中南财经政法大学
青年学术文库

混沌序列密码的理论与应用实现

Theory and Application Implementation of Chaotic Stream Cipher

邓涯双 ○著

中国社会科学出版社

中南财经政法大学
青年学术文库

混沌序列密码的理论与应用实现

Theory and Application Implementation of Chaotic Stream Cipher

邓涯双 ○ 著

中国社会科学出版社

图书在版编目（CIP）数据

混沌序列密码的理论与应用实现／邓涯双著．—北京：中国社会科学出版社，2018.9

（中南财经政法大学青年学术文库）

ISBN 978－7－5203－2805－0

Ⅰ.①混… Ⅱ.①邓… Ⅲ.①密码学 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2018)第 155342 号

出 版 人 赵剑英
责任编辑 徐沐熙
特约编辑 宋 玥
责任校对 李盛楠
责任印制 戴 宽

出 版 中国社会科学出版社
社 址 北京鼓楼西大街甲 158 号
邮 编 100720
网 址 http://www.csspw.cn
发 行 部 010－84083685
门 市 部 010－84029450
经 销 新华书店及其他书店

印刷装订 北京君升印刷有限公司
版 次 2018 年 9 月第 1 版
印 次 2018 年 9 月第 1 次印刷

开 本 710×1000 1/16
印 张 14.25
插 页 2
字 数 182 千字
定 价 42.00 元

凡购买中国社会科学出版社图书，如有质量问题请与本社营销中心联系调换
电话：010－84083683

本书受中南财经政法大学出版基金资助

《中南财经政法大学青年学术文库》
编辑委员会

前　言

在信息时代，网络空间安全问题至关重要，甚至可能会危及一个国家的政治、经济、军事、文化和社会生活等诸多方面。如“棱镜门事件”揭秘了美国运用网络技术窃取其他国家核心机密、商业秘密等重要信息。因此，在信息不对等的情况下，反窃取的唯一有效手段就是保证信息的机密性。密码技术是保障网络空间安全的基础，在近二十多年来获得空前发展，应用领域不断拓展，理论与技术也实现了由传统密码向现代密码的重大变革。国家中长期科学和技术发展规划纲要（2007—2020 年）中指出要“重点研究开发国家基础信息网络和重要信息系统中的安全保障技术，开发……新的密码技术等”。新型密码技术包括量子密码、混沌密码和生物密码。因此，研究具有自主知识产权的新型密码技术，对保证网络空间安全具有极其深远的科学意义和实际的应用价值。

混沌是一种在确定性系统中产生的类随机行为。混沌系统以其复杂的动力学行为受到研究者们的热烈追捧，由此促进了混沌科学的长足发展。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问题之一。作为其应用的混沌保密技术兴起于 1990 年前后，目前已成为当今世界信息安全研究的重要前沿领域之一。

自 1989 年 Matthews（马修斯）首次提出第一个混沌流密码方

案以来，混沌序列密码研究受到了国内外的广泛重视，但依然存在许多关键问题亟待解决。众所周知，混沌是定义在实数域上的确定性系统，而密码体制是建立在有限域或某个有限代数空间上的变换。当用混沌设计密码体制时，通常需将实数域上的混沌系统（连续混沌）在空间和时间上同时进行离散化，进而设计密码体制。事实上，现有的混沌序列密码体制大都是基于有限精度下实现的连续混沌（包括狭义的连续混沌系统和时间离散混沌系统）设计的。一方面，混沌在数字世界会发生坍塌，混沌系统的非周期性、初值敏感性这些原本属于连续相空间的动力学行为都会消失。另一方面，已有混沌序列密码多是基于固定参数混沌系统设计的。然而，固定参数混沌系统的输出序列往往具有平稳的统计特性且会携带系统特征，使得攻击者有可能利用获取到的系统轨道信息或输出密钥流信息对系统进行有效统计分析。考虑到统计分析建立在平稳性假设的基础之上，抵抗统计分析的有效方法就是使待考察对象输出序列具有非平稳性。因此，研究解决混沌保密中上述关键问题的理论和方法，并且设计出密码学意义下安全的混沌源，是混沌保密技术亟待解决的关键问题。

