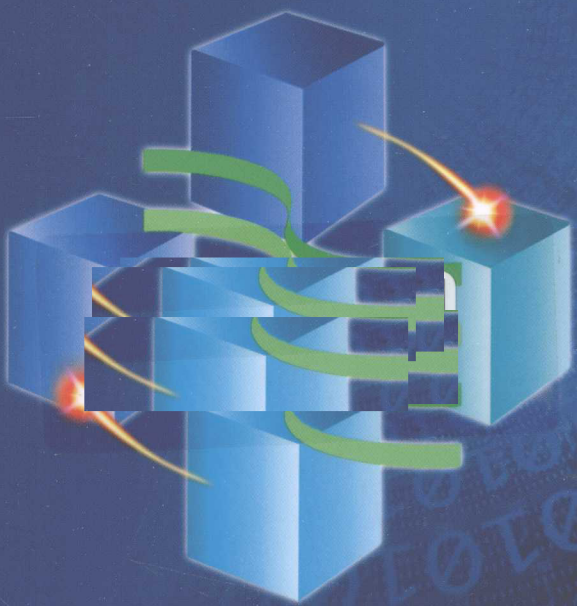
几类复杂动力学系统的密码分析与设计

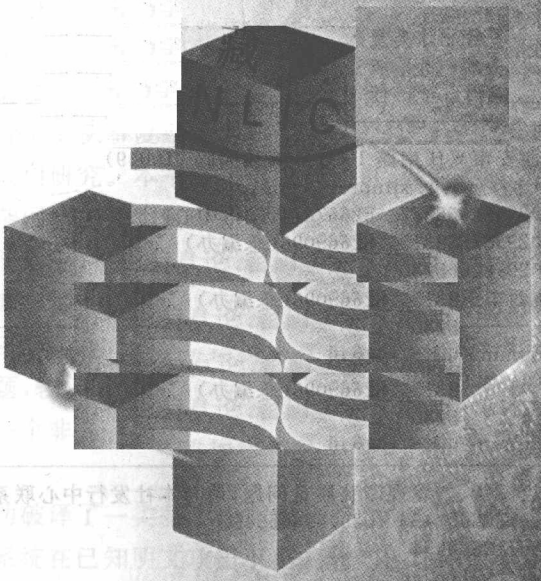
米波 著



西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

几类复杂动力学系统的密码分析与设计

米波 著



西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

内容提要

本书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。

本书适用于信息安全和非线性系统类专业人员参考。

图书在版编目(CIP)数据

几类复杂动力学系统的密码分析与设计/米波著. —西安：西安交通大学出版社，2010.9

ISBN 978-7-5605-3715-3

Ⅰ. ①几… Ⅱ. ①米… Ⅲ. ①动力系统(数学)-密码术-研究 Ⅳ. ①O19②TN918.1

中国版本图书馆 CIP 数据核字(2010)第 172747 号

书　　名	几类复杂动力学系统的密码分析与设计
著　　者	米　波
责任编辑	李　佳　田　华
出版发行	西安交通大学出版社 (西安市兴庆南路 10 号　邮政编码 710049)
网　　址	http://www.xjtupress.com
电　　话	(029)82668357　82667874(发行中心) (029)82668315　82669096(总编办)
传　　真	(029)82668280
印　　刷	陕西丰源印务有限公司
开　　本	850mm×1168mm　1/32　**印张** 4.25　**字数** 103 千字
版次印次	2010 年 9 月第 1 版　2010 年 9 月第 1 次印刷
书　　号	ISBN 978-7-5605-3715-3/TN·127
定　　价	18.00 元

读者购书、书店添货、如发现印装质量问题，请与本社发行中心联系、调换。

订购热线：(029)82665248　(029)82665249

投稿热线：(029)82664954

读者信箱：jdlgy@yahoo.cn

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。

成功破译了一类基于递归细胞自动机置换的图像加密算法，指出该系统在已知明文攻击下是脆弱的。在不改变算法基本结构的情况下，讨论了其可能的改进，分析了系统中密钥流发生器的设

计缺陷，并提出一种具有良好随机统计特性和不可预测性的细胞自动机密钥流发生器。

讨论了细胞神经网络一些可应用于密码设计的性质。研究了细胞神经网络中的混沌现象和布尔函数实现方法。

分析了无线传感器网络中密钥分配的限制条件，提出一种基于复杂网络同步的无线传感器网络密钥分配方案。

最后，本书对已完成的工作进行了全面的总结，并对今后的研究方向进行了展望。

该书的编写过程得到了重庆大学博士生导师廖晓峰教授的支持和帮助。麦欢欢、段书凯、陈勇博士也为本书的撰写提供了大量有价值的意见和建议，在此一并致谢。

作　者

2010 年 6 月

目 录

第1章 绪 论

1.1 研究背景与课题意义

以计算机和网络通信为代表的新技术革命，预示着人类正全面迈入信息化社会。随着人们生产、生活方式以及思想观念的巨大转变，信息已成为社会发展、文明进步中一种不可或缺的资源，而我国更是提出了《2006—2020年国家信息化发展战略》，将信息化提升到国家战略的高度。利用计算机和网络对信息进行收集、加工、存储以及交换等，已逐渐成为各行各业不可或缺的手段。而各种信息系统的建立和使用也造成了我们对计算机，尤其是对数据库和网络的依赖。

