国外著名高等院校
信息科学与技术优秀教材

密码学基础

（第二卷）

FOUNDATIONS OF CRYPTOGRAPHY

Volume II Basic Applications

〔以色列〕Oded Goldreich 著
温巧燕 杨义先 郭奋卓 张 劼 译
柯品惠 高 飞 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（第二卷）

[以色列] Oded Goldreich 著

温巧燕 杨义先 郭奋卓 张 劼 译

柯品惠 高 飞 审校

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

密码学基础. 第2卷/（以）戈德里克（Goldreich，O.）著；温巧燕，杨义先译.
—北京：人民邮电出版社，2005.5
国外著名高等院校信息科学与技术优秀教材

ISBN 7-115-13122-8

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（2005）第026443号

版 权 声 明

Oded Goldreich: Fundamentals of Cryptography Volume II Basic Applications
Copyright © Oded Goldreich 2004
Authorized translation from the English language edition published by the Press Syndicate of the University of Cambridge.
All rights reserved.

本书中文简体字版由英国剑桥大学出版社授权人民邮电出版社出版。未经出版者书面许可，对本书任何部分不得以任何方式复制或抄袭。

版权所有，侵权必究。

国外著名高等院校信息科学与技术优秀教材

密码学基础（第二卷）

◆ 著 [以色列] Oded Goldreich
译 温巧燕 杨义先 郭奋卓 张 劼
审 校 柯品惠 高 飞
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
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：20.75
字数：505千字 2005年5月第1版
印数：1－3 500册 2005年5月北京第1次印刷

著作权合同登记号 图字：01-2004-6139号

ISBN 7-115-13122-8/TP・4452

定价：42.00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、定义及构造。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学问题。本书的重点是澄清基本概念并论述解决几个主要密码问题的可行性，而不侧重于对特殊方法的描述。

《密码学基础》第一卷主要讨论的是单向函数、伪随机性和零知识证明。本书在第一卷的基础上接着讨论加密、签名和一般的密码协议。本书可作为密码学、应用数学、信息安全等专业的研究生教材，也可作为相关专业人员的参考用书。

注意：本书第一卷内容共 4 章，为了体现顺序性，第二卷的章号与第一卷的章号衔接，因此本书（第二卷）正文从第 5 章开始。本书（第二卷）附录与第一卷的附录序号衔接，因此本书附录为附录 C。本书第一卷已由人民邮电出版社出版，书名：《密码学基础》，书号：10355。

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

此为试读，需要完整PDF请访问：www.ertongbook.com

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，随着因特网的迅速普及，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，各种国际国内密码学术会议频繁召开，许多大学都开办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能步步登高的学子大有裨益。这正是我们花费大量精力翻译本书的初衷。

本书第一卷出版后，得到了同行专家的高度评价，许多研究工作者表示，该书基础深厚，中译本出版的非常必要和及时。于是，应出版社之约，我们又组织翻译了第二卷。在翻译过程中，得到了蔡吉人院士的支持与鼓励，他还花时间审阅了初稿。北京邮电大学信息安全中心的钮心忻教授、徐国爱博士等给予了大力

的支持与协助，秦素娟博士协助校对了部分书稿。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）、国家自然科学基金项目（编号：90204017、60373059）、教育部博士点基金项目（编号：20040013007）和国家 863 项目（编号：2002AA143041）的资助，在此表示感谢。

译者

2005 年于北京

序

1949年C.E.Shannon发表著名论文"Communication Theory of Secrecy"之前的几千年时间里，密码学仅仅是一些加密技巧的组合，没有系统的理论基础。上世纪70年代初美国国家标准局正式向社会公开招标，以透明竞争的方式征集民用数据加密标准，至此，密码学的神秘面纱被揭开，密码学的研究和应用从秘密走向公开，从专用机构走向民间。1976年，美国学者W.Diffie和M.E.Hellman在其发表的论文"New Directions in Cryptography"中提出了一种崭新的密码体制，开创了公钥密码学的新纪元，标志着密码学的研究和实践由传统走向现代。如今工业界和学术界对现代密码的研究与应用都十分重视，大多数国家和地区都成立了密码学学会，定期举办各种学术会议，出版学术刊物和著作。特别是近年来，许多高等院校都先后开办了信息安全相关专业，并将"密码学"作为本科生和研究生教育的一门重要课程，因此，优秀的密码学教材的撰写和引进就成了当前我国教育界的一个重要课题。最近，教育部组织专家编写了"全国信息安全专业本科教学规范"，其中对《现代密码学》课程的教学大纲进行了明确的阐述，这对规范我国密码学的本科教材建设具有重要的推动作用。但是，针对密码学的研究生教育，目前还没有出台类似的规范。

