分类号 TN918, N93 密级 公开

U D C

西安交通大學

博 士 学 位 论 文

数字化混沌密码的分析与设计

李树钧

指导教师姓名 蔡元龙 教 授 西安交通大学

牟轩沁 教 授 西安交通大学

申请学位级别 博 士 专业名称 信息与通信工程

论文提交日期 2003年4月 论文答辩日期 2003年6月

答辩委员会主席 王育民(西安电子科技大学)

评 阅 人 陈关荣(香港城市大学)

黄国和(香港城市大学)

王育民(西安电子科技大学)

徐健学(西安交通大学)

殷勤业(西安交通大学)

2003年4月 (最后修订：2009年5月13日)

论文题目: 数字化混沌密码的分析与设计
专　　业: 信息与通信工程
研究方向: 混沌加密
博 士 生: 李树钧　　(签名) _____
指导教师: 蔡元龙 教授　　(签名) _____
　　牟轩沁 教授　　(签名) _____
论文类型: 应用基础

摘　　要

自从二十世纪80年代以来，应用数字化混沌系统构造新型密码系统的想法收到了越来越多的关注。这样一个想法来自混沌理论和纯粹密码学之间的自然联系：强混沌系统的动力学特性大致对应着高强度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拟混沌现象（我们甚至可以在Shanon关于保密系统理论的经典文章里面看到混沌的影子）。一般而言，目前存在两种不同的混沌密码范式，一种是模拟化的混沌保密通信系统（大多基于混沌同步技术），另外一种是在数字计算机上实现的混沌密码系统。本文主要讨论数字化混沌密码系统，也就是位于混沌理论和纯粹密码学之间的研究领域。

早在1990年前后，数字化混沌密码就曾经有过短暂的繁荣时期，但是很快就由于负面的密码分析工作而很快消退。第二次繁荣在2000年前后兴起，有大量的研究结果发表，出现了不少很有希望的进展。尽管相当数量新提出的数字混沌密码还是很快被分析了，但是仍有很多直到目前尚未遇到真正有效的攻击。另外，一些设计混沌密码的通用方法已经出现，这些方法往往对系统的安全性做了相当细致的分析，从而具有较高的实用价值和安全性，这样的例子如使用由混沌系统生成的(固定的或者动态更新的)S盒的分组密码。

但是，作为数字化混沌密码设计中的一个重要问题，数字化混沌系统的动力特性退化却没有受到大多数混沌密码设计者应有的重视。本文的目的之一就是要强调这个问题的重要性，并给出一些初步的分析结果（参考本文成果的第一点）。

本文关于数字化混沌密码的研究设计下面三个方面：数字化混沌系统动力特性退化的理论分析；数字化混沌密码的分析；和新的混沌密码的设计方法。具体说来，本文的主要成果包括如下几个方面：

1. 由于逐段线性混沌映射(PWLCM)具有优良的动力学特性，并且具有简单的软硬件实现方法，因此在数字化混沌密码的设计中得到了广泛的应用。针对数字化逐段线性混沌映射，本文提出了一组动力学指标，可以用来定量地衡量数字混沌系统动力特性退化的程度。严格的理论分析给出了准确计算这些

动力学指标的办法。这些指标可以用来对几种改善动力特性退化的方法做比较评价，也可以用来发现数字化混沌密码系统中的安全缺陷。

2. 基于上面研究的逐段线性混沌映射动力学特性退化的理论结果，本文对复旦大学周红等人提出的几种混沌流密码进行了弱密码分析，并在此基础上提出了一类密码分析方案。本文对一些可能的改进方案进行了比较，给出了几种可行的改进方案。

3. E. Alvarez等人于1999年提出了一种混沌密码，该密码通过在一个伪随机序列中搜索明文的办法来生成密文。但是该密码很快就被G. Alvarez等人在2000年破解。本文分析了原密码方案不安全的几个本质缺陷，提出了一种改进方案以抵抗已知攻击。

4. M. S. Baptista等人于1998年提出了另外一种基于搜索的混沌密码，该密码方案在提出后受到了广泛关注，近年来陆续有密码分析和改进方案发表。本文分析了Goce Jakimoski与Ljupčo Kocarev提出的一类攻击，指出它的性能并不够强，并提出了一种措施改进原密码方案使之可以抵抗Jakimoski-Kocarev攻击和G. Alvarez于2003年新提出的攻击。

5. 针对S. Papadimitriou等人于2001年提出的一种概率分组密码，我们的分析指出该密码既不实用也不安全。我们同时更正了该密码中存在一些错误分析。

6. J.-C. Yen和J.-I. Guo等人近年来陆续提出了几种混沌图像加密算法。本文对其中的两种算法进行了密码分析，发现它们在已知/选择明文攻击下是不安全的。

7. 在前面关于数字化混沌系统的理论分析和对部分混沌密码的密码分析的基础上，本文提出了一类新的混沌伪随机比特发生器，并将其代替LFSR来构造混沌流密码，分析表明CCS-PRBG有希望用来设计性能优于其他混沌流密码和基于LFSR的流密码的密码系统。另外，本文还提出了一种基于多(2^n个)混沌系统的快速密码系统，该系统针对实时视频加密的需求做了专门设计，可以满足视频加密在速度和格式上的需求。

关键词： 混沌系统；密码学；密码分析；流密码；分组密码；伪随机序列；逐段线性混沌映射(PWLCM)；图像加密

Title: Analyses and New Designs of Digital Chaotic Ciphers
Major: Information and Communication Engineering
Specialty: Chaotic Cryptography
Name: Shujun LI Signature: _____
Supervisor: Prof. Yuanlong CAI Signature: _____
Prof. Xuanqin MOU Signature: _____
Type: Applied Foundation

Abstract (英文摘要)

Since 1980s, the idea of using digital chaotic systems to design new ciphers has attracted more and more attention. The use of chaos in cryptography depends on the natural relation between the two research areas: strong dynamical properties of chaotic systems implies strong cryptographical properties of cryptosystems, and the basic way to make cryptosystems have good strong cryptographical properties implies quasi-chaos (we even can find the phantom of chaos in Shanon's classic paper on theory of secrecy systems). Basically speaking, there are two paradigms of applying chaos for secure applications: analog chaotic secure communications (mainly based on chaos synchronization technique) and digital chaotic ciphers realized in computers. This dissertation only focuses on digital chaotic ciphers, i.e., the area lying between chaos theory and pure cryptography in finite-state (digital) world.

The first boom of research on digital chaotic ciphers occurred near 1990, but decayed rapidly after some negative works on the security of proposed ciphers. The research boom returned in late 1990s, and much more contributions are made to get many promising achievements. Although a number of recently-proposed digital chaotic ciphers have been cryptanalyzed, many others have not been effectively attacked. Also, some general ways to digital chaotic ciphers have been proposed and more careful considerations are made to ensure their security, such as the chaotic block ciphers based on fixed or dynamic S-boxes.

However, as an important issue in the design of digital chaotic ciphers, dynamical degradation of digital chaotic systems has not been seriously considered by most designers of digital chaotic ciphers. One task of this dissertation is to emphasize significance of this issue and to give some initial investigations.

Our contributions in this dissertation involve the following three aspects about digital chaotic ciphers: theoretical analyses of dynamical degradation of digital chaotic systems, cryptanalyses of digital chaotic ciphers, and new proposals of digital chaotic ciphers. The main achievements contained in this disserta-

tion are as follows:

1. Because of piecewise linear chaotic maps (PWLCM-s) have perfect dynamical properties and can be realized simply in both hardware and software, they are widely used in digital chaotic ciphers. Aiming at digital PWLCM-s, a series of measurable dynamical indicators are proposed to quantitatively measure the dynamical degradation of PWLCM-s in (fixed-point) finite precision. Rigorous theoretical analyses are given to show how to calculate the dynamical indicators. The proposed dynamical indicators are used to compare performances of different remedies to dynamical degradation of digital chaotic systems, and are used to find security defects in digital chaotic ciphers.

2. Based on the theoretical results on dynamical degradation of PWLCM-s (see above), some digital chaotic stream ciphers proposed by Hong Zhou et al. are cryptanalyzed with weak-key analyses. Possible solutions to enhance concerned ciphers are compared and some ones are suggested as practical remedies.

3. In 1999, E. Alvarez et al. proposed a chaotic cipher based on searching plaintext in a pseudo-random sequence generated from chaotic systems, but soon it was broken by G. Alvarez et al. in 2000. This dissertation proposes a modified scheme to enhance its security by avoiding some essential defects in original cipher.

4. In 1998, M. S. Baptista proposed a searching based chaotic cipher, which attracted much attention after its proposal. Some cryptanalytic works and modifications are made in recent years. This dissertation points out the deficiency of an attack proposed by Goce Jakimoski and Ljupčo Kocarev, and presents a remedy to resist Jakimoski-Kocarev attack and some new attacks proposed by G. Alvarez in 2003.

5. This dissertation analyzes problems of a probabilistic chaotic cipher proposed by S. Papadimitriou et al. in 2001 and finds it is insecure and impractical. Also, some wrong results in this cipher are pointed out and rectified.

6. J.-C. Yen and J.-I. Guo et al. proposed several chaotic image encryption methods in recent years. This dissertation breaks two Yen-Guo chaotic image encryption methods with known/chosen plaintext attack, and finds more security problems in one method.

7. Based on theoretical results on digital chaotic systems and cryptanalyses of several recently-proposed chaotic ciphers, this dissertation proposes a new

chaotic PRBG and uses it to design chaotic stream ciphers with better overall performances. The proposed chaotic PRBG can be used instead of LFSR in conventional stream-cipher cryptography to construct more flexible ciphers. This dissertation also proposes a fast chaotic cipher employing multiple (2^n) chaotic systems. This fast cipher is specially designed to fulfill needs of real-time video encryption.

Keywords: chaotic system; cryptography; cryptanalysis; stream cipher; block cipher; pseudo-random sequence; piecewise linear chaotic map (PWLCM); image encryption

目录

第一部分

数字化混沌密码：现状回顾与相关理论问题

第一章 绪论

§1.1 研究背景与课题意义

作为一个令人惊讶的自然科学分支，混沌理论自二十世纪60年代快速地发展起来*，并最终在70年代得到了基本确立。与混沌相关的早期研究涉及了许多完全不同的研究领域，如数学[2–5]，物理学[6–8]，生物学[9]，化学[10, 11]，工程领域[12, 13]，等等[14, 15]。混沌最广为人知的特性就是所谓的“蝴蝶效应”(正规地说应该称为对初始条件和/或控制参量的敏感性，或者正的Lyapunov指数)[12, 13, 16]，这个特性使得由确定性方程产生的混沌轨道随着时间的流逝而变得越来越“不可预测”。

一些研究者已经指出在混沌理论和密码学之间存在着紧密的联系[17–22]。许多混沌系统的基本特性，如遍历性(ergodicity)、混合性(mixing)、确定性(exactness) †和对初始条件的敏感性，都可以和密码学中的混淆(confusion)和散布(diffusion)概念联系起来。因此，使用混沌系统去开发新的密码设计思路就变得很自然了。另外，由于很多混沌系统在过去的几十年里面已经得到了深入的研究，在混沌领域有大量的既有成果可供设计混沌密码和分析性能所用。自二十世纪80年代以来，已经出现了很多不同的混沌密码系统以及相关的分析成果[18–22, 24–141]。

有趣的是，在密码学中使用混沌的想法甚至可以追溯到Shanon在1949年发表的经典论文“Communication Theory of Secrecy Systems”[142]。当然，他不可能使用当时尚未诞生的“混沌”(chaos)一词，他只是提到好的保密系统中所需要的好的混合变换(mixing transformations)可以使用基本的“rolled-out and folded-over”操作得到。考虑一下Baker映射和Smale马蹄这类的典型混沌系统我们就可以知道，在混沌系统中，“拉伸并折叠”(stretch-and-fold)是常见的引发混沌的原因，显然Shanon所说的好的混合变换可以被看做是限制在有限空间内的(混沌)映射(当然这不是严格意义上的)[14, 15]。在文献[19]中，Ljupčo Kocarev等人演示了一种使用混沌映射构造类似DES的分组密码的通用方法。最近几年里，使用混沌构造S盒并将其用于分组密码设计的想法陆续有一些新的研究报道，如Ljupčo Kocarev等人的文章[105, 108]，Jesús Urías的文章[52]和我们的文章[112]。这些研究显示混沌可以很自然地在传统密码学的框架下得到运用，就象传统密码学中一些其他的常用基本算法一样。

另外，既然好的密码特性是通过确定性的密码系统产生的伪随机混乱状态保证的(考虑一下分组密码中经常用到的取模操作和非线性S盒使有意义的明文变成“乱码”似的密文[143, 144])，从算法的角度看，任何好的密码系统也可以看成是一个混沌或者拟混沌系统[145]。好的密码系统对明文加密带来的密文混乱状态，非

*关于混沌的早期工作可以一直追溯到1890年前后H. Poincaré所做的关于三体运动的复杂性问题[1]。
†关于相关概念的定义，请参考文献[23]。

常类似于由复杂动力系统产生的混沌现象[17]。已有文献报道这方面的问题，在文献[21]中，Marc Götz等人的研究表明在某些传统流密码中存在着(拟)混沌行为。实际上，当混沌系统在计算机上以有限精度实现时，模(mod)操作经常被使用来描述混沌方程的离散形式[86, 89, 96, 119, 120, 124]，而我们知道，取模在传统密码学中是最基本的常用操作。

通过以上讨论，我们有理由相信关于混沌密码学的研究有助于丰富传统密码学的内容，为好的密码系统的设计提供更多的设计思路和手段。另外，在本文的后续章节，我们将发现关于混沌密码学的研究也可以丰富关于离散时间离散空间的混沌系统(也就是所谓的数字化混沌系统)的理论知识。

显然，混沌密码学是一个横跨多个学科的研究领域，它涉及了非线性动力学(混沌理论)、(传统)密码学、通信工程等多个领域。这使得关于混沌密码学的文献往往散布在各个相关学科，而不象其他领域那么集中。除了少量文献发表在密码学相关的会议和杂志外[20, 22, 25, 44, 54–56, 59–61, 63, 64, 109]，大部分文献都是在密码学以外的领域发表的，尤其是在物理和电子工程领域。观察本文的参考文献列表即可看到，大部分文章发表在下述地方：*Physics Letters A*，*Int. J. Bifurcation and Chaos*, *Physical Review*系列，*IEEE Trans. on Circuits and System*和*IEEE Int. Symposium on Circuits and Systems*。

在混沌密码学中，一般有两个基本的设计模式：第一个模式对应模拟**混沌**保密系统，它们一般是在模拟电路系统中基于混沌同步技术实现的[24]；第二个模式则对应在计算机(或者数字电路)上实现的**数字化**混沌密码系统，它们和混沌同步技术无关。一般而言，基于同步的混沌保密系统是设计用来实现有扰信道上的保密通信，一般不能直接推广到传统密码学中去。更为重要的一点是，大量的密码分析工作已经表明大部分基于混沌同步的保密通信系统都不够安全，恶意的攻击者可能从截获的信号中恢复和秘密参数相关的部分有用信息(甚至可能近似确定这些参数)[25–29, 32, 36, 39–41]。因此，尽管混沌同步技术目前仍然在保密通信领域得到广泛的研究，但是相关的成果对于传统密码学而言价值比较小。本文主要致力于研究混沌密码学和传统密码学之间的部分，也就是所谓的数字化混沌密码。在下一章本文将给出一个数字化混沌密码研究现状的详细而尽可能全面的介绍。

§1.2 本文的主要成果

本文中关于数字化混沌密码的研究最早来自于我们在医学成像系统中对图像安全问题的兴趣。当作者于1999年参与RA3900II型DSA(Digital Subtraction Angiography，数字血管造影[146])系统的时候，医学影像在网络环境下的安全传输问题得到了一定的关注。后来，在一项国家自然科学基金(编号30070225)和一项国家“863”计划项目(编号2001AA114152)的部分支持下，关于数字化混沌密码的研究得以开展，本文将叙述我们在这个方向获得的已有成果。

本文关于数字化混沌密码的研究成果可以归纳为下面三个大的部分：数字化混沌系统的动力学特性退化的理论分析；一些最近提出的数字化混沌密码的分

析；设计数字化混沌密码的新思路。第一个方面的研究是后面两个方面的基础，而第二个方面的研究又是第三个方面的另外一个基础。总的来说，本文的主要成果可以总结为以下几点：

1. 由于逐段线性混沌映射(PWLCM，Piecewise Linear Chaotic Map)具有良好的动力学特性，并且易于使用软硬件实现，因此在数字化混沌密码中得到了广泛的应用。但是，目前还没有一个系统的关于数字化混沌系统动力学特性退化的理论框架，因此给数字化混沌密码的理论分析带来了实际的困难。针对逐段线性混沌映射，本文发现了一组动力学指标可以用来定量描述混沌系统在有限精度下实现时的动力学特性退化。研究了这组动力学指标的计算方法并得到了一些严格的理论结果。这些结果可以用来定性地比较几种对数字化混沌系统动力学特性退化的补救措施的性能，也可以用来在相关的数字化混沌密码和混沌伪随机发生器中发现潜在的缺陷。

2. 基于上面提出的逐段线性混沌映射的动力学指标，对复旦大学周红等人(1997、1998年间)提出的一类混沌流密码进行了弱密钥分析，并提出了一种基于弱密钥分析的改进穷举攻击方法，可以将密钥熵降低两个比特。讨论了几类可能的改进方案及其性能，其中的几种方案被推荐使用以改善原密码系统的安全性。

3. E. Alvarez等人于1999年提出了一种基于搜索机制的混沌密码，该密码通过在一个伪随机序列中搜索明文的办法生成密文。不过很快这种混沌密码就被G. Alvarez等人于2000年成功攻击。本文分析了E. Alvarez等人密码不能抗击G. Alvarez等人提出的密码分析的原因，提出了一种改进方案以增强原密码的安全性。

4. M. S. Baptista于1998年提出了另外一类基于搜索机制的混沌密码。这类密码在提出后受到了较多关注，后面的几年时间里陆续有密码分析和改进方案发表。本文指出Goce Jakimoski和Ljupčo Kocarev在2001年提出的一类攻击在实际中并不是很有效，并提出了一种原密码的改进方案以抵抗所有已知攻击。在提出的改进方案中，发现了一种本文称为“概率解密”的有趣现象，它在密码学中的可能应用将在我们的后续研究中继续进行。

5. S. Papadimitriou等人于2001年提出了一种基于混沌系统的快速概率密码方案。本文分析了在该密码系统中存在的问题，指出该方案不安全，也不实用。同时纠正了原密码方案中的一些错误结论。

6. 近年来中国台湾的J.-C. Yen和J.-I. Guo(等人)陆续提出了多种混沌图像加密方法。本文对其中的两种方法(CKBA和BRIE)进行了密码分析，指出它们在已知/选择明文攻击下是不安全的；对BRIE的一些特殊的安全问题也做了详细讨论。

7. 基于本文对数字化混沌系统的理论研究和对部分数字化混沌密码的分析工作，本文提出了一类新的混沌伪随机发生器并使用它构造新的混沌流密码，这些混沌流密码较其他混沌流密码而言具有更好的整体性能。该类混沌伪随机发生器可以替代LFSR(线性反馈移位寄存器)作为流密码的一个核心组件设计更为安全灵活的流密码。

8. 基于本文对数字化混沌系统的理论研究和对部分数字化混沌密码的分析工作，本文提出了一类快速混沌密码方案。该方案为实现实时视频加密进行了特殊设计。分析表明该类密码方案可以在不损失安全性的情况下实现相当高的加密速度。该类方案可以看成是数字化(混沌)密码的一种新的通用模型。

§1.3 本文的组织

本文的主体可以分为三个大的相对独立的部分，每个部分对应本文成果涉及的数字化混沌密码的三个方面(见上)。第二章主要对目前数字化混沌密码的研究现状做了一个详尽的回顾。第三章主要介绍关于数字化混沌系统(逐段线性混沌映射)动力学特性退化问题的理论研究。第四章到第七章是一些最近提出的数字化混沌密码的分析工作。第八和第九章介绍两种新的密码设计方法。最后一章给出本论文的总结，并指出了未来的研究发展方向。下面是一个关于各章内容的较为详细的介绍：

第二章对二十世纪80年代以来直到目前(2003年)的数字化混沌密码研究现状给出了一个详尽的回顾。按照设计方法的不同，所有(本文作者所了解的)数字化混沌密码被分为三个大类进行了详细的介绍。作为数字化混沌密码设计和分析中的一个非常重要的问题，从理论和实践两个方面对数字化混沌系统在有限精度下的动力学退化问题做了详细讨论。其他有关问题也做了较为细致的讨论，并给出了我们对这些问题的一些建议和看法。

第三章着重分析逐段线性混沌映射(PWLCM)的一组动力学指标以及它们在数字化混沌密码中的应用。研究发现这组动力学指标可以定量描述数字化逐段线性混沌映射的动力学特性退化，并且这组指标的值由控制参数唯一确定，这些控制参数一般在数字化混沌密码中被选做密钥(或者密钥的一部分)。这组指标的一个较为独立的应用是：它们可以用来定性比较几种改善数字化混沌系统动力学特性退化的错误的性能。这一章得到的结论结果将在下一章得到应用，用于分析周红等人提出的一类混沌流密码。

基于第三章给出的数字化逐段线性混沌映射的理论结果，第四章对周红等人提出的一类混沌流密码进行了弱密钥分析。在弱密钥分析的基础上，提出了一种增强的穷举攻击方法，可以使得密钥熵相对简单穷举攻击降低两个比特。尽管密钥熵的降低并不是很明显，该攻击对于弱密钥的攻击则非常奏效，因此原密码方案需要做一定的改进以强化安全性，避免弱密钥的出现。讨论一些可能的改进方案，其中的几种被推荐在应用中使用，当然更多的研究还需要继续以证实这些改

进方案的实际效果。

第五章描述我们关于基于搜索机制的数字化混沌密码的相关工作。两种典型的基于搜索的数字化混沌密码分别于1999和1998年被E. Alvarez等人和M. S. Baptista提出。一些有关的密码分析和改进方案在近年来陆续被报道，已经知道上述两种密码都不够安全。针对E. Alvarez等人的密码方案，本文分析了该方案不安全的原因并提出了一种改进方法以抵抗相关攻击。针对M. S. Baptista的密码方案，本文指出Goce Jakimoski和Ljupčo Kocarev于2001年提出的一种攻击方法在实际中并不是特别有效，并提出了一类改进方案抵抗Jakimoski-Kocarev攻击和其他的几种新近提出的攻击方法(由G. Alvarez等人于2003年提出)。在本文提出的M. S. Baptista密码的改进方案中，一种称为“概率解密”的现象被观察到，它的未来可能应用留待我们的后续研究。

第六章的内容是关于S. Papadimitriou等人2001年提出的概率混沌密码方法的密码分析。由于这种混沌密码的特殊实现方法，分析发现这种密码方案既不安全，也不够实用。该密码中一些错误的分析结果也在本文中得到了纠正。

第七章的内容显示J.-C. Yen和J.-I. Guo提出的两类混沌图像加密方法是不够安全的，它们不能抵抗已知/选择明文攻击。另外，对其中一种混沌图像加密方法的其他安全缺陷也进行了细致的分析。大致来说，这一章中给出的分析思路也适合于对J.-C. Yen和J.-I. Guo(等人)提出的其他几种混沌加密算法进行密码分析，这些留待我们将来的工作完成。

第八章提出了一种基于双混沌系统的新型混沌伪随机比特发生器，本文称之为CCS-PRBG。理论分析和实验都表明CCS-PRBG具有理想的密码学特性。作为CCS-PRBG在流密码中应用例子，提出了几种可能的混沌流密码结构。初步分析表明这些混沌流密码可以达到较其他混沌流密码更好的整体性能。

第九章提出了一种面向实时视频加密的快速混沌加密方案。这类快速混沌密码采用下述思路实现快速加密并保证安全性：1) 使用了多个(2^n个)混沌系统；2) 组合了一个混沌流密码和一个混沌分组密码；3) 在混沌分组密码部分中使用了时变的S盒；4) 使用了内部(密文)反馈机制。这种密码的速度在700MHz的赛扬(Celeron)®CPU上可以达到46Mbps的速度，这个速度比大多数数字化混沌密码都要快得多，甚至比一些传统密码还要快。初步分析表明，通过代码优化，其加密速度还可以继续提高。

最后一章对全文进行了总结并给出了一些关于未来研究的展望。特别地，这一章给出了一些我们关于设计数字化混沌密码的建议。

第二章　基于数字混沌系统的密码学

§2.1　数字化混沌密码研究的历史回顾

尽本文作者所知，第一篇使用复杂动力学系统设计密码的文章是Wolfram在Crypto'85上发表的文章[44]，这篇文章提出了一种基于胞元自动机的密码系统。第二篇相关文章[45]也是关于胞元自动机密码的。不过这两篇文章并没有得到太多的关注。第一篇明确提到“混沌密码”并得到广泛关注和引用的文章是Robert A. J. Matthews于1989年发表的文章[55]，该文提出了一种基于变形Logistic映射的混沌流密码方案*。自从Matthews的流密码提出以来，数字化混沌密码受到了来自不同领域研究者越来越多的关注[18–22, 44–141]；同时数字化混沌密码的分析工作也随之发展起来，已经知道一些混沌保密系统是不够安全的[19–21, 36, 50, 56, 61, 63, 67, 88, 97, 100–103, 109, 111, 126–131, 139–141]。

Matthews的文章发表以后，主要是在密码学领域，数字化混沌密码的研究形成了一个小的研究热点并持续了大概四年的时间[46, 55–67, 67, 68]。这个研究热点的一个有趣的标志是三篇有关文章[60, 63, 64]同时出现在同一届会议上－EuroCrypt'91，至少六篇相关文章[55–57, 61, 62, 68]出现在密码学杂志*Cryptologia*上。在之后的几年时间里，部分由于文献[56, 61–63, 67, 68]中给出的负面分析结果，这个方向的研究变得沉寂下去，只有很少量的文献发表[47–49, 69–74]。1997年以后，一些新的数字化混沌密码[18–21, 50–52, 75–93, 132]的提出开启了新一轮的研究热潮，自2000年以来的三年多的时间里发表文章的数量几乎和以前这个方向的文章总数一样多[22, 35, 36, 53, 54, 94–100, 104–131, 133–141]。在最近几年，已有几篇关于数字化混沌密码的综述发表[19–21, 31, 101–103]，但是很多数字化混沌密码并没有得到介绍，而在2000年以后出现的成果[22, 35, 36, 53, 54, 94–100, 104–131, 133–141]更是几乎没有涉及。本章将试图给出一个这个方向研究的尽可能详细的回顾，并讨论数字化混沌密码设计中的一些相关问题及其解决方案。关于未来研究的一些建议和展望在本论文的最后一章给出。

基本上，数字化混沌密码有两种通用的设计思路：1) 使用混沌系统生成伪随机密钥流，该密钥流直接用于掩盖明文；2) 使用明文和/或密钥作为初始条件和/或控制参数，通过迭代/反向迭代多次的办法得到密文。第一种思路对应流密码，而第二种则对应着分组密码。除了以上两种之外，最近几年又出现一些新的设计思路，比如在分组密码中使用混沌生成S盒[52, 105, 108, 112]，和基于搜索机制的数字化混沌密码[84, 90, 104, 110, 113–116, 122, 123, 128]。和混沌密码在私钥系统中的研究比起来，混沌思想在公钥系统中的研究可谓少之又少。尽本文作者所知，只有四篇文献涉及这个方向的研究[42, 45, 46, 69]。不过，2003年刚刚出现在*Physical Review Letters*上的一篇文章[42] 看起来可能为混沌公钥系统的开发提供了一种有趣的新思路。

*有意思的是，混沌密码学的两种完全独立的想法几乎同时出现。就是在第二年(1990年)，L. M. Pecora和T. L. Carroll发现了混沌同步技术并提出了基于混沌同步的保密通信方案[24]。

本章的组织如下：§2.2，§2.3和§2.4分别介绍下面三个类别的数字化混沌密码：典型的混沌流密码，典型的混沌分组密码，其他所有的数字化混沌密码方案*。在第三类中的很多密码方案相当新颖(大部分是在2000年或者2000年以后提出的)，其中包含不少看起来是很有希望的思路。在§2.5中，本文主要讨论下述问题：当混沌系统在有限精度下实现时，其动力学特性会发生退化，数字化混沌密码在设计中必须克服这个严重问题。关于数字化混沌密码设计的更多考虑及其可能的解决方案在§2.6进行讨论。最后一节是本章的结论。

§2.2 典型的混沌流密码

§2.2.1 基于混沌伪随机数发生器的流密码

由于混沌系统可以产生“不可预测”的伪随机轨道，许多研究集中在使用混沌系统构造伪随机数发生器(PRNG)的相关算法及性能分析上面[17, 55, 58, 64–66, 71, 72, 72, 74, 77, 78, 80–82, 86, 92, 95, 95, 125, 147–165]。对于连续混沌系统而言，很多混沌伪随机序列已经被证明具有优良的统计特性。

大部分混沌流密码的核心部分是混沌伪随机数发生器，它的输出作为密钥流掩盖(一般采用异或操作)明文。两类主要的生成混沌伪随机数的方法是：A1) 抽取混沌轨道的部分或者全部二进制比特[55, 71, 72, 80–82, 86, 95, 125, 165]；A2) 将混沌系统的定义区间划分为m†个不相交的子区域，给每个区域标记一个唯一的数字$0 \sim m-1$，通过判断混沌轨道进入哪个区域来生成伪随机数[58, 64–66, 72, 74, 77, 78, 92]。需要注意这两类方法之间存在一定的联系：A1中的所有伪随机数发生器可以看作是A2中的特例，而一些属于A2的伪随机数发生器[58, 66, 78]又可以看作A1中的特例。

在大部分基于混沌伪随机数发生器的混沌流密码中，只使用了单个混沌系统。很多不同的混沌系统已经被采用：Logistic映射[66, 71, 99, 125]以及它的变形[55]，两维Hénon映射[64, 95]，Chebyshev映射[72]，逐段线性混沌映射[22, 71, 74–78, 80–82, 107, 117]，逐段非线性混沌映射[92]，p-adic离散混沌系统[86]，一阶非均匀采样数字锁相环(DPLL，Digital Phase-Locked Loop)电路[58, 65, 163]，等等。

作为一种增强安全性(在某些混沌密码中还可能提高加密速度)的通用手段，多混沌系统的使用被一些研究者建议[22, 71, 99]。在文献[71]中，Bernoulli移位映射和Logistic映射被同时使用，这两个混沌系统的输出首先进行异或，然后再掩盖明文。文献[99]提出了一种类似的流密码，也是基于两个独立的混沌映射，其中一个混沌映射被密文扰动。在文献[22]中，两个混沌系统的输出$\{x_1(i)\}, \{x_2(i)\}$按照下面的方法比较生成伪随机比特流：$\{k(i)\}$：如果$x_1(i) > x_2(i)$，则$k(i) = 1$，如果$x_1(i) < x_2(i), k(i) = 0$, 如果$x_1(i) = x_2(i)$则不输出任何数(这样一种混沌伪随机

*或者称它们为“非典型的混沌密码”，可以作为2003年全球(尤其是我国)抗击“非典型肺炎”的一个纪念。

†很自然地，从方便实现的角度考虑，$m = 2^n$。

比特发生器被称为CCS-PRBG)。在满足某些条件的情况下，生成的伪随机比特序列具有优良的密码学特性。文献[22]给出了一些基于CCS-PRBG的混沌流密码以说明CCS-PRBG的应用潜力。关于CCS-PRBG的更多细节，请参看第8章。

由[56, 61, 62, 67]中的工作可以得知，已经知道几种混沌流密码[55, 57, 64]是不安全的。在文献[141]中，我们对周红等人在文献[82]中提出的一类混沌流密码进行了弱密钥分析，并提出了一类改进的穷举攻击以降低攻击复杂度(更多的细节请参考第4章)。对于其他混沌流密码的安全性，还有更多的研究工作要做。

§2.2.2 通过混沌逆系统方法设计的流密码

在基于混沌同步的保密通信系统研究的推动，U. Feldmann等人在文献[73] 中提出了一种设计混沌保密通信系统的通用模式，它被称之为混沌逆系统法(chaotic inverse system approach)。从概念上讲，混沌逆系统的设计思路相当于重新描述了普通密码的一般设计模式，因此该方法也可以用来指导数字化混沌密码系统的设计(并且不限于流密码或者分组密码)。实际上，有不少的混沌保密通信系统可以使用这种模型加以描述。文献[21, 83]详细地研究了这类混沌密码的一种一般结构和密码分析。

观察混沌逆系统加密方法的一般结构，可以看出这类结构更象分组密码，而不是流密码。为什么本小节将讨论的数字化混沌密码归入混沌流密码呢？实际上，所有本小节将要介绍的混沌密码虽然相当于工作在CBC模式下的分组密码，从整体上看更象是自同步的流密码，密文反馈经过处理之后的输出直接用于掩盖(采用模加操作)明文。既然明文不是被核心组件(类似分组密码的部分)直接加密，而是被核心组件生成的密钥流加密，因此我们倾向于认为这样的混沌密码为混沌流密码，而不是混沌分组密码，以强调它们在结构上与基于混沌伪随机数发生器的流密码的相似之处。一个比较明显的例子是：文献[82] 中的混沌密码明显是一个混沌流密码(基于混沌伪随机数发生器)，我们没有理由把文献[75, 76]中提出的基于混沌逆系统法构造的混沌密码看成是分组密码，因为这三种密码在结构和算法上根本就是一样的。

文献[70, 75, 76, 98]提出了几种基于混沌逆系统的数字化混沌密码。它们的结构可以基本上都可以表示如下：$y(t) = u(t) + f_e(y(t-1), \cdots, y(t-k)) \bmod 1$，这里$u(t)$，$y(t)$分别表示明文和密文，$f_e(\cdot)$是一个从反馈密文生成掩盖明文的伪随机密钥流的$k$元函数。在文献[70]中，$f_e(t) = a \cdot y(t-1) + b \cdot y(t-2)$。在文献[75, 76]中，$f_e(t) = F^m(y(t-1), p)$，这里$F(x, p)$是一个在$L$-bit($L < m$)有限精度下实现的逐段线性混沌映射：

$$F(x,p) = \begin{cases} x/p, & x \in [0, p) \\ (x-p)/(0.5-p), & x \in [p, 0.5] \\ F(1-x, p), & x \in [0.5, 1) \end{cases} 。 \tag{2.1}$$

文献[98] 中提出的混沌密码实际上是文献[75, 76]中密码的一个变形，采

用了双分辨率(dual-resolution)技术以增强安全性。假设明文分组大小为$L = 8$，给定一个保密整数$P \gg 2^L$和另外七个保密参数$p_1, p_2, p_3, c_1, c_2, c_3, c_4$，其加密过程可以描述如下：$y(t) = u(t) + \left\lfloor 2^L \cdot F^8_{PWL}(u'(t)) \right\rfloor \bmod 2^L$，这里$u'(t) = \left[\sum_{i=1}^{4} \frac{c_i}{P} \cdot y(t-i)\right] \bmod 1$，

$$F_{PWL}(x) = \begin{cases} x/p_1, & x \in [0, p_1) \\ (x-p_1)/(p_2-p_1), & x \in [p_1, p_2] \\ 1.0-(x-p_2)/(p_3-p_2), & x \in [p_2, p_3] \\ 1.0-(x-p_3)/(1.0-p_3), & x \in [p_3, 1) \end{cases}。 \tag{2.2}$$

显然，上述映射是逐段线性混沌映射(2.1)的一个推广版本(取消了原映射相对$x = 0.5$的对称性)。在文献[111]中，上述密码被选择密文攻击分析，不过这篇分析文章中给出的主要结论有点问题：原密码方案中的F^8_{PWL}被简化为F_{PWL}。但是多次迭代却是原方案中保证混沌系统的保密参数p_1, p_2, p_3安全的一个重要因素，这在周红等人的文献[75, 76, 82]中已有详细的论证。作为抵抗“选择密文攻击”的一个解决办法，F^m_{PWL}被文献[111]再次推荐*。

文献[119, 124]中提出的混沌密码也是基于混沌逆系统法设计的(尽管原作者没有这样声称)。单向耦合映射网格(OCML, One-way Couple Map Lattices)在该类密码中采用，并且多个映射单元同时用于加密和解密。文献[124]中的混沌密码的整体性能号称超过了AES(Advanced Encryption Standard)[166]，这个结论尚待确认。

文献[70]中提出的密码方案已经知道对已知/选择明文攻击是不安全的[88]。周红等人在文献[75]中指出了一些常见混沌逆系统方案的安全问题。我们的最近工作表明周红等人的密码在严格密码学意义上也不够安全(参看第4章)。关于其他混沌密码的安全性，尚需更多研究工作证实。

§2.3 典型的混沌分组密码

§2.3.1 基于逆向(迭代)混沌系统的分组密码

使用混沌系统的逆向迭代构造密码系统的想法最早是由T. Habutsu等人在[59, 60]中提出。为了方便后文的叙述，我们称这种密码为HNSM密码(以文献[59, 60]的四个作者姓的首字母命名)。给定一个秘密密钥p和如下的tent映射$F_p(x)$以及它的(随机)逆向映射$F_p^{-1}(x)$：

$$F_p(x) = \begin{cases} x/p, & x \in [0, p] \\ (1-x)/(1-p), & x \in (p, 1] \end{cases}, \tag{2.3}$$

*在n-bit有限精度下，文献[111]推出$m \geq n/2$可以足够保证抗攻击性，但是这个结论实际上还嫌不足，按照文献[82]的分析，$m \geq n \cdot \log_2 \left(\max(p_1, p_2-p_1, p_3-p_2, 1.0-p_3)^{-1}\right)$是必要的。

$$F_p^{-1}(x) = \begin{cases} px, & b = 0 \\ 1-(1-p)x, & b = 1 \end{cases}, \tag{2.4}$$

这里b是一个在{0,1}上均匀分布的随机比特变量。该密码按照如下方式加密每个明文分组$P \in (0,1)$为密文C：$C = F_p^{-n}(P)$，这里需要生成n个随机比特$b_1 \sim b_n$来确定每次逆向迭代的输出。很自然地，明文P可以容易地通过正向混沌迭代恢复：$P = F_p^n(C) = F_p^n(F_p^{-n}(P))$。由于在逆向迭代中存在量化噪声，密文中必须包含更多的有效位数以保证解密结果的正确性。

由于tent映射的逐段线性性和n个随机比特的使用，E. Biham提出了一种选择密文攻击和一种已知明文攻击成功地分析了HNSM混沌密码[63]。这个事实在密码学文献中被广泛引用，以说明混沌加密的不安全性[143, 144]。但是，我们的分析发现，Biham攻击的实际复杂度相当高而不是那么实用，而且可以利用一些简单的技术对HNSM密码进行改进，以抵抗Biham攻击[131]。

在HNSM混沌密码提出以后的几年里面，几种改进方案在文献[47, 48, 79, 91, 107, 116, 117]中被提出。文献[47, 48]中采用触发胞元自动机(Toggle Cellular Automata)替代tent映射；文献[79]采用定义在单位平面$[0,1]\times[0,1]$上的二维动力学系统，文献[91]则采用了定义在$[0,L)\times(0,\pi)$上的一个粒子反射混沌系统。文献[107, 117]定义了一个在有限离散空间$\{1/M, 2/M, \cdots, M/M\}$上的一一离散混沌映射$\tilde{f}_a$，该映射在整数空间$\{1,2,\cdots,M\}$上的版本$\tilde{F}_A$被用来构造混沌密码。文献[107, 117]的方案通过将混沌映射数字化为一一映射的办法避免了随机比特的使用。文献[116]采用了多了4分段的逐段线性映射，在一个有限长密钥序列的驱动下进行加密。到目前未知，上述改进方案的安全性仍待进行深入的考查。作为一个负面的报道，文献[116]中提出的改进方案已经被G. Alvarez等人成功地破解[127]，其采用的攻击方法是Biham攻击的推广。

文献[47, 48, 52]中提出的胞元自动机密码也采用了逆向迭代的思路，由于它们都是基于胞元自动机的，而且也不是“典型”的混沌分组密码，我们将在后续的小节里面对它们进行介绍。文献[93]使用延迟动力学系统设计了一类分组密码，该类密码也可以看作是HNSM密码的一种变形。

§2.3.2 基于正向迭代混沌系统的分组密码

这类混沌密码在文献[18, 85, 89, 96, 120, 136]中提出，其中的大部分是面向图象加密的[18, 85, 89, 136]。

文献[18, 85, 89, 136]中提出的密码均基于二维混沌映射。它们的基本加密流程可以描述如下：通过(正向)迭代一个二维映射来伪随机置乱明文图象中的像素(即搅乱像素在明文图象中的位置)，然后利用某些替换算法压平明文图象的直方图(对应明文图象中像素灰度的概率分布)；重复以上过程n次得到密文图象。为了实现对(不同分辨率)明文图象的伪随机置乱，必须对采用的二维混沌映射在离散网格(格点对应像素)上做适当的数字化，使原来的二维混沌映射对任何分辨

率的图象均为一一变换(置换)，如文献[18]中的离散Baker映射，文献[85]中的离散Kolmogorov流，以及文献[89, 136]中的截断Baker变换。实际上，受二维混沌映射驱动的伪随机置换与替换算法的组合使得密码分析变得相当困难。到目前为止，尚未见到有关的密码分析报道。

文献[96, 120]中提出的混沌密码基于两种级联起来的不同混沌系统f, g。为了保证解密的正确性，两个数字化混沌系统的混沌轨道周期必须是固定的值。假设P_i, C_i分别代表第i个明文和第i个密文，加密过程可以表示为$C_i = g[k, f(n, P_i)]$，相应的解密为$C_i = g[K-k, f(N-n, P_i)]$，这里$N, K$分别表示混沌映射$f, g$的固定轨道周期。尽管尚未有密码分析报道，我们认为使用固定周期是不合理的*，因为这会使得加密解密速度变得异常得慢，并且使得已知/选择明文攻击变得可能(N, K不可能太大)。

§2.4 其他数字化混沌密码：新世纪的新思路

在本节中我们将对2000年前后提出的有关混沌密码的新思路做一个回顾。对胞元自动机密码和混沌公钥密码系统的介绍也在本节给出。鉴于我们的密码分析工作主要是针对本节介绍的混沌密码，关于其中部分密码的更多细节也可以在本文的后续章节里面看到。

§2.4.1 基于搜索机制的混沌密码(参考第5章)

在文献[84, 90]中，一类基于在伪随机序列中搜索明文机制的混沌密码被提出。在本文中我们一般简称这样的混沌密码为基于搜索的混沌密码(searching-based chaotic ciphers)。由于它们在设计上的特殊性，很难将它们硬性归入流密码或者是分组密码的范畴：M. S. Baptista提出的密码更象流密码，而E. Alvarez等人提出的密码更象是分组密码，它们的改进方案有的更象流密码，而有的则更象分组密码。

对于M. S. Baptista在文献[84]中提出的密码，被搜索的伪随机序列是混沌轨道本身。加密过程可以大致描述如下：将混沌系统的定义区间的一部分划分为S个单元区间，这些单元区间分别代表S个不同的明文符号；迭代混沌系统超过N_0次直到其轨道进入代表当前明文符号的单元区间，如果这时一个伪随机数发生器的输出$\kappa \geq \eta$ (这里$\kappa, \eta \in [0,1]$)，则输出当前迭代次数C_N作为密文。该密码使用Logistic映射作为混沌系统，当然其他的混沌系统也是可行的。该密码同时具有流密码和分组密码的一些特点，不过更象流密码。

对于E. Alvarez等人在文献[90]中提出的密码，被搜索的伪随机序列是从混沌轨道$\{x_n\}$按照下述二值化策略生成的：$x_n \leq U \to 0, x_n > U \to 1$，这里$U$是一个阈值参数，它可以是时变的。对于一个长度为$b_i$比特的明文，密码按照如下方式进行加密：任选一个初始条件，迭代混沌系统按照上述方法产生一个伪随机

*比较一下看，几乎所有的其他混沌密码都尽可能地试图避免可预测的轨道周期长度。

序列C，在该序列中寻找当前明文，如果找到则输出当前混沌系统的状态、当前的阈值参数U_i和明文长度b_i作为密文，如果在很长一段序列中都未找到明文，则将明文长度减少一个比特重复上述过程。该密码中使用的混沌系统是下述tent映射：

$$F(x) = \begin{cases} rx, & x \in [0, 0.5] \\ r(1-x), & x \in (0.5, 1] \end{cases} 。 \tag{2.5}$$

从本质上讲，这种密码是一个具有数据扩展和时变分组大小的分组密码。

在E. Alvarez等人的密码方案提出后不久，G. Alvarez等人就指出这种密码是相当弱的，当使用了上述的tent映射(2.5)时，它很容易被四种不同的攻击方法攻破[97]。稍后，在文献[100]中，G. Jakimoski和L. Kocarev也独立地提出了一种已知明文攻击成功地分析了E. Alvarez等人的密码系统。在文献[110]中，我们分析了原密码方案不安全的本质原因，并提出了一类改进方案抵抗上述攻击：选择混沌系统的初始状态和控制参数作为密钥，迭代混沌系统产生伪随机序列C，按照相同的办法在C中寻找明文，如果能找到明文，则将当前的迭代次数作为输出密文。显然，这种改进方案和M. S. Baptista的密码方案比较类似。

M. S. Baptista的密码方案在提出后得到了较广泛的关注，一些其他研究者提出了几种改进方案以增强其性能。在文献[104]中，W.-K. Wong等人建议使用一个额外的伪随机数以改善原密码中不均匀的密文概率分布。在文献[114]中，K.-W. Wong引入动态更新的查找表技术以获得更快的加密速度和增强安全性。在文献[123]中K.-W. Wong等人进一步提出了增强的动态查找表技术，并引入一个(临时)会话密钥(session key)以减少原密码的密文扩展。作为一个附加的成果，K.-W. Wong在文献[122]中将动态查找表技术同时用于加密和哈希(hashing)。在文献[113]中，A. Palacios和H. Juarez建议使用多个耦合的混沌映射网络中发生的交替混沌(cycling chaos)增强原密码方案的安全性。

在2002年，在E. Alvarez等人的密码基础上，文献[90]的同一研究小组又提出了两种新的密码方案[115, 116]，作为对原密码方案的改进。文献[115]中方案的两个主要特点是：1) 使用耦合映射网络替代了单一的Logistic混沌映射；2) 将密文替换为混沌迭代的次数，这使得该改进密码成为一种Baptista型的密码。文献[116]中提出的新方案使用了反向迭代进行设计，如我们在§2.3.1中介绍的，该方案并不安全。

一个共同点是都使用了多个混沌映射，而不像原系统只采用了一个单独的tent映射：文献[115]中使用了耦合映射网络(coupled maps network)，文献[116]中则使用了多个逐段线性混沌映射。文献[116]中提出的密码也采用了我们在§2.3.1中提到的逆向混沌迭代的思路。

在文献[100]中，G. Jakimoski和L. Kocarev对M. S. Baptista的密码进行了密码分析，指出它在已知明文攻击下是不安全的(该类攻击实际上是一次一密攻击)。关于这种一次一密攻击的更细致的讨论可以在文献[126]中找到，该文献中使用符号动力学对该类攻击进行了更清楚明确的描述，并提出了另外三种基于符号动力学的攻击方案。从概念上讲，由于在密码结构上的相似性，所有上述攻击

方法也可以用来攻击文献[104, 110, 113, 114, 122, 123]中提出的改进方案。不过文献[114, 122, 123]中的改进密码方案对符号动力学的攻击方法[126]具有一定的抵抗能力，由于动态查找表混淆了混沌轨道和密文之间的关系。在文献[128]中，我们认为Jakimoski-Kocarev攻击[100]在实践中并不是特别有效，并提出了一类改进方法抵抗Jakimoski-Kocarev攻击。看起来我们的方法也可以抵抗基于符号动力学的攻击方案，因为混沌系统的迭代次数(即原密码方案中的密文)被成功掩盖了。关于基于搜索的混沌密码的更多讨论，请参考本文的第5章。

§2.4.2 在分组密码中使用混沌构造S盒

和数字化混沌密码设计中出现的其他想法比起来，使用数字化混沌生成分组密码S盒可能是一个很有希望和潜力的想法，它可以自然而成功地将混沌密码学和传统密码学连接在一起。有两种不同的构造“混沌”S盒的思路：动态的“混沌”S盒和固定的“混沌”S盒。

利用混沌生成动态的S盒

在密码系统中使用动态替换和置换的想法很早就被Terry Ritter在1990年前后发表的文章[167, 168]中提出过。Ritter的动态方案比较类似于W.-K. Wong(等人)在文献[114]中提出的动态查找表技术。

尽本文作者所知，使用混沌构造S盒的想法最早可以在一种基于胞元自动机的密码[52]中找到。这里S盒是由一个胞元自动机产生的，这个自动机被两个初始密钥k^{-1}和k^0确定，S盒在加密端和解密端分别通过反向迭代和正向迭代确定。如果我们将动态替换操作看成是类似流密码中的掩盖函数(如异或)，那么这种基于胞元自动机的密码更象是流密码，而非分组密码。

另外，在文献[87]中，厦门大学的郭东辉等人使用神经网络中的混沌吸引子设计了一种概率分组密码。在该密码中，一个伪随机数发生器和一个子密钥M一起控制一个神经网络产生随机密文。这里，从明文到密文的时变替换可以被看作是动态的S盒。郭东辉等人已经用硬件实现了这类密码的一个实际系统[94]。

在文献[112]中，我们首次明确提出了使用混沌构造动态S盒的想法。我们在该文中提出了一种由一个混沌流密码和一个混沌分组密码构成的快速混沌组合密码系统。该密码系统中共使用了2^n+1逐段线性映射，其中2^n个混沌系统用于加密(称为ECS，Encryption Chaotic System)，另外一个作为控制器控制整个密码系统的运行(称为CCS，Control Chaotic System)。CCS的初始条件和控制参数作为系统的密钥。在混沌流密码部分中，2^n个ECS被迭代(在CCS的控制下决定迭代哪个ECS)以掩盖明文。在分组密码部分中，一个伪随机的S盒通过对2^n个ECS的当前状态进行排序被动态更新，然后被用来替换被流密码部分掩盖的明文。两个部分都被CCS控制。初步的分析表明这种密码可以实现相当高的加/解密速度，尤其是在硬件实现情况下。不过文献[112]中给出的原始方案存在不安全的地方，我们将在第9章中通过引入内部反馈(或者密文反馈)对其进行改进以增强安全性。

在文献[118]中一种新的混沌分组密码采用了类似的思路：迭代tent映射(2.3)动态生成伪随机的噪声向量(noise vector)和S盒对明文进行加密。该密码运行在CBC(Cipher Block Chaining)模式[143, 144]下，密文反馈使得已知/选择、明文分析变得困难。

最后，需要特别提到的是，文献[114, 122, 123]中提出的动态查找表技术实际上也相当于动态S盒，不过这里动态更新策略本身不受混沌系统控制。另外，文献[106]中提出的生成2^e个顺序置乱整数的方法也可以用来生成动态S盒。

使用混沌生成固定的S盒

遵循传统分组密码的一般设计思路，L. Kocarev等人建议使用混沌系统构造S盒(非线性轮函数)[19, 105, 108]。他们提出了两种生成“混沌”S盒的方法：a) 直接定义一个原混沌映射的离散化一一映射的版本，例如文献[19]中的离散化映射(4) 和文献[108]中的映射(12)；b) 迭代一个混沌映射生成2^n顺序置乱的整数$1, 2, \cdots, 2^n$，然后利用它们构造一个$n \times n$的S盒*。最近，L. Kocarev等人的进一步分析表明这样的方法生成的S盒可以抵抗差分攻击和线性攻击[121]。

实际上，L. Kocarev等人的方法属于使用混沌系统设计好的非线性S盒的方法，而不是设计新的数字化混沌分组密码框架的方法。这也就意味着这种由混沌生成的固定S盒可以很自然在传统密码学框架内使用。类似地，可以有很多种不同的方法从数字化混沌生成S盒，只要设计出来的S盒足够好，它们就可以直接在传统分组密码中使用而不必和混沌系统本身发生关系。显然，前文提到的所有生成动态“混沌”S盒的方法都可以用来生成这种固定的“混沌”S盒。我们有理由相信，固定的“混沌”S盒必将丰富密码学家的设计工具箱。

由于针对S盒的各种攻击方法都需要足够多的已知/选择密文才可能生效，动态S盒应该可以更自然而简单地抵抗针对S盒弱点进行的密码分析。另外，我们在文献[112]和第9章中的分析表明动态S盒可能是一个构造快速混沌密码的捷径。出于这样的考虑，我们认为动态“混沌”S盒有希望成为未来数字化混沌密码的一个基本组件。

§2.4.3 一种基于混沌系统的概率分组密码(参考第6章)

文献[106]中提出了一种基于混沌系统的概率分组密码。一个包含K个不同的耦合方程(K个自变量)的混沌系统被用来生成2^d个虚拟吸引子，这2^d虚拟吸引子包含2^e个不同的虚拟状态$1, 2, \cdots, 2^e$，这里$e > d$。给定一个置换矩阵$\mathbf{P}_{2^d \times 1}$，密文从分配到第$\mathbf{P}[M_C]$个虚拟吸引子的所有状态里面随机选取，这里$M_C$表示$d$比特的当前明文。尽管文献[106]的作者声称该密码具有很好的安全性，我们发现该密码存在很多严重的问题[130]：

- 在该密码的实际实现和高安全性之间存在不可协调的矛盾：明文和密文的大

*关于产生置换整数的具体方法，请参考文献[105, 108]。

小d, e必须足够大以保证高安全性，而它们又必须足够小以使得该密码的实际实现成为可能。

- 关于所有可能的虚拟状态的数量的推导是错误的。
- 安全性分析是不正确的，对于穷举攻击的安全性被高估了。
- 密码的快速加密和解密恰恰依赖于第一个缺陷：d和e在取值大小上的矛盾。
- 当数字化混沌系统在有限精度下实现时，动力学特性的退化必须使用一些方法加以改善。
- 没有明确地描述如何从2^e个整数中选择2^d个虚拟吸引子和如何伪随机地分配2^e个虚拟状态到2^d个吸引子，也没有明确描述如何生成置换矩阵$\mathbf{P}$。

关于该密码分析的更多细节，请参考第6章。

§2.4.4 基于胞元自动机的密码

一个胞元自动机(CA, cellular automata)可以看作是一个模拟离散动力学系统的并行运算机。尽管两种基于CA的密码[44, 45]很早就出现了，在过去的十几年的时间里还是没有太多的CA密码被提出、分析和深入研究[44–54]。这里本文将给出本文作者所知的CA密码的简要介绍，其中的一种CA密码由于已经在前面的§2.4.2介绍过了，这里就不再赘述了。