本书主要从混沌序列密码的安全性角度出发，重点研究有限状态空间上安全、可控混沌源的构造、实现和分析。在此基础上，设计出安全、可靠的非平稳混沌序列密码模型。

全书共分为七章。第一章，介绍了混沌动力学的基础知识。主要包括混沌的基本概念、特性和典型的混沌系统。第二章，简要介绍了混沌控制的相关理论及其实现方法。主要包括混沌控制的基本概念和方法，以及混沌同步控制和反控制的简单理论、模型与实现方法。第三章，介绍了有限状态空间上混沌系统的构造和实现。第四章，从安全性的角度阐述了变参数混沌源的构造理论与方法。第五章和第六章分别介绍了数字混沌系统的两种控制方法。阐述了如

何基于混沌控制和反控制理论与方法设计出具有密码学意义上的安全数字混沌源。第七章，介绍了一种变参数混沌序列密码方案及其如何实现。

本书的编写得到了国家自然科学基金项目（编号：61702554、61505061）、“十三五”国家密码发展基金（编号：MMJJ20170109）、国家社会科学基金项目（编号：16CXW019）和密码科学技术国家重点实验室开放课题（编号：MMKFKT201613）等的资助，在此一并表示感谢！同时也要感谢国家自然科学基金委、国家密码管理局多年来对本研究团队所给予的支持和帮助！在此要特别感谢胡汉平教授一直以来给予的指导和支持！

在本书的创作过程中，刘凌锋、谢飞龙等博士，苏威、周志鹏、余志均、胡云畅等硕士也对本书的编写做出了重要贡献。另外，书中还参考了一些国内外专家和同行的论文及书籍，在此一并向相关作者表示衷心的感谢！

由于写作时间仓促，加之作者水平有限，书中难免有遗漏或者不足之处，敬请读者批评指正。

目　录

第一章

混沌动力学的基础理论

牛顿的经典力学理论是现代科学的奠基石。根据牛顿定律，人们可以解释诸多自然现象，如海水的涨落、月亮的椭圆运动、自由落体等。经典物理学认为如果给予系统特定的初始条件，则可准确地预测该系统在未来任何时刻的状态，这就是所谓的确定论可预测性思想。皮埃尔·西蒙·拉普拉斯（Pierre. Simon. Laplace）的一段名言更是把这一思想阐述得更为淋漓尽致："如有这么一位智者，他能够洞悉所有使得大自然生机勃勃的力量，能够了解大自然所有元素的状态。那么，如果我们给他提供足够多的数据……无论是未来还是过去，所有的一切将会尽数展现在他眼前，没有任何的东西会是无法洞悉的。"

然而，从19世纪开始，一系列的研究显示，决定论可预测性在大部分系统中是错误的。19世纪80年代，法国数学家亨利·庞加莱（Poin. Care）在研究天文力学中的三体问题时发现：三体引力相互耦合作用能产生惊人的复杂性，致使"初始条件的微小差异会在最终现象中产生巨大的差别……预测变成了不可能的事。"这是科学家们首次认识到确定性系统中存在着内在随机性——混沌现象。这一情况在1963年达到了高潮。1963年，麻省理工气象学家爱德华·劳伦兹（Edward. Lorenz）在美国《大气科学杂志》上发表了《确定性的非周期流》一文，他从对流问题中提取出一个三维

自治系统用于描述天气的演变情况，即我们后来熟知的 Lorenz 模型。在该模型中，他看到了一种细致的几何结构，并且发现了天气对初始条件的敏感依赖性。因此，在 1972 年美国科学促进会的一次学术会议上，劳伦兹给出了一个形象的比喻，“巴西的一只蝴蝶扇动几下翅膀，可能会改变 3 个月后美国德克萨斯州的气候”，这就是著名的“蝴蝶效应”。遗憾的是，劳伦兹开创性的模型并没有立即引起人们的关注。直到 1975 年，李天岩与詹姆斯·约克（J. A. York）在美国数学月刊上发表了题为《周期 3 蕴含着混沌》一文，首次提出“混沌”一词并给出了其第一个数学定义。其他数学家和物理学家通过这篇论文才逐渐了解到了劳伦兹的工作。自此，“chaos”一词被正式使用[1]。

