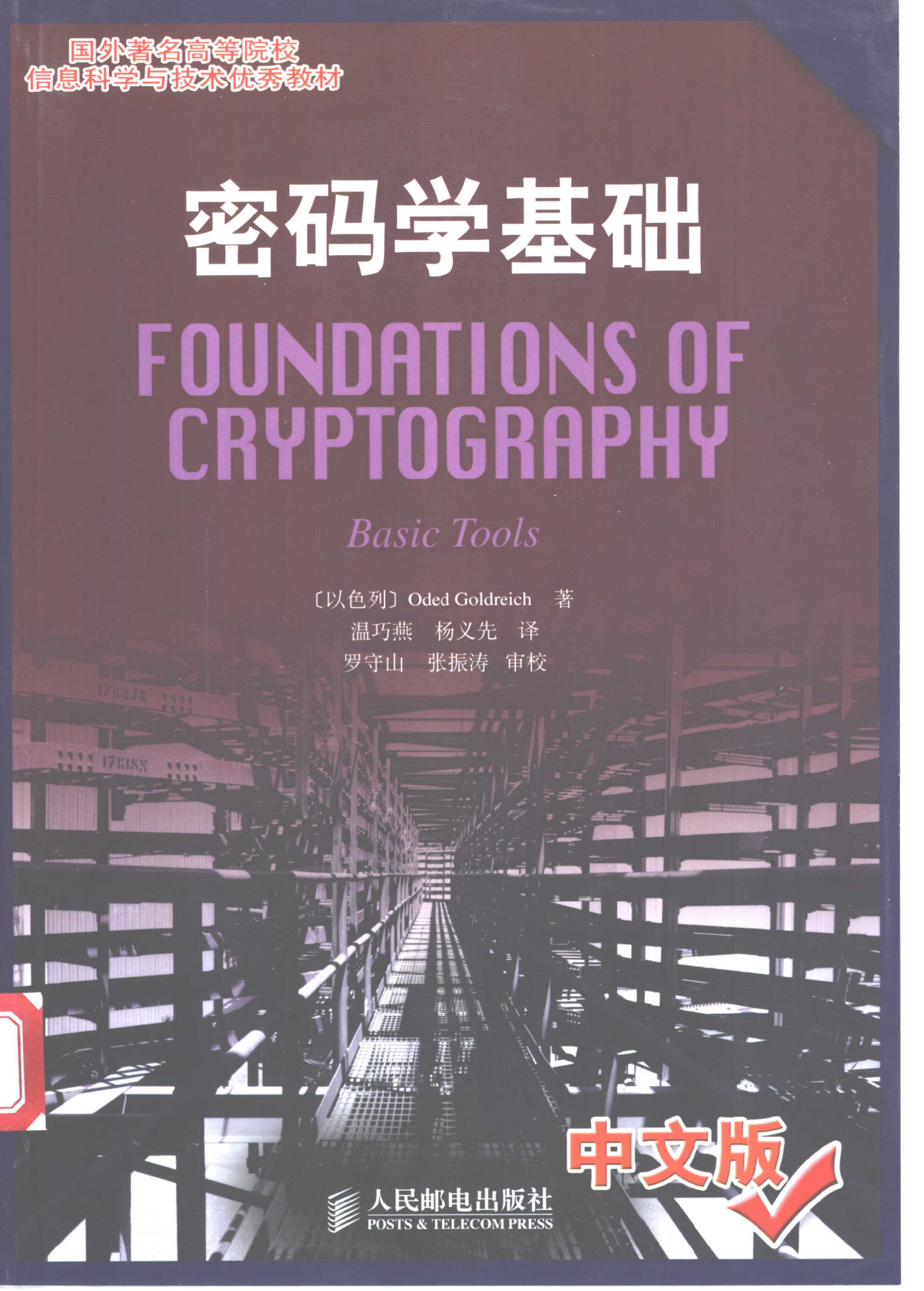
国外著名高等院校
信息科学与技术优秀教材

密码学基础

FOUNDATIONS OF CRYPTOGRAPHY

Basic Tools

〔以色列〕Oded Goldreich 著
温巧燕 杨义先 译
罗守山 张振涛 审校



中文版

人民邮电出版社
POSTS & TELECOM PRESS

国外著名高等院校信息科学与技术优秀教材

密码学基础

[以色列] Oded Goldreich 著

温巧燕 杨义先 译

罗守山 张振涛 审校

人民邮电出版社

图书在版编目（CIP）数据

密码学基础/（以）戈德里克（Goldreich，O.）编著；温巧燕，杨义先译.—北京：人民邮电出版社，2003.9
国外著名高等院校信息科学与技术优秀教材
ISBN 7-115-10355-0