在最早提出的CA密码[44]中，一种被称为rule 30的特殊CA被用作伪随机数发生器并用来构造流密码，密钥是该CA的初始条件。在文献[45, 46]中，一种可逆的非齐次(non-homogeneous)CA被小心地加以构造，以使得另外一个CA(上面那个CA的逆)可以通过解复杂的方程组来得到，该特点被用来设计加解密不对称的公钥密码系统。在文献[47, 48]中触发(toggle)CA被反向迭代(就象文献[59, 60]中的混沌密码一样)来使明文得到加密，解密通过正向迭代恢复明文。该密码的设计者也建议了使用Logistic映射替代CA的加密方案。关于上述CA密码的一个较为详细的比较和分析可以在专利文献[48]中找到。

自1994年以来，P. P. Chaudhuri等人先后提出了几种不同的CA密码[49, 53, 54]。文献[49]中的CA密码已经知道是不安全的，因为它不能改变密钥并且该密码产生一个纺射群(*affine group*)的子群，而不是一个交换群(*alternating group*)[50]。在文献[53]中，另外一种CA密码被提出，不过它还是落入了纺射群的限制因此仍然不能达到预期的安全性。在文献[54](2002年底)中，P. P. Chaudhuri等人再次提出了一类新的基于CA的密码，并且用硬件实现了一个实际系统。他们通过理论分析和实验声称该密码比DES性能好得多，而可以与AES相媲美，而其加密解密吞吐量则较DES和AES都大。该密码太新，还需要更多的研究以支持原作者对其性能的分析。

§2.4.5 混沌公钥密码

在§2.1中我们已经提到，根据我们收集的资料，到目前为止只有四种混沌公钥密码系统被报道过。其中的两种混沌公钥密码[45, 46]是基于胞元自动机的，在前面一小节我们已经做了简单介绍。这两种公钥密码的安全性尚待考察，到目前尚未有相关的密码分析报道。因此，本节我们将着重介绍文献[42, 69]中提出的另外两类混沌公钥密码。

Fengi Hwu在他的博士论文[69]第VI章中提出了一类混沌公钥密码，该密码是ElGamal公钥方案[143, 144]的一个变形，它的大致工作原理如下：每个用户选择并公开一组参数(a_0, a_n, α)作为其公开密钥并选择一个整数n作为秘密密钥，这里α在$\{1, \cdots, p-1\}$上均匀分布，a_n迭代下述数字化混沌映射n次(以a_0为初始值)得到：$F(x) = \alpha x \bmod p$或者$F(x) = x^2 \bmod p$(或者其他更复杂的数字化混沌映射，如$F(x) = x^r + d \bmod p$)。整数p是一个大素数(200个比特左右)并且使得$p-1$有一个大的素因子、α是p的一个生成元。在上述条件下，加密和解密过程可以用如下步骤加以描述：

- **发送方的加密过程**：发送方随机生成一个秘密的正整数k，然后以a_0为初始条件迭代混沌系统k次得到a_k，并且以a_n为初始条件迭代k次得到a_{n+k}；
- **信道上传输的密文**：传输的密文由下面两个部分构成：$c_1 = a_k$，$c_2 = m \times a_{n+k} \bmod p$；
- **接受方的解密**：发送方以$c_1 = a_k$为初始条件迭代混沌系统n次得到$s = a_{n+k}$，然后几个通过下式得到明文：$m = (c_2/s) \bmod p$。

很明显，上述公钥密码几乎和ElGamal方案完全一样，除了采用了不同的单向函数。尽管Fengi Hwu声称该方案的安全性和ElGamal方案相同，它的实际可行性似乎有点问题。对每次通信过程而言，发送方必须迭代混沌系统$2k$次，而合法的接受方必须迭代n次。但是，由于一般来说k和n不可能非常大，否则加密和解密速度会变得过慢而无法在实际中使用。另外，如果一个攻击者从a_0开始迭代混沌系统，一旦他得到a_n也就意味着秘密密钥n被破解，这里所需要的运算复杂度只有n次混沌迭代，这和合法的接受方解密的速度一样快！以上分析表明，如果n太大，那么该密码系统会变得不实用；如果n太小，那么该密码系统就一点都不安全。事实上，上述问题的本质原因是：对于一般的(数字化)混沌系统不存在多次迭代的有效简化算法，这不像公钥密码学中常用的幂函数$x^\alpha \bmod p$，使用加法链(*addition chaining*)技术可以将正向迭代的运算复杂度急剧降低[143, 169]。

另外一种基于混沌的公钥系统最近(2003年)在文献[42]中提出的。该公钥方案被称为分布式动力学加密(DDE, distributed dynamical encryption)。该类公钥密码系统按照下述方式工作：将一个$D_T + D_R$维的动力学系统分割为一个包含D_T系统变量的发送方子(公开)系统和包含D_R个系统变量的接收方(秘密)子系统。发送方传送一个嵌入了明文信号$m(n)$的标量信号$s_t(n)$给接收方，接收方则反送另外一个标量信号$s_r(n)$给发送方。给定整个动力学系统的两个不同的吸引子，每个明文

比特$m(n)$通过判断系统在L次混沌迭代后收敛到哪个吸引子来得到。这种DDE系统的性能通过一个偶合映射网格得到了演示。在该混沌公钥密钥系统中，对每个比特而言上述的吸引子的位置需要经常改变以抵抗明文攻击，但是这种吸引子的改变可能极大地加大接收方的运算负担。当信道中存在噪声的情况下，文献[42]的作者分析了如何抵抗一类基于隐Markov模式(HMM，Hidden Markov Model)的攻击，指出较大的噪声可能导致安全性的降低。尽管在该混沌公钥方案中可能发现更多的安全性问题，但是本文作者还是相信这类混沌公钥密码系统可能开启了一个公钥密码学的新方向。

§2.4.6 混沌图象加密方法

有不少数字化混沌密码专门为图象加密的目的而进行了特殊设计[18, 85, 89, 132–138]。在文献[18, 85, 89, 136]中提出的混沌图象加密算法已经在§2.3.2“典型的混沌分组密码”一节做过了介绍。我们所知的其他所有混沌图象加密方法[132–135, 137, 138]都是由J.-C. Yen和J.-I. Guo(等人)提出的。Yen-Guo混沌图象加密方法基本上都是遵循下述思路设计的：一个混沌系统用来生成伪随机序列，该序列用来控制像素的伪随机秘密置换或者替换。从严格的密码学意义上讲，所有的Yen-Guo图象加密方案似乎都不够安全，因为它们都不能从本质上抗击已知/选择明文攻击，部分加密方法抗击已知/选择明文攻击的能力相当弱，只需要一个明文/密文图象对即可破解出等效密钥。对于其中两类混沌图象加密方法的详细分析在我们的文章[139, 140]中给出。本文的第7章详细地介绍了我们在上述两个文献中的结论。

§2.5 数字化混沌的动力学特性退化

对于数字化混沌密码而言，鉴于使用的混沌系统都是在有限精度下实现的，我们有理由怀疑它们是否还能在连续系统中保持良好的动力学特性：在经典混沌理论中，所有的动力学系统都是定义在连续域上的，它们的动力学特性往往只在具有正的Lebesgue测度的连续相空间中才有意义。在本小节中，我们将讨论下面几个和数字化混沌有关的问题：在连续混沌变为数字化混沌的过程中会发生什么本质变化？连续混沌系统的动力学特性在数字空间中是否仍然保持？混沌的数字化对数字化混沌密码的性能有什么影响？尽管在数字化混沌密码设计领域仅有不多的研究者考虑过上述问题及其解决方法[80, 170, 171]，我们认为关于数字化混沌的讨论对于保证数字化混沌密码的理论安全性是**非常**重要的。事实上，对数字化混沌系统动力学特性分析的忽视是一些数字化混沌密码不安全的本质原因[67, 141]，也是为什么大部分纯粹密码学家不太相信数字化混沌密码安全性的一个主要原因[144, §3.6]。

当我们在数字电路或者计算机中模拟混沌时，相应的动力学系统会在时间和空间两个方向上被离散化，也就是说，它们会成为定义在有限精度离散时间和

空间网格上的离散时间离散变量的混沌系统(*discrete-time and discrete-value chaotic systems*)[102]。一种理解这种离散化混沌系统的自然思路是把它们考虑为被迭代过程中的量化(四舍五入、截尾或者进位)噪声扰动的ϵ-离散化混沌系统[172]，这里ϵ代表离散网格中邻域单元之间的最大距离。在本文中，我们只考虑在二进制数字化空间中的离散化混沌系统(即在2^{-L}-离散化空间中的混沌系统，这里L是数字算法的有限精度)，并称这样的离散化混沌系统为数字化混沌系统(*digital chaotic systems*)。在本文中，数字化混沌有时也被称为拟混沌(*pseudo chaos*)[145]，被量化噪声扰动的混沌轨道被称为拟混沌轨道(*pseudo chaotic orbits*)[173]以强调它们与连续混沌和混沌轨道的本质不同。

§2.5.1 理论问题：数字化混沌系统的动力学特性退化

当我们在数字化密码中使用混沌的时候，很多研究者发现数字化混沌系统存在动力学特性退化，这种退化对数字化混沌密码的安全有不可忽视的影响[61, 67, 80, 81, 109, 141, 170, 171]。实际上，由于在数字计算机和数值仿真试验中发现了很多有关数字化混沌的奇怪现象，在混沌理论界有关数字化混沌的病态现象被广泛地报道和研究[109, 145, 171–205]。为描述这些病态现象(本文称之为动力学特性退化)是如何发生的，假设混沌在2^{-L}-离散化的数字化空间中实现，我们来分别考虑下面的几个有关数字化混沌的事实。

不可捉摸的量化误差(噪声)

在每次数字化混沌迭代中不可避免地要引入量化误差，这种量化误差会使得拟混沌轨道以一种非常复杂而不可控(不可预测)的方式偏离连续系统下的实际混沌轨道。由于混沌系统对初始条件(以及控制参数)的敏感性，有限精度下的拟混沌轨道在经过有限的几次迭代*之后就会变得与真实轨道完全不同。在文献[190]中给出了一个很好的关于这种量化效应的演示：对一个逐段线性混沌系统，当系统分别以单精度浮点运算和双精度浮点运算实现的情况下，得到的拟混沌轨道在拓扑结构上完全不同，而且两个轨道都和理论计算得到的精确轨道完全不同(参看文献[190]中的Fig. 5至Fig. 7)。另外一个关于数字化算法(浮点运算)和数字化动力学系统之间关系的工作在文献[188]中报道，该文献中的分析显示甚至一点点看起来无关紧要的数字化算法上的小修改都会彻底改变拟混沌轨道的结构。

尽管在给定有限计算精度和给定算法的情况下，所有的量化误差都完全是确定性的，但是精确知道(观测、存储)并处理这种在数字化迭代中发生的量化噪声在技术上几乎是不可能的。这使得量化噪声本身也象是一种“量化混沌”，既然量化函数本身也是限制在有限空间内的强非线性函数†。一些随机扰动模型已经被提出以描述数字化混沌系统中的量化噪声[23, 172, 194]，但是它们并不能准确地估计

*迭代的具体次数可以通过Lyapunov指数或者Kolmogorov熵进行大致的估算。

†当然，“量化混沌”这个词本身并不是那么正式，我们只是可以概念化地把它看作是连续混沌的一个合理的近似推广。不过，考虑到目前尚没有一个真正意义上严格的关于混沌的定义[17]，“量化混沌”在某种意义上看也可能是严格的。

某些数字化混沌系统的动力学行为，因而受到了一些研究者的批评(一些反例在文献[186]中被给出，如$p = 0.5$时的tent映射：$F(x) = 1 - 2|x - 0.5|$)。

既然量化噪声除了“量化混沌”的存在之外不能告诉我们关于混沌系统更多有意义的东西，我们不妨把注意力转移到拟混沌轨道的长期动力学行为上去，已经有大量的研究发现了一些颇为有用的结果。

长期动力学：不可抗拒的周期性

既然数字化混沌迭代是限制在一个包含2^L元素的离散空间中，很显然每条拟混沌轨道最后都不可避免会变成周期性的[206]，也就是说，最终总要进入一个循环而该循环的周期必然不大于2^L。

在图2.1中，我们给出了一个典型的拟混沌轨道的示意图。一般来说，每条拟混沌轨道包括两个连通的部分：$x_0, x_1, \cdots, x_{l-1}$和$x_l, x_{l+1}, \cdots, x_{l+n}$，在本文中它们分别被称为*暂态分枝*(*transient branch*)和*循环*(*cycle*)。对应地，l和$n+1$分别被称为*暂态(分枝)长度*(*transient length*)和*循环周期*(*cycle period*)，$l+n$称为*轨道长度*(*orbit length*)(请注意其他研究者可能使用不同的术语)。

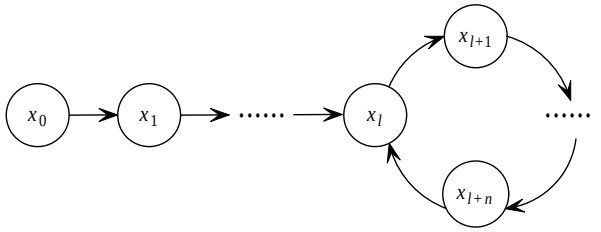


图 2.1: 一个数字化混沌系统的一条典型的拟混沌轨道

从概念上讲，对同一个数字化混沌系统而言，所有的拟混沌轨道最后都进入到少量的几个有限循环中去，这也就意味着数字化混沌系统的离散相空间收缩到一个小于2^L的离散吸引子上去。显然，数字化相空间的这种塌缩必将破坏连续混沌系统的遍历性。举一个简单的例子，当tent映射$F(x, p)$(2.3)在4比特有限精度下以四舍五入量化算法实现时，取$p = 3/2^4$，我们可以计算出所有的拟混沌轨道并得到如图2.2所示的拟混沌轨道示意图。可以看到，所有的拟混沌轨道最后都收缩到0、9这两个不动点和$\cdots \to 5 \to 14 \to 2 \to 11 \to 6 \to 12 \to \cdots$这个有限循环上去。

我们希望知道下面这些问题的答案：如何估计暂态长度和循环周期的最大值/平均值以及有限循环的个数？这些参数是否足够大以使得对连续混沌系统动力学特性的模拟是有意义的？

由于在有关混沌的研究中数值模拟有着非常重要的作用，自从混沌理论确立以来，有大量的研究试图对上面的问题给出一个可行的答案[145, 173, 174, 176, 178, 179, 183–186, 191, 192, 196, 201, 204]。不过，正如B. V. Chirkikov和F. Vivaldi在文献[145]中提到的，由于缺乏关于离散(数字化)混沌系统的遍历性理

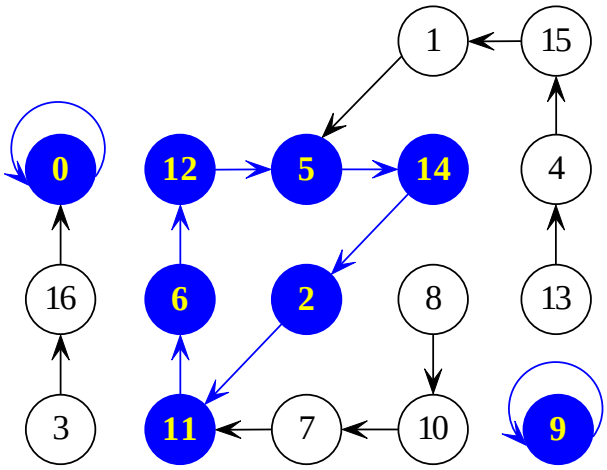


图 2.2: 数字化tent映射$F(x,p)$的拟混沌轨道示意图，$p=3/2^4$，实现精度为4比特，量化算法为四舍五入。标有数字i的节点表示二进制小数$x=i/2^4$。

论，对相关参数的严格估计(尤其是平均长度)非常之难。既然理论分析过于困难，统计试验的办法(Monte Carlo法)被广泛采用以探索这些问题的可能答案*。同时，关于随机映射[169]的理论分析也被用来作为估计数字化混沌系统参数的一个合理参照[173, 174, 198, 203, 204]。在F. Rannou[174]和Y. E. Levy[173]的早期工作的推动下，关于拟混沌轨道度量方面的一个重要发现被勾勒出来并在不同的混沌系统中得到反复确认，这个重要发现就是标度律(scaling law)，它实际上也暗示着拟混沌轨道的分形特征†。简单地讲，令$\epsilon=2^{-L}$，标度律揭示了如下有关事实：

- 暂态长度以及循环周期的最大值和平均值全部服从指数规律$O(\epsilon^{-d})$，这里d是一个由(连续)混沌系统方程唯一确定的正的指标量。一般来说$\epsilon^{-d}\ll 2^L$(对一一的Hamilton映射，$\epsilon^{-d}\ll 2^L$可能不满足[174, 176])。
- 有限循环的数量满足量级$O(\ln\epsilon^{-1})=O(L)$。
- 不同的循环周期的出现频率随着循环周期的增加而按指数衰减[184, 185]，这意味着存在大量的具有短循环周期的拟混沌轨道。

当然了，应当注意上述结论只是在一般意义下成立，某些特殊的数字化混沌还是不满足这个规律。比如，对于两种典型的混沌映射$F(x)=1-2|x-0.5|$(tent映射)和$F(x)=2x \bmod 1$(Bernoulli移位映射)，标度律给出的有关暂态长度和循环周期的估计值是没有任何意义的，这是因为这两种映射在二进制数字空间中产生的拟混沌轨道的暂态长度不会大于有限精度L，而且最终所有的拟混沌轨

*一些比较特殊的方法也被发展起来以简化分析，如文献[177]中提出的基于树状结构的分析法，和文献[182, 187, 189, 197, 200, 205]中使用的基于数论或者代数结构的相关工具。到现在为止，这些工具的使用和导出的结论还局限在少数具有特殊结构的混沌系统中，如p-adic映射和两维Hamilton映射。

†在文献[185]中，这种标度律和相关混沌系统的吸引子的分形维数被直接关联在一起。

道最终总会收敛到周期为1的循环(即固定点)上去：$\forall i \geq N, F^i(x) \equiv 0$。这说明，我们在实际应用中使用上述标度律时还是需要格外小心，以避免降低系统的实际性能。

影子周期轨道的零测度问题

D. V. Anosov和R. Bowen发展起来的β-影子引理经常被用来证明连续混沌系统数值模拟的有效性。影子引理保证在拟混沌轨道的旁边总有一条真正的混沌轨道以足够小的误差伴随[175, 207]。但是，该引理对于数字化混沌的意义很小，因为影子轨道即使存在也必然是周期的，而周期轨道在连续混沌系统中的测度一般是零。显然，这些影子轨道的零测度实际上是由于离散空间在连续空间中的零测度造成的。另外，相空间的离散化也会导致不稳定的混沌轨道变成稳定的，而这些不稳定的混沌轨道显然不能正确反映混沌系统的真正动力学特性。β-影子引理在处理数字化混沌映射方面的无效问题在文献[180, 181]中也有相关讨论.

关于这个问题的极端例子，我们还是来看看前面反复提到的定义在单位区间[0,1]上的混沌映射$F(x) = 1 - 2|x - 0.5|$和$F(x) = 2x \bmod 1$。对于这两种典型的混沌映射，在迭代过程中没有引入任何量化误差，因此每条拟混沌轨道都成为相应连续混沌系统的真实轨道。但是，对于所有的精度$n \leq N$的二进制小数，拟混沌轨道会在最多n次迭代之后收敛到0。作为比较，对于具有无限有效位数的任意实小数(这样的小数在区间[0,1]上是稠密的，具有与整个单位区间相同的Lebesgue测度)，拟混沌轨道的长度为无穷，而混沌系统的真正动力学特性正是由这样的无限小数体现的。

退化的动力学特征：遍历性，不变测度(分布)，Lyapunov指数，还有更多？

正如我们在前面提到的，所有的拟混沌轨道最终都是周期的，而且它们的循环周期可能相当得短(尽管具有很长周期的拟混沌轨道也可能是存在的[186])，所有的影子轨道在连续域上测度为0。以上事实都暗示着连续混沌在数字化空间上的塌缩，也就是说，很多动力学特性存在丧失的危险，如遍历性、不变测度和正的Lyapunov指数。为了研究数字化混沌系统中可能存在的这种危险，从理论和试验两个不同的角度已有不少的工作展开[171, 174, 175, 179, 184, 186, 194, 196, 203]。尽管已有一些正面的结果报道，我们注意到这些结论往往只是在平均(统计)[171]或者试验的意义上成立。

另外，数字化混沌还存在一些其他的病态行为，M. Blank在文献[172, 195]中从理论的角度对其中的一部分做了较为细致的分析。我们相信关于数字化混沌一定还有更多细致而古怪的现象尚待发现。尽管已有大量的研究在这个领域展开，至今尚没有一个成形的系统理论供准确分析数字化混沌系统的动力学之用*。尽本文作者所知，目前最全面最详细的关于数字化混沌的讨论在M. Blank的书

*最近，在文献[202]中，一个使用汉明(Hamming)距离替代欧氏(Euclidean)距离的数字化混沌模型被提出，一些数字化混沌在该模型上被研究。

《关于混沌动力学中离散化和连续性的一些问题》(*Discreteness and Continuity in Problems of Chaotic Dynamics*)[172]中给出，不过这本书稍微有点老，而且内容并不太全面。

§2.5.2 现实问题：如何在实际应用中克服数字化混沌的动力学退化？

当我们在数字化应用中使用混沌的时候，一个很重要的问题是如何避免数字化混沌系统的动力学特性退化以使得设计的数字系统的实际性能不会降低得太多。

首先，我们来讨论如何在数字计算机上实现混沌系统。一般而言，有两种不同的实现途径。在第一种途径中，连续混沌系统的系统方程不被改变，每一次混沌迭代的近似值通过一定的数字化算法(定点，浮点甚至其他更为复杂的算法)来得到。这种方法是一种在数字化世界中实现混沌系统的一般正规途径。在第二种途径中，原始的连续混沌系统的系统方程通过“无害”*的小修改推广到相应的数字化离散空间中去以使得构造的数字化系统与连续系统具有“等效”的动力学特性。在大多数应用中，数字化混沌系统是使用第一种方法构造的，以第二种方法构造的大多数数字化混沌系统[18, 89, 105, 107, 108, 117, 136]一般是用来简化动力学特性分析和/或提高数字化系统整体性能的。在实际应用中使用第二种方案时，设计者必须格外小心以防止看起来“无害”的修正可能带来的有害缺陷。

接下来我们来讨论数字化混沌系统在实际应用中的真正难题：如何修正数字化混沌系统才能有效地克服动力学特性退化？正如我们在前文已经探讨过的，目前在理论层面还没有一个可用的这方面的系统框架。幸运的是，下面几种可能的补救错误已经在实践中被提出以解决这个难题：使用更高的有限精度[56, 61]，级联多个数字化混沌系统[149]，以及对数字化混沌系统的(伪)随机扰动[80, 81, 99, 170, 190, 195, 199, 203]。所有的解决办法都主要是在工程领域讨论并使用的，其中基于扰动的办法得到较多的研究。我们关于逐段线性混沌映射(PWLCM)的细致分析表明(参看§3.4.1)：基于扰动策略在性能上比其他两种要好，因此我们强烈推荐在数字化混沌密码中使用这个方法解决数字化混沌系统动力学特性退化的问题(我们的几乎所有文章都采用了这个方法[22, 109, 110, 112])。尽管扰动策略的提出者们显然不知道这种策略是否具有合理的理论支撑，它确实得到了来自混沌理论领域的支持[190, 195, 203]。事实上，正如我们在前文提到的，量化噪声的随机扰动模型在理论界已被广泛采用以研究数字化混沌系统的动力学特性。工程中使用的扰动策略在理论界只是随机扰动模型的一个必然的副产品。粗略地讲，扰动策略可以成功地改善数字化混沌的动力学特性退化以满足不同应用的不同需求，这里面当然也包含数字化混沌密码。

不过，由于实现细节的差异，存在几种不同的扰动实现方案[80, 81, 99, 170, 199]，并不是所有的扰动方案都具有相同的性能。到目前为止有三种典型的扰动方案：扰动混沌系统变量(混沌轨道)，扰动控制参数，同时扰动系统变量和控制参

*请注意，由于数字化混沌系统分析上的复杂性，实际上一般很难做到真正的“无害”。这里，我们简单地套用这个词而不过多地涉及它的严格含义。

数[199]。对于逐段线性混沌映射，我们将指出：扰动系统变量的方案比扰动控制参数的方案可以提供更好的实际效果(更多细节请参考§3.4.1)。我们也建议使用混合的方案以增强一类混沌流密码的安全性(参看§4.6.6)。

一般而言，扰动的基本策略可以描述如下；运行一个在相应的离散空间(即数字化混沌系统的定义区间)上满足均匀分布的简单伪随机数(PRNG)发生器，产生一个伪随机的小扰动信号$pt(n)$，它以异或或者其他扰动函数叠加(扰动)到当前的混沌轨道上去，这种叠加每隔$\Delta \geq 1$次混沌迭代执行一次。由文献[80, 170]，已经知道扰动后的混沌轨道的长度T'将被扰动信号的周期T所控制：$T' = \sigma \cdot \Delta \cdot T$，这里$\sigma$是一个正整数。如果扰动PRNG产生的伪随机信号的周期为最大长度2^L(假设该PRNG以相同的精度实现)，则扰动混沌轨道的长度将成为$\sigma \cdot \Delta \cdot 2^L$，这个长度已经超过离散空间的大小$2^L$，在绝大多数实际应用中应该都可以满足需求了。

§2.6 如何构造一个好的数字化混沌密码：更多问题

除了数字化混沌的动力学特性退化以外，对于数字化混沌密码而言，还有一些其他的问题需要仔细考虑以避免可能的缺陷和提高设计密码的整体性能。可能的缺陷包括：使用单个混沌系统带来的潜在不安全因素，过慢的加解密速度，过于复杂的系统实现(过高的实现成本)，等等。对于大多数在2000年以后出现的数字化混沌而言，这些问题都没有得到应有的重视。尽管最近一些问题被部分研究者注意到并采用了一些实际办法来解决这些问题[56, 61, 80–82, 92, 98, 101–103, 107, 117, 170, 171]，目前还缺乏一个关于这些问题和解决方案的较为完整系统的讨论。在这节里面，本文将试图讨论一些比较典型的问题，并结合理论和实践给出一些可行的建议。

§2.6.1 如何选择混沌系统？

当我们开始着手设计数字化混沌密码的时候，第一个需要面对的问题就是：选择什么样的混沌系统才合适？这里我们通过把这个问题分解成几个子问题来阐述我们的观点。当然了，正如我们在上一节提到的，我们假定选定的混沌系统会以适当的方法(比如扰动策略)克服动力学特性退化的问题。

设计“万用”混沌密码还是“专用”密码？

如果一个数字化混沌密码可以在很多不同的混沌系统上工作良好，这将是一个非常棒的性能，我们姑且称之为“万用”(*chaotic-system-free*)*混沌密码。不过，下面几个原因使得设计“万用”混沌密码变得不太可行和不必要(关于第一个原因的部分证据参看[17])：

*在§8.3.4中，我们将讨论一种狭义的“万用性”，为了与这里的广义概念区分，狭义的“万用性”我们称为“混沌系统的自由选择性”。

1. 尽管目前混沌理论已经发展得相当丰富，但是还不存在一个统一的关于“混沌”的定义。对于几种不同的“混沌”定义的深入研究发现，没有哪一个定义可以同时覆盖所有广为承认的混沌系统。
2. 如果超过一个以上的混沌系统动力学特性被采用的话，不同的动力学特性之间的独立性将导致“万用性”的意义变得暧昧。
3. 一般来说不同的混沌系统具有不同的动力学特性(比如不同的不变分布)，这使得“万用性”的设计变得困难。
4. 许多简单而典型的混沌系统可以在大多数实际应用中很容易地实现(比如逐段线性混沌映射)，因此对“万用性”的需求在实际应用中并不那么重要。

以上讨论暗示数字化混沌应基于特定的混沌系统而进行设计，这实际上也是我们关于这个问题的观点。当然，这里“特定”一词并不意味着混沌系统本身，而是指混沌系统的动力学特性。

选择什么混沌系统？

在数字化混沌密码中选择混沌系统时，有两个主要的问题需要考虑：1) 选择的(数字化)混沌系统的动力学特性是否可以保证设计的密码系统的安全性；2) 选择的混沌系统的实现是否足够简单以提高加解密速度和节省实现成本。第二个问题意味着混沌系统越简单，相应的混沌密码的整体性能越好。关于第二个问题的更多讨论在后面还会提到，这里我们集中讨论第一个问题。第一个问题实际上包含两个侧面：选择的混沌系统的动力学特性是否适合相应混沌密码的需求；选择的混沌系统的这种动力学特性对于不同的控制参数而言是否足够稳定。比如，如果一个数字化混沌密码依赖于遍历性，那么选择的混沌系统应当对于所有的控制参数而言都是遍历的。

回忆一下我们在 §2.2 到 §2.4 中给出的数字化混沌密码的综述，可以知道很多具有明确的混沌特性和简单的系统方程的混沌系统被使用：逐段线性混沌映射[22, 59, 60, 71, 74–78, 80–82, 90, 96, 98, 106, 107, 110, 112, 116–118, 120]，Logistic映射[48, 66, 71, 79, 84, 99, 104, 105, 108, 113–115, 119, 122–125, 132, 134, 135, 137, 138]以及它的变形[55]，胞元自动机[44–54]，两维Baker映射[18, 89, 136]，两维Hénon映射[64, 95]，混沌神经网络[87, 94, 133]，耦合映射网格/网络[42, 106, 115, 119, 124]，逐段非线性混沌映射[79, 92]，拟混沌数字滤波器[70]，等等。毫不奇怪，最常用的混沌系统是两类在混沌理论中研究得最多的系统：Logistic映射$F(x) = rx(1-x)$和逐段线性混沌映射(如tent映射)。

Logistic映射的广为使用显然是由于它是最有名的展现复杂动力学行为的混沌系统[14, 15, 208]，而且它也是最简单的混沌系统之一。不过在密码学中使用Logistic映射有下面几个缺点：1) 它的不变分布是不均匀的，因此产生的混沌轨道可能不能保证混沌密码要求的平衡特性；2) 当且仅当$r = 4$时，该映射才是一个单位区间[0,1]上的满射并具有足够强的混沌特性；当控制参数r不同

时，Logistic映射的动力学特性是不一样的，该特点可能被攻击者使用以降低攻击复杂度[97]。因此，为了保证数字化混沌密码的高安全性，我们不建议使用Logistic映射。

逐段线性混沌映射(PWLCM)的使用基于其下述特点[209]：1) 均匀的不变分布；2) 遍历性，混合性和确定性；3) 呈指数衰减的相关函数；4) 使用硬件和软件都可以很容易地实现(类似Logistic映射)。需要注意的是上述特点只对部分逐段线性映射是正确的。在文献[90]中，逐段线性映射(2.5)被使用，不过该映射仅当$r = 4$时才满足上述特性(完全和Logistic映射类似，实际上他们是两类拓扑共轭的混沌映射[208])。另外，即使对于严格满足上述特性的逐段线性映射，我们证明了仍然存在可度量的动力学特性退化(参考第3章)；幸运的是，使用一些实际补救措施可以弥补逐段线性映射的这个缺陷。总结起来，在仔细考虑并克服逐段线性映射的问题的情况下*，这类混沌映射是一类比较理想的候选系统，可以满足数字化混沌密码在整体性能上的要求。

另外一类数字化混沌密码的候选混沌系统是桑涛等人在文献[92]中提出的逐段非线性混沌映射。该类映射具有和逐段线性映射类似的混沌动力学特性，并且能够克服逐段线性性带来的潜在安全问题，不过这类映射中的平方根运算需要浮点算法，这不利实现快速加解密和降低系统实现成本。我们建议仅当系统实现的简单性变得不重要的时候，并且浮点运算单元可以采用的情况下，才使用这类混沌映射。

一个还是多个混沌系统？

对这个问题的答案随着不同应用的不同需求而变化。宽松一点讲，多个混沌系统的同时使用应该有利于增强安全性，并且可能有利于提高硬件实现下的加解密速度；不过在软件实现下，为了实现更高的速度，较少的混沌系统可能是有利的。一些更多的讨论在下面一个小节给出。

这里，我们来解释一下使用多个混沌系统是如何增强数字化混沌密码的安全性的。我们知道，几乎所有的数字化混沌密码在提出的时候都被声称是安全的，但是很快就发现很多系统并不像设计者们宣称的那样安全。原因往往在于下面这个事实：对于很多混沌密码而言，密文和混沌轨道之间的相关性很强，这样，使用一些从混沌轨道中提取信息的理论工具[25–29, 32, 109]，攻击者就可能从密文中得到一些关于系统变量或者控制参数的有用信息以降低攻击复杂度。因此，使用多个混沌系统代替单个混沌系统就可能增强安全性，因为多个混沌系统的混合“应当”使得上述密码分析变得更难，尤其是当这些混沌系统具有不同的初始条件(和控制参数)和/或不同的系统方程的情况下。这样一个想法已经在一些数字化混沌密码中得到了应用[22, 42, 71, 99, 106, 112, 119, 124]，部分理论和试验分析暗示两个混沌系统可能已经足够提供可接受的安全性[22]。

*另外一个有关逐段线性混沌映射的安全危险是它的逐段线性性，在混沌密码缺乏仔细的设计的情况下，这可能使得线性攻击成为可能[63]。

§2.6.2 如何获得快速的加解密速度？

很奇怪，很多研究者在设计数字化混沌密码时(完全)忽略了加解密速度问题，从而导致设计出来的混沌密码以非常慢的速度运行。一个典型的例子是M. S. Baptista在文献[84]中提出的密码，加密每个明文至少需要$N_0 = 250$次混沌迭代，这使得加解密速度变得异常得慢。但是，如果混沌密码不能提供足够高的加解密速度(即便可以提供优秀的密码学特性)，从密码学的角度看它们也会变得价值不大，因为在传统密码学中已有太多的密码方案可以同时提供高安全性和快速加解密[143, 144]。最近，一些具有快速加解密速度的数字化混沌密码已经被提出[22, 106, 112, 123]。事实上，不少以前的数字化混沌密码的运行速度也可以通过仔细设计的算法和代码优化得到提高。在本小节中，我们来看看主要是什么原因导致了过慢的加解密速度，并给出一些提高速度的基本原则。

仔细研究已经提出的数字化混沌密码，我们发现下面的几个和加解密速度相关的事实：

- 很多数字化混沌密码(比如[18, 42, 47, 48, 58–60, 66, 71, 75, 79, 82, 84, 85, 87, 89–91, 94, 96, 98, 104, 107, 110, 113–117, 120, 122, 125, 165]中的密码)采用了多次迭代加密一个明文单元，这急剧地降低了加密解密速度。由于大部分混沌流密码加密一个明文单元只需要一次混沌迭代(或相对较少的迭代次数)，因此其加解密速度比大部分混沌分组密码快得多。

- 混沌流密码的加解密速度主要由混沌迭代耗费的时间确定。这说明，混沌系统越简单，加解密速度就会越快。显然，逐段线性混沌映射是最简单的一类混沌映射，每次混沌迭代只需要一次或两次乘法(除法)和几次加减法(比较)操作。这是另外一个我们推荐逐段线性混沌映射的原因。

- 部分数字化混沌密码[84, 90, 104, 110, 113–115, 122, 125]具有时变的加解密速度，这可能使得它们不能在要求固定速率的场合下使用。

- 由于浮点算法一般比定点算法慢得多，我们建议尽可能地使用定点算法。这也就意味着我们要尽量避免使用那些以复杂的函数定义而需要浮点运算单元的混沌系统[19, 55, 72, 79, 92, 113]。

- 硬件实现中的并行处理机制使得数字化混沌密码的硬件速度大大高于软件实现。因此，数字化混沌密码的设计中包含一些并行运算在硬件实现中是有利的。比如，当耦合映射网格(或者胞元自动机)在数字化混沌密码中使用时，加解密速度可能变得异常得快[119, 124]。

§2.6.3 系统实现问题

简单的低成本的软硬件实现对于一个好的数字化密码而言是非常重要的一个问题。实际上，系统实现问题是一个密码系统在实际应用中是否能够被最终用户

接受的关键因素，既然现在有那么多的密码都可以较低的成本提供足够的安全性。

下面几个有关系统实现的事实需要在数字化混沌密码的设计中加以考虑(一些在前面已经讨论过，在这里再次提出以强调它们从实现的角度看也是非常必要的)：

- 采用的混沌系统越简单，系统实现也就越简单，实现成本也就越低。现在我们再次发现逐段线性映射可能是设计数字化混沌密码的最好选择。
- 定点算法比浮点算法好，因为后者会增加实现成本和实现复杂度(而不止是会降低加解密速度)。
- 对于支持并行运算的硬件实现而言，(耦合的或者独立)多个混沌系统有利于提高加解密速度并增加抗攻击复杂度。
- 另外一个关于数字化密码的不错的特点是使用可接受的额外成本实现可扩充的安全性和附加的功能。这样的数字化混沌密码在我们的文章[22, 112]中可以找到。

§2.7 本章小结

由于混沌系统的动力学特性可以用来实现密码系统要求的密码学特性，数字化混沌系统可能成为设计新的数字化密码的源泉。在本章中，我们对自二十世纪80年代以来(直到2003年本论文定稿之前)数字化混沌密码的研究给出了一个全面的回顾。绝大多数公开发表的数字化混沌密码都被归类讨论并做了一定的比较。本章对数字化混沌密码设计中的一些问题也做了详细讨论，并给出了一些可能的解决方案。考虑到一些新的数字化混沌具有相当不错的密码学特性，我们相信混沌密码学有助于理解混沌和安全的本质，并丰富密码学的设计素材库。

第三章 数字化分段线性混沌映射的一组可测动力学指标

§3.1 引言

我们在上一章讲到，自二十世纪80年代以来，使用数字化混沌系统构造密码系统的想法得到了广泛的研究。由§2.5中的讨论，我们已经知道数字化混沌系统具有复杂的动力学特性退化，因此关于这种动力学特性退化的理论分析在数字化混沌密码的设计中具有重要的作用。尽管关于数字化混沌系统的动力学特性退化的一些粗糙的度量已经被勾勒出来(如拟混沌轨道长度方面的一些量级上的统计学度量)，但是对于特定的数字化混沌系统而言仍然缺乏有效的理论指标对其动力学特性做确切的描述。而我们在§2.6.1中已经提到，数字化混沌密码应当为特定的混沌系统而设计，这种指标的缺乏会使得密码性能的理论分析变得困难。另外，在§2.5.2中我们提到(伪)随机的数字化扰动可以有效地改善数字化混沌系统的动力学特性退化，但是这种扰动如果不小心使用的话(伪随机扰动也是确定性的)，还是可能带来一些安全性缺陷。

在本章中，针对数字化一维逐段线性映射(PWLCM，Piecewise Linear Chaotic Map)，本文将引入一组可度量的动力学指标，它们可以定量地刻画不同控制参数下数字化PWLCM的动力学特性退化的程度。简而言之，这组动力学指标的定义如下：假设$F(\cdot)$是一个在n-比特有限精度下以定点算法实现的数字化PWLCM，给定一个在离散空间均匀分布的离散随机变量x，定义n个动力学指标如下：$P_j = P\{F(x)$的最低j个比特全部为$0\}(j = 1 \sim n)$。针对某些逐段线性混沌映射(如tent映射)，我们惊奇地发现下述“奇怪”的现象：$P_1 \sim P_n$的值由所有线性分段的斜率的*分辨率*(关于分辨率的正式定义参看§3.2.2)唯一确定，而不是它们的具体值。当我们画出这些指标相对不同斜率的图象时，出现了非常强的规则模式。深入的研究发现，对于一般的PWLCM，上述结论可以作定性的推广。

这组动力学指标可以看作是数字化PWLCM的“拟遍历性”的一种统计度量，也可以看成是数字化不变分布相对其连续版本偏离的一种可度量证据。从本质上讲，这些指标反映了PWLCM的每个线性分段上的数字化除法的塌缩，以及多个线性分段上的这种塌缩的累积效应。很自然地，这种数字化算法的塌缩进而造成数字化PWLCM动力学特性的塌缩(退化)。因而我们可以预测这类的塌缩在其他数字化混沌系统和其他数字化算法(如浮点算法)中应当也存在，更多连续混沌在数字世界中的未知现象还有待未来的探索。由于本章引入了一种从算法的角度分析数字化混沌系统的系统方法，我们希望沿着这种分析思路可能在未来得到更多的成果*。

基于本章提出的数字化PWLCM的可度量的动力学指标，我们对几种改善数

*但是，这样的研究对于使用浮点算法的数字化混沌系统将难得多。如果有一些新的理论工具用来描述有关的浮点函数的运算过程，这种分析可能会变得容易一些。

字化混沌系统动力学特性退化的不同方案做了一个定性的比较，这些方案在上一章已经提到：使用更高的有限精度，级联多个数字化混沌系统和基于扰动的策略。分析结果再次确认了随机扰动模型和相关试验得到的结果：扰动策略可能是更好的改善方案。另外，我们的比较分析揭示了另外一个关于扰动策略的事实：扰动系统变量应当比扰动控制参数具有更好的效果，这在试验中很少被注意到。除此之外，本章对这组动力学指标在混沌密码学和混沌伪随机数发生器方面的应用也做了详细讨论。分析发现这组动力学指标可以用来发现数字化混沌密码中的隐藏系统缺陷，比如周红等人的流密码[75, 76, 82]中存在的弱密钥问题，在该类混沌流密码中扰动被简单地使用以改善数字化混沌系统的动力学特性退化(更多细节参看第4章)*。关于本章提出的动力学指标的全部讨论强调了理论分析工具在数字化混沌系统应用中的重要性。

本章是我们的文章[109]的一个扩充版本。在[109]中，我们只是对一维PWLCM(2.1)严格证明了相关结论，并将有关结论推广到斜tent映射(2.3)。本章将[109]中的有关理论结果(动力学指标的精确计算方法)推广到更为一般的PWLCM上去。

本章的内容安排如下。在§3.2中我们给出了关于PWLCM的预备知识、一些预备定义、部分预备引理和推论。§3.3集中介绍本章提出的动力学指标，从数学上严格地证明了一些关于这组动力学指标计算方面的定理，并以两类典型的PWLCM(2.1)和(2.3)为例解释了这组动力学指标的具体数学意义。在§3.4中，我们比较了三种改善数字化混沌系统动力学特性退化的措施的性能，并解释了它们在密码学和伪随机数发生器中的应用。最后一节是本章小结，同时给出了关于未来研究的一些评论。

§3.2 预备知识

§3.2.1 一维逐段线性混沌映射(PWLCM)

正像其名字暗示的那样，一个逐段线性映射(PWLM，Piecewise Linear Map)就是一个由多个线性分段构成的映射(可能包含有限个断点)。一个典型的PWLM就是tent映射(2.3)。

由于并非所有的PWLM都具有混沌性态，本章将主要讨论一类具有良好的动力学特性的逐段线性混沌映射(PWLCM，piecewise linear chaotic map)，在许多数字化混沌密码[22, 59, 60, 71, 74–78, 80–82, 90, 96, 98, 106, 107, 110, 112, 116–118, 120]中使用的PWLCM都属于这类PWLCM。但是，需要注意的是本章的主要结论对于其他PWLCM也是成立的。

给定一个实数区间$X = [\alpha, \beta] \subset \mathbb{R}$，考虑下述逐段线性映射$F : X \to X$：

$$i = 1 \sim m, F(x)|C_i = F_i(x) = a_i x + b_i, \tag{3.1}$$

*实际上，正是我们对周红等人在文献[82]中提出的流密码进行的统计分析促使我们发现了这组动力学指标，并促使我们把相关结论推广到一般的PWLCM。

这里$\{C_i\}_{i=1}^m$是区间X的一个划分，它满足$\bigcup_{i=1}^m C_i = X$和$C_i \cap C_j = \varnothing, \forall i \neq j$。我们称上述映射满足*逐段映满性*(*piecewise onto* property)，如果上述映射的每个线性分段将F_i映射到X上去：$\forall i = 1 \sim m, F_i(C_i) = X$。如果$X = [0,1]$，该映射称为*归一化*(*normalized*)的一维逐段线性映射(PWLM)。显然，任何一维PWLM都可以通过简单的线性操作变换为归一化形式：

$$F_{[0,1]}(x) = \frac{F\left(\frac{x-\alpha}{\beta-\alpha}\right) - \alpha}{\beta - \alpha}. \tag{3.2}$$

很明显，原一维PWLM和其归一化映射是拓扑共轭的。

一个*逐段映满*的一维PWLM一般是混沌的并且在其定义域X上满足如下动力学特性：1) 它的Lyapunov指数$\lambda = -\sum_{i=1}^m \mu(C_i) \cdot \ln \mu(C_i)$并且满足$0 < \lambda < \ln m$，这里$\mu(C_i) = ||C_i||/(\beta - \alpha)$；2) 它是确定的，混合的和遍历的；3) 它具有均匀的不变分布函数$f(x) = 1/\|X\| = 1/(\beta - \alpha)$；4) 它的自相关函数$\tau(n) = \frac{1}{\sigma^2} \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1}(x_i - \bar{x})(x_{i+n} - \bar{x})$随着$n \to \infty$趋向于0，这里$\bar{x}, \sigma$分别表示变量$x$的均值和方差；特别的，当$\sum_{i=1}^m \text{sign}(a_i) \cdot \|C_i\|^2 = 0$满足时，$\tau(n) = \delta(n)$。性质1、3、4可以使用文献[209]中给出的类似方法推导出来，性质2的满足是由于$\forall x \in X$并且除m个线性分段交接处的接点/断点以外$|F'(x)| = |a_i| > 1$成立[23]。下面，不失一般性，我们将使用PWLCM这个缩写词表示上面这种混沌的逐段线性映射(PWLM)。

我们知道[23, 210]，均匀的不变分布函数(性质3)意味着均匀的输入将产生均匀的输出，以及从几乎所有的初始条件出发的混沌轨道会趋向于相同的均匀分布$f(x) = 1/(\beta - \alpha)$。但是，这个结论对于数字化混沌映射并不再成立。假设一个一维PWLCM在包含2^n个有限状态的离散空间中实现(即系统实现精度为n比特)。取2^n不同的离散状态作为该混沌映射的输入，由于一维PWLCM是多对一的映射，经过一次混沌迭代之后不同的输出状态的数目将比2^n小。也就是说，对于一个数字化一维PWLCM而言，**离散均匀分布的输入不能产生离散均匀分布的输出**，或者说**一个离散均匀分布的随机变量经过数字化混沌迭代之后将变得不再满足离散均匀分布**。在本章中，我们将试图探讨这样一个问题：我们能否准确地度量一个数字化PWLCM对离散均匀输入的混沌输出的不均匀性？考虑任何一维PWLCM都和它的归一化映射拓扑共轭，我们将只讨论归一化PWLCM以简化问题的讨论和相应的理论分析。

为了方便后面的叙述以及相关理论结论的证明，我们将介绍一些预备定义和有用的预备结论。在§3.2.2中，我们给出一些基本定义(定义1、2、3)以描述n-比特有限精度下单位区间$X = [0,1]$的离散空间，以及在该离散空间上的数字化算法操作的定义(定义4、5)。在§3.2.3中，我们给出了一些与§3.2.2中引入的定义相关的预备结论。

§3.2.2 预备定义

定义 3.1: 一个离散集合$S_n = \{a|a = \sum_{i=1}^{n} a_i \cdot 2^{-i}, a_i \in \{0,1\}\}$称为一个***分辨率(resolution)***为n的***数字集(digital set)***。$\forall i < j$, S_i称为S_j的***分辨率(resolution)***为i的***数字子集(digital subset)***。特别的，定义$S_0 = \{0\}, S_\infty = [0,1]$。

我们有$\{0\} = S_0 \subset S_1 \subset \cdots \subset S_i \subset \cdots \subset S_\infty = [0,1]$。

定义 3.2: 定义$V_i = S_i - S_{i-1} (i \geq 1)$以及$V_0 = S_0$。$V_i$称为一个***分辨率(resolution)***为i的***数字层次(digital layer)***。$\forall p \in V_i$，i称为p的***分辨率(resolution)***。S_n的划分$\{V_i\}_{i=0}^{n}$称为S_n的***完全多分辨率分解(complete multi-resolution decomposition)***；$\{V_i\}_{i=0}^{\infty}$称为$S_\infty = [0,1]$的***完全多分辨率分解***。对于S_n，它的分辨率n也称为***分解级数(decomposition level)***。

我们有$\bigcup_{i=0}^{n} V_i = S_n$, $V_i \cap V_j = \varnothing (\forall i \neq j)$以及$\|V_i\| = 2^{i-1} (\forall i \geq 1)$，这里$\|V_i\|$表示$V_i$的大小。一个二进制小数$p \in V_i$的分辨率实际上代表它的二进制表示形式重最后一个非零比特的位置，即$p = 0.b_1 b_2 \cdots b_i \overbrace{0 \cdots 0}^{n-i} (b_i \neq 0)$。也可以说，**$p$的分辨率实际上就是$p$的二进制有限精度**。

定义 3.3: $\forall n > m$，$D_{n,m} = S_n - S_m$称为S_n和S_m的***数字差集***或者参数为n和m的***数字差集(digital difference set)***。当$m = 0$时，$D_{n,0}$可以简写为D_n。$\{V_i\}_{i=m}^{n}$称为$D_{n,m}$的***完全多分辨率分解***，$n - m$称为$D_{n,m}$的***分解级数***。

定义 3.4: 一个函数$G : \mathbb{R} \to \mathbb{Z}$称为一个***近似转换函数(ATF，approximate transformation function)***，如果$\forall x \in \mathbb{R}$，$|G(x) - x| < 1$。有三种基本的*ATF*: *1)* $\lfloor \boldsymbol{x} \rfloor$ **–** ***floor***函数*(截尾)*，不大于x的最大整数；*2)* $\lceil \boldsymbol{x} \rceil$ **–** ***ceil***函数*(进位)*，不小于x的最小整数；*3)* $\mathbf{round}(\boldsymbol{x})$ **–** ***roundoff***函数*(四舍五入)*，最接近x的整数。$\forall x \in \mathbb{R}$，定义它的***小数部分(decimal part)***为$\mathbf{dec}(\boldsymbol{x}) = x - \lfloor x \rfloor$。

上述**三种**ATF(注意**不是所有**的ATF)具有下述的有用性质，这些性质的证明非常简单我们在这里忽略它们。

ATF性质1：$\forall m \in \mathbb{Z}, G(x+m) = G(x) + m$;

ATF性质2：$a < x < b \Rightarrow \lfloor x \rfloor \leq G(x) \leq \lceil x \rceil$。

定义 3.5: 一个函数$G_n : S_\infty \to S_n$称为一个***分辨率(resolution)***为n的***数字化近似转换函数(DATF，digital approximate transformation function)****，如果$\forall x \in S_\infty = [0,1]$，$|G_n(x) - x| < 1/2^n$。在本文中将只讨论下述三种*DATF*(它们也是在数字化算法中使用最为广泛的三种*DATF*): *1)* $\mathbf{floor}_{\boldsymbol{n}}(\boldsymbol{x}) = \lfloor x \cdot 2^n \rfloor / 2^n$; *2)* $\mathbf{ceil}_{\boldsymbol{n}}(\boldsymbol{x}) = \lceil x \cdot 2^n \rceil / 2^n$; *3)* $\mathbf{round}_{\boldsymbol{n}}(\boldsymbol{x}) = \mathrm{round}(x \cdot 2^n)/2^n$。

*按照M. Blank在[172, 第5章]中使用的术语，G_n被称为一个2^{-n}-离散化算子(*operator of* 2^{-n}-*discretization*)。在本文中，为了使得叙述更为简单，我们将使用DTAF这个术语。

上述**三种**DATF(与ATF类似，**不是所有**的DATF)具有下述的有用性质，这些性质可以很容易的从**ATF性质1和性质2**导出。

DATF性质1: $\forall m \in \mathbb{Z}, G_n(x + m/2^n) = G_n(x) + m/2^n$;

DATF性质2: $a < x < b \Rightarrow \text{floor}_n(a) \leq G_n(x) \leq \text{ceil}_n(b)$。

§3.2.3 预备引理和推论

对于三种基本的ATF–$\lfloor\cdot\rfloor$，$\lceil\cdot\rceil$和round$(\cdot)$，我们有下面的引理3.1和推论3.1，它们将用来简化下一节定理的证明。

引理 3.1: $\forall n \in \mathbb{Z}^+, a \geq 0$，下述事实成立:

1. $n \cdot \lfloor a \rfloor \leq \lfloor n \cdot a \rfloor \leq n \cdot \lfloor a \rfloor + (n-1)$；当且仅当$\text{dec}(a) \in \left[0, \frac{1}{n}\right)$时$n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor$;
2. $n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$；当且仅当$\text{dec}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$时$n \cdot \lceil a \rceil - (n-1) = \lceil n \cdot a \rceil$;
3. $n \cdot \text{round}(a) - \lfloor n/2 \rfloor \leq \text{round}(n \cdot a) \leq n \cdot \text{round}(a) + \lfloor n/2 \rfloor$；当且仅当$\text{dec}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$时$n \cdot \text{round}(a) - \lfloor n/2 \rfloor = \text{round}(n \cdot a)$。

证明: 我们分别证明这三个子引理如下：

1. 由于$a = \lfloor a \rfloor + \text{dec}(a)$，$n \cdot a = n \cdot \lfloor a \rfloor + n \cdot \text{dec}(a)$。考虑到$0 \leq \text{dec}(a) < 1$，我们有$0 \leq n \cdot \text{dec}(a) < n \Rightarrow 0 \leq \lfloor n \cdot \text{dec}(a) \rfloor \leq n - 1$。由$\lfloor\cdot\rfloor$的定义可知$\lfloor n \cdot a \rfloor = \lfloor n \cdot (\lfloor a \rfloor + \text{dec}(a)) \rfloor = n \cdot \lfloor a \rfloor + \lfloor n \cdot \text{dec}(a) \rfloor \Rightarrow n \cdot \lfloor a \rfloor \leq \lfloor n \cdot a \rfloor \leq n \cdot \lfloor a \rfloor + (n-1)$，这里$n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor \Leftrightarrow \lfloor n \cdot \text{dec}(a) \rfloor = 0$，也就是说，$0 \leq n \cdot \text{dec}(a) < 1 \Leftrightarrow \text{dec}(a) \in \left[0, \frac{1}{n}\right)$。