随后，混沌进入蓬勃发展的阶段。到了 20 世纪 80 年代后期，相关的研究突然火热起来，而成千上万的科研文章也证实了混沌的存在。目前，混沌的概念早已在普通人之间广泛地普及开来，且无论是在生物学、生理学、心理学、数学、物理学、化学、电子学、信息科学，还是在天文学、经济学、气象学，甚至在音乐、艺术等领域，混沌均得到了广泛的应用。

在人类的科学史上还没有哪一个概念或理论能与“混沌”相比，能把众多的学科和领域联系在一起，成为它们共同的语言。混沌科学的倡导者之一，美国海军部官员斯来辛格（Shlesinger）曾有言：“20 世纪科学将永远铭记的只有三件事，那就是相对论、量子力学和混沌”，混沌可算得上 20 世纪物理学上的第三次革命了。正如著名物理学家安迪尔森·莫特（AdilsonE. Motter）和戴维 K. 坎贝尔（David K. Canpbell）在混沌理论诞生 50 周年（2013 年）受邀在《今日物理》上评论所指出的，“混沌集与其他的物理革命不同，与相对论和量子力学相比，混沌并不是关于特定物理现象的一种理论。相反的是，混沌是所有科学范式的转型，混沌可以提供

很多用于分析各个领域奇特行为的概念和方法”。

第一节　混沌的基本概念

一　混沌的定义

混沌是确定性系统中呈现出的一种类随机行为。这种行为是非线性系统中的一种新的存在形式。尽管混沌现象已得到人们的普遍关注，但迄今为止，混沌还没有一个统一的定义，这也就意味着人们对混沌并没有一个统一的认知。目前不同领域的科学家已从不同的角度阐述了自己对混沌的理解，尽管表述的方式不尽相同，彼此在逻辑上也不一定等价，但它们在本质上是一致的。下面依次给出几种典型的混沌定义[25]。

Li-Yorke 混沌定义[1]　设 $I\subset R$，f：$I\to I$ 的连续映射，若存在点 $a\in I$，令 $b=f(a)$，$c=f^2(a)$，$d=f^3(a)$，满足如下条件：

$$d\leqslant a<b<c(d\geqslant a>b>c)$$

则：

1）对任意的 $k=1$，2，…，f 有 k 周期点；

2）存在不可数子集 S⊂［a，b］，S 中无周期点，且满足

a. 对任意 x，$y\in S$，有 $\liminf\limits_{n\to\infty}|f^n(x)-f^n(y)|=0$；

b. 对任意 x，$y\in S$，$x\neq y$，有 $\limsup\limits_{n\to\infty}|f^n(x)-f^n(y)|>0$；

c. 对任意的 $x\in S$ 和 f 的任意周期点 $y\in I$，有 $\limsup\limits_{n\to\infty}|f^n(x)-f^n(y)|>0$.

人们通常把满足条件 1）和 2）的映射称为 Li-Yorke 意义下的混沌映射。该混沌定义是李天岩和他的导师 York 于 1975 年给出的第一个混沌定义。显然，当 f 具有周期为 3 的点时，上述结论自然成立。这就是著名的“周期三意味着混沌”。

受 Li-Yorke 工作的启发，1978 年，Marotto（马洛特）将 Li-Yorke 意义下的混沌定义推广到 n 维情形。考察如下 n 维离散系统：

$$x_{k+1}=f(x_k),\ x_k\in R^n,\ k=0,1,2\cdots$$

其中，f 是关于 x 的连续可微函数，记 $B_r^0(x)$ 为圆心在点 x 处半径为 r 的开球，$B_r(x)$ 为其闭包。则有如下 Marotto 定理。

