

# 《密码学基础（第二卷）》

图书基本信息

# 《密码学基础（第二卷）》

## 内容概要

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。

# 《密码学基础（第二卷）》

## 作者简介

Oded Goldreich是以色列魏茨曼学院的计算机科学教授，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和SIAM Journal on Computing杂志的编辑，出版了《现代密码学、概

## 书籍目录

第5章 加密体制	5.1 基本定义	5.1.1 私钥体制和公钥体制比较	5.1.2 加密体制的句法
5.2 安全的定义	5.2.1 语义安全	5.2.2 加密的不可分辨性	5.2.3 安全定义的等价性
5.2.4 多组消息	5.2.5* 均匀复杂度的处理方法	5.3 安全加密体制的构造	5.3.1* 序列密码
5.3.2 预备知识：分组密码	5.3.3 私钥加密体制	5.3.4 公钥加密体制	5.4* 高于窃听的
安全性	5.4.1 概述	5.4.2 密钥依赖的被动攻击	5.4.3 选择明文攻击
5.4.4 选择密文攻击	5.4.5 非延展加密体制	5.5 其他	5.5.1 关于加密体制的使用
5.5.2 关于信息理论的安全	5.5.3 关于一些流行的加密体制	5.5.4 历史记录	5.5.5 关于进一步阅读的建议
5.5.6 未决问题	5.5.7 习题	第6章 数字签名和消息认证	6.1 背景知识和定义
6.1.1 两种体制：概述	6.1.2 对统一处理的介绍	6.1.3 基本机制	6.1.4 攻击和安全
6.1.5* 变体	6.2 长度受限的签名体制	6.2.1 定义	6.2.2 长度受限的签名体制的功能
6.2.3* 无碰撞哈希函数的构造	6.3 消息认证体制的构造	6.3.1 对文档应用一个伪随机函数	6.3.2* 哈希隐藏
的其他内容和基于状态的MACs	6.4 签名体制的构造	6.4.1 一次签名体制	6.4.2 从一次签名体制到一般的签名体制
6.4.3* 通用单向哈希函数及其应用	6.5* 一些其他性质	6.5.1 惟一签名	6.5.2 超安全签名体制
6.5.3 离线/在线签名	6.5.4 增量签名	6.5.5 伪造终止签名	6.6 其他
6.6.1 签名体制的利用	6.6.2 信息论安全	6.6.3 一些流行体制	6.6.4 历史记录
6.6.5 关于进一步阅读的建议	6.6.6 未决问题	6.6.7 习题	第7章 一般密码协议
7.1 概述	7.1.1 方法的定义和一些模型	7.1.2 一些已知结果	7.1.3 构造范例
7.2* 两方情况：定义	7.2.1 句法结构	7.2.2 半诚实模型	182 7.2.3 恶意模型
187 7.3* 秘密计算(两方)函数性	7.3.1 秘密约化和一个合成定理	7.3.2 协议：定义和构造	7.3.3 秘密计算
$c_1+c_2=(a_1+a_2) \cdot (b_1+b_2)$	7.3.4 电路计算协议	7.4* 加强的(两方)半诚实行为	7.4.1 协议编译器：动机和概述
7.4.2 安全约化和一个合成定理	7.4.3 编译器：使用的函数性	7.4.4 编译器本身	7.5* 推广到多方的情形
7.5.1 定义	7.5.2 半诚实模型中的安全性	7.5.3 恶意模型：概括和序言	7.5.4 第一个编译器：抵制半诚实行为
7.5.5 第二个编译器：有效地阻止中断	7.6* 在秘密信道模型中的完全安全	7.6.1 定义	7.6.2 半诚实模型中的安全性
7.6.3 恶意模型中的安全性	7.7 其他	7.7.1* 三个预留的问题	7.7.2* 并发执行
7.7.3 最后的注释	7.7.4 历史记录	7.7.5 关于进一步阅读的建议	7.7.6 未决问题
7.7.7 习题	附录C 对第1卷的修正和补充	C.1 加强的陷门置换	C.2 关于伪随机函数的变量
C.3 关于强证据不可分辨性	C.3.1 关于并行合成	C.3.2 关于定理4.6.8和一个事后补记	C.3.3 结论
C.4 关于非交互零知识	C.4.1 关于有高效的证明者策略的NIZK	C.4.2 关于无限的NIZK	C.4.3 关于自适应的NIZK
C.5 关于零知识的一些进展	C.5.1 构造零知识协议	C.5.2 在安全性证明中使用攻击者的程序	C.6 其他的一些纠错和注释
C.7 其他的格言	参考文献		

# 《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：[www.tushu000.com](http://www.tushu000.com)