Ⅰ．密… Ⅱ．①戈… ②温… ③杨… Ⅲ．密码—理论—高等学校—教材 Ⅳ．TN918.1

中国版本图书馆 CIP 数据核字（2003）第 056367 号

版 权 声 明

国外著名高等院校信息科学与技术优秀教材

密码学基础

◆ 著 [以色列] Oded Goldreich
译 温巧燕 杨义先
审 校 罗守山 张振涛
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：18.5
字数：446 千字 2003 年 9 月第 1 版
印数：1-4 000 册 2003 年 9 月北京第 1 次印刷

著作权合同登记 图字：01－2002－0398 号

ISBN 7-115-10355-0/TP・2914

定价：35.00 元

本书如有印装质量问题，请与本社联系 电话：(010)67129223

内容提要

密码学涉及解决安全问题的计算系统的概念化、定义以及构造。密码系统的设计必须基于坚实的基础。本书对这一基础问题给出了系统而严格的论述：用已有工具来定义密码系统的目标并解决新的密码问题。本书集中讨论：计算复杂性（单向函数）、伪随机数以及零知识证明。本书的重点在于澄清基本概念并论述解决密码问题的可行性，而不侧重于描述某种具体方法。

本书可作为密码学、应用数学、信息安全等专业的教材，也可作为相关专业人员的参考用书。

出版说明

2001年，教育部印发了《关于“十五”期间普通高等教育教材建设与改革的意见》。该文件明确指出，“九五”期间原国家教委在“抓好重点教材，全面提高质量”方针指导下，调动了各方面的积极性，产生了一大批具有改革特色的新教材。然而随着科学技术的飞速发展，目前高校教材建设工作仍滞后于教学改革的实践，一些教材内容陈旧，不能满足按新的专业目录修订的教学计划和课程设置的需要。为此该文件明确强调，要加强国外教材的引进工作。当前，引进的重点是信息科学与技术和生物科学与技术两大学科的教材。要根据专业（课程）建设的需要，通过深入调查、专家论证，引进国外优秀教材。要注意引进教材的系统配套，加强对引进教材的宣传，促进引进教材的使用和推广。

邓小平同志早在1977年就明确指出：“要引进外国教材，吸收外国教材中有益的东西。”随着我国加入WTO，信息产业的国际竞争将日趋激烈，我们必须尽快培养出大批具有国际竞争能力的高水平信息技术人才。教材是一个很关键的问题，国外的一些优秀教材不但内容新，而且还提供了很多新的研究方法和思考方式。引进国外原版教材，可以促进我国教学水平的提高，提高学生的英语水平和学习能力，保证我们培养出的学生具有国际水准。

为了贯彻中央“科教兴国”的方针，配合国内高等教育教材建设的需要，人民邮电出版社约请有关专家反复论证，与国外知名的教材出版公司合作，陆续引进一些信息科学与技术优秀教材。第一批教材针对计算机专业的主干核心课程，是国外著名高等院校所采用的教材，教材的作者都是在相关领域享有盛名的专家教授。这些教材内容新，反映了计算机科学技术的最新发展，对全面提高我国信息科学与技术的教学水平必将起到巨大的推动作用。

出版国外著名高等院校信息科学与技术优秀教材的工作将是一个长期的、坚持不懈的过程，我社网站（www.ptpress.com.cn）上介绍了我们陆续推出的图书的详细情况，敬请关注。希望广大教师和学生将使用中的意见和建议及时反馈给我们，我们将根据您的反馈不断改进我们的工作，推出更多更好的引进版信息科学与技术教材。

