第一图书网, tushu007.com

<<数字签名>>

图书基本信息

书名：<<数字签名>>

13位ISBN编号：9787118078107

10位ISBN编号：7118078107

出版时间：2012-1

出版时间：国防工业出版社

作者：任伟

页数：173

字数：200000

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

第一图书网, tushu007.com

内容概要

本书是第一本综合介绍在设计可证明安全签名方案时所用到的理论原理和技术的书籍。该书不但帮助读者更好地理解数字签名提供的安全保证，还包含了对密码学文献中几乎所有安全签名方案的全面描述和详细证明。

本书是大学生、大学教师以及研究者的有益参考，可作为理论密码学课程的补充资料来自学，或作为研究生研讨班的教材。

作者简介

作者:(美)Katz

书籍目录

第一部 分预备知识
第1章 数字签名的背景和定义
1.1 数字签名方案简介
1.2 计算安全
1.2.1 计算安全中的称谓
1.2.2 记法
1.3 签名方案的定义
1.4 安全定义的动机
1.5 形式化的(正式的)安全定义
1.5.1 随机消息攻击下的安全性
1.5.2 已知消息攻击下的安全性
1.5.3 适应性选择消息攻击下的安全性
1.6 安全定义间的关系
1.7 从较弱原语达到CMA安全
1.7.1 从RMA安全到CMA安全
1.7.2 从KMA安全到CMA安全
1.8 从不可伪造性到强不可伪造性
1.9 扩展消息长度
1.10 进一步阅读
第2章 密码学困难假设
2.1 通用密码学假设
2.1.1 单向函数和单向置换
2.1.2 陷门置换
2.3.3 构造抗碰撞的Hash函数
2.3.4 构造通用单向HaslI函数
2.4 Hash函数在签名方案中的应用
2.4.1 增加消息长度
2.4.2 减小公钥的长度
2.5 进一步阅读
第二部分 不需要随机预言模型的数字签名方案
第3章 基于通用假设的构造方法
3.1 Iamport一次签名方案
3.2 从一次签名方案构造签名方案
3.2.1 链式(Chain—Baseo ’) ” 签名
3.2.2 树式(1"ree—Base~1) ” 签名
3.2.3 一种无状态签名的解决方案
3.3 从单向函数构造签名
3.3.1 将组成部分集成到一起
3.3.2 对构造方法的思考
3.4 进一步阅读
第4章 基于(强)RsA假设的签名方案
4.1 简介
4.1.1 技术准备
4.1.2 本章纲要
4.2 基于RSA假设的方案

第一图书网, tushu007.com

4.2.1 Dwork—Naor方案
4.2.2 Cramer—Damgard方案
4.2.3 Hohenberger—Wate方案
4.3 基于强RSA假设的方案
4.3.1 强RSA假设
4.3.2 已知消息攻击下的安全性
4.3.3 Cramer—Shoup方案
4.3.4 Fischlin方案
4.3.5 Gennaro—Halevi—Rabin方案
4.4 进一步阅读
第5章 基于双线性映射构造的方案
5.1 简介
5.1.1 技术准备
5.1.2 本章纲要
5.2 Boneh—Boyen方案
5.3 Wate方案
5.4 进一步阅读
第三部分 基于随机预言模型的数字签名方案
第6章 随机预言模型
6.1 基于随机预言模型的安全证明
6.2 随机预言机方法是合理的
6.3 实践中的随机预言机模型
6.4 进一步阅读
7.2 FDH的改进的安全规约
7.3 概率FDH
7.4 具有紧规约的更简单的变种
7.5 进一步阅读
第8章 基于身份识别的签名方案
8.1 身份识别方案
8.2 从身份识别方案到签名方案
8.2.1 Fiat—Shamir变换
8.2.2 两种有用的标准
8.2.3 无需随机预言模型的一次签名方案
8.3 一些安全的身份识别方案
8.3.1 Fiat—Shamir方案
8.3.2 Guillou—Quisquater方案
8.3.3 Micali／Ong—SchnolT方案
8.3.4 Schnon—方案
8.4 进一步阅读
参考文献

第一图书网, tushu007.com

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