<<密码学基础>>

图书基本信息

书名：<<密码学基础>>

13位ISBN编号：9787505381780

10位ISBN编号：7505381784

出版时间：2003-1

出版时间：电子工业出版社

作者：Goldreich

页数：372

字数：564

<<密码学基础>>

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。
本书对这一基本问题给出了系统而严格的论述：用已有工具来定义密码的目标并解决新的密码学问题。
全书集中讨论了基本的数学工具：计算困难性、伪随机性以及零知识证明等。
本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。

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Springer出版社出版了“ Modern Cryptography,Probabilistic Proofs and Pseudorandomness ”一书。

<<密码学基础>>

书籍目录

版权说明