<<数字签名理论>>

图书基本信息

书名：<<数字签名理论>>

13位ISBN编号：9787030183224

10位ISBN编号：7030183223

出版时间：2007-1

出版时间：科学出版社发行部

作者：赵泽茂

页数：231

字数：283000

<<数字签名理论>>

内容概要

数字签名技术是实现网络通信身份认证的核心技术，也是实现信息机密性、完整性和不可否认性的关键技术，广泛应用于网络通信、电子商务和电子政务等领域。

本书全面讲解了数字签名理论的基本知识，介绍了国内外数字签名理论与技术的若干最新理论和应用成果，其中许多成果是作者多年来教学和研究的结晶。

全书分9章，第1、2章介绍了数字签名的原理、功能、数学基础知识、分类、安全性和设计方法；第3～5章分别详细介绍了基于离散对数、椭圆曲线和身份的数字签名方案及相关的成果；第6～9章分别介绍了代理签名方案、盲签名方案、群签名方案、多重签名方案及近期最新理论研究成果。

本书可作为密码学、信息安全、应用数学、计算机科学、通信、信息科学及信号处理等专业的高年级本科生和研究生的教学参考书，也可作为信息安全、网络安全、密码学等领域的工程技术和研究人员的参考资料。

作者简介

赵泽茂，1965年3月生，四川蓬溪人，杭州电子科技大学通信工程学院副教授，硕士生导师。
1985年四川师范大学数学专业毕业，1990年中南大学应用数学专业毕业，获理学硕士学位，2005年获南京理工大学计算机应用专业工学博士学位。

先后在Applied Mathematics and Computation、Joumal of Electrorlics等国内外重要学术期刊上发表论文30余篇，其中被SCI、EI和ISTP收录多篇。
主持或参与省部级等各类科研项目多项。
目前主要从事密码学与信息安全的教学和科研工作。

<<数字签名理论>>

书籍目录

前言第1章　数字签名概述　1.1　研究背景和意义　1.2　数字签名原理　1.3　数字签名的功能　1.4　数字签名技术的应用　小结第2章　基本概念和方法　2.1　数学基础　2.2　公钥密码体制　2.3　数字签名定义和分类　2.4　数字签名的安全性　2.5　数字签名方案的设计方法　小结　参考文献第3章　基于离散对数的数字签名方案　3.1　引言　3.2　离散对数签名方案　3.3　ElGamal型签名方案　3.4　Schnorr数字签名方案　3.5　DSA数字签名方案　3.6　MR签名方案　3.7　HMP认证加密方案　3.8　MLR签密方案　3.9　Okamoto数字签名方案　3.10　GOST数字签名方案　小结　参考文献第4章　基于椭圆曲线的数字签名方案　4.1　引言　4.2　椭圆曲线的基本概念和理论　4.3　椭圆曲线密码体制　4.4　ECMR签名方案　4.5　ECMR签密方案　4.6　ECMLR签密方案　小结　参考文献第5章　基于身份的数字签名方案　5.1　引言　5.2　基于ID的密码体制　5.3　短签名方案　5.4　Liu签名方案　5.5　Hess签名方案　5.6　基于ID的签名方案的一般化形式　5.7　基于ID的密钥协商协议　小结　参考文献第6章　代理签名方案　6.1　引言　6.2　代理签名体制及其基本类型　6.3　基于离散对数的代理签名方案　6.4　基于椭圆曲线的代理签名方案　6.5　基于双线性对的代理签名方案　6.6　基于身份的代理签名方案　6.7　匿名代理签名方案　小结　参考文献第7章　盲签名方案　7.1　引言　7.2　基于因子分解的盲签名方案　7.3　基于离散对数的盲签名方案　7.4　广义ElGamal型弱盲签名　7.5　代理盲签名方案　7.6　基于身份的盲签名方案　7.7　部分盲签名方案　小结　参考文献第8章　群签名方案　8.1　引言　8.2　基于离散对数的群签名方案　8.3　基于知识签名的群签名方案　8.4　基于双线性对的群签名方案　8.5　环签名方案　参考文献第9章　多重数字签名方案　9.1　引言　9.2　广播多重签名方案　9.3　有序多重签名方案　9.4　代理多重签名方案　9.5　多重代理签名方案　9.6　多重代理多重签名方案　9.7　多重盲签名方案　参考文献

版权说明