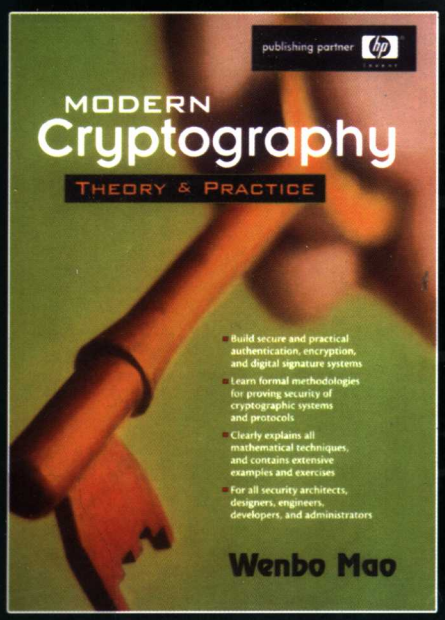
国外计算机科学教材系列

现代密码学理论与实践

Modern Cryptography: Theory and Practice



英文版

[英] Wenbo Mao 著

PRENTICE HALL PTR

PHEI

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

现代密码学理论与实践

（英文版）

Modern Cryptography: Theory and Practice

〔英〕 Wenbo Mao 著

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

第I部分是密码学与信息安全的入门性介绍。第II部分介绍学习本书必备的数学背景知识，也可作为学习现代密码学理论基础的系统背景知识。第III部分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。第IV部分介绍应用密码学和信息安全中一个重要的概念——认证。第V部分对公钥密码技术（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VI部分包括两个技术章节和一个简短的评述。

本书适合大学本科生、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、企业信息安全系统管理人员或者生产安全产品的软/硬件开发商以及刚开始从事密码学或计算机安全方面研究的博士生等使用。

版权贸易合同登记号 图字：01-2004-1759

图书在版编目（CIP）数据

现代密码学理论与实践 = Modern Cryptography：Theory and Practice/（英）毛文博（Mao,W.）著. —北京：电子工业出版社，2004.5
ISBN 7-5053-9816-4
Ⅰ.现... Ⅱ.毛... Ⅲ.密码－理论－英文 Ⅳ.TN918.1

中国版本图书馆CIP数据核字（2004）第029125号

责任编辑：吴 源
印 刷：北京市李史山胶印厂
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
北京市海淀区翠微东里甲2号 邮编：100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：46.625 字数：1180千字
印 次：2004年5月第1次印刷
定 价：69.00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

A SHORT DESCRIPTION OF THE BOOK

Many cryptographic schemes and protocols, especially those based on public-key cryptography, have basic or so-called "textbook crypto" versions, as these versions are usually the subjects for many textbooks on cryptography. This book takes a different approach to introducing cryptography: it pays much more attention to *fit-for-application* aspects of cryptography. It explains why "textbook crypto" is only good in an ideal world where data are random and bad guys behave nicely. It reveals the general unfitness of "textbook crypto" for the real world by demonstrating numerous attacks on such schemes, protocols and systems under various real-world application scenarios. This book chooses to introduce a set of practical cryptographic schemes, protocols and systems, many of them standards or de facto ones, studies them closely, explains their working principles, discusses their practical usages, and examines their strong (i.e., fit-for-application) security properties, often with security evidence formally established. The book also includes self-contained theoretical background material that is the foundation for modern cryptography.

PREFACE

Our society has entered an era where commerce activities, business transactions and government services have been, and more and more of them will be, conducted and offered over open computer and communications networks such as the Internet, in particular, via WorldWideWeb-based tools. Doing things online has a great advantage of an always-on availability to people in any corner of the world. Here are a few examples of things that have been, can or will be done online:

> Banking, bill payment, home shopping, stock trading, auctions, taxation, gambling, micro-payment (e.g., pay-per-downloading), electronic identity, online access to medical records, virtual private networking, secure data archival and retrieval, certified delivery of documents, fair exchange of sensitive documents, fair signing of contracts, time-stamping, notarization, voting, advertising, licensing, ticket booking, interactive games, digital libraries, digital rights management, pirate tracing, ...

