

<<混沌加密算法与Hash函数构造研究>>

图书基本信息

书名：<<混沌加密算法与Hash函数构造研究>>

13位ISBN编号：9787121130229

10位ISBN编号：712113022X

出版时间：2011-4

出版时间：电子工业出版社

作者：王永，李昌兵，何波 编著

页数：197

字数：291000

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>

## <<混沌加密算法与Hash函数构造研究>>

### 内容概要

本书紧跟混沌密码学的国际前沿，探讨了当前基于混沌理论的加密算法和Hash函数设计两项热点技术。

在混沌基本理论和密码学的基础上，详细介绍了混沌分组密码、混沌流密码、混沌图像加密算法、混沌公钥密码和混沌Hash函数，以及混沌加密算法和Hash函数的安全性分析指标，探析了基于混沌的加密算法和Hash函数的最新国际研究成果，以及混沌密码算法设计的主要思路和发展趋势。

本书可作为高等院校数学、计算机、通信、信息安全等专业从事混沌密码研究的本科生、研究生、教师和科研人员的研究用书或参考资料。

本书可作为高等院校数学、计算机、通信、信息安全等专业从事混沌密码研究的本科生、研究生、教师和科研人员的研究用书或参考资料。

## 书籍目录

## 第1章 混沌理论基础与混沌密码学的发展

## 1.1 混沌理论基础

## 1.1.1 混沌的定义

## 1.1.2 混沌的运动特征

## 1.1.3 混沌的判断准则

## 1.2 密码学基础知识

## 1.2.1 密码学基本概念

## 1.2.2 流密码系统简介

## 1.2.3 分组密码系统简介

## 1.2.4 公开密钥密码系统简介

## 1.2.5 密码分析与算法安全

## 1.2.6 消息认证与Hash函数简介

## 1.3 混沌密码学的发展

## 1.3.1 混沌与密码学的关系

## 1.3.2 混沌密码的起源与研究现状

## 1.4 本章小结

## 第2章 基于混沌的分组加密算法

## 2.1 基于混沌的S盒设计方法

## 2.1.1 S盒简介

## 2.1.2 S盒的性能评价标准

## 2.1.3 基于混沌的S盒设计方法

## 2.2 混沌和代数群运算结合的分组加密算法

## 2.2.1 分段线性映射

## 2.2.2 基于混沌和代数群运算的分组加密算法

## 2.2.3 安全性与性能分析

## 2.3 基于混沌的动态S盒分组加密算法

## 2.3.1 混沌映射的选择与分析

## 2.3.2 S盒构造算法描述

## 2.3.3 S盒仿真试验与性能测试

## 2.3.4 一种基于动态S盒的加密算法[10,50]

## 2.4 本章小结

## 第3章 基于混沌的流加密算法

## 3.1 随机序列与伪随机序列的检测标准

## 3.1.1 频率测试 (FT)

## 3.1.2 块内频率测试 (FTB)

## 3.1.3 游程测试 (RT)

## 3.1.4 块内比特1的最长游程测试 (LROBT)

## 3.1.5 二进制矩阵阶测试 (BMRT)

## 3.1.6 离散傅里叶变换 (谱测试 (DFTT))

## 3.1.7 非重叠模板匹配测试 (NTMT)

## 3.1.8 重叠模板匹配测试 (OTMT)

## 3.1.9 Maurer通用统计测试 (MUST)

## 3.1.10 LZ压缩测试 (LZCT)

## 3.1.11 线性复杂度测试 (LCT)

## 3.1.12 串行测试 (ST)

## &lt;&lt;混沌加密算法与Hash函数构造研究&gt;&gt;

- 3.1.13 近似熵测试 (AET)
  - 3.1.14 累积和测试 (CST)
  - 3.1.15 随机偏离测试 (RET)
  - 3.1.16 随机偏离变量测试 (REVT)
  - 3.2 基于混沌的伪随机数发生器
    - 3.2.1 从混沌序列中获取整数序列的常用方法
    - 3.2.2 基于混沌的伪随机字节流产生方法
    - 3.2.3 基于时空混沌的伪随机数发生器
  - 3.3 基于时空混沌的快速流密码算法
    - 3.3.1 基本运算的执行效率对比
