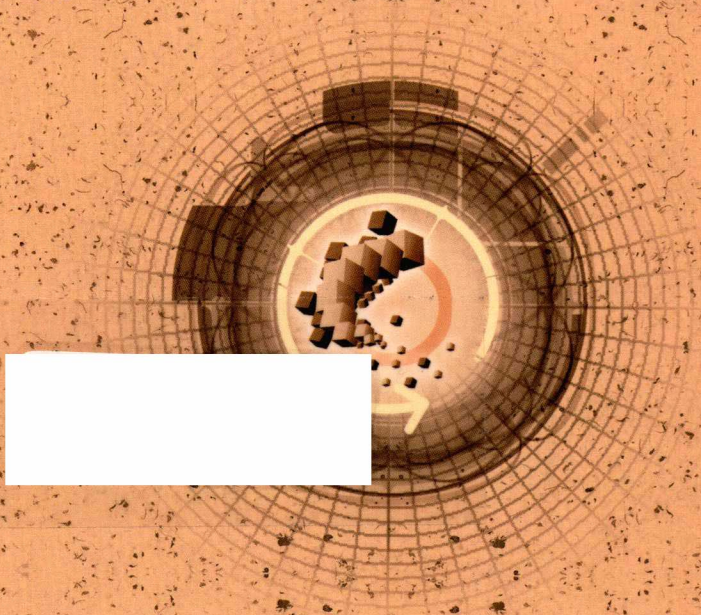
混沌理论
在密码学中的应用

◎郭凤鸣　涂 立　著



北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

混沌理论在密码学中的应用

郭凤鸣　涂　立　著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

混沌理论在密码学中的应用 / 郭凤鸣，涂立著 . —北京：北京理工大学出版社，2015. 12

ISBN 978 - 7 - 5682 - 1535 - 0

Ⅰ. ①混…　Ⅱ. ①郭…②涂…　Ⅲ. ①混沌理论 - 应用 - 密码 - 通信理论　Ⅳ. ①TN918. 1

中国版本图书馆 CIP 数据核字（2015）第 285473 号

出版发行 / 北京理工大学出版社有限责任公司
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 / （010）68914775（总编室）
　　（010）82562903（教材售后服务热线）
　　（010）68948351（其他图书服务热线）
网　　址 / http：//www. bitpress. com. cn
经　　销 / 全国各地新华书店
印　　刷 / 北京九州迅驰传媒文化有限公司
开　　本 / 710 毫米 ×1000 毫米　1/16
印　　张 / 13. 5
字　　数 / 256 千字
版　　次 / 2015 年 12 月第 1 版　2015 年 12 月第 1 次印刷
定　　价 / 49. 00 元

责任编辑 / 张慧峰
文案编辑 / 张慧峰
责任校对 / 周瑞红
责任印制 / 马振武

序　言

随着网络的发展及信息普及度的提高，安全问题日益突出。其中，密码是关系到信息安全的一个重要的方面，而混沌密码更是密码学的一个全新的研究方向。

混沌理论作为新兴学科，已经迅速融入到了多个学科。混沌映射所具有的初值敏感性、随机性、参数敏感性和不可预测性等特点，如“蝴蝶效应”，使得基于混沌理论的图像加密算法成为一个研究热点。随着混沌映射系统参数的多少，混沌映射的维数也不同。绝大多数学者都采用低维的混沌映射，而高维混沌映射相比于低维映射参数更多，也更复杂。混沌系统本身是一种复杂的非线性动态系统，具有非周期性、类随机性和非重复性三大特性，对初始条件和混沌参数非常敏感，致使生成的混沌序列具有良好随机性、相关性和复杂性，是一种伪随机序列，并具有难以分析和预测的复杂结构，这些特性都非常适合于信息的安全保密工作。

目前大部分文献提及的加密算法大多是为了提高图像的加密速度，都将图像作为特殊的数据流，并且没有对中间相遇攻击的情况进行差分分析，体现不出穷举攻击算法的安全性，分析结果不明确。针对传统利用混沌理论对数据加密时运算开销大、运算效率不高等问题，作者提出了一种利用混沌理论的独立密钥 DES 图像加密算法。其主要创新点就是采用混沌二值序列加密算法的设计，使得加密和解密运算开销和运算效率得到了较大的提高。仿真实验结果验证了本书提出的算法具有有效性和实用性，对图像进行加密达到了更高的安全性

