

<<密码学基础（第二卷）>>

图书基本信息

书名：<<密码学基础（第二卷）>>

13位ISBN编号：9787121008405

10位ISBN编号：7121008408

出版时间：2005-2-1

出版时间：电子工业出版社

作者：戈德赖克

页数：798

字数：627000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<密码学基础（第二卷）>>

### 内容概要

密码学涉及解决通信保密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。

本书继上一卷对这一基础问题再次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。

全书详细阐述了三种基本应用：加密、签名和一般的密码学协议。

该书的重点是澄清基本概念及证明密码学问题解决方法的可行性，而不侧重于对特殊方法的描述。

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

。

#### 作者简介

Oded Goldreich 以色列魏茨曼科学研究所的计算机科学教授，现任Meyer W.Weisgal讲座教授。作为一名活跃的学者，他已经发表了大量密码学方面的论文，是密码学领域公认的世界级专家。他还是“Journal of Cryptology”，“SIAM Journal on Computing”杂志的编辑，1999年在Spri

## 书籍目录

5 Encryption Schemes 5.1. The Basic Setting 5.1.1. Private-Key Versus Public-Key Schemes 5.1.2. The Syntax of Encryption Schemes 5.2. Definitions of Security 5.2.1. Semantic Security 5.2.2. Indistinguishability of Encryptions 5.2.3. Equivalence of the Security Definitions 5.2.4. Multiple Messages 5.2.5.\* A Uniform-Complexity Treatment 5.3. Constructions of Secure Encryption Schemes 5.3.1.\* Stream-Ciphers 5.3.2. Preliminaries: Block-Ciphers 5.3.3. Private-Key Encryption Schemes 5.3.4. Public-Key Encryption Schemes 5.4.\* Beyond Eavesdropping Security 5.4.1. Overview 5.4.2. Key-Dependent Passive Attacks 5.4.3. Chosen Plaintext Attack 5.4.4. Chosen Ciphertext Attack 5.4.5. Non-Malleable Encryption Schemes 5.5. Miscellaneous 5.5.1. On Using Encryption Schemes 5.5.2. On Information-Theoretic Security 5.5.3. On Some Popular Schemes 5.5.4. Historical Notes 5.5.5. Suggestions for Further Reading 5.5.6. Open Problems 5.5.7 Exercises

6 Digital Signatures and Message Authentication 6.1. The Setting and Definitional Issues 6.1.1. The Two Types of Schemes: A Brief Overview 6.1.2. Introduction to the Unified Treatment 6.1.3. Basic Mechanism 6.1.4. Attacks and Security 6.1.5.\* Variants 6.2. Length-Restricted Signature Scheme 6.2.1. Definition 6.2.2. The Power of Length-Restricted Signature Schemes 6.2.3.\* Constructing Collision-Free Hashing Functions 6.3. Constructions of Message-Authentication Schemes 6.3.1. Applying a Pseudorandom Function to the Document 6.3.2.\* More on Hash-and-Hide and State-Based MACs 6.4. Constructions of Signature Schemes 6.4.1. One-Time Signature Schemes 6.4.2. From One-Time Signature Schemes to General Ones 6.4.3.\* Universal One-Way Hash Functions and Using Them 6.5.\* Some Additional Properties 6.5.1. Unique Signatures 6.5.2. Super-Secure Signature Schemes 6.5.3. Off-Line/On-Line Signing 6.5.4. Incremental Signatures 6.5.5. Fail-Stop Signatures 6.6. Miscellaneous 6.6.1. On Using Signature Schemes 6.6.2. On Information-Theoretic Security 6.6.3. On Some Popular Schemes 6.6.4. Historical Notes 6.6.5. Suggestions for Further Reading 6.6.6. Open Problems 6.6.7. Exercises

7 General Cryptographic Protocols 7.1. Overview 7.1.1. The Definitional Approach and Some Models 7.1.2. Some Known Results 7.1.3. Construction Paradigms 7.2.\* The Two-Party Case: Definitions 7.2.1. The Syntactic Framework 7.2.2. The Semi-Honest Model 7.2.3. The Malicious Model 7.3.\* Privately Computing (Two-Party) Functionalities 7.3.1. Privacy Reductions and a Composition Theorem 7.3.2. The OT Protocol: Definition and Construction 7.3.3. Privately Computing  $c + c_2 = (a_1 + a_2) \cdot (b_1 + b_2)$  7.3.4. The Circuit Evaluation Protocol 7.4.\* Forcing (Two-Party) Semi-Honest Behavior 7.4.1. The Protocol Compiler: Motivation and Overview 7.4.2. Security Reductions and a Composition Theorem 7.4.3. The Compiler: Functionalities in Use 7.4.4. The Compiler Itself 7.5.\* Extension to the Multi-Party Case 7.5.1. Definitions 7.5.2. Security in the Semi-Honest Model 7.5.3. The Malicious Models: Overview and Preliminaries 7.5.4. The First Compiler: Forcing Semi-Honest Behavior 7.5.5. The Second Compiler: Effectively Preventing Abort 7.6.\* Perfect Security in the Private Channel Model 7.6.1. Definitions 7.6.2. Security in the Semi-Honest Model 7.6.3. Security in the Malicious Model 7.7. Miscellaneous 7.7.1.\* Three Deferred Issues 7.7.2.\* Concurrent Executions 7.7.3. Concluding Remarks 7.7.4. Historical Notes 7.7.5. Suggestions for Further Reading 7.7.6. Open Problems 7.7.7. Exercises

Appendix C: Corrections and Additions to Volume 1  
 C.1. Enhanced Trapdoor Permutations C.2. On Variants of Pseudorandom Functions C.3. On Strong Witness Indistinguishability C.3.1. On Parallel Composition C.3.2. On Theorem 4.6.8 and an Afterthought C.3.3. Consequences C.4. On Non-Interactive Zero-Knowledge C.4.1. On NIZKs with Efficient Prover Strategies C.4.2. On Unbounded NIZKs C.4.3. On Adaptive NIZKs C.5. Some Developments Regarding Zero-Knowledge C.6. Additional Corrections and Comments C.7. Additional Motives

Bibliography  
 Index  
 Note : Asterisks indicate advanced material.

<<密码学基础（第二卷）>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>