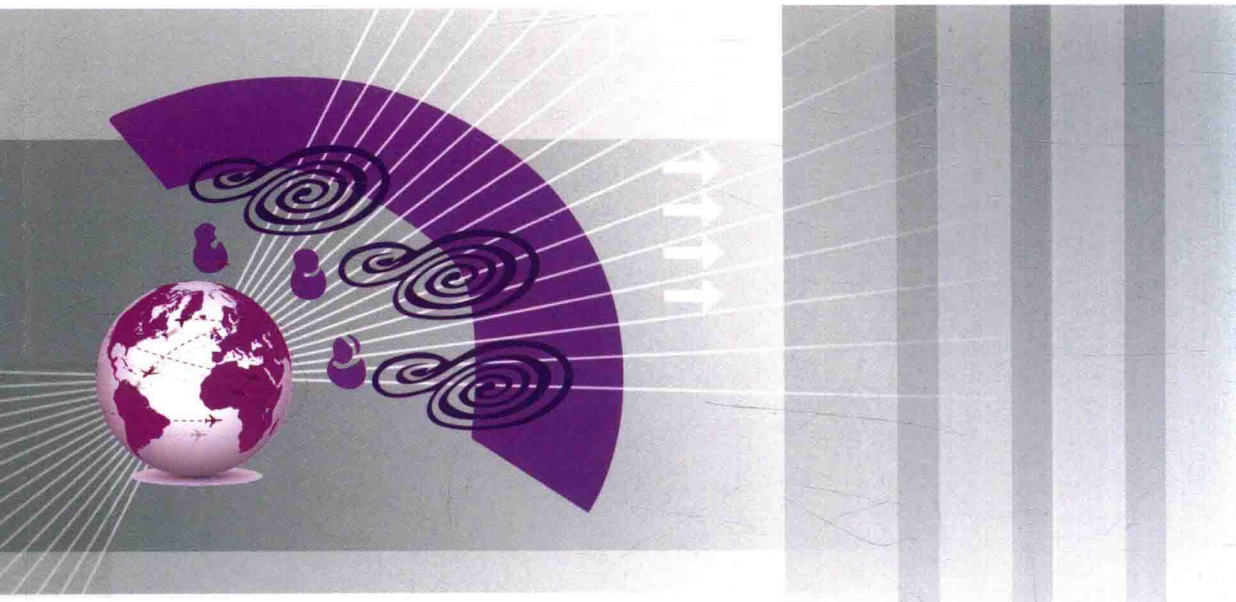
信息化网络平台研究丛书

混沌密码学与信息安全

徐　刚◎著



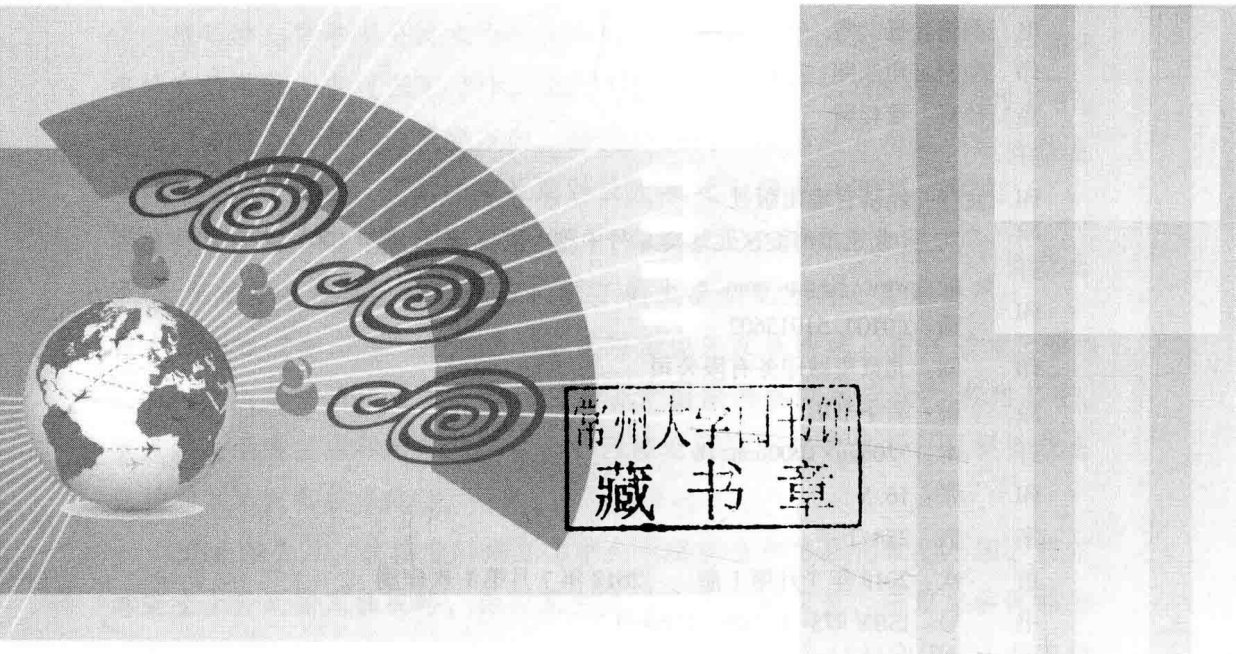
CHAOTIC CRYPTOGRAPHY AND INFORMATION SECURITY

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

信息化网络平台研究丛书

混沌密码学与信息安全

徐 刚◎著



CHAOTIC CRYPTOGRAPHY AND
INFORMATION SECURITY

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

图书在版编目（CIP）数据

混沌密码学与信息安全/徐刚著. —北京：经济管理出版社，2018.3
ISBN 978-7-5096-5766-9

Ⅰ.①混… Ⅱ.①徐… Ⅲ.①密码学 ②信息安全 Ⅳ.①TN918.1 ②TP309

中国版本图书馆 CIP 数据核字（2018）第 086941 号

组稿编辑：杨 雪
责任编辑：杨 雪 王 硕
责任印制：司东翔
责任校对：董杉珊

出版发行：经济管理出版社
（北京市海淀区北蜂窝 8 号中雅大厦 A 座 11 层 100038）
网 址：www.E-mp.com.cn
电 话：（010）51915602
印 刷：北京玺诚印务有限公司
经 销：新华书店
开 本：720mm×1000mm/16
印 张：16.5
字 数：254 千字
版 次：2018 年 7 月第 1 版 2018 年 7 月第 1 次印刷
书 号：ISBN 978-7-5096-5766-9
定 价：59.00 元

作者简介

徐刚，男，1979年10月生，博士，副教授，中国计算机学会会员，中国密码学会会员。主要研究领域为混沌密码学、计算机信息安全。

组稿编辑：杨　雪

