

<<对称密码学>>

图书基本信息

书名：<<对称密码学>>

13位ISBN编号：97871111106746

10位ISBN编号：7111106741

出版时间：2002-8

出版时间：机械工业出版社

作者：张玉清胡予濮肖国镇

页数：263

字数：388000

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>

## <<对称密码学>>

### 内容概要

本书是信息与网络安全基础——对称密码学的专著，全面论述了对称密码学中的各种基本问题和最新研究进展。

本书部分成果来源于国家自然科学基金资助项目，ISN国家重点实验室开放课题基金资助项目和国防重点实验室预研基金资助项目。

著作论述了密码函数与信息泄露、序列密码和分组密码等内容，详细介绍了密码体制的安全性概念，密码函数的安全性指标——相关免疫函数、非线性性、差分与高阶差分，相关免疫函数的自然延伸——弹性函数；介绍序列的伪随机性，线性复杂度的计算，几何序列、对数序列、缩减序列及有特殊用途的稀疏序列；讨论简捷快速的分组密码体制；这是目前软硬件加密标准的主流。

同时介绍几个著名的分组密码设计方案，包括IDEA、RCS、RC6、Twofish和著名的软件加密算法SAFER+等。

书中还给出几个重要的分组密码的C-源程序代码。

本书面向信息安全领域的科研工作者，网络安全工程技术人员，信息安全专业的师生和从事通信、电子、计算机科学的科技人员等。

## &lt;&lt;对称密码学&gt;&gt;

## 书籍目录

## 前言

## 第一篇 密码函数与信息泄露

## 第1章 密码体制的安全性

## 1.1 密码体制与密码函数

## 1.2 密码体制的安全性之一完善保密性

## 1.3 密码体制的安全性之二计算安全性

## 1.4 完善保密性与计算安全性的比较

## 1.5 完善保密性的获得密钥协商

## 1.5.1 优先提取

## 1.5.2 信息协调

## 1.5.3 保密增强

## 1.6 优先提取与优先退化

## 1.7 存在主动攻击时的保密增强

## 参考文献

## 第2章 相关免疫函数

## 2.1 相关免疫布尔函数及其基本性质

## 2.2 相关免疫阶与代数次数的相互制约

## 2.3 相关免疫布尔函数的构造和计数

## 2.3.1 结构定理

## 2.3.2 一阶相关免疫布尔函数的构造和计数

## 2.3.3 高阶相关免疫布尔函数的构造和计数

## 2.4 布尔函数的广义相关免疫性

2.5  $GF(q)$  上的相关免疫函数

## 参考文献

## 第3章 弹性函数

## 3.1 弹性函数及其基本性质

## 3.2 弹性函数的存在性与唯一性

## 3.3 弹性函数的构造

## 3.4 仿射函数的弹性阶

## 3.5 弹性阶上确界与代数次数的关系

## 参考文献

## 第4章 非线性性

## 4.1 布尔函数的非线性度和线性度

## 4.2 布尔函数非线性度与相关免疫阶的关系

## 4.3 高度非线性布尔函数Bent函数

## 4.4 高度非线性均衡布尔函数的构造

4.4.1  $n = 2m$ 4.4.2  $n = 2m(2 + 1)$ ,  $S$ 为奇数4.4.3  $n$ 为奇数

## 4.5 特征为2的域上的多输出函数的非线性性

## 4.6 一般有限域上的函数的非线性性

## 参考文献

## 第5章 密码函数的其它安全设计

## 5.1 差分分布

## 5.2 特殊的差分分布：雪崩与扩散

## &lt;&lt;对称密码学&gt;&gt;

5.3 高阶差分分布

5.4 高阶自相关性

5.5 正形置换

5.6 全距置换

参考文献

第二篇 序列密码

第6章 序列密码的基础理论

6.1 序列的线性复杂度和最小周期

6.2 序列的根表示和迹表示

6.3 和序列与乘积序列

6.4 m-序列及其密码学特性

6.5 密钥序列的稳定性

6.6 线性递归序列的综合

6.6.1 B - M算法

6.6.2 Games - Chan算法

6.7 序列密码的研究现状简述

6.7.1 伪随机序列的生成现状

6.7.2 对序列密码的攻击现状

6.7.3 序列密码的某些非主流问题

参考文献

第7章 前馈序列

7.1 Bent序列

7.2 几何序列