2. i) 当$\text{dec}(a) = 0$：$\lceil n \cdot a \rceil = n \cdot a = n \cdot \lceil a \rceil$；ii) 当$\text{dec}(a) \in (0,1)$：假设$\text{dec}'(a) = 1 - \text{dec}(a) \in (0,1)$，$a = \lceil a \rceil - \text{dec}'(a)$，则$n \cdot a = n \cdot \lceil a \rceil - n \cdot \text{dec}'(a)$。考虑到$0 < n \cdot \text{dec}'(a) < n$，我们有$n \cdot \lceil a \rceil - n < n \cdot a = n \cdot \lceil a \rceil - n \cdot \text{dec}'(a) < n \cdot \lceil a \rceil$。由$\lceil\cdot\rceil$的定义可知$n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$, where $n \cdot \lceil a \rceil = \lceil n \cdot a \rceil \Leftrightarrow n \cdot \text{dec}'(a) \in (0,1)$，则$\text{dec}(a) \in (1 - \frac{1}{n}, 1)$。综合以上两个方面可以得到：$n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$，当且仅当$\text{dec}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$时有$n \cdot \lceil a \rceil = \lceil n \cdot a \rceil$。

3. 由round$(\cdot)$的定义可知$\text{round}(a) - 1/2 \leq a \leq \text{round}(a) + 1/2$。因而$n \cdot \text{round}(a) - n/2 \leq n \cdot a < n \cdot \text{round}(a) + n/2$。i) 当$n$是偶整数时，显然有$n \cdot \text{round}(a) - n/2 \leq \text{round}(n \cdot a) < n \cdot \text{round}(a) + n/2$。ii) 当$n$是奇整数时，$n \cdot \text{round}(a) - n/2 + 1/2 \leq \text{round}(n \cdot a) < n \cdot \text{round}(a) + n/2 - 1/2$，也就是说，$n \cdot \text{round}(a) - (n-1)/2 \leq \text{round}(n \cdot a) < n \cdot \text{round}(a) + (n-1)/2$。综合上面两个方面可得：$n \cdot \text{round}(a) - \lfloor n/2 \rfloor \leq \text{round}(n \cdot a) \leq n \cdot \text{round}(a) + \lfloor n/2 \rfloor$，这里$n \cdot$

$\text{round}(a) = \text{round}(n \cdot a) \Leftrightarrow n \cdot \text{round}(a) - 1/2 \leq n \cdot a < n \cdot \text{round}(a) + 1/2$，即$\text{dec}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$。

证毕。 ■

推论 3.1: $\forall n \in \mathbb{Z}^+, a \geq 0$，下述事实成立：

1. 当且仅当$\text{dec}(a) \in \left[0, \frac{1}{n}\right)$时$\lfloor n \cdot a \rfloor \equiv 0 \pmod{n}$；
2. 当且仅当$\text{dec}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$时$\lceil n \cdot a \rceil \equiv 0 \pmod{n}$；
3. 当且仅当$\text{dec}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$时$\text{round}(n \cdot a) \equiv 0 \pmod{n}$。

该推论可以由引理3.1很容易地导出。

接下来我们介绍引理3.2，它给出了关于数字化除法x/p的高位$n-i$个比特和低位i个比特的一些有用结论，这里$x, p \in S_n$。

引理 3.2: $\forall p \in D_i = S_i - \{0\} (1 \leq i \leq n), x \in S_n$。假设$p = N_p/2^i, x = N_x/2^n$，这里$N_p, N_x$是满足下列条件的整数：$1 \leq N_p \leq 2^i - 1$，$0 \leq N_x \leq 2^n - 1$。我们有下列的三个结论，这里$G_0(\cdot)$表示与$G_n(\cdot)$对应的$ATF$，在后文中$G_0(\cdot)$表示同样的含义，不再赘述：

$$1. \quad G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}, \tag{3.3}$$

$$2. \quad \text{floor}_{n-i}(G_n(x/p)) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}, \tag{3.4}$$

$$3. \quad G_n(x/p) \bmod \frac{1}{2^{n-i}} = \frac{G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right)}{2^n}。 \tag{3.5}$$

证明：由于$x/p = \frac{N_x/2^n}{N_p/2^i} = \frac{N_x/N_p}{2^{n-i}} = \frac{\lfloor N_x/N_p \rfloor + (N_x \bmod N_p)/N_p}{2^{n-i}}$，我们有$G_n(x/p) = \frac{G_0(2^i \cdot \lfloor N_x/N_p \rfloor + 2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}$。由$ATF$性质1，我们可以将$G_n(x/p)$重写为如下形式：

$$G_n(x/p) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}。 \tag{3.6}$$

下面我们分以下两种不同的情况讨论上述方程：

a) 当$N_x \bmod N_p = 0$时：$G_n(x/p) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + 0 \in S_{n-i}$；

b) 当$N_x \bmod N_p = k \neq 0$时：显然$1 \leq k \leq N_p - 1$。考虑到$p < 1$，我们有$2^i/N_p > 1$，则$1 < 2^i \cdot (N_x \bmod N_p)/N_p < 2^i - 1$。因而，由$ATF$性质2，$1 \leq G_0(2^i \cdot (N_x \bmod N_p)/N_p) \leq 2^i - 1$。所以，

$$\frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{1}{2^n} \leq G_n(x,p) \leq \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{2^i - 1}{2^n} \Rightarrow G_n(x,p) \notin S_{n-i}。 \tag{3.7}$$

由a)和b)中的讨论，我们可以推出$G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}$。

同时，当$N_x \mod N_p = 0$时，$\text{floor}_{n-i}(G_n(x/p)) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$；当$N_x \mod N_p = k \neq 0$时，$\text{floor}_{n-i}(G_n(x/p)) \geq \frac{\left\lfloor \lfloor N_x/N_p \rfloor + 1/2^i \right\rfloor}{2^{n-i}} = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$并且$\text{floor}_{n-i}(G_n(x/p)) \leq \frac{\left\lfloor \lfloor N_x/N_p \rfloor + (2^i-1)/2^i \right\rfloor}{2^{n-i}} = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$，因此最后我们可以得到$\text{floor}_{n-i}(G_n(x/p)) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$。

由以上结论和方程(3.6)，下述结论成立：

$$G_n(x/p) \bmod \frac{1}{2^{n-i}} = \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}。$$

证毕。 ■

下面的引理3.3和推论3.2还是描述S_n上的数字化除法x/p的性质。和引理3.2一起，它们反映了S_n上的数字化除法x/p的一些本质特性，并在后文中有关PWLCM统计特性的证明中起着重要作用。

引理 3.3: *假设n是一个奇数，随机整数变量K在$\mathbb{Z}_n = \{0,\cdots,n-1\}$上离散均匀分布，下述结论成立：$K' = f(K) = (2^i \cdot K) \bmod n$在$\mathbb{Z}_n$上离散均匀分布，即$\forall k \in \{0,\cdots,n-1\}$，$P\{K'=k\} = 1/n$。*

证明: 我们知道，$(\mathbb{Z}_n, +)$是一个阶数为n的有限循环群，当且仅当$\gcd(a,n) = 1$时a是该群的一个生成元，这里“+”表示模加运算：$(a+b) \mod n$(参看[211]60页上的定理2)。因此，由于$\gcd(a,n) = \gcd(2^i,n) = 1$，$a = 2^i \mod n$是$\mathbb{Z}_n$的一个生成元。考虑到$K' = (2^i \cdot K) \bmod n = (a \cdot K) \bmod n$，我们可以知道$f : \mathbb{Z}_n \to \mathbb{Z}_n$是一个一一双射。于是马上可得：由于$K$在$\mathbb{Z}_n$上满足离散均匀分布，$K' = f(K)$在$\mathbb{Z}_n$上满足离散均匀分布。也就是说，$\forall k \in \{0,\cdots,n-1\}, P\{K'=k\} = 1/n$。得证。 ■

推论 3.2: *假设n是一个奇数，随机整数变量K在$\mathbb{Z}_n = \{0,\cdots,n-1\}$上离散均匀分布。则$\text{dec}(2^i \cdot K/n)$在$S = \{x | x = k/n, k \in \mathbb{Z}_n\}$上离散均匀分布。*

该推论是引理3.3的直接结果。

§3.3 数字化PWLCM的动力学指标及其准确值的计算方法

基于§3.2.2中给出的预备定义，现在让我们看看如何描述一个在n比特有限精度下实现的数字化一维(归一化)PWLCM $F(x) : I \to I$，这里$I = [0,1]$。

考虑$1 \notin S_n$以及$1 \equiv 0 \pmod 1$，为了简化讨论和证明，我们重定义$[0,1)$上(不用[0,1]以简化问题的讨论)的归一化PWLCM为如下形式：

$$F_{[0,1)}(x) = F(x) \bmod 1 = \begin{cases} F(x), 0 \le F(x) < 1 \\ 0, \quad F(x) = 1 \end{cases} 。 \tag{3.8}$$

这样一个重定义不会对本章的理论结果产生任何本质影响，原因将在下文中说明。使用$\mathcal{F}_n(x)$表示n比特有限精度下的$F_{[0,1)}$，我们有$\mathcal{F}_n = G_n \circ F_{[0,1)} : S_n \to S_n$，这里$G_n(\cdot)$是一个DATF，即$\text{floor}_n(\cdot)$、$\text{ceil}_n(\cdot)$或$\text{round}_n(\cdot)$。

§3.3.1 动力学指标

现在我们给出本章提出的动力学指标的正式定义。$\forall x = 0.b_n b_{n-1} \cdots b_2 b_1 \in S_n$，定义$P_j(x)$为最低$j$个比特$b_j \cdots b_1$全为0的概率，一个等效的定义是$P_j(x) = P\{x \in S_{n-j}\}$。本章下面所有的讨论都围绕下述$n$个动力学指标展开：

$$\forall j = 1 \sim n, P_j(\mathcal{F}_n(x)) = P\{\mathcal{F}_n(x) \in S_{n-j}\} \tag{3.9}$$

这里$\mathcal{F}_n = G_n \circ F_{[0,1)} : S_n \to S_n$是一个归一化的数字化一维PWLCM，$x$是一个在$S_n$上离散均匀分布的离散随机变量。

如果x在S_n上满足离散均匀分布，$P_j(x) = 2^{-j}$。相应地，如果$\mathcal{F}_n(x)$在S_n上满足离散均匀分布则$P_j(\mathcal{F}_n(x)) = 2^{-j}$。但是，在§3.2.1中我们已经提到由于空间离散化带来的动力学特性退化，$\mathcal{F}_n(x)$不满足离散均匀分布。也就是说，**至少**存在**一个**j，满足$P_j(\mathcal{F}_n(x)) \neq 2^{-j}$。那么我们是否可以从理论上推导$P_j(\mathcal{F}_n(x))(1 \le j \le n)$的具体值以度量这种动力学特性退化呢？在本章中我们将给出一个肯定的答案。这个答案揭示了数字化一维PWLCM的离散迭代的一些本质而重要的特性，并且触及到了数字化算法内核的一些内在的微妙性质。由于可以准确计算$P_j(\mathcal{F}_n(x))(1 \le j \le n)$的值，而已知至少一个动力学指标满足$P_j(\mathcal{F}_n(x)) \neq 2^{-j}$，$P_1(\mathcal{F}_n(x)) \sim P_n(\mathcal{F}_n(x))$就可能反映$\mathcal{F}_n(x)$在离散均匀输入信号$x$驱动的情况下的不均匀程度。这是我们为什么把这$n$个概率值称为数字化一维PWLCM的动力学指标的原因。

有了上述动力学指标的定义，我们可以来解释为什么前面对归一化PWLCM的重定义(3.8)不会影响有关$P_j(\mathcal{F}_n(x))$的结果。尽管$1 \notin S_n$，我们可以将1表示为二进制形式$1.\overbrace{0\cdots0}^{n}$。把1和$0 = 0.\overbrace{0\cdots0}^{n}$进行比较，可以看到0和1对$P_j(\mathcal{F}_n(x))(1 \le j \le n)$所做的贡献是完全相同的。因此，重定义(3.8)不会影响每个指标的具体值。

为了简化叙述和证明，在后文我们将使用简写符号P_j表示$P_j(\mathcal{F}_n(x))$。后文的内容可以分为四个部分：在§3.3.2中我们研究单个线性分段上的动力学指标$P_j(1 \le j \le n)$；然后在§3.3.3中讨论一般的数字化PWLCM的动力学指标；一维PWLCM(2.1)和(2.3)作为典型的例子在§3.3.4中做了细致的研究，以演示动力学

指标的具体数学含义；最后一个小节讨论多次复合PWLCM(也就是PWLCM的多次迭代)$\mathcal{F}_n^k(x)$的动力学指标。

§3.3.2 单个线性分段上的$P_j(1 \le j \le n)$

从本质上讲，一个数字化一维PWLCM的动力学特性是它的所有线性分段的综合结果。在这个小节中我们将着重研究如何在每个线性分段上计算$P_j(1 \le j \le n)$，这里$\mathcal{F}_n(x) = G_n(x/p), x \in C = [0,p) \cap S_n$。由于一个PWLCM的每个线性分段都可以通过线性变换简化为x/p的形式，该PWLCM的动力学指标可以通过综合所有线性分段上的$P_j(1 \le j \le n)$值得到。这里请注意，本小节给出的结论实际上适用于任何一维PWLM。

引理 3.4: 假设一个离散随机变量x在离散空间$C = [0,p) \cap S_n$上满足离散均匀分布，令$p = N_p/2^i \in D_i = S_i - \{0\}$，这里$N_p$是一个属于$\{1,\cdots,2^i-1\}$的整数。对于一个数字化线性函数$\mathcal{F}_n(x) = G_n(x/p)$而言，$\text{floor}_{n-i}(\mathcal{F}_n(x))$在$S_{n-i}$上满足离散均匀分布，也就是说，$\forall k \in \{0,\cdots,2^{n-i}-1\}$，$P\left\{\text{floor}_{n-i}(\mathcal{F}_n(x)) = k/2^{n-i}\right\} = 1/2^{n-i}$。

证明: 令$x = N_x/2^n$，由$x \in [0,p) \cap S_n$以及$p = N_p/2^i$，可以导出$0 \le N_x \le 2^{n-i} \cdot N_p - 1$。因为$x$在$C$上离散均匀分布，则$N_x$在整数集合$\{0,\cdots,2^{n-i} \cdot N_p - 1\}$上离散均匀分布。

考虑$\mathcal{F}_n(x) = G_n(x/p)$，由引理3.2中的方程(3.4)，我们有$\text{floor}_{n-i}(\mathcal{F}_n(x)) = \lfloor N_x/N_p \rfloor/2^{n-i}$。既然$N_x$在$\{0,\cdots,2^{n-i} \cdot N_p - 1\}$上离散均匀分布，则$\lfloor N_x/N_p \rfloor$在$\{0,\cdots,2^{n-i}-1\}$上满足离散均匀分布，即$\text{floor}_{n-i}(\mathcal{F}_n(x))$在$S_{n-i}$上满足离散均匀分布。得证。 ■

引理 3.5: 假设一个离散随机变量x在离散集合$C = [0,p) \cap S_n$上满足离散均匀分布，令$p = N_p/2^i \in D_i = S_i - \{0\}$，这里$N_p$是一个属于$\{1,\cdots,2^i-1\}$的整数。对于一个数字化线性函数$\mathcal{F}_n(x) = G_n(x/p)$而言，下述结论成立：$i \le j \le n$, $P_j = 1/\left(N_p \cdot 2^{j-i}\right)$。

证明: 类似引理3.4的证明，令$x = N_x/2^n$，可以知道N_x在整数集合$\{0,\cdots,2^{n-i} \cdot N_p - 1\}$上满足离散均匀分布。下面我们分别考虑两种不同的情况：

a) $j = i$：由于$\mathcal{F}_n(x) = G_n(x/p)$，由引理3.2中的方程(3.3)，可以知道当且仅当$N_x \equiv 0 \pmod{N_p}$时$\mathcal{F}_n(x) \in S_{n-i}$成立。考虑有$2^{n-i}$个整数满足$N_x \equiv 0 \pmod{N_p}$以及$N_x$在$\{0,\cdots,2^{n-i} \cdot N_p - 1\}$上满足离散均匀分布，$\mathcal{F}_n(x) \in S_{n-i}$的概率为$\dfrac{2^{n-i}}{2^{n-i} \cdot N_p} = \dfrac{1}{N_p}$。也即，$P_i = \dfrac{1}{N_p} = \dfrac{1}{N_p \cdot 2^{i-i}}$。

b) $i+1 \le j \le n$：令$\mathcal{F}_n(x) = 0.b_n b_{n-1} \cdots b_2 b_1$，$P_j = P\left\{\mathcal{F}_n(x) \in S_{n-i} \wedge b_j \cdots b_{i+1} = \overbrace{0\cdots0}^{j-i}\right\}$。回顾引理3.4的证明过程，可

以知道事件$\mathcal{F}_n(x) \in S_{n-i}$和事件$b_j \cdots b_{i+1} = \overbrace{0 \cdots 0}^{j-i}$是独立的，因此$P_j = P\{\mathcal{F}_n(x) \in S_{n-i}\} \cdot P\left\{b_j \cdots b_{i+1} = \overbrace{0 \cdots 0}^{j-i}\right\}$。由引理3.4可知，$F_n(x,p)$的高位$n-i$个比特组合的值在$\{0, \cdots, 2^{n-i}-1\}$上离散均匀分布，因此$P\left\{b_j \cdots b_{i+1} = \overbrace{0 \cdots 0}^{j-i}\right\} = \frac{1}{2^{j-i}}$。最后，我们有$P_j = P_i \cdot \frac{1}{2^{j-i}} = \frac{1}{N_p \cdot 2^{j-i}}$。

综合以上两种情况可得，$i \le j \le n$, $P_j = \frac{1}{N_p \cdot 2^{j-i}}$。证毕。 ■

引理 3.6: 假设一个离散随机变量x在离散集合$C = [0,p) \cap S_n$上满足离散均匀分布，令$p = N_p/2^i \in V_i (1 \le i \le n)$(请注意**不是**上面引理中的$\boldsymbol{D_i}$)，这里$N_p$是一个属于$\{1, \cdots, 2^i - 1\}$的奇整数。对于一个数字化线性函数$\mathcal{F}_n(x) = G_n(x/p)$而言，如下结论成立：

$$1 \le j \le i-1,\ P_j = \begin{cases} \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p}, & G_n(\cdot) = \mathrm{floor}_n(\cdot) \text{或} \mathrm{ceil}_n(\cdot) \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & G_n(\cdot) = \mathrm{round}_n(\cdot) \end{cases} 。 \tag{3.10}$$

证明：类似引理3.4的证明，令$x = N_x/2^n$，可以知道N_x在整数集合$\{0, \cdots, 2^{n-i} \cdot N_p - 1\}$上满足离散均匀分布。

因为$\mathcal{F}_n(x) = G_n(x/p)$，由引理3.2的方程(3.5)，可以知道$\mathcal{F}_n(x)$的低位$i$个比特由$G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right)$确定。可以推出$\mathcal{F}_n(x) \in S_{n-j} \Leftrightarrow G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right) \equiv 0 \pmod{2^j}$。定义$\hat{N}_x = N_x \bmod N_p$，由于$N_x$的均匀分布，$\hat{N}_x$在$\{0, \cdots, N_p - 1\}$上满足离散均匀分布。再定义$a = \frac{2^i \cdot \hat{N}_x/N_p}{2^j}$，我们可以将$G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right)$重新表示为$G_0(2^j \cdot a)$。由推论3.1我们有：

$$\begin{gathered} G_0(2^j \cdot a) \equiv 0 \pmod{2^j} \\ \Updownarrow \\ \mathrm{dec}(a) \in \begin{cases} \left[0, \frac{1}{2^j}\right), & G_0(\cdot) = \lfloor \cdot \rfloor \\ \left(1 - \frac{1}{2^j}, 1\right) \bigcup \{0\}, & G_0(\cdot) = \lceil \cdot \rceil \\ \left[0, \frac{1}{2^{j+1}}\right) \bigcup \left[1 - \frac{1}{2^{j+1}}, 1\right), & G_0(\cdot) = \mathrm{round}(\cdot) \end{cases} 。 \end{gathered} \tag{3.11}$$

由推论3.2($p \in \boldsymbol{V_i}$保证了N_p是一个**奇**整数)，可知$\mathrm{dec}(a) = \frac{k}{N_p}(k = 0 \sim N_p - 1)$在其取值集合上也是均匀分布的。根据(3.11)，我们可以推出：

$$\begin{array}{c} G_0(2^j \cdot a) \equiv 0 \pmod{2^j} \\ \Updownarrow \\ k \in \begin{cases} \left[0, \dfrac{N_p}{2^j}\right), & G_0(\cdot) = \lfloor \cdot \rfloor \\ \left(N_p - \dfrac{N_p}{2^j}, N_p\right) \bigcup \{0\}, & G_0(\cdot) = \lceil \cdot \rceil \\ \left[0, \dfrac{N_p}{2^{j+1}}\right) \bigcup \left[N_p - \dfrac{N_p}{2^{j+1}}, N_p\right), & G_0(\cdot) = \mathrm{round}(\cdot) \end{cases} \end{array} \quad (3.12)$$

考虑k是一个整数，可以进一步得到：

$$\begin{array}{c} G_0(2^j \cdot a) \equiv 0 \pmod{2^j} \\ \Updownarrow \\ k \in \mathbb{Z} \\ \text{并且} \\ k \in \begin{cases} \left[0, \left\lfloor \dfrac{N_p}{2^j} \right\rfloor\right], & G_0(\cdot) = \lfloor \cdot \rfloor \\ \{0\} \bigcup \left[N_p - \left\lfloor \dfrac{N_p}{2^j} \right\rfloor, N_p - 1\right], & G_0(\cdot) = \lceil \cdot \rceil \\ \left[0, \left\lfloor \dfrac{N_p}{2^{j+1}} \right\rfloor\right] \bigcup \left[N_p - \left\lfloor \dfrac{N_p}{2^{j+1}} \right\rfloor, N_p - 1\right], & G_0(\cdot) = \mathrm{round}(\cdot) \end{cases} \end{array} \quad (3.13)$$

由k在整数集合$\{0, \cdots, N_p - 1\}$上的均匀分布性，我们可以很容易地得到P_j的值：

$$\begin{aligned} P_j &= P\left\{\mathcal{F}_n(x) \in S_{n-j}\right\} \\ &= P\left\{G_0(2^j \cdot a) \equiv 0 \pmod{2^j}\right\} \\ &= \begin{cases} \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p}, & G_0(\cdot) = \lfloor \cdot \rfloor \text{或} \lceil \cdot \rceil \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & G_0(\cdot) = \mathrm{round}(\cdot) \end{cases} \end{aligned} \quad (3.14)$$

显然，方程(3.10)成立。证毕。 ■

定理 3.1: 假设一个离散随机变量x在离散集合$C = [0, p) \cap S_n$上满足离散均匀分布，令$p = N_p/2^i \in V_i (1 \le i \le n)$，这里$N_p$是一个属于$\{1, \cdots, 2^i - 1\}$的奇整数。对于一个数字化线性函数$\mathcal{F}_n(x) = G_n(x/p)$而言，如下结论成立：

$$P_j = \begin{cases} \dfrac{1}{N_p \cdot 2^{j-i}}, & i \le j \le n \\ \left\{ \begin{array}{cc} \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p}, & G_n(\cdot) = \mathrm{floor}_n(\cdot) \text{或} \mathrm{ceil}_n(\cdot) \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & G_n(\cdot) = \mathrm{round}_n(\cdot) \end{array} \right\}, & 1 \le j \le i-1 \end{cases} \quad (3.15)$$

证明：该定理可以由引理3.5和引理3.6直接导出。 ■

§3.3.3 数字化PWLCM的$P_j(1 \le j \le n)$

如何计算n个动力学指标的值？

基于数字化线性函数$\mathcal{F}_n(x) = G_n(x/p)$上的$P_j(1 \le j \le n)$，我们可以计算一个数字化PWLCM的动力学指标$P_j(1 \le j \le n)$的具体值。给定一个归一化的一维PWLCM(3.1)，我们可以将每个线性分段$F_i(x) = a_i x + b_i$重写为如下形式：$F_i(x_i') = x_i'/p_i$，$x_i' \in [0, p_i)$，这里$p_i = 1/|a_i|$，$x_i' = \text{sign}(a_i) \cdot (x + b_i/a_i)$。由于$|a_i| > 1$，$p_i \in (0,1) \subset [0,1] = S_\infty$。再由方程(3.8)中的重定义，我们可以将一维PWLCM重新表示为如下形式：

$$i = 1 \sim m, F(x_i')|C_i' = F_i(x_i') = x_i'/p_i, x_i' \in C_i' = [0, p_i)。 \tag{3.16}$$

当该一维PWLCM在n-比特有限精度下实现时，第i个线性分段F_i表示为$\mathcal{F}_n^{(i)}$。

令$p_i = N_{p_i}/2^{r_i} \in V_{r_i}$，这里$r_i$是$p_i$的分辨率。用$P_j^{(i)}$表示概率$P_j|x \in C_i$，由全概率公式[212]，可知数字化一维PWLCM的第j个动力学指标P_j的值为：

$$P_j = \sum_{i=1}^{m} P_j^{(i)} \cdot \|C_i\| = \sum_{i=1}^{m} P_j^{(i)} \cdot |p_i| = \sum_{i=1}^{m} P_j^{(i)} \cdot \frac{N_{p_i}}{2^{r_i}}。 \tag{3.17}$$

令$\mathcal{P}_j^{(i)} = P_j^{(i)} \cdot \|C_i\|$，我们有$P_j = \sum_{i=1}^{m} \mathcal{P}_j^{(i)}$。根据定理3.1，很容易得到：

$$\mathcal{P}_j^{(i)} = \left\{ \begin{array}{c} 1/2^j \\ \left\{ \begin{array}{cc} \frac{\lfloor N_{p_i}/2^j \rfloor + 1}{2^{r_i}}, & G_n(\cdot) = \text{floor}_n(\cdot)\text{或ceil}_n(\cdot) \\ \frac{2 \cdot \lfloor N_{p_i}/2^{j+1} \rfloor + 1}{2^{r_i}}, & G_n(\cdot) = \text{round}_n(\cdot) \end{array} \right\} \end{array} \begin{array}{l} , \ r_i \le j \le n \\ , \ 1 \le j \le r_i - 1 \end{array} 。 \tag{3.18}$$

因而，当$\max_{i=1}^{m}(r_i) \le j \le n$时$P_j$的值为：

$$P_j = \frac{m}{2^j}, \tag{3.19}$$

当$1 \le j \le \min_{i=1}^{m}(r_i) - 1$时$P_j$的值为：

$$P_j = \left\{ \begin{array}{ll} \sum_{i=1}^{m} \frac{\lfloor N_{p_i}/2^j \rfloor + 1}{2^{r_i}}, & G_n(\cdot) = \text{floor}_n(\cdot)\text{或ceil}_n(\cdot) \\ \sum_{i=1}^{m} \frac{2 \cdot \lfloor N_{p_i}/2^{j+1} \rfloor + 1}{2^{r_i}}, & G_n(\cdot) = \text{round}_n(\cdot) \end{array} \right. 。 \tag{3.20}$$

当$\min_{i=1}^{m}(r_i) \le j \le \max_{i=1}^{m}(r_i) - 1$时，我们可以使用方程(3.18)计算每个$\mathcal{P}_j^{(i)}$的值得到最终的$P_j$。

接下来让我们来分析一下P_j是如何反映数字化PWLCM的动力学特性退化的，以及P_j的值是如何随着j的变化而变化。这里，我们使用$\overline{\boldsymbol{P}}_j$表示平衡的动力学指标$2^{-j}$，也就是当$\mathcal{F}_n(x)$在$S_n$上离散均匀分布时的指标值。

随着j的变化动力学指标的值如何变化？

当$\max_{i=1}^{m}(r_i) \leq j \leq n$，$P_j$是$\overline{\boldsymbol{P}}_j$的$m$倍，这里$m$是$\mathcal{F}_n(x)$的线性分段的数目。由于$m \geq 2$，可以看到这个事实强烈暗示着$\mathcal{F}_n(x)$在$S_n$上有规则的动力学特性退化。这时$P_j$不仅独立于控制参数$p_1, \cdots, p_m$的分辨率，也独立于它们的具体值和DATF的选择。

当$1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$，$P_j$的值和$p_1, \cdots, p_m$的具体值以及DATF的选择相关。尽管在$p_1 \sim p_m$未知的情况下我们不能计算指标的具体值，我们仍然可以推导出指标值的上下限。由于N_{p_i}是一个奇整数，$N_{p_i}/2^j$和$N_{p_i}/2^{j+1}$都不是整数，则我们有*：

$$\begin{aligned} N_{p_i}/2^j - 1 < \lfloor N_{p_i}/2^j \rfloor < N_{p_i}/2^j, \\ N_{p_i}/2^{j+1} - 1 < \lfloor N_{p_i}/2^{j+1} \rfloor < N_{p_i}/2^{j+1}。 \end{aligned} \tag{3.21}$$

将上式代入方程(3.20)并考虑到$\sum_{i=1}^{m} |p_i| = \sum_{i=1}^{m} \|C_i\| = 1 \Rightarrow \sum_{i=1}^{m} N_{p_i}/2^{r_i} = 1$†，我们可以得出下面的结论：

$$\text{当} G_n(\cdot) = \text{floor}_n(\cdot) \text{或} \text{ceil}_n(\cdot)，\ \frac{1}{2^j} < P_j < \frac{1}{2^j} + \sum_{i=1}^{m} \frac{1}{2^{r_i}}。 \tag{3.22}$$

$$\text{当} G_n(\cdot) = \text{round}_n(\cdot)，\ \frac{1}{2^j} - \sum_{i=1}^{m} \frac{1}{2^{r_i}} < P_j < \frac{1}{2^j} + \sum_{i=1}^{m} \frac{1}{2^{r_i}}。 \tag{3.23}$$

一般来说，$r_1, \cdots, r_m$越大，P_j和平衡指标值$\overline{\boldsymbol{P}}_j = 2^{-j}$越接近，即$P_j - 2^{-j}$越小。这里请注意当$G_n(\cdot) = \text{round}_n(\cdot)$时$P_j$可能等于$\overline{\boldsymbol{P}}_j = 2^{-j}$，一个例子是PWLCM(2.1)和斜tent映射(2.3)(我们将在下一小节证明这个结论)。

最后，再让我们来研究当$\min_{i=1}^{m}(r_i) \leq j \leq \max_{i=1}^{m}(r_i) - 1$时的$P_j$值。显然，这时$P_j$也依赖于$p_1, \cdots, p_m$的具体值和$G_n(\cdot)$的选择，不过这种依赖性相对$1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$时的指标值要弱。而且，$j$越小，这种依赖性越强。

观察$\max_{i=1}^{m}(r_i) \leq j \leq n$和$1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$时的$P_j$值，我们可以**定性**地得出一个**直觉**的结论：当j从n逐渐变化到$\max_{i=1}^{m}(r_i)$的过程中，P_j保持固定为$\overline{\boldsymbol{P}}_j = 2^{-j}$的$m$倍；当$j$从$\max_{i=1}^{m}(r_i)$变化到1的过程中，$P_j$和$\overline{\boldsymbol{P}}_j = 2^{-j}$之间的倍数趋向于越来越小。当然了，对于不同的数字化PWLCM，实际的特性将有所不同，不过上述结论**大致**上应该是成立的。

*$\forall a \in \mathbb{R} - \mathbb{Z}$，我们有$a - 1 < \lfloor a \rfloor < a$，这是floor函数定义的一个自然结果。

†请注意这个结论仅对逐段映满的PWLCM成立，而不是对所有的普通PWLM成立。

如何理解动力学指标与PWLCM动力学特性退化之间的关系？

从总体上讲，当$G_n(\cdot) = \text{round}_n(\cdot)$时，至少$n+1-\max_{i=1}^{m}(r_i)$个指标满足$P_j \neq 1/2^j$；而当$G_n(\cdot) = \text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$时，全部$n$个指标都满足$P_j \neq 1/2^j$。考虑到$\max_{i=1}^{m}(r_i) \leq j \leq n$时$P_j = m/2^j$，一个数字化PWLCM的动力学特性退化可以使用线性分段的数目定量地进行衡量。这实际上意味着下述事实：一个数字化PWLCM的线性分段越多，其动力学特性退化趋向于越严重。

这组动力学指标的另外一个功能是区分不同控制参数下的不同的动力学特性退化。对于一个给定的数字化一维PWLCM，我们来看看存在于动力学特性退化和控制参数p_i的分辨率r_i之间的微妙关系。对于m个控制参数的集合$\boldsymbol{p} = \{p_1, p_2, \ldots, p_m\}$，定义$\widetilde{P} = \frac{1}{n} \cdot \sum_{j=1}^{n} \frac{P_j}{\overline{\boldsymbol{P}_j}}$为$\boldsymbol{p}$的平均退化因子(*average degradation factor*)，它用来定量地反映一个参数集为$\{p_1, p_2, \ldots, p_m\}$的数字化PWLCM的动力学特性退化的程度。显然，$\widetilde{P}$越大，动力学特性退化就越严重。对于两个具有不同的控制参数集$\boldsymbol{p}$和$\boldsymbol{p'}$数字化PWLCM$\mathcal{F}_n(x)$和$\mathcal{F}'_n(x)$，如果$\widetilde{P} > \widetilde{P}'$，我们称$\boldsymbol{p}$比$\boldsymbol{p'}$弱(*weaker*)，或者$\boldsymbol{p'}$比$\boldsymbol{p}$强(*stronger*)，这种关系用$\boldsymbol{p} \prec \boldsymbol{p'}$(或$\boldsymbol{p'} \succ \boldsymbol{p}$)来表示。如果$P_j > P'_j$，我们称$\boldsymbol{p}$在分辨率$j$下比$\boldsymbol{p'}$弱(*weaker at resolution j*)，或者$\boldsymbol{p'}$在分辨率j下比$\boldsymbol{p'}$强(*stronger at resolution j*)，这种关系用$\boldsymbol{p} \prec_j \boldsymbol{p'}$(或者$\boldsymbol{p'} \succ_j \boldsymbol{p}$)来表示。对于一个单独的控制参数$p_i (1 \leq i \leq m)$，在假设其他控制参数在参数空间随机均匀分布的情况下，上述强弱关系可以类似地定义。由我们前面的讨论可以看出：分辨率r_i越小，控制参数p_i越弱。

由以上讨论，既然$P_j \neq 2^{-j}$意味着混沌输出的非均匀性，本章提出的动力学指标可以看成是数字化PWLCM的拟遍历性的一个统计度量，也可以看成是数字化不变分布相对连续分布的可度量偏离的证据。在下面一个小节，通过两个具体的例子，我们将说明下面有关数字化PWLCM的有趣现象：所有线性分段斜率的分辨率越小，$|P_j - \overline{\boldsymbol{P}_j}|$就会越大。那么小的分辨率到底意味着什么呢？让我们把一个分辨率为i的线性分段斜率p写成$p = \frac{N_p}{2^i} = 2^{n-i} \cdot \frac{N_p}{2^n}$，可以看到小的分辨率$i$实际上意味着大的乘法因子$2^{n-i}$。当我们在$n$-比特定点算法下执行数字化除法$x/p$时，假设$x = N_x/2^n$，该除法可以表示为$x/p = 2^{n-i} \cdot \frac{N_x}{N_p}$，这里$2^{n-i}$意味着左移操作，这种操作显然会使得相应的动力学指标值变大。从本质上讲，这些指标反映了数字化(定点)除法在每个线性分段上的塌缩，以及多个线性分段塌缩的累积效应。很自然地，这种数字算法的塌缩会进而造成数字化PWLCM动力学特性的塌缩(退化)。

特别地，如果一个数字化PWLCM的系统方程是已知的，更多的细致结论可能被揭示出来。在下面一个小节中，我们将给出PWLCM(2.1)和斜tent映射(2.3)的$P_j (1 \leq j \leq n)$具体值*。对这两类PWLCM，所有的n个指标$P_j (1 \leq j \leq n)$都由控制参数p的分辨率唯一确定，而独立于控制参数的具体值。由于这两

*尽管我们在文章[109]中已经给出了针对这两类PWLCM的有关结论，§3.3.4中给出的证明是基于方程(3.19)和方程(3.20)的，与[109]中的证明方法不太一样。

类PWLCM中都只有一个控制参数，一些关于P_j的有意义的现象可以更清楚地显示出来。

§3.3.4 两个具体的例子

为了计算数字化PWLCM(2.1)和(2.3)的动力学指标$P_j(1 \le j \le \min_{i=1}^{m}(r_i)-1)$的值，我们先来引入一个新的引理。

引理 3.7: $\forall j, N, N' \in \mathbb{Z}^+$，$N, N'$是奇整数并且$2^j|(N+N')$，则我们有$\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = (N+N')/2^j - 1$。

证明: 由于$a = \lfloor a \rfloor + \mathrm{dec}(a)$，$\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = \left(N/2^j - \mathrm{dec}(N/2^j)\right) + \left(N'/2^j - \mathrm{dec}(N'/2^j)\right)$。令$N = n_1 \cdot 2^j + n_2, N' = n_1' \cdot 2^j + n_2'$以及$N+N' = 2^k (k \ge j)$，我们有$\mathrm{dec}(N/2^j) = (N \bmod n)/2^j = n_2/2^j, \mathrm{dec}(N'/2^j) = (N' \bmod n)/2^j = n_2'/2^j$。由于$N, N'$是奇整数，可以得到$n_2 > 0, n_2' > 0$。由$2^j|(N+N')$，显然有$n_2 + n_2' = 2^j \Rightarrow \mathrm{dec}(N/2^j) + \mathrm{dec}(N'/2^j) = 1$，于是得到$\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = (N+N')/2^j - 1$。证毕。 ■

数字化PWLCM(2.1)的动力学指标$P_j(1 \le j \le n)$

注意：考虑到$0 < p < 1/2$，p的分辨率是集合$\{2, \ldots, n\}$中的一个整数。

定理 3.2: 假设一个离散随机变量x在S_n上离散均匀分布。$\forall p \in V_i (2 \le i \le n)$，对数字化*PWLCM(2.1)*下述结论成立:

1. 当$G_n(\cdot) = \mathrm{round}_n(\cdot)$时，$P_j = \begin{cases} 4/2^j, & i \le j \le n \\ 4/2^i, & j = i-1 \\ 1/2^j, & 1 \le j \le i-2 \end{cases}$；

   当$G_n(\cdot) = \mathrm{floor}_n(\cdot)$或$\mathrm{ceil}_n(\cdot)$时，$P_j = \begin{cases} 4/2^j, & i \le j \le n \\ 1/2^j + 2/2^i, & 1 \le j \le i-1 \end{cases}$；

2. $\forall k \in \{0, \cdots, 2^{n-i}-1\}$，$P\left\{\mathrm{floor}_{n-i}(F_n(x,p)) = k/2^{n-i}\right\} = 1/2^{n-i}$。

证明: 对于PWLCM(2.1)，$m = 4$。四个线性分段的斜率分别是$p_1 = p_4 = p$，$p_2 = p_3 = 1/2 - p$。由$p \in V_i$，$r_1 = r_2 = r_3 = r_4 = i$，$\max_{i=1}^{4}(r_i) = \min_{i=1}^{4}(r_i) = i$。

当$i \le j \le n$时，由方程(3.19)，可以导出

$$P_j = 4/2^j。 \tag{3.24}$$

当$1 \le j \le i-1$时，我们分别考虑下面的两种不同情况：$G_n(\cdot) = \mathrm{floor}_n(\cdot)$或$\mathrm{ceil}_n(\cdot)$，和$G_n(\cdot) = \mathrm{round}_n(\cdot)$。

i) $G_n(\cdot)=\text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$：由方程(3.20)，我们有

$$\begin{aligned} P_j &= \sum_{i=1}^{4}\frac{\lfloor N_{p_i}/2^j\rfloor+1}{2^i} \\ &= 2\cdot\sum_{i=1}^{2}\frac{\lfloor N_{p_i}/2^j\rfloor+1}{2^i} \\ &= 2\cdot\frac{\lfloor N_{p_1}/2^j\rfloor+\lfloor N_{p_2}/2^j\rfloor+2}{2^i}。\end{aligned} \tag{3.25}$$

由于$p_1+p_2=1/2\Rightarrow N_{p_1}+N_{p_2}=2^{i-1}\Rightarrow 2^j|(N_{p_1}+N_{p_2})$，由引理3.7可得：

$$\begin{aligned} P_j &= 2\cdot\frac{(N_{p_1}+N_{p_2})/2^j-1+2}{2^i} \\ &= 2\cdot\frac{2^{i-1-j}+1}{2^i}=\frac{1}{2^j}+\frac{2}{2^i}。\end{aligned} \tag{3.26}$$

ii) $G_n(\cdot)=\text{round}_n(\cdot)$：由方程(3.20)，我们有

$$\begin{aligned} P_j &= \sum_{i=1}^{4}\frac{2\cdot\lfloor N_{p_i}/2^{j+1}\rfloor+1}{2^i} \\ &= 2\cdot\sum_{i=1}^{2}\frac{2\cdot\lfloor N_{p_i}/2^{j+1}\rfloor+1}{2^i} \\ &= 2\cdot\frac{2(\lfloor N_{p_1}/2^{j+1}\rfloor+\lfloor N_{p_2}/2^{j+1}\rfloor)+2}{2^i} \\ &= 4\cdot\frac{\lfloor N_{p_1}/2^{j+1}\rfloor+\lfloor N_{p_2}/2^{j+1}\rfloor+1}{2^i}。\end{aligned} \tag{3.27}$$

当$j<i-1$时，$N_{p_1}+N_{p_2}=2^{i-1}\Rightarrow 2^{j+1}|(N_p+N_p')$，由引理3.7可得：

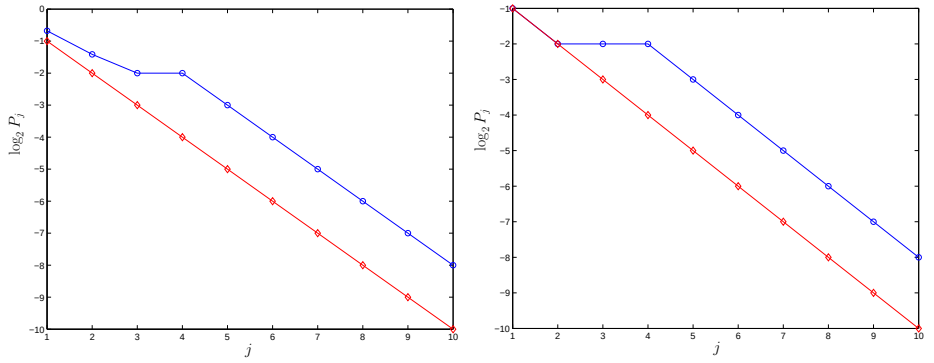
$$\begin{aligned} P_j &= 4\cdot\frac{(N_{p_1}+N_{p_2})/2^{j+1}-1+1}{2^i} \\ &= 4\cdot\frac{2^{i-j-2}}{2^i}=\frac{1}{2^j}。\end{aligned} \tag{3.28}$$

当$j=i-1$，$N_{p_1}+N_{p_2}=2^{i-1}\Rightarrow 2^{j+1}\nmid(N_{p_1}+N_{p_2})(j+1=i>i-1)$，引理3.7不成立，不过我们可以直接计算概率$P_j$：$N_{p_1}<2^i, N_{p_2}<2^i$，因此$N_{p_1}/2^{j+1}<1\Rightarrow\lfloor N_{p_1}/2^{j+1}\rfloor=0, N_{p_2}/2^{j+1}<1\Rightarrow\lfloor N_{p_2}/2^{j+1}\rfloor=0$，则有

$$P_j=4\cdot\frac{0+0+1}{2^i}=\frac{4}{2^i}。 \tag{3.29}$$

由方程(3.24)–(3.29)，可知第一个结论成立。另外，第二个结论可以直接从引理3.4推出。证毕。 ■

定理3.2说明了下述事实：如果x在S_n上满足离散均匀分布，数字化PWLCM(2.1)在S_n上并不满足离散均匀分布；但是$\forall p\in S_i$，$\mathcal{F}_n(x)$的高位$n-i$个比特组合而成的随机变量在S_{n-i}上满足离散均匀分布。关于该定理的真实含义，请参看图3.1。

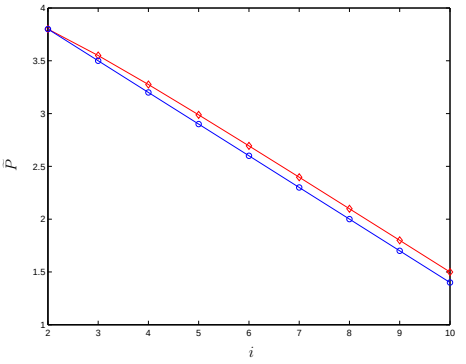


a) $G_n(\cdot) = \text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$　　b) $G_n(\cdot) = \text{round}_n(\cdot)$

○：$\log_2 P_j$；◇：$\log_2 \overline{\boldsymbol{P}}_{\boldsymbol{j}} = -j$

图 3.1: 当$p = 3/16 \in V_4 \subset S_4$时的$\log_2 P_j (1 \le j \le n)$，有限精度为$n = 10$

由定理3.2，我们可以推出动力学特性退化和控制参数p的分辨率i之间的严格关系：分辨率i越小，p越弱(参看图3.2)。关于这个事实的算法上的解释，请参考下一小节的讨论。



○：$G_n(\cdot) = \text{round}_n(\cdot)$；◇：$G_n(\cdot) = \text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$

图 3.2: $\widetilde{P}$和i之间的关系，$n = 10$

推论 3.3: *对数字化PWLCM(2.1)，给定两个不同的控制参数$p \in V_i, p' \in V_{i'}$，这里$i, i' = 2 \sim n$。我们有：$i < i' \Leftrightarrow p \prec p'$。*

证明：考虑如下两个方面：

a) 当$G_n(\cdot) = \text{round}_n(\cdot)$时，

$$\frac{P_j}{\overline{\boldsymbol{P}}_{\boldsymbol{j}}} = \frac{P_j}{2^{-j}} = \begin{cases} 4, & i \le j \le n \\ 2, & j = i-1 \\ 1, & 1 \le j \le i-2 \end{cases} 。 \tag{3.30}$$

则我们可以推出$\widetilde{P}$的值：

$$\begin{aligned}\widetilde{P} &= \frac{1}{n}\cdot\sum_{j=1}^{n}\frac{P_j}{\overline{\boldsymbol{P}_{\boldsymbol{j}}}}\\ &= \frac{1}{n}\cdot(4\cdot(n-i+1)+2+1\cdot(i-2))\\ &= 4\left(1+\frac{1}{n}\right)-\frac{3i}{n}。\end{aligned}\tag{3.31}$$

b) 当$G_n(\cdot)=\text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$时，

$$\frac{P_j}{\overline{\boldsymbol{P}_{\boldsymbol{j}}}}=\frac{P_j}{2^{-j}}=\begin{cases}4 & ,\ i\le j\le n\\ 1+2^{j-(i-1)} & ,\ 1\le j\le i-1\end{cases}。\tag{3.32}$$

则可以推出$\widetilde{P}$的值：

$$\begin{aligned}\widetilde{P} &= \frac{1}{n}\cdot\sum_{j=1}^{n}\frac{P_j}{\overline{\boldsymbol{P}_{\boldsymbol{j}}}}\\ &= \frac{1}{n}\cdot\left(4\cdot(n-i+1)+\sum_{j=1}^{i-1}\left(1+\frac{2^j}{2^{i-1}}\right)\right)\\ &= \frac{1}{n}\cdot\left(4\cdot(n-i+1)+(i-1)+2\left(1-\frac{1}{2^{i-1}}\right)\right)\\ &= \left(4+\frac{5}{n}\right)-\frac{1}{n}\cdot\left(3i+\frac{4}{2^i}\right)。\end{aligned}\tag{3.33}$$

可以看到，对于任何DATF，$\widetilde{P}$关于i是一个递减函数。也就是说，$i<i'\Leftrightarrow\widetilde{P}>\widetilde{P}'\Leftrightarrow p\prec p'$。证毕。 ■

注释 3.1: 这里有一个***绝对弱(absolutely weak)***的控制参数$p=1/4\in V_2$，它满足$P_1=P_2=4/2^2=1$。也就是说，当$p=1/4$时$\mathcal{F}_n(x)$的最低两个比特总是0。另外，$\forall x_0\in V_i(2\le i\le n)$，在$\lceil i/2\rceil$次迭代之后，拟混沌轨道将收敛到$0$：$\forall k\ge\lceil i/2\rceil,\mathcal{F}_n^k(x_0)=0$。这样一个特殊的一维*PWLCM*实际上是(对称)*tent*映射$F(x)=1-2|x-1/2|$的具有四个线性分段的版本，后者的数字化动力学特性在前面已经作为数字化混沌系统的极端例子在§2.5中讨论过了。

定理 3.3: 假设一个离散随机变量x在S_n上满足离散均匀分布。$\forall p\in(0,1/2)\cap S_n$，对于数字化*PWLCM*(2.1)下述事实成立：

1. $\forall p\in D_{i,1}=S_i-S_1=\bigcup_{k=2}^{i}V_i$，$P_i=4/2^i$；
2. $\forall p\in V_{i+1}$；$P_i=2/2^i$；
3. $\forall p\in V_j(j\ge i+2)$，$P_i=\begin{cases}1/2^i & ,\ G_n(\cdot)=\text{round}_n(\cdot)\\ 1/2^i+2/2^j & ,\ G_n(\cdot)=\text{floor}_n(\cdot)\text{或}\text{ceil}_n(\cdot)\end{cases}$。

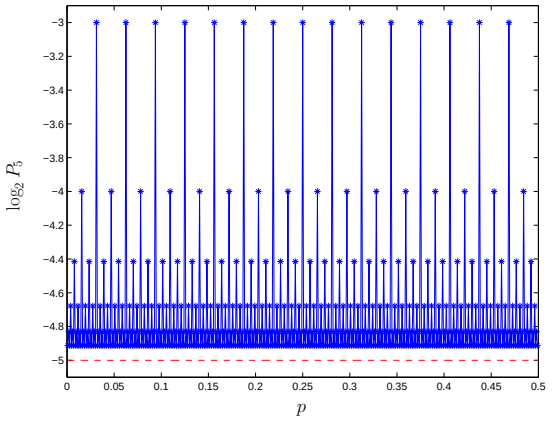


图 3.3: $\log_2 P_5$相对p的变化，这里$n = 10$，$G_n(\cdot) = \text{floor}_n(\cdot)$
(虚线表示平衡的指标值$\log_2 \overline{P}_5 = -5$)

证明：该定理是定理3.2中第一个结论的另外一种等效形式。 ■

注释 3.2: 定理3.3告诉我们：对于具有不同分辨率(即位于不同的数字层次V_i)的控制参数p，至少有一个指标值是不同的。换句话说，***p*的分辨率可以由*n*个指标值$P_1 \sim P_n$唯一确定**。

在图3.3中，我们给出了的P_5关于p变化的试验数据，相关参数为$n = 10$，$G_n(\cdot) = \text{floor}_n(\cdot)$。说实话，当第一次画出图3.3中的曲线时，其中出现的强规则样式着实令本文作者感到震惊，当时上面的理论结论都尚未得到证明。这也是促使我们提出相关的动力学指标的初始动力。

数字化斜tent映射(2.3)的$P_j(1 \le j \le n)$

对于数字化斜tent映射(2.3)，我们很容易导出和定理3.2和3.3类似的两个定理。这里我们略去相关的证明过程。

定理 3.4: 假设一个离散随机变量x在S_n上满足离散均匀分布。$\forall p \in V_i (1 \le i \le n)$，对于斜*tent*映射(2.3)下述事实成立：

1. 当$G_n(\cdot) = \text{round}_n(\cdot)$，$P_j = \begin{cases} 2/2^j & , \ i \le j \le n \\ 1/2^{j-1} & , \ 1 \le j \le i-1 \end{cases}$；

   当$G_n(\cdot) = \text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$，$P_j = \begin{cases} 2/2^j & , \ i \le j \le n \\ 1/2^j + 1/2^i & , \ 1 \le j \le i-1 \end{cases}$；

2. $\forall k \in \{0, \cdots, 2^{n-i} - 1\}$，$P\{\text{floor}_{n-i}(F_n(x,p)) = k/2^{n-i}\} = 1/2^{n-i}$。

推论 3.4: 对于数字化斜*tent*映射(2.3)，给定两个不同的控制参数$p \in V_i$，$p' \in V_{i'}$，这里$i, i' = 1 \sim n$。我们有：$i < i' \Leftrightarrow p \prec p'$。

定理 3.5: 假设一个离散随机变量x在S_n上满足离散均匀分布。$\forall p \in (0,1) \cap S_n$，对于斜*tent*映射(2.3)下述事实成立：

1. $\forall p \in D_i = S_i - \{0\} = \bigcup_{k=1}^{i} V_i$，$P_i = 2/2^i$；
2. $\forall p \in V_j (j \geq i+1)$，$P_i = \begin{cases} 1/2^i & , G_n(\cdot) = \text{round}_n(\cdot) \\ 1/2^i + 1/2^j & , G_n(\cdot) = \text{floor}_n(\cdot) \text{或} \text{ceil}_n(\cdot) \end{cases}$。

§3.3.5 $\mathcal{F}_n^k(x)$的$P_j(1 \leq j \leq n)$

根据上一小节的讨论，我们知道一个离散均匀分布的信号在经过一次数字化PWLCM的混沌迭代后会变得不满足均匀分布。这种不均匀性会随着迭代的进行变得越来越严重，也即，$\mathcal{F}_n^k(x)$的分布会随着k的增加变得越来越不均匀。一般来说，随着k的增加，$P_j(1 \leq j \leq n)$对于大多数控制参数而言是增加的但是也有零星的部分控制参数会减小，指标值相对控制参数和j的规则模式会慢慢消退。

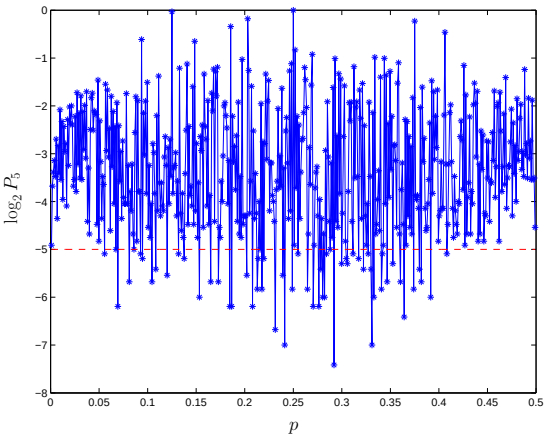


图 3.4: $\mathcal{F}_n^{32}(x)$的$\log_2 P_5$相对p的变化
(虚线表示平衡的指标值$\log_2 \overline{P}_5 = -5$)