责任编辑：杨　雪　王　硕

封面设计：

前　言

随着国民经济的快速发展以及社会的不断进步，我国已经成为名副其实的网络大国，网民数量和智能手机的持有量都位居世界前列，而我国的网络空间正面临诸多的安全威胁，成为了网络攻击最大的受害国，整体安全水平与网络强国相比仍然有不小差距。

密码学与信息安全技术的研究与完善，是应对以上安全威胁和网络攻击的有效手段。在《国家“十二五”科学和技术发展规划》中将密码基础理论列为重大科学问题研究方向，强调加快网络与信息安全技术创新、保障网络与信息安全。《国家中长期科技发展规划纲要（2006~2020）》中明确提出要重点研究新型密码技术。“高维系统全局分叉和混沌”和“高维/无限维非线性系统动力学与控制”的主要研究方向在国家自然科学基金委员会的“十二五”发展规划中被列为优先发展领域。在《“十三五”国家科技创新规划》重大科技项目中，“国家网络空间安全”名列其中，重点发展涵盖信息和网络两个层面的网络空间安全技术体系，以提升信息保护和网络防御技术能力。

2014 年 2 月，我国专门成立了中央网络安全和信息化领导小组，将信息安全上升到国家级战略，由国家主席习近平担任组长，着重完善网络安全的顶层制度设计。2015 年“混沌密码理论及应用”（F020701）首次被列为国家自然科学基金重点项目的资助领域。

在国外，1998 年美国国防部通过多学科大学研究计划资助加州大学的科研项目“基于非线性动力学和混沌的数字通信装置”（DE-FG03-95ER14516，1998-2003）总计 750 万美元。2001 年欧盟在第 5 科技框架计划资助多个西欧国家科学家联合从事项目“激光二极管发射器实现混沌光通信”（IST-2000-29683，2001-2004，310 万欧元）研究。

从国家安全战略层面，开展混沌密码设计、分析及其在多媒体保密通信中的应用研究，将推动我国下一代互联网、物联网和实施国家宽带网等科技产业化工程的安全运行，具有重大理论意义和实际应用价值。