由Oded Goldreich教授编写的《密码学基础》一书是一本很有特色的针对研究生的密码学教科书。该书分为两卷，其中，第一卷已经出版。现在出版的是该书的第二卷。该书有以下特点：

1."数学味"较浓。全书特别突出"基础"，对所有内容的讨论几乎都是从最基础部分开始，所以，读者必须具有较好的数学功底和严谨的逻辑思维习惯。这样做的优点是有利于读者进行更深入的密码学后继学习和研究，缺点是可能使部分更关心应用的读者失去认真研读的耐心。

2. 系统性较强。书中对相关概念、定义、引理、定理、协议等的描述层次分明，非常规范和系统，逻辑推理深入且仔细。这样做的优点是能够有效训练高校学生的学习和科研能力，缺点是容易使部分特殊兴趣的读者陷入过多的精细概念之中从而"只见树木，难见森林"。

3. 目标明确。本书的选题很精简，重点讨论了密码学的核心部分（加密体制、数字签名、消息认证和通用密码协议），对每个问题都是从研究意义、定义、被解决的可行性来加以论述。这样做的优点是对每个主题的研究非常深入且完整，缺点是容易忽略密码学的众多应用。

综合各方面的情况，我认为本书不仅是广大密码学理论研究者非常有益的参考书，也是相关专业研究生密码学基础教育的参考教材。

北京邮电大学信息安全中心杨义先教授和温巧燕教授组织科研力量相继翻译出版了这本经典著作的第一卷和第二卷，这是一件有意义的工作。据我所知，为了保证翻译质量，他们付出了辛勤劳动，比如，多次召开研讨会，讨论相关翻译难题；将翻译初稿提交给国内相关权威专家征求意见等。我衷心祝愿该书能为我国广大密码学研究工作者提供有意义的帮助，也希望该书的出版和发行能为我国密码学基础研究起到一定的推动作用。相信随着我国大批密码学优秀科班学生的毕业，我国密码学的理论和应用研究将会再上一个新台阶。

中国工程院院士

2005 年 4 月 13 日

目 录

此为试读，需要完整PDF请访问：www.ertongbook.com

加密体制

第5章

直到20世纪70年代，人们普遍地理解密码学就是构造加密体制，即可以在不安全的信道中进行秘密的数据交换的技术。自从20世纪70年代以来，其他的一些工作（如数字签名）也被认为是属于密码学的范畴（甚至被认为是密码学的核心）。然而，加密体制的构造依然被认为是密码学的核心任务。

在本章中，我们回顾一下一些著名的私钥和公钥加密体制。更重要的是，我们定义了所指的一个加密体制的安全的含义。这个定义是整个领域的基石，并且本章的大部分篇幅会用来考虑这个问题的各个方面。我们同时会给出几个安全的（私钥和公钥）加密体制的构造。事实证明在加密的过程中（不仅仅是密钥生成阶段）随机性的使用对安全而言是必要的。

结构安排。主要内容（5.1～5.3节）是针对被动攻击（窃听）下的安全。作为对照，在5.4节，我们讨论了在主动攻击下的安全，及在选择密文攻击下的健壮性。其余的内容在5.5节中给予讨论。

教学提示。建议重点放在基本的定义（5.1及5.2.1～5.2.4节）和满足这些定义的可行性（如5.3.3和5.3.4.1节给出的简单构造）。对主动攻击下的安全的总体的了解（5.4.1节）也是值得推荐的。我们假设读者对前面章节的内容（特别是2.2，2.4，2.5，3.2～3.4和3.6节）比较熟悉。熟悉这些内容比较重要不仅因为我们使用了这些章节的记号和结果而且还因为我们使用了类似的证明技巧（如果读者不是第一次接触这种技巧的话，我们也这么做）。