在本书的前半部分，作者列举了一维、二维、三维和高维混沌方程，并用分布概率、分叉图、相图等工具分析了这些混沌方程，并分别在这些传统方程上做出了一定的改进，构造出了一序列具有更优的混沌方程。在后半部分列出了位置变换、灰度变换、像素值扩散、嵌入式隐藏加密等方法，在此基础上提出了构建图像加密新算法的思路，并将前半部分构造的新型混沌方

程应用到新算法中，得到了良好的加密效果。

本书概念清晰，重点突出，由浅入深，循序渐进，在繁重的教学、管理工作之余，作者郭凤鸣老师坚持科研，注重积累，能写出这种有深度的佳作实属难得，是新世纪知识分子的榜样，为师甚慰！

合肥工业大学
电气与自动化工程学院　院长
教授、博导

目　录

第 1 章　混沌理论简介

1.1　引　　言

混沌可以看成是一种无周期的有序，是自然界中客观存在的有界的、不规则的、复杂的运动形式。1963 年，美国麻省理工学院气象学家洛伦兹（E. N. Lorenz）发现了著名的 Lorenz 吸引子，提出了著名的“蝴蝶效应”（The Butterfly Effect），并由此推断出长期的天气预报不可预测。“蝴蝶效应”常用于天气、股票市场等长时段难预测的复杂系统中。此效应说明，事物发展的结果，对初始条件具有极为敏感的依赖性，初始条件的极小偏差，将会引起结果的极大差异。洛伦兹在他的演讲和论文中常用有诗意的蝴蝶阐述混沌对初值的敏感依赖性：“一只蝴蝶在巴西轻拍翅膀，可以导致一个月后德克萨斯州的一场龙卷风；在一个确定的动力系统中，初始条件的极小偏差，将会引起结果的极大差异。”这种现象说明，系统的结果，对初始条件具有极为敏感的依赖性。

1975 年美国数学家 Yorke 和他的研究生李天岩在论文《周期 3 蕴含混沌》一文中首先引入了 Chaos（混沌）一词，从而开创了混沌这一新的科学研究领域。

在确定性的非线性动力系统中混沌现象的发现，被混沌科学的倡导者 M. F. Shlesinger 誉为 20 世纪物理学的三次革命（相对论、量子理学、混沌现象）之一。

1.2　混沌理论基础

1.2.1　混沌理论的研究史及其发展

混沌理论的开端，最早可以追溯到 19 世纪末 20 世纪初法国数学家庞加

莱（Jules Henri Poincare）所做的一系列关于太阳系中三体问题（three - body problem）的研究。庞加莱在1913年把动力学和拓扑学结合起来研究，并运用相图、拓扑学以及相空间截面的方法，指出三体引力相互作用能产生出惊人的复杂行为。确定性方程的某些解存在不可预见性，使得三体问题在一定范围内不能精确求解，因此结果是随机的。庞加莱成了第一个发现混沌确定系统的人，并为现代的混沌理论打下了基础。

苏联概率论大师 Andrey Nikolaevich Kolmogorov 将香农（C. E. Shannon）在1948年提出的信息论引入混沌理论的研究中，在混沌基础理论研究方面做出了一系列贡献。

20世纪70年代开始，众多的科学家都开始在各自的研究领域发现和研究混沌现象：

1971年，法国物理学家 D. Ruelle 和荷兰数学家 F. Takens 发表了著名论文《论湍流的本质》，首次用混沌来解释湍流发生的本质。他们发现动力系统存在特别复杂的新型吸引子，命名为奇怪吸引子（strange attractor），并引入耗散系统，证明同这种吸引子有关的运动为混沌运动，发现了第一条通向混沌的道路；

1976年，美国数学生态学家 May R. 在美国《自然》杂志上发表了题为《具有复杂动力学过程的简单数学模型》的论文，在文中提出了著名的人口（虫口）方程，即 Logistic 模型。他用数值计算研究虫口模型，发现随机运动中会出现稳定的周期运动；