随着国内经济信息化水平的提高与电子商务的快速发展，人们在网上进行银行转账、电子支付等操作也越来越多，随之而来的网络安全事件几乎每天都发生在人们身边，各种钓鱼网站、木马和蠕虫病毒等的入侵与破坏，黑客窃取客户端支付应用的账号与密码等，时时威胁着个人隐私信息和财产的安全，每位网民都面临着前所未有的信息安全挑战与威胁，而由此带来的经济损失更是数目惊人，难以估量。

物联网、云计算和大数据等信息技术的飞速发展，使得多媒体数据如图像、音频、视频在传输、存储、处理等方面的安全性越来越引起人们的重视。多媒体数据所具有的冗余强、数据量大及相邻元素之间的强相关性等特征，使得传统的文本加密算法不适合于多媒体数据的加（解）密。

同时，传统的文本加密算法对于多媒体数据加（解）密来说，实时加密实现难度大，破坏原有多媒体数据的专有存储格式等弊端都暴露了出来，为通信安全带来了新的挑战。

设计安全性高而又实用的密码系统是当今密码学界研究的热点。混沌现象是非线性动力系统中出现的对初始条件敏感的、确定性的、类似随机的复杂动力学行为，混沌分组密码的研究是近年来研究最多的领域之一。当前的一些研究成果对混沌密码系统及其部件的安全性做了相当细致的分析，从而使这些密码算法具有较高的实用价值和安全性。

本书对混沌密码的设计与分析进行了较为全面的介绍，主要涉及以下内容：

本书介绍了利用多（高）维混沌系统构造高强度、安全性能好的S盒方法。借助于混沌系统的优良特性，阐述了采用多（高）维混沌系统加仿射变换的数学方法，构造出高安全性的S盒方法，并对构造的混沌S盒进行相关密码分析。

在时空混沌系统特性的分析基础上，本书针对现有的基于混沌的Hash函数的构造中并行性以及运算效率不高的问题，描述了一种并行的基于时空混沌的单向Hash函数的构造方法。该方法利用了帐篷映射计算简单的

特点，结合交叉耦合映像格子避免有限精度实现产生的短周期行为，通过参数调制的方法实现并行计算。

时空混沌相对于低维混沌系统具有更长的周期和更多正的 Lyapunov 指数，使得其在理论上可以用于设计性能良好的 Hash 函数。仿真实验及相关密码学分析表明，该方案很好地达到了 Hash 函数的各项性能要求，既有很高的安全性，又很好地实现了并行计算，从而提高了执行的效率。

本书基于 Logistic 映射和时空混沌系统，介绍了一个密钥长度为 256 bit 的图像分组密码算法，将 256 bit 的明文图像分组加密为等长的密文。算法引入的辅助密钥和设计的迭代次数敏感地依赖于明文分组和密钥，交替迭代混沌系统及 Arnold 映射实现了像素值的扰乱和位置置乱。计算机仿真和密码分析表明，该算法具有对明文和密钥敏感、密钥空间大、可扩展性强等特点，具有良好的加密效果，适用于安全通信领域。

基于 Chebyshev 多项式及有限域上的 Chebyshev 多项式，将其与类 ElGamal 算法结合，详细介绍了混沌公钥密码算法和身份认证方案的设计方法，并对其进行了相关密码学分析，指出其漏洞，为混沌公钥密码算法及身份认证算法的设计指出思路和方向。

本书的主要内容安排如下：

（1）第 1 章至第 4 章对传统密码学与信息安全领域涉及的基础理论和原理做了介绍，包括密码学基础知识、分组密码学基础、Hash 函数及数字图像加密基础。

（2）第 5 章对混沌的概念、性质及研究方法做了总结与概述。

（3）第 6 章对混沌密码学中混沌分组密码、混沌 S 盒的构造、混沌 Hash 函数的构造及混沌图像加密技术进行了详细归纳和分析。

（4）第 7 章介绍了基于多（高）维混沌系统和低维混沌系统与仿射变换相结合的 S 盒的构造与分析方法；密码分析证明了构造的 S 盒具有很好的抵抗差分分析和线性分析的能力。