5.1 基本定义

粗略地说，加密体制就是使得通信双方能在不安全的信道上进行信息的秘密交换。因此，基本集合由发送方、接收方、可能被窃听的不安全的信道及攻击者组成。目的就是使得发送方能通过不安全的信道把信息传送给接收方，同时又不让攻击者知道通信的内容。因此，我们必须把发送方想发送的真实（秘密的）信息和在不安全信道上传送的信息区别开来。前者称之为明文，而后者称之为密文。显然，密文必须和明文区别开来，否则攻击者通过窃听就能轻易获取明文信息。这样，发送方就必须把明文转换成对应的密文，使得接收方能够从密文中恢复明文，而攻击者恢复不了。从而，应该有些东西能够把接收方（能从对应的密文中恢复明文）和攻击者（不能恢复明文）区别开来。特别地，接收方应该掌握一些攻击者不知道的东西，我们称之为密钥。

一个加密体制由使用适当的密钥把明文转变成密文的方法和它的反过程组成。这些密钥

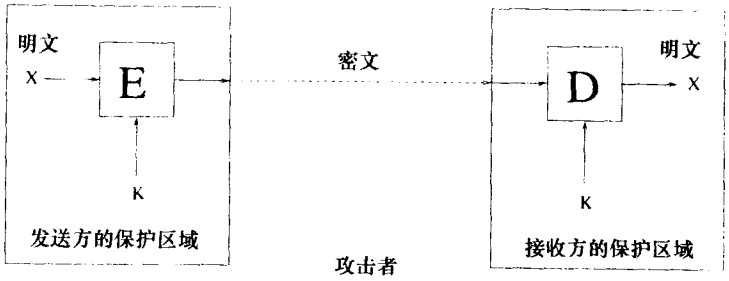
是完成这些转换的基本因素。正式地说,这些转换由相应的算法完成:把给定的明文和适当的(加密)密钥转换成密文的加密算法以及给定密文和适当(解密)密钥能从中恢复明文的解密算法。事实上,我们还需要去考虑第三个算法,即用来生成密钥的概率算法(密钥生成算法)。这个算法必须是概率的(否则通过调用这个算法攻击者也能得到和发送者一样的密钥)。我们强调攻击者也知道加密体制本身(即前面讲的三个算法)。体制的安全性主要依赖于假设攻击者不知道真正使用的密钥。①

根据这些原理,一个加密体制由三个算法组成。这些算法是公开的(对各方都是已知的)。两个主要的算法是*加密算法*,它把明文转换成密文,和*解密算法*,它把密文转换成明文。由这些原理,解密算法必须使用接收方知道而攻击者不知道的密钥。密钥由第三个算法生成,称之为*密钥生成器*。进一步地,不难看出加密过程也必须依赖密钥完成(否则发送的信息就有可能被一个不同的潜在接收方阅读)。因此,密钥生成算法应该生成一对(相关的)密钥,一个用于加密,另一个用于解密。给定明文和加密密钥,加密算法产生密文,同时输入密文和对应的解密密钥,解密算法产生明文。我们强调解密密钥的知识对后面的转换是必要的。

5.1.1 私钥体制和公钥体制比较

加密体制的不同主要指前面提到的密钥对的关系的不同(即加密密钥和解密密钥)。较简单(较早)的约定是加密密钥和解密密钥是相同的。这样的体制称为**私钥(或对称)体制**。

私钥加密体制。为了使用私钥体制,合法的双方首先必须商定一个秘密密钥。可以这样来做,先由一方随机生成密钥,然后通过一个安全的(不能被攻击者窃听)的(第二条)信道(不同于主要信道)把密钥传送给另一方。关键的一点就是密钥是独立于明文生成的,因此它可以在明文定下来之前就生成并交换密钥。假定合法的双方已经商定了一个(秘密)密钥,他们就可以利用这个密钥进行秘密通信(如图 5.1 所示):发送方利用密钥对要发送的明文进行加密,接收方利用同样的密钥从密文中恢复明文。因此,私钥加密是一种超越时间的扩展秘密信道的方法:如果双方今天可以使用秘密信道(他们当前都在同一物理区域),但是明天就不能用了。则他们可以今天就使用秘密信道进行密钥交换,然后明天用这个密钥进行秘密通信。



