国家科学技术学术著作出版
NFAPST

新型混沌电路与系统的设计原理及其应用

禹思敏 著

科学出版社

国家科学技术学术著作出版基金资助出版

新型混沌电路与系统的设计原理及其应用

禹思敏 著

科学出版社

北京

内 容 简 介

本书详细论述了新型混沌电路与系统的设计原理及其在多媒体混沌保密通信中的应用与技术实现，共 19 章。其中，第 1～3 章介绍混沌的基本概念、李氏指数的数值计算方法与应用、离散时间混沌系统。第 4～8 章介绍高维连续时间超混沌系统的设计，包括具有多个正李氏指数的连续时间超混沌系统、耗散系统与保守系统中的无简并高维连续时间超混沌系统、无简并高维连续时间超混沌系统的平均特征值准则、具有多控制器的无简并高维连续时间超混沌系统、可配置任意多个正李氏指数的连续时间超混沌系统。第 9～11 章介绍整数域和数字域混沌系统，包括单个随机位迭代更新的 1 维整数域混沌系统、多个随机位迭代更新的 1 维整数域混沌系统、高维整数域和数字域混沌系统。第 12～19 章介绍新型混沌电路与系统在多媒体混沌保密通信中的应用，包括定点算法和状态机控制的通用 FPGA 混沌信号发生器、视频混沌保密通信系统的设计与 FPGA 实现、广域网传输实时远程视频混沌保密通信与 ARM 实现、多核多进程与 H.264 选择性加密的视频混沌保密通信、多核多线程与 H.264 编码后加密的视频混沌保密通信、视频混沌保密通信的手机实现、组播多用户和广域网传输的语音混沌保密通信、高维混沌映射单向 Hash 函数。

本书可作为电子科学与技术、信息与通信工程、控制科学与工程及相关专业的研究生教材或教学参考书，也可供自然科学和工程技术领域的高校教师和研究人员参考。

图书在版编目（CIP）数据

新型混沌电路与系统的设计原理及其应用 / 禹思敏著. —北京：科学出版社，2018.11

ISBN 978-7-03-059216-3

Ⅰ. ①新… Ⅱ. ①禹… Ⅲ. ①混沌理论-应用-电路设计 Ⅳ. ①TM02

中国版本图书馆 CIP 数据核字（2018）第 244260 号

责任编辑：裴 育 纪四稳 / 责任校对：张小霞

责任印制：师艳茹 / 封面设计：蓝 正

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

河北鹏润印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 11 月第 一 版 开本：720×1000 1/16

2018 年 11 月第一次印刷 印张：34 1/2

字数：670 000

定价：198.00 元

（如有印装质量问题，我社负责调换）

作 者 简 介

禹思敏 1957 年 5 月出生，2001 年毕业于华南理工大学电路与系统专业，获工学博士学位。广东工业大学自动化学院二级教授、博士生导师，广东省攀峰重点学科、一级学科博士点“控制科学与工程”学术带头人，国家自然科学奖二等奖、教育部自然科学奖一等奖、广东省科学技术奖二等奖获得者，广东省南粤优秀教师，广东省优秀博士论文、优秀硕士论文指导教师。兼任中国密码学会混沌保密通信专业委员会委员、中国电子学会电路与系统分会混沌与非线性电路专业委员会第一届委员会副主任委员、德国施普林格出版社非线性电路 Brief 丛书编委会委员等学术职务。主持和承担国家及省部级科研项目 18 项，其中主持国家自然科学基金面上项目 4 项，承担国家自然科学基金重点项目 1 项、国家重点研发计划子课题 1 项。在 *IEEE Transactions*、《中国科学》等国内外期刊上发表 SCI 收录论文 80 多篇，*IEEE Transactions* 论文 13 篇，被 SCI 引用 1800 多次，H 指数 25，ESI 高被引论文 6 篇；出版教材 3 部、学术专著 3 部；申请和授权国家发明专利 20 项。在非线性电路系统理论与技术，多涡卷和多翅膀等复杂拓扑结构混沌吸引子的生成、实现与应用，混沌电路与系统的设计，连续时间系统与切换系统的反控制，混沌密码理论与应用，多媒体混沌保密通信研发等方面取得了一系列有价值的成果。

