

<<混沌密码学原理及其应用>>

图书基本信息

书名：<<混沌密码学原理及其应用>>

13位ISBN编号：9787030246776

10位ISBN编号：7030246772

出版时间：2009-7

出版时间：科学出版社

作者：廖晓峰 等著

页数：274

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>

## <<混沌密码学原理及其应用>>

### 前言

1999年10月, 我受香港城市大学电子工程系黄国和 (K.W.Wong) 博士的邀请到香港做为期一年的合作研究。

当时我的主要工作集中于时滞神经网络的分岔与混沌现象的研究, 还未涉及混沌应用于信息安全领域。但是黄国和博士每周都与他的博士生和硕士生们讨论混沌密码方面的学术问题, 由此引起了我对此领域的兴趣。

但由于我的工作重心并不在此, 加之时间紧迫, 也未参加他们的“混沌密码”研究小组的讨论。

当时我就打算回到重庆大学后带一批博士生和硕士生从事“混沌密码学”的研究。

在我的第一批博士中肖迪 (本书的作者之一) 和邓绍江是最先从事“混沌密码学”研究的, 第二批博士中陈勇 (本书的作者之一) 和张林华也从事“混沌密码学”的研究。

我陆续培养了十余名从事这方面研究工作的博士。

我们从2000年9月开始举办的“混沌密码学”讨论班, 一直持续到现在, 同时我也先后派出了一些博士生到黄国和博士那里进行合作研究, 他们分别是向涛 (本书的作者之一)、周庆、王永、杨华干和韦鹏程。

随着计算机和网络技术的日益普及, 信息安全已成为学术界和企业界所共同关注的研究热点和关键问题。

安全功能的复杂性以及攻击手段的层出不穷, 迫切需要研究和开发出更多安全、高效、可靠的信息安全技术。

学术界正在探讨将一些非传统的新颖方法引入信息安全领域。

将混沌理论引入信息安全领域是当前国际非线性科学和信息科学两个学科交叉融合的热门前沿课题之一。

比如我国的《国家中长期科学和技术发展纲要 (2006-2020)》在支持的重点领域及其优先主题“核心数学及其在交叉领域的应用”的主要研究方向就包括“离散问题、随机问题、量子问题以及大量非线性问题中的数学理论和方法等”。

我国国家自然科学基金在2003年的重大项目“网络与信息安全研究计划”中也将“复杂性理论在信息安全中的应用及密码算法分析研究”列入了计划。

混沌和密码学之间具有天然的联系和结构上的某种相似性, 启示着人们把混沌应用于密码学领域。

混沌的轨道混合特性 (与轨道发散和初始值敏感性直接相联系) 对应于传统加密系统的扩散特性; 而混沌信号的类随机特性和对系统参数的敏感性对应于传统加密系统的混乱特性。

可见, 混沌所具有的优异混合特性保证了混沌加密器的扩散和混乱作用可以和传统加密算法一样好。

另外, 很多混沌系统与密码学常用的Feistel网络结构是非常相似的。

通过类比研究混沌理论与密码学, 可以彼此借鉴各自的研究成果, 促进共同的发展。

## <<混沌密码学原理及其应用>>

### 内容概要

混沌密码学是非线性科学与密码学交叉融合的一门新的科学。

《混沌密码学原理及其应用》取材新颖，概念清晰，书中不仅介绍了数字混沌学所涉及的基础理论和各种代表性的算法，同时也涵盖了混沌密码学的最新研究成果，以及本学科最新的发展方向。