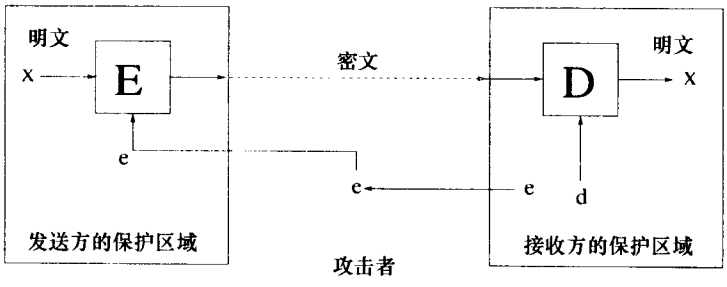
发送方和接收方都知道密钥 K,但是攻击者不知道。例如,发送方随机生成密钥 K 并通过一个完全保密的第二信道(不同于这里所显示的)把密钥 K 传送给接收方。

图 5.1 私钥加密体制:一个例子

① 事实上,在许多情形,符合利益的做法是把体制本身公开,因为这样才能获得(独立的)专家对此体制安全性的评价。

一个简单的私钥加密体制是一次一密(one-time pad)。密钥是均匀选取的 n 比特,然后把它和明文进行异或(XOR)得到密文。同样的方法可以从密文得到明文。显然,一次一密提供了绝对的安全性。然而,密钥的使用是没效率的;换句话说,它要求密钥具有和要交换的信息一样的长度。作为对照,本章的其余部分考虑这样的加密体制,它可以用来对没有限制的(关于 n 的多项式)长度进行数据的安全通信。特别地,n 比特长的密钥用来对明显大于 n 比特长的信息进行安全通信。

公钥加密体制。20 世纪 70 年代出现了一种新的加密体制。这种所谓的**公钥(非对称)**加密体制,加密密钥不同于解密密钥。进一步,由给定的加密密钥不可能得到解密密钥。这种体制可以不使用安全信道进行安全通信。相反地,双方都利用密钥生成算法产生一对密钥。一方(记之为 P)保留解密密钥,记之为 d_P,保密或公开加密密钥,记之为 e_P。现在,任意一方可以用加密密钥 e_P 加密私有信息并传送给 P。P 可以用解密密钥 d_P 解密密文,但是其他人做不了(见图 5.2 所示)。



接收方生成一对密钥对 (e,d),并公开加密密钥 e,同时保密解密密钥 d。

图 5.2　公钥加密体制:一个例子

5.1.2　加密体制的句法

我们现在来定义加密体制的基本机制。这个定义并未提及体制的安全性(这是下一节的主题)。

定义 5.1.1(加密体制):加密体制是这样的三元组 (G,E,D),它是满足如下两个条件的概率多项式时间算法:

1. 对输入 1^n,算法 G(称之为**密钥生成器**)产生一对比特串。
2. 对 $G(1^n)$ 中的每一对 (e,d),及对每个 $\alpha \in \{0,1\}^*$,算法 E(**加密**)和 D(**解密**)满足

$$\Pr[D(d,E(e,\alpha)) = \alpha] = 1$$

这里概率空间是取遍了算法 E 和 D 的所有内部投掷硬币的可能。

把 n 看作密码体制的安全参数。$G(1^n)$ 中的每个 (e,d) 由加密密钥和解密密钥对组成。$E(e,\alpha)$ 表示用加密密钥 e 对明文 $\alpha \in \{0,1\}^*$ 进行加密,同时 $D(d,\beta)$ 表示用解密密钥 d 对密文 β 进行解密。

我们强调定义 5.1.1 并未提及安全,因此平凡(不安全的)算法也满足这个定义(即 $E(e,\alpha) \stackrel{\text{def}}{=} \alpha$ 且 $D(d,\beta) \stackrel{\text{def}}{=} \beta$)。进一步地,定义 5.1.1 也没有把私钥加密体制和公钥加密体制区别开来。这两种体制的区别会在安全定义中加以介绍:在公钥加密体制中,"破解算法"把加密密

