

<<密码基础理论与协议>>

图书基本信息

书名：<<密码基础理论与协议>>

13位ISBN编号：9787302267591

10位ISBN编号：7302267596

出版时间：2012-1

出版时间：清华大学出版社

作者：张薇，杨晓元，韩益亮 著

页数：225

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>

## <<密码基础理论与协议>>

### 内容概要

本书内容涉及现代密码学的基础理论和重要协议，包括计算复杂性理论、密码函数与序列密码变换理论、典型分组密码体制、公钥密码及其安全性、数字签名、多方密码协议及可证明安全理论。

本书可作为密码学、信息安全、网络安全、电子商务等专业的科研人员、工程技术人员参考，也可供相关专业的研究生及大学本科生使用。

## &lt;&lt;密码基础理论与协议&gt;&gt;

## 书籍目录

## 第1章计算复杂性理论

- 1.1算法的复杂性
- 1.2利用dtm程序解决判定问题
- 1.3p与np
- 1.4多项式变换与np完全问题

## 参考文献

## 第2章密码函数

- 2.1频谱理论简介
  - 2.1.1布尔函数
  - 2.1.2walsh 变换
  - 2.1.3chrestenson谱
- 2.2布尔函数的非线性准则
  - 2.2.1非线性度
  - 2.2.2线性结构与退化性
  - 2.2.3严格雪崩准则及扩散准则
- 2.3相关免疫函数
  - 2.3.1函数的相关免疫性
  - 2.3.2相关免疫函数的构造
- 2.4bent函数及其性质
  - 2.4.1bent函数的定义
  - 2.4.2bent函数的构造
  - 2.4.3bent函数的密码学价值

## 参考文献

## 第3章序列密码

- 3.1概述
  - 3.1.1加密方式
  - 3.1.2理论保密的密码体制
- 3.2序列密码的基础理论
  - 3.2.1周期序列的极小多项式及m序列
  - 3.2.2序列的线性复杂度
  - 3.2.3和序列与乘积序列
  - 3.2.4密钥序列的稳定性
- 3.3密钥序列的产生方法
  - 3.3.1前馈序列
  - 3.3.2多路复合序列
  - 3.3.3钟控序列
  - 3.3.4产生密钥序列的其他方法
- 3.4序列密码的安全性
  - 3.4.1布尔函数的最佳仿射逼近与baa攻击
  - 3.4.2dc攻击
- 3.5序列密码的应用
  - 3.5.1rc4密码
  - 3.5.2a5密码
  - 3.5.3欧洲nessie工程及estream工程简介
- 3.6混沌流密码

## <<密码基础理论与协议>>

3.6.1混沌密码学概述

3.6.2混沌流密码体制

参考文献

### 第4章分组密码

4.1数据加密标准des

4.2高级加密标准aes

4.2.1背景及算法概述

4.2.2算法细节

4.3差分分析

4.3.1差分分析的基本原理

4.3.2对迭代分组密码实施差分分析的一般过程

4.4线性分析

4.4.1对des算法圈函数的线性逼近

4.4.2线性逼近方程的建立

4.4.3线性逼近方程的求解

4.5对分组密码的其他攻击方法

4.5.1截段差分分析

4.5.2高阶差分分析

4.5.3非线性分析

4.5.4square攻击

参考文献

### 第5章公钥密码

5.1典型公钥密码

5.1.1diffie-hellman密钥交换

5.1.2rsa密码

5.1.3elgamal密码

5.1.4rabin密码

5.1.5ntru密码

5.2椭圆曲线密码

5.2.1椭圆曲线(elliptic curve)

5.2.2椭圆曲线公钥密码

5.2.3基于椭圆曲线密码的密码协议

5.3超椭圆曲线密码

5.3.1超椭圆曲线

5.3.2除子与jacobian群

5.3.3超椭圆曲线jacobian群中的运算

5.3.4超椭圆曲线密码体制

5.3.5基于hcc的密码协议

5.4基于身份的公钥密码体制

5.4.1概述

5.4.2基于身份的签名体制

5.4.3bf方案及其安全性

5.4.4基于身份的密钥共享

参考文献

### 第6章数字签名与签密

6.1数字签名的基本概念

6.1.1定义

## <<密码基础理论与协议>>

- 6.1.2对数字签名的攻击
  - 6.1.3数字签名的安全性
  - 6.2标准化的数字签名方案
    - 6.2.1rsa签名算法
    - 6.2.2dsa签名算法
    - 6.2.3ecdsa签名算法
  - 6.3代理签名
    - 6.3.1代理签名的定义
    - 6.3.2代理签名的安全性质
    - 6.3.3代理签名的分类
    - 6.3.4基于离散对数的代理签名
  - 6.4群签名
    - 6.4.1群签名的定义
    - 6.4.2群签名的安全性质
    - 6.4.3camenisch-stadler群签名
    - 6.4.4acjt群签名
  - 6.5签密
    - 6.5.1签密的定义
    - 6.5.2y.zheng基于短签名的签密方案scs
    - 6.5.3bao& deng可公开验证的签密
    - 6.5.4第一个基于标准数字签名算法的签密
    - 6.5.5基于dsa的签密方案sc-dsa
    - 6.5.6相关问题
  - 6.6广义签密
    - 6.6.1广义签密的定义
    - 6.6.2广义签密ecgsc
    - 6.6.3相关问题
- 参考文献

### 第7章多方密码协议

- 7.1门限密码体制
  - 7.1.1秘密共享
  - 7.1.2门限方案的变体
  - 7.1.3秘密共享的应用
- 7.2零知识证明
  - 7.2.1基本概念
  - 7.2.2零知识证明的形式化定义
  - 7.2.3零知识证明协议
- 7.3安全多方计算
  - 7.3.1概述
  - 7.3.2半诚实模型下的安全多方计算协议
  - 7.3.3安全多方计算的研究前沿

### 参考文献

### 第8章可证明安全技术基础

- 8.1形式化证明技术概述
- 8.2形式化安全性定义
  - 8.2.1攻击模型
  - 8.2.2加密的安全性定义

## <<密码基础理论与协议>>

8.2.3签名的安全性定义

8.3随机预言机模型

8.3.1预言机模型概述

8.3.2基于随机预言机模型的加密方案

8.3.3基于随机预言机模型的签名方案

8.3.4对随机预言机模型的讨论

8.4标准模型下可证明安全的加密方案

8.4.1修改的elgamal算法

8.4.2ind-cca安全的cramer-shoup方案

8.4.3ind-cca2安全的cramer-shoup方案

8.5数字签名的可证明安全性

参考文献

<<密码基础理论与协议>>

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>