<<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

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、杨华千和韦鹏程。

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年的重大研究项目“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。

<<混沌密码学原理及其应用>>

书籍目录

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