7.3 几何序列之例一GMW序列

7.4 几何序列之例二瀑布型GMW序列

7.5 NO序列

参考文献

第8章 对数序列

8.1 对数序列的定义、定理

8.2 对数序列之例一Legendre序列

8.3 对数序列之例二R为奇素数

8.4 对数序列之例三R为2的幂

8.5 对数序列的推广广义Jacobi序列

参考文献

第9章 钟控序列

9.1 Jennings复合序列

9.2 停一走生成器

9.3 Gunther生成器

9.4 缩减序列互缩序列

9.5 缩减序列自缩序列

9.6 缩减序列广义自缩序列

9.7 广义自缩序列的特例

参考文献

第10章 稀疏序列

10.1 稀疏序列与信息隐藏

10.2 自缩乘积序列与自扩序列

10.3 基于GF (q) 上m-序列的稀疏序列

## &lt;&lt;对称密码学&gt;&gt;

## 10.4 基于乘方剩余符号的稀疏序列

## 参考文献

## 第三篇 分组密码

## 第11章 分组密码的设计与安全性

## 11.1 分组密码的设计准则

## 11.1.1 安全性

## 11.1.2 简捷性

## 11.1.3 有效性

## 11.1.4 透明性和灵活性

## 11.1.5 加解密相似性

## 11.2 分组密码的设计技巧

## 11.2.1 计算部件

## 11.2.2 计算部件的组合

## 11.2.3 关于密钥长度

## 11.3 分组密码的工作模式

## 11.4 典型攻击方法

## 11.4.1 朴素的攻击：穷举搜索

## 11.4.2 差分密码分析

## 11.4.3 线性密码分析

## 11.4.4 计时攻击和能量攻击

## 11.5 分组密码的随机算法

## 参考文献

## 第12章 分组密码DES

## 12.1 DES概述

## 12.2 DES的计算部件

12.2.1 初始置换IP与其逆置换IP<sup>-1</sup>

## 12.2.2 扩充变换E

12.2.3 8个S盒S<sub>1</sub>、S<sub>2</sub>、...、S<sub>8</sub>

## 12.2.4 置换P

## 12.3 DES的加密算法和解密算法

## 12.4 DES的C-源程序代码

## 12.5 DES的安全性

## 12.6 对DES的差分密码分析

## 参考文献

## 第13章 各种分组密码设计方案

## 13.1 分组密码IDEA

## 13.2 IDEA的C-源程序代码

## 13.3 RC5与RC6

## 13.4 RC5与RC6的C-源程序

## 13.5 Feistel网络的变形

## 13.6 分组密码Twofish简介

## 13.7 Twofish的C-源程序

## 参考文献

## 第14章 AES算法 ( RIJNDAEL )

## 14.1 AES竞争过程及RIJNDAEL概述

## 14.2 RIJNDAEL的数学基础和设计思想

## 14.2.1 有限域GF(2)

## &lt;&lt;对称密码学&gt;&gt;

14.2.2 系数在GF(2)上的多项式

14.2.3 设计思想

14.3 算法说明

14.3.1 状态、密钥种子和轮数

14.3.2 轮函数

14.3.3 密钥扩展

14.3.4 RIJNDAEL密码的加密算法

14.3.5 加解密的相近程度 / 解密算法

14.4 实现方面

14.4.1 8位处理器

14.4.2 32位处理器

14.4.3 并行性

14.4.4 解密算法的实现

14.4.5 硬件适应性

14.5 设计选择的诱因以及安全性分析

14.6 RIJNDAEL的C-源程序代码

参考文献

第15章 分组密码SAFER+及其变形

15.1 SAFER+ 概述

15.2 SAFER+ 的C-源程序代码

15.3 SAFER+ M算法描述

15.4 SAFER+ M与SAFER计算量和数据量的比较

15.5 SAFER+ M的加解密相似性

15.6 SAFER+ M的安全性

15.6.1 线性层的扩散性能：与SAFER+ 比较

15.6.2 SAFER+ M的差分密码分析

参考文献

<<对称密码学>>

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>