《混沌密码学原理及其应用》全面而详细地介绍了混沌密码学的理论和相关算法。

全书共分为6章，包括混沌理论与密码学基础、基于混沌的分组密码、基于混沌的流密码、混沌公钥密码技术、混沌Hash函数、混沌密码学的安全应用等内容。

《混沌密码学原理及其应用》可供高等院校数学、计算机、通信、信息安全等专业本科生、研究生、教师和科研人员参考。

## &lt;&lt;混沌密码学原理及其应用&gt;&gt;

## 书籍目录

前言?第1章 混沌理论与密码学基础?1.1 混沌理论基础?1.1.1 混沌理论的历史回顾?1.1.2 混沌的定义?1.1.3 混沌运动的特征?1.1.4 混沌研究的判据与准则?1.1.5 几种典型的混沌系统?1.1.6 混沌的应用?1.2 密码学概述?1.2.1 现代密码学?1.2.2 密码学基本概念?1.2.3 密码系统的分类?1.2.4 对称密钥密码系统?1.2.5 公钥密码?1.2.6 分组密码?1.2.7 序列密码?1.2.8 随机数发生器?1.2.9 Hash函数?1.2.10 密码分析与算法安全?1.2.11 混沌密码学?第2章 基于混沌的分组密码?2.1 分组密码简介?2.2 分组密码的工作模式?2.2.1 电子密码本 (ECB) 模式?2.2.2 密码分组链接 (CBC) 模式?2.2.3 密码反馈 (CFB) 模式?2.2.4 输出反馈 (OFB) 模式?2.3 分组密码的设计原则?2.4 分组密码的体系结构?2.4.1 代替置换结构?2.4.2 Feistel结构?2.4.3 其他结构?2.5 基于SPN (Feistel) 结构的混沌分组密码?2.5.1 混沌S盒的设计?2.5.2 基于Feistel结构的混沌分组密码?2.6 基于检索机制的混沌分组密码?2.7 基于迭代机制的混沌分组密码?2.7.1 基于逆向迭代混沌系统的分组密码?2.7.2 基于正向迭代混沌系统的分组密码?第3章 基于混沌的流密码?3.1 流密码的相关知识?3.1.1 流密码系统?3.1.2 典型的传统流密码简介?3.2 随机数与伪随机数的检测标准?3.2.1 频率测试?3.2.2 块内频率测试?3.2.3 游程测试?3.2.4 块内比特1的最长游程测试?3.2.5 二进制矩阵阶测试?3.2.6 离散傅里叶变换 (谱) 测试?3.2.7 非重叠模板匹配测试?3.2.8 重叠模板匹配测试?3.2.9 Maurer通用统计测试?3.2.10 LZ压缩测试?3.2.11 线性复杂度测试?3.2.12 串行测试?3.2.13 近似熵测试?3.2.14 累积和测试?3.2.15 随机偏离测试?3.2.16 随机偏离变量测试?3.3 基于混沌的流密码?3.3.1 基于混沌逆系统的流密码?3.3.2 混沌逆系统加密存在的问题与改进?3.3.3 从混沌系统中抽取二进制序列的方法?3.3.4 基于简单混沌系统的随机数产生方法?3.3.5 基于时空混沌的多比特随机数发生器?3.3.6 基于混沌空间划分的流密码?3.4 基于转换表的混沌加密算法?3.4.1 转换表的设计?3.4.2 加密与解密?3.4.3 算法的安全性分析?第4章 混沌公钥密码技术?4.1 公钥密码概述?4.1.1 RSA算法?4.1.2 ElGamal算法?4.1.3 椭圆曲线密码算法?4.1.4 基于混沌理论的公钥密码系统?4.2 细胞自动机公钥密码体制?4.2.1 细胞自动机密码系统?4.2.2 具体例子?4.3 一种ElGamal变形的混沌公钥密码?4.3.1 概述?4.3.2 公钥协议?4.3.3 具体例子?4.3.4 安全性分析?4.4 基于分布混沌系统公钥加密的加性混合调制?4.4.1 概述?4.4.2 分布动态加密?4.4.3 基于加性混合的DDE方案?4.4.4 安全性分析?4.5 基于Chebyshev映射的公钥密码算法?4.5.1 Chebyshev多项式的基本性质及推广?4.5.2 算法的描述?4.5.3 算法的安全性?4.5.4 进一步的研究结果?4.5.5 算法的改进?4.5.6 算法的应用实例?4.6 基于环面自同构的混沌公钥密码系统?4.6.1 环面的定义?4.6.2 环面自同构?4.6.3 算法的描述?4.6.4 算法的证明?4.6.5 抗攻击分析?4.6.6 实验方法和结果?4.6.7 算法的应用实例?4.6.8 递归数列和LUC系统?4.7 基于多混沌系统的公钥加密新技术?4.7.1 多混沌系统?4.7.2 基于多混沌系统的公钥加密方案描述?4.7.3 改进的实例?4.7.4 性能分析?第5章 混沌Hash函数?5.1 Hash函数?5.2 简单混沌映射的Hash函数构造?5.2.1 典型算法一?5.2.2 典型算法二及其演化算法?5.2.3 典型算法三?5.2.4 典型算法四?5.2.5 典型算法五?5.3 复杂混沌映射的Hash函数构造?5.3.1 典型算法一 (超混沌)?5.3.2 典型算法二 (调整时空混沌参数)?5.3.3 典型算法三 (调整时空混沌状态)?5.3.4 典型算法四 (调整时空混沌状态)?5.4 复合混沌映射的Hash函数构造?5.5 混沌神经网络的Hash函数构造?5.5.1 典型算法一?5.5.2 典型算法二?5.6 并行混沌Hash函数构造?5.6.1 算法结构?5.6.2 算法描述及其构造特点?5.6.3 性能分析?5.7 一种基于混沌的加密Hash组合算法?5.7.1 Wong算法及其安全分析?5.7.2 改进算法及其性能分析?5.7.3 其他的改进思路?第6章 数字混沌密码学的安全应用?6.1 引言?6.2 空域加密算法?6.3 频域加密算法?6.4 数字图像置乱算法研究发展?6.5 图像加密算法?6.5.1 像素位置变换?6.5.2 像素灰度变换?6.5.3 像素灰度链接变换?6.5.4 局部不同加密次数的图像加密?6.5.5 图像加密技术新进展?6.6 数字图像信息加密?6.7 图像加密评价标准?6.7.1 均方误差 (MSE) 和峰值信噪比 (PSNR)?6.7.2 直方图?6.7.3 相邻像素相关性分析?6.7.4 密钥空间分析?6.8 对加密算法的攻击?6.8.1 密钥的穷尽搜索?6.8.2 密码分析?6.9 加密图像的抗攻击性?6.9.1 剪裁攻击?6.9.2 噪声攻击?6.9.3 抗攻击算法?6.10 图像加密的用途?6.10.1 在邮政电子政务中的应用研究?6.10.2 在其他方面的应用研究?6.11 混沌在数字水印中的应用?6.11.1 数字水印技术概述?6.11.2 混沌数字水印?参考文献?