目前，各种信息化系统已逐渐成为国家关键的基础设施，它们支持着网络通信、电子商务、电子政务、电子金融、网络教育、网络计算以及公安、军事、医疗、社保等各个方面的应用。然而，随着信息重要性的日益突出，其安全问题已成为制约信息技术应用的一个巨大障碍。信息可能包含社会、政府、个人、军事等方面大量有价值甚至十分敏感的信息，由于它随时可能遭受到非法访问、窃取、篡改、阻截等恶意攻击，使得人们的生产、生活乃至国家安全受到威胁，也严重影响到国家信息化进程的持续健康发展。

事实上，信息系统的脆弱性是其本身所固有的。因此，人们有必要对其安全性问题进行全面、系统的研究。为维护信息社会的正常运行，政策、法律手段固然重要，但各种技术方法才是最为直接、有效的手段。信息安全技术涉及的范围很广，它主要包括密码技术、防火墙技术、虚拟专用网络技术、病毒与反病毒技术、数据库

安全技术、操作系统安全技术、物理安全与保密技术以及信息伪装、数字水印、电子现金、入侵检测、安全智能卡、PKI、网络安全协议等[1]。

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[2]。1949 年，他在《保密系统的通信理论》一文中[3]，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[4]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。事实上，一个新的加密机制只有在相当长的时间内经受住了密码分析的考验，才具有一定的应用价值。即便如此，随着密码分析学的不断发展，攻击方案的不断改进和计算机技术的日益更新，许多传统的加密方法已很容易被攻破。如广泛使用的 m -序列，只需知道 $2n$ 个比特(n 为寄存器的级数)的码元就能

破译该系统[1]；美国的加密标准 DES(56 比特)已经于 1997 年 6 月 17 日被攻破；2005 年又报道在商业应用中极其广泛的 Hash 散列算法 MD5 和 SHA1 已被成功的攻击；另据报道，1024 比特的 RSA 也可能在 2010 年被攻破。由此可见，信息安全领域亟待提出更为安全有效的信息保护手段。随着基础理论和实验条件的进步，人们逐渐意识到，一些非传统的信息加密与隐藏方法具有可观的研究价值和应用前景，而基于复杂动力学系统的密码学理论也因此受到广泛关注。

在特定的条件下，复杂动力学系统可能产生无组织的行为或不规则的进化。这种无序状态可能导致混沌现象或长周期序列的产生，从而启示人们将其应用于密码学领域。利用混沌来防止信息泄露的研究有两个分支，一种是通过混沌载波通信以提供保密性，一般称为混沌保密通信；而另一种是抛弃电信意义上的调制解调，设计基于密码学概念的混沌加密算法，在密钥的控制下保证信息安全，通常称为基于混沌的数字加密。混沌系统的一些基本特性，如确定性、对初始条件的敏感性、混合性、快速衰减的自相关性、长期不可预测性和伪随机性等，都同密码学的基本要求相一致。而其遍历性(ergodicity)和混合性(mixing)也很好地满足了密码学中混乱(confusion)和扩散(diffusion)的基本原则。因此，在上世纪六、七十年代，混沌密码学成为信息安全领域的研究热点，并建立起一套完善的理论体系。1951 年，冯·诺依曼正式提出了细胞自动机的概念。由于其简单的结构经过多次迭代就可以产生复杂的行为，因此受到学术界的高度重视。2002 年，沃尔弗拉姆(Wolfram)在其《一种新科学》一书中[5]，把细胞自动机提高到与牛顿三大定律相同的高度，认为它将成为所有科学的基础。在书中，他曾多次暗示“细胞自动机可以利用简单的规则产生出复杂的，类似随机的行为”，而这也正是密码学领域所关注的特性，使其成为近年来密码学研究的一个新方向。作为一种特殊的复杂动力学系统，细胞神经网络不但具有混沌、分叉等一些复杂的动力学

行为，它也能够通过参数的设计，实现细胞自动机的所有功能。尽管细胞神经网络已广泛应用于图像处理、模式识别的研究并取得了很好的效果，但还尚未涉足密码学领域。因此，它极有可能成为信息安全中下一个关注的焦点。