人民邮电出版社

译者序

人类对密码的研究与应用已有几千年的历史，但密码学作为一门系统科学则仅仅是上个世纪 50 年代的事情。1949 年，信息论的创始者 Shannon 发表的著名论文“保密通信的信息理论”将密码学的研究纳入了科学的轨道，使密码学正式成为一门科学。1976 年，美国著名学者 Diffie 和 Hellman 的经典论文“密码学的新方向”奠定了公钥密码学的基础，它标志着密码学的研究和实践由传统走向现代。1977 年，美国公布并实施的数据加密标准 DES，揭开了密码学的神秘面纱，使密码学的研究和应用从秘密走向公开，吸引了众多学者和技术人员对其进行研究，从此密码学成为了一门蓬勃发展的学科。而今，随着互联网的迅速普及，信息安全问题引起了全人类的重视，密码学作为信息安全的核心更得到了长足发展。现在，大多数国家或地区都已经成立了密码学会，国际国内各种密码学术会议频繁召开，许多大学都开设了密码学专业并进行本科生和研究生的招生和培养。总之，与密码学相关的众多活动极大地促进了它的研究与应用。如今，密码学理论研究已比较成熟，国内外已出版了大量有关密码学的书籍，许多著名学者都基于自己的研究出版了专著，这些著作各具特色，其中有不少佳作适合做教材。Oded Goldreich 教授所著的《密码学基础》一书就是一本很有特色的密码学教科书，其最显著的特点就是“基础”二字，正如该书前言中引用的那样：

“没有根基也许可以造一座小屋，但绝不能造一座坚固的大厦。”

密码学所关心的是构造一些能抵抗任何攻击的机制，这种密码机制的设计是一项十分困难的任务，它必须建立在坚实的基础之上。本书对这一基础问题给出了系统而严格的论述。

根深才能叶茂。相信这本书对于希望在密码学的殿堂里有所造诣的学子们大有裨益。这正是我们花费大量精力翻译本书的初衷。

参加本书翻译工作的还有郭奋卓、张洁、麻小宁、安宁、付华等，特别是郭奋卓博士协助我们完成了全书的统稿和审校。本书在翻译过程中，还得到了北京邮电大学信息安全中心钮心忻博士、徐国爱博士等的支持与协助，在此一并对他们表示衷心地感谢。

本书的出版得到了国家973项目（编号：G1999035804）、国家自然科学基金重大项目（编号：90204017）和国家863项目（编号：2002AA143041）的资助，在此表示感谢。

杨义先
北京邮电大学
2003年于北京

前 言

没有根基也许可以造一座小屋，
但绝不能造一座坚固的大厦。
Eng. Isidor Goldreich（1906～1995）

密码学所关心的是构造一些能抵抗任何攻击的机制。构造这样的机制是为了使系统在遭受企图让它们偏离规定功能的恶意攻击下，依旧能保持期望的功能。

密码机制的设计是一个十分困难的任务。人们不能仅依靠有关系统运行环境的典型状态的直观知识。的确，攻击系统的*对手*（adversary）可能企图控制操作环境使之成为非典型状态。人们不可能满足于设计用来抵抗特定攻击的反攻击手段，因为对手（将在系统设计完成后才行动）可能试图以和设计者所预料的大不相同的方式来攻击此机制。虽然上述断言似乎是不证自明的，但是，仍有一些人期望在实践中忽略这些赘述不会导致实际损失。事实证明这样的愿望很少能达到；基于伪装的密码机制迟早会被破坏。

按照上述观点，我们认为就对手可能使用的特定*策略*（strategy）进行假设是没有什么意义的，惟一合理的假设是对手的计算*能力*（ability）。进一步说来，我们认为密码系统的设计必须建立在*坚实的基础*（firm foundation）之上，专门方法和试探方法则是非常危险的。当设计者对机制即将运行的环境十分了解时，试探方法可能有意义，但是密码机制将不得不在恶意选择的环境中运行，这一环境是超出设计者所预料的。

本书旨在提供坚实的密码学基础知识。密码学的基础包括：范例、方法和抽象化的技巧、定义，以及提供对自然的“安全考虑”的解决方案。我们将提出一些这样的范例、方法和技术，并通过对它们的使用而掌握它们。我们的重点是澄清这些基本概念，并且论证解决这些核心密码问题的可行性。

解决一个密码问题（或说明一种安全需求）是由*定义阶段*（definitional stage）和*构造阶段*（constructive stage）组成的过程。首先，在定义阶段，基于固有利害关系的功能必须标识出来，适当的密码问题也必须被定义。试图列出所有未曾预料的情况是不

可行的，而且容易出错。相反，人们应该按照想象的理想模型中的操作方法定义此功能，然后需要一种候选解决方案在真实且被明确定义的模型（表示对手的能力）中仿真此操作。定义阶段完成后，接着就是构造一个满足此定义的系统。这样的构造可以使用一些更简单的工具，它的安全性可以通过这些工具的性质来证明（当然，实际中这样的机制也必须满足某些特定的效率要求）。