前　言

本书以若干新型混沌电路与系统的设计原理及其在多媒体混沌保密通信中的应用与技术实现作为主要研究对象，归纳和总结了近年来作者在上述研究领域中取得的一系列科研成果。

本书第一部分重点叙述无简并高维超混沌系统的设计。无简并高维超混沌系统具体是指正李氏指数的个数 L^+ 能够达到可能的最大个数的一类高维超混沌系统。对于 n 维连续时间自治系统，设正李氏指数的个数为 L_c^+，负李氏指数的个数为 L_c^-，零李氏指数的个数为 L_c^0，它们之间满足 $n=L_c^++L_c^-+L_c^0$。如果正李氏指数的个数达到了可能的最大个数，即满足 $L_c^+=n-2$，则称为无简并高维连续时间超混沌系统。如果正李氏指数个数仅满足 $L_c^+=n-2-d$，则称为有简并高维连续时间超混沌系统，其中 $d>0$ 为正李氏指数的简并度，是衡量正李氏指数个数减少的一个量化指标，d 越大，正李氏指数个数减少的程度也越大。对于 n 维离散时间自治系统，如果正李氏指数的个数达到了可能的最大个数，即满足 $L_d^+=n$，则称为无简并高维离散时间超混沌系统。但如果正李氏指数的个数仅满足 $L_d^+=n-d$，则称为有简并高维离散时间超混沌系统。通常情况下将连续系统和离散系统的正李氏指数是否发生简并的两种情况统称为无简并高维超混沌系统或有简并高维超混沌系统。对于连续时间混沌系统，必须有一个零指数和至少一个负指数，而离散系统则无此要求。

在简并无法消除的情况下，正李氏指数的个数不能随着系统维数的拓展而增加，这种单纯通过拓展系统维数而不能增加正李氏指数个数的高维系统设计方法并无实质性的研究意义。例如，一个 3 维离散混沌系统和一个 10 维离散混沌系统，如果这两个系统都只有一个正李氏指数，除维数上的差异之外，其他动力学性质并没有本质上的区别。但如果后者是无简并的，有 10 个正李氏指数，那么，两者的动力学性质将会出现较大的差异。这种差异具体体现在混沌的统计特性能否通过严格的 TestU01 测试和度量混沌系统统计特性的 KS 熵值大小。众所周知，这些指标是混沌加密算法安全性所需的必要条件。

无简并高维超混沌系统和有简并高维超混沌系统在维数相同的条件下，从动力学行为、混沌化的程度以及统计特性等多个方面来进行比较，它们之间都存在较大的差异。根据混沌理论，混沌系统的本质特征由混沌轨道的拉伸折叠变换决

定。只有一个正李氏指数的混沌系统，相邻轨道之间只有一个方向上的拉伸折叠变换和发散度(即指数分离度)，而多个正李氏指数的混沌系统具有多个不同方向上的拉伸折叠变换和发散度。在混沌系统全局有界条件下，如果正李氏指数的个数 L^+ 越多，并且正李氏指数的值 LE^+ 越大，则系统具有更大强度的以及更多不同方向上的拉伸折叠变换，且整个系统的行为更复杂，从而导致无简并系统与有简并系统的动力学性质出现较大的差异。

为了解决正李氏指数发生简并的问题，本书第一部分重点介绍一种无简并高维超混沌系统设计的新方法，其适用范围是用一致有界的控制器对渐近稳定的标称系统实施反控制来构造无简并高维超混沌系统，通过控制器的闭环极点配置，使得当受控系统在两类鞍焦平衡点处对应的特征值的正实部个数分别满足 $n-1$ 和 $n-2$ 时，正李氏指数的个数能够达到 $L^+=n-2$。但在实际情况中，混沌系统的解 $\boldsymbol{x}(t)$ 遍历地分布在整个相空间中，设混沌系统的状态方程为 $\dot{\boldsymbol{x}}=f(\boldsymbol{x})$，对应的雅可比矩阵为 $\boldsymbol{J}(\boldsymbol{x})=\partial f(\boldsymbol{x})/\partial \boldsymbol{x}$，则雅可比矩阵 $\boldsymbol{J}(\boldsymbol{x})$ 也是状态变量 $\boldsymbol{x}$ 的函数，根据 $\boldsymbol{J}(\boldsymbol{x})$ 计算得到的特征值 $\lambda_i(\boldsymbol{x})$ $(i=1,2,\cdots,n)$ 也是随着 $\boldsymbol{x}$ 的变化而变化的。仅考虑在两类鞍焦平衡点处对应的特征值的正实部个数分别满足 $n-1$ 和 $n-2$，虽然能解决维数不是很高情况下正李氏指数的无简并问题，但这只是一个必要条件，对于 $n>12$ 的高维系统，可以举出许多反例说明，即便满足这个必要条件，正李氏指数的个数也不一定能够满足 $L^+=n-2$，存在简并度 $d>0$ 的情况。但如果进一步考虑在控制器的一个周期内所有雅可比矩阵对应的平均特征值的正实部个数满足 $n-2$，就有可能进一步解决这个问题。