1978年，美国物理学家费根鲍姆（Edward Albert Feigenbaum）发表了题为《Quantitative universality for class of nonlinear transformation》的论文。他在研究以 Logistic 映射为代表的一类单峰映射时，发现了倍周期分岔通向混沌的两个普适常数：收敛常数 δ 和标度常数 α；

1981年，荷兰数学家 F. Takens Whitney 提出的拓扑嵌入定理，引入了重整化群思想，提出了判定奇怪吸引子的实验方法。

混沌被认为是继相对论和量子力学后，20世纪物理学的第三次重大发现。与前两次革命相似，混沌也一样冲破了牛顿力学的教规。第一次国际混沌会议主持人之一的物理学家 J. Ford 指出：相对论消除了关于绝对空间与时间的幻想，量子力学消除了关于可控测量过程的牛顿式的梦，而混沌则消除了拉普拉斯关于决定论式可预测性的幻想。

1.2.2　混沌的定义

迄今，学术界对“混沌”尚缺乏统一的普遍接受的一般定义，但是至少有几种不同的定义基本勾画了“混沌”的本来面目。动力系统混沌性的数学定义有多个，但最常见的有 Li - Yorke 定义和 Devancy 定义。

Li - Yorke 从数学的角度作出了严格定义。Li - Yorke 定理为：设 $f(x)$ 是 $[a, b]$ 上的连续自映射，若 $f(x)$ 有 3 个周期点，则对任何正整数 n，$f(x)$ 有 n 个周期点。

混沌的定义如下：闭合区间 I 上的连续自映射 $f(x)$，若满足下列条件，则一定出现混沌现象：

（1）f 的周期点的周期无上界。

（2）闭区间 I 上存在不可数子集 s，满足

a. $\forall x, y \in s, x \neq y$ 时，有 $\limsup\limits_{n\to\infty} |f^n(x) - f^n(y)| > 0$；

b. $\forall x, y \in s$，有 $\liminf\limits_{n\to\infty} |f^n(x) - f^n(y)| = 0$；

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

在 Li - Yorke 的混沌定义中，条件 a 和 c 表明子集中的点 x 和 y 相当分散又相当集中，条件 b 则表明子集不会趋近于任意周期点。该定义指出，在任何系统中是否存在 3 周期是判断混沌是否存在的准则。

Li - Yorke 的混沌定义刻画了混沌运动的以下三个重要特征：

（1）存在可数的无穷多个稳定的周期轨道。

（2）存在不可数的无穷多个稳定的非周期轨道。

（3）至少存在一个稳定的非周期轨道。

1.2.3　混沌运动的特点

无论何种定义，概括地说，混沌系统的复杂动力学具有如下基本特性：

（1）有界性。系统的运动轨道局限在一个有限的区域之内，系统从整体上来说是稳定的。

（2）内随机性。混沌貌似噪声，但不同于噪声。它由完全确定的方程描述，无须附加任何随机因数，系统都会表现出类似随机性的行为。

（3）混沌吸引子的几何特性是具有分形（分数维数）。例如，Lorenz 吸引子就具有分形的结构，混沌吸引子具有自相似嵌套结构，还具有连续功率谱。

（4）遍历性（无周期，或无限大周期）。在混沌吸引域内，混沌运动是各态经历的，在有限的时间内，混沌轨道会经历混沌区间里面的每一个点。

（5）对初始条件的敏感依赖性。只要初始条件稍有偏差或扰动，就会使得系统的最终状态出现巨大的差异。因此混沌系统的长期演化行为是不可预测的。

（6）混沌吸引子在相空间内整体上是有界的，但是在吸引子内相轨迹具有高度不稳定性，除了最大的 Lyapunov 指数大于零外，还具有有限值的拓扑熵和测度熵。

（7）混合性。对任意两个可以任意小但长度不为零的开区间 I 和 J，可以发现，I 中的初值通过迭代，最终将到达 J 区间里面的点。

（8）混沌的几何与统计特征有：局部不稳定而整体稳定；奇怪吸引子；分数维；正 Lyapunov 指数；正测度熵。

（9）不动点。在连续动力系统中，相空间中有一点 x_0，若满足当 $t\to\infty$ 时，轨迹 $x(t)\to x_0$，则 x_0 为不动点。

（10）排斥点。相空间中不稳定的不动点。不管轨迹的初始点如何接近排斥点，经过足够长的时间，轨迹总会与之远离。

自然科学中的混沌效应常用“蝴蝶效应”“差之毫厘，失之千里”来描述；社会科学中的混沌效应则有“一失足成千古恨”的例子。以下我们用计算机仿真，来说明混沌系统对初值的敏感性。