## <<混沌密码学原理及其应用>>

### 章节摘录

第1章 混沌理论与密码学基础    1.1 混沌理论基础    20世纪下半叶，非线性科学得到了蓬勃发展。

其中，对混沌现象的研究占了极大的份额。

半个世纪以来，人们对混沌运动的规律及其在自然科学各个领域的表现有了十分丰富的认识。

一般而言，混沌现象隶属于确定性系统而难以预测（基于其动力学形态对于初始条件的高度灵敏性），隐含于复杂系统但又不可分解（基于其具有稠密轨道的拓扑特征），以及呈现多种“混乱无序却有规则”的图像（如具有稠密的周期点）。

1.1.1 混沌理论的历史回顾    在现实世界中，非线性现象远比线性现象广泛。

混沌现象是指在确定性系统中出现的一种貌似无规则、类似随机的现象，是自然界普遍存在的复杂运动形式。

人们在日常生活中早已习以为常的种种现象，如钟摆的摆动、山石的滚动、奔腾的小溪、岸边海浪的破碎、股市的涨跌、漂浮的云彩、闪电的路径、血管的微观网络、大气和海洋的异常变化、宇宙中的星团乃至经济的波动和人口的增长……在它们看似杂乱无章的表面现象下却蕴涵着惊人的运动规律。

最早对混沌进行研究的是法国的庞加莱（H.Poincare）。

1913年，他在研究能否从数学上证明太阳系的稳定性问题时，把动力学系统和拓扑学有机地结合起来，并提出三体问题在一定范围内，其解是随机的。

## <<混沌密码学原理及其应用>>

### 编辑推荐

1 揭示了混沌与密码学之间的关系；2 介绍了混沌密码学的最新研究成果和最新发展方向；3 阐述了混沌在分组密码、序列密码和公钥密码等方面的研究；4 探讨了混沌密码学在图像、信息安全等领域的应用。

<<混沌密码学原理及其应用>>

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>