密钥管理是对称密码体系中一个不容忽视的问题，是保证信息安全的关键。尽管密钥管理协议在传统的网络中已经有了非常成熟的应用，但随着 ad-hoc 网络、无线传感器网络的兴起，我们不得不考虑其特殊的设备资源、组织结构，从而对密钥分配体制重新进行设计。复杂网络，特别是小世界网络，能够很好地描述各种自组织网络特定的拓扑结构，同时，它也具有诸如混沌、分岔、同步等复杂的动力学行为。因此，将复杂网络应用于密钥分配是非传统密码体制中一个值得关注的方面。

虽然基于复杂动力学系统的密码学研究在近些年来取得了可喜的进展，但仍存在一些重要的基本问题尚待解决。同时，复杂系统的基础理论也在不断地发展，许多新的科研成果对密码学研究具有很高的启发价值和借鉴意义。数字产品种类的多样性、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。一些非传统的新颖方法不仅丰富了密码学研究的内容，更为信息安全领域注入了新的活力。因此，设计具有自主知识产权的新型高性能的非传统密码体制是当前亟待解决的重要问题。

本书主要致力于复杂动力学系统在密码设计方面的应用研究。对基于混沌理论、细胞自动机、细胞神经网络以及复杂网络的加密系统设计、密钥分配等问题进行了详尽的讨论和分析；提出了复杂动力学系统在密码学应用中的优势和值得注意的问题；开辟了密码学研究的新思路，有助于丰富现代密码学的内容。

1.2　主要研究内容及成果

复杂动力学系统在密码学领域具有相当广泛的应用，本书仅涉及其中很小一部分，主要包括以下几个方面。

① 给出了细胞自动机、细胞神经网络以及复杂网络等几类复杂动力学系统的基本概念，分析了它们的研究现状。在对基于混沌理论、细胞自动机的一些典型的密码学方案进行了简要介绍的同时，指出了细胞神经网络以及复杂网络在密码学领域的研究价值。

② 提出了一种基于算术编码的混沌加密系统，从信息论、密码学的观点分析了文中的密钥流发生方法、密文长度等对系统安全和性能的影响，利用复杂动力学系统理论将算术编码等同于一个非线性动力学系统并对其进行了推广。系统设计也考虑了算法的可移植性，并解决了数字化后混沌动力学行为出现退化的缺点。

③ 成功破译了一类基于细胞自动机的图像加密系统，指出该系统在选择明文攻击下是脆弱的。在对算法本身进行改进的同时，分析了系统中密钥流发生器所存在的一些缺陷，提出了新的伪随机数序列产生方法。

④ 从混沌和布尔函数两个方面讨论了细胞神经网络可用于密码设计的一些性质。分析了细胞神经网络中的超混沌现象，并用细胞神经网络进行了布尔函数的鉴别和实现。

⑤ 提出了一种将复杂网络的同步现象用于无线传感器网络密钥分配的思想。

⑥ 最后对本书进行了全面的总结，并对今后的研究方向进行了展望。

1.3 本书的组织结构

本书主要的章节内容安排如下。

第1章简单介绍了本书的研究背景、意义和主要的研究内容及成果。

第2章对几类复杂动力学系统进行了详尽的论述。首先对目前基于混沌理论的密码技术进行了详细介绍，回顾了细胞自动机的研究背景和基本概念，对其在密码学领域的研究现状进行了系统的描述。然后，给出了细胞神经网络及复杂网络的一些基本概念，讨论了其理论和应用的研究进展。

第3章在香农保密系统信息理论的基础上提出一种基于算术编码的混沌加密系统，并通过实验和理论分析证明它不仅在性能上优于其它方法，而且具有更好的安全特性。

第4章对一类基于递归细胞自动机置换的图像加密算法进行了密码学安全分析，指出其在已知明文攻击下是脆弱的，并在不改变算法基本结构的情况下讨论了可能的改进。同时，分析了系统中密钥流发生器的设计缺陷，提出一种新的细胞自动机密钥流发生器并对其随机统计特性和线性复杂度进行了测试。