本书的重点在于几个构造型（archetypical）密码问题（例如，加密和签名机制）和几个核心工具（例如，计算难题、伪随机性和零知识证明）。对于每个问题（或工具），我们首先给出其固有的利害关系（或它的直观目标），然后定义这个问题（或工具），最后证明这个问题可以被解决（或这个工具可以被构造）。在最后一步中，我们着重于证明解决此问题的可行性，而不是给出一个切实可行的解决方案。对于给定（或已知）解决方案的实用性（或不实用性）的级别，我们只作为次要问题来讨论。

计算难题

前面提及的特殊构造（和这个领域的大多数构造一样）仅当某种计算困难（即难题）存在时才能存在。特别地，所有这些问题和工具（直接或间接）都要求能生成难题的实例，这一能力在单向函数的定义（进一步讨论参见 2.1 节）中可以获得。于是，单向函数就成为了大多数密码学问题的最小要求。正如我们将要看到的那样，实际上它们对许多密码学问题来说都足够了（其余的可以通过扩充和扩展单向函数存在这一假设来解决）。

仅凭我们目前对有效计算的理解并不能证明单向函数存在。特别地，单向函数的存在性意味着 $\mathcal{NP}$ 不包含于 $\mathcal{BPP}$ ⊇ $\mathcal{P}$（“大多数”都不是），这一结论能够解决计算机科学方面的许多著名难题。为了证明这一假设的合理性，我们只能给出数百（或数千）位学者的联合信任。而且，这些信任是关于一个简单描述的假设，其有效性基于几个公认的猜想，这些猜想是某些领域的核心（例如，对整数进行因数分解是困难的这一猜想就是计算数论的核心）。

既然无论如何我们都需要一定的假设，那么我们为何不假设我们想要的，即某一固有的密码学问题的解决方案的存在性呢？首先，我们要知道想做什么。如前所述，我们必须首先阐述要做什么，即：我们必须经过典型、复杂的定义阶段，但一旦完成了定义，我们就能假设导出的定义满足要求吗？却却相反。事实是：导出的定义并不意味着它一定能满足，人们可以很容易地定义不存在（没有定义中的明显事实）的对象。要证明一个定义是可行的（因此直观上的安全性条件可以完全满足），方法是构造一个基于更*易于理解*（better-understood）的假设（即更普遍更为广泛认同的假设）。例如，考虑零知识证明的定义，这样的证明（在非平凡的意义上）完全存在并非完全先验的。首先可以通过为二次剩余类命题提出一个零知识证明系统来证明这一概念的非平凡性，（没有附加信息）二次剩余类命题是难于校验的。接着，与先验信任相反，后面将证明单向函数的存在性意味着任意 $\mathcal{NP}$ 命题都可以用零知识证明。这样，那些根本不知道是否成立的事实（以及那些被认为是错误的事实）都可以通过变形为广泛认同的假设（总之没有它们，许多现代密码学问题就失去依托）来证明其成立。总之，并非所有假设都是等价的，因此把一个复杂的、新的、有疑问的假设转变成一个被广泛认同的简单（或者仅仅是简单）假设是非常重要的。把新任务的解决方案转变成一个已知的简单任务的假定安全方案就意味着：给出一个使用已知原型的构造，可以解决新的任务。这就意味着，我们不但知道（或假设）新任务是可以解决的，而且还能找到一个基于某一原型的解

决方案，这一原型是已知的，并有几个可供选择的实现方法。

结构和先决条件

我们的目标是给出密码学的基本概念、技巧和结论。如前所述，我们的重点在于阐明基本概念及其相互关系。这可以通过一种不依赖于某些通用数论例子的特性的方法来实现。这些特殊的例子在这个领域的发展中起着核心作用，并为所有的密码学原型提供了最切合实际的实现方法，但是这并不表示我们的陈述必须和它们相关联。相反，当我们把概念在抽象层提出，并把它们从特定的实现方法中分离出来时，我们才能以最好的方式阐明它们。与本书关系最紧密的背景知识都是以算法（包括随机化算法）的基本知识、可计算性和初等概率论的方式提出的。某些构造法的实现需要基于（计算性的）数论的背景知识，但是本书并非真的需要这一知识（为了证明本书提出的一些实现方法的实例，本卷在附录中给出了最密切相关的背景知识）。