在图3.4中，我们给出了$\mathcal{F}_n^{32}(x)$的P_5相对p的变化，这里$\mathcal{F}_n(x)$是一维PWLCM(2.1)，相关参数为$n = 10$，$G_n(\cdot) = \text{floor}_n(\cdot)$。和图3.4、图3.3比较一下，我们可以看到$P_5$的值对于大部分控制参数是增加的，对于少量控制参数变得更小，有些参数下的指标值(如$p = 1/16$)甚至增加到接近1。图3.3中出现的强规则模式在图3.4中一点也分辨不出来了。

以我们的观点，这样一种混乱状态的出现应该是由于连续混沌本身的内在复杂性和数字化混沌动力学特性退化的综合结果。这里，我们提出一个新的问题并试图回答它：在$\mathcal{F}_n^k(x)$如此混乱的动力学指标样式中是否还可以发现什么规律？由于$\mathcal{F}_n(x)$的$P_j(1 \leq j \leq n)$的具体值可以严格的计算出来，我们觉得$\mathcal{F}_n(x)$的有关结论或许可以定性地推广以反映$\mathcal{F}_n^k(x)$的动力学特性的某个侧面。

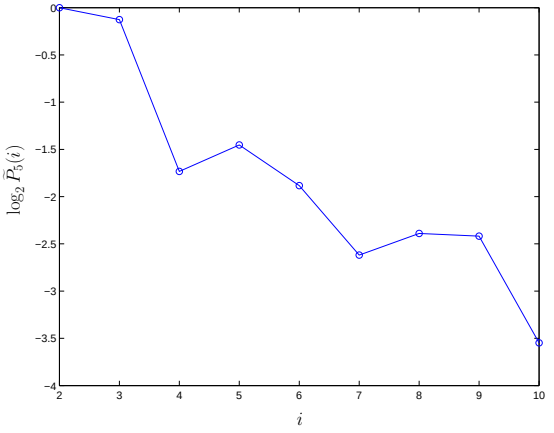


图 3.5: $\mathcal{F}_n^{32}(x)$的$\log_2 \widetilde{P}_5(i)$

为了简化讨论，让我们以数字化PWLCM(2.1)为例。由推论3.3，可知最弱的控制参数是$p = 1/4 \in V_2$，次弱的是位于V_3中的那些参数，然后是那些位于$V_4, V_5, \cdots, V_n$中的参数。以上事实实际上对于$\mathcal{F}_n^k(x)$仍然是**近似地**和**在概念上**成立的：使用$\widetilde{P}_j(i)$表示所有具有相同分辨率i的控制参数下的P_j的平均值，计算显示$\widetilde{P}_j(i)$**大致上**仍然是相对i递减的。对于图3.4中给出的数据，相应的$\widetilde{P}_5(i)$在图3.5中给出。没错，我们确实在图3.4中的杂乱背后捕捉到了隐藏的有序化现象。

§3.4 动力学指标的相关应用

在本节中，让我们来看看如何在实际应用中使用本章提出的动力学指标以发现问题和增强性能。

§3.4.1 几种改善数字化PWLCM混沌动力学特性退化的方案之性能比较

在§2.5.2中，我们介绍了三种不同的方案用以改善数字化混沌系统的动力学特性退化：使用更高的有限精度[56, 61]，级联多个数字化混沌系统[149]，和对混沌系统施加(伪)随机扰动[80, 81, 99, 170, 190, 195, 199, 203]。本章提出的动力学指标可以用来定性地比较这三种改善方案在实践中的性能。

使用更高的有限精度

考虑到拟混沌轨道的循环周期的标度律，在文献[56, 61]中D. Wheeler建议使用更高的有限精度改善短周期给Matthews混沌流密码[55]带来的安全问题。但是，我们在§2.5.1中提到，存在大量的拟混沌轨道，它们的长度较所有拟混沌轨

道的平均值$O(2^{n/2})$短得多(回顾一下循环周期的分布)。因此使用更高的分辨率只能增加所有拟混沌轨道的平均长度，而不能真正有效地增加每条拟混沌轨道的长度。也就是说，这个改善方案不是一个很好的改善数字化混沌系统动力学特性退化的办法。我们可以使用数字化PWLCM的动力学指标重新发现这个结论。

由方程(3.19)可知当$\max_{i=1}^{m}(r_i) \leq j \leq n$时$P_j = m \cdot \overline{\boldsymbol{P}}_j$。我们已经提到$m$可以看作时一个数字化PWLCM动力学特性退化的基本度量。从这个意义上看，更高的有限精度并不能从本质上改善动力学特性退化，既然m对于一个数字化PWLCM是固定的。另外，下述事实也反映了使用更高的精度改善动力学特性退化的问题：更高的分辨率根本不能改变任何在低分辨率下控制参数的强弱。比如，对于数字化PWLCM(2.1)，在任何精度下$p = 1/4$总是绝对弱，并且所有的控制参数$\forall p \in V_i$在更高的精度$n \geq i$下都一样的弱。

因而，假设原有限精度为n，使用更高的精度$n' > n$只是通过引入$n' - n$个新的数字层次$V_{n+1} \sim V_{n'}$来改善平均性能，而不是改善原精度下的问题。

级联多个数字化混沌系统

文献[149]的作者建议使用两个级联的混沌系统增大拟混沌轨道的长度，其中一个混沌系统用来每隔N次迭代初始化(控制)另外一个混沌系统。这样一种办法可以将混沌轨道的长度增加到原来的$O(N)$。不过，由我们在本章中给出的分析可知，它不能改进数字化混沌系统输出的不均匀性。

考虑k个数字化PWLCM被级联，第i个PWLCM的输出用来每隔N_i次迭代初始化第$i+1$个PWLCM。则整个系统的轨道长度会增加到原来的$O\left(\prod_{i=1}^{k} N_i\right)$倍。假设第一个数字化PWLCM的输入在$S_n$上满足离散均匀分布，显然该PWLCM的输出不满足$S_n$上的离散均匀分布。而这个不均匀的输出接着用来作为第二个PWLCM的输入，这种不均匀性会变得更严重。以这样一种观点看来，k个级联的数字化PWLCM实际上类似于$\mathcal{F}_n(x)$的k次复合，也即具有类似于$\mathcal{F}_n^k(x)$的动力学行为，后者已经在§3.3.5中讨论过了。因此，级联多个混沌系统会使得最终输出的动力学特性更不理想，虽然它可以延长得到的拟混沌轨道的长度。

基于扰动的策略

用扰动改善数字化混沌系统的动力学特性退化的策略分别由J. Černák在文献[199]中和周红等人在文献[170]中独立提出。稍后，桑涛等人在文献[80]中将周红等人的扰动策略做了简单的推广，并在文献[81]中提出了一种稍加改进的方案。

这里，我们简单介绍一下文献[80]中提出的扰动方法，后文的讨论将主要围绕这种扰动策略展开。给定一个简单的满足均匀分布的PRNG，运行该PRNG生成一个小的扰动信号$\{S_p(i)\}$，该信号每隔Δ次迭代就扰动一下混沌轨道$\{x(i)\}$，这里Δ是一个正整数，扰动操作可以使异或或者模加。如图3.6所示，一般有两种可能的扰动配置方案，根据扰动点的不同我们分别称它们为扰动配置A和扰动配

置B(扰动配置A在文献[80, 81, 170]中采用，扰动配置B在文献[199]中可以见到)。假设$\oplus$表示扰动操作，上述两种扰动配置可以用如下方程表示：

$$\text{扰动配置A} \quad : \quad x(i+1) = \mathcal{F}_n(x(i)) \oplus S(i), \tag{3.34}$$

$$\text{扰动配置B} \quad : \quad x(i+1) = \mathcal{F}_n(x(i) \oplus S(i)), \tag{3.35}$$

这里，如果$i \bmod \Delta = 0$，则$S(i) = S_p(i/\Delta)$，否则$S(i) = 0$。扰动策略提出的初

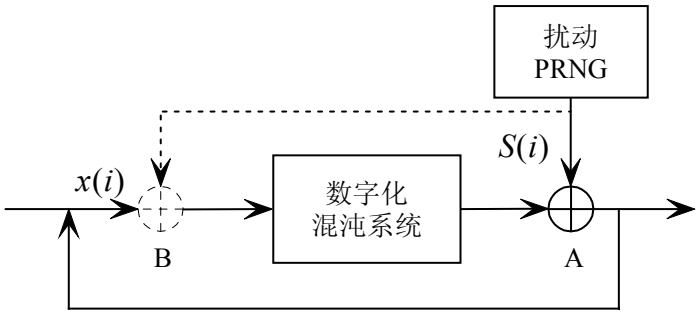


图 3.6: 两种可能的扰动配置方案

衷是延长拟混沌轨道的长度，从这点来看两种不同的配置具有类似的效果。不过从问题的另外一面考虑，我们将指出扰动配置A优于扰动配置B。

不像其他两种改善方案，扰动策略也可以改善数字化混沌系统输出的不均匀性。在§3.3.5中，我们已经指出随着混沌迭代的进行，这种不均匀性会变得越来越严重。考虑到施加的扰动信号会每隔Δ次迭代平滑一次拟混沌轨道，这暗示着被扰动的拟混沌轨道的不均匀性应当和$\mathcal{F}_n^{\Delta}(x)$近似。当$\Delta = 1$，扰动策略的性能达到最优化。从这点看起来，既然扰动配置A同时扰动输入和输出，而扰动配置B只扰动输入，很显然扰动配置A较扰动配置B而言在改善混沌输出的不均匀性方面具有更好的效果。

由以上讨论可见，扰动策略是一个相当不错的改善数字化混沌系统动力学特性退化的实际措施。

在文献[199]中也提出了另外一种不同的扰动策略，在该策略中$S_p(i)$用来扰动数字化混沌系统的控制参数而不是拟混沌轨道。这样一种扰动方法也可以有效地增加拟混沌轨道的长度，但是在改善混沌输出的不均匀性方面不是很有效。考虑到在该扰动方案中对不均匀性的改善是通过混合不同控制参数的动力学特性而实现的，可以知道该方案对不同的控制参数具有不同的性能：对于那些较平均水平弱的控制参数，比如数字化PWLCM(2.1)中的$\forall p = 1/4 \in V_2$，不均匀性会得到改善；而对于那些较平均水平强的控制参数而言，比如数字化PWLCM(2.1)中的$\forall p \in V_n$，这种不均匀性反而可能变得更差。基于这样一个事实，我们认为这种扰动策略的性能应当比上述的扰动配置B更差。

尽管扰动策略可以有效地改善数字化混沌系统的动力学特性退化，扰动后的数字化混沌系统中仍然存在一定程度的动力学退化，因此在特定的应用(尤其是对

安全性很敏感的数字化混沌密码)中仍然需要格外小心以避免潜在的缺陷。更进一步的讨论将在下面两个小节给出。

§3.4.2 在数字化混沌密码中的应用

我们知道，数字化一维PWLCM在数字化混沌密码中广为使用[22, 59, 60, 71, 74–78, 80–82, 90, 96, 98, 106, 107, 110, 112, 116–118, 120]。关于数字化一维PWLCM的动力学指标$P_1 \sim P_n$的理论结果对于这类混沌密码的分析和设计是很有用的。

在§3.3中，我们已经知道数字化一维PWLCM的指标值$P_j (1 \leq j \leq n)$和所有线性分段斜率的分辨率具有密切的关系。因此，通过观察这n个动力学指标值，有可能确定这些斜率的分辨率。这个事实可以用来在某些数字化混沌密码中分辨弱密钥并设计相应的密码分析方法。

在文献[82]中，周红等人提出了一种基于数字化一维PWLCM(2.1)的混沌流密码。该密码的加密流程可以描述如下：使用一个最大长度LFSR(线性移位寄存器)产生一个伪随机信号$\{u_0(i) \in S_n\}$，该信号用来产生一个伪随机密钥流$k(i) = \mathcal{F}_n^k(u_0(i))$，这里$\mathcal{F}_n(x)$在$n$-比特有限精度下实现并且要求$k > n$。文献[170]中提出的扰动策略被采用以改善$\mathcal{F}_n(x)$的动力学特性退化。密钥是控制参数$p$，密钥空间为$(0, 1/2) \cap S_n$。

由我们在§3.3.4中得到的关于$\mathcal{F}_n(x)$的结论以及扰动策略的实际性能，我们可以找到很多弱密钥，它们可以被比简单穷举攻击更小的攻击复杂度攻破。令密钥p的分辨率是i。在已知/选择明文攻击下，由于密钥流$k(t)$是已知的，通过观察n动力学指标值$P_1 \sim P_n$可以得到i。当然了，为了得到正确的指标值，最后一轮扰动必须去掉；由于扰动策略本身是公开的，去除最后一轮扰动变得自然而容易。一旦分辨率i知道了，攻击者就可以仅在子密钥空间$(0, 1/2) \cap V_i$中搜索密钥p，子密钥空间的大小要比整个密钥空间$(0, 1/2) \cap S_n$要小。由定理3.3，考虑到P_j最大值$P_j = 4/2^i$和次大值$P_j = 2/2^i$之间的差异$2/2^i$对于区分分辨率足够大(参考图3.4)，可以得出预计的已知/选择明文数量为$O(2^i)$。另外，分辨率i越小，密钥p可以被越快地找到，则密钥越弱。一个极端的例子：几个已知/选择明文就足够确定最弱的密钥$p = 1/4$。应用以上想法攻击相关的混沌密码，可以算出整体密钥熵降低了两个比特。试验和仿真结论证实了这个想法的可行性。

实际上，对于周红等人在文献[75, 76]中提出的另外一种类似的混沌密码，上述分析方法也是可行的。更多的有关细节可以在下一章或者我们的文章[141]中找到。一些增强周红等人的混沌密码安全性的补救措施在下一章也有详细讨论。基本上，所有针对周红等人的混沌密码的补救措施也可以用来增强一般数字化混沌密码的安全性。

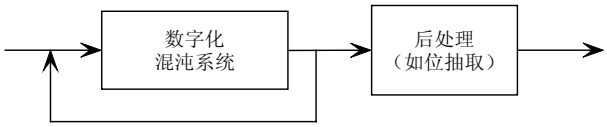
§3.4.3 在混沌伪随机数发生器中的应用

如我们在§2.2中提到的，许多研究者已经建议使用数字化一维PWLCM构造伪

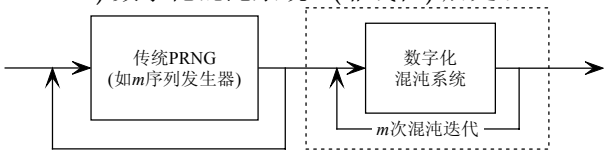
随机数发生器，其中相当一部分是为数字化混沌流密码而专门设计的。由于数字化一维PWLCM输出的不均匀性，由数字化PWLCM生成的伪随机数可能是不平衡的。例如，如果数字化PWLCM(2.1)被使用并且控制参数$p = 1/4$，如果拟混沌轨道的最低两个比特用来生成伪随机比特，这个伪随机比特将变成固定的0比特串$000\cdots$(回顾定理3.2和注释3.1)。在很多混沌伪随机数发生器中，这个问题被简单地忽略了。

为了增强生成的伪随机数的平衡性，需要采用一些补救措施，由于扰动策略可以提供不错的改善动力学特性退化的作用，它再次被建议使用。由于在扰动后系统仍然存在一定程度的非均匀性，较强的控制参数应当比较弱的控制参数有更重要的地位。如果可能，我们建议只使用那些最强的控制参数，如那些位于V_n中的控制参数。

在下文中，我们将讨论两种不同的混沌伪随机数发生器的结构，并解释数字化一维PWLCM在其中的角色。这两种结构如图3.7a和图3.7b所示。



a) 数字化混沌系统+ (非线性) 后处理



b) 传统PRNG + 数字化混沌系统

图 3.7: 两种混沌伪随机数发生器的通用结构

第一种结构(图3.7a)在很多混沌流密码和混沌伪随机数发生器中被采纳。大多数情况下，只有单个数字化混沌系统被使用，不过我们在文献[22]中建议使用一对混沌系统以提供更高的安全性。该类结构中最简单的版本是后处理函数为$f(x) = x$的情形，也即拟混沌轨道未经任何后处理直接输出。最常用的后处理是所谓“位抽取”(bit-extracting)算法：从拟混沌轨道的二进制表示形式中抽取有限个(一般是连续的)比特。

在混沌PRNG的安全应用中，如果数字化一维PWLCM在第一种结构中和某种位抽取后处理算法一起使用，我们建议抽取拟混沌轨道的中间部分的比特生成伪随机数，这是由于下面两个事实：1) 连续的混沌状态的高位比特之间的相关性较低位比特强*；2) 数字化PWLCM的动力学特性退化主要表现在低位比特上(回顾引理3.4)并且伪随机扰动也主要作用在低位比特上。举个例子，如果控制参数为$p \in V_n$的一维PWLCM(2.1)被使用，表示拟混沌轨道为二进制形

*考虑如下事实：如果我们得到了两个连续的混沌状态的高$n/2$个比特，则有可能**近似**地得到控制参数的值；但是我们一般得不到有关控制参数的任何有用信息，如果只是已知低$n/2$个比特。

式$0.b_n b_{n-1}\cdots b_1, b_i \in \{0,1\}$，抽取中间$n/3$个比特$b_{\lfloor 2n/3\rfloor}\cdots b_{\lceil n/3\rceil}$是可行的。

另外一个可能的解决方案是组合当前混沌状态的不同比特。一般来说，不同比特的组合是非常强的非线性操作，它可以在不增加过多的运算负担的情况下极大地增加伪随机数的复杂性。另外，使用多个(甚至所有的)以前状态的累积状态产生伪随机数也可以获得不错的效果。在文献[128]中，我们提出了一种累积方法和一种组合方法以增强Baptista密码的安全性。

第二种结构(图3.7b)的使用可以在文献[82]中找到。在该结构中，数字化混沌系统是作为传统PRNG的后处理单元出现的，用以增加传统PRNG生成的伪随机数的复杂性(例如增加m序列的线性复杂度[144, 213])。

当数字化一维PWLCM在第二种结构中使用时，由于数字化PWLCM具有近似均匀的分布，前端的传统PRNG生成的伪随机数的分布不会被改变。因此，这种结构也可以用在需要非均匀分布伪随机数的场合。显然，数字化混沌系统可以看作是一个非线性的平滑滤波器。在这样一种结构中，如果$m = 1$或者$\Delta = 1$，我们可以使用$\text{floor}_{n-i}(\mathcal{F}_n(x))$产生良好的伪随机输出(回顾引理3.4和定理3.2的第二个结论)。例如，假设控制参数为$p \in V_{\lfloor n/2\rfloor}$的数字化PWLCM(2.1)被使用，最终输出的高位$n - \lfloor n/2\rfloor$个比特会近似保持前端PRNG输出伪随机数的分布。当较强的控制参数被使用时，较低的比特也可以输出作为生成的伪随机数的一部分。例如，$\forall p \in V_n$，高位$\lceil 2n/3\rceil$比特基本上都是可用的。哪些比特可以在实际应用中采用需要通过试验具体确定。

§3.5 本章小结

当混沌系统在有限状态离散空间中实现时，其动力学特性会与连续混沌理论框架中的特性完全不同，即会产生动力学特性退化。在混沌系统的数字化应用中这个问题有着重要的意义。在本章中，我们针对数字化一维PWLCM提出了一组动力学指标，并详尽地讨论了它们的计算方法，虽然理论分析主要针对一类逐段映满的数字化一维PWLCM展开，但是给出的分析可以很容易地推广到一般的PWLCM。相关的理论结论表明：在离散均匀输入的驱动下，数字化混沌输出不满足离散均匀分布，这种非均匀性可以定量地使用n个力学指标衡量：$1 \le j \le n, P_j = P\{\mathcal{F}_n(x) \in S_{n-j}\}$。

对于其他并非仅仅使用除法定义的混沌映射，本章的结论不能直接推广。如果更为复杂的需要浮点算法的数学函数在系统方程中使用，寻找可度量的动力学指标并分析相关数字化混沌系统的特性将变得异常困难，这是由于浮点小数在离散空间中以一种完全不均匀的方式分布*。如果只是混沌迭代使用浮点算法进行，所有的混沌状态仍然使用定点存储，分析可能会变得容易一些。

在未来的研究中，一些分析其他数字化混沌系统的理论工具尚待发掘。作为可能的解决方案的基础，不同的数学函数在有限精度下的算法模型(包括定点和浮

*这种不均匀性导致很多著名的病态行为，如在有限精度下求解某些病态方程可能得到完全错误的解。

点算法)应当首先被建立起来。比如，为了分析在文献[92]中提出的逐段非线性混沌映射，我们需要有一个关于函数$\sqrt{x}$如何在有限精度下计算的合理模型。

第二部分

一些最近提出的数字化混沌密码的分析

第四章　周红等人提出的一类混沌流密码的分析

§4.1　引言

U. Feldmann等人于1996年提出了一种称为混沌逆系统法(*inverse system approach*)的混沌安全保密通信的通用模型[73]。不久周红等人指出混沌逆系统法设计的部分保密通信系统的安全缺陷，它们使得这些系统的安全性从严格的密码学意义看不够安全[75]。

作为一种可能的解决方案，周红等人在文献[75, 76]中提出了一种增强的基于混沌逆系统法的混沌加密模型。与U. Feldmann等人的模型不同，周红等人模型是基于一类在有限精度下实现的数字化PWLCM。除了上述混沌加密模型，周红等人还提出了其他几种基于数字化PWLCM的混沌流密码[74, 77, 78, 82]。

从理论上讲，周红等人提出的所有混沌密码都是基于数字化PWLCM密钥流的混沌流密码。周红等人的密码可以分为两个基本类型：一类使用均匀分布的输入信号驱动多次混沌迭代产生密钥流[75, 76, 82]；另外一类通过对拟混沌轨道进行非线性后处理生成密钥流，当拟混沌轨道进入相空间的不同区域时，输出不同的密钥比特流[74, 77, 78]。

到现在为止，尚未见到关于周红等人的密码的分析工作报道。唯一的相关工作是桑涛等人于1999年报道的[92]。桑涛等人指出：由于周红等人在文献[77]中提出的密码中使用了PWLCM，其逐段线性性可能导致某些潜在的不安全性。尽管桑涛等人没有给出实际的攻击方案，考虑到线性分析在密码学中有着重要的作用[143, 144]，这种担心并不是没有道理的。为了避免这个问题，桑涛等人建议使用一类逐段非线性混沌映射代替PWLCM。很显然桑涛等人的建议也适用于周红等人的其他几种混沌密码[74, 78]。

在本章中，我们试图给出周红等人在文献[75, 76, 82]中提出的混沌密码的一些密码分析结果。

尽管周红等人已经注意到在有限精度下实现的数字化混沌映射存在动力学特性退化问题，并且提出了扰动策略改善这种退化[74, 82, 170]，但是很奇怪他们没有在文献[75, 76]中建议使用扰动策略改善这种退化。但是很显然，对于数字化混沌密码，数字化混沌系统的动力学特性退化是不能忽略的，既然它会破坏密钥流的均匀分布并可能引入弱密钥。在本章中，针对周红等人在文献[75, 76]中提出的混沌密码，以一种比周红等人的文献[170]更为基本的分析方法，我们将重新研究数字化混沌给相关的混沌密码带来的安全隐患。

在讨论完数字化混沌带来的安全问题之后，根据我们在上一章中给出的关于数字化PWLCM的理论结果，我们将指出在周红等人的混沌流密码中存在大量弱密钥。在弱密钥分析的基础上，我们提出一类增强的(多分辨率)穷举攻击方案，它比简单穷举攻击具有更小的平均攻击复杂度。在这类攻击中，密钥越弱，攻击

完成的速度越快。其整体密钥熵较简单穷举攻击降低了两个比特。尽管密钥熵的减小并不是很明显，该攻击对于相关密码中的弱密钥非常有效(其中最弱的密钥是$p = 1/4$)。为了增强周红等人的密码的安全性，我们讨论了一些可能的解决方案，其中的几种可能用于避免弱密钥带来的安全问题。

§4.2 周红等人的混沌密码

所有本章讨论的周红等人的密码都是基于我们前面反复提到的一维PWLCM(2.1)。该映射的图象参看图4.1。 在§3.2.1中我们已经知道逐段映满

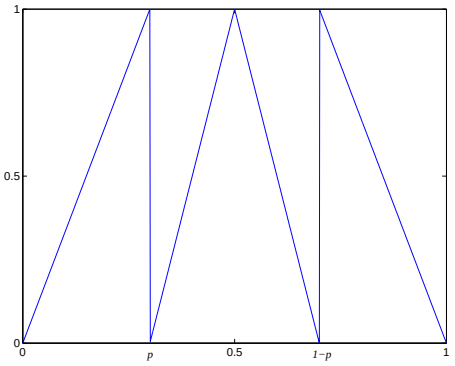


图 4.1: 周红等人的混沌流密码中使用的PWLCM

的PWLCM具有相当优良的动力学特性。很明显上述PWLCM是逐段映满的，因此其动力学特性适于构造混沌密码。

在文献[82]中，一个n阶m-序列$c(t)$用来生成驱动信号$u_0(t) = \sum_{i=1}^{n} 2^{-i} c(t+i-1)$，该信号作为上述PWLCM的初始条件通过多次迭代生成密钥流$k(t) = u_k(t) = F^k(u_0(t), p)$。与大部分流密码一样，然后将密钥流与明文逐比特异或生成密文。为了克服数字化PWLCM(2.1)的动力学特性退化可能带来的安全隐患，扰动策略[170]被建议使用。这里的m-序列可以使用任何其他具有(近似)均匀分布的伪随机序列替代。

如前述，文献[75, 76]中的混沌密码是用来改善以前的混沌逆系统密码系统的安全性的。一种典型的密码如下所示：

$$\begin{aligned} &\text{加密：} y(t) = \Big[u(t) + F^k(y(t-1), p)\Big] \pmod 1, \\ &\text{解密：} u(t) = \Big[y(t) - F^k(y(t-1), p)\Big] \pmod 1, \end{aligned} \tag{4.1}$$

这里$u(t)$是明文，$y(t)$是密文，p是密钥。按照周红等人的讨论，PWLCM(2.1)应当在n-比特有限精度下实现，并且需要满足$n < k$以避免由已知/选择明文/密文对恢复密钥p的可能。

实际上，文献[75, 76]中的密码是带密文反馈的流式密码。由于在大多数情况下密文$y(t)$一般满足近似均匀分布，我们可以把它们看成是文献[82]中密码的一种变形：文献[75, 76]中的$y(t-1)$对应文献[82]中的$u_0(t)$。

在图4.2中我们给出了上述密码的一个简明图示，其中“方法一”表示文献[82]中的混沌密码，“方法二”表示文献[75, 76]中的混沌密码。需要注意的是在文献[75, 76]中周红等人并未建议使用扰动策略，因此扰动模块只在“方法一”中存在。

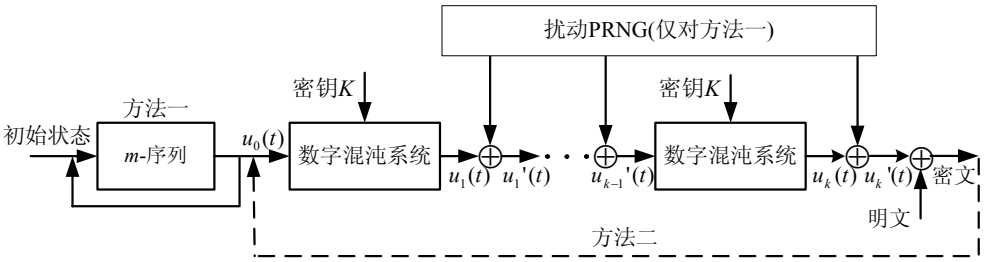


图 4.2: 文献[75, 76, 82]中提出的混沌密码

在上一章中我们已经证明数字化PWLCM(2.1)的动力学指标值与控制参数p的分辨率具有可度量的关系。在扰动算法已知的情况下，扰动策略的使用不能有效地掩盖这种关系。因此，周红等人的密码对已知/选择明文攻击是不安全的，其中存在弱密钥。在后文中我们将对周红等人的密码进行弱密钥分析，然后介绍一种增强的穷举攻击并分析其性能。最后，我们讨论一些可能的解决方案以修补弱密钥带来的安全缺陷。

§4.3 数字化PWLCM(2.1)的动力学特性退化的再分析及其对周红等人提出的密码方案(4.1)安全性的影响

正如我们在§2.6.1中推荐的那样，由于PWLCM具有优良的动力学特性，如果数字化PWLCM的动力学退化问题通过适当的措施得到解决，则PWLCM是设计数字化混沌密码的一个很好的选择。由于周红等人没有在文献[75, 76]中建议使用扰动策略增强系统的安全性，在本节中我们将重新研究数字化PWLCM(2.1)的动力学特性退化问题以及它对密码方案(4.1)安全性的影响。本节可以看作是我们前面章节理论分析的一个实际例子。

首先，让我们用一个简单的例子来说明数字化PWLCM(2.1)的动力学特性退化是如何使得周红等人的密码方案(4.1)不安全的。不失一般性，采用我们在§3.2.2中给出的定义和符号，假设有限精度$n = 8$，$G_n(\cdot) = \mathrm{floor}_n(\cdot)$。当$p = 3/8$，$y(t-1) = 1/16$时，可以算出$F_n^9(y(t-1), p) = 0$。由于$k \geq n+1 =$

9，$F_n^k(y(t-1),p)=F_n^9(y(t-1),p)=0$。因而，

$$y(t)=\left\lfloor u(t)+F_n^k(y(t-1),p)\right\rfloor \bmod 1=u(t)。\tag{4.2}$$

也就是说，明文$u(t)$没有经过任何加密直接输出为密文！进一步的试验表明，当$p=3/8$时，在$y(t-1)\in S_n$的所有$2^8=256$种可能取值中有114个使得$y(t)=u(t)$成立。这样高的信息泄漏率($114/256\approx 44.5\%$)将使得唯密文攻击和已知明文攻击成为可能。因此，我们说$p=3/8$是一个非常弱的密钥。显然，考虑到对连续域内的混沌映射$P\{F^k(x,p)=0\}=0$(该映射是遍历性的[209])，可知这个严重问题是由于数字化PWLCM(4.1)的动力学特性退化造成的。

接下来让我们看看在周红等人的密码方案(4.1)中到底有多少弱密钥。粗略地讲，对于密钥p，如果$y(t)=u(t)$的概率大于2^{-n}，就可以认为p是弱密钥。$y(t)=u(t)$的概率越大，相应的密钥也就越弱。为了定量地度量一个给定密钥p的强弱，定义一个如下的*弱密钥因子*(*weak factor*)$\alpha(n,k,p)$：

$$\alpha(n,k,p)=P\left\{F_n^k\left(y(t-1),p\right)=0\right\}\Big/2^{-n}。\tag{4.3}$$

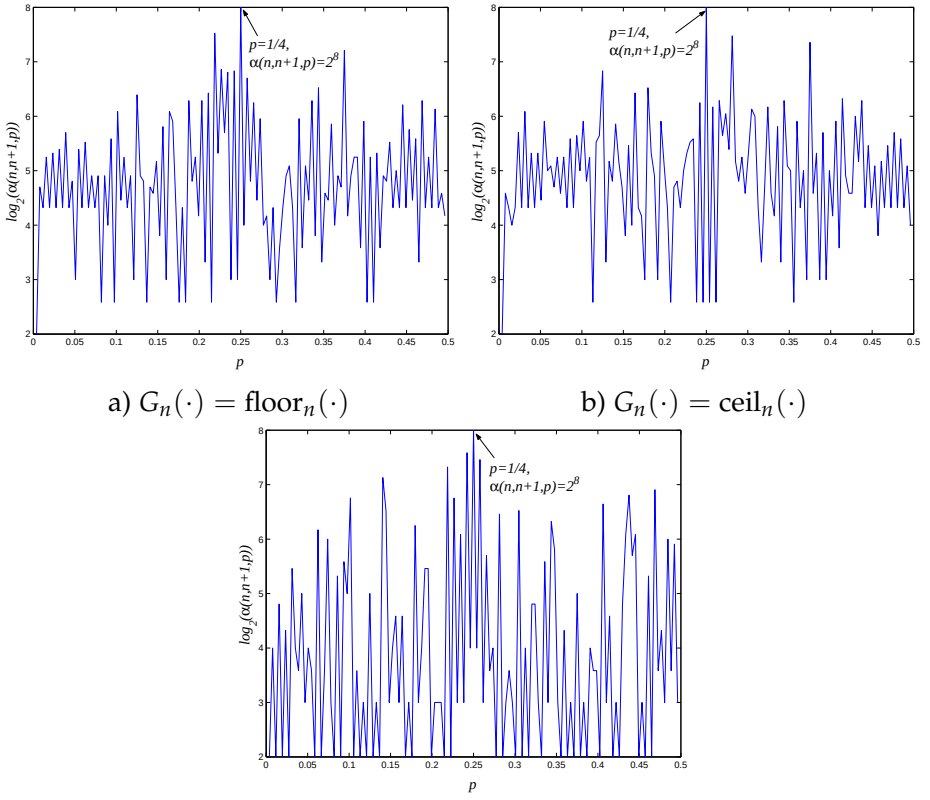
这里，$\alpha(n,k,p)>1$意味着p是弱密钥；并且$\alpha(n,k,p)$越大，相应的密钥p越弱。另外，当$F_n^k(y(t-1),p)$在S_n上均匀分布时，$\alpha(n,k,p)=1$(即$P\left\{F_n^k(y(t-1),p)=0\right\}=2^{-n}$)，因此$\alpha(n,k,p)$也可以部分反映$F_n^k(y(t-1),p)$在$S_n$上分布的不均匀性。由(4.3)可知$k_1>k_2\Rightarrow\alpha(n,k_1,p)\geq\alpha(n,k_2,p)$，这说明$\alpha(n,n+1,p)$是$\alpha(n,k,p)$的下限。因而，在后文的叙述和试验中，我们始终假设$k=n+1$(实际上，由于过多的混沌迭代会加重运算负担，$k=n+1$也是周红等人的密码中的最优取值)。

当$n=8$时，$G_n(\cdot)$分别取$\mathrm{floor}_n(\cdot)$，$\mathrm{ceil}_n(\cdot)$和$\mathrm{round}_n(\cdot)$，图4.3给出了$\log_2(\alpha(n,n+1,p))$相对不同密钥的值。由图中所示的试验数据，我们可以发现下述事实：

- **事实1**：$\alpha(n,n+1,p)>1$几乎处处成立，很多密钥非常弱：$\alpha(n,n+1,p)\gg 1$。
- **事实2**：最弱的密钥是$p=1/4$，它使得$\alpha(n,n+1,p)=2^8$，因此$P\{y(t)=u(t)\}=1$(密码系统消失了！).
- **事实3**：当$G_n(\cdot)=\mathrm{round}_n(\cdot)$时弱密钥的数量较$G_n(\cdot)=\mathrm{floor}_n(\cdot)$和$G_n(\cdot)=\mathrm{ceil}_n(\cdot)$时为少，弱密钥因子的绝对值也小，这说明$\mathrm{round}_n(\cdot)$可以比其他两种DATF提供更高的安全性。既然$\mathrm{round}_n(\cdot)$会在混沌迭代中引入较小的量化误差，这个现象看起来是自然而合理的。

显然，上述事实显示周红等人的密码方案(4.1)从严格的密码学角度看是不安全的。

回顾我们在上一章中引入的动力学指标，显然$\alpha(n,1,p)=P_n/2^{-n}$。根据§3.3.4中给出的理论结果，上述有关弱密钥的试验观察可以可以定性地得到解



a) $G_n(\cdot) = \mathrm{floor}_n(\cdot)$ b) $G_n(\cdot) = \mathrm{ceil}_n(\cdot)$

c) $G_n(\cdot) = \mathrm{round}_n(\cdot)$

图 4.3: 弱密钥因子$\log_2(\alpha(n, n+1, p))$相对$p$的变化，$n = 8$

释。作为一个典型的PWLCM，我们已经证明了其动力学指标$P_j = P\{F_n(x,p) \in S_{n-j}\}(j = 1 \sim n)$满足定理3.2和定理3.3。这两个定理指出数字化PWLCM(4.1)的动力学特性退化可以通过控制参数的分辨率来度量。一般而言，控制参数p的分辨率越小，动力学退化就越严重。根据这样一个结论，最弱的密钥应当是$p = 1/4$因为它具有最小的分辨率2，这和从图4.3中的试验数据得到的事实2是一致的。

当然，由于$k > n > 1$，关于P_j和p的分辨率之间的严格数学结论不能简单地推广以解释$\alpha(n,k,p) = P\{F_n^k(x,p) = 0\}/2^{-n}$关于$p$的变化情况。观察图4.3，除了分辨率较小的控制参数以外，可以看到部分具有相当大的分辨率的密钥也变得很弱，如$p = 29/128$和$p = 31/128$(都具有分辨率$n-1 = 7$)。这意味着数字化混沌系统的动力学特性退化随着k的增大变得越来越严重和复杂，这也是我们在§3.3.5中提到过的一个定性结论。

根据上面的讨论，我们可以得出结论：如果不采取一定的措施改善数字化PWLCM(2.1)的动力学特性退化，则周红等人在文献[75, 76]中提出的密码方案是不安全的。很自然地，我们可以使用在文献[170]中提出的扰动策略解决这个问题。不过，在下面一节，我们将指出在使用了扰动策略之后仍然存在一些安全问

题。

§4.4 弱密钥分析和一种增强的穷举攻击方案

在§3.2.1中已经提到，PWLCM(2.1)具有均匀的不变分布函数$f^*(x) = 1$，这意味着如下事实：如果输入信号$u_0(t)$在定义域上$I = [0,1]$上满足均匀分布，那么PWLCM的输出信号$u_1(t) = F(u_0(t), p)$也满足I上的均匀分布。这个特点是周红等人的密码的安全基础之一。但是，我们在§3.3.4中已经证明，当这样一个PWLCM在有限精度下实现时，会发生动力学特性退化，并且这种退化可以使用n个动力学指标定量地加以描述。

现在让我们回想一下上一章给出的有关结论。当PWLCM(2.1)在n-比特精度下实现时，如果输入信号$u_0(t)$满足离散均匀分布，则混沌输出信号$u_1(t) = F(u_0(t), p)$不满足离散均匀分布。$u_1(t)$相对离散均匀分布的偏离可以使用n个动力学指标$P_1 \sim P_n$进行刻画：1) $\forall p \in S_n$，$P_j > 1/2^j$；2) P_j的值由p的分辨率唯一确定(定理3.2和定理3.3)；3) P_j的最大可能取值为$4/2^j$，次大可能取值为$2/2^j$。上面的第三条暗示我们可能通过观察这n个动力学指标值$P_1 \sim P_n$得到p的分辨率，也就是得到p位于哪个数字层次的信息。这个事实开启了一扇发现弱密钥和减小攻击复杂度的后门。

我们在§4.2中提到，本章讨论的三种混沌密码具有类似的结构，因此在本节中我们将主要对文献[82]中的混沌密码做密码分析。在后文中我们将采用§3.2.2中的定义和符号以使得论述更为清楚。

对于PWLCM(2.1)，考虑$0 < p < \frac{1}{2}$，当它在n-比特有限精度下实现时，密钥空间为$S_n \cap (0, \frac{1}{2})$，简单穷举攻击的密钥熵为$K = \log_2(2^{n-1} - 1) K \approx n - 1$。为了方便下面的叙述，定义$S'_i = S_i \cap (0, \frac{1}{2}), V'_i = V_i \cap (0, \frac{1}{2})$，以及$S'_n$的完全多分辨率分解为$\{V'_i\}_{i=2}^n$，这里$S'_n = \bigcup_{i=2}^n V'_i$，$\forall i \neq j, V'_i \cup V'_j = \varnothing$(分解级数为$n-1$)。

§4.4.1 弱密钥分析

在S'_n上执行完全多分辨率分解，我们可以得到$S'_n = \bigcup_{i=2}^n V'_i$。由定理3.3(考虑$V'_i \subset V_i$)，对于位于不同数字层次$V'_i, V'_j (i \neq j)$的两个密钥$p \neq q$，在它们的动力学指标值$P_{i_1} \sim P_{i_n}$和$P_{j_1} \sim P_{j_n}$之间存在可区分的差异。因此，在$n$个动力学指标值全部已知的情况下，我们可能得到密钥的分辨率。一旦得到p的分辨率，我们就可以仅在整个密钥空间的一个子集V_i中搜索密钥，这将使得攻击复杂度变低。p的分辨率越小，要搜索的密钥子集V'_i也就越小(2^{i-2}可能的密钥)，攻击成功得越快。换句话说，分辨率越小，密钥越弱。

接下来问题变成了：我们怎样才能得到$P_1 \sim P_n$的值？由于周红等人密码的特殊结构，在已知/选择明文攻击框架下观察$P_1 \sim P_n$的值是可能的。为了简化讨论，假设PWLCM的第i次迭代输出为$u_i(t)$，第i扰动后的输出为$u'_i(t) = u_i(t) \oplus pt_i(t)$(这里$pt_k(t)$是第$i$次的扰动信号)，则密钥流$k(t) = u'_k(t)$(参考图4.2)。

当明文$P(t)$和密文$C(t)$都已知的情况下，$k(t)$可以通过$P(t) \oplus C(t)$计算出来。既然扰动算法的所有细节都是公开的，我们可以从$k(t)$中去掉最后一轮扰动信号$pt_k(t)$得到未经扰动的最后一轮混沌迭代输出$u_k(t) = k(t) \oplus pt_k(t)$。考虑到$u_k(t) = F(u'_{k-1}(t), p)$和第$k-1$次的扰动输出$u'_{k-1}(t)$在$S'_n$上近似满足离散均匀分布[170]，则可知$u_k(t)$服从定理3.2和定理3.3，也就是说，$P_1 \sim P_n$的值可以通过观察$u_k(t)$得到。随着已知/选择明文数量的增加，$P_1 \sim P_n$的估计值将逐渐收敛到上面两个定理确定的理论值上去。由于在每个指标值的最大值和次大值之间存在足够的可分辨差异$4/2^j - 2/2^j = 2/2^j$，p的分辨率将在一定数量的已知明文/密文对之后被确定下来。

为了显示周红等人的密码中弱密钥的存在以及如何确定密钥的分辨率，让我们来考虑整个密钥空间中最弱的密钥$p = 1/4 \in V'_2$。由定理3.2可知$P_2 = 1$，这意味着$u_k(t)$最低两个比特始终为0。当$p = 1/4$选作密钥时，通过观察$u_k(t)$我们可以很快地发现$P_2 = 1$这个事实(P_2的次大值是$1/2$)，然后马上可以推出$p = 1/4$。当$p \in V'_3$时$P_2 = P_3 = 1/2$，上述过程会变得稍微复杂一些：计算P_2和P_3的估计值确定$p \in V'_3$–使用$P_3 = 1/2 = 4/2^3$确定$p \in S'_3$，使用$P_2 = 1/2 < 1 = 4/2^2$确定$p \notin S'_2$，得到分辨率之后就可以在数字层次V'_3中搜索得到正确密钥了(只有$2^{3-1} - 2^{2-1} = 2$个可能的密钥$1/8$和$3/8$)。类似地，当$p \in V'_i$，需要观察P_{i-1}和P_i的值以确定分辨率i，子密钥空间V'_i中要搜索的密钥总数为$2^{i-1} - 2^{i-2} = 2^{i-2}$。上面关于弱密钥的论述总结在表4.1中。

表 4.1: 分辨率不同的密钥的比较

p的分辨率	2	3	$\cdots$	i	$\cdots$
需要观察的指标值	P_2	P_2, P_3	$\cdots$	P_{i-1}, P_i	$\cdots$
需要的明文数量	$O(2^2)$	$O(2^3)$	$\cdots$	$O(2^i)$	$\cdots$
搜索的密钥子空间	V'_2	V'_3	$\cdots$	V'_i	$\cdots$
密钥子空间的大小	1	2	$\cdots$	2^{i-2}	$\cdots$

显然，当周红等人的密码在n-比特有限精度下实现时，整个密钥空间可以划分为$n-1$个子空间$V'_i (2 \le i \le n)$，它们的密码学强度随着i的减小呈指数减小。作为一个自然的结论，如果我们将有限精度从n增加到n'，$n'-n$个新的子密钥空间$V'_{n+1} \sim V'_{n'}$被引入，但是所有在原精度下的弱密钥的强度没有发生任何变化*。

由以上讨论可知，确定密钥分辨率的基本流程如下所述。对于每个已知/选择明文，计算$u_k(t)$并得到$P_2 \sim P_n$的估计值(由于V_1不在密钥空间中P_1可以忽略)。当每个P_i稳定在一个小范围内波动时，即可使用下述规则确定分辨率i：如果P_i收敛到最大可能取值$4/2^i$，并且P_{i-1}收敛到次大可能取值$2/2^{i-1}$，则分辨率为i。所需已知/选择明文的数量为$O(2^i)$。由所需的明文数量可知，p的分辨率i越小，通过观察得到分辨率i的速度越快，相应的密钥也越弱。稍后在§4.5中，我们将通过一些实际的仿真试验证实这里弱密钥分析的正确性和可行性。

*我们在后面会提到，这个事实使得提高系统实现精度的改善措施成为一种比较消极的手段。

§4.4.2 一种增强的穷举攻击

由上节的讨论，我们可以很容易地导出一类增强的穷举攻击方法，这是一类已知/选择明文攻击，并且具有比简单穷举攻击小的复杂度。在这种攻击方案中，首先密钥的分辨率i通过一定数量的已知/选择明文/密文对得到，然后在子密钥空间V_i'中执行密钥穷举搜索得到正确的密钥。该攻击方法的C语言描述如下：

- **所需条件**：已知/选择明文和相应的密文，扰动算法的公开细节(即已知的$u_k(t)$)；
- **变量说明**：`u_k[t]` $-u_k(t)$，`P[i]` $-P_i$的估计值，`Pn[i]` $-u_k(t) \in S_{n-i}$的出现次数，`e1[i]` $-$一个确定`P[i]`近似等于P_i最大值的阈值参数，`e2[i-1]` $-$另外一个确定`P[i-1]`近似等于P_{i-1}次大值的阈值参数；
- **初始化操作**：`for(i=2;i<=n;i++) {Pn[i]=0;P[i]=0;}`
- **确定密钥的分辨率i**：

```
for(t = 0; ; t++)
{    for(i = 2; i <= n; i++)
     {    temp = floor(u_k[t]*pow(2,n));
          if((temp << (n-i)) == 0)
          { Pn[i]++; P[i] = Pn[i]/t; }
     }
     for(i = 2; i <= n; i++)
     {    if(fabs(P[i]-4/pow(2,i)) <= e1[i]
          && fabs(P[i-1]-2/pow(2,i-1)) <= e2[i-1])
               goto end;
     }
}
end: printf("当前密钥的分辨率为%d",i);
```

对于上述流程我们有几个注释：

- **注释1**：请注意将`u_k[i]`转换为整数的操作需要浮点乘法，这是相当耗时的操作。事实上，由于文献[75, 76, 82]中所有的小数都是用二进制定点性质表示的，我们可以将它们考虑为整数，这样浮点所需的浮点乘法就被转化为快速的左移操作。
- **注释2**：由于$u_k(t)$只是近似(不严格)服从定理3.2和定理3.3，在估计值和理论值之间存在一个小的误差。因此，为了提高攻击的鲁棒性，阈值参数`e1[i]`和`e2[i-1]`是必需的。这两个阈值参数地选择准则是0 <`e1[i]`< $1/2^i$和0 <`e2[i-1]`< $1/2^{i+1}$，它们的实际取值可以根据试验具体确定。

- **注释3**：在文献[82]中，m-序列用来生成$u_0(t)$，因此$u_0(t)$永远都是正数(即总不等于0)，这可能影响估计概率值和理论值之间的对应性：当$u_0(t)=0$，$\forall i \in [1,n]$，$F_n(u_0(t),p)=0 \in S_{n-i}$，因此$u_0(t) \neq 0$会使得实际概率值较理论值偏小。幸运的是，由于扰动的使用，$u'_{k-1}(t)$近似服从S_n上的离散均匀分布，$u'_{k-1}(t) \neq 0$因此上述影响被避免了。对于文献[75, 76]中的密码方案，密文$y(t-1)$近似服从均匀分布，一般不存在这个问题。
- **注释4**：有一个判断`P[i-1]`是否收敛到P_{i-1}次大值的等效方法：只需要判断`P[i-1]`是否明显小于P_{i-1}的最大值。这样的话，第二个阈值参数`e2[i-1]`可以被取消或者它的取值可以放宽松一些。
- **注释5**：为了避免得到错误的分辨率，我们建议引入一个稳定指示因子η。仅当`P[i]`和`P[i-1]`连续服从指定的条件至少η次时，才输出分辨率i。尽管η会使得所需的已知/选择明文数量有所增加(不过一般不大)，它有助于提高攻击的稳定性。

- **搜索密钥子空间V'_i**：以一个明文/密文对作为判断准则，在V'_i中搜索正确的密钥。搜索密钥的平均数量为$2^{i-2}/2 = 2^{i-3}$。

§4.4.3 增强穷举攻击的性能分析

在本小节中，我们来分析一下上一小节提出的增强穷举攻击的性能，这里我们假设密钥在整个密钥空间S'_n中均匀地随机选取，这在实际应用中是合理的。

1. **已知/选择明文的平均数量**：
   $$N_p = \sum_{i=2}^{n} \frac{2^{i-2}}{2^{n-1}-1} \cdot 2^{i-2} = \frac{2^{2n-1}-1}{3\cdot(2^{n-1}-1)} \approx \frac{2^{n-1}}{3}。$$
2. **搜索密钥的平均数量(搜索复杂度)**：
   $$N_k = \sum_{i=2}^{n} \frac{2^{i-2}}{2^{n-1}-1} \cdot 2^{i-3} = \frac{2^{2n-2}-1}{6\cdot(2^{n-1}-1)} \approx \frac{2^{n-2}}{3}。$$
3. **该攻击下的密钥熵**：
   $H(K) = \sum_{i=2}^{n} \frac{2^{i-2}}{2^{n-1}-1} \cdot (i-2) = \frac{(n-3)\cdot 2^{n-1}+2}{2^{n-1}-1} \approx n-3$，这比$n-1$小两个比特(简单穷举攻击下的密钥熵)。

由以上结论，我们可以看到该攻击的整体性能比简单穷举攻击好，但是所需的已知/选择明文数量有些大，并且密钥熵的改善并不是特别得理想。实际上，该攻击的重要性体现在下面两个事实上：1) 在使用很弱的密钥的情况下*，该攻击可以非常**有效**地攻击相关的密码系统；2) 数字化混沌系统的动力学特性退化带来的安全缺陷表明设计一个真正安全的数字化混沌密码相当困难。

*一般而言，分辨率不大于$n/2$的密钥都相当得弱。从最严格的观点出发，只有分辨率为n的密钥是不弱的，但是这样的密钥的数量只有全部密钥的一半。

§4.5 试验和仿真

为了验证本章前面给出的理论分析的正确性，我们做了一些试验测试前面给出的结论。试验数据和理论分析是完全一致的，证实了基于弱密钥的攻击方案的可行性。在试验中，混沌密码的相关参数选择如下：

- 有限精度$n = 10$(周红等人在[82]中也采用了这样的精度，采用较低的精度是为了简化试验设计并使得统计分析成为可能)；
- DATF选作$\text{floor}_n(\cdot)$；
- 混沌迭代的次数$k = n + 1 = 11$；
- 驱动m-序列的本征多项式[214]为$1 + x^3 + x^{10}$，初始状态为1；
- 一个m-序列发生器用来产生扰动信号，其本征多项式是$1 + x^2 + x^3 + x^8 + x^{10}$，初始状态为1；
- 被扰动的拟混沌轨道位数$n_m = 5$。

§4.5.1 扰动的性能

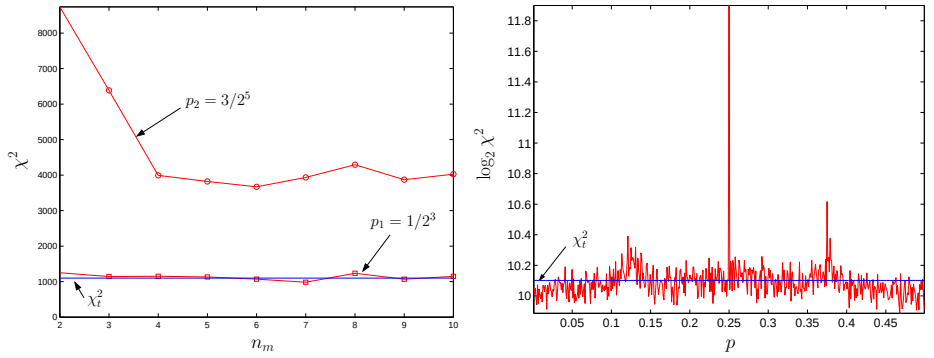
弱密钥的存在依赖于一个基本的条件：$u'_{k-1}(t)$近似满足离散均匀分布。首先，一些试验用来验证文献[82, 170]中给出的这方面的结论，即用来验证$u'_{k-1}(t)$是否满足离散均匀分布这个前提。

周红等人在文献[170]中给出了一个定性的规则确定所需的扰动位数：$n_m = \lceil \log_2(k_{max} + 1) \rceil$，不过这个估计值有点偏大，而且随着密钥的不同而变化(这使得扰动策略的实现变得过于复杂)。我们试图通过试验重新研究这个问题。我们发现如下事实：1) 扰动少量的比特就已经足够改善混沌输出的分布均匀性；2) 当n_m超过某个阈值之后，扰动的效果增加变得很缓慢；3) 密钥越弱，同一个n_m对分布均匀性的改善效果越差。当$n = 10$时，$n_m = 5$即可达到满意的效果。

当$n = 10, k = 11$时，我们对$u'_k(t)$进行了Pearson-χ^2测试[212]。测试参数为：显著性因子$\alpha = 5\%$，分区间数$m = 1024$，拒绝阈值$\chi^2_\alpha(m-1) = 1098.5$。当$p = 1/2^3, 3/2^5$时，不同的扰动位数$n_m$的效果显示在图4.4a中；当$n_m = 5$时，不同密钥的效果显示在图4.4b中。