例 1 一维 Logistic 混沌系统的迭代求解。

Logistic 混沌系统模型：$x_{n+1}=\mu x_n(1-x_n)$，取 $\mu=4$

系统 1 及初值：$x_{n+1}=\mu x_n(1-x_n)$，$x_0=0.7$

系统 2 及初值：$y_{n+1}=\mu y_n(1-y_n)$，$x_0=0.7+10^{-10}$

我们用 MATLAB 进行仿真，对以上两个系统各迭代 1 000 次，得到两组混沌序列，以及图 1.2.1 和图 1.2.2 两组混沌序列的对比图。观察初始状态的细微差别，我们可以发现，长时间的迭代计算导致后来的巨大差别——这就是混沌运动对初始条件的极端敏感性。

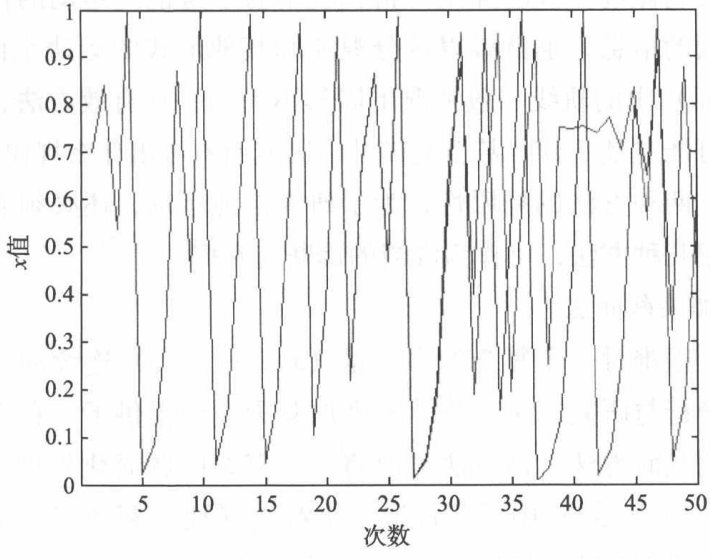


图 1.2.1　前 50 次迭代结果的数据对比图

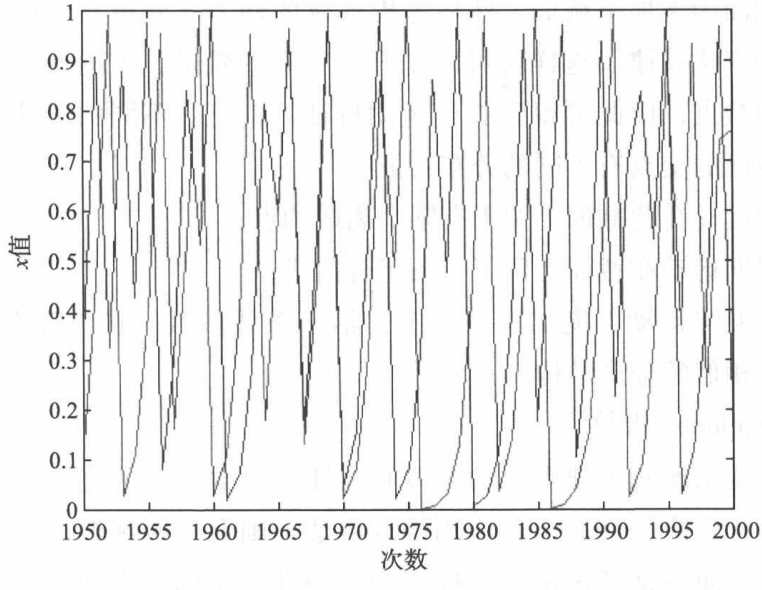


图 1.2.2　1 950 ~ 2 000 次迭代结果的数据对比图

1.2.4　混沌系统的判据与准则

为了研究混沌运动，我们可以采用直接观察状态变量随时间的变化和在相空间（或相平面）观察其轨迹这两种方法。但是很明显，混沌运动是很复杂的，有时即使长时间直接观察状态随时间的变化，也不一定能看出一点头