本著作的构成　本著作由三部分构成（参见图 0.1，本书是第一卷），将分别在三卷中介绍：基本工具、基本应用和在基础之上的知识。第一卷包括一个介绍性的章节和第一部分内容（基本工具），讲述了关于计算难题（单向函数）、伪随机性和零知识证明的知识。这些基本工具将用于第二卷中的基本应用，第二卷是由加密、签名和通用密码协议组成的。

本著作是按逻辑划分为三卷的。而且，这样划分还有如下优点：不必等其他部分完成就可以出版第一卷；同理，我们期望在几年内完成第二卷，然后不必等第三卷完成就可以出版第二卷。

第一卷的结构　第一卷是由一个介绍性的章节（第 1 章）以及关于计算难题（单向函数）、伪随机性和零知识证明的章节（分别对应于第 2～4 章）组成的。另外，还包括两个附录，其中一个是对第 2 章的简单概括。图 0.2 描述了第一卷的主要结构。

第一卷：绪论和基本工具
- 第 1 章：绪论
- 第 2 章：计算复杂性（单向函数）
- 第 3 章：伪随机发生器
- 第 4 章：零知识证明系统

第二卷：基本应用
- 第 5 章：加密机制
- 第 6 章：签名机制
- 第 7 章：通用密码协议

第三卷：在基础之上的知识
- …

图 0.1　本著作的结构

每章结尾给出了一些历史记录、对进一步阅读的建议、一些未决问题和一些习题。习题主要是用来帮助读者理解主要内容和测试其理解程度的，而不是用来检测或鼓励创造力的。未决问题都是相当著名的，我们还建议读者了解一下它们目前的发展状态（例如在我们的即

时更新布告站点上)。

本书的布告站点 我们打算维护一个列出各种类型修正的站点，站点地址是http://www.wisdom.weizmann.ac.il/~oded/foc-book.html。

第1章：绪论
- 本书涉及的主要问题（1.1节）
- 概率和计算方面的背景知识（1.2和1.3节）
- 严密处理的目的（1.4节）

第2章：计算复杂性（单向函数）
- 动机和定义（2.1和2.2节）
- 单向函数：弱单向隐含了强单向（2.3节）
- 多样性（2.4节）和提高性阅读材料（2.6节）
- 核心断言（2.5节）

第3章：伪随机发生器
- 动机和定义（3.1～3.3节）
- 基于单向置换的构造（3.4节）
- 伪随机函数（3.6节）
- 提高性阅读材料（3.5节和3.7节）

第4章：零知识证明
- 动机和定义（4.1～4.3节）
- 对*NP*问题的零知识证明（4.4节）
- 提高性阅读材料（4.5～4.11节）

附录A：计算数论中的背景知识

附录B：第二卷摘要

参考文献

图0.2 本卷的大致结构

如何使用本书

本书可以用作教科书和参考书。也就是说，它既是面向初学者的又是面向专家学者的。为了达到此目标，本书基础阅读材料的描述是非常详细的，这样大多数计算科学的大学生都能掌握它。程度高的学生（和专家学者）可能会觉得这些部分的进度太慢了，但是我们尝试让他们可以很容易就跳过这些细节部分。特别地，证明过程通常是按一种模式描述的。首先我们给出主要思想的高度概括，然后才开始具体细节的描述。从精练描述到具体细节的转变通常用“详述如下”的字眼来指示。

在有些地方（就像本段这样首行缩进的段落中），我们给出了一些直接而又乏味冗长的细节。还有一些地方（更少），这样的段落给出了与本书的主题关联不大的结论的证明过程。

更高级的阅读材料通常以更快的进度和更少的细节提出。希望我们试图使大范围的读者

都满意，不会不利于任何读者。

教学　本书给出的阅读材料一方面超出了一学期课程所能覆盖的内容，另一方面又缺乏一般人所期望了解的密码学知识。为了调和这些冲突的需求，我们对基础的和高级的阅读材料加以区分，并（在每章的最后一节）对进一步阅读提出建议。特别地，那些标记星号的小节是供高级阅读使用的。

本著作第一卷和第二卷试图提供密码学基础教程所需要的所有阅读材料。对一学期的课程来说，教师一定要跳过所有的高级阅读材料（在目录中用星号标记的），甚至可能需要略过一些基础阅读材料；请参考图 0.3 的建议。根据年级，应该覆盖一个合理层次上的基础阅读材料（例如，所有标记了“要点”的阅读材料和一些“可选”的阅读材料）。第一卷和第二卷也可以用作两学期课程的教科书。不管是哪种情况，第一卷都只覆盖了一学期课程的前半部分，后半部分包含在第二卷中。同时，我们建议后半部分使用其他教材。附录 B 给出了第二卷的简短概括和推荐的其他教材（此外，第二卷中这 3 章的片段和/或初稿分别能在一些早期的文档［99］、［100］和［98］中得到）。