§4.5.2 $P_2 \sim P_n$的估计值

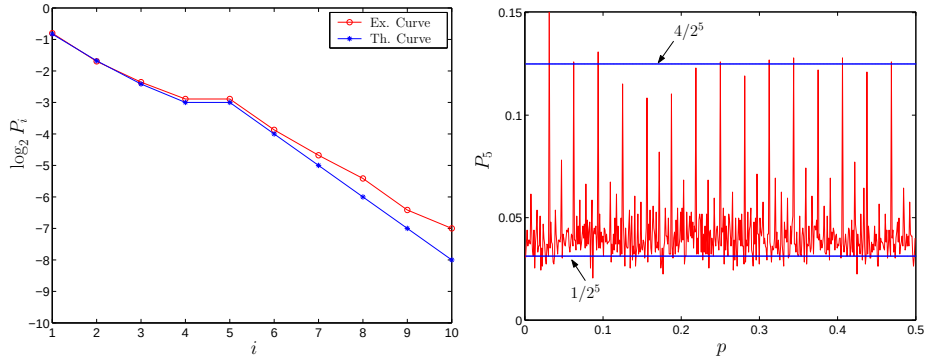
由于$u'_{k-1}(t)$在S'_n上近似满足离散均匀分布，由定理3.2和定理3.3，由$u_k(t)$计算出来的$P_2 \sim P_n$的估计值应当收敛到理论取值上去。当然，$u'_{k-1}(t)$的实际分布并不是严格的均匀分布，在`P[i]`$(i = 2 \sim n)$和理论值之间存在一定的差异。我们的试验表明这种差异足够小，不会影响密钥分辨率的区分度。



a) 不同扰动位数n_m的扰动效果　　b) 当$n_m = 5$时不同密钥的扰动效果

图 4.4: $u'_k(t)$的Pearson-χ^2测试

在图4.5中，我们给出了由$u_k(t)$计算出来的估计值和理论值之间的比较。将图4.5a、b和图3.1a和图3.3进行比较，可以看到估计值和理论值之间基本是吻合的。图4.5a显示当$p = 3/2^5$时试验曲线和理论曲线之间的差异是可接受的(请注意这里我们使用了对数坐标以放大差异的显示效果)。当i接近n时，与较小的i相比，这种差异变得较大，这是由于i比较大时的P_i值比较小，因而对$u'_{k-1}(t)$的不均匀性比i较小时的P_i更为敏感(考虑$i < j \rightarrow P_i > P_j$)。图4.5b显示在$P_5$的最大可能取值和次大可能取值之间存在足够大的差异，该差异对于确定密钥的分辨率是必需的。尽管对于所有分辨率为5的密钥而言，P_5存在一定的波动，但是这种波动并没有影响到密钥分辨率的判断。这种波动的存在也是两个阈值参数必须使用的原因。

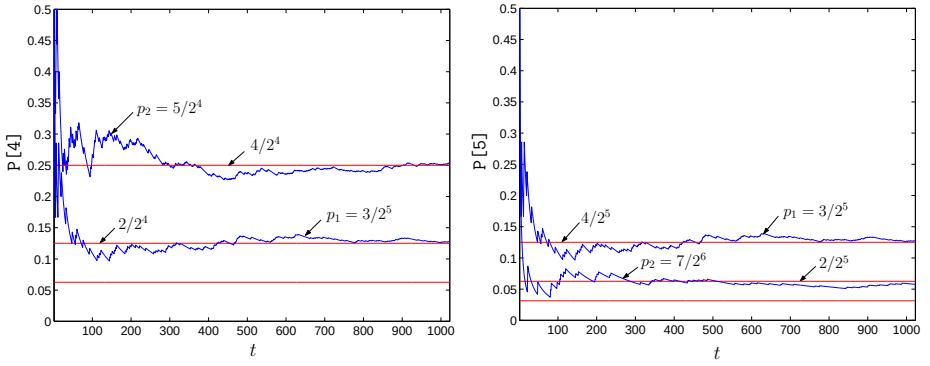


a) 当$p = 3/2^5$时$P_1 \sim P_n$的估计值　　b) 不同密钥下的P_5估计值

图 4.5: 由$u_k(t)$得到的$P_1 \sim P_n$的估计值和理论值的比较

§4.5.3 一个实际的攻击例子

最后，假设选用的密钥为$p = 3/2^5 \in V_5'$，我们给出了一个对周红等人密码[82]的实际攻击例子。图4.6a和图4.6b分别给出了P[4]和P[5]随着已知/选择明文数量增加而变化的曲线。可以看到经过一个短暂的过渡期后P[4]和P[5]就逐渐收敛到理论值$2/2^5$和$4/2^5$上去了(存在小的波动)。一旦P[5]和P[4]进入了阈值参数e1[5]和e2[4]限定的区间内η次，分辨率$i = 5$就可以确定了，然后在子密钥空间中的搜索就可以开始了。所需的观察明文数量大概为$O(2^5)$。作为比较，图4.6a中同时给出了$p = 5/2^4 \in V_4'$时P[4]的变化曲线，图4.6b中给出了$p = 7/2^6 \in V_6'$时的P[5]变化曲线。可以看到具有不同分辨率的密钥对应的曲线随着已知明文数量的增加而逐渐分离。



a) 相对t(已知明文数量)的P[4]变化曲线：$p = 3/2^5, 5/2^4$

a) 相对t(已知明文数量)的P[5]变化曲线：$p = 3/2^5, 7/2^6$

图 4.6: 对密钥$p = 3/2^5$的一个攻击实例

§4.6 可能的补救措施

为了避免弱密钥带来的安全缺陷，在本节中我们将讨论一些可能的补救措施以及它们的性能。不少措施也可以作为有益的设计原则增强其他数字化混沌密码的安全性。对每种补救措施，我们在标题中使用一个词“是”、“否”或者“不定”来表明我们对该措施在实际应用中的建议。

§4.6.1 使用更高的有限精度：否

似乎增大有限计算精度是增强数字化混沌密码安全性的最简单最方便的方法。由我们在前面给出的讨论，可以看到更高的有限精度可以使得密钥熵变大。但是，正如我们在§4.4.1指出的那样，当我们将有限精度由n增加到n'时，整体安全性的增加是通过引入$n' - n$个新的子密钥空间实现的，在原精度下的所有弱密钥一点都不能得到增强。

另外一些线索暗示更高的精度甚至可能使情况变得更糟。当扰动策略没有被使用时，试验显示我们在§4.3中分析的弱密钥不能随着有限精度n的增加而得到有效地改善。图4.7中给出了密钥分别为$p = 3/8$，$1/16$和$13/64$时的弱密钥因子随n的变化曲线。可以看到随着n的增大，$\alpha(n, n+1, p)$反而变得越来越大。

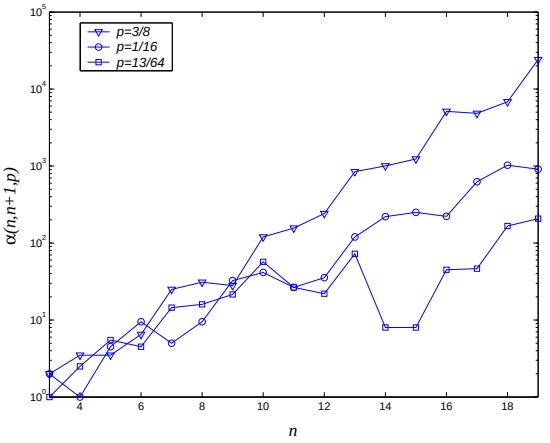


图 4.7: $\alpha(n, n+1, p)$相对$n = 6 \sim 19$的变化曲线(Y轴采用了对数坐标)

因此我们认为使用更高的有限精度不是一个根本的补救措施。

§4.6.2 使用更复杂的混沌系统：不定

我们知道，周红等人的密码中的弱密钥的存在依赖于数字化PWLCM在有限精度下的动力学特性退化。那么如果使用其他的混沌系统能否增强相关密码的安全性呢？或许这是一个根本的解决方案。当然了，使用的混沌系统必须满足PWLCM(2.1)具有的优良的动力学特性。一个可能的候选系统是文献[92]中提出的逐段非线性混沌映射：

$$F(x) = \begin{cases} \frac{1}{a_i}\left(\sqrt{4a_i\left(\frac{x-c_i}{c_{i+1}-c_i}\right) + (1-a_i)^2} - 1\right), & x \in [c_i, c_{i+1}) \\ 1, & x = 1 \\ F(-x), & x \in [-1, 0) \end{cases}, \tag{4.4}$$

这里$0 = c_0 < c_1 < \cdots < c_N = 1$，$a_i \in (-1, 0) \cup (0, 1)$并且$\sum_{i=0}^{N-1}(c_{i+1} - c_i) \cdot a_i = 0$。已经知道上述映射具有均匀的不变分布$f(x) = 0.5$[92]，这是周红等人的密码中使用的PWLCM(4.1)的一个重要特点。这样的一个映射可行吗？要回答这个问题并不那么容易。由于数字化PWLCM(2.1)中存在的动力学特性退化在其他数字化混沌系统中也存在(回顾§2.5中的讨论)。因此，从本质上讲，使用任何复杂的混沌系统并不能避免动力学特性退化。由于目前还没有一个关于数字化混沌系统动力

学特性退化的完整理论，选择一个“真正”比PWLCM(2.1)好的混沌系统并不那么简单。另外，更复杂的混沌系统的使用会加重运算负担，进而影响加解密速度和增加实现成本。在更可信的理论证据出现之前，在使用复杂的混沌系统问题上我们必须非常小心。

§4.6.3 使用秘密的扰动参数：是？

我们在前面已经提到，仅当扰动策略的细节已知时，攻击者才有可能从密钥流得到$u_k(t)$进而计算出$P_2 \sim P_n$来判断密钥的分辨率。

因此，如果我们掩盖了扰动算法的相关细节，相关混沌密码的安全性可能得到改善。由Kerckhoffs原则[143, 144]，扰动算法本身不可能是保密的，我们必须将相关的扰动参数设置为秘密的，如$P_2 \sim P_n$的种子，扰动PRNG的参数以及被扰动的位数。但是，使用这样一种措施，一旦攻击者得到了关于扰动的部分子密钥，他/她还是可以对剩余的部分密钥实施攻击。因此，我们必须想办法取消这两部分密钥之间的相关性。一个可能的措施是使用一个单独的密钥同时产生混沌系统的初始条件/控制参数和扰动PRNG的秘密参数，这里生成的扰动PRNG的参数字长最好不要比密钥字长小。

§4.6.4 隔离拟混沌轨道和密钥流：是？

我们已经知道从$k(t) = u'_k(t)$中去掉最后一轮扰动信号而得到$u_k(t)$的可能性是导致周红等人的密码安全性缺陷的实际原因。因此增强其安全性的一个自然的想法是在掩盖明文之前将$u'_k(t)$和$k(t)$隔离，也就是说，使得$k(t) = F_{ins}(u'_k(t)) \neq u'_k(t)$，这里$F_{ins}(\cdot)$是一个非线性隔离函数。如果隔离函数选择得当使得$u_k(t)$的具体值被成功地掩盖(从攻击者的角度看)，则从$k(t)$计算$P_i$的可能性就会马上被禁止掉。有很多种办法可以实现这样一个功能：使用非线性原则从拟混沌轨道生成伪随机密钥流[78, 98]，组合多个混沌系统的逆混沌轨道产生密钥流[22, 71]，对$k(t)$的比特进行伪随机置换，将拟混沌轨道转换为其他伪随机模式[106, 112]，等等。当然，使用这样一个方法实际上使得混沌密码的安全性主要依赖于隔离算法而不是混沌系统本身。还需要更进一步的研究以确认上述隔离策略是否会带来其他安全缺陷。

§4.6.5 避免使用弱密钥：是

另外一个简单的补救措施是避免所有弱密钥的使用。从最严格的观点出发，只有分辨率为n的密钥是不弱的，密钥应当从V'_n中均匀地随机选取，而不是从S'_n中。这样的话，对简单穷举攻击的密钥熵由$n-1$降低为$n-2$，由于分辨率是固定的对本章提出的增强穷举攻击的密钥熵也仍然是$n-2$。

当n较大时，我们可以放松只有分辨率为n的密钥这个严格条件，而只是避免使用“很弱”的部分密钥，比如我们可以只避免使用分辨率低于$n/2$的密钥。这

样一种放松的条件实际上是提供了一个抗击基于弱密钥攻击的安全性的下限。

这个方法的缺点是牺牲了不少可用的密钥，因此是一种比较消极的措施。但是该方法的简便性使得它成为实际应用中一种很有效和可行的方案。在其他措施的性能被证实之前，我们推荐使用该方法。

§4.6.6 同时扰动混沌轨道和控制参数：是

文献[199]中建议通过扰动控制参数的办法改善数字化混沌系统的动力学特性退化。在§3.4.1中我们已经知道这样一种扰动策略不如扰动混沌轨道效果更好。不过，在这里我们可以结合两种不同的扰动方法以增强周红等人密码的安全性。对控制参数的扰动用来混淆n个观察指标值$P_1 \sim P_n$对于密钥分辨率的可区分性。我们认为这个方法在实际中也是可行的。

§4.7 本章小结

本章讨论了周红等人在文献[75, 76, 82]中提出的一类混沌密码的安全性问题以及可能的补救措施。本章的讨论强调了在数字化混沌密码设计中的两个问题：1) 数字化混沌系统的动力学特性退化必须通过适当的方式加以改善以防止密码安全性的退化，混沌系统在连续域看起来很棒的动力学特性并不能保证相关密码在数字世界中的安全性；2) 甚至在采用了一些措施改善动力学特性退化的情况下，仍然可能存在一些威胁系统安全性的漏洞。第二个问题意味着对数字化混沌密码设计而言，数字化混沌系统的理论研究是非常重要的。

第五章 基于搜索机制的数字化混沌密码的分析

§5.1 引言

在§2.4.1中，我们已经对基于搜索机制的数字化混沌密码[84, 90, 104, 110, 113–116, 122, 123, 128]及相关的密码分析工作[97, 100, 126]给出了一个简要的介绍。本章将介绍我们关于这类密码的下述工作：1) 如何增强E. Alvarez等人的密码[90]以抵抗G. Alvarez等人提出的攻击[97]；2) 对M. S. Baptista密码[84](以及其他几种类似的密码[104, 110, 113, 114, 122, 123])的Jakimoski-Kocarev攻击[100]的观点；3) 改进M. S. Baptista密码(及其他类似密码)以抵抗所有的已知攻击[100, 126]。

本章可以分为两个大的部分，分别讨论E. Alvarez等人的密码和M. S. Baptista的密码。在第一部分中，我们讨论了E. Alvarez等人的密码为什么不能抗击G. Alvarez等人的攻击*，并提出了一种增强方案以抵抗G. Alvarez等人提出的所有攻击。在第二部分中，我们给出了Jakimoski-Kocarev攻击M. S. Baptista密码的实际性能分析，并提出了一种改进措施以有效地抵抗Jakimoski-Kocarev攻击；由于文献[126]中提出的基于符号动力学的攻击依赖于与Jakimoski-Kocarev攻击类似的条件(混沌迭代次数在密文中出现)，因此这种改进措施也可以抵抗这样的攻击。

本章的组织如下所述。在§5.2中我们通过分析E. Alvarez等人的密码的两种本质缺陷(对其他的次要缺陷也做了一定讨论)，解释了为什么该密码对相关攻击不安全。一种对E. Alvarez等人密码的改进方案及其详细分析在§5.3中给出。理论分析和试验都表明改进方案满足良好的密码学特性(当然，还需要更多的研究去证实其安全性)。在§5.4中，我们对M. S. Baptista的密码给出一个较为细致的介绍以方便后文的讨论。Jakimoski-Kocarev攻击和我们关于该攻击性能的讨论在§5.5中给出。一种抵抗Jakimoski-Kocarev攻击和其他攻击的改进措施在§5.6讨论。最后一节是本章小结。

§5.2 E. Alvarez等人的混沌密码及其本质缺陷

§5.2.1 一个简单的介绍

E. Alvarez等人的密码是一种对称的分组密码，它将每个明文分组加密为一个三元密文组。与普通的分组密码不同，它的分组大小是时变的。基于一个d维的混沌系统$x_{n+1} = F(x_n, x_{n-1}, \cdots, x_{n-d+1})$，加密和解密流程如下所述。首先，选择混沌系统的控制参数作为密钥，以及一个整数b_{max}作为明文的最大分组大小。对于一个大小为$b_i = b_{max}$的明文分组，选择一个阈值参数U_i，按照下述规则从拟混沌轨道$\{x_n\}$产生一个比特链C_i：$x_n \le U_i \to 0$，$x_n > U_i \to 1$。在C_i中

*文献[97]的作者们并未显式地给出他们提出的攻击成功的原因。

搜索当前明文分组第一次出现的位置，记录$(U_i, b_i, \mathbf{X}_i)$作为对应的密文分组，这里$\mathbf{X}_i = (x_i, x_{i-1}, \cdots, x_{i-d+1})$表示在该位置混沌系统的当前状态。如果当前明文分组在很长一段C_i中都不能找到，$b_i = b_i - 1$然后搜索过程重新开始直到密文生成为止。tent映射(2.5)被用来演示该密码的性能，控制参数r被选作密钥。

然而，仅在上述密码提出几个月以后，G. Alvarez等人指出：当tent映射(2.5)被使用时，该密码很容易被攻破。在他们的文章中，G. Alvarez等人提出了四种不同的攻击，分别属于选择密文攻击，选择明文攻击，已知明文攻击和唯密文攻击。他们也指出了该混沌密码中存在的一些其他缺陷。作为一个结论，即使使用其他混沌系统替代tent映射，G. Alvarez等人认为该混沌密码完全是不安全的。在后面的小节中，我们将分析E. Alvarez等人密码中的两个本质缺陷，这是这两个缺陷使得该密码不安全。

§5.2.2 缺陷一：X_i在密文中的出现

第一个本质缺陷是$\boldsymbol{X}_i$在密文中的出现。考虑该密码中使用的混沌系统的动力学特性不仅依赖于密钥(控制参数)，也依赖于初始条件，攻击者可能从$\boldsymbol{X}_i$中得到一些有用的信息以降低攻击复杂度。

实际上，在E. Alvarez等人的密码中确实存在信息泄漏，泄漏概率$P_l \geq E(1/b_i)$，这里$E(x)$表示x的数学期望。显然，由于$b_i \leq b_{max}$，可知$P_l \geq E(1/b_i) \geq 1/b_{max}$。给定一个密文分组$(U_i, b_i, \mathbf{X}_i)$，让我们来看看明文分组$P_i = P_{i,0}P_{i,1}\cdots P_{i,b_i-1}$的$b_i$个比特是如何被加密的，而有关明文的信息又是如何泄漏的。由于合法用户是知道密钥(控制参数)的，他们可以从$\boldsymbol{X}_i$得到b_i个混沌状态$\{x_{i+j}\}_{j=0}^{b_i-1}$。然后明文分组$P_i$就可用从$\{x_{i+j}\}$以及阈值参数$U_i$按照如下规则恢复：

for $j = 0$ to $b_i - 1$ do
    if $x_{i+j} \leq U_i$ then $P_{i,j} = 0$
    else $P_{i,j} = 1$
end

显然，即使不知道密钥，也可以通过比较x_i和U_i而直接得到b_0。所以，非法用户在唯密文攻击下总是可以得到每个明文分组中的b_0。也就是说，至少$1/b_i$的明文分组信息通过密文分组泄漏了出来。总的来说，信息泄漏的概率P_l不会小于$E(1/b_i) \geq 1/b_{max}$。一般b_{max}不会很大，否则加密速度会变得非常慢，这样信息泄漏就会变得过大而使得该密码在安全应用中不够安全。

另外，如果攻击者知道了密钥r的近似值r'，他/她就可以从$\boldsymbol{X}_i$出发使用符号动力学对明文进行猜测。r'越接近r，猜测成功的概率越高。这个事实意味着该混沌密码对密钥不够敏感，这对于一个好的密码系统是不希望出现的[143, 144]。文献[97]的作者使用这样一个事实提出了一种唯密文攻击($r' = 2$)。当密钥接近2时，他们发现这样的一种猜测可以相当高的概率揭示明文分组。当然，随着真实的密钥r逐渐远离2，猜测成功的概率也会下降，但是我们需要记住对任何密钥而言该

混沌系统的信息泄漏都不会低于$1/b_{max}$这个事实。

还有，文献[97]中提出的选择密文攻击也是基于$\boldsymbol{X}_i$在密文中出现从而可以提供关于密钥的部分信息这个事实。通过选择$\boldsymbol{X}_i$使之足够接近0并观察明文的变化，攻击者可能在很短的步骤内得到密钥。

§5.2.3 缺陷二：使用不同密钥时混沌系统具有不同的动力学特性

对于tent映射(2.5)而言，使用不同的密钥(控制参数)时其动力学特性是完全不同的，一些动力学指标被控制参数r(密钥)唯一确定。这样的动力学指标包括：拟混沌轨道访问的区间，Lyapunov指数，Kolmogrov熵以及不同控制参数下不同周期窗口的出现[207, 208, 210, 215]。由于这种动力学的差异可以从一定数量的密文中的$\boldsymbol{X}_i$提取出来，它可以用来设计一些可能的攻击方法。

如文献[97]中描述的那样，不同密钥时拟混沌轨道的不同访问区间很容易用来实现已知/选择明文攻击。当控制参数为r时，拟混沌轨道的访问区间为$[r(1-r/2), r/2]$。在已知足够多密文的情况下，攻击者可以得到访问区间的近似上下限，从而得到密钥的近似值。而我们在前面已经讲到，该混沌密码对密钥不那么敏感，因此近似的密钥值就可以用来以足够高的成功概率解密密文。当然，攻击者也可以在近似值附近的一个小范围内穷举搜索密钥的精确值，这比搜索这个密钥空间所需的复杂度要低得多。

由于$\boldsymbol{X}_i$必须已知才能进行上述的密文统计，文献[97]中的选择明文攻击和已知明文攻击同时依赖于该混沌密码的两个缺陷。因此，如果第一个缺陷被避免，文献[97]中的所有攻击都会变得不可行。但是为了避免可能的其他潜在攻击，我们认为两种缺陷都应当尽可能地避免。

§5.2.4 其他缺陷

G. Alvarez等人在文献[97]中也提到了一些其他缺陷：使用了过低的有限精度，关于如何选择初始状态和密钥缺乏具体的描述，密钥对密文的敏感性不强。最后一个缺陷我们在§5.2.2中也提到了。其他的缺陷对于原密码都不是那么重要，可以通过仔细的实现细节来解决。

除了以上缺陷，原混沌密码系统中还存在另外一个严重的问题，就是它的加密速度太慢。很明显加密速度主要由C_i中明文分组的搜索过程决定。假设C_i在{0,1}上是平衡，那么每个明文分组在某个位置上出现的概率为$1/2^{b_i}$，因此搜索过程可以看做是基本概率为$p = 1/2^{b_i}$的Bernoulli试验。试验所需的次数满足几何分布，其数学期望为2^{b_i}[212]。如果C_i是不平衡的，所需的平均试验次数会比2^{b_i}大。b_i不会很小以防止穷举攻击，也不能很大以防止加密速度变得过慢(和其他传统密码比较起来)。另外，b_i太大会使得$b_i = b_i - 1$的发生概率变大而使得加密速度进一步变慢。这样一种矛盾使得b_{max}的选择变得困难。在原密码方案中，$b_{max} = 16$，这个数值有点小可能带来潜在的安全问题，又有点大使得加密速度变得相当慢。

§5.3 E. Alvarez等人的混沌密码的一种改进方案

在本节中我们提出一种E. Alvarez等人密码的改进方案。该方案可以避免前面提到原密码方案的缺陷，因此可以抵抗所有G. Alvarez等人提出的攻击，具有更好的性能。试验证实该改进方案的密码学特性是相当不错的。

§5.3.1 描述

不失一般性，我们采用一维混沌映射构造新的密码系统。给定一个定义在区间$I = [a, b]$上的映射$x_{n+1} = F(x_n, p)$，这里p是控制参数。要求该映射满足下述条件：它在I上是遍历的，并且具有均匀的不变分布函数[23]。以上条件是为了避免前面提到的第二个缺陷，也可以使得统计密码分析变得困难。PWLCM是满足这样条件的混沌映射，比如斜tent映射(2.3)和一维PWLCM(2.1)。这里请注意tent映射(2.3)和原密码方案中采用的tent映射(2.5)是完全不同的(尽管它们都称为tent映射)。

基于一个满足上述条件的混沌映射，改进密码方案如下所述。请注意该改进方案和M. S. Baptista是相似的*：迭代次数被用作密文的一部分。

- *密钥*：$K = (x_0, p)$，这里x_0是混沌映射的初始条件。
- *输入 – 明文*：$P_1 P_2 \cdots P_i \cdots$，这里$P_i$的大小为$b_i \le b_{max}$。
- *加密过程*：和原方案很类似。对于大小为$b_1 = b_{max}$的第一个明文分组P_1，从x_0迭代运行混沌映射，选择一个阈值参数U_1以与原密码方案相同的规则产生一个比特链C_1。在C_1中找到P_1出现的位置，记录(U_1, b_1, n_1)作为密文分组，这里n_1表示自x_0开始的混沌映射迭代次数。如果P_1在很长一段时间内都无法在C_1中找到，$b_1 = b_1 - 1$搜索重新开始。对于第二个以及后面的其他明文分组，加密过程和第一个基本完全相同，只是混沌映射不再是从x_0开始迭代，而是从上个密文分组输出时的状态开始。
- *输出 – 密文*：$(U_1, b_1, n_1), (U_2, b_2, n_2), \cdots, (U_i, b_i, n_i), \cdots$。实际上，阈值参数$U_i$可以是固定的，这样密文就被简化为$(b_1, n_1), (b_2, n_2), \cdots, (b_i, n_i), \cdots$。一般而言，阈值参数应当选择为使$C_i$平衡的数值，即使得$P\{C_i = 0\} = P\{C_i = 1\}$。这可以从混沌映射的不变分布推导出来。对于前面提到的两种PWLCM，建议阈值是0.5，即定义域$I = [0, 1]$的中点。
- 对于知道密钥的合法用户而言，*解密过程*是相当容易的，对每个密文分组重新产生正确的C_i即可。

*尽管我们提出的改进方案可以看作是E. Alvarez等人的原密码方案和M. S. Baptista密码的一个结合，实际上与M. S. Baptista密码类似的想法是我们独立提出的。当我们在2001年7月向*Physics Letters A*投寄文章[110]时，我们还没有得到[84]的拷贝并阅读其内容。

可以看到，在该改进方案中原密码方案的两个缺陷都被避免了。另外，与原密码方案不同，改进方案更像是一个流密码而不是分组密码。这个事实使得我们可以在密码中使用较小的b_{max}，从而从一定程度上缓解了安全性和加密速度之间的矛盾。

正如我们在§2.5.2中建议的，数字化混沌系统的动力学特性退化应当使用扰动方法加以改善。显然扰动不能太大以防止破坏原数字化混沌系统的本征动力学特性。不过对于上述的改进混沌密码而言，混沌系统只是用来产生不可预测的、平衡的、具有足够长周期的伪随机比特链，而混沌系统本身的确切动力学是否保持并不那么重要。这意味着扰动信号可以稍微大一些。实际上，我们的试验表明：扰动信号越大，试验结论和理论分析吻合得越好，搜索过程也会越快(加密速度越快)。这是由于较大的扰动信号会使得拟混沌轨道的分布变得更为均匀，从而使得生成的伪随机序列更加理想。因此我们建议使用较大的扰动信号而不是较小的扰动信号，这样扰动后的混沌系统成为一个由数字化混沌和扰动PRNG的伪随机性构成的超复杂的非线性动力系统。这里，混沌系统的非线性保证了系统的安全性，扰动PRNG则通过平滑退化的拟混沌轨道保证了伪随机比特链的理想特性。

§5.3.2 密码学特性

首先，我们先给出如下声明：由于密文中的b_i只是用来指示对应明文分组大小的，我们在后文中将只把n_i看作是“真正”的密文。

我们知道，好的密码的两个主要密码学特征是混淆和散布，在传统密码学中它们一般通过密文的平衡性和雪崩效应来实现[143, 144]。但是我们提出的改进密码方案有着不同的特点：密文是不平衡的，n_i越大，它在密文中出现的概率也越小。假设C_i是平衡的i.i.d.(独立同分布的)比特序列，搜索过程可以看成是基本概率为$1/2^{b_i}$的Bernoulli试验；则我们可以推出n_i的离散分布列：

$$P\{n_i = k\} = \frac{1}{2^{b_i}} \cdot \left(1 - \frac{1}{2^{b_i}}\right)^{k-1}, \tag{5.1}$$

对于不同的密钥和明文该分布列在理论上是独立而且相同的。

那么这种不平衡的特点如何使得该改进密码方案实现混淆和散布的呢？事实上，上述密文分布存在下面四个有关事实：1) 对于不同的明文，密文具有相同的离散分布列；2) 对于不同的密钥(控制参数和初始条件)，密文具有相同的离散分布列；3) 对于两个仅有一比特差异的明文，密文是完全不同的；4) 对于两个仅有一比特差异的密钥而言，密文也是完全不同的。前两个事实对应着混淆，而后面两个事实对应着散布。

由于我们的改进密码方案可以克服原方案中的本质缺陷，而且具有良好的混淆和散布特性，与原系统相比我们可以使用较小的b_{max}。因此加密速度会变得快一些。但是，由于耗时的搜索操作仍然被使用，加密速度仍然要比大部分传统密码要慢。假设混沌迭代的速度是每秒执行s次迭代；则平均加密速度将是$s \cdot E(b_i)/E(n_i) \approx s \cdot b_{max}/2^{b_{max}}$ bps (比特/秒)。因而，这样一个混沌加密系统

只能用在非实时应用中，比如网络上的短消息传输或者计算机上的小文件的安全存储。当然，当$b_{max}=1,2$，加密速度会变得很快：大概$s/2$ bps。但是，需要进一步的研究去发现使用如此小的b_{max}可能带来的安全隐患。

最后，让我们看看该改进方案的密钥熵。当有限精度为n比特时，控制参数和初始条件都表示为定点二进制小数，因此密钥熵为$2n$。在大部分计算机中n可以选择为32或者64，这样密钥熵即为64或者128，这对于一个安全的密码基本上已经足够。如果需要更高的安全性，可以考虑使用更大的n。

§5.3.3 加密后压缩密文

该密码系统中存在一个不是太要紧的问题：密文的大小比明文大小大得多(当$n_i \leq 2^{bmax+1}$时超过两倍)。压缩密文可以解决这个问题。由于密文是不平衡的，那么可以使用基于统计的无损压缩技术对它进行压缩，如Huffman编码[216]。首先，将密文分为两个不同的比特流：$b_1b_2\cdots b_i\cdots$和$n_1n_2\cdots n_i\cdots$。然后分别使用Huffman编码压缩这两个比特流。根据方程(5.1)，对于比特流$n_1n_2\cdots n_i\cdots$，压缩后的密文分组平均大小为b_{max}。对于比特流$b_1b_2\cdots b_i\cdots$，由于每个b_i都以较大的概率等于b_{max}，压缩后的密文分组平均大小接近1。这样，整个压缩的密文分组的平均大小接近$b_{max}+1$，只比明文分组的最大长度多一个比特。

§5.3.4 试验结果

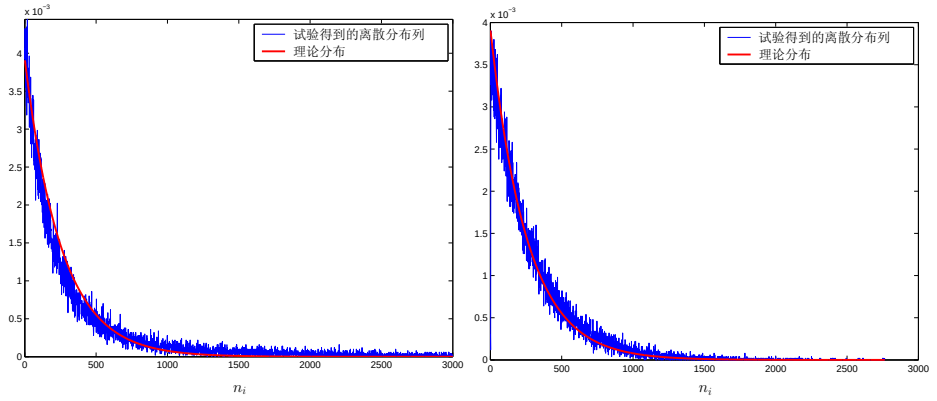
基于tent映射(2.3)，我们建立了一个试验密码系统以测试其密码学特性。这里有限精度为$n=32$比特，$b_{max}=8$，扰动PRNG是一个最大长度LFSR(m-LFSR)，其阶数为n，本征多项式为$1+x+x^{27}+x^{28}+x^{32}$[214]。扰动间隔$\Delta=n$*，扰动m-LFSR的所有比特都用来扰动拟混沌轨道。

如我们前面提到的，n_i的理论离散分布列如方程(5.1)所示。图5.1a给出了当明文离散均匀分布时的试验数据和理论曲线的对照。当明文为59 59 $\cdots$ 59 $\cdots$时，试验结果在图5.1b中给出。加密明文的数量为50,000。当密钥(控制参数和初始条件)随机地选择为不同的数值时，可以得到类似的结果。这样，混淆特性被证实了。

其他试验用来测试散布特性。当明文、控制参数和初始条件分别具有最小差异时，两个相应密文中n_i的差值显示在图5.2a–c中。相关参数的最小差异如下所示：

- 明文之间的最小差异(参看图5.2a)：**195** 195 $\cdots$ 195 $\cdots$和**196** 195 $\cdots$ 195 $\cdots$；
- 控制参数之间的最小差异(参看图5.2b)：$p_1=\mathbf{31849}/2^{32}$和$p_2=\mathbf{31848}/2^{32}$；

*注意$\gcd(\Delta,2^n-1)=1$，这对于获得最大长度的比特序列C_i是有好处的。



a) 明文离散均匀分布时n_i的试验分布　b) 明文固定为59 59 $\cdots$ 59 $\cdots$时n_i的试验分布

图 5.1: n_i的离散分布列：试验与理论对照

- 初始条件的最小差异(参看图5.2c)：$x_{0,1} = \mathbf{40332}/2^{32}$和$x_{0,2} = \mathbf{40333}/2^{32}$。

§5.4 M. S. Baptista的混沌密码及其改进版本

在本节我们使用一种不同于原始文献[84]中的描述方法对M. S. Baptista的混沌密码及其改进版本给出一个详细的介绍，以使后文关于Jakimoski-Kocarev攻击的描述和分析更为明了。给定一个一维混沌映射$F: X \to X$，将一个子区间$[x_{min}, x_{max}) \subseteq X$划分为$S$个$\epsilon$-区间$X_1 \sim X_S$：$X_i = [x_{min} + (i-1)\varepsilon, x_{min} + i\varepsilon)$，这里$\varepsilon = (x_{max} - x_{min})/S$。假设明文消息由$S$个不同的字符$\alpha_1, \alpha_2, \cdots, \alpha_S$组成，使用一个双射

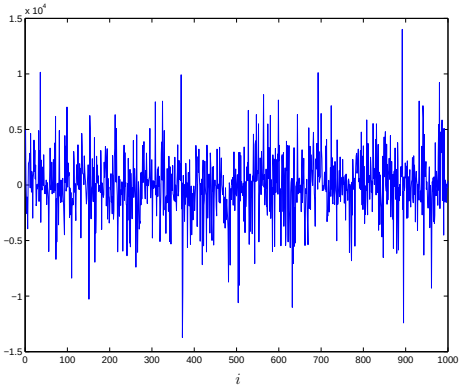
$$f_S : \boldsymbol{X}_{\boldsymbol{\epsilon}} = \{X_1, X_2, \cdots, X_S\} \to \boldsymbol{A} = \{\alpha_1, \alpha_2, \cdots, \alpha_S\} \tag{5.2}$$

将不同的ϵ-区间和不同的字符关联起来。定义一个新的函数$f'_S : X \to \boldsymbol{A}$：如果$x \in X_i$，则$f'_S(x) = f_S(X_i)$。

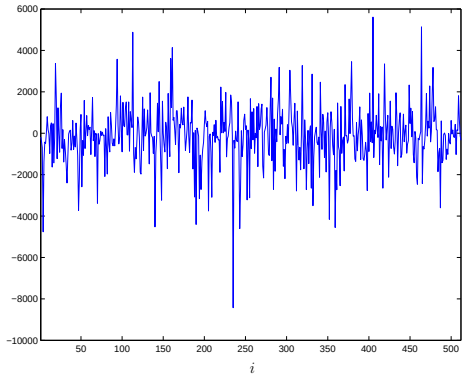
给定一个明文消息$M = \{m_1, m_2, \cdots, m_i, \cdots\}(m_i \in \boldsymbol{A})$，M. S. Baptista的密码可以描述如下：

- 混沌系统：Logistic映射$F(x) = rx(1-x)$。
- 密钥：关联映射S^*，Logistic映射的初始条件x_0以及控制参数r。
- 加密过程：

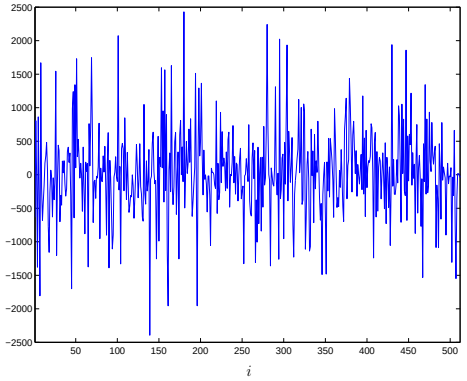
*从实现和Kerckhoffs原则[143, 144]的角度考虑，我们认为该映射f_S不应当用作密钥的一部分。



a) 两个具有最小差异的明文对应的n_i差值



b) 两个具有最小差异(2^{-n})的控制参数对应的n_i差值



c) 两个具有最小差异(2^{-n})的初始条件对应的n_i差值

图 5.2: 两个不同密文中的n_i差值

  - 第一个明文字符m_1：从x_0开始迭代混沌系统寻找一个满足$f'_S(x) = m_1$的混沌状态x，记录迭代次数C_1作为第一个密文消息单元，并计算$x_0^{(1)} = F^{C_1}(x_0)$；
  - 第i个明文字符m_i：从$x_0^{(i-1)} = F^{C_1+C_2+\cdots+C_{i-1}}(x_0)$开始迭代混沌系统寻找一个满足$f'_S(x) = m_i$的混沌状态$x$，记录迭代次数$C_i$作为第$i$个密文消息单元，并计算$x_0^{(i)} = F^{C_i}\left(x_0^{(i-1)}\right)$。

- 解密过程：对于每个密文单元C_i，从上一次混沌状态$x_0^{(i-1)} = F^{C_1+C_2+\cdots+C_{i-1}}(x_0)$开始迭代混沌系统$C_i$次，使用$x_0^{(i)} = F^{C_i}\left(x_0^{(i-1)}\right)$和关联映射$f_S$导出明文字符$m_i$。

- C_i的限制：每个密文消息单元C_i应当满足约束$N_0 \leq C_1 \leq N_{max}$(在文献[84]中$N_0 = 250$，$N_{max} = 65532$)。由于在$[N_0, N_{max}]$中存在许多可选

的C_i值，一个额外的参数$\eta \in [0,1]$用来选择一个合适的值：如果$\eta = 0$，则C_i选作满足$f_S^t(x) = m_i$的最小迭代次数；如果$\eta \neq 0$，C_i选作同时满足$f_S^t(x) = m_i$和$\kappa \geq \eta$的最小迭代次数，这里κ是一个在区间$[0,1]$上满足正态分布的伪随机小数。

- *一个吹毛求疵的注解*：在文献[84]中，M. S. Baptista没有提到一旦出现$C_i > N_{max}$我们应该怎么办。看起来M. S. Baptista认为C_i永远不可能大于N_{max}。但是，从严格的观点来看，我们不这样认为。这里，假设$F(x)$以均匀的概率$p = 1/S$访问每个ϵ-区间，我们可以得到：

$$P\{C_i > N_{max}\} = P\{C_i - N_0 > N_{max} - N_0\} = (1-p)^{N_{max}-N_0}。 \tag{5.3}$$

图5.3给出了上述概率值相对$N_{max} - N_0$的曲线。可以看到，在IEEE双精度浮点算法下[217]，当$N_{max} - N_0$超过10000后该概率值下溢为0。但是，尽管当N_{max}足够大时该概率值非常小，它仍然不等于0。为了使得该密码在严格的意义上没有缺陷，我们加入这样一条规则到上述的加密/解密过程中去：当$C_i = N_{max}$，密文是一个二元组(N_{max}, m_i)。由于$P\{C_i > N_{max}\}$足够小，这样一个微小的信息泄漏不会带来任何安全问题。当然，如果使用的N_{max}足够大，我们认为丢弃这个吹毛求疵的附加规则也是可行的。在后文中，我们将始终假设N_{max}足够大，从而使得$P\{C_i > N_{max}\} = 0$在概率意义上是正确的(该假设将在§5.6中使用)。

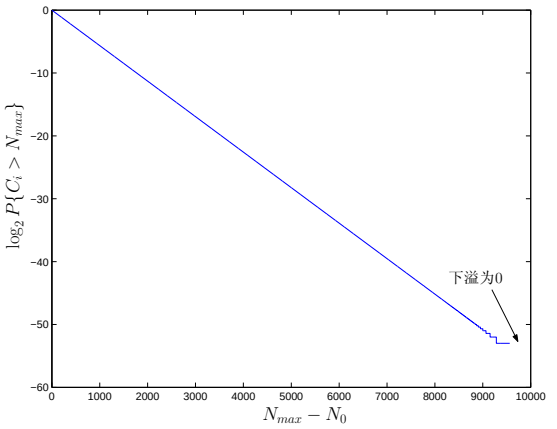


图 5.3: $P\{C_i > N_{max}\}$相对$N_{max} - N_0$的变化曲线

上述混沌密码有两个缺陷：a) 密文的分布不是平衡的，C_i的出现概率随着其值自N_0增加到N_{max}成指数衰减；b) 加密每个明文字符至少需要N_0次混沌迭代，这使得加密速度相比其他传统密码而言太慢了。

在文献[104]中，W.-K. Wong等人改进了上述密码系统：对于每个明文字符m_i，首先生成一个在0和r_{max}(一个预先定义的整数)之间离散均匀分布的伪

随机整数r_C，迭代混沌系统r_C次，然后继续迭代它直到找到一个混沌状态x满足$f_S^t(x) = m_i$，记录迭代次数C_i作为当前的密文消息单元。这样一种改进的密码系统避免了原密码系统的第一个缺陷，但是第二个缺陷却变得更糟了(平均而言，加密每个明文字符需要多得多的混沌迭代从而使得加密速度进一步变慢)。在文献[114]中，K.-W. Wong建议动态更新关联映射f_S(在K.-W. Wong文中称为查找表，Look-Up-Table)以提高加密速度。但是一定数量的混沌迭代仍然是需要的，因此加密速度仍然比一般的传统密码慢得多。一个很新的进展还是由K.-W. Wong等人在文献[123]中给出的，在该文中一个会话密钥被引入以实现发送端和接受端混沌系统之间的同步，在经过一个多次迭代的同步期之后，加解密过程才开始。这篇文章的主要贡献是采用下述办法有效地减小了密文大小：将密文中的C_i替换为每个明文字符在动态查找表中的索引值。

§5.5 Jakimoski-Kocarev攻击及其性能分析

§5.5.1 Jakimoski-Kocarev攻击

在文献[100]中，G. Jakimoski和L. Kocarev提出了一种针对M. S. Baptista的原始密码的已知明文攻击。该攻击基于如下事实：通过观察明文/密文对，攻击者可以得到密文的“感兴趣时刻”(moment of interest)和明文字符之间的一张关联表，这里一个密文单元C_i的“感兴趣时刻”定义为$n = \sum_{j=1}^{i} C_j$(自x_0开始的混沌迭代总次数)。该关联表可以用来解密部分明文，如果其对应密文的“感兴趣时刻”n在该表中再次出现。在文献[100]中给出了一个具体的例子说明这种攻击：假设两个明文消息“subject”和“to”已知，它们分别被加密为*272 258 305 285 314 276 422*和*254 267*。这样，攻击者可以得到表5.1中所示的关联表。使用这个关联表，攻击者可以解密部分明文，如果对应密文的“感兴趣时刻”出现在该表中。比如，一个密文*272 249*可以马上被解密为“so”(*272*意味着“s”，$272 + 249 = 521$意味着“o”)。显然，如果已知更多的明文/密文对，这张关联表可能包含更多的关联关系，从而更多的密文可以使用这张表加以解密。

表 5.1: 由两个已知明文“subject”和“to”得到的关联表

n	*254*	*272*	*521*	*530*	*835*	*1120*	*1434*	*1710*	*2132*
m_i	t	s	o	u	b	j	e	c	t

很显然，Jakimoski-Kocarev攻击主要依赖于混沌迭代次数C_i在密文中出现这个事实，这使得该攻击对于M. S. Baptista密码的所有改进方案都是可行的，另外它也可用来攻击我们在§5.3中和文献[110]中提出的E. Alvarez等人密码的改进方案。在下文中我们将把注意力主要放在M. S. Baptista提出的原始密码方案上。

§5.5.2 我们关于Jakimoski-Kocarev攻击性能的观点

文献[100]声称“统计测试显示仅使用4000个明文/密文对，即有超过90%的感兴趣时刻可以被恢复出来”。看起来似乎该攻击作为一种攻击相关混沌密码系统的工具相当棒。但是，以我们的观点，其性能并不像文献[100]号称的那么有效。我们列举下面几个原因来支持我们的观点。

事实一：为了解密一个密文单元，平均而言需要已知一个以上的明文单元。如果一个攻击者已知一个具有i个不同字符的明文消息，他/她可以得到i个不同的关联关系，并利用这i个关联关系解密i个密文单元。也就是说，为了解密一个密文单元，必须首先知道一个明文字符。当已知明文字符的数量N_p增加时，可以成功解密的密文单元(即感兴趣时刻)的数量N_c也会增加。但是，由于不同明文消息中的密文字符可能产生相同的关联关系，N_c的增加速度比N_p要慢。当已知明文的数量增加时，N_c的增加速度会变得越来越小，参看图5.4中给出的N_c相对N_p增加的试验曲线。因而，为了解密一个密文单元，所需的明文字符数量要大于1。这说明Jakimoski-Kocarev攻击有点像穷举攻击。

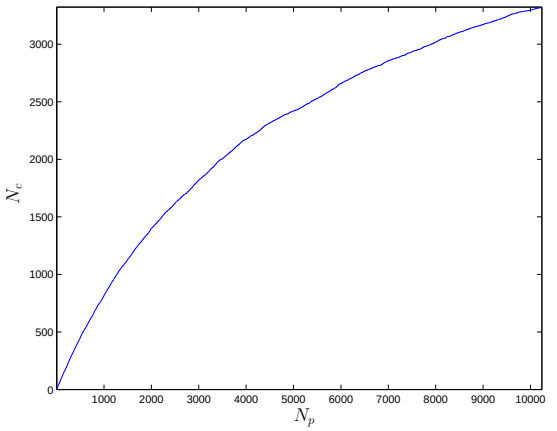


图 5.4: N_c相对N_p增加的试验曲线
(相关的参数
为$S = 256$，$b = 3.78$，$x_0 = 0.43203125$，$x_{min} = 0.2$，$x_{max} = 0.8$。1024个明文消息用来产生该曲线，每个明文消息包含10个随机明文字符。)

事实二：如果所有的已知明文消息最多包含i个明文字符，则解密位置大大超过i的明文字符几乎是不可能的，解密对应的“感兴趣时刻”大于$i \cdot N_{max}$的明文字符则完全不可能。对于一个给定的明文消息，如果前面i个明文字符(以及相应的密文单元)已知，解密该明文中后续的明文字符时完全不可能的。另外，甚至在很多明文消息的前i个明文字符都已知的情况下，解密位置大大超过i的明文字符从概率意义上讲是不可能的。事实上，由于C_i在密文中出现概率的指数化递减(请参看文献[84]中的Fig. 3和文献[104]中的Fig. 1)：随着明文字符的位置从i逐渐增大，攻击成功的概率将成指数衰减；而一旦明文字符的“感兴趣时刻”超过$i \cdot N_{max}$，攻

击成功的概率就马上变为0。例如，给定一个被原M. S. Baptista密码加密的明文消息“*Can you give me any help to break this chaotic cryptosystem*”，假设攻击者已知的全部明文消息都只能得到最前面三个明文字符，则对他/她而言解密上面明文中的最后一个词“*cryptosystem*”几乎是(概率上)不可能的，尽管他/她可以以很高的概率解密第一个词“*Can*”。

事实三：*由于相同的明文字符可能被加密为不同的密文单元，M. S. Baptista的密码方案更像一个流密码，而不是分组密码。但是Jakimoski-攻击是按照攻击分组密码的思路设计的，可能不太适用于流密码。* 考虑一个普通的基于密钥流$\{k_i\}$的异或操作的流密码，存在类似于Jakimoski-Kocarev攻击的一类已知明文攻击：一旦一个明文消息的头l个明文字符已知，攻击者即可通过异或明文字符与密文字符得到头l个异或密钥$k_1 \sim k_l$，然后所有使用同一个密钥加密的明文的头l个明文字符都可以被成功地解密(但是第l个明文字符以后的所有明文字符仍然是安全的)。一般而言，从严格密码学角度考虑，这样的攻击方法不能推出产生密钥流$\{k_i\}$的密钥，也不能破解所有已知明文字符以后的所有明文字符，因此这样的攻击不被认为是一种有效的攻击方案[143, 144]。类似地，Jakimoski-Kocarev攻击也不是一种攻击相关混沌密码的足够强的工具。

事实四：*在已知密文中如果不是所有的密文单元都已知，则解密明文消息中的任何明文字符都不可能。* 为了计算一个密文单元C_i的“感兴趣的时刻”，以前的全部$i-1$个密文单元都必须是已知的：$n = \sum_{j=1}^{i} C_j$。很自然地，如果攻击者没能观察并记录下所有的密文单元，他/她甚至不可能解密一个明文字符。例如，给定一个明文消息“Who am I”，如果攻击者只观察到“ho am I”对应的密文单元，他/她将无法从明文/密文对中获得任何可用关联。这个事实降低了Jakimoski-Kocarev攻击在实际应用中的有效性。

由以上事实可见，Jakimoski-Kocarev攻击不像作者在文献[100]中声称的那样有效。但是我们应当如何理解“*...仅需要4000个明文/密文对，即可恢复90%以上的感兴趣时刻*”这句话呢？假设明文消息的最大长度为l_{max}，“感兴趣时刻”的最大值将为$(N_{max} - N_0 + 1) \cdot l_{max}$。由事实一和事实二，由4000个明文消息得到的“感兴趣时刻”的数量N_c将满足$N_c < N_p \cdot l_{max} = 4000 \cdot l_{max}$，该值比$90\% \cdot (N_{max} - N_0 + 1) \cdot l_{max} = 0.9 \cdot (65532 - 250 + 1) \cdot l_{max} = 58754.7 \cdot l_{max}$小得多。很明显，“90%”这个百分比是模糊和不准确的。实际上，通过4000个明文/密文对，大约90%以上不同的明文字符S值可以在关联表中得到。但是这样一个事实并不能用来说明攻击的有效性，因为在M. S. Baptista密码中不同的密文单元可能对应着相同的明文字符(考虑事实三)。

§5.6 一种抵抗Jakimoski-Kocarev攻击的改进措施

尽管Jakimoski-Kocarev攻击并不是很有效，它在某些场合下对于减轻攻击复杂度仍然是有用的。在本节中，我们将提出一种简单的措施以提供抵抗Jakimoski-Kocarev攻击的能力。这样一种措施对于所有的相关密

码[84, 104, 110]都是可行的。另外，我们提出的措施也可以有效地抵抗文献[126]中提出的新的基于符号动力学的攻击方案，因为这些攻击和Jakimoski-Kocarev攻击一样都也依赖于下面的事实：混沌迭代次数C_i在密文中的出现。

§5.6.1 描述

在介绍我们提出的改进措施之前，让我们先来看看Jakimoski-Kocarev攻击是如何工作的。我们知道，每个密文单元C_i代表混沌系统(从$x_0^{(i-1)}$开始)进入代表当前明文字符m_i的ϵ-区间的迭代次数，因此$C_1 \sim C_i$可以累积起来而得到“感兴趣时刻”$n = \sum_{j=1}^{i} C_j$。如果明文字符m_i对攻击者是已知的，他/她就可以直接得到“感兴趣时刻”n和明文字符m_i之间的关联关系，并使用这种关系解密任何对应同一个“感兴趣时刻”n的密文单元。

显然，如果我们可以切断建立“感兴趣时刻”和明文字符之间关联的道路，Jakimoski-Kocarev攻击就会马上失效。这里，我们使用混沌掩盖技术实现这个目的，这里的混沌掩盖技术有点类似DES^X、Khufu和Khafre等传统密码系统中使用的“白化”技术(whitening)[143, §15.6]。

一个挫败Jakimoski-Kocarev攻击的自然想法是避免计算“感兴趣时刻”$n = \sum_{j=1}^{i} C_j$的可能性。如何做到这点呢？一个可能的办法是使用当前的混沌状态$x_0^{(i)} = F^{C_1+C_2+\cdots+C_i}(x_0)$掩盖密文$C_i$。由于$C_i$是一个16-比特的整数($250 \le C_i \le 65532$)而一般$x_0(i)$具有更多的比特数，某种比特抽取函数需要用来从混沌状态$x_0^{(i)}$的二进制表示中选择16个比特出来掩盖C_i。请注意这里的比特抽取函数不能随意选择以避免泄漏有关当前混沌状态的信息，这点将在下一节做更详细的讨论。掩盖操作可以使任何非线性函数，比如异或或者模加。

假设比特抽取函数为$f_{be}(\cdot)$，掩盖操作为$\oplus$，我们可以使用下述的措施增强原M. S. Baptista密码(包括其他相关密码[104, 110, 113, 114, 122, 123])的安全性以抵抗Jakimoski-Kocarev攻击。

加密：对于第i个明文字符m_i，从$x_0^{(i-1)}$开始迭代混沌系统寻找一个混沌系统状态x满足$f'_S(x) = m_i$(以及其他由N_0，N_{max}，η，κ定义的条件)，记录自$x_0^{(i-1)}$开始的迭代次数为$\widetilde{C}_i$，$x_0^{(i)} = F^{\widetilde{C}_i}(x_0^{(i-1)})$。则$m_i$对应的第$i$个密文单元为$C_i = \widetilde{C}_i \oplus f_{be}\left(x_0^{(i)}\right)$。