钥作为额外的输入(因此 $e \neq d$),然而在私钥加密体制中 e 并没有提供给"破解算法"(因此,不失一般性我们可以假设 $e = d$)。

我们强调定义要求密码体制能对所有明文进行运算。特别地,也适用于那些长度超过加密密钥长度的明文(这样就排除了前面提到的信息论安全的一次一密体制)。

记号。在本书中后面的部分,我们用 $E_e(\alpha)$ 表示 $E(e,\alpha)$,$D_d(\beta)$ 表示 $D(d,\beta)$。在不引起混淆的时候,我们也略去下标。同样,我们用 $G_1(1^n)$(相应地 $G_2(1^n)$)表示密钥对 $G(1^n)$ 的第一(第二)部分。即 $G(1^n) = (G_1(1^n), G_2(1^n))$。不失一般性,我们假设 $|G_1(1^n)|$ 和 $|G_2(1^n)|$ 都和 n 是多项式相关的,而且这个整数可以有效地从另一个整数计算得到。(事实上,我们甚至可以假设 $|G_1(1^n)| = |G_2(1^n)| = n$;见习题 6。)

注释。在不明显影响其实用性的前提下,定义 5.1.1 可以从几个方面放宽条件。例如,我们可以放宽(2)的条件并允许有可以忽略的解密错误发生(即 $\mathrm{Pr}[D_d(E_e(\alpha)) \neq \alpha] < 2^{-n}$)。同样地,我们可以假设条件(2)可以对除了 $G(1^n)$ 中一个可忽略的测度集的其他密钥对成立。这些放宽的条件至少有一个对(公钥)加密体制是必要的建议。

对可能的明文集(和密文集)做一些限制也可以作为放宽的条件。例如,我们可以限制条件(2)中 α 的长度是 $l(n)$,这里 $l:\mathbb{N} \to \mathbb{N}$ 是一些给定的函数。给定后面类型的加密体制(明文长度为 l),我们可以把明文长度切分为长度为 $l(n)$ 的块,并对每个块应用有限制条件的加密体制,从而构造出如定义 5.1.1 的加密体制(注意,这样构造的加密体制的安全性要求有限制条件的加密体制在使用同一密钥对多组明文进行加密的时候能保持安全)。更多的细节参看 5.2.4 和 5.3.2 节的内容。

5.2 安全的定义

本节我们将给出安全的两个基本定义并证明它们是等价的。第一个定义,称之为语义安全(*semantic security*),是最自然的一个。语义安全是类似于仙农给出的完全保密的定义的计算复杂性(它要求从密文中不能得到有关明文的任何信息)。不严格地说,如果从密文中提取有关明文的任何信息是不可行的,就称这个加密体制是语义安全的(即不可能性用不可行代替)。第二个定义更带有技巧的味道。它解释安全性就是不能分辨一对消息的加密结果。这个定义在示范一个提出的加密体制的安全性以及在分析一个利用加密体制的安全协议的时候是很有用的。

我们强调定义 5.2.1 给出的定义比要求不能从密文中恢复明文的要求严格得多。后者的要求是对一个安全的加密体制的最小的要求,但是这样的要求是很弱的。例如,我们肯定不会使用一个会泄露前面部分明文的加密体制(虽然不能从密文中恢复整个明文)。一般地,应用中的密码体制应该满足如果获取明文的部分信息就危及整个应用的安全性。在特定的应用中,哪些部分信息会危及安全性是很难(甚至不可能)回答的问题。但是,我们希望设计一些独立于应用的加密体制。当我们这样做的时候,我们假定任何的部分信息都可能对一些应用的安全产生影响。因此,我们要求不能从密文中获取有关明文的任何信息。进一步,明文可能是均匀分布的。我们要求在这种情形下依然能保持部分信息的安全。就是说,给定明文的任何先验信息,从密文中获取任何新的信息(超过了从明文的先验信息获得的信息)是不可行的。

此为试读,需要完整PDF请访问: www.ertongbook.com