绪。如果不对它做进一步的加工分析，就不易了解混沌运动的性质和有关频谱成分等方面的信息，也就难以区分混沌和其他形式的运动。直接观察相空间（或相平面）中的轨线一般情况下固然不失为一种有效方法，但当运动复杂时，轨线可能混乱一片，甚至充满某一区域而看不出什么规律。

鉴于以上两种方法的局限性，为了研究混沌运动，还必须有其他有效方法。下面介绍几种方法，可作为混沌的诊断与判据。

（1）庞加莱截面法。

有时候，很难对一个复杂的多变量（x_1，…，x_n）连续动力学系统的轨道直接进行分析与研究，法国数学家庞加莱为我们提供了一种有效的研究方法，即庞加莱截面方法。该方法可以将一个复杂问题简化处理。在多维空间（x_1，$\dot{x}_1$，…，x_n，$\dot{x}_n$）中适当选取一个截面（要有利于观察系统的运动特征和变化，如截面不能与轨线相切，更不能包含轨线面），这个截面可以是平面，也可以是曲面。在此截面上令某一对共扼变量（如 x_1，$\mathrm{d}x_1/\mathrm{d}t$）取固定值，称此截面为庞加莱截面，然后考虑连续的动力学轨道与此截面相交的一系列交点的变化规律。这样就可以抛开相空间的轨道，借助计算机画出庞加莱截面上的截点，由此可得到关于运动特征的信息。不同的运动形式通过截面时，与截面的交点有不同的分布特征：

①周期运动在此截面上留下有限个离散的点；

②准周期运动在截面上留下一条闭合曲线；

③对于混沌运动，庞加莱截面上是沿一条线段或一曲线弧分布的点集，而且具有自相似的分形结构。

（2）Lyapunov 指数。

由于可能出现的不规则运动，对非线性动力学系统的完善的定性描述似乎是一个不可解决的问题。若应用统计方法，则会有所帮助。即考虑某些平均值的演化，而不是考虑由一个确定初始条件发出的一根轨道。目前，在表征混沌运动方面显示出重大意义的统计特征值之一的就是 Lyapunov 指数。它是对相空间中相近轨道的平均收敛性或平均发散性的一种度量。

混沌系统由相空间的不规则轨道奇怪吸引子来描述。奇怪吸引子的一个明显特征就是吸引子临近点的指数离析。因为相空间中的点表示整个物理系统，所以临近点的指数离析意味着在长时间情况下，初始状态完全确定的系统会不可避免地发生变化。这种行为就是系统对初始条件具有敏感依赖性的反应。而引入的 Lyapunov 指数恰可定量表示奇怪吸引子的这种运动状态。

对于 n 维相空间中的连续动力学系统，考察一个无穷小 n 维球面的长时间演化。由于流的局部变形特性，球面将变为 n 维椭球面。第 i 个 Lyapunov 指数按椭球主轴长度 $p_i(t)$ 定义为公式（1.2.1）：

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln \frac{p_i(t)}{p_i(0)} \tag{1.2.1}$$

公式（1.2.1）说明，Lyapunov 指数的大小表明相空间中相近的平均收敛或发散的指数率。Lyapunov 指数是很一般的特征数值，它对每种类型的吸引子都有定义。n 维相空间有 n 个实指数，故也称为谱，并按其大小排列，一般令 $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3 \cdots \geqslant \lambda_n$。一般来说，具有正和零 Lyapunov 指数的方向，都对支撑起吸引子起作用，而负 Lyapunov 指数对应着收缩方向。这两种因素对抗的结果就是伸缩与折叠操作，这就形成奇怪吸引子的空间几何形状。因此，对于奇怪吸引子而言，其最大 Lyapunov 指数 λ_1 为正的（另外也至少有一个 Lyapunov 指数是负的），并且 Lyapunov 指数 λ_1 越大，系统的混沌性越强；反之亦然。