解密：对于每个密文单元C_i，首先迭代混沌系统N_0次，并设置$\widetilde{C}_i = N_0$，然后执行如下操作(如果$\eta \neq 0$，这样的操作仅当$\kappa \ge \eta$成立时才进行)：如果$\widetilde{C}_i \oplus f_{be}(x) = C_i$则使用当前的混沌状态$x$导出明文字符$m_i$，然后继续解密下一个密文单元；否则迭代混沌系统一次并执行$\widetilde{C}_i ++$，直到上述条件满足为止。

在下面的小节中，我们将指出强比特抽取函数$f_{be}(\cdot)$可以掩盖C_i的具体值，并使得Jakimoski-Kocarev攻击和文献[126]中提出的符号动力学攻击不可行。但是，仔细地研究上述解密过程，我们会发现可能以较小的概率得到错误的明文字符：当$\widetilde{C}_i \oplus f_{be}(x) = C_i$，恢复的“$C_i$”可能是错误的，从而使得恢复出来的混沌状态是错误的。不幸的是，在我们的文章[128]中，我们过于随意地忽略了这个问题。

现在我们试图修补上述加密/解密过程以解决这个缺陷。如果可能，稍后我们将投寄一篇注释性的文章给*Physics Letters A*以纠正我们在[128]中的错误。

纠正文献[128]中的错误

首先，让我们来看看这个问题有多严重。在加密端，我们按照如下的方法来估计一下错误的概率。当且仅当真实的C_i从未在输出密文时的混沌状态x以前出现过时，解密结果才是正确的。也就是说，对于一个给定的$\widetilde{C}_i$，正确恢复$\widetilde{C}_i$而从得到正确明文字符的概率为：

$$\begin{aligned} P_c\left(\widetilde{C}_i\right) &= P\left\{\bigwedge_{k=N_0}^{\widetilde{C}_i-1}\left(k\oplus f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right)\neq C_i\right)\right\} \\ &= P\left\{\bigwedge_{k=N_0}^{\widetilde{C}_i-1}\left(f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right)\neq k\oplus C_i\right)\right\}。 \end{aligned} \tag{5.4}$$

一般地，假设C_i的大小为n个比特(对于M. S. Baptista密码$n=16$)和混沌轨道$\left\{F^k\left(x_0^{(i-1)}\right)\right\}$在相关区间上均匀分布，我们有$\forall C_i, P\left\{f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right)=C_i\right\}=2^{-n}$，即$P\left\{f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right)\neq k\oplus C_i\right\}=1-2^{-n}$。假设$f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right)=k\oplus C_i(k=N_0\sim\widetilde{C}_i-1)$是相互独立的事件，可以推出$P_c\left(\widetilde{C}_i\right)=(1-2^{-n})^{\widetilde{C}_i-N_0}$。显然，随着$\widetilde{C}_i$趋向无穷大，$P_c\left(\widetilde{C}_i\right)\to 0$，这意味着经过足够长的时间之后加密过程会退化成为对明文的随机猜测。

考虑到$\widetilde{C}_i$的非均匀分布，对于第一个明文字符m_1，由全概率公式可以得出最终的解密端正常工作概率$P_{c,1}$*：

$$\begin{aligned} P_{c,1} &= \sum_{k=N_0}^{N_{max}} P\{\widetilde{C}_i=k\}\cdot P_c(k) \\ &= \sum_{k=N_0}^{N_{max}} P\{\widetilde{C}_i=k\}\cdot(1-2^{-n})^{k-N_0}。 \end{aligned} \tag{5.5}$$

为简化分析计，不失一般性，假设$F(x)$以相同的概率$p=1/S$访问每个ϵ-区间†，我们有$P\{\widetilde{C}_i=k\}=p(1-p)^{k-N_0}$，然后可得

$$\begin{aligned} P_{c,1} &= \sum_{k=N_0}^{N_{max}} p(1-p)^{k-N_0}\cdot(1-2^{-n})^{k-N_0} \\ &= \sum_{k'=0}^{N_{max}-N_0} p\cdot q^{k'}=p\cdot\frac{1-q^{N_{max}-N_0}}{1-q}, \end{aligned} \tag{5.6}$$

*假设$P\{C_i>N_{max}\}=0$，参看§5.4中我们那个吹毛求疵的注释。

†Logistic映射并不严格满足这个条件，因此我们建议在M. S. Baptista密码中使用PWLCM替代Logistic映射。

这里$q = (1-p)\cdot(1-2^{-n})$。当$S = 256, n = 16, N_0 = 250, N_{max} = 65532$(原始M. S. Baptista密码中的值)，$P_c \approx 0.9961240899211136$(使用Matlab®在IEEE双精度浮点算法下计算出来的结果)。考虑到$1/(1-P_c) \approx 258$，可以看到在大约258个解密的明文消息中会出现一个首字符出错的消息。这里需要注意的是一旦出现错误的明文比特以后，后续的所有明文比特都以接近1的较高概率出错，即存在错误传播问题。很显然，对于位于其他位置($i > 1$)的明文字符，错误传播使得问题变得更糟了：

$$P_{c,i} = \left(\prod_{j=1}^{i-1} P_{c,j}\right)\cdot\frac{p\left(1-q^{N_{max}-N_0}\right)}{1-q} = \left(\prod_{j=1}^{i-1} P_{c,j}\right)\cdot P_{c,1} = P_{c,1}^{i}。 \tag{5.7}$$

随着i的增大，概率$P_{c,i}$以指数速度衰减。一旦$P_{c,i}$变得小于$1/S$，则随机猜测将取代解密器成为解密端发生的实际过程。

考虑到当被加密的文件是一篇文章或者是一个数字化图象时，错误的明文比特可以容易地被人分辨出来，因此这样一个特点可能用来实现一个新而有趣的类似于可视加密术[218]的密码系统。在未来中我们将研究能否将该概率解密特点在传统密码中进行推广。

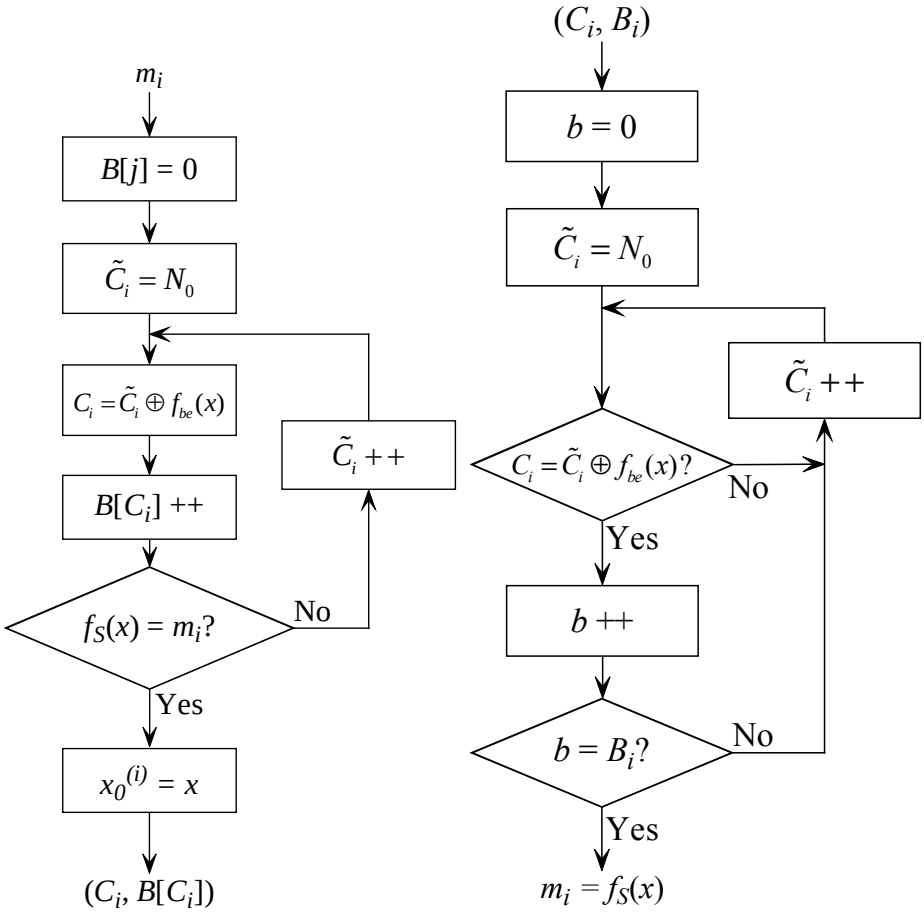
接下来让我们回到主线上来，由于$P_c < 1$我们不得不修补上面的改进加密解密方案以使得$P_c \equiv 1$. 为了做到这一点，我们如下修改上述的加密/解密过程：

加密：一个存储单元被分配用来存储$N_{max} - N_0 + 1$个代表$C_i = N_0 \sim C_i = N_{max}$的临时变量$B[N_0] \sim B[N_{max}]$。对第$i$个明文字符$m_i$，首先复位所有的存储单元$B[i](i = N_0 \sim N_{max})$为0，然后自$x_0^{(i-1)}$迭代混沌系统$N_0$次，设置$\widetilde{C}_i = N_0$，然后进行如下操作：$C_i = \widetilde{C}_i \oplus f_{be}(x)$，$B[C_i]++$，如果当前混沌状态$x$满足$f_S(x) = m_i$，则产生一个二元组密文$(C_i, B[C_i])$，并设置$x_0^{(i)} = x$然后转向下一个明文字符$m_{i+1}$；否则重复上述过程直到一个密文被产生。

解密：对每个密文单元(C_i, B_i)，首先迭代混沌系统N_0次，并设置$\widetilde{C}_i = N_0$，然后进行如下操作(如果$\eta \neq 0$，这样的操作仅当$\kappa \geq \eta$成立时才进行)：如果$\widetilde{C}_i \oplus f_{be}(x) = C_i$第$B_i$次成立，则使用当前的混沌状态$x$导出明文字符$m_i$并转向下一个密文单元$(C_{i+1}, B_{i+1})$；否则迭代混沌一次并执行$\widetilde{C}_i++$，直到上述条件满足。

在图5.5中我们给出了上述改进的加密解密过程的流程图，其中$\boxed{B[i]=0}$表示复位所有的$B[i]$为0，$\boxed{\widetilde{C}_i' = N_0}$表示执行$N_0$次混沌迭代和$\widetilde{C}_i' = N_0$，$\boxed{\widetilde{C}_i'++}$表示执行一次混沌迭代和$\widetilde{C}_i'++$。

与M. S. Baptista原密码相比，上述改进方案以增加实现复杂度为代价增强了抵抗相关攻击的安全性：1) 由于对每个明文字符都需要复位$N_{max} - N_0 + 1$个临时变量$B[i]$为0，从而使得加密速度变得慢了一些；2) 密文大小有了更大的扩展($B[C_i]$被加入到密文中去)；3) 需要一个额外的存储单元保存$N_{max} - N_0 + 1$个临时变量$B[i]$，当$B[i]$是2-比特整数时，所需的内存大小为$2\times(N_{max} - N_0 + 1)$字节(当$N_{max} = 65532$和$N_0 = 250$时，不会超过128 KB)。幸运的是，额外的内存需求在几乎所有的数字计算机上都不是很大的负担(128 KB对于一个拥有100MB以上



a) 加密过程　　b) 解密过程

图 5.5: M. S. Baptista密码的改进方案的修正加密/解密过程

内存的计算机应该不算大)，而且当该密码使用支持并行处理的硬件实现时，对加密速度的影响也不大*。因此，我们认为上述改进的密码方案在实际应用中还是有价值的。当然了，如果加密速度可以被进一步提高，密文大小可以进一步减小(W.-K. Wong在文献[123]中的改进密码系统可以作为可能的候选方案)，则相应的密码方案会更好。

§5.6.2 讨论

由于攻击者无法通过观察明文/密文对来计算$\sum_{j=1}^{i} C_j$，上述改进的密码方案对Jakimoski-Kocarev攻击是免疫的。

*所有$N_{max} - N_0 + 1$个临时变量$B[i]$可以在一个时钟周期内实现同时复位，这取消了对加密速度的负面影响。另外，使用预计算机制和延迟设计，混沌迭代可以与$C_i = \tilde{C}_i \oplus f_{be}(x)$，$B[C_i]++$和$f_S(x) = m_i$?并行运行。

但是，我们需要仔细地配置该改进方案以避免可能由位抽取函数$f_{be}(\cdot)$带来的新的不安全问题：由于在该密码中密文的分布是不平衡的，攻击者可能以较高的概率猜测当前混沌状态的部分比特。假设$f_{be}\left(x_0^{(i)}\right)$直接从当前混沌状态的二进制表示$x_0^{(i)} = 0.b_1b_2\cdots b_j\cdots$中抽取16个比特，我们可以发现$x_0^{(i)}$的部分信息可能泄漏出来。我们知道，尽管密文单元$C_i$是16-比特的整数，$C_i \geq 2^{12}$的概率相当小(参看文献[84]中的Fig. 3和文献[104]中的Fig. 1)。因而，如果我们假设四个高位比特都是0的话，这样一个假设将以高概率成立，也即，关于$x_0^{(i)}$的4个比特的信息可能从$f_{be}\left(x_0^{(i)}\right)$中泄漏出来。对于$i = 1$，这样的信息泄漏可以被用来穷举搜索$F^{C_1}(x_0)$，其搜索复杂度比搜索$x_0$小。一旦攻击者得到了$F^{C_1}(x_0)$，他/她即可使用它解密任何不小于$C_1$的密文单元。

上述分析表明$f_{be}\left(x_0^{(i)}\right)$不应当泄漏关于$x_0^{(i)}$的有用信息，也就是说，该函数应该在密码学意义上足够强以防止攻击者从$f_{be}\left(x_0^{(i)}\right)$得到任何关于$x_0^{(i)}$的信息。在下面我们将给出两类可用的位抽取函数，作为例子演示如何使得$f_{be}\left(x_0^{(i)}\right)$足够强。使用这两类函数，攻击者将很难从$f_{be}\left(x_0^{(i)}\right)$的部分比特得到$x_0^{(i)}$的信息。

第一类函数是

$$f_{be}\left(x_0^{(i)}\right) = f'_{be}\left(\bigoplus_{j=0}^{C_1+\cdots+C_i} F^j(x_0)\right) = f'_{be}\left(x_0 \oplus F(x_0) \oplus \cdots \oplus x_0^{(i)}\right), \tag{5.8}$$

这里$f'_{be}(x)$可以是任何从x的二进制表示形式中抽取16个比特的函数。使用这样一类位抽取函数，攻击者只能得到有关$\bigoplus_{j=0}^{C_1+\cdots+C_i} F^j(x_0)$的信息。考虑到$C_i \geq N_0 = 250$，攻击者几乎完全不可能从$f_{be}\left(x_0^{(i)}\right)$得到任何有关$x_0^{(i)}$的信息。

第二类函数是

$$f_{be}\left(x_0^{(i)}\right) = \sum_{j=0}^{15} 2^j \cdot b\left(F^j(x_0^{(i)}), \left\lfloor F^{j+m}(x_0^{(i)}) \cdot 2^n \right\rfloor \bmod 16\right), \tag{5.9}$$

这里$m \geq 1, n \geq 4$并且$b(x, j) = \lfloor x \cdot 2^j \rfloor \bmod 2$。在该类位抽取函数中，全部16个比特来自不同的混沌状态，抽取的比特位置又是由另外一个不同的混沌状态确定的($m \geq 1$)。显然，这个类别的函数很容易扩展出许多变形版本，比如我们可以将$j + m$变为$j - m$或者改变$b(\cdot)$的定义。

我们也可以将上面两类位抽取函数组合起来得到更为复杂的位抽取函数，这可能进一步增进安全性。

另外，在上述改进密码方案中取消密文分布的不均匀性，也可以有效避免位抽取函数$f_{be}\left(x_0^{(i)}\right)$带来的安全隐患。这里有两种可能的办法消除密文分布的不均匀性。采用这样的措施之后，位抽取函数应当可以任意选取。

- *方法一*：使用W.-K. Wong等人在文献[104]中提出的改进密码方案。密文的分布可以被改善为近似均匀分布，这样信息泄漏变得不可能了(参看文献[104]中的Fig. 2)。

- *方法二*：引入压缩机制。在$\widetilde{C}_i$得到以后，使用无损压缩算法对其进行压缩(如Huffman压缩算法[216])以取消信息冗余，即使得$\widetilde{C}_i$的分布变得均匀，然后再使用$f_{be}\left(x_0^{(i)}\right)$掩盖压缩后的$\widetilde{C}_i$。这里请注意：$\widetilde{C}_i$越小，其出现概率越大，压缩后的$C_i$比特数越小，因此需要越少的比特数掩盖$\widetilde{C}_i$。由于压缩后每个密文大小变得不同，需要额外的数据指示当前密文的大小。

由以上讨论，可以看到我们提出的M. S. Baptista密码的改进版本比原密码系统安全。为了攻击改进方案，混沌系统的初始状态x_0和控制参数r必须首先被破解才能得到$x_0^{(i)}$，这也就意味着对密钥的穷举攻击。当然，该方案中还存在着一个问题：加解密速度较原密码方案慢一些(慢得不多)。

§5.7 本章小结

本章展示了我们关于基于搜索的混沌密码的研究工作。讨论了两类相关攻击：G. Alvarez等人提出的针对E. Alvarez等人的密码的攻击，和针对M. S. Baptista密码的Jakimoski-Kocarev攻击。提出了两种改进方案：一种用于增强E. Alvarez等人的密码方案抵抗G. Alvarez等人的攻击，一种用于增强M. S. Baptista密码抵抗Jakimoski-Kocarev攻击。对M. S. Baptista密码的改进方案的相关讨论引出了一个有趣的具有概率解密特点的密码系统，它具有类似于可视加密术的特点，或许可以在将来实现传统密码学中的一些特殊功能。

尽管两种基于搜索的混沌密码的安全性被增强了，由于搜索过程本身很耗时，加密速度基本上没有得到改善。基本上，所有的基于搜索的混沌密码的加密速度都比大部分传统密码要慢得多。这是一个还没有最后解决的问题。在将来的研究中我们会试图找到这个问题的解决方案，但是或许任何可能的解决方案都会使得加密结构发生彻底的改变，而使得到的密码系统不再是一个基于搜索的混沌密码。

第六章 S. Papadimitriou等人的数字化混沌密码的分析

§6.1 引言

作为一个在混沌密码领域较为活跃的研究小组，S. Papadimitriou等人先后提出了几种混沌密码[30, 33, 106, 219]。在文献[106]中，他们提出了一种新的数字化混沌密码，它是一种基于多个差分方程的混沌系统的对称概率分组密码。在本章中，我们将指出该混沌密码的一些问题，其中一些使得S. Papadimitriou等人的这种混沌密码不实用而且不安全，另外一些表明需要采取一些改进措施增强该密码的性能。

本章的组织如下。在下一节中，我们给出一个S. Papadimitriou等人混沌密码的简单介绍。§6.3给出该混沌密码问题的详细分析和讨论。一个具体的分析例子在§6.4中给出以证实本章理论分析的正确性。一些存在于S. Papadimitriou等人的密码中的一些有积极意义的想法在§6.5中给出。本章小结在最后一节给出。§6.3.2中一个结论的较为冗长的证明在本章的附录中给出。

§6.2 S. Papadimitriou等人的混沌密码

为了读者的方便，在本节中我们简要地介绍一下S. Papadimitriou等人的混沌密码以及在他们的文章中给出的一些相关的分析结论。关于更多的分析和论述，请参看他们的原文。

S. Papadimitriou等人的密码是一种对称的概率分组密码，它将d-比特的明文加密为e-比特的密文($e > d$)。其加密和解密过程可以描述如下。这里，请注意我们重新组织了文献[106]中给出的加密解密步骤，以使得论述更为清晰明了。

加密：

1. 给定一个(或多个)混沌系统产生一个归一化的(缩放到单元区间$[0,1]$上去)拟混沌轨道$\{x(n)\}_{i=1}^{\infty}$。

2. 使用$\{x(n)\}_{i=1}^{\infty}$构造一个虚拟状态空间(*virtual state space*)，即一个有2^d个虚拟吸引子(*virtual attractors*)的列表，这2^d个虚拟吸引子中包含如下2^e个虚拟状态(*virtual states*)$1 \sim 2^e$：在序列$\{\text{round}(x(n) \cdot 2^e)\}_{i=1}^{\infty}$中搜索$1 \sim 2^e$直到所有的整数都被找到为止(次序被扰乱)；选择$2^d$个状态作为虚拟吸引子并(伪随机地)将剩下的$2^e - 2^d$个状态分配到这$2^d$个吸引子上去。

3. 使用一个(一一的)置换矩阵$\mathbf{P}$将每个虚拟吸引子V_a和一个消息字符联系起

来。这里，**P**是一个索引自0开始的1×2^d向量*，其元素为2^d个扰乱的位于1和2^e之间的虚拟吸引子。

4. 按照如下方式加密一个明文字符$M_c = 0 \sim 2^d - 1$：首先使用$V_a = \mathbf{P}[M_c]$将M_c映射到一个虚拟吸引子上去，然后从该吸引子中伪随机地选择一个虚拟状态S_{V_a}作为密文。

显然，最后一步使得该密码称为一个概率分组密码。

解密：

1. 使用与加密过程中的步骤1和2相同的方法重建虚拟状态空间。
2. 确定**P**的“逆矩阵”$\mathbf{P}^{-1}$，它是一个索引自1开始的1×2^d向量，其元素为$0 \sim 2^d - 1$。$\mathbf{P}^{-1}$应当满足下列条件：$\forall M_c = 0 \sim 2^d - 1$，$\mathbf{P}^{-1}\left[\mathbf{P}[M_c]\right] = M_c$。
3. 检索当前密文S_{V_a}位于哪个虚拟吸引子V_a中，然后恢复明文字符：$M_c = \mathbf{P}^{-1}[V_a]$。

将2^e个虚拟状态和2^d个虚拟吸引子之间的关联写作一个(多对一的)满映射$\boldsymbol{F}_v : \boldsymbol{V}_s \rightarrow \boldsymbol{V}_a$，这里$V_s, V_a$分别表示所有的虚拟状态的集合和所有虚拟吸引子的集合。基于$\boldsymbol{F}_v$，我们可以形式化地把S. Papadimitriou等人的密码写成如下这个样子：加密– $S_{V_a} = \boldsymbol{F}_v^{-1} \circ \mathbf{P}(M_c)$，解密– $M_c = \mathbf{P}^{-1} \circ \boldsymbol{F}_v(S_{V_a})$。由于$\boldsymbol{F}_v^{-1}$不是唯一的，加密成为概率性的，但是解密完全是确定性的，因为$\mathbf{P}^{-1} \circ \boldsymbol{F}_v$是确定性的。

S. Papadimitriou等人采用了如下具有多个差分方程的混沌系统构造归一化的拟混沌轨道：

$$i = 1 \sim K: \qquad x_i(n+1) = \sum_{j=1}^{K} a_{ij} \cdot f_i\left(b_{ij} \cdot x_j(n) \bmod R_i + L_i\right), \tag{6.1}$$

这里$R_i = U_i - L_i$，$[L_i, U_i]$是f_i的定义域。由于逐段线性性有助于简化系统设计，并且可以使得上述混沌映射具有足够好的动力学特性，$f_i(i = 1 \sim K)$†被建议为具有N个断点的逐段线性函数。既然这里总共有K个混沌子系统，任何子系统的拟混沌轨道或者其中部分拟轨道的组合都可以用来生成加解密所需的虚拟状态空间‡.

关于该混沌密码的安全性，文献[106]中考虑了两种可能的攻击方法：1) 直接重建虚拟状态空间；2) 精确模拟混沌系统的动力学行为以重建虚拟状态空间。第一种攻击的复杂度通过估计所有可能的虚拟状态空间的数量进行计算，[106]中得到的结论为$(k!)^m \cdot k^{n-k \cdot m}$，这里$k = 2^d$，$n = 2^e$($m$是每个虚拟吸引子中包含的虚拟

*尽管S. Papadimitriou等人称**P**为向量(甚至矩阵)，我们认为将它看作是一个将消息字符映射到虚拟吸引子的单射函数更合理一些。

†在文献[106]中，S. Papadimitriou等人将$f_i, i = 1 \sim K$误写为$f_i, i = 1 \sim K - 1$。

‡这个问题在S. Papadimitriou等人的文章中没有提到，不过在他们的C++实现代码中，第一个子系统的拟混沌轨道被采用。如果需要相关的C++代码，可以给S. Papadimitriou发e-mail到stergios@heart.med.upatras.gr。本文作者有一份该代码的拷贝。

状态的最小数量)*。第二种攻击的复杂度使用S. Papadimitriou等人在另外两篇文献中采用的类似方法进行推导。

S. Papadimitriou等人声称的该密码的其他优点还有：1) 选用的混沌系统的逐段线性性使得计算复杂度很小，密码很容易实现升级和降级；2) 试验显示该密码的加密速度比其他很多传统密码快得多，如DES，IDEA和RC5。

§6.3 S. Papadimitriou等人混沌密码中的问题

在本节中，我们将指出S. Papadimitriou等人混沌密码中存在下列问题并给出详细的讨论。

- 在该密码的实际实现和高安全性之间存在不可协调的矛盾：明文和密文的大小d, e必须足够大以保证高安全性，而它们又必须足够小以使得该密码的实际实现成为可能。
- 关于所有可能的虚拟状态的数量的推导是错误的。
- 安全性分析是不正确的，对于穷举攻击的安全性被高估了。
- 密码的快速加密和解密恰恰依赖于第一个缺陷：d和e在取值大小上的矛盾。
- 当数字化混沌系统在有限精度下实现时，动力学特性的退化必须使用一些方法加以改善。
- 没有明确地描述如何从2^e个整数中选择2^d个虚拟吸引子和如何伪随机地分配2^e个虚拟状态到2^d个吸引子，也没有明确描述如何生成置换矩阵$\mathbf{P}$。

§6.3.1 d和e取值上的矛盾

在S. Papadimitriou等人的密码中，明文分组大小为d比特，密文分组大小为e比特。为了提供高安全性，d和e必须足够大。但是，我们注意到d和e必须足够小，以使得虚拟状态空间的建立和存储称为可能。让我们考虑如下两个事实：i) 消耗在虚拟状态空间建立上的时间为$O(2^e)$；ii) 虚拟状态空间需要的存储空间大小为$O(2^e)$。显然，e不能太大，一般来说$e > 30$在一般的PC机上就已经几乎不能实现($2^{30} = 1$G，这么大的存储空间会使得虚拟状态空间的建立**非常非常得慢**，并在一个内存不大于1GB的PC上的密码实现完全**不可能**)。这样，既然d和e不能太大，一旦攻击者得到$O(2^e)$个密文及其对应的明文，他/她就有可能精确重建虚拟状态空间以攻破该密码。这意味着该密码对已知/选择明文攻击是不安全的[143, 144]。在较弱的条件下，如果攻击者可以得到足够的(但是少于2^e)明文和对应的密文，他/她就有可能使用伪造的密文欺骗合法用户。

*在文献[106]中，在该式中使用了N, K, M，但是这里的N, K很容易和方程(6.1)中的N和K混淆。为了避免这种混淆，在本章中我们使用小写的n, k, m代替文献[106]中的N, K, M。

实际上，传统密码学的一个核心任务就是设计一个在密钥控制下的、由明文到密文的非线性单射，这里的非线性双射和文献[106]中的虚拟状态空间的作用是完全相同的。一般而言，这个用来加密明文和解密密文的非线性双射是使用密钥表示的非线性操作，而不是象文献[106]中的虚拟状态空间那样事先计算好的。那么为什么不直接使用预先计算并存储好的非线性双射呢？这是由于当明文和密文的大小足够大时，该映射的表示和存储会变得实际不可行。例如，让我们考虑一下DES：明文和密文的大小为64比特，显然，使用有限的存储空间，我们不可能表示和存储一个将2^{64}个明文映射到2^{64}个密文的映射($2^{64} = 16GG!!$)。这里，我们愿意引用B. Schneier在他的密码学畅销书《应用密码学》(Applied Cryptography)[143, §14.10.7]中的说法：*如果你有一个巨大的存储器可以存储巨大的S盒，那么设计一个安全的分组密码会变得非常容易。* 从这样一种观点看，S. Papadimitriou等人的密码中使用的虚拟状态空间这个基本想法既**不实际**也**不安全**。

§6.3.2 所有可能的虚拟状态空间数量的错误推导

在文献[106]中，为了估计S. Papadimitriou等人的密码对直接重建虚拟状态空间的安全性，所有可能的空间数量被推导出来：$(k!)^m \cdot k^{n-k\cdot m}$。基于上述结论，S. Papadimitriou等人声称该密码的安全性比其他的传统密码要高得多，如DES，IDEA和RSA。

在本小节中，我们指出文献[106]中给出的上述有关推导是错误的，正确的空间数量不是$(k!)^m \cdot k^{n-k\cdot m}$。观察文献[106]中给出的推导过程，原因可以通过下面两个事实加以解释：1) 由于不同的mk个状态可能在第一阶段被选中，该数值可能被**低估**；2) 由于部分排列被重复计数，该数值可能被**高估**。对于第二个问题，我们可以给出一个例子。下面两种排列A和B是相同的，但是在S. Papadimitriou等人的推导中被重复计数：A和B中所有的状态都被分配到相同的吸引子，只是对于A而言一个状态S_{V_a}在**第一**阶段被分配到吸引子V_a中，对于B而言一个状态S_{V_a}在**第二**阶段被分配到吸引子V_a中。既然上面两个问题通过矛盾的方式影响最终结果，真实的数量可能比$(k!)^m \cdot k^{n-k\cdot m}$大，也可能比该值小。

在下面，我们将试图通过另外一种途径解决这个问题。我们注意到如下事实：分配到同一个吸引子中的所有虚拟状态的次序不会影响密文的解密，尽管这会使得同一个明文对应的密文不同。因而，所有可能的虚拟状态空间的数量可以重新描述为下述组合问题的解：*将n个**不同**的球放入k个**不同**的箱子，每个箱子中最少放m个球($n \geq mk$)，有多少种可能的放法？*

上述组合问题的正确解是什么呢？事实上，尽本文作者所知，除了少量特例(第二类Stirling数是$m = 1$时该问题的特例[220])，到目前为止该问题尚不存在显式的解析解。假设所求的数量为$g(n)$，目前对该问题的最好的解是一个递推解：当$n = mk$时：

$$g(n) = \binom{mk}{m, m, \cdots, m} = \frac{(mk)!}{(m!)^k}。 \tag{6.2}$$

当$n > mk$时：

$$g(n) = \frac{\sum_{t=mk}^{n-1} g(t)\left(k \cdot \binom{n+m-1}{t} - \binom{n+m-1}{t-1}\right)}{\frac{n-mk}{k} \cdot \binom{n+m-1}{n}}。 \tag{6.3}$$

上述递推解的推导比较繁琐，因此我们将它放在本章的附录中。上述结果与文献[106]中给出的结果完全不同。比如，当$n = mk$，正确值应当是$\frac{(mk)!}{(m!)^k}$，但是文献[106]中导出的结果为$(k!)^m$。在多数情况下，S. Papadimitriou等人导出的结果比真实值要小。那么我们是否可以说S. Papadimitriou等人的密码安全性被低估了？答案是**否定的**，我们将在下面一个小节讨论这个问题。

§6.3.3 不当的安全性分析

在上一小节，我们已经指出所有可能的虚拟空间的数量$g(n)$应当为方程(6.2)和(6.3)表示的数值，而不是文献[106]中给出的$(k!)^m \cdot k^{n-k\cdot m}$。在本小节中，我们将进一步指出$g(n)$的数值和所有可能的密钥数量不能直接用来证明密码的安全性，也就是说，S. Papadimitriou等人在文献[106]中给出的安全性分析是不恰当的。这是下述事实**F1**至**F4**的自然结论。

F1) *大部分虚拟状态空间太相近而不能保证混沌密码的高安全性。*为了定量描述两个虚拟状态空间A, B的差异(相似性)，我们首先定义A和B之间的**距离**这样一个概念：$d(A,B) = \sum_{i=1}^{n} \mathrm{Com}(A_i, B_i)$，其中$A_i, B_i$分别表示A和B中包含第$i$个虚拟状态的虚拟吸引子，

$$\mathrm{Com}(A_i, B_i) = \begin{cases} 1, & A_i \neq B_i \\ 0, & A_i = B_i \end{cases}。 \tag{6.4}$$

这里，$d(A,B) = 1 \sim n$表示A, B中被分配到不同虚拟吸引子的虚拟状态的数量。显然，$d(A,B)$越小，两个虚拟状态空间A, B越接近。

作为$d(A,B)$性质的一个自然结论，对于均匀分布的明文，相似的虚拟状态空间会产生相似的密文。因而，攻击者可以使用一个相似的虚拟状态空间代替真实的状态空间解密大部分密文(使用的虚拟状态空间和真实的越相似，越多的明文可以被解密)。为了得到足够高的安全性，两个可用的虚拟状态空间A, B之间的距离应当足够大($d(A,B) = n$是理想的，$d(A,B) \geq n/2$在大多数情况下是可行的)，但是这样的“**好的**”虚拟状态空间的数量要比方程(6.2)和(6.3)中给出的数值**小的多得多**。

F2) *并不是所有的虚拟状态空间都可以用混沌系统(6.1)构造出来。*一旦拟混沌轨道$\{x(i)\}_{i=1}^{\infty}$和虚拟状态空间的构造算法给定，生成的虚拟状态空间也就唯一确定了。这意味着所有可能生成的虚拟状态空间的数量被所有可能的拟混沌轨道的数量所控制，并不只是由方程(6.2)和(6.3)唯一确定。那么到底有多少可能的拟混

沌轨道呢？显然，拟混沌轨道的数量被所有可能的密钥的数量确定，也就是所有的控制参数和初始条件的数量。

在S. Papadimitriou等人的密码中，方程(6.1)的下述控制参数被用作密钥*：$a_{ij}, b_{ij} (i, j = 1 \sim K)$，$R_i, L_i (i = 1 \sim K)$和$f_1 \sim f_K$的$NK$个断点值(如果$f_1 = f_2 = \cdots = f_K$则只有$N$个断点值)†。假设上述参数的计算敏感度均为$2^{-L}$($L$是采用的有限精度)并且全部参数都限制在区间$[0, 1]$上，我们可以粗略地计算出所有可能的密钥数量‡：$\mathcal{N}_{\mathcal{K}} = (K^2 + 2K) \cdot 2^L + K \cdot \prod_{i=0}^{N-1} (2^L - i)/N!$。一般地，$2 < N \ll 2^L$并且$2 < K \ll 2^L$，则$\mathcal{N}_{\mathcal{K}} \approx K \cdot 2^{LN}/N!$(当$f_1 = f_2 = \cdots = f_K$时，$\mathcal{N}_{\mathcal{K}} \approx 2^{LN}/N!$)。

F3) *不同的密钥可能产生相同的虚拟状态空间。*如果$\mathcal{N}_{\mathcal{K}} > g(n)$这个事实显然是正确的。和上一个事实**F3**一起，我们可以看到S. Papadimitriou等人密码的安全上限为$\min(g(n), \mathcal{N}_{\mathcal{K}})$。因而，尽管当$n = 2^e$和$m = 2^d$足够大时($d = e = 8$就算足够大了)$g(n)$可能非常**巨大**，但是S. Papadimitriou等人密码的实际安全性还要被$\mathcal{N}_{\mathcal{K}}$所限制。由上面一段中导出的$\mathcal{N}_{\mathcal{K}}$的近似值，S. Papadimitriou等人密码在穷举攻击下的密钥熵一般近似等于$LN - \log_2(K/N!)$，当d和e很小而使得$g(n) < \mathcal{N}_{\mathcal{K}}$成立时，可能比$LN - \log_2(K/N!)$还要小。

F4) *由于我们在§6.3.1中讨论的d和e取值方面的矛盾，S. Papadimitriou等人的密码对已知/选择明文攻击、选择密文攻击都是不安全的。*这个问题在§6.3.1中已经讨论过了。可以看到S. Papadimitriou等人的密码对这三种攻击的密钥熵都只有e，一般来说，它比$LN - \log_2(K/N!)$要小得多。

§6.3.4 其他问题

*该密码完美的加密速度依赖于关于d和e取值的矛盾。*在文献[106]的Table 2中给出了该密码和一些传统密码加密速度的比较，测试平台是一台96MB内存的433MHz的赛扬(Celeron)® PC。S. Papadimitriou等人的密码的加密速度达到了一个非常高的值：327.2Mbps，这比其他的所有密码都要快得多。这近乎完美的加密速度可以这样来解释：一旦虚拟状态空间建立起来，加密和解密过程(最后一步)就可以通过简单的查找表(Look-Up-Table)操作来实现。但是请记住这个优点是建立在下述缺陷基础上的：整个虚拟状态空间必须首先建立起来并存储在内存中，而我们§6.3.1中已经指出在这个缺陷使得密码不实用和不安全。

*没有明确地描述如何从2^e个整数中选择2^d个虚拟吸引子和如何伪随机地分配2^e个虚拟状态到2^d个吸引子，也没有明确描述如何生成置换矩阵$\mathbf{P}$。*由于很多伪随机编码算法都可以用来实现上述的三种操作，这个问题不像其他问题那么严重。当然了，不同的算法会导致不同的伪随机性，从而可能导致不同的性能。另

*初始条件在文献[106]中没有被用作密钥的一部分。在S. Papadimitriou等人的C++代码中，0.1用来初始化$x_1(0) \sim x_K(0)$。

†在文献[106]中，f_i的断点数量在Sec. 2.2用N表示，而在Sec. 3则变成了n。在本论文中，我们始终使用N。

‡S. Papadimitriou等人在文献[106]中没有给出$\mathcal{N}_{\mathcal{K}}$的具体推导过程，只是建议读者参看他们的另外两篇文章[30, 219]。这里，我们使用一种不太相同的办法推导$\mathcal{N}_{\mathcal{K}}$的值。

外，如果我们知道了哪种算法被使用，或许可能对生成的虚拟状态空间进行分析。这样的分析可能导致一些新的攻击方法，使其攻击复杂度低于穷举攻击。

在有限计算精度下实现的混沌系统的动力学特性退化。我们在§2.5.1中已经指出，这样的动力学特性退化在所有的数字化混沌系统中都能存在，而且必须使用适当的措施加以改善。

§6.4 一个实际例子

为了强调S. Papadimitriou等人的密码中存在的安全性和实用性之间的矛盾，这里我们通过一个具体的例子进行进一步的解释。考虑到混沌系统只是用来生成具有高密钥熵的虚拟状态空间，我们将采用Logistic映射$F(x) = 4x(1-x)$替代文献[106]中建议的混沌系统以简化问题的讨论和试验设计，这不会对密码的性能有任何实际的影响。假设$d = 6, e = 8$，密钥选作Logistic映射的初始条件$x_0 = 0.1111$。不失一般性，令$m = 3$，2^d个虚拟吸引子、其他$2^e - 2^d$个虚拟状态的分配(即映射$\boldsymbol{F}_v$)和置换矩阵$\mathbf{P}$都在下述伪随机数发生器的控制下生成*：系统中内嵌的伪随机函数`rand`，(秘密或者公开的)初始种子为$s = 0.2222$。这里请注意x_0和s都没有故意地选择为特殊值以支持我们的分析。建立起来的映射$\boldsymbol{F}_v$(即虚拟状态和虚拟吸引子之间的关联关系)和置换矩阵$\mathbf{P}$分别显示在图6.1和图6.2中。

对于这样一个密码系统，如果我们可以得到足够的已知/选择明文/密文对，就可能得到确定性的解密函数$\mathbf{P}^{-1} \circ \boldsymbol{F}_v$。既然$d, e$不能太大，我们可以将这个函数在计算机中存储为查找表去解密后续的密文。所需的已知/选择明文数量是多少呢？在图6.3中，在假设明文在离散集合$\{0, 1, \cdots, 2^d - 1\}$上均匀分布的前提下，我们给出了得到的虚拟状态/虚拟吸引子的数量和已知/选择明文数量之间的关系。可以看到$O(2^e)$明文就已经足够得到所有2^e个虚拟状态(即所有的可能密文)，$O(2^d)$个明文就足够得到全部2^d个虚拟吸引子。$O(2^e)$个明文意味着什么？考虑到明文是6-比特数，$O(2^8)$个明文仅仅意味着大约192个字节，大概相当于一个较长的英文句子。一旦所有的2^e个虚拟状态都得到了，我们就可以重建密文-明文映射(即解密函数)$\mathbf{P}^{-1} \circ \boldsymbol{F}_v$。显然，这个安全性缺陷是由$d, e$过小的值造成的。如果增加$d, e$的值以提高抵抗这类攻击的能力，$\boldsymbol{F}_v$的建立和存储会变得实际上不可行。

最后，让我们来看看所有可能的映射$\boldsymbol{F}_v$的数量。当$n = 2^e = 256, m = 3, k = 2^d = 64$时，$n$个球在$k$个箱子中(每个里面最少$m$个球)的所有可能放法如此之大以至于绝大多数科学运算软件都会溢出：$g(n) \gg 10^{308} \approx 2^{1023}$。但是，所有可能的初始条件$x_0$的数量一般远远小于$g(n)$。当$x_0$是一个IEEE标准的双精度浮点小数(64-比特)时[217]时，$\mathcal{N}_k = 2^{62} \ll g(n)$。因而，抵抗穷举攻击的复杂度为$O(\min(g(n), \mathcal{N}_k)) = O(2^{62})$。但是，由§6.3.1中的分析和上面的试验数据我们可以知道，在已知/选择明文攻击下的复杂度只有$O(2^e) = O(2^8) \ll O(2^{62})$。

*正如我们在§6.3.4指出的，文献[106]没有给出这方面的具体指令。

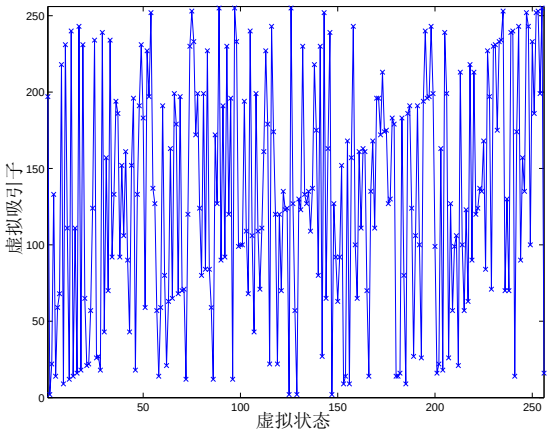


图 6.1: 关联映射$\boldsymbol{F}_v$

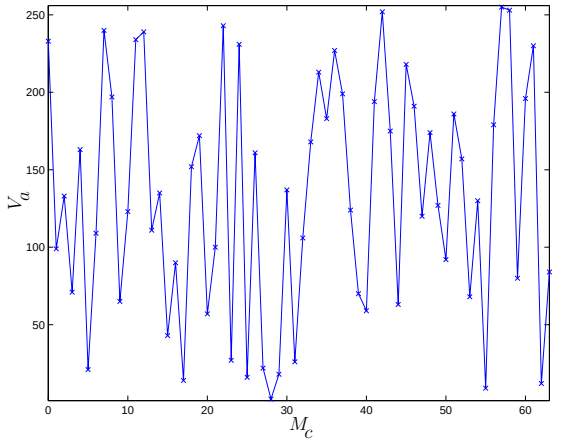


图 6.2: 置换矩阵**P**

§6.5 S. Papadimitriou等人的混沌密码中的积极一面

尽管S. Papadimitriou等人的混沌密码有不少问题，并且其基本结构不适合构造安全的混沌分组密码，该密码中采用的一些基本想法可能还是有用的。

一个有用的想法是将S. Papadimitriou等人的混沌密码从分组密码变换为流密码的可能性，这可能可以禁止重建虚拟吸引子列表和置换矩阵**P**的攻击方法(通过已知/选择明文)。一种可能的办法是产生时变的置换矩阵**P**，或者使用一个流式子密码混淆S. Papadimitriou等人的混沌密码的密文。在数字化混沌密码中使用这样的想法的例子在第2章中已经提到。

另外一个有用的点子是由拟混沌轨道构造虚拟状态空间的想法，它可能用来生成无陷门的非线性的S盒($n \times m$)[143, 144]。显然，这样的混沌S盒依赖于

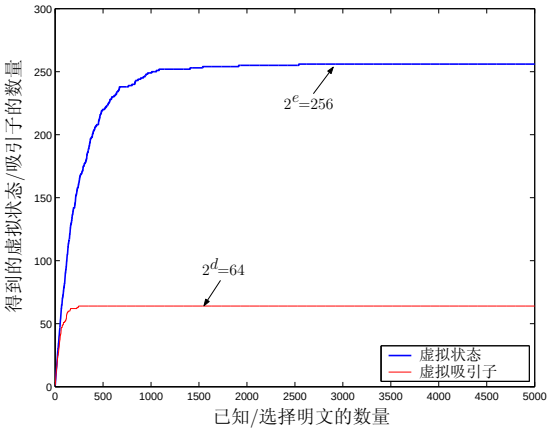


图 6.3: 由已知/选择明文得到的虚拟状态的数量

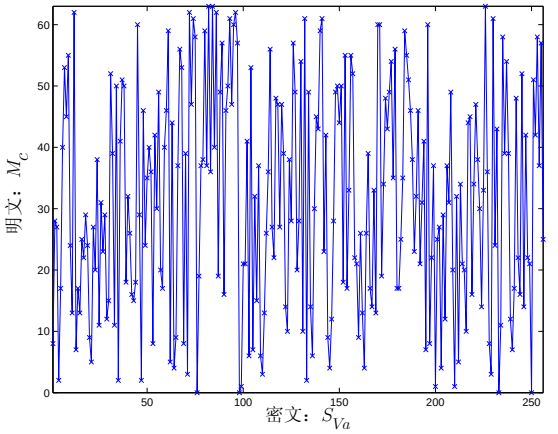


图 6.4: 由$O(2^e)$个已知/选择明文重建的密文-明文映射$\mathbf{P}^{-1} \circ \boldsymbol{F}_v$

密钥，因此可以集成到一些传统密码中构造新的基于混沌的分组密码。实际上，正如我们在§2.4.2中提到的，这类基于混沌S盒的密码已经被一些研究者提出[52, 105, 108, 112]，不过还需要更细致的研究以分析这类密码的性能。

§6.6 本章小结

在本章中，我们指出了S. Papadimitriou等人在文献[106]中提出的一类混沌密码的缺陷：1) d和e太小不能同时保证密码的实际实现和高安全性；2) 所有可能的虚拟状态空间的推导是错误的；3) 不当的安全性分析导致密码的安全性被高估了；4) 相当快的加密速度依赖于第一个缺陷；5) 数字化混沌系统的动力学特性退化需要补救；6) 缺乏明确的指示说明如何构造虚拟状态空间。

一般而言，由于d和e很小，S. Papadimitriou等人的密码是不实用，而且对已知/选择明文攻击和选择密文攻击不安全。如果关于d和e取值的缺陷被消除的话，关于加密速度的优点就会消失。另外，根据我们在§6.3.3中的讨论，该密码对穷举攻击的安全性不像文献[106]中分析的那么强，对穷举攻击的密钥熵不会大于$LN - \log_2(K/N!)$。

附录：§6.3.2中组合问题的递推解

这里，我们给出方程(6.2)和(6.3)的推导过程。

假设$g(n)$是相对n的所有可能的方法的数量。由于

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{a_1+a_2+\cdots+a_k=n} \binom{n}{a_1, a_2, \cdots, a_k} x_1^{a_1} x_2^{a_2} \cdots x_k^{a_k}, \tag{6.5}$$

我们有

$$g(n) = \sum_{\substack{a_1+a_2+\cdots+a_k=n \\ a_i \geq m}} \binom{n}{a_1, a_2, \cdots, a_k}。 \tag{6.6}$$

考虑下述指数生成函数：

$$\begin{aligned} \sum_{n\geq mk} g(n)\frac{x^n}{n!} &= \sum_{n\geq mk} \left(\sum_{\substack{a_1+a_2+\cdots+a_k=n \\ a_i \geq m}} \binom{n}{a_1, a_2, \cdots, a_k} \right) \frac{x^n}{n!} \\ &= \sum_{n\geq mk} \left(\sum_{\substack{a_1+a_2+\cdots+a_k=n \\ a_i \geq m}} \frac{n!}{a_1! \cdot a_2! \cdots a_k!} \right) \frac{x^{a_1+a_2+\cdots+a_k}}{n!} \\ &= \left(\sum_{a\geq m} \frac{x^a}{a!} \right)^k 。 \end{aligned} \tag{6.7}$$

从而$\left(\sum_{a\geq m} \frac{x^a}{a!} \right)^k$是$g(n)$的生成函数。

显然，导出用n, m, k表示的$g(n)$显式解析表达式是困难的，因此让我们来研究如何得到$g(n)$的递推解析式。

将方程(6.7)重写为$\sum_{i\geq mk} g(i)\frac{x^i}{i!} = \left(\sum_{a\geq m} \frac{x^a}{a!} \right)^k$，并对两边同时求导可得：

$$\sum_{i\geq mk-1} g(i+1)\frac{x^i}{i!} = k \cdot \left(\sum_{j\geq m} \frac{x^j}{j!} \right)^{k-1} \cdot \left(\sum_{j\geq m-1} \frac{x^j}{j!} \right), \tag{6.8}$$

两边同乘以$\sum_{j\geq m}\frac{x^j}{j!}$，

$$\begin{aligned}\left(\sum_{j\geq m}\frac{x^j}{j!}\right)\cdot\left(\sum_{i\geq mk-1}g(i+1)\frac{x^i}{i!}\right) &= k\cdot\left(\sum_{a\geq m}\frac{x^a}{a!}\right)^k\cdot\left(\sum_{j\geq m-1}\frac{x^j}{j!}\right)\\ &= k\cdot\left(\sum_{a\geq mk}g(a)\frac{x^a}{a!}\right)\cdot\left(\sum_{j\geq m-1}\frac{x^j}{j!}\right)\end{aligned}。\tag{6.9}$$

方程(6.9)的左边(LHS)为

$$\begin{aligned}\text{LHS} &= \sum_{i\geq mk+m-1}\left(\sum_{\substack{s+t=i\\ s\geq m\\ t\geq mk-1}}\left(\frac{g(t+1)}{s!t!}x^i\right)\right)\\ &= \sum_{i\geq mk+m-1}\left(\sum_{\substack{s+t=i\\ s\geq m\\ t\geq mk-1}}g(t+1)\binom{i}{s}\right)\frac{x^i}{i!}。\end{aligned}\tag{6.10}$$

方程(6.9)的左边(RHS)为

$$\begin{aligned}\text{RHS} &= k\cdot\sum_{i\geq mk+m-1}\left(\sum_{\substack{s+t=i\\ s\geq m-1\\ t\geq mk}}\left(\frac{g(t)}{s!t!}x^i\right)\right)\\ &= \sum_{i\geq mk+m-1}k\cdot\left(\sum_{\substack{s+t=i\\ s\geq m-1\\ t\geq mk}}g(t)\binom{i}{s}\right)\frac{x^i}{i!}。\end{aligned}\tag{6.11}$$

从而我们有下述结论：当$i\geq mk+m-1$时，

$$\sum_{\substack{s+t=i\\ s\geq m\\ t\geq mk-1}}g(t+1)\binom{i}{s}=k\cdot\sum_{\substack{s+t=i\\ s\geq m-1\\ t\geq mk}}g(t)\binom{i}{s}。\tag{6.12}$$

由于$s+t=i$，$\binom{i}{s}=\binom{i}{t}$，则上式可以转换为如下形式：

$$\sum_{t=mk-1}^{i-m}g(t+1)\binom{i}{t}=k\cdot\sum_{t=mk}^{i-m+1}g(t)\binom{i}{t}。\tag{6.13}$$

在上式左侧作变量代换$t'=t+1$可得

$$\sum_{t'=mk}^{i-m+1}g(t')\binom{i}{t'-1}=k\cdot\sum_{t=mk}^{i-m+1}g(t)\binom{i}{t}。\tag{6.14}$$

由方程(6.14)，我们可以得到$g(n)$的递推解。

当$n = mk$时：

$$g(n) = \binom{mk}{m, m, \cdots, m} = \frac{(mk)!}{(m!)^k}。 \tag{6.15}$$

当$n > mk$时：令$i - m + 1 = n$，$i = n + m - 1$。将$i = n + m - 1$代入方程(6.14)可得：

$$\sum_{t=mk}^{n} g(t)\binom{n+m-1}{t-1} = k \cdot \sum_{t=mk}^{n} g(t)\binom{n+m-1}{t}。 \tag{6.16}$$

化简上述方程得到：

$$g(n) = \frac{\sum_{t=mk}^{n-1} g(t)\left(k \cdot \binom{n+m-1}{t} - \binom{n+m-1}{t-1}\right)}{\frac{n-mk}{k} \cdot \binom{n+m-1}{n}}。 \tag{6.17}$$

由方程(6.15)和方程(6.17)，该问题得解。

第七章 两类Yen-Guo混沌图象加密算法的分析

§7.1 引言

随着互联网的迅猛发展，网络上的数字图象的传输和交换变得越来越频繁，这使得数字图象的安全性变得越来越重要。另外，在很多应用场合数字图象的安全存储和传输都需要特定的可靠性高的安全性，比如付费电视，医学成像系统，军用图象数据库/通信系统，还有在线图象服务(如在线的个人相册)，等等。为了满足图象安全的需要，很多图象加密算法被提出[18, 85, 89, 132–138, 221–225]，不过其中的一些算法[223–225]已经知道是不安全的[221, 226]。

我们在§2.4.6中已经提到，不少混沌图象加密算法[18, 85, 89, 132–138]已经被提出，其中的相当一部分是由J.-C. Yen和J.-I. Guo(等人)提出的[132–135, 137, 138]。Yen-Guo图象加密算法基本上都遵循一个类似的设计思路：一个混沌映射(Logistic映射在所有的Yen-Guo混沌图象加密算法中使用)作为一个混沌PRNG，该PRNG用来控制图象象素的秘密置换或替换。从严格的密码学角度看，大部分Yen-Guo混沌图象加密算法都不够安全，已知/选择明文攻击的复杂度比穷举攻击小(部分加密算法可以被在仅有几个已知明文图象的情况下被攻破)。本章将介绍我们关于两种Yen-Guo混沌图象加密算法的密码分析工作，这两类图象加密算法分别被J.-C. Yen和J.-I. Guo(等人)称为CKBA(Chaotic Key-Based Algorithm)[134]和BRIE(Bit Recirculation Image Encryption)[132]。两种方法都没有经过仔细的设计以避免已知/选择明文攻击，因此都不够安全。Yen-Guo混沌图象加密算法的不安全说明需要加强信号/图象处理领域和密码学两个领域研究之间的联系。