And more can be imagined.

Fascinating commerce activities, transactions and services like these are only possible if communications over open networks can be conducted in a secure manner. An effective solution to securing communications over open networks is to apply cryptography. Encryption, digital signatures, password-based user authentication, are some of the most basic cryptographic techniques for securing communications. However, as we shall witness many times in this book, there are surprising subtleties and serious security consequences in the applications of even the most basic cryptographic techniques. Moreover, for many "fancier" applications, such as many listed in the preceding paragraph, the basic cryptographic techniques are no longer adequate.

With an increasingly large demand for safeguarding communications over open networks for more and more sophisticated forms of electronic commerce, business and services[a], an increasingly large number of information security professionals

[a]Gartner Group forecasts that total electronic business revenues for business to business (B2B) and business to consumer (B2C) in the European Union will reach a projected US $2.6 trillion in

will be needed for designing, developing, analyzing and maintaining information security systems and cryptographic protocols. These professionals may range from IT systems administrators, information security engineers and software/hardware systems developers whose products have security requirements, to cryptographers.

In the past few years, the author, a technical consultant on information security and cryptographic systems at Hewlett-Packard Laboratories in Bristol, has witnessed the phenomenon of a progressively increased demand for information security professionals unmatched by an evident shortage of them. As a result, many engineers, who are oriented to application problems and may have little proper training in cryptography and information security have become "roll-up-sleeves" designers and developers for information security systems or cryptographic protocols. This is in spite of the fact that designing cryptographic systems and protocols is a difficult job even for an expert cryptographer.

The author's job has granted him privileged opportunities to review many information security systems and cryptographic protocols, some of them proposed and designed by "roll-up-sleeves" engineers and are for uses in serious applications. In several occasions, the author observed so-called "textbook crypto" features in such systems, which are the result of applications of cryptographic algorithms and schemes in ways they are usually introduced in many cryptographic textbooks. Direct encryption of a password (a secret number of a small magnitude) under a basic public-key encryption algorithm (e.g., "RSA") is a typical example of textbook crypto. The appearances of textbook crypto in serious applications with a "non-negligible probability" have caused a concern for the author to realize that the general danger of textbook crypto is not widely known to many people who design and develop information security systems for serious real-world applications.

Motivated by an increasing demand for information security professionals and a belief that their knowledge in cryptography should not be limited to textbook crypto, the author has written this book as a *textbook on non-textbook cryptography*. This book endeavors to:

- Introduce a wide range of cryptographic algorithms, schemes and protocols with a particular emphasis on their *non-textbook* versions.
- Reveal general insecurity of textbook crypto by demonstrating a large number of attacks on and summarizing typical attacking techniques for such systems.
- Provide principles and guidelines for the design, analysis and implementation of cryptographic systems and protocols with a focus on standards.
- Study formalism techniques and methodologies for a rigorous establishment of

2004 (with probability 0.7) which is a 28-fold increase from the level of 2000 [5]. Also, eMarketer (page 41 of [105]) reports that the cost to financial institutions (in USA) due to electronic identity theft was US $1.4 billion in 2002, and forecasts to grow by a compound annual growth rate of 29%.

strong and fit-for-application security notions for cryptographic systems and protocols.

- Include self-contained and elaborated material as theoretical foundations of modern cryptography for readers who desire a systematic understanding of the subject.

Scope

Modern cryptography is a vast area of study as a result of fast advances made in the past thirty years. This book focuses on one aspect: introducing fit-for-application cryptographic schemes and protocols with their strong security properties evidently established.

