<<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

出版时间：人民邮电出版社

作者：Oded Goldreich

页数：277

字数：446

译者：温巧燕

<<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

<<密码学基础 (平装)>>

版权说明