本章的组织如下。在§7.2中，我们对CKBA和BRIE作一简单介绍。CKBA的密码分析工作在§7.3中给出，并给出了一些例子说明攻击的可行性。BRIE的一些特殊的安全问题在§7.4中给出。对BRIE的密码分析在§7.5中进行讨论。一些具体的试验结果也包含在§7.4和§7.5中。在§7.6中我们讨论了对CKBA和BRIE可能的改进措施。最后一节是本章小结。

§7.2 两类Yen-Guo图象加密方法：CKBA和BRIE

§7.2.1 CKBA：Chaotic Key-Based Algorithm(基于混沌密钥的算法)

CKBA的加密过程可以简要地描述如下。假设明文图象的尺寸为$M \times N$。选择两个字节变量$key1$、$key2$和一个混沌系统(Logistic映射)的初始条件$x(0)$作为系统密钥。运行该混沌系统产生拟混沌轨道$\{x(i)\}_{i=0}^{MN/8-1}$(假设$MN|8$)。然后由$x(i)$的16-比特二进制表示形式$x(i) = 0.b(16i+0)b(16i+1)\cdots b(16i+15)$生成一个伪随机比特序列$\{b(i)\}_{i=0}^{2MN-1}$。一旦生成了$\{b(i)\}$，加密过程即可开始。对明

文象素$f(x,y)(0 \le x \le M-1, 0 \le y \le N-1)$，对应的密文象素$f'(x,y)$由下述规则确定：

$$f'(x,y) = \begin{cases} f(x,y) \text{ XOR } key1，b'(x,y) = 3 \\ f(x,y) \text{ XNOR } key1，b'(x,y) = 2 \\ f(x,y) \text{ XOR } key2，b'(x,y) = 1 \\ f(x,y) \text{ XNOR } key2，b'(x,y) = 0 \end{cases}， \tag{7.1}$$

这里$b'(x,y) = 2 \times b(l) + b(l+1)$，$l = x \times N + y$。XOR和XNOR操作都是对合的，因此解密过程和加密过程完全相同。由于并不是所有的密钥都可以产生视觉上足够混乱的密文图象，需要满足下述选择$key1$和$key2$的准则：$\sum_{i=0}^{7}(a_i \oplus d_i) = 4$，这里$key1 = \sum_{i=0}^{7} a_i \times 2^i$，$key2 = \sum_{i=0}^{7} d_i \times 2^i$。

§7.2.2 BRIE：Bit Recirculation Image Encryption(比特循环移位图象加密法)

BRIE的基本加密思路是象素值的循环移位，该移位操作被一个混沌伪随机序列所控制。BRIE的密钥是两个整数α, β和一个一维混沌系统(Logistic映射)的初始条件$x(0)$。这里，我们假设明文图象的尺寸为$M \times N$。运行该混沌系统生成拟混沌轨道$\{x(i)\}_{i=0}^{\lceil (MN+1)/8 \rceil - 1}$。然后由8-比特二进制表示形式$x(i) = 0.b(8i+0)b(8i+1)\cdots b(8i+7)$生成一个伪随机比特流$\{b(i)\}_{i=0}^{MN}$。对于明文象素$f(x,y)(0 \le x \le M-1, 0 \le y \le N-1)$，对应的密文象素$f'(x,y)$如下确定：

$$f'(x,y) = ROLR_p^q(f(x,y)), \tag{7.2}$$

这里$p = b(N \times x + y)$，$q = \alpha + \beta \times b(N \times x + y + 1)$，$ROLR_p^q$是一个由参数$p$控制的$q$比特循环移位操作：

$$ROLR_p^q(x = b_7 b_6 \cdots b_0) = \begin{cases} \sum_{i=0}^{7} b_i \cdot 2^{(i-q+8) \bmod 8}, p = 0 \\ \sum_{i=0}^{7} b_i \cdot 2^{(i+q) \bmod 8}, p = 1 \end{cases}。 \tag{7.3}$$

解密过程可以表示为：

$$f(x,y) = ROLR_{1-p}^q(f'(x,y)) = ROLR_p^{8-q}(f'(x,y))。 \tag{7.4}$$

显然，BRIE是一种象素值替换密码，即位置(x,y)处的密文象素仅由相同位置的明文象素决定。J.-C. Yen和J.-I. Guo声称BRIE需要很低的运算复杂度，而且由于$b(i)$包含$MN+1$个由混沌迭代生成的秘密比特，因此也具有很高的安全性。但是，我们将指出在BRIE中存在一些严重的安全问题，并指出已知/选择明年文攻击可以攻破BRIE。BRIE逐列加密明文图象，这在实际应用中不是很方便。在本章中，我们将BRIE改为在逐行加密模式下运行，这不会影响BRIE的任何性能。

§7.3 CKBA的密码分析

§7.3.1 唯密文攻击

J.-C. Yen和J.-I. Guo声称：由于$\{b(i)\}_{i=0}^{2MN-1}$有$2MN$个伪随机比特，CKBA抵抗唯密文攻击的复杂度为2^{2MN}。事实上这个说法是不对的，考虑下述事实：这$2MN$个比特被混沌系统方程和其初始条件$x(0)$唯一确定，而x_0只有16个秘密比特。实际上CKBA的密钥是$key1$，$key2$和$x(0)$，在唯密文攻击下通过穷举攻击可以得到密钥。由于密钥总共包含$2\times 8+16=32$个比特，密钥熵应为32。考虑到密钥选择的限制$\sum_{i=0}^{7}(a_i\oplus d_i)=4$，不是所有的密钥都可以在CKBA中使用，在全部$2^{16}\times 2^8\times 2^8=2^{16}$个密钥中只有$2^{16}\times 2^8\times C_8^4=2^{24}\times 70\approx 2^{30}$个密钥是可用的。因此密钥熵大概为$14+16=30$。

准确的攻击复杂度可以如下估计。平均而言，对于一幅明文图象，生成所有的$\{b(i)\}$需要$MN/8$次混沌迭代，以及$(2^8\times 70)\times MN=17920\times MN\approx 2^{14}\times MN$次XOR/XNOR操作。假设一次混沌迭代与一次XOR/XNOR操作耗时相等，则总的攻击复杂度为$2^{15}\times\left(\frac{MN}{8}+2^{14}\times MN\right)\approx 2^{29}MN$。当$M,N$不太小时($M>4$，$N>4$)，这个复杂度比$2^{2MN}$要小得多。以上分析说明CKBA对穷举攻击的安全性被其作者J.-C. Yen和J.-I. Guo高估了。由于数字计算机和分布式运算的快速发展，一个实际安全的密码需要$O(2^{128})$量级的安全复杂度，CKBA的安全性显然不够。不失一般性，假设$M=N=1024=2^{10}$(这是一幅较大的数字图象的典型尺寸)，攻击复杂度为$2^{29}MN=2^{49}$。

§7.3.2 已知/选择明文攻击

在已知/选择明文攻击中，CKBA可以在仅仅已知/选择一幅明文图象及其密文图象的情况下被攻破。假设攻击者已知一幅明文图象f和其对应的密文图象f'(大小均为$M\times N$)。对于明文象素$f(x,y)$，密文象素$f'(x,y)$必为下述四个值中的一个：$f(x,y)$ XOR $key1$，$f(x,y)$ XNOR $key1$，$f(x,y)$ XOR $key2$，$f(x,y)$ XNOR $key2$。由于a XNOR $b=a$ XOR $\bar{b}$，$f(x,y)$ XOR $f'(x,y)$必为下述四个值中的一个：$key1$，$\overline{key1}$，$key2$，$\overline{key2}$。因此，如果我们将f和f'进行XOR操作，可以得到一幅掩模图象f_m，如果一幅密码图象的大小不比$M\times N$大的话，我们可以使用f_m替代密钥K解密该密文图象。对于尺寸大于$M\times N$的密文图象而言，左侧的MN个明文象素可以成功地解密。得到f_m的计算复杂度只有$O(MN)$，它独立于密钥$key1$，$key2$和$x(0)$。

如果我们要解密一个具有较大尺寸的密文图象的全部内容，就需要知道正确的密钥值$K=\{key1,key2,x(0)\}$。基于f_m，可以很容易地计算出K。由于f_m只包含四个可能的灰度值：$\{key1,\overline{key1},key2,\overline{key2}\}=\{k_1,k_2,k_3,k_4\}$，通过穷举猜测我们可以得到$key1$和$key2$的正确值。这个搜索过程如下所述：

- **第一步**：猜测$key1=k_m$(令$m=1\sim 4$)，以及$key2=k'_{m'}$(令$m'=1\sim$

2)，这里k_1'和k_2'是在$key1$已经确定的情况下的两个可能的值(另外两个是$key1$和$\overline{key1}$)。

- **第二步**：使用下述规则对所有象素计算$b'(x,y)$：

$$b'(x,y)=\begin{cases}3, & f_m(x,y)=key1\\ 2, & f_m(x,y)=\overline{key1}\\ 1, & f_m(x,y)=key2\\ 0, & f_m(x,y)=\overline{key2}\end{cases}。\tag{7.5}$$

- **第三步**：由$b'(x,y)$生成拟混沌轨道$\{x(i)\}_{i=0}^{MN/8-1}$。
- **第四步**：检验$\{x(i)\}_{i=0}^{MN/8-1}$是否满足混沌方程。如果是的话，则搜索过程结束，并输出当前的$key1$，$key2$和$x(0)$，这就是正确的密钥值K。这里请注意我们实际上不需要计算整个拟混沌轨道，而只需要计算两个混沌状态$x(0)$和$x(1)$，这对于判断拟混沌轨道是否满足混沌方程已经足够了。

显然，从f_m推出密钥K的计算复杂度主要由第二步和第三步决定。一般来说，该复杂度为$O(MN)$，大约等于得到f_m的复杂度。

对于比已知/选择明文图象尺寸大的密文图象，还有另外一个可能的办法解密该密文图象。由§2.5中的讨论我们知道：当混沌系统在L-比特有限计算精度下实现时，拟混沌轨道的周期循环会比2^L小得多。对于CKBA而言，有限精度为$L=16$，每个拟混沌轨道的周期不会大于2^{16}，这与许多明文图象的尺寸相比不够大。对一个256×256的图象，生成的拟混沌轨道$\{x(i)\}$的长度为$MN/8=2^{13}$。对于很多初始条件$x(0)$而言，$\{x(i)\}$的循环周期甚至比2^{13}还要小。这样的话，如果已知掩模图象f_m的尺寸为$256\times256=2^{16}$或者更大时，我们可能从该图象得到一个完整的拟混沌轨道周期，从而得到任何尺寸的掩模图象。这也就是说，不需要得到准确的密钥K，一个尺寸足够大(大于等于256×256)的掩模图象f_m就可以解密所有的密文图象了。我们的试验支持这个论断(参看下一小节和图7.4)。假设较大的密文图象尺寸为$M'\times N'$，由f_m得到f_m'的复杂度为$O(M'N'+MN)$。

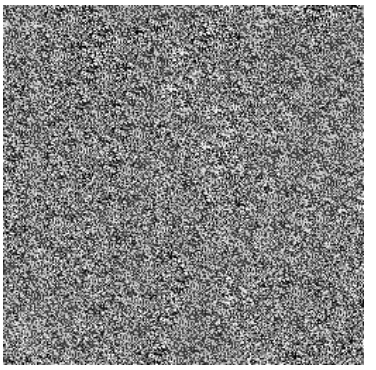
我们知道，已知/选择明文攻击在同一个密钥被反复使用加密多个明文的情况下非常有用，尤其是很大数量的明文都使用同一个密钥加密的情况[143, 144]。作为一个好的密码系统，抵抗已知明文攻击的能力是非常重要的，而且一般是需要的，这是因为下述事实：如果禁止同一密钥的反复使用，密钥管理在很多应用中将会变得更为复杂不便和困难。显然，文献[134]中建议的使用CKBA加密MPEG视频流不是一个明智的做法。一旦加密视频流中的一个明文帧被攻击者得到，他/她就等于得到了所有的帧，即整个视频流。

§7.3.3 试验

为了验证上面的已知/选择明文攻击的实用性，我们在本小节给出一些实际的试验结果。控制参数$r=4$的Logistic映射在我们的试验中用作混沌系统，它

以16-比特精度实现。

a) Lenna.bmp(256×256)



b) 加密后的Lenna.bmp

图 7.1: 一个已知/选择明文图象和相应的密文图象：CKBA

对于一个伪随机产生的密钥$K = \{key1, key2, x(0)\}$，一个已知的256×256的明文图象f(Lenna.bmp)及其密文图象f'在图7.1中给出。我们可以很容易地得到掩模图象$f_m = f$ XOR f'(图7.2a)。

当K密钥用来加密另外一幅尺寸相同的明文图象时(图7.2b–c)，密文图象可以直接用f_m解密(参看图7.2d)。

当K用来加密一个具有较大尺寸的密文图象(384×384，参看图7.3a–b)时，f_m只能解密图象左侧MN个象素(参看图7.3c)。为了解密整个图象，我们需要由f_m导出正确的密钥K。使用上一小节描述的方法，我们可以很快得到$key1 = 92, key2 = 36, x(0) = 12830/2^{16}$，然后整个密文图象即可被解密(参看图7.3d)。

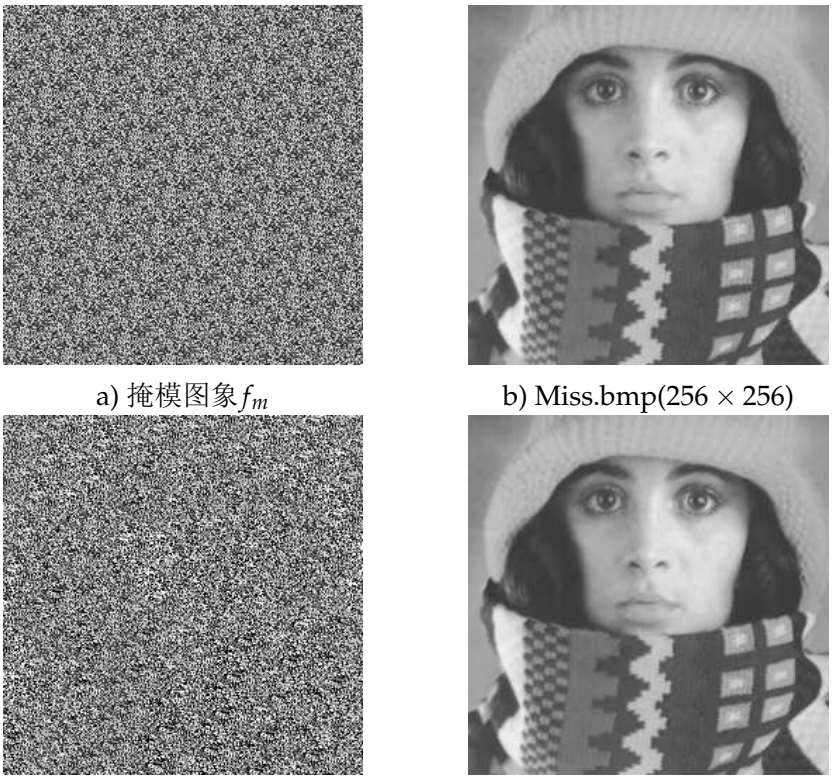
在一小节中，我们还提到了另外一种解密较大明文图象的办法。观察由已知明文图象Lenna.bmp(256×256)得到的掩模图象f_m(图7.2c)，我们可以看到一种规则的模式重复出现了9次。这意味着$\{x(i)\}_{i=0}^{MN/8-1}$的循环周期大约等于$2^{16}/(8 \times 9) = 2^{16}/72$。因此，由$f_m$我们可以很容易地得到$384 \times 384$明文图象的掩模图象$f'_m$，$f'_m$显示在图7.4a中。使用$f'_m$的解密结果显示在图7.4b中。

§7.4 BRIE的一些安全缺陷

§7.4.1 *ROLR*操作的本质缺陷

由伪随机混沌序列$\{b(i)\}$控制的*ROLR*操作是BRIE的核心。在BRIE中使用时，*ROLR*有两个本质缺陷，这会降低BRIE的安全性，并限制其在实际中的应用范围。

1) 加密后部分明文象素可能保持不变($f'(x,y) = f(x,y)$)。如果一幅图象中包含过多的这种象素，则明文图象在密文图象中可能朦胧可见。明文象素可



a) 掩模图象f_m　b) Miss.bmp(256×256)

c) 加密后的Miss.bmp　d) 使用f_m解密的Miss.bmp

图 7.2: 使用f_m破解加密的Miss.bmp：CKBA

以分为下述四种类别*。**C1**) 0，255：$f'(x,y) \equiv f(x,y)$，$\forall \alpha, \beta$。**C2**) 85，170：如果$\alpha \bmod 2 = 0$，当$q = \alpha$时$f'(x,y) = f(x,y)$；如果$\alpha + \beta \bmod 2 = 0$，当$q = \alpha + \beta$时$f'(x,y) = f(x,y)$；如果$\alpha \bmod 2 = (\alpha + \beta) \bmod 2 = 0$，$f'(x,y) \equiv f(x,y)$。**C3**) 17, 34, 51, 68, 102, 119, 136, 153, 187, 204, 221, 238：如果$\alpha \bmod 4 = 0$，当$q = \alpha$时$f'(x,y) = f(x,y)$；如果$\alpha + \beta \bmod 4 = 0$，当$q = \alpha + \beta$时$f'(x,y) = f(x,y)$；如果$\alpha \bmod 4 = (\alpha + \beta) \bmod 4 = 0$，$f'(x,y) \equiv f(x,y)$。**C4**) 其他所有的灰度值：如果$\alpha \bmod 8 = 0$，当$q = \alpha$时$f'(x,y) = f(x,y)$；如果$\alpha + \beta \bmod 8 = 0$，当$q = \alpha + \beta$时$f'(x,y) = f(x,y)$；如果$\alpha \bmod 8 = (\alpha + \beta) \bmod 8 = 0$，$f'(x,y) \equiv f(x,y)$。

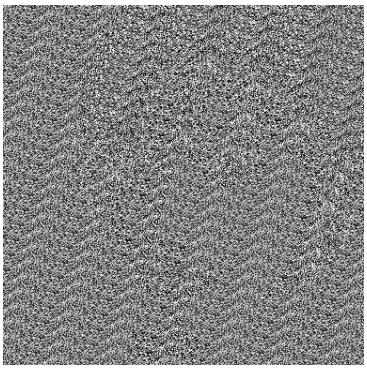
2) 对于明文图象中具有固定灰度值的区域而言，最多八种†灰度值可能出现在密文图象的该区域中。这个事实可能造成该区域的边缘在密文图象中可分辩。

显然，如果密文图象中包含太多灰度值无变化的象素和/或明文图象具有太多的灰度值固定的子区域，仅仅通过观察密文图象就可能从中得到一些关于明

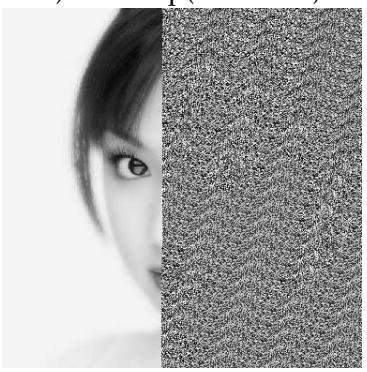
*不同的重复模式在象素的不同灰度值的二进制表达形式中出现：C1) 八个重复比特– 0 (00000000)，1 (11111111)；C2) 四个重复的2-比特片断– 85 (01010101)，170 (10101010)；C3) 两个重复的4-bit片断– 17 (00010001)，等等；C4 – 没有任何重复模式。

†该数值由固定灰度的取值决定：C1 – 1，C2 – 1或2，C3 – $1 \sim 4$，C4 – $1 \sim 8$。

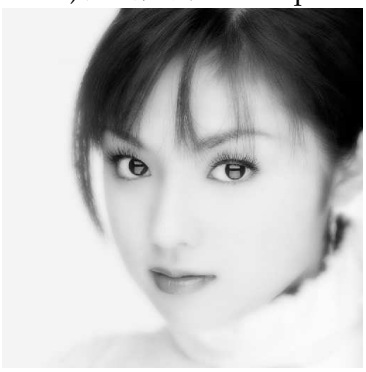
a) Girl.bmp(384 × 384)



b) 加密后的Girl.bmp

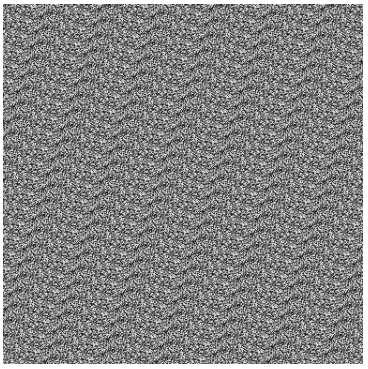


c) 使用f_m解密的Girl.bmp



d) 使用f_m得到K后解密的Girl.bmp

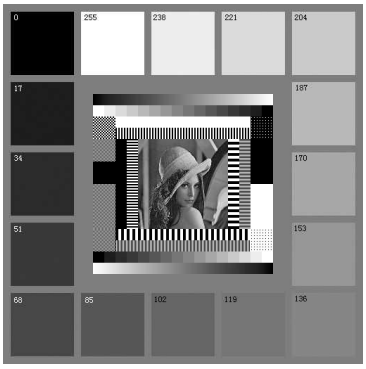
图 7.3: 使用f_m得到K破解加密的Girl.bmp：CKBA



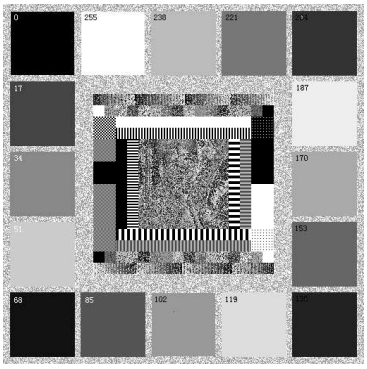
a) 由f_m(256 × 256)得到的掩模图象f'_m(384 × 384)

b) 使用f'_m解密的Girl.bmp

图 7.4: 使用由f_m得到的新掩模图象f'_m破解加密的Girl.bmp：CKBA



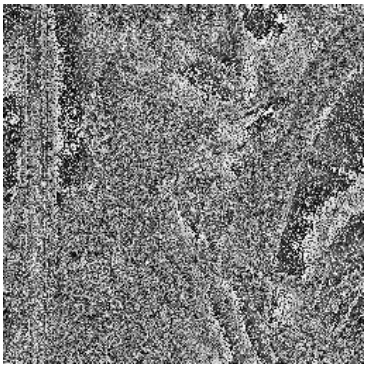
a) Test_Pattern.bmp



b) 加密后的Test_Pattern.bmp

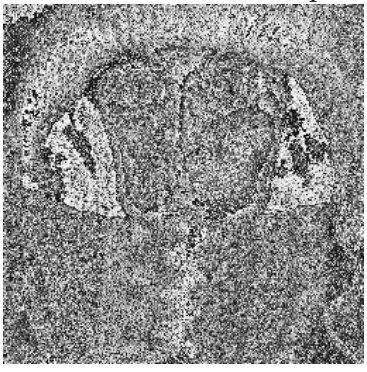
图 7.5: 使用BRIE加密的一幅特殊图象

a) Lenna.bmp



b) 加密后的Lenna.bmp

c) Miss.bmp



d) 加密后的Miss.bmp

图 7.6: 使用BRIE加密的图象Lenna.bmp和Miss.bmp，参数为$\alpha = 5, \beta = 1, x(0) = 0.75$

文图象的有用信息。在图7.5中，我们给出了针对一个特别设计的图象的试验结果，该图象包含了全部四种类别的象素(16个正方形区域的灰度值依次为0, 17, 34,

..., 221, 238, 255)。相关参数为$\alpha = 2, \beta = 4, x(0) = 0.75$，混沌系统选作控制参数为3.9的Logistic映射。

实际上，第二个事实可以推广到更为一般的情形。对于一个给定的子区域，如果全部灰度值都比较接近并且只有少量灰度值的低位字节是不同的，在密文的相应子区域中会有强边缘浮现。一般而言，子区域中灰度值越接近，这种边缘就越清晰。在图7.6中，Lenna.bmp和Miss.bmp作为例子演示了这个问题。我们可以在密文图象中找到明文图象的很多重要的大边缘。

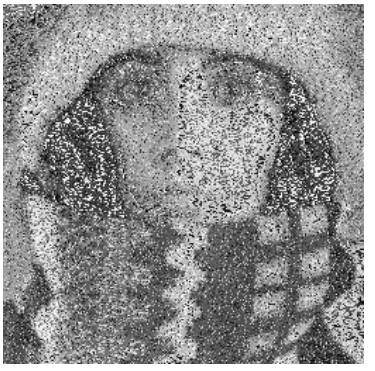
§7.4.2 关于α, β的安全问题

α, β的选取在文献[132]中没有提到。我们发现α, β必须服从下述三个限制以避免可能的不安全因素，满足这些限制的值只有$7 \times 7 - 7 - 2 = 40$个，这比原来的数量小得多，对密码分析是有利的。

R1) $\mathbf{1 \le \alpha \le 7, 1 \le \beta \le 7}$。考虑到$ROLR_p^q = ROLR_p^{q+8}$，这个限制是很自然的。

R2) $\boldsymbol{\alpha + \beta \neq 8}$。如果$\alpha + \beta = 8$，超过一半的灰度值将服从$f'(x,y) = f(x,y)$(回顾上一小节的讨论)。这个事实会导致明文图象在密文图象中粗糙地显示出来(密文图象类似叠加了较大椒盐噪声[216]的明文图象)。在图7.7中，我们给出了$\alpha = 6, \beta = 2, x(0) = 0.75$时图象Lenna.bmp和Miss.bmp的加密结果。

a) 加密后的Lenna.bmp



b) 加密后的Miss.bmp

图 7.7: 使用BRIE加密的Lenna.bmp和Miss.bmp，参数为$\alpha = 6, \beta = 2, x(0) = 0.75$(与图7.6比较)

R3) $\boldsymbol{\alpha \bmod 8 \neq 1, 7}$或者$\boldsymbol{(\alpha + \beta) \bmod 8 \neq 1, 7}$。如果不满足该限制(当$\alpha = 1, \beta = 6$或者$\alpha = 7, \beta = 2$)，由于$ROLR_p^7 = ROLR_{1-p}^1$并且$ROLR_p^9 = ROLR_p^1$，所有的明文象素将被1-比特的$ROLR$操作加密。结果，相当大的明文图象的可视信息会由密文图象中泄漏出来。当$\alpha = 1, \beta = 6, x(0) = 0.75$时，关于图象Lenna.bmp和Miss.bmp的加密结果在图7.8中给出。可以看到密文图象包含如此之多的强边缘以至于明文图象很容易大致猜测出来。

a) 加密后的Lenna.bmp

b) 加密后的Miss.bmp

图 7.8: 使用BRIE加密的Lenna.bmp和Miss.bmp，参数为$\alpha = 1, \beta = 6, x(0) = 0.75$(与图7.6比较)

§7.4.3 被高估的对穷举攻击的安全性

在文献[132]中J.-C. Yen和J.-I. Guo声称：由于密文图象由$\{b(i)\}_{i=0}^{MN}$确定，共有2^{MN+1}种可能的加密结果；而所有的$\{b(i)\}$对违法用户而言都是保密的，重建$\{x(i)\}_{i=0}^{\lceil (MN+1)/8 \rceil - 1}$是非常困难的，因此BRIE是足够安全的。然而，由于下述事实上述论断是不正确的：全部$MN+1$个比特由混沌系统及其初始条件$x(0)$唯一确定。一旦攻击者得到$x(0)$，他/她即可重建$\{b(i)\}_{i=0}^{MN}$而解密密文图象。$x(0)$可以通过穷举攻击得到。当然，为了破解BRIE，我们还需要知道α, β。

现在让我们计算一下所有可能的密钥数量。假设混沌系统采用双精度浮点运算进行迭代，则$x(0)$具有63个有效比特(由于$x(0) \geq 0$符号位必然是零)。考虑到可用的α, β数量为40，密钥总数为40×2^{63}。

穷举攻击的确切计算复杂度可以如下估算。对于每个密钥，产生$\{b(i)\}_{i=0}^{MN}$需要$\lfloor (MN+1)/8 \rfloor$次混沌迭代，加密密文图象需要MN次$ROLR$操作。假设一次混沌迭代和一次$ROLR$操作耗费相同的时间，平均的穷举攻击复杂度为$(40 \times 2^{63}/2) \times 9(MN+1)/8 \approx 2^{67.5} \times MN$，当$M, N$不太小时该复杂度比$2^{MN}$小得多。假设$M = N = 512 = 2^9$，攻击复杂度为$2^{67.5} \times MN = 2^{85.5} \ll 2^{MN} = 2^{262144}$。显然，BRIE对穷举攻击的安全性被J.-C. Yen和J.-I. Guo在文献[132]中高估了。

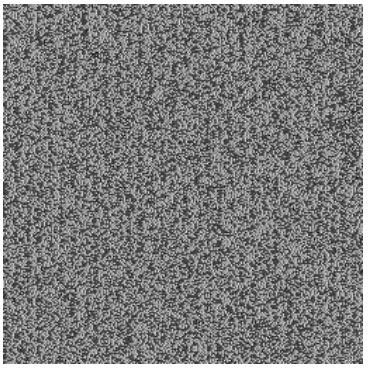
§7.5 BRIE的已知/选择明文攻击

如果攻击者得到一幅明文图象，他/她就可能马上攻破BRIE，这对应着已知/选择明文攻击。

§7.5.1 使用掩模矩阵Q攻击BRIE

假设已知/选择明文图象为f，其对应的密文图象为f'(尺寸均为$M \times$

N)。对于明文象素$f(x,y)$，密文象素$f'(x,y)$必然是下述的八个值中的一个：$ROLR_0^1(f(x,y)) \sim ROLR_0^7(f(x,y))$。通过比较$f(x,y)$和$f'(x,y)$，我们可以很容易地找到至少一个整数*$q(x,y)$满足$f'(x,y) = ROLR_0^{q(x,y)}(f(x,y))$。重复以上过程，我们可以得到一个掩模矩阵$Q = [q(x,y)]_{M\times N}$。如果$f(x,y)$属于类别C4(回顾§7.4.1)，该整数$q(x,y)$可以用来解密其他密文图象中该位置上的密文象素。如果$f(x,y)$属于类别$C1 \sim C3$，一般来说$q(x,y)$不能用来解密同一位置上的其他密文象素。幸运的是，对于大多数数字图象，灰度属于类别$C1 \sim C3$的象素要大大少于属于C4的象素。这说明掩模矩阵Q可以用来解密以同一密钥加密的其他密文图象。如果密文图象的尺寸不大于Q的尺寸，除了少数象素外明文图象可以被完全恢复。选择Lenna.bmp作为已知/选择明文图象，我们得到了一个掩模矩阵Q并成功地用它解密了使用同样密钥加密的另外一幅图象Miss.bmp。掩模矩阵Q和解密后的Miss.bmp图象在图7.9中给出，其中Q按照下述原则转换为一个伪灰度图象f_Q：$F_Q(x,y) = q(x,y) \times 32$。可以看到只有极少量的明文象素没有被恢复，这些象素对应的Lenna.bmp中的明文象素灰度值属于类别$C1 \sim C3$。



a) 由已知图象Lenna.bmp得到的掩模矩阵Q

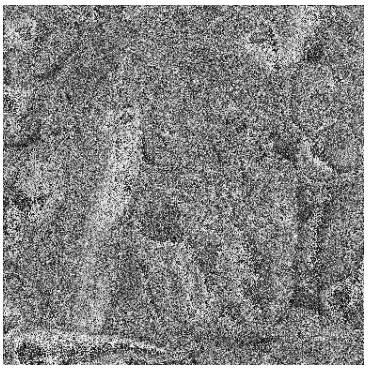
b) 使用Q解密的Miss.bmp

图 7.9: 使用掩模矩阵Q破解BRIE加密的Miss.bmp，参数为$\alpha = 5, \beta = 1, x(0) = 0.75$

使用Q作为破解工具有下面两个问题：a) 对于尺寸大于$M \times N$的密文图象，只有大约$M \times N$个象素可以被恢复。如果图象比$M \times N$大的太多，被恢复的部分可能不能反映整个图象的正确内容。图7.10给出了一个较大的图象Peppers.bmp的解密结果，它的尺寸为384×384。b) 如果已知明文包含太少的C4象素，则没有足够多的有效$q(x,y)$用来解密密文象素。增加已知明文图象的数量，可以解决第二个问题。

*如果$f(x,y)$属于类别C4，仅有一个这样的整数存在。对于类别C1，这样的整数数量为8；对于C2，为4；对C3，为2。

a) Peppers.bmp(384 × 384)



b) 加密后的Peppers.bmp

c) 使用Q解密的Peppers.bmp

图 7.10: 使用掩模矩阵Q破解BRIE加密的Peppers.bmp，参数为$\alpha = 5, \beta = 1, x(0) = 0.75$

§7.5.2 由Q确定密钥

很明显，Q存在的问题的一个最根本的解决办法就是得到密钥α, β和$x(0)$。一旦得到Q，我们可以使用下述步骤找到α, β以及等效的$x(0)$。

第一步：将已知/选择明文图像划分为8个象素为单位的块，然后寻找一个C4象素$f(x^*, y^*)$，使得其后的连续两个块包含的象素全部都是C4象素(一般来说这是容易的)。

第二步：令$\alpha' = 1 \sim 7$，$\beta' = 1 \sim 7$。

第三步：如果α'，β'不服从§7.4.2中的限制**R1**，**R2**和**R3**回到**第二步**；

第四步：计算下述数值：$q(1) = \alpha', q(2) = (\alpha' + \beta') \bmod 8, q(3) = 8 - q(1), q(4) = (8 - q(2)) \bmod 8$。

第五步: 由$f(x^*, y^*)$开始的16个C4象素的掩模参数$q(x, y)$得到16个比特$b(1) \sim b(16)$*：

- 如果$q(x, y) \notin \{q(1), q(2), q(3), q(4)\}$，返回**第二步**；

*注意对于任意α, β，$\{q(1), q(3)\} \cap \{q(2), q(4)\} = \varnothing$始终成立。

- 如果$q(x,y) \in \{q(1), q(3)\}$，$b(i) = 0$；
- 如果$q(x,y) \in \{q(2), q(4)\}$，$b(i) = 1$。

第六步：使用$b(1) \sim b(16)$构造两个二进制小数：$x1 = \sum_{i=1}^{8} b(i) \times 2^{-i}$和$x2 = \sum_{i=1}^{8} b(i+8) \times 2^{-i}$。
第七步：如果$x2$和$x1$服从混沌方程，将当前的α'和β'标记为正确参数的候选值。返回**第二步**直到$\alpha' = 7$并且$\beta' = 7$。
第八步：在所有的候选参数中寻找正确的α和β。
第九步：穷举攻击$x1$的其他$n-8$个未知比特，这里n是拟混沌轨道的实现精度。

在上述过程中，如果16个连续的C4象素是明文图象的头16个象素的话，$x1 = x(0)$；否则$x1$是一个$x(0)$的等效密钥，因为$x1$可以用来解密所有在$x1$之后出现的密文象素。上述过程的搜索复杂度主要由第九步决定。当$n = 63$(双精度浮点算法)，复杂度为2^{55}，还是有点大。但是和简单穷举攻击比较起来(参看§7.4.3)，密钥熵降低了至少$\log_2(40 \times 2^8) \approx 13.3$个比特。

§7.6 如何改进CKBA和BRIE?

在前面我们已经通过理论分析和试验表明CKBA和BRIE对已知/选择明文攻击都不够安全。在本节中我们将讨论如何增强这两类混沌图象加密算法及相关措施的性能。

§7.6.1 改进CKBA

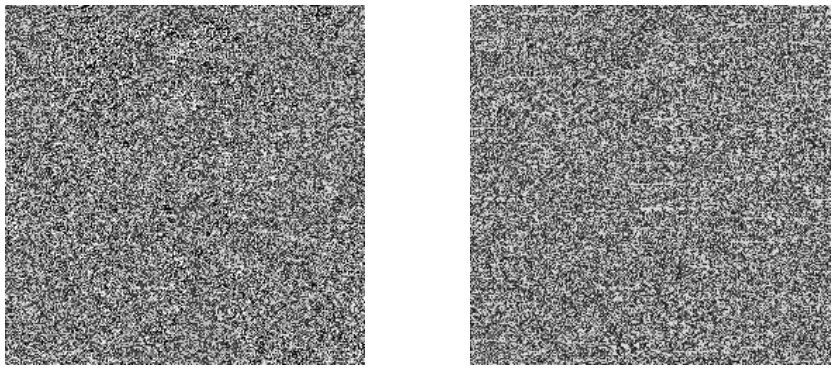
增强CKBA安全性的最简单的办法是增加*key*1和*key*2的比特数n，以及$x(0)$的实现精度n'。相应地，选择*key*1和*key*2的准则也变为$\sum_{i=0}^{7}(a_i \oplus d_i) = n/2$*。这样一种简单的增强型CKBA对唯密文攻击具有更强的抵抗力。假设$n > 8$，$n' > 16$，可以算出攻击复杂度为$(2^{n'-1}/(n'/2)) \times (2^n \times C_n^{n/2}/2) \times (MN)^2 = 2^{n+n'-1}/n' \times C_n^{n/2} \times (MN)^2$。当$n = n' = 32$(考虑32-比特的数据在数字计算机中使用最为广泛)以及$M = N = 512 = 2^9$时，复杂度近似等于$2^{123.16}$。另外，当$n' = 32$时，$\{x(i)\}_{i=0}^{MN/8-1}$的循环周期对于大多数明文图象就已经足够大了†，因此由已知的掩模图象f_m得到较大的f'_m会变得困难得多。但是，该措施不能增加由f_m得到K的复杂度，因为该复杂度仅由M和N确定。

另外一种措施是在混沌系统中增加控制参数作为密钥的一部分。该措施可以增强抵抗唯密文攻击的强度，因为不同的控制参数会使得拟混沌轨道(即便初始条件相同)完全不同。但是它不能增强抵抗已知/选择明文攻击的强度。显然，f_m还是可以在不知道控制参数的情况下得到，然后控制参数和初始条件被同时从f_m导出。

*该准则也可以改为其他形式，比如$\sum_{i=0}^{7}(a_i \oplus d_i) \in [n_1, n_2] \subseteq [1, n-1]$。这样看起来简单的改变可能会使抗唯密文攻击的复杂度上升几个比特。

†甚至一个巨大的图象(4096×4096)，MN也只有$2^{24} \ll 2^{32}$。

最后，让我们讨论一下使用其他的混沌伪随机序列会有什么效果。显然，这会使得从f_m导出K变得更为困难。但是，f_m仍然可以用来解密尺寸不大于已知/选择明文图象尺寸的密文图象，唯密文攻击的复杂度也不会受任何影响。为了避免由已知的f_m得到尺寸较大的f'_m，我们建议使用较大的n'或者浮点算法生成$\{x(i)\}_{i=0}^{MN/8-1}$。在图7.11中我们给出了在浮点算法下Lenna.bmp的密文图象和掩模图象。与图7.1b和图7.2a相比，可以看到掩模图象和密文图象变得更乱，而且没有明显的重复模式出现了。不过，复杂的混沌伪随机序列算法和浮点算法需要更高的运算复杂度，因而会使得CKBA的运行速度变慢。



a) 使用浮点算法加密的Lenna.bmp　　b) 浮点算法下的掩模图象

图 7.11: 在CKBA中使用浮点算法

总结一下，增强CKBA对唯密文攻击的复杂度很容易，但是增强抵抗已知/选择明文攻击的复杂度则非常难。事实上，不能抵抗已知/选择明文攻击的本质原因是CKBA的加密过程本身(参看方程(7.1))。如果我们通过改变加密流程来增强安全性，CKBA就不再是CKBA而变成了完全不同的一种加密系统。

§7.6.2 改进BRIE

为了增强BRIE对穷举攻击的安全性以及由Q得到密钥的复杂度，一些简单的修改即可收到不错的效果，如增加$x(0)$的实现精度，增加混沌系统的控制参数作为密钥的一部分，等等。但是这些措施一般都不能增强使用Q作为密码分析攻击的安全性。

为了避免Q带来的已知/选择明文攻击的危险，可以采用一些复杂的修改，比如级联一个后继密码扰动BRIE加密后的密文图象[143]，或者使用由密文象素和附加的密钥伪随机生成的α和β[22, 151]。这样的话改进BRIE的安全性强主要由新引入的部分保证，而不是BRIE本身。

§7.7 本章小结

在本章中，我们指出在文献[132, 134]中提出的两类Yen-Guo混沌图象加密算法CKBA和BRIE是不安全的。使用一对明文/密文图象，已知/选择明文攻击可以破解这两种加密方法。BRIE中存在的更多安全问题也被发现并详细讨论。

从概念上讲，本章给出的密码分析方法也可以推广用来攻击其他的Yen-Guo(混沌)图象加密算法。我们的密码分析给出的教训说明在信号/图象处理和密码学之间缺少互动，它们之间的联系需要更多的相关研究来推动。

第三部分

设计数字化混沌密码的新思路

第八章 基于CCS-PRBG(双混沌系统伪随机比特发生器)的混沌流式密码

基于前面给出的研究综述和一些最近提出的数字化混沌密码的分析工作，本章和下面一章将介绍一些设计数字化混沌密码的新思路。这两章的内容基于我们从不安全的数字化混沌密码那里吸取来的教训，以及从那些现在还保持安全性的数字化混沌密码中得到的启示。本章将介绍一种新的混沌伪随机比特发生器(PRBG)并讨论该混沌PRBG在流密码术中的应用。下一章将介绍一种快速混沌加密系统，它是一种包含一个混沌流密码部分和一个混沌分组密码部分的混合密码系统。在两章中都使用了多混沌系统以强化设计的混沌密码的安全性(回顾我们在§2.6.1中的讨论)。

§8.1 引言

正如我们在§2.2.1中介绍的，很多基于混沌伪随机数发生器(PRNG)的流密码已经被提出。由于混沌流密码中使用的大部分混沌PRNG都只采用了单个混沌系统，可能存在一些潜在的动力学攻击方法从拟混沌轨道中提取有用的信息，比如那些在基于混沌同步的保密通信系统领域中广为使用的一些信息分析方法[25–29, 32, 36, 39–41]。另外，一些基于混沌PRNG的流密码[55, 57, 64, 82]被成功分析的事实也暗示了这种危险。我们在§2.6.1中建议使用多个混沌系统，这是一个增强数字化混沌密码抵抗动力学分析安全性的通用办法。事实上，已有几种数字化混沌流密码采用了多混沌系统[22, 42, 112, 119, 124]，但是这些密码的部分设计者并没有意识到使用多混沌系统的全部优点。

在本章中，我们研究仅使用两个(“多”混沌系统的最少数目)混沌系统实现对潜在攻击的较高安全性以及更好的整体性能(将加密速度和系统实现也考虑在内)的可能性。提出了一种基于一对混沌系统的新型伪随机比特发生器(PRBG)，缩写为CCS-PRBG。初步的理论分析和试验结果表明该PRBG具有良好的密码学特性，并可以用来构造高安全性的流密码。随意一点说，我们可以将CCS-PRBG看作是一个“优秀”的非线性PRBG。当设计一个新的流密码时，我们可以象在传统流密码学中使用LFSR和NLFSR[143, 144]那样使用该CCS-PRBG。当然，CCS-PRBG比LFSR具有更高的安全性显然是正确的，它看起来至少具有和NLFSR一样的安全性。作为CCS-PRBG在流密码学中的应用，我们介绍了几种典型的基于CCS-PRBG的混沌流密码方案，它们可以实现一个安全性和实用性之间的较好折中(较高的加密速度，较低的系统实现成本)。

本章的组织如下所述。在§8.2中，介绍了CCS-PRBG及其在有限精度下的数字化实现。关于CCS-PRBG密码学特性的分析，包括部分试验结果，在§8.3中给出。在§8.4中，给出了一些基于CCS-PRBG的流密码例子及它们的安全性分析。最后一节给出本章小结和一些未来研究的开放话题。

§8.2 基于双混沌系统的PRBG(CCS-PRBG)

在本论文前面的内容中，我们已经提到：由于生成的伪随机序列可能泄漏一些关于混沌系统的信息，基于单个混沌系统混沌的PRNG是潜在地不安全的。在本节中，我们提出一种基于一对混沌系统的新型伪随机比特发生器(PRBG)，由于**两个**混沌系统被用来生成混合的伪随机比特，它可以提供较其他混沌PRBG较高的安全性。在本章中我们称之为CCS-PRBG，这是“Couple Chaotic Systems Based PRBG”一词的缩写。CCS-PRBG使用的基本思路是通过比较两个不同的、渐近独立的拟混沌轨道来生成伪随机比特，看起来它在密码学意义上足够强，可以避免由伪随机比特获取有关混沌系统信息的可能性。象在流密码学中使用其他PRBG一样，一些基于CCS-PRBG的混沌流密码被提出，关于这些密码的讨论将在§8.4中给出。

§8.2.1 定义

假设有两个不同的一维混沌映射$F_1(x_1, p_1)$和$F_2(x_2, p_2)$：$x_1(i+1) = F_1(x_1(i), p_1)$，$x_2(i+1) = F_2(x_2(i), p_2)$，其中$p_1, p_2$是控制参数，$x_1(0), x_2(0)$是初始条件，$\{x_1(i)\}$和$\{x_2(i)\}$表示两条拟混沌轨道。

定义一个伪随机比特序列如下：

$$k(i) = g(x_1(i), x_2(i)) = \begin{cases} 1, & x_1(i) > x_2(i) \\ \text{不输出}, & x_1(i) = x_2(i) \\ 0, & x_1(i) < x_2(i) \end{cases} 。 \tag{8.1}$$

当满足一些条件时，则该混沌PRBG将具有优良的密码学特性，我们称之为“基于双混沌系统的伪随机比特发生器(**C**ouple **C**haotic **S**ystems based **P**seudo-**R**andom **B**it **G**enerator)”，简写为CCS-PRBG。这些条件是：

- *R1)* – $F_1(x_1, p_1)$和$F_2(x_2, p_2)$是定义在同一个区间$I = [a, b]$上的满混沌映射；
- *R2)* – $F_1(x_1, p_1)$和$F_2(x_2, p_2)$在I上遍历，具有唯一的不变分布函数$f_1(x)$和$f_2(x)$；
- *R3)* – 满足下列两个条件之一：$f_1(x) = f_2(x) = f(x)$，或者$f_1(x), f_2(x)$都相对$x = (a+b)/2$偶对称；
- *R4)* – 当$i \to \infty$时，$\{x_1(i)\}, \{x_2(i)\}$渐近独立。

如果一个混沌映射被常数$c \in I$替代，则$k(i)$将简化为文献[58]中提出的伪随机序列和文献[151]中提出的混沌阈值序列。从这样一种角度看，CCS-PRBG可以被看作是上面的混沌伪随机序列的具有“伪随机的时变阈值参数”的推广版本：一个拟混沌轨道被另外一个轨道二值化，第二个拟混沌轨道的作用就像文献[58, 151]中的阈值常数。另外，既然$\{x_2(i)\}$可以看作是$\{x_1(i)\}$的二值化序列，反之亦然，因此我们也可以将CCS-PRBG看作是两个互控的混沌PRBG。

§8.2.2 基于扰动的数字化实现

当CCS-PRBG在数字系统中实现时，我们建议使用文献[80]中的扰动策略改善CCS-PRBG中使用的混沌系统的动力学特性退化。该策略描述如下：

使用两个简单的PRNG产生两个伪随机信号*，这两个信号用于扰动$\{x_1(i)\},\{x_2(i)\}$的最低n_l个比特，扰动间隔为Δ_1,Δ_2。在硬件实现和软件实现中，最大长度线性反馈移位寄存器(m-LFSR)和编程语言中的标准内嵌函数`rand()`分别是最好的选择。与文献[80]不同，这里我们建议如下规则确定n_l：$n_l \geq \lceil \lambda \cdot \log_2 e \rceil = \lceil 1.44\lambda \rceil$，其中$\lambda$是被扰动混沌映射的Lyapunov指数。上述规则的原因是：当有限精度为n-比特时，平均而言，两个输入信号之间的最小差异(等于2^{-n})经过一次混沌迭代以后会变为$e^{\lambda} \cdot 2^{-n}$(在定点算法下)。为了保持混沌系统的动力学特性，还要求满足$n_l \ll n$。尽管扰动信号比混沌信号小得多，由于混沌系统的初值敏感性，它仍然可以将$\{x_1(i)\},\{x_2(i)\}$扰动成为相当复杂的轨道。数字化混沌和扰动PRNG的伪随机性组合使得基于混沌理论的攻击方法和传统密码分析方法都变得更为困难。

一个存在于CCS-PRBG中的小问题是：当$x_1 = x_2$时，$g(x_1,x_2)$不输出任何伪随机比特，这在需要固定传输速率的保密通信中会带来不便，因为偶尔的空输出会使得CCS-PRBG暂时停止。在这样的时刻，一个额外的简单PRNG-3可以被引入确定输出$k(i)$。带有扰动的数字化CCS-PRBG实现如图8.1所示。可以看到该结构的硬件和软件实现都比较简单。

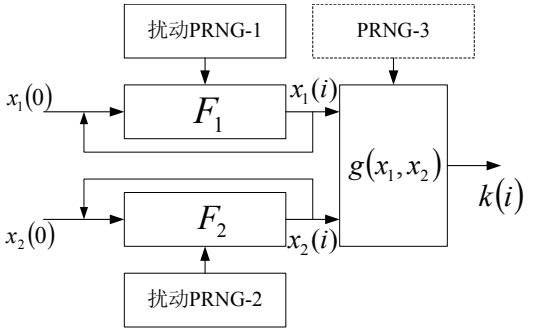


图 8.1: 基于扰动的CCS-PRBG数字化实现

§8.3 数字化CCS-PRBG的密码学特性

数字化CCS-PRBG产生的$\{k(i)\}$满足下述密码学特性：1) $\{0,1\}$上的平衡性；2) 长循环周期；3) 高线性复杂度，接近循环周期的一半；4) 类似$\delta(\cdot)$的自

*关于如何生成扰动信号的更多细节，请参看文献[80]。当然我们可以使用不同于文献[80]中的方法实现这个目的，唯一的要求是产生的信号需要在被扰动的混沌系统的定义区间上近似均匀分布。

相关函数；5) 接近0的互相关函数；6) 混沌系统的自由选择性(chaotic-system-free)*。详细的讨论和试验结果在下面给出。

§8.3.1 平衡性

定理 8.1: *如果两个混沌映射满足前面提到的条件R1–R4，我们可以得到$P\{k(i)=0\}=P\{k(i)=1\}$，即$k(i)$在$\{0,1\}$上是平衡的。*

证明: 由于$F_1(x_1,p_1)$和$F_2(x_2,p_2)$在$I=[a,b]$上是遍历的(条件R2)，对于几乎所有的初始条件，生成的混沌轨道都将得到相同的分布函数$f_1(x),f_2(x)$[23]。由条件R4，混沌轨道$\{x_1(i)\},\{x_2(i)\}$是渐近独立的，因此随着$i\to\infty$，$x_1>x_2$和$x_1<x_2$的概率将为：

$$P\{x_1>x_2\} = \int_a^b\int_a^x f_1(x)f_2(y)\,\mathrm{d}y\,\mathrm{d}x \tag{8.2}$$

$$P\{x_1<x_2\} = \int_a^b\int_a^x f_2(x)f_1(y)\,\mathrm{d}y\,\mathrm{d}x \tag{8.3}$$

当条件R3成立时，我们可以证明$P\{x_1>x_2\}=P\{x_1<x_2\}$：

R3–1) $f_1(x)=f_2(x)=f(x)$：

$$P\{x_1>x_2\}=P\{x_1<x_2\}=\int_a^b\int_a^b f(x)f(y)\,\mathrm{d}y\,\mathrm{d}x。 \tag{8.4}$$

R3–2) $f_1(x),f_2(x)$都关于$x=(a+b)/2$偶对称：

定义x_1,x_2的镜像轨道为$x_1'=b-x_1,x_2'=b-x_2$。由$f_1(x),f_2(x)$的对称性，x_1',x_2'将具有相同的分布$f_1(x),f_2(x)$，然后可得：

$$P\{x_1>x_2\}=P\{x_1'<x_2'\}=\int_a^b\int_a^{x'} f_2(x')f_1(y')\,\mathrm{d}y\,\mathrm{d}x=P\{x_1<x_2\}。 \tag{8.5}$$

考虑到$x_1>x_2\to k(i)=1$还有$x_1<x_2\to k(i)=0$，我们有$P\{x_1>x_2\}=P\{x_1<x_2\}\Rightarrow P\{k(i)=0\}=P\{k(i)=1\}$。得证。 ■

显然，上述推导过程还是基于连续混沌系统的。当混沌系统以扰动策略数字化实现时，每条拟混沌轨道将不时地被小扰动信号扰动到一个相邻拟轨道上去。这样的结果就是，几乎所有的轨道都趋向于$f_1(x),f_2(x)$的离散版本(带有一点平滑效果)。对于$f_1(x),f_2(x)$的离散版本，将上述推导中的$\int$替换为$\sum$，结论仍然近似成立：方程(8.2)和(8.3)被替换为

$$P\{x_1>x_2\}=\sum_{x=a}^{b}\sum_{y=a}^{x}P_1\{x_1=x\}\cdot P_2\{x_2=y\} \tag{8.6}$$

*这个概念我们在§2.6.1中提到过，并称之为“万用性”，这里的“混沌系统的自由选择性”是指狭义的“万用性”，即一大类混沌系统都可以自由选用，并且给出了选用的原则和条件。

和

$$P\{x_2 > x_1\} = \sum_{x=a}^{b} \sum_{y=a}^{x} P_2\{x_1 = x\} \cdot P_1\{x_2 = y\}。 \tag{8.7}$$

当数字化CCS-PRBG以扰动策略实现时，x_1, x_2相对$x = 1/2$近似对称，我们可以得到下述结论$P\{x_1 > x_2\} \approx P\{x_1 < x_2\}$。因此，对于带有扰动的数字化CCS-PRBG，平衡性仍然近似保持。

