# 《几类复杂动力学系统的密码分析与设肌

## 图书基本信息

书名：《几类复杂动力学系统的密码分析与设计》

13位ISBN编号：9787560537153

10位ISBN编号：7560537154

出版时间：2010-9

出版社：西安交通大学出版社

作者：米波

页数：127

# 《几类复杂动力学系统的密码分析与设肌

## 前言

随着计算机与通信技术的飞速发展，社会对信息和信息技术的依赖性不断增强，预示着信息化时代的到来。然而，信息随时都有可能遭受窃取、篡改、伪造和重放等各种攻击，成为信息社会建设的瓶颈。因此，为维护信息化社会的有序运作，信息安全受到了各界的广泛关注。　　密码系统是解决信息安全问题最基本的手段。复杂系统的动力学行为和密码学之间有着天然的联系。它的一些动力学特性大致对应着密码系统的某些安全特征，而具有良好混合性的传统密码系统又暗示着复杂的动力学现象。目前，已提出了大量基于混沌和细胞自动机的密码设计方案，并进行了系统的分析。而细胞神经网络和复杂网络的动力学行为也得到了深入的理论研究，具有很好的密码学应用前景。　　作者主要从事复杂动力学系统在信息安全技术特别是密码学方面的应用研究。本书在对细胞自动机、混沌系统、细胞神经网络以及复杂网络等几类复杂动力学系统的密码学研究现状进行详细分析的基础上，根据信息论、密码学和复杂动力学系统理论提出一种基于算术编码的混沌加密系统。该系统解决了算法的可移植性、数字化后混沌动力学行为出现退化以及密钥相同时密钥流不变等问题，较以往算法有更好的性能和安全性。同时，将算术编码等同于一个非线性动力学系统，分析了它对系统安全性所作的贡献。

# 《几类复杂动力学系统的密码分析与设肌

## 内容概要

《几类复杂动力学系统的密码分析与设计》是作者在研究几类复杂动力学系统的密码分析与设计问题并取得了一些有意义和有实用价值研究成果的基础上编写而成。书中介绍和讨论了四个方面的内容：基于算术编码的混沌加密系统的分析与设计，基于细胞自动机的图像加密算法的分析与设计，细胞神经网络的密码学特性分析以及基于复杂网络的密钥分配问题研究。
《几类复杂动力学系统的密码分析与设计》适用于信息安全和非线性系统类专业人员参考。

# 《几类复杂动力学系统的密码分析与设肌

## 书籍目录

# 《几类复杂动力学系统的密码分析与设肌

## 章节摘录

作为一门综合性的交叉学科，密码学以计算机科学、数学、通信、控制等诸多学科为背景，是信息安全的基础，是保障信息系统安全最为关键的技术和最为基本的手段。尽管古老，但真正意义上的密码学却起源于香农（Shannon）确立现代信息论之后。1949年，他在《保密系统的通信理论》一文中，用信息论的观点对信息保密问题进行了全面的阐述，从而宣告了现代密码学体系的诞生。随后，DES、IDEA、AES等一些经典的对称密码体系逐渐成为公认的加密标准。1976年，狄非（Diffe）和海尔曼（Hell-man）的《密码编码学新方向》一文首次证明了无共享密钥保密通信的可能性，带来了密码学研究的第二次飞跃，为公钥密码算法RSA、ElGamal等的设计提供了理论基础。　　根据Kerckhoff原则，一个密码系统的安全性完全取决于对密钥的保密而与算法无关。无论算法多么安全，一旦密钥信息泄露，数据的机密性、完整性、认证性将难以得到保证。因此，密钥管理在信息系统安全中是至关重要的。尽管公钥密码体制避免了共享密钥的通信问题，但由于其运行速度慢，密钥长度长，且安全性无法得到证明，根本无法替代对称密码的主导地位，而通常用于密钥分配、数字签名等方面。　　即使密钥得到了妥善的管理，也并不意味着一个密码系统就是绝对安全的。作为密码学的两个重要分支，密码编码学在寻求高效、可靠的加密机制的同时，密码分析学也正致力于信息的破译或消息的伪造。

# 《几类复杂动力学系统的密码分析与设肌

## 版权说明