The book is organized into the following six parts:

Part I This part contains two chapters (1—2) and serves an elementary-level introduction for the book and the areas of cryptography and information security. Chapter 1 begins with a demonstration on the effectiveness of cryptography in solving a subtle communication problem. A simple cryptographic protocol (first protocol of the book) for achieving "fair coin tossing over telephone" will be presented and discussed. This chapter then carries on to conduct a cultural and "trade" introduction to the areas of study. Chapter 2 uses a series of simple authentication protocols to manifest an unfortunate fact in the areas: pitfalls are everywhere.

As an elementary-level introduction, this part is intended for newcomers to the areas.

Part II This part contains four chapters (3—6) as a set of mathematical background knowledge, facts and basis to serve as a self-contained mathematical reference guide for the book. Readers who only intend to "knowhow," i.e., know how to use the fit-for-application crypto schemes and protocols, may skip this part yet still be able to follow most contents of the rest of the book. Readers who also want to "know-why," i.e., know why these schemes and protocols have strong security properties, may find that this self-contained mathematical part is a sufficient reference material. When we present working principles of cryptographic schemes and protocols, reveal insecurity for some of them and reason about security for the rest, it will always be possible for us to refer to a precise point in this part of the book for supporting mathematical foundations.

This part can also be used to conduct a systematic background study of the theoretical foundations for modern cryptography.

Part III This part contains four chapters (7—10) introducing the most basic cryptographic algorithms and techniques for providing privacy and data integrity

protections. Chapter 7 is for symmetric encryption schemes, Chapter 8, asymmetric techniques. Chapter 9 considers an important security quality possessed by the basic and popular asymmetric cryptographic functions when they are used in an ideal world in which data are random. Finally, Chapter 10 covers data integrity techniques.

Since the schemes and techniques introduced here are the most basic ones, many of them are in fact in the textbook crypto category and are consequently *insecure*. While the schemes are introduced, abundant attacks on many schemes will be demonstrated with warning remarks explicitly stated. For practitioners who do not plan to proceed with an in-depth study of fit-for-application crypto and their strong security notions, this textbook crypto part will still provide these readers with explicit early warning signals on the general insecurity of textbook crypto.

Part IV This part contains three chapters (11—13) introducing an important notion in applied cryptography and information security: authentication. These chapters provide a wide coverage of the topic. Chapter 11 includes technical background, principles, a series of basic protocols and standards, common attacking tricks and prevention measures. Chapter 12 is a case study for four well-known authentication protocol systems for real world applications. Chapter 13 introduces techniques which are particularly suitable for open systems which cover up-to-date and novel techniques.

Practitioners, such as information security systems administration staff in an enterprise and software/hardware developers whose products have security consequences may find this part helpful.

Part V This part contains four chapters (14—17) which provide formalism and rigorous treatments for strong (i.e., fit-for-application) security notions for public-key cryptographic techniques (encryption, signature and signcryption) and formal methodologies for the analysis of authentication protocols. Chapter 14 introduces formal definitions of strong security notions. The next two chapters are fit-for-application counterparts to textbook crypto schemes introduced in Part III, with strong security properties formally established (i.e., evidently reasoned). Finally, Chapter 17 introduces formal analysis methodologies and techniques for the analysis of authentication protocols, which we have not been able to deal with in Part IV.

Part VI This is the final part of the book. It contains two technical chapters (18—19) and a short final remark (Chapter 20). The main technical content of this part, Chapter 18, introduces a class of cryptographic protocols called zero-knowledge protocols. These protocols provide an important security service which is needed in various "fancy" electronic commerce and business applications: verification of a claimed property of secret data (e.g., in conforming with a business requirement) while preserving a strict privacy quality for the

claimant. Zero-knowledge protocols to be introduced in this part exemplify the diversity of special security needs in various real world applications, which are beyond confidentiality, integrity, authentication and non-repudiation. In the final technical chapter of the book (Chapter 19) we will complete our job which has been left over from the first protocol of the book: to realize "fair coin tossing over telephone." That final realization will achieve a protocol which has evidently-established strong security properties yet with an efficiency suitable for practical applications.