    - 3.3.2 快速伪随机数发生器的设计分析
    - 3.3.3 伪随机数发生器的算法描述
    - 3.3.4 流加密和解密算法
    - 3.3.5 算法的性能分析
  - 3.4 基于混沌空间划分的流密码
    - 3.4.1 基于混沌空间划分的流加密算法
    - 3.4.2 改进的算法及其安全性分析
  - 3.5 一种基于多个Logistic映射的流加密算法
    - 3.5.1 加密和解密算法
    - 3.5.2 性能分析
  - 3.6 本章小结
- 第4章 基于混沌的图像加密算法
- 4.1 基于混沌的图像置乱方法
    - 4.1.1 猫映射
    - 4.1.2 面包师映射
    - 4.1.3 标准映射
  - 4.2 基于置乱扩散结构的图像加密算法
  - 4.3 基于三维猫映射的图像加密算法及其安全性分析
    - 4.3.1 二维猫映射到三维猫映射的扩展
    - 4.3.2 扩散变换
    - 4.3.3 密钥产生规则
    - 4.3.4 图像加密/解密算法描述
    - 4.3.5 算法的性能分析
    - 4.3.6 对算法的攻击
  - 4.4 改进的置乱扩散型图像加密算法
    - 4.4.1 变控制参数的图像加密算法
    - 4.4.2 合并置乱与扩散操作的图像加密算法
  - 4.5 本章小结
- 第5章 基于混沌的公钥加密算法
- 5.1 混沌公钥算法简述
  - 5.2 基于Chebyshev映射的公钥密码算法
    - 5.2.1 Chebyshev多项式定义和性质
    - 5.2.2 公钥加密算法
    - 5.2.3 算法软件实现中的问题分析
    - 5.2.4 算法的安全性分析
  - 5.3 对基于Chebyshev映射的公钥算法的攻击
  - 5.4 改进的Chebyshev公钥加密算法

## <<混沌加密算法与Hash函数构造研究>>

- 5.4.1 有限域中的Chebyshev多项式及其性质
- 5.4.2  $T_n(x)$ 中 $x$ 的取值分析
- 5.4.3  $T_n(x)$ 自相关函数的二值特性
- 5.4.4 改进的算法描述与安全分析
- 5.5 本章小结
- 第6章 基于简单混沌映射的Hash函数
  - 6.1 基于变混沌参数的Hash函数构造
    - 6.1.1 算法描述
    - 6.1.2 对Hash函数的分析
  - 6.2 基于广义混沌映射切换的Hash函数
    - 6.2.1 切换混沌映射的益处
    - 6.2.2 算法描述
    - 6.2.3 算法分析
    - 6.2.4 算法小结
  - 6.3 基于DM结构的混沌Hash函数构造
    - 6.3.1 Hash函数构造算法设计
    - 6.3.2 算法的安全与性能分析
  - 6.4 一类基于混沌映射构造Hash函数碰撞分析
    - 6.4.1 对一种基于二维混沌映射的Hash函数的碰撞分析
    - 6.4.2 对一种基于广义混沌映射切换的Hash函数的碰撞分析
    - 6.4.3 构造混沌Hash函数的建议
  - 6.5 本章小结
- 第7章 基于时空混沌的Hash函数
  - 7.1 时空混沌模型分析
    - 7.1.1 耦合映像格子模型
    - 7.1.2 有限精度下耦合映像格子序列的周期
    - 7.1.3 耦合映像格子模型中格子间的同步稳定性
  - 7.2 基于时空混沌的Hash函数构造与分析
    - 7.2.1 基于调整时空混沌参数的Hash函数构造方案
    - 7.2.2 基于调整时空混沌状态的Hash函数构造算法
    - 7.2.3 改进的基于调整时空混沌状态的Hash函数
  - 7.3 基于二维耦合映像格子的Hash函数构造方案
    - 7.3.1 二维耦合映像格子模型的分析与参数设置
    - 7.3.2 算法描述和单轮迭代次数的确定
    - 7.3.3 性能与安全性分析
    - 7.3.4 对比分析
    - 7.3.5 其他分析
  - 7.4 本章小结
- 参考文献

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>