每讲一小时。1～15 讲覆盖第一卷的内容，16～28 讲覆盖第二卷的内容。

第 1 讲：绪论、背景知识等。

（视年级而定）

第 2～5 讲：计算复杂性（单向函数）

要点：定义（2.2 节），核心断言（2.5 节）

可选：弱单向隐含了强单向（2.3 节），以及 2.4.2～2.4.4 节

第 6～10 讲：伪随机发生器

要点：定义问题和构造（3.2～3.4 节）

可选：伪随机函数（3.6 节）

第 11～15 讲：零知识证明

要点：一些定义和构造（4.2.1、4.3.1、4.4.1～4.4.3 节）

可选：4.2.2、4.3.2、4.3.3、4.3.4、4.4.4 节

第 16～20 讲：加密机制

定义和构造（参考附录 B1.1～B1.2）

（加密章节也可以参见手稿［99］的片段。）

第 21～24 讲：签名机制

定义和构造（参考附录 B.2）

（签名章节也可以参见手稿［100］的片段。）

第 25～28 讲：通用密码协议

定义方法和通用构造（概述）。

（参考附录 B.3，也可以参见［98］。）

图 0.3　密码学基础的一学期教学计划

虽然一门课程可以只用第一卷作为教材，但是这样的课程不可以作为密码学上的独立课程，因为本卷根本没有涉及加密和签名的基本任务。

实际应用 本书的目标是为密码学提供理论基础。如前所述，这些基础对任何合理的密码学知识的应用来说都是必需的。当然，合理的应用不单单需要理论基础，然而本著作没有给出任何超出理论基础的知识。不过，有了合理的基础，我们就可以学习和评价其他地方（例如［158］）出现的各种有关实际应用的建议。另一方面，如果缺乏合理的基础就不能评判对实际应用的建议，这反过来又会导致不合理的决策。对设计一个能抵抗对手攻击的机制来说，没有什么比误解这些攻击的概念危害更大了。

感谢

首先，我要感谢对我的专业发展有重大影响的 3 位著名人物：Shimon Even，Silvio Micali 和 Shafi Goldwasser。Shimon Even 引导我迈入理论计算科学的殿堂，并密切地领导我迈出第一步。Silvio Micali 和 Shafi Goldwasser 引导我研究密码学基础，并和我分享他们为进一步发展这些基础所做的努力。

我曾与许多研究人员合作过，但是我觉得与 Benny Chor 和 Avi Wigderson 的合作对我的专业发展和事业的影响最大。我要感谢他们，既为他们对我的相关研究的无私奉献，也为和他们一起工作时的兴奋与愉悦。

同时我也要对 Leonid Levin 表示特别的感谢。多年来，我和 Leonid 曾有过许多有趣的讨论，有时我要花很长时间才能意识到这些讨论对我是多么有帮助。

接着，我还要感谢一些同事和朋友，我和他们在密码学和相关问题上彼此有着重要影响。他们包括 Noga Alon，Boaz Barak，Mihir Bellare，Ran Canetti，Ivan Damgard，Uri Feige，Shai Halevi，Johan Hastad，Amir Herzberg，Russell Impagliazzo，Joe Kilian，Hugo Krawcyzk，Eyal Kushilevitz，Yehuda Lindell，Mike Luby，Daniele Micciancio，Moni Naro，Noam Nisan，Andrew Odlyzko，Yair Oren，Rafail Ostrovsky，Erez Petrank，Birgit Pfitzmann，Omer Reingold，Ron Rivest，Amit Sahai，Claus Schnorr，Adi Shamir，Victor Shoup，Madhu Sudan，Luca Trevisan，Salil Vadhan，Ronen Vainish，Yacob Yacobi 和 David Zuckerman。

假如我没有遗漏对我在本书的相关问题上有重要影响的人，对我有恩惠的人是非常多的。其中一定包括许多参考书目中提及的论文的作者，也包括许多我没有引用的有关密码学论文的作者，以及许多有关整个计算理论（本书中理所当然视之为理论）的论文的作者。

最后，我要感谢 Alon Rosen，他仔细审阅了初稿并提出了许多修正建议。

目 录