

<<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

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>

## <<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。

## &lt;&lt;可证明安全算法与协议&gt;&gt;

## 书籍目录

《数学与现代科学技术丛书》序

前言

第一部分 基础知识

第1章 数学基础

1.1 数论

1.1.1 同余及剩余类

1.1.2 中国剩余定理

1.1.3 欧拉函数  $\varphi(n)$

1.1.4 二次剩余

1.1.5 素性检测

1.2 复杂性理论

1.2.1 计算复杂性与时间复杂性

1.2.2 复杂性分类

1.2.3 随机算法

1.3 信息论

参考文献

第2章 密码学基础

2.1 密码体制

2.1.1 对称加密体制

2.1.2 公钥加密体制

2.1.3 两者的比较

2.2 数字签名

2.2.1 基本概念及原理

2.2.2 经典算法

2.3 Hash函数

2.4 伪随机函数

2.4.1 伪随机序列生成器

2.4.2 伪随机函数

2.5 消息认证码

2.5.1 对MAC的要求

2.5.2 基于DES的MAC

2.6 零知识证明

参考文献

第3章 可证明安全理论基础

3.1 基本思想

3.2 困难问题假设

3.3 安全模型

3.3.1 数字签名方案的安全模型

3.3.2 公钥加密方案的安全模型

3.4 RO模型和标准模型方法论

参考文献

第二部分 加密体制

第4章 对称加密

第5章 公钥密码

第6章 可证明安全加密体制

## <<可证明安全算法与协议>>

### 第三部分 数字签名

第7章 可证明安全数字签名方案

第8章 盲签名

第9章 代理签名

第10章 多重签名与聚合签名

第11章 指定验证者签名

第12章 签密

### 第四部分 密钥协商

第13章 密钥协商概述

第14章 基于PKI的密钥协商协议

第15章 基于身份的密钥协商协议

第16章 基于口令的密钥协商协议

第17章 密钥协商协议的应用

《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

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>