（5）第 8 章提出了基于时空混沌的一种并行 Hash 函数的构造方法，并作了相应的密码分析；仿真结果表明，这种方法提高了运行效率，适于在并行平台推广。

（6）第 9 章设计了一种基于交替迭代混沌系统的图像加密算法，该算

法引入了辅助密钥，具有很强的可扩展性；实验仿真的结果表明，这种图像加密算法具有很高的安全性。

（7）第10章利用Chebyshev多项式优良的密码学性能，详细介绍了两种混沌公钥密码算法的设计方法，并对其进行密码学分析。

（8）第11章介绍了一种带有身份认证功能的密钥协商方案和基于有限域Chebyshev多项式的身份认证算法，并对算法的安全性作了分析与总结。

（9）第12章介绍了无简并高维超混沌系统的构造及其密码算法的设计方法，给出了硬件实现的途径与方式。

（10）第13章对本书的工作进行了总结并对以后的研究工作做了展望。

本书在撰写过程中，得到了很多业内人士的大力支持与帮助。感谢已故的香港城市大学电子工程系K. W. Wong（黄国和）博士在本人访问学习期间所给予的指导与点拨，在此深切缅怀。感谢北京科技大学闵乐泉教授和北京电子科技学院赵耿教授，他们在科研工作上的谆谆教诲和指导、严谨的治学态度使我受益良多。感谢读博士期间课题组的郝舒欣和袁阳，为本书提供了一手的资料和成果，还要感谢河南财经政法大学计算机与信息工程学院领导以及科研处同事在本书撰写过程中所提供的帮助与支持。

由于作者水平有限、编写时间仓促，所以书中错误和不足之处在所难免，恳请广大读者批评指正。

目录 Contents

1 信息安全与密码学算法

密码技术是信息与网络安全技术的核心，它主要由密码编码技术和密码分析技术两部分构成。密码编码技术的主要任务是寻求产生安全性高的有效密码算法和协议，基于一些数学原理或其他手段来隐藏信息，以达到对信息进行加密认证的要求。密码分析技术的主要任务是研究密码编码技术的漏洞和弱点，获取密钥、破译密码或伪造论证信息，实现窃取机密信息、干扰信息传输或进行破坏活动。

1.1 密码学基础

密码学是一门古老而又年轻的学科，其起源可以追溯到几千年前的古埃及、古巴比伦、古罗马和古希腊，最早的古典密码主要应用于战争、外交等领域。交战双方都为了保护自己的通信安全、窃取对方情报而研究各种方法，这也是密码学主要包含的两部分内容：一是为保护自己的通信安全进行加密算法的设计和研究；二是为窃取对方情报而进行密码分析。因此，密码学是这一矛盾的统一体。

1.1.1 密码学简史

密码技术是密码学的核心，密码技术的发展历程分为三个阶段：手工阶段（古代密码）、机械阶段（古典密码）和计算机阶段（现代密码）。

1.1.1.1. 手工阶段的古代密码

密码起初只是人们之间的一种游戏或是艺术，但人类自从有了战争，就面临着通信安全的更高需求，密码技术便应运而生，许多古代文明包括埃及人、希伯来人等，都在实践中逐步发明了一套独特的密码系统。

比较典型的古代加密方法是斯巴达人将纸条缠绕在木棒上的加密技术。公元前400年斯巴达军官之间为了传递秘密信息，将一张羊皮纸条缠绕在一个锥形指挥棒上，将要保密的信息写在纸上，然后解下羊皮纸，上面的消息就变得杂乱无章，但将它绕在另一个同等尺寸的棒子上后，就能恢复出原始的消息。

我国古代的记载中也有一些有趣的密码学技术，比如以藏头诗、藏尾诗及绘画等形式，将要表达的真正意思或“密语”隐藏在诗文或图画中的特定位置，一般人很难发现隐藏其中的消息。

可见自从有了文字以来，人们为了某种需要总是想方设法隐藏某些信息，以达到保证信息安全的目的，但是这些方法相对简单，只能靠人为的手工操作来完成加（解）密。这些古代加密方法体现了密码学的若干要素，比如隐藏和混乱。

1.1.1.2 机械阶段的古典密码

古典密码的加密方法一般是使用手工或机械变换的方式进行文字置换。古典密码系统已经初步体现出近代密码系统的雏形，比古代加密方法复杂，安全性得到了进一步的提升。古典密码的代表密码体制主要有：单表代替密码、多表代替密码及转轮密码。Caesar密码就是一种典型的单表代替密码；多表代替密码有Playfair密码、Vigenere密码和Hill密码；著名的Enigma密码是第二次世界大战中使用的转轮密码。

Caesar密码是已知的最早的代换密码，采用的是用手工或是机械的方式，将明文字母替换成其他字母、数字或符号的方法。Caesar密码是将26个英文字符选择后移3位的方法进行加密，解密只需将密文前移3位。密码表可以自由选择前移或后移几位，移动的位数也就是密钥。显然Caesar密码的密钥总数只有25个，采用尝试所有密钥进行解密的方法只需测试25次即可破解，这种算法的安全性较低，但在当时技巧性已经足够强了。