本书第二部分主要介绍满足 Devaney 混沌定义的整数域和数字域混沌系统的设计。改善或补偿数字域中混沌动力学退化的各种方法以及提出在数字域上构造混沌的新理论是近年来国内外关注的一个热点课题。目前，人们虽然采用了多种不同的改善或补偿数字域中混沌动力学退化的方法来研究这个问题，但更为重要的是另辟蹊径，提出在数字域上构造混沌的新理论与新方法来解决这个问题。

众所周知，混沌严格的数学定义，如 Devaney 混沌定义和 Li-Yorke 混沌定义等，都是针对“无限时间”和“无限精度”的条件而言的。混沌特性的数学定义都是渐近的，如李氏指数是用极限定义的、功率谱是用无穷傅里叶级数表示的。由于计算机和数字器件都是“有限精度”，人们无法实现严格数学定义的混沌，只能在“有限时间”和“有限精度”的“数字域”中实现“数字混沌”。在没有外部控制的条件下，对于一个数字域上的“自治混沌系统”本身而言，在整数域或数字域上的状态数为有限的情况下，它不可能具有数学意义上真正的混沌特

性。因此，解决问题的根本途径是必须引入某种外部的控制方法来解决数字域混沌的建模问题。例如，采用外部随机序列控制的单个随机位或多个随机位迭代更新的方法，构造满足 Devaney 混沌定义的 1 维和高维整数域或数字域混沌系统。

本书第三部分主要介绍多媒体混沌保密通信及其在 ARM、FPGA 和手机等硬件平台上的应用与技术实现。混沌密码不能总是停留在理论分析与设计的阶段，最终必须走向实际应用。这就需要解决两个重要的瓶颈问题：一是如何保证整个系统的安全性，二是如何获得硬件设计与实现的可行性。混沌密码的硬件设计与实现则是多媒体混沌保密通信走向实际应用的一项重要研究工作，其科学意义体现在“实践是检验真理的标准”。经过严格密码分析检测的混沌密码是否具有实用性，在很大程度上取决于该混沌密码设计算法在硬件实现方面的实际可行性，硬件实现是检验混沌密码合理性的重要实验手段和事实依据。

目前，国内外通常采用计算机数值仿真的方法来检验混沌密码算法和多媒体混沌保密通信。相对于数值仿真，硬件实现具有更大的技术难度，需要更高的实验手段。由于技术原因，现有的混沌密码及其保密通信方案，绝大多数仅给出了计算机数值仿真结果，而硬件实现结果的报道偏少。特别是，包括发送端、接收端和实际传输信道在内的整个多媒体混沌保密通信系统的硬件实现结果尤为偏少。文献统计分析表明，只有少量混沌加密相关论文附有硬件实现，这在很大程度上归咎于硬件实现通常比数值仿真技术难度更大。

与数值仿真不同，硬件实现还需要考虑整个系统的硬件资源、硬件实现条件、实际信道环境和实时性受限等一系列实际问题。现有许多混沌密码方案，尽管数值仿真容易实现，但在硬件资源和实时性受限的情况下，硬件实现则很难甚至无法获得实验结果。因此，人们需要统筹兼顾各方面的因素，提出既能保证安全性又能保证硬件实现的优选方案。在此基础上，进一步从硬件设计与实现的角度解决广域网传输的实时远程视频、语音、图像等多媒体混沌保密通信的应用问题，并针对不同应用业务、应用环境和应用平台进行优化和融合，使混沌密码从理论分析与设计走向实际应用。

多年来，作者的研究工作在很大程度上受益于国家和省部级科研项目的连续资助。借此机会，衷心感谢国家自然科学基金面上项目(61172023、61671161)、国家自然科学基金重点项目(61532020)、国家重点研发计划子课题(2016YFB0800401)的资助。衷心感谢香港城市大学陈关荣院士、中国科学院数学与系统科学研究院吕金虎研究员。作者在从事研究过程中得到了许多同行的支持和帮助，其中的许多结果是作者与合作者共同完成的，在此表示衷心感谢。衷心感谢家人的长期支

持和理解。衷心感谢科学出版社的大力支持和帮助。

由于作者水平有限，书中难免存在疏漏或不足之处，热诚期待广大同行和读者批评指正。

禹思敏

2017 年 10 月于广州

目　录