Needless to say, a description for each fit-for-application crypto scheme or protocol has to begin with a reason why the textbook crypto counterpart is unfit for application. Invariably, these reasons are demonstrated by attacks on these schemes or protocols, which, by the nature of attacks, often contain a certain degree of subtleties. In addition, a description of a fit-for-application scheme or protocol must also end at an analysis that the strong (i.e., fit-for-application) security properties do hold as claimed. Consequently, some parts of this book inevitably contain mathematical and logical reasonings, deductions and transformations in order to manifest attacks and fixes.

While admittedly fit-for-application cryptography is not a topic for quick mastery or that can be mastered via light reading, this book, nonetheless, is not one for in-depth research topics which will only be of interest to specialist cryptographers. The things reported and explained in it are well-known and quite elementary to cryptographers. The author believes that they can also be comprehended by non-specialists if the introduction to the subject is provided with plenty of explanations and examples and is supported by self-contained mathematical background and reference material.

The book is aimed at the following readers.

- Students who have completed, or are near to completion of, first degree courses in computer, information science or applied mathematics, and plan to pursue a career in information security. For them, this book may serve as an advanced course in applied cryptography.

- Security engineers in high-tech companies who are responsible for the design and development of information security systems. If we say that the consequence of textbook crypto appearing in an academic research proposal may not be too harmful since the worst case of the consequence would be an embarrassment, then the use of textbook crypto in an information security product may lead to a serious loss. Therefore, knowing the unfitness of textbook crypto for real world applications is necessary for these readers. Moreover, these readers should have a good understanding of the security principles behind the fit-for-application schemes and protocols and so they can apply the schemes and the principles correctly. The self-contained mathematical foundations material in Part II makes the book a suitable self-teaching text for

these readers.

- Information security systems administration staff in an enterprise and software/hardware systems developers whose products have security consequences. For these readers, Part I is a simple and essential course for cultural and "trade" training; Parts III and IV form a suitable cut-down set of knowledge in cryptography and information security. These three parts contain many basic crypto schemes and protocols accompanied with plenty of attacking tricks and prevention measures which should be known to and can be grasped by this population of readers without demanding them to be burdened by theoretical foundations.
- New Ph.D. candidates beginning their research in cryptography or computer security. These readers will appreciate a single-point reference book which covers formal treatment of strong security notions and elaborates these notions adequately. Such a book can help them to quickly enter into the vast area of study. For them, Parts II, IV, V and VI constitute a suitable level of literature survey material which can lead them to find further literatures, and can help them to shape and specialize their own research topics.
- A cut-down subset of the book (e.g., Part I, II, III and VI) also form a suitable course in applied cryptography for undergraduate students in computer science, information science and applied mathematics courses.

Acknowledgements

I am deeply grateful to Feng Bao, Colin Boyd, Richard DeMillo, 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 and Stefek Zaba. These people gave generously of their time to review chapters or the whole book and provide invaluable comments, criticisms and suggestions which make the book better.

The book also benefits from the following people answering my questions: 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 and Moti Yung.

I would also like to thank Jill Harry at Prentice-Hall PTR and Susan Wright at HP Professional Books for introducing me to book writing and for the encouragement and professional support they provided during the lengthy period of manuscript writing. Thanks also to Jennifer Blackwell, Robin Carroll, Brenda Mulligan, Justin Somma and Mary Sudul at Prentice-Hall PTR and to Walter Bruce and Pat Pekary at HP Professional Books.

I am also grateful to my colleagues at Hewlett-Packard Laboratories Bristol, including David Ball, Richard Cardwell, Liqun Chen, Ian Cole, Gareth Jones, Stephen Pearson and Martin Sadler for technical and literature services and management support.

Please send suggestions and corrections to the author (wenbo.mao@hp.com). Many thanks! Corrections will be listed on the website for the book:

www-uk.hpl.hp.com/people/wm/mctp.html

Bristol, England

May 2003

CONTENTS