

<<密码学基础 (平装)>>

图书基本信息

书名：<<密码学基础 (平装)>>

13位ISBN编号：9787115103550

10位ISBN编号：7115103550

出版时间：2003-9

出版单位：人民邮电出版社

作者：Oded Goldreich

页数：277

字数：446

译者：温巧燕

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 (平装)>>

内容概要

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。

<<密码学基础 (平装)>>

作者简介

Oded Goldreich是Weizmann学院计算机科学教授，也是Meyer W.Weisgal Professorial Chair的成员。作为一名活跃的学者，他已经发表了大量密码学论文，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，出版了《现代密码

<<密码学基础 (平装)>>

书籍目录

第1章 绪论 1 1.1 密码学：概述 1 1.2 概率论基础知识 6 1.3 计算模型 9 1.4 严密处理的目的 15 1.5 其他
第2章 计算复杂性 23 2.1 单向函数：动机(单向函数的意义) 24 2.2 单向函数的定义 25 2.3 弱单向函数
隐含强单向函数 2.4 单向函数的多样性 2.5 核心断言 (Hard-Core Predicates) 49 2.6 单向函数的有效放大 59 2.7 其他 67
第3章 伪随机发生器 77 3.1 启发性讨论 78 3.2 计算不可分辨性 79 3.3 伪随机发生器定义 85 3.4 基于单向置换的构造 94 3.5 基于单向函数的构造 103 3.6 伪随机函数 113 3.7 伪随机置换 124 3.8 其他 128
第4章 零知识证明系统 140 4.1 零知识证明：动机 141 4.2 交互证明系统 145 4.3 零知识证明：定义 4.4 NP零知识证明 169 4.5 否定结果 187 4.6 证据不可分辨性和隐藏性 192 4.7 知识证明 198 4.8 计算合理性证明(参数) 209 4.9 常数轮零知识证明 217 4.10 非交互零知识证明 225 4.11 证明者零知识证明 234 4.12 其他 241
附录A 计算数论背景 250
附录B 第2卷摘要 256
参考文献

<<密码学基础 (平装)>>

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>