第5章从混沌和布尔函数两个方面来考察细胞神经网络一些可用于密码设计的性质。讨论了细胞神经网络中混沌和布尔函数的实现方法。

第6章分析了无线传感器网络中密钥分配的一些特殊要求，并根据其拓扑结构的复杂网络特性，提出一种基于复杂网络同步的密钥分配方法。

第7章是对本书内容的总结，并对基于复杂动力学系统的密码学研究前景进行了展望。

第2章 典型的混沌密码与其它的复杂动力学系统

2.1 混沌密码学

混沌是一种特殊的运动形式，是指在确定非线性系统中，不需附加任何随机因素亦可出现的类似随机的行为。混沌系统具有确定性、有界性、对初值的极端敏感性、长期不可预测性、正的最大Lyapunov指数、遍历性等特点。随着对混沌理论研究的不断深入，其成果也被扩展应用到其它学科领域，应用范围也越来越广泛。由于混沌的特点与密码学的特性相吻合，混沌理论于上世纪80年代末开始得到密码学界的关注，现已取得了许多研究成果。由于混沌系统对初值和控制参数的极端敏感，任何初值的微小偏差都会导致结果的显著变化，由混沌系统生成的混沌序列是一种非线性序列，具有伪随机性和非周期性，其结构复杂难以分析和预测，可以提供具有良好随机性、相关性和复杂性的伪随机序列，这些特性使混沌序列有可能成为一种实际可用的密码体制，为密码技术的研究开辟了一条新的研究途径。混沌理论及其发展历程在2006年陈勇的博士学位论文[6]中已有详细介绍，下面我们仅对基于混沌理论的密码技术进行讨论。

2.1.1 混沌密码学的发展概况

混沌变换所具有的混合、对参数和初值的敏感性等基本特性和密码学的天然关系早在Shannon的经典文章[3]就已提到。并据此提出了密码学中用于指导密码设计的两个基本原则：扩散

(diffusion)和混乱(confusion)。扩散是将明文冗余度分散到密文中使之分散开来,以便隐藏明文的统计结构,实现方式是使得明文的每一位影响密文中多位的值。混乱则是用于掩盖明文、密文和密钥之间的关系,使密钥和密文之间的统计关系变得尽可能复杂,导致密码攻击者无法从密文推理得到密钥。

混沌的轨道混合(mixing)特性(与轨道发散和初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[3]。可见,混沌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中常用的 Feistel 网络结构是非常相似的,比如标准映射、Henon 映射,等等[8-12]。

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。但是混沌毕竟不等于密码学,它们之间最重要的区别在于:密码学系统工作在有限离散集上,而混沌却工作在无限的连续实数集上。此外,传统密码学已经建立了一套分析系统性能和安全性的理论,密钥空间的设计方法和实现技术亦比较成熟,从而能保证系统的安全性;而目前混沌加密系统还缺少这样一个评估算法性能和安全性的标准。表 2.1 给出了混沌理论与传统密码算法的相似点与不同之处。

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。一方面,混沌动力学中的一些物理量,可能成为密码安全性的一种标度,比如:在混沌动力学中,Lyapunov 指数能有效地表示相空间内邻近轨道的平均指数发散率,而基于混沌动力学与密码学的类比研究,可以尝试将 Lyapunov 指数的概念应用到加密系统中去有效地测度密码的发散程度;在混沌动力学中,Kolmogorov 熵可以有效地表示信息在加密过程中信息量的损失速率,尝试应用 Kolmogorov 熵的概念来有效地标度迭代密码系统中迭代轮数的确定;一些具有良好密码特性的混沌变换还可以作为密码变换的侯选者。另一方面,一些典型的密码分析

工具也可以用于混沌理论的分析。由于密码学设计中十分强调引入非线性变换，因而可以肯定地说，混沌等非线性科学的研究成果将极大地促进密码学的发展。

表 2.1　混沌理论与密码学的相似与不同之处

	混沌理论	传统密码学
相似点	对初始条件和控制参数的极端敏感性	扩散
	类似随机的行为和长周期的不稳定轨道	伪随机信号
	混沌映射通过迭代，将初始域扩散到整个相空间	密码算法通过加密轮产生预期的扩散和混乱
	混沌映射的参数	加密算法的密钥
不同点	混沌映射定义在实数域内	加密算法定义在有限集上
	?	密码系统安全性和性能的分析理论

关于如何选取满足密码学特性要求的混沌映射是一个需要解决的关键问题。L. Kocarev 等在文献[12]中给出了在这方面的一些指导性建议。选取的混沌映射应至少具有如下三个特性：混合特性(mixing property)、鲁棒性(robust)和具有大的参数集(large parameter set)。需要指出具有以上属性的混沌系统不一定安全，但不具备上述属性则得到的混沌加密系统必然是脆弱的。

① 混合特性：将明文看作初始条件域，则混合属性是指将单个明文符号的影响扩散到许多密文符号中去，显然，该属性对应密码学中的扩散属性。具有混合属性的系统有较好的统计特性，当迭代次数 $n\to\infty$ 时，密文的统计性质不依赖于明文的统计性质，因此由密文的统计结构不能得到明文的结构。

② 鲁棒性：鲁棒性是指在小的参数扰动下，混沌系统仍保持