Marotto 定理[5] 如果连续映射 f 具有一个满足如下两个条件的返回扩张不动点：

1）f 在 $B_r(x^*)$ 内连续可微，如果 $f(x^*)=x^*$ 且对于所有 $x\in B_r(x^*)$，$Df(x)$ 所有特征值的模均大于 1；

2）存在 $x^0\in B_r(x^*)$，$x^0\neq x^*$，使得对某个正整数 m，有 $f^m(x^0)=x^*$ 且 $|Df^m(x^0)|\neq 0$。

则系统（1.1）是 Li-Yorke 意义下的混沌。也就是说，

1）存在正整数 N，使得对于任意整数 $p\geqslant N$，f 有 p 周期点；

2）存在一不规则集 S（不可数且不包含周期点），使得

a）$f(S)\subset S$；

b）对任意 x，$y\in S$，$x\neq y$，有 $\limsup\limits_{x\to\infty}\|f^n(x)-f^n(y)\|>0$；

c）对任意的 $x\in S$ 和 f 的任意周期点 y，有 $\limsup\limits_{x\to\infty}\|f^n(x)-f^n(y)\|>0$。

3）存在不可数子集 $S_0\subset S$，使得对于任意 x，$y\in S$，有 $\liminf\limits_{x\to\infty}\|f^n(x)-f^n(y)\|=0$；

德瓦尼（Devaney）于 1989 年提出了另一种混沌定义。他把混沌归结为三个特征：不可预测性、不可分解性、具有规律性行为。

Devaney 混沌定义[7] 设 S 为一集合，$f: S\to S$ 的连续映射称为在 S 上是混沌的，如果

1）f 有初值敏感性，即存在 $\varepsilon>0$，对任意 x 及其邻域 U，均存在 $y\in U$，$n\in Z^+$ 使得 B_i；

2）f是拓扑传递的，即对于任意两开集 U、$V \subset S$，存在 $k \in Z^+$，使得 $f^k(U) \cap V \neq \varnothing$；

3）周期点在 V 中稠密。

要想理解简单的确定性系统如何会导致系统长期行为对初值的敏感依赖性，关键要理解混沌的几何特性，即系统内在的非线性作用在系统演化过程中形成的“拉伸”与“折叠”变换。美国拓扑学家 Smale 对此做出了重要贡献。

马蹄混沌定义[14]　考察一映射 f：$D \to R^2$，$D = \{(x, y) \in R^2 \mid 0 \leqslant x \leqslant 1, 0 \leqslant y \leqslant 1\}$，映射 f 在 x 方向上压缩，在 y 方向上拉伸，然后再折叠弯曲放到 D 内，不断重复此过程就形成了类似马蹄形状的图形，则映射 f 被称为 Smale 马蹄变换。如图 1－1 所示。

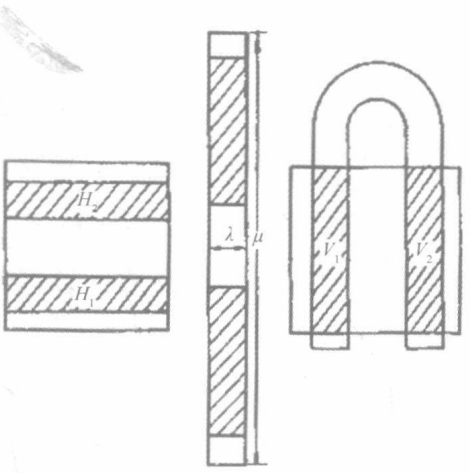

图 1－1　Smale 马蹄变换

伸缩和折叠这两种非线性变换导致了动力系统的轨迹在相空间中呈现出复杂的几何特征。伸缩使得轨道不断分离从而不断发散，但仅有伸缩还不足以扰乱系统相空间，还必须通过折叠变换。在混沌区域中，相空间的伸缩与折叠以永不停歇的方式进行着，使得系统的相轨迹不断穿插缠绕，分离又相聚，完全隐藏了初始状态的一