<<可证明安全算法与协议>>

图书基本信息

书名：<<可证明安全算法与协议>>

13位ISBN编号：9787030335401

10位ISBN编号：7030335406

出版时间：2012-3

出版时间：科学

作者：张华//温巧燕//金正平

页数：522

<<可证明安全算法与协议>>

内容概要

近年来，可证明安全算法与协议是信息安全、密码学等研究领域的重要问题之一。《可证明安全算法与协议》以作者张华、温巧燕及其课题组在该领域多年来的研究成果为主体，结合国内外学者的代表性成果，系统论述了可证明安全密码算法与协议的设计与分析，详细介绍了该研究方向的发展情况，并提出一些与之紧密相关的新研究课题。

全书分四部分，共17章。
第一部分(第1～3章)系统介绍了密码算法和协议设计中的基础知识；第二部分(第4～6章)论述了可证明安全的加密体制；第三部分(第7～12章)对数字签名进行了深入研究；第四部分(第13～17章)阐述了可证明安全的密钥协商协议及其应用。

本书既可作为对可证明安全算法与协议感兴趣的读者的入门教材，也可作为可证明安全理论研究工作者的参考用书，同时适合密码学、信息安全、数学、计算机及相关学科的高年级本科生、研究生、教师和科研人员阅读参考。

<<可证明安全算法与协议>>

书籍目录

《数学与现代科学技术丛书》已出版书目

<<可证明安全算法与协议>>

版权说明