对于规则（轨道）运动，当初始状态已知时，人们可以预言任何系统的状态。对于混沌运动，由于其对初始状态的敏感依赖性，人们很难对系统的状态做出预测。对于相空间中开始极靠近的状态点，时间不长时，两点的轨道大体很相近，可以认为系统的轨道是确定的，从而还可以对运动做出预测；时间越长，两点的轨道越来越发散分离，从而对状态的预测也就变得越来越不可能了。这种使轨道相互分离的趋势就是相体积扩张。

对于一维运动，可以取满足公式（1.2.2）的 t 作为对状态可否预测的分解时间（设 t_c 为一临界时间，$t < t_c$，状态大体还可预测；$t > t_c$，对系统状态只能做概率描述）。

$$\varepsilon e^{\lambda t_c} = 1 \tag{1.2.2}$$

由公式（1.2.2）可得公式（1.2.3）：

$$t_c = \frac{1}{\lambda} \lg \frac{1}{\varepsilon} \tag{1.2.3}$$

对于多维运动，可以推广上式，即根据公式（1.2.3）用 K 代替 λ，于是得到时间极限，即公式（1.2.4）所示：

$$t_c = \frac{1}{K} \lg \frac{1}{\varepsilon} \tag{1.2.4}$$

公式（1.2.3）和公式（1.2.4）中的 ε 可看做是确定系统状态的精度，它对 t_c 的影响是对数形式，不如 K 的影响大。所以运动越混乱（K 越大），对

运动状态可预测的时间 t_c 越小。可见最大 Lyapunov 指数 λ_1 的倒数决定了吸引子的行为经多长时间后不可预测。

对于耗散系统，Lyapunov 指数谱不仅描述了各条轨道的性态，而且还描述了从一个吸引子的吸引域出发的所有轨道的稳定性性态。

对于一维（单变量）情形，吸引子只可能是不动点（稳定定态）。此时 Lyapunov 指数是负的。

对于二维情形，吸引子可能是不动点，又或者是极限环。对于不动点，任意方向的相空间中两靠近点之间的距离都要收缩，故这时两个 Lyapunov 指数都应该是负的，即 $(\lambda_1, \lambda_2) = (-, -)$。至于极限环，如果在相空间中沿垂直于环线的方向上取两靠近点，它一定会收缩，此时 Lyapunov 指数是负的；当在相空间中沿轨道切线方向取两靠近点，极限环既不增大也不缩小，可以想象，这时 Lyapunov 指数等于零（这类不终止于不动点而又有界的轨道至少有一个 Lyapunov 指数等于零，证明可参考 Haken 的《Advanced Synergetics》）。所以，极限环的 Lyapunov 指数是 $(\lambda_1, \lambda_2) = (0, -)$。

同样可知，在三维情形下有下面六种情况：

$(\lambda_1, \lambda_2, \lambda_3) = (-, -, -)$，不动点；

$(\lambda_1, \lambda_2, \lambda_3) = (0, -, -)$，极限环；

$(\lambda_1, \lambda_2, \lambda_3) = (0, 0, -)$，二维环面；

$(\lambda_1, \lambda_2, \lambda_3) = (+, +, -)$，不稳极限环；

$(\lambda_1, \lambda_2, \lambda_3) = (+, 0, 0)$，不稳二维环面；

$(\lambda_1, \lambda_2, \lambda_3) = (+, 0, -)$，奇怪吸引子。

对于三维相空间中的不动点，很显然其三个 Lyapunov 指数均是负的。对于极限环，由于垂直于环线的两个方向的其他轨道都要趋于此极限环，故有两个 λ_i 值是负的。对于二维环面，垂直于环面法线的 Lyapunov 指数自然是负的，另外两个在环面上互相垂直方向的 λ_i 则都应等于零。对于不稳极限环和不稳二维环面，自然是分别把极限环和二维环面中 λ_i 的负号变为正号。对于奇怪吸引子，沿轨道方向的 λ_i 等于零。此外，如前所述，奇怪吸引子是稳定和不稳定（或收敛和分离）两种因素共同作用的结果，因此它的另两个 Lyapunov 指数一个是正的，另一个是负的。

在四维连续耗散系统中，有三类不同的奇怪吸引子，它们是：

$(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (+, +, 0, -)$

$(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (+, 0, -, -)$