§8.3.2 伪随机比特序列的长周期循环

不失一般性，假设两个m-LFSR用作扰动PRNG，它们的阶数分别为L_1, L_2，扰动间隔分别为Δ_1, Δ_2。则$\{x_1(i)\}, \{x_2(i)\}$的循环周期分别为$\sigma_1\Delta_1(2^{L_1} - 1), \sigma_2\Delta_2(2^{L_2} - 1)$，这里$\sigma_1, \sigma_2$是两个正整数[80]。因而，比特序列$\{k(i)\}$的循环周期将为：

$$\mathrm{lcm}(\sigma_1\Delta_1(2^{L_1} - 1), \sigma_2\Delta_2(2^{L_2} - 1))。 \tag{8.8}$$

当Δ_1, Δ_2和L_1, L_2满足条件$\gcd(\Delta_1, \Delta_2) = 1$和$\gcd(2^{L_1} - 1, 2^{L_2} - 1) = 1$时，$\{k(i)\}$的循环周期为：

$$\mathrm{lcm}(\sigma_1, \sigma_2) \cdot \Delta_1\Delta_2(2^{L_1} - 1)(2^{L_2} - 1) \approx \mathrm{lcm}(\sigma_1, \sigma_2) \cdot \Delta_1\Delta_2 2^{L_1+L_2}。 \tag{8.9}$$

这样的一个循环周期对于大多数应用来说足够长了。此外，还有一些方法可以用来进一步延长该循环周期，比如文献[81]中的方法。

§8.3.3 高线性复杂度和理想的相关特性

实际上，条件*R4*和$\{k(i)\}$的平衡性暗示：随着$i \to \infty$，$\{k(i)\}$趋向于是一个i.i.d.(独立同分布)的比特序列。因此，该序列应该具有类似$\delta(\cdot)$的自相关和接近0的互相关。另外，已经知道(参看[227])i.i.d.二进制序列的线性复杂度大约为其长度的一半，因此$\{k(i)\}_{i=1}^{n}$的线性复杂度将为$n/2$*。

现在让我们讨论一下在什么情况下条件*R4*才会成立。对于任何混沌映射，即便初始条件或者控制参数只有一点很小的差异，混沌轨道在经过有限次迭代之后都会变得完全不同。如果有一些和混沌轨道相关的信息，这种信息会随着$i \to \infty$而趋向于0。两个混沌轨道之间的相关性可以看作是这样的信息。在混沌理论中，Kolmogorov熵被定义用来衡量这种信息消失的速度。对于一维混沌映射，Kolmogorov熵等于Lyapunov指数[208, 210]。如果初始信息为H，经过$\eta \approx H/\lambda$次迭代以后该信息就可以认为已经消失[58]，这里λ是Lyapunov指数。当混沌系统在有限精度下实现时，由于量化误差和小的扰动信号的影响该信息甚至会衰减地更快。因此我们可以知道，如果在两个混沌轨道之间存在初

*$\{k(i)\}$的长度为$L = \mathrm{lcm}(\sigma_1\Delta_1(2^{L_1} - 1), \sigma_2\Delta_2(2^{L_2} - 1))$，而不是无穷。因此，$\{k(i)\}_{i=1}^{\infty}$的线性复杂度应该为$L/2$，也不是无穷。

始差异的话，这种差异会随着$i \to \infty$而变得渐近无关。可见，*R4*的一个等效条件$\{x_1(i)\} \neq \{x_2(i)\}$，也就是说，$F_1 \neq F_2$，或者$x_1(0) \neq x_2(0)$，或者$p_1 \neq p_2$。

由于在η次迭代之后$\{x_1(i)\}, \{x_2(i)\}$才是独立的，我们建议丢弃$\{k(i)\}$的头m个比特，这里$m > \eta$。这意味着在$\{k(i)\}$输出之前需要先进行m次两个混沌映射的预迭代。由于m并不太大，这样的预迭代只需要一点多余的计算负担。

尽管本小节给出的讨论完全是理论化和定性的，试验数据强烈支持我们的理论结果(更多细节参看图8.2和§8.3.5)。在以后的研究中，我们将试图找到CCS-PRBG生成的$\{k(i)\}$是i.i.d.二进制序列*的严格证明。

§8.3.4 混沌系统的自由选择性(Chaotic-System-Free)

考虑存在很多不同的混沌映射满足条件*R1*和*R2*，而条件*R3*和*R4*只是限制了两个混沌系统之间的关系，我们称CCS-PRBG具有“混沌系统的自由选择性”(*chaotic-system-free*，或者狭义的“万用性”)，这个称呼用来强调CCS-PRBG可以在很多混沌系统上使用这个事实。回顾我们在§2.6.1中的讨论，这样一种特性对于数字化混沌密码是相当理想的。由于PWLCM满足上述的条件*R1*–*R4*，我们还是继续推荐它们在CCS-PRBG中的使用。

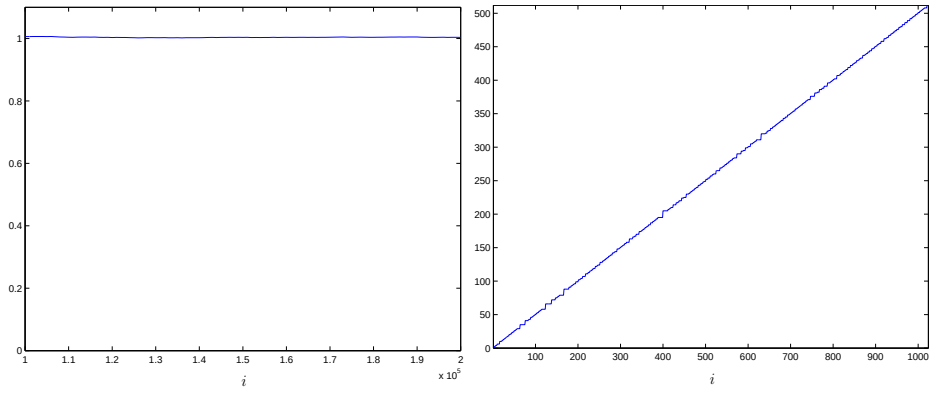
§8.3.5 试验结果

一些试验验证了带有扰动的数字化CCS-PRBG的密码学特性的理论分析。两个混沌映射都被选择为PWLCM(2.1)。有限计算精度为$n = 32$比特。扰动PRNG选为两个m-LFSR，它们的阶数分别为$L_1 = 16$、$L_2 = 17$，扰动间隔分别为$\Delta_1 = 99$、$\Delta_2 = 101$。预迭代的次数$m = 16$。初始条件和控制参数都是随机生成的，$k(i)$的大量的子序列随机地从不同位置选取出来以测试CCS-PRBG的密码学特性。0:1比、线性复杂度和一个子序列的自相关函数分别在图8.2a–c中给出。在图8.2d中给出了两个初始条件相同但是具有最小差异2^{-n}的控制参数的比特序列的子序列的互相关。可以看到试验结果和理论分析完全相符。

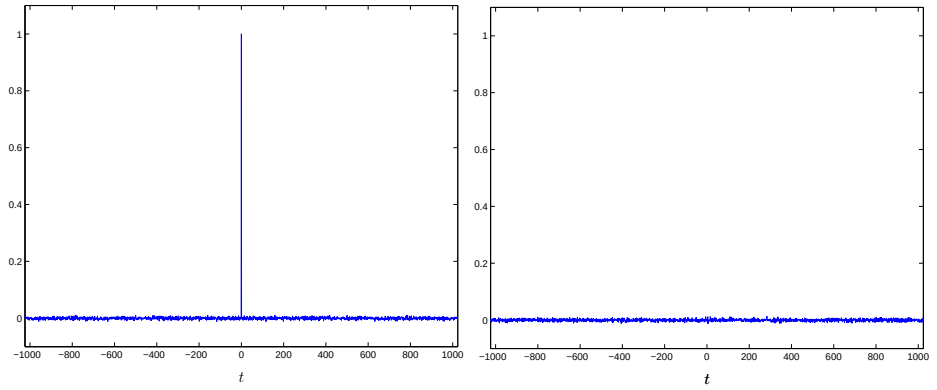
§8.4 使用数字化CCS-PRBG构造流密码

基于数字化CCS-PRBG，很多不同的实际流密码系统可以被构造出来。我们将看到这些流密码可能对其他数字化混沌密码中存在的问题提供一个较好的解决。使用CCS-PRBG的不同配置，很多流密码可以在不损失安全性的前提下，很方便地得到较低的成本和简单的系统实现。这里，数字化CCS-PRBG替代了LFSR在传统流密码学中的角色。

*当然，由于两个涉及的拟混沌轨道实际上都是确定性的，这里的i.i.d特性只在近似意义上成立。



a) 0:1比　　b) 线性复杂度



c) 自相关　　d) 互相关

图 8.2: 数字化CCS-PRBG的密码学特性

§8.4.1 一些流密码的例子

• 密码一

给定一个带扰动的数字化CCS-PRBG，初始条件$x_1(0), x_2(0)$和控制参数选作密钥。$\{k(i)\}$直接用来加密(一般采用异或操作)明文和解密密文。

显然，该密码是基于数字化CCS-PRBG的密码中最简单的一种类型。如果系统实现精度为n比特，密钥熵则为$4n$。该密码通过硬件和软件都可以很容易地以较低成本实现。在一个800MHz的奔腾(Pentium)IIIPC上，一个基于PWLCM (2.1)的软件实现版本使用Turbo C 2.0开发以测试其速度。实际的加密速度在定点算法下达到了9 Mbps。这样一个速度比很多其他的数字化混沌密码要快得多，在很多安全应用中都是可以接受的。在硬件实现下，加密速度可以提高得很多，可以大致估算如下：假设时钟主频为s MHz，有限精度为n-比特，加密速度的估计值大约为$\frac{s}{n}$ Mbps(每个n-比特数字除法消耗大约n个时钟)。

将一些简单的修改作用于密码一，更高的密钥熵(更高的安全性？)和更高的

加密速度可以在仅增加不大的运算负担和实现成本的情况下得到。两个这样的例子在下面给出。

• 密码二

给定四个一维混沌系统$CS_0 \sim CS_3$，以及五个m-LFSR：$m\text{-}LFSR_0 \sim m\text{-}LFSR_4$，其中$m\text{-}LFSR_0 \sim m\text{-}LFSR_3$用来扰动$CS_0 \sim CS_3$。在$CS_0 \sim CS_3$的每次迭代之前，首先使用$m\text{-}LFSR_4$生成两个2-比特伪随机数$pn1(i)$和$pn2(i)$。如果$pn2(i) = pn1(i)$，执行$pn2(i) = pn1(i) \oplus 1$；否则不作任何事情。然后选择$CS_{pn1(i)}$和$CS_{pn2(i)}$构成数字化CCS-PRBG生成$k(i)$。密钥是所有混沌系统的初始条件和控制参数。

在n比特运算精度下密钥熵为$8n$。$m\text{-}LFSR_4$使得密码分析更为复杂和困难，从而使得密码二较密码一更为安全，速度和密码一基本相当，而代价仅仅是一倍左右的实现复杂度。

• 密码三

对于一些定义在$I = [0,1]$上的混沌映射，比如PWLCM(2.1)，不变分布为$f(x) = 1$。当它们在数字计算机上实现时，拟混沌轨道的每个比特在$\{0,1\}$上都是平衡的。基于这样一个事实，我们可以定义一种CCS-PRBG的推广版本。这里我们假设有限精度为n比特。对于$F_1(x_1, p_1)$和$F_2(x_2, p_2)$的一次迭代而言，按照如下规则生成n个比特$K(i) = k_0(i) \ldots k_{n-1}(i)$：

for $j = 0$ to $n-1$ do
$x_1(i,j) = x_1(i) \gg j$
$x_2(i,j) = x_2(i) \ll j$
$k_j(i) = g(x_1(i,j), x_2(i,j))$
end

这里»和«分别表示循环右移和循环左移操作。显然，这样一个基于推广CCS-PRBG的流密码的加密速度比密码一和密码二要快大约n倍，但是并没有损失安全性。当密码三在支持并行运算的硬件中实现时，当时钟主频为s MHz，其加密速度可以接近s Mbps*。这样一个速度接近很多基于LFSR的传统流密码，比如Geffe发生器和钟控发生器，而比其他复杂的流密码要快很多[143, 144]。如果我们将密码二和密码三组合起来，安全性和密码速度可以同时得到较大提高。事实上，为了进一步增强密码三的安全性，我们可以引入另外一个$m\text{-}LFSR_5$伪随机地控制x_1和x_2的移位方向。

在表8.1中，我们给出了上述三种密码以及密码二和密码三的组合密码的性能比较。基于LFSR的密码也列在该表中作为参照。在该表中n是有限精度，a表示密码一的实现成本。注意基于LFSR的流密码大都不够安全，尽管它们的实现成本更

*显然，其速度主要由混沌迭代的定点除法决定。由于一次n-比特的数字化除法消耗大约n个时钟周期，密码三的加密速度将接近$\frac{s}{n} \cdot n = s$ Mbps。

低。和其他数字化混沌流密码比较起来，密码三可能是一个很有希望的流密码基本组件，可以用来构造具有理想的整体性能的混沌流密码。CCS-PRBG的另外一个可能用途是与其他密码技术一起构造乘积密码系统。如，CCS-PRBG可以用在我们下一章将要介绍的CVES中进一步增强其安全性。

表 8.1: 基于CCS-PRBG的流密码的比较

	密钥熵	加密速度(硬件实现)	实现成本
密码一	$4n$	$\frac{s}{n}$ Mbps	a
密码二	$8n$	$\frac{s}{n}$ Mbps	$2a$
密码三	$4n$	s Mbps	a
密码二＋密码三	$8n$	s Mbps	$2a$
基于LFSR的密码	/	s Mbps	$< a$

§8.4.2 安全性

一般来说，上述密码的安全性可以通过我们在§8.3中讨论的数字化CCS-PRBG的密码学特性来保证。但是我们知道很多密码被证实是不安全的，尽管它们看起来都有着“很好”的密码学特性。因此我们还是需要研究一下基于数字化CCS-PRBG的密码对于已知的攻击是否是安全的。

首先，让我们考虑那些在基于混沌同步的保密通信系统中发展起来的密码分析方法[25–29, 32, 36, 39–41]。它们可以成功攻击相关系统的原因主要是：混沌同步技术本身使得从密文中抽取混沌系统的有关信息成为可能。由于传送的信号必须保证发送端和接收端的同步，抽取出来的信息可能可以用来恢复混沌轨道并提取掩盖的明文信息。对于数字化CCS-PRBG，由于没有使用混沌同步技术，而且两个不同的混沌轨道用来生成伪随机密钥流$k(i)$，从密文提取这两个混沌系统的动力学信息变得异常困难。另外，伪随机的扰动也进一步增强了抵抗分析的能力。即使在明文已知的情况下，仅从$k(i)$提取两个混沌轨道几乎不可能。因此，那些用于攻击基于混沌同步的保密通信系统的动力学方法，一般不能用来攻击带扰动的数字化CCS-PRBG。

其他的已知密码分析方法基本上都是针对特定混沌密码的特殊特点而生效的。文献[56, 61]中的密码分析方法是由于数字化混沌系统的动力学特性退化，这在数字化CCS-PRBG的实现中已经通过扰动加以解决。文献[67]中提出的分析方法是基于两维Hénon映射的一个特殊弱点，不能推广到其他混沌系统。文献[63, 88, 97]中的分析方法则与相关密码的特殊弱点有关，不能用来攻击结构完全不同的基于CCS-PRBG的密码。

可以看出基于数字化CCS-PRBG的密码对于所有已知的密码分析都是安全的。当然，在我们可以说“基于数字化CCS-PRBG的密码是足够安全的”之前，还需要做更多关于数字化CCS-PRBG的更多密码分析工作。但是以上的讨论暗示数字化CCS-PRBG可能是构造高安全性低成本流密码的一个有希望的新想法。

在数字化CCS-PRBG中有一个值得注意的问题。假设$x_1(0) = x_2(0)$，当控制参数为p_1, p_2时，产生的伪随机序列为$k(i)$；交换两个混沌系统的控制参数，产生的序列为$k'(i)$。如果这两个混沌映射的系统方程相同，又使用相同的扰动PRNG以及相同的扰动参数($\Delta_1 = \Delta_2$)，则显然有$k'(i) = \overline{k(i)}$，这是$g(x_2, x_1) = \overline{g(x_1, x_2)}$的自然结果。这样一个缺陷会使密钥空间减少为原来的1/2。为了避免这个缺陷，需要使用不同的扰动PRNG或者扰动间隔，并且$m > \max(\Delta_1, \Delta_2)$；使用方程不同的两个混沌映射也可以解决这个问题，如采用PWLCM(2.1)和斜tent映射(2.3)。

§8.5 本章小结

在本章中一种新型的基于双混沌系统的混沌PRBG(称为CCS-PRBG)被提出，并用来构造新的数字化混沌流密码。理论分析和试验都显示数字化CCS-PRBG具有理想的密码学特性。类似LFSR在传统流密码学中的角色，数字化CCS-PRBG可以作为设计新的流密码的一个核心组件。

对于CCS-PRBG而言，有如下几个开放的研究话题：

- 如我们在§8.3.3中提到的，$\{k(i)\}$是i.i.d.序列的严格证明仍然是一个未解决的问题。
- 一些基于CCS-PRBG的流密码的实现细节(硬件和软件)尚待继续研究。
- 针对数字化CCS-PRBG的可能的密码分析方法还需要更多的研究工作。

第九章 一种加密速度甚快的混沌加密新方法

§9.1 引言

在今日的数字化世界中，由于数字产品在网络上的通信越来越频繁，数字化图象/视频的安全性正日益变得重要。另外，在一些特殊的数字应用中，数字图象/视频的高可靠安全需求是很重要的，如付费电视，保密视频会议以及医学成像系统，等等*。一般来说，高度发达的现代密码学可以为这种需求提供完美的解决方案。我们知道，自从二十世纪70年代以来，很多相当优秀的密码系统被提出并得到广泛应用，如DES，IDEA和RSA[143, 144]。但是很多传统密码不能直接用来在实时应用中加密数字视频，因为其加密速度不够快，尤其当它们使用软件实现时。另外，数字视频中不同的压缩算法的存在也使得将加密模块集成到整个系统中变得更为复杂。因而，需要一些专门设计的加密方法提供对实时视频的保护。

近年来，已有不少专门的视频加密方案被提出[221, 228–237]，其中的大多数都属于联合压缩-加密方法，用来为MPEG视频流提供可靠的安全性[229, 230, 232–237]。由文献[238–240]中的工作可知，一些视频加密方案从严格的密码学角度看是不够安全的。事实上，在很多视频加密系统中，安全性和加密速度之间存在一定的矛盾[238]。

本章考虑如下问题：是否可能使用数字化混沌设计快速加密系统以解决目前实时视频加密中的问题？由我们在第2章中对数字化混沌密码的综述可知，大多数混沌密码以相当慢的速度运行，这使得很难劝说最终用户接受混沌密码作为实际应用的解决方案。我们已经在上一章引入了基于CCS-PRBG的流密码放松这个问题对实际应用的限制(密码三在硬件实现情况下可以相当高的速度运行)。但是流密码有着它的本质缺陷：为了避免已知/选择明文攻击，密钥不能重用。在本章中，我们将研究一种设计混沌密码的新思路，该思路支持密钥的重用，并可以使得混沌密码的加密速度变得相当快。

基于这样一种新的思路(在下一节介绍)，一种混沌视频加密系统(简写为CVES)被仔细地设计以满足实时视频加密的需求。初步分析表明该系统是安全的，并能够以非常快的速度运行，并且其硬件和软件实现都比较简单。CVES独立于任何视频压缩算法，因而不会被明文视频的格式所限制，这是CVES相对其他视频加密方法的一个重要优点。而且，一种扩展的CVES版本可以支持加密视频的随机检索(在可接受的最大延时下)。

作为本文的主要内容的最后一章，本章不应看作是对数字化混沌密码设计难题的真正解决，而只是一种试图发现一般设计结构和设计原则的积极尝试。或许我们提出的加密算法很快可以被发现是不安全的，但是我们相信这样一种尝试有助于发现有关“我们能做什么”和“我们不能做什么”的更多信息。我们的密码分析经验暗示设计一个真正安全的数字化混沌密码比攻击它更困难。事实上，我

*第7章提到了数字图象安全的重要性，加上数字视频的安全性，可以把本章的内容看成是数字多媒体的安全性需求。

们在文献[112]中提出的原始的CVES方案就是不够安全的。尽管CVES的安全性将在本章中得到增强，现在说该增强版本就是安全的还太早。

本章的组织如下。CVES使用的新的混沌密码设计思路在§9.2中给出。CVES及其扩充版本RRS-CVES(支持随机检索的CVES)在§9.3中进行详细的描述。CVES/RRS-CVES的性能分析在§9.4中给出，从加密速度，安全性，系统实现以及试验仿真四个方面进行讨论。最后一节给出本章小结。

§9.2 设计思路的概念化描述

使用混沌实现快速加密思路的核心是组合一个简单的混沌流密码和一个简单的混沌分组密码(具有时变的S盒)构成一个更为复杂的乘积密码系统。正如我们在第2章中讨论的，多混沌迭代的使用是导致混沌密码运行速度慢的首要原因，但是过少的迭代可能会带来安全隐患。因而，我们试图通过组合一个混沌流密码和一个混沌分组密码来使得单次混沌迭代成为可能(在不损失安全性的前提下)。CVES的设计实践表明这样一种想法确实是可行的。

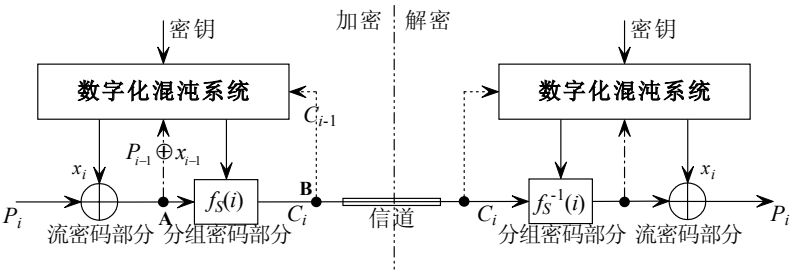


图 9.1: 一种使用混沌设计密码的新思路

该想法可以描述如下：假设P_i, C_i分别表示第i个明文和第i个密文(都是n-比特的数据)，加密过程定义如下：

$$C_i = f_S\left(P_i \oplus x_i, i\right), \tag{9.1}$$

这里$f_S(\cdot, i)$是一个时变的$n \times n$的S盒(一个定义在$\{0, 1, \cdots, 2^n - 1\}$上的一一单射)，$x_i$是由一个(或多个)混沌系统的拟混沌轨道得到。这里，f_S也可以被混沌映射伪随机地控制。密钥选作混沌系统的初始条件和控制参数。关于该想法的加密解密过程，参看图9.1。为了增加得到的密码抵抗攻击的复杂度，内部反馈(发生在点**A**的$P_{i-1} \oplus x_{i-1}$)和密文反馈(发生在点**B**的C_{i-1})是有用的。这样一种密码可以看作是一个简单流密码和一个简单分组密码的组合。

这里，让我们看看为什么内部反馈和/或密文反馈是必要的。如果没有任何反馈的话，上述密码将变成下述弱化版本：

$$C_i = f'_S\left(P_i, i\right), \tag{9.2}$$

这里f'_S对于每个位置i而言是固定不变的。这样一种密码实际上是一种流密码，采用了时变的函数$f'_S(i)$代替普通流密码中的异或操作(参看图9.2)。尽管它比一般的采用异或操作的流密码具有更好的安全性，选择明文攻击还是可以破解它，并在仅选择2^n个明文的情况下得到所有的$f'_S(\cdot,i)$：$0\cdots0\cdots$，$1\cdots1\cdots$，$\cdots$，$(2^n-1)\cdots(2^n-1)\cdots$。当$2^n$不够大的时候，选择明文攻击非常奏效。然而，如果$2^n$太大，可能会使得生成时变的$f_S$并保持高的加密速度变得困难(甚至实际不可行)。实际上，在CVES中$n=8$，这对于抵抗上述选择明文攻击而言实在是太小了。

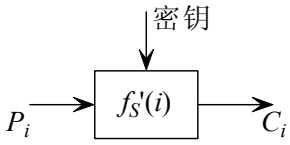
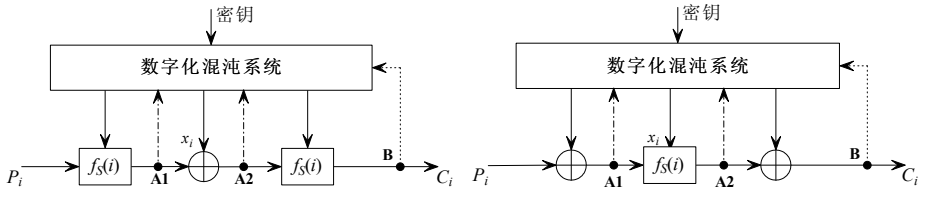


图 9.2: 图9.1中密码的无反馈弱化版本

作为一个该矛盾的解决方案，引入反馈以使得f'_S也依赖于前面N_p个明文，从而可能使得上述选择明文攻击变得实际不可行。这时抵抗上述选择明文/密文攻击的强度会增加到$2^{n\cdot N_p}$。当然，就像在分组密码的CBC模式一样，这里必然存在差错传播问题，传播长度为$N_p\cdot n$个比特。对于视频应用而言，N_p可以相对大一些。

关于反馈有一个并非琐碎的问题：对于第一个明文，由于没有以前的明文可用，f'_S还是固定的。需要引入一个初始向量(IV，initial vector)解决这个问题：对于每个明文消息，开始的$N_p\cdot n$个比特被随机产生并作为IV加密/解密第一个有意义的明文。只要$2^{n\cdot N_p}$足够大，则对于攻击者而言实施攻击就变得概率上不可行了(成功概率足够小)。

尽管我们发现了一些证据支持上述密码的安全性，还是可能存在一些未知的攻击方案。一旦出现这样的问题，图9.3中的两种扩充的模型将被作为进一步的可能解决方案(模型2中的第二个XOR操作可以被其他函数替代，如$x+b \bmod 2^n$)，目前尚无关于这两种模型的研究展开。请注意在本节介绍的密码中，数字化混沌系统实际上并不是必需的组件，其他密码学单元可以用来代替数字化混沌密码的作用。在未来的研究中我们也要探讨将该思路扩展到传统密码学中的可能性。



a) 扩充模型一　　b) 扩充模型二

图 9.3: 图9.1中密码的两类扩充模型

§9.3 混沌视频加密方案– CVES (Chaotic Video Encryption Scheme)

混沌视频加密系统(CVES)如图9.4所示，它是我们在文章[112]中提出的原始CVES的增强版本*。明文视频被逐簇逐簇的加密，这里一簇是一个或多个视频帧。

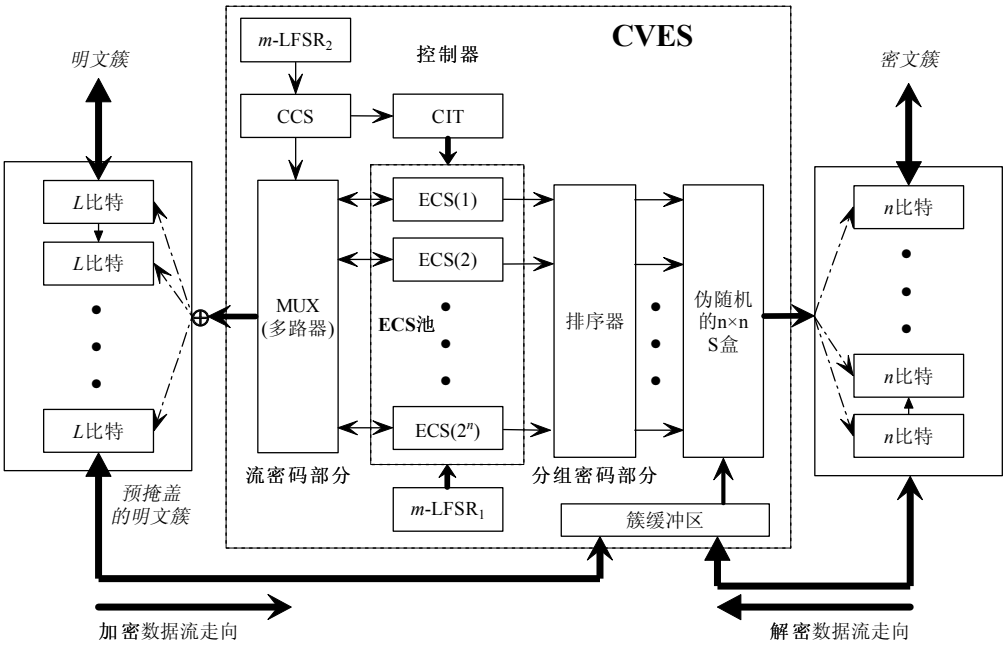


图 9.4: CVES的加密和解密流程

实际上，我们可以把视频流看作是无任何视频格式的数据流，并将其固定大小的字节块看作一个簇。这样的加密结构使得CVES独立于视频格式本身，从而不会带来与格式相关的副作用(如先加密后压缩造成的视频流数据扩增等)。显然，这个特点使得我们可以很自然地将其他视频加密方法中用到的一些基本思路和CVES接合起来，以得到更好的综合性能。如我们可以将压缩视频的“部分加密”(Partial Encryption)[221]思路与CVES接合起来，仅使用CVES加密视频流中的部分关键数据，这样可以极大地提高加密速度。类似地，我们也可以只用CVES加密视频流中的关键帧(如MPEG视频流中的*I*-帧[241])，而跳过其他类型的帧(如MPEG视频流中的*P*-帧和*B*-帧)不处理。

§9.3.1 组件

在描述CVES的加密和解密流程之前，我们先来介绍一下CVES的组成组件。

*由于未采用反馈机制，文献[112]中的原CVES是不够安全的。

1) **ECS池**：2^n个数字化混沌系统，它们被称为“加密混沌系统”(ECS，Encryption Chaotic Systems)并被表示为ECS(1) $\sim$ ECS(2^n)，组成了CVES的核心部分–ECS池。所有的2^n个ECS都是基于同一个定义在$I = [0,1]$上的一维混沌映射$F_e(x_e, p_e)$，只是控制参数$p_e(1) \sim p_e(2^n)$和/或初始条件可能不同。所有的ECS都在L-比特有限精度下通过扰动策略实现，最大长度LFSRm-LFSR$_1$用作扰动PRNG。该扰动m-LFSR$_1$的阶数为L_1，并且这2^n个ECS的扰动间隔分别为$\Delta_e(1) \sim \Delta_e(2^n)$。$2^n$个ECS的当前混沌状态表示为$x_e(1) \sim x_e(2^n)$，存储于$2^n$个$L$-比特的存储单元中。

2) **CCS**：一个单独的数字化混沌系统用来控制2^n个ECS的初始化和迭代过程。它被称为控制混沌系统(CCS，Control Chaotic System)。CCS也是基于一个定义在$I = [0,1]$上的一维混沌映射$F_c(x_c, p_c)$，它可能和F_e不同。CCS也在L-比特有限精度下以扰动策略实现，另外一个最大长度LFSRm-LFSR$_2$用作扰动PRNG。m-LFSR$_2$的阶数为L_2，并且CCS的扰动间隔为Δ_c。

3) **CIT**：一个控制信息表(CIT，Control Information Table)用来存储CVES需要的内部控制信息。关于其中的内容，参看§9.3.2和§9.3.3。CCS和CIT构成控制器单元。

4) **流密码部分**：一个被CCS控制的$2^n \times 1$的MUX(多路分配器)用来在不同的时刻选择一个ECS产生一个L-比特的混沌密钥，该密钥用来逐L-比特块异或当前的*明文簇*。被流密码部分加密后的*明文簇*称为*预掩盖的明文簇*。

5) **分组密码部分**：一个$2^n \times 2^n$的L-比特排序器和2^n个n-比特的存储单元$S[0] \sim S[2^n - 1]$构成一个伪随机S盒发生器(PRSBG，Pseudo-Random S-Boxes Generator)。产生的伪随机$n \times n$的S盒用来逐n-比特块替换*预掩盖的明文簇*。这里请注意在加密端的伪随机S盒和解密端的伪随机S盒是互逆的。

6) **簇缓冲区**：一个内存缓冲器用来临时存储当前*簇*和NC_{max}个L-比特的内部反馈变量：$N_F(1) \sim N_F(NC_{max})$，当每个预掩盖的明文被分组密码部分加密时它们用来伪随机地扰动产生的S盒$S[0] \sim S[2^n - 1]$。为了使每个明文簇的前几个明文块也依赖于前一个明文簇中的对应N_p个明文块，我们把存储的预掩盖明文块的数目增加到$NC_{max} + N_p$。这样，整个簇缓冲区由两部分组成：$N_F(1) \sim N_F(NC_{max})$和$N_F(-(N_p - 1)) \sim N_F(0)$。

§9.3.2 加密/解密流程

基于前面介绍的CVES的组件，我们可以如下描述加密流程。这里，我们将$x_e(1) \sim x_e(2^n)$，$p_e(1) \sim p_e(2^n)$和x_c, p_c看作是L-比特的整数，而不是$[0,1]$上的二进制小数(L-比特精度，定点算法)，以简化描述。

- **密钥**：$K = \{x_c, p_c\}$，密钥空间为2^{2L}。
- **初始化**：

a) 将CCS迭代$\eta \geq \lceil \lambda_c \rceil$次得到伪随机扰动间隔$\Delta_c$，该值应是一个比$2^n$小的素数。

b) 迭代CCS大约2^n次得到所有ECS的2^n个非零的伪随机初始条件$x_{e0}(1) \sim x_{e0}(2^n)$。将这$2^n$个初始条件存储在CIT中。

注释：如果在CCS的拟混沌轨道中出现了0，则迭代的次数会比2^n大一点。但是这样一个事件的发生概率在$L \geq 16$和$L \geq 2n$时很小。比如，当$L = 16, n = 8$时，该概率大约为0.00389866021632。有另外一个途径解决这个小问题：一旦CCS的混沌状态变成0，就马上使用扰动PRNG扰动它，然后使用扰动后的拟轨道产生$x_{e0}(i)$。这样的话，迭代次数将始终为2^n。

c) 再迭代CCS大约2^n次生成所有ECS的2^n个非零(参看上一条的注释)伪随机的控制参数$p_{e0}(1) \sim p_{e0}(2^n)$。如果至少有两个控制参数是相同的，则抛弃所有的$2^n$个控制参数并重复上述过程。将这$2^n$个控制参数存储在CIT中。

注释一：如果L不比n大的很多，出现相同控制参数的概率可能是比较高的，会使得初始化过程变得太慢。比如，当$n = 8, L = 16$，该概率大约为0.4。因此需要满足$L \gg n$，这会使得该概率接近0。比如，$n = 8, L = 24$时，该概率大约为0.002。

注释二：实际上，相同控制参数的要求可以按照如下方式得到放松：仅当至少两个ECS具有相同的控制参数并且同时具有相同的初始条件的时，初始化才重新复位。在这种情况下，该概率会变得足够小以至于我们可以完全忽略这个问题。比如，当$L = 16, n = 8$时，该概率大约为0.000007659167674645 14。

d) 对2^n个初始状态$x_{e0}(1) \sim x_{e0}(2^n)$进行排序以产生初始S盒(一个$0 \sim 255$的伪随机置换)$S[0] \sim S[2^n - 1]$。该序列按照如下方法初始化扰动间隔：

$$\Delta_e(i) = \begin{cases} P_r(S[i]), & 0 \leq S[i] \leq I_{max} \\ P_r(\text{rand}(I_{max})), & I_{max} + 1 \leq S[i] \leq 2^n \end{cases}, \tag{9.3}$$

这里$P_r(0) = 1$和$P_r(i)(i > 0)$表示从2开始的第i个素数，$\text{rand}(n)$表示一个生成1到n之间的整数的伪随机函数。I_{max}个素数$P_r(1) \sim P_r(I_{max})$通过预先计算得到并存储在CIT中。

注释：I_{max}的一个建议值是31($P_r(31) = 127$)，这对于得到流密码部分的长循环周期已经足够。更多讨论参看§9.4.2。

e) 将每个ECS(i)迭代$\eta \geq \lceil \lambda(i) \rceil$次，这里$\lambda(i)$表示ECS($i$)的Lyaponov指数。最后，依次迭代每个ECS(i)直到生成NC_{max}个L-比特随机整数，然后用这些随机数初始化$N_F(1) \sim N_F(NC_{max})$。

- **加密流程**：一个*明文簇*首先被流密码部分加密，然后被分组密码部分加密。我们分别描述这两部分的工作方法。
  - **流密码部分**：流密码部分对*明文簇*逐L-比特块加密。假设当前的L-比特明文块为当前明文簇中的第$i(i = 1 \sim NC_{max})$个明文块$P_L(i)$。加密流

程可以表示如下：运行CCS一次，得到$I_n = (x_c \bmod 2^n) + 1$，然后迭代ECS$(I_n)$一次并执行$\widetilde{P}_L(i) = P_L(i) \oplus x_e(I_n)$*。注意对每个明文块仅被选中的ECS迭代一次，这有利于提高加密速度和增强安全性。加密流程运行直到当前明文簇中的所有明文块都被加密，然后预掩盖的明文簇被送往分组密码部分进行下一步加密。

– **分组密码部分**：分组密码部分是一个简单的具有$n \times n$的时变S盒的替换密码，该S盒同时伪随机地受控于2^n个ECS和簇缓冲区的内容。将L-比特的反馈变量$N_F(1) \sim N_F(NC_{max})$重新划分为$n$-比特的整数†$N_{Fn}(1) \sim N_{Fn}(NC_{max} \cdot L/n)$，类似地将$\widetilde{P}_L(1) \sim \widetilde{P}_L(NC_{max})$重新划分为$\widetilde{P}_{Ln}(1) \sim \widetilde{P}_{Ln}(NC_{max} \cdot L/n)$。然后使用当前的S盒按照如下方式替换预掩盖的明文簇中的每个n-比特块：$C_n(i) = S\left[\left(\widetilde{P}_{Ln}(i) + N_{Fn}(i)\right) \bmod 2^n\right]$ $(i = 1 \sim NC_{max} \cdot L/n)$。在当前明文簇被加密以后，通过对$2^n$个混沌状态$x_e(1) \sim x_e(2^n)$进行排序得到新的S盒($S[0] \sim S[2^n - 1]$存储排序结果)。最后如下设置簇缓冲区：将$N_F(NC_{max}) \sim N_F(NC_{max} + 1 - N_p)$复制到$N_F(0) \sim N_F(-(N_p - 1))$，对$i = 0 \sim NC_{max} - 1$设置$N_F(i+1) = N_F(i) \oplus \widetilde{P}_L(i) \oplus \widetilde{P}_L(i - N_p)$。

注释：显然，类似CBC模式，头$NC_{max} + N_p$个L-比特的明文块不像后面的那么安全。因此一个伪随机生成的$(NC_{max} + N_p) \cdot L$-比特的IV需要插入到每个明文视频的头部(插入一个随机初始帧也可以)。

在当前明文簇加密完成之后，流密码部分继续加密下一个明文簇。加密过程运行直到所有的明文簇都加密完成。

- **解密流程**：解密流程是加密的逆过程(参看图9.4)。密文簇首先被分组密码部分解密，这里的S盒是加密过程中S盒的逆。然后预解密的密文簇被流密码部分解密。

由以上描述，我们可以看到CVES可以看作是图9.3b中的扩充模型的一种简化版本：第二个异或操作被f_S中的“mod 2^n”代替。由于这种额外的操作使得CVES更为安全‡，看起来图9.3中的三重加密机制或许确实是有用的。

§9.3.3 支持随机检索的改进版CVES–RRS-CVES

在上一节中提出的CVES中，由于CCS和所有ECS的拟混沌轨道无法通过密文簇的位置来预测，密文视频的随机检索并不支持。为了解密一个密文簇，我们首先必需解密前面的所有密文簇。也就是说，该CVES方案仅支持顺序检索，而不支持随机检索。不过，我们可以对原CVES方案做一些修改以增加这种功能。改进

*如果最后一个明文块包含的比特数$L' < L$，仅使用$x_e(I_n)$的高L'个比特加密明文块，并设置$\widetilde{P}_L(i)$的其他比特为0。当然，视频流本身需要一定的机制以确定L'的正确值。

†任何明文簇的大小应当可以被n整除，否则需要加入某些同步标记，视频流也需要特殊的格式支持。当$n = 8$，满足这个条件一般而言是非常容易的。

‡文献[112]中的原始CVES方案没有采用这样的额外操作，因而是不够安全的。

后的CVES称为支持随机检索的CVES(RRS-CVES，Random-Retrieval-Supported CVES)。

- **初始化**：除了原CVES方案中的初始化操作a)∼e)，需要加入下述三个初始化操作：

  a′) 产生复位信息：运行CCS2 + 2^n次产生两个L-比特的伪随机数p_+、x_+和2^n个m-比特的伪随机数$\tau_e(1) \sim \tau_e(2^n)$*，将它们存储在CIT中。这里，$\tau_e(i)(i = 1 \sim 2^n)$需要满足下述条件：$\gcd(\tau_e(i), 2) = 1$和$\tau_e(i) \geq \tau_{min}$，这里$\tau_{min}$不应太小。关于$m$和$\tau_{min}$的选取，我们将在§9.3.4中给出一些讨论。这$2 + 2^n$个额外的伪随机数用来对$2^n$个ECS定时复位(用来支持随机检索)。

  b′) 产生混沌迭代的次序：对2^n个预先生成的控制参数$p_{e0}(1) \sim p_{e0}(2^n)$进行排序以得到一个排序序列$r_e(1) \sim r_e(2^n)$，这里$r_e(i) = 1 \sim 2^n$。该序列存储在CIT中，并用来控制$2^n$个ECS的迭代次序。

  c′) 初始化迭代计数器：2^n个L-比特的存储单元$C_1(1) \sim C_1(2^n)$用来存储2^n个ECS的迭代次数。另外2^n个L-比特的存储单元$C_2(1) \sim C_2(2^n)$用来存储2^n个ECS的复位次数。设置全部$2 \cdot 2^n$个L-比特存储单元为0。

  总结起来，对于RRS-CVES而言，在CIT中存储有下面的数据：1) *初始状态* – $x_{e0}(1) \sim x_{e0}(2^n)$；2) *控制参数* – $p_{e0}(1) \sim p_{e0}(2^n)$；3) *扰动间隔* – $\Delta_e(1) \sim \Delta_e(2^n)$；4) *素数列表* – $P_r(1) \sim P_r(I_{max})$；5) *复位信息* – $\tau_e(1) \sim \tau_e(2^n)$ and p_+, x_+；6) *混沌迭代的次序序列* – $r_e(1) \sim r_e(2^n)$；7) *迭代/复位计数器* – $C_1(1) \sim C_1(2^n)$和$C_2(1) \sim C_2(2^n)$。在原始的CVES中，只有前面四种数据需要存储。

- **加密流程**：在RRS-CVES中，流密码部分使用复位机制加以改进，但是分组密码部分没有任何变动。$r_e(1) \sim r_e(2^n)$用来选择一个ECS加密当前的明文块，而不再象原CVES中通过迭代一次CCS决定迭代哪个ECS：对于第i个明文块，选择ECS($r_e(i \bmod 2^n)$)作为当前的ECS。对于任何ECS(i)，在其运行一次以后，将其迭代计数器加一：$C_1(i) + +$。如果$C_1(i) \bmod \tau_e(i) = 0$，则按照如下方法对ECS($i$)**复位**：$x_{e0}(i) = (x_{e0}(i) + x_+) \bmod 2^L$，$x_e(i) = x_{e0}(i)$，以及$C_1(i) = 0, C_2(i) + +$。如果$C_2(i) \bmod \tau_e(i) = 0$，按照如下方式对ECS($i$)**复位**：$p_{e0}(i) = (p_{e0}(i) + p_+) \bmod 2^L$，$p_e(i) = p_{e0}(i)$以及$C_1(i) = C_2(i) = 0$。

- **解密流程**：进行类似于加密流程的修改。

由RRS-CVES的加密流程，我们可以看到下述事实。将密文视频看作是L-比特的数据流，如果我们知道一个密文簇在整个L-比特流中的位置，就可能在可接

*一个m-比特的伪随机数x'可以通过L-比特的混沌状态x按照如下方式产生：$x' = x \bmod 2^m$或者$x' = x >> (L - m)$。

受的最大延时内重建所有ECS的相应状态。假设一个密文簇的位置为I_L，即该密文簇之前的所有L-比特簇总数为I_L。我们可以如下重建所有2^n个ECS：

1. $I_{ECS} = (I_L \bmod 2^n) + 1$，$I'_L = I_L/2^n$；
2. $i = 1 \sim 2^n$：$I_{c1}(i) = I'_L/\tau_e(i)$，$I'_{c1}(i) = I'_L \bmod \tau_e(i)$，$I_{c2}(i) = I_{c1}/\tau_e(i)$；
3. $i = 1 \sim 2^n$：$x_e(i) = (x_{e0}(i) + I_{c1}(i) \cdot x_+) \bmod 2^L$，$p_e(i) = (p_{e0}(i) + I_{c2}(i) \cdot p_+) \bmod 2^L$；
4. $i = 1 \sim 2^n$：如果$r_e(i) = 1 \sim I_{ECS}$，运行ECS(i)$I'_{c1}(i) + 1$次，否则(如果$r_e(i) = I_{ECS} + 1 \sim 2^n$)则运行ECS($i$)$I'_{c1}(i)$次；
5. 采用正常的解密方法解密当前密文簇。

可以看到需要一些预计算以重建2^n个ECS的当前状态。随机检索的最大延时由第四步中的混沌迭代的次数决定：

$$\sum_{r_e(i)=1}^{I_{ECS}} (I'_{c1}(i) + 1) + \sum_{r_e(i)=I_{ECS}+1}^{2^n} I'_{c1}(i) = \sum_{i=1}^{2^n} I'_{c1}(i) + I_{ECS}。 \tag{9.4}$$

假设每次混沌迭代耗费的时间为τ_0，最大延时τ将满足$2^n \cdot \tau_{min} \leq \tau/\tau_0 < 2^{n+m}$。在§9.4.1中，我们将进一步讨论这个问题。

§9.3.4 配置CVES和RRS-CVES

为了在实际应用中优化CVES和RRS-CVES，一些参数需要仔细地进行配置。

首先，我们需要仔细地选择混沌系统。如我们在本文中一再建议的，PWLCM再次被推荐在CVES中使用以获得最佳性能。

三个基本的参数为L，n和N_p。1) L：由于密钥空间为2^{2L}，L应当足够大以保证安全性。另外，为了简化CVES在数字计算机中的实现，$L = 32$或者64被建议使用。如果需要更高的密钥熵，需要引入额外的密钥。如，$x_{e0}(1)$和$p_{e0}(1)$可以作为新的秘密参数，使用ECS(1)产生$x_{e0}(2) \sim x_{e0}(2^n)$和$p_{e0}(2) \sim p_{e0}(2^n)$；2) n：显然，CVES/RRS-CVES的实现复杂度和n具有指数关系：需要$O(2^n \cdot L)$个存储比特。因而，n不能太大，我们建议$n = 8$。3) N_p：如我们在前面提到的，这个参数是用来保证对选择明文攻击安全性的，我们建议$N_p \cdot L \geq 256$。

已经知道2^n个ECS和CCS的扰动参数对于改善数字化混沌系统的动力学特性退化是很有用的。在文献[80]中，作者指出扰动间隔可以非常大，比如当$L = 40$时可取10^6。但是我们认为从严格的密码学角度看它们不应太大*。当$I_{max} = 31$时，最大的扰动间隔为127(自2开始的第31个素数)，这在实际中是可行的。

簇的大小是CVES/RRS-CVES的另外一个重要参数。尽管该大小不必是固定的，但是固定的簇大小有助于简化实现和性能的估计。假设一个簇包

*考虑如下事实：甚至当L足够大时，还是存在一些具有相当短循环周期的拟混沌轨道。一个极端的例子还是数字化tent映射$F(x) = 1 - 2|x - 0.5|$，自$a/2L$开始的任何拟混沌轨道经过最多L次迭代之后总会收敛到0。

含NC_{max}个L-比特块。在后面我们将看到NC_{max}可以用来调节加密速度。一般而言，NC_{max}越大，加密速度就越快。进一步的分析在§9.4.1中给出。如果簇大小是可变的，平均大小$\overline{P}_{max}$可以用来大致估算加密速度。

对于RRS-CVES，m和τ_{min}用来控制2^n个ECS的复位操作。一般地，我们建议$m \leq n$和$\tau_{min} \geq 2^{n/2}$。这样最大延时将满足$2^{3n/2} \leq \tau/\tau_0 \leq 2^{2n}$。既然$n$不是太大，这样一个最大延时在大多数实时应用中是可接受的(参看§9.4.1)。

§9.4 性能估计

§9.4.1 速度问题

基于两个组成部分的加密速度，我们可以大致估算整个CVES的速度。一般而言，CVES/RRS-CVES的硬件系统会比软件系统的运行速度快得多，因为并行运算机制在硬件实现中是可能的。不失一般性，假设全部ECS和CCS都是由方程(2.1)实现的，并且簇大小固定为$NC_{max} \cdot L$个比特。

硬件实现：一般地，一次L-比特的定点除法消耗L个时钟周期，则每次混沌迭代大致消耗L个时钟周期。如果使用多级流水技术，流密码部分可以每L个时钟周期加密一个L-比特明文块。假设排序器消耗的一次排序时间为τ_s(时钟周期)，对于大多数耗时的排序器，$\tau_s = 2^n \cdot (2^n - 1)$；对于速度优化的排序器，$\tau_s = n \cdot 2^n$。分组密码部分可以每个时钟周期加密一个$n$-比特单元。综合起来，对于一个明文簇，消耗的总的时钟数为$L \cdot NC_{max} + \tau_s + NC_{max} \cdot L/n$。如果时钟主频为$f_b$ MHz，最终的CVES加密速度为$f_b \Big/ \left(1 + \frac{1}{n} + \frac{\tau_s}{L \cdot NC_{max}}\right)$ Mbps。显然，NC_{max}可以用来调节加密速度。当$L = 32, n = 8$，$\tau_s = n \cdot 2^n$和$NC_{max} = n \cdot 2^n = 2048$，加密速度为$\frac{32}{37} f_b$ Mbps。这样的速度比很多快速传统密码都快。当然，这里的估算结果只是理论值，实际的速度还和具体实现细节有很大的关系。

由以上讨论，可以看到：当$NC_{max} \geq \tau_s/L$时，实际的加密速度主要由流密码部分决定；而当$NC_{max} < \tau_s/L$时则主要由分组密码中的排序决定。对于CVES/RRS-CVES的大多数应用，我们建议$NC_{max} = n \cdot 2^n$。当$L \geq 32, n = 8$时，NC_{max}将比τ_s/L大(甚至对于最为耗时的排序器，也有$\tau_s/L = 2^n \cdot (2^n - 1)/L < n \cdot 2^n$)。因而，在大多数应用中，在排序器的设计中可以主要考虑如何简化硬件规模，而不是如何提高加密速度。

如果额外的缓冲区用来支持流水式加密/解密，那么加密速度将仅由两个密码子系统中较慢的部分决定。也就是说，加密速度成为$\min\left(f_b, f_b \Big/ \left(\frac{1}{n} + \frac{\tau_s}{L \cdot NC_{max}}\right)\right)$ Mbps。当$NC_{max} \geq \tau_s/L$时，速度约为f_b Mbps。

软件实现：由于并行运算一般不可用，软件实现会比硬件实现慢得多。有理由推测软件实现的速度会比硬件实现慢很多倍。一个参数为$L = 16, n = 8$的试验系统使用Microsoft® Visual C++开发出来以测试在Microsoft® Windows™平台下的实际速度。试验数据表明最终速度大概是CPU频率的$1/L$。比如，在一个1.4GHz的奔腾(Pentium)®IVCPU上，速度大

约为83Mbps(1.4G/L = 87.5Mbps)；在一个700MHz赛扬(Celeron)®CPU上，速度大约为46Mbps(700M/L = 43.75M)。这样的速度对于一个软件密码而言已经相当快了(特别是对于混沌密码)。作为一个参照，256-比特的AES在一个600MHz的CPU上的速度大致为66Mbps[166]。

在我们的试验系统中，我们发现流密码部分(其核心为数字化PWLCM)在最终速度中起着主导作用。在上述的1.4GHz奔腾(Pentium)®IVCPU上，流密码部分的速度大约为107Mbps，而分组密码部分的速度则大约为636Mbps！将流密码部分的速度(107Mbps)和最终速度(83Mbps)比较一下，看起来我们的C++代码应该可以继续优化以得到更高的速度(接近100Mbps)。关于这个问题，我们发现一个线索：当我们将Visual C++ 6.0的编译开关由“Default”改为“Maximized speed”之后，流密码部分的速度反而变低为98Mbps。这个奇怪的现象(“最大化的速度”反而比“缺省速度”低)暗示我们的C++代码确实存在需要优化的地方。在未来的研究中我们将试图发现有关这个问题的更多结论。

最后让我们来讨论一下消耗在初始化过程的时间和RRS-CVES的最大延时。

对于CVES的初始化过程，最耗时的操作是大约$(2+\eta)\cdot 2^n$次混沌迭代和一次2^n个数据的排序过程，这大约意味着$(2+\eta)\cdot 2^n\cdot L + n\cdot 2^n$个时钟周期。假设$\eta = 4 > \lceil\lambda\rceil = 2$，消耗时间大约为$(6L+n)\cdot 2^n$个时钟周期。当$L = 32, n = 8$时，时间为51,200个时钟周期。类似地，对于RRS-CVES，主要初始化过程的消耗时间可以计算出来：大约为$(3+\eta)\cdot 2^n\cdot L + 2\cdot n\cdot 2^n = ((3+\eta)\cdot L + 2n)\cdot 2^n$个时钟周期。假设$\eta = 4$并且$L = 32, n = 8$，时间为61,400个时钟周期。显然，初始化消耗的时间并不多。

关于RRS-CVES随机检索的最大延时，我们已经在§9.3.4中指出大约为$2^{3n/2} \le \tau/\tau_0 \le 2^{2n}$。当$L = 32, n = 8$时，该值为$2^{17} \le \tau \le 2^{21}$个时钟周期(考虑到$\tau_0$等于$L$个时钟周期)。如果$f_b \ge 200$MHz，最大延时不会超过10个毫秒。

§9.4.2 安全性

基本的密码学特性

CVES具有下列基本的密码学特性，它们是一个好的密码的基本要素。

1) 平衡性：由于2^n个ECS的拟混沌轨道具有均匀的分布函数，则被流密码部分掩盖的明文簇也具有均匀的分布。考虑到分组密码只是对预掩盖的明文簇进行替换操作，这种操作不会改变分布特性因为S盒实际上是一个一一映射。这说明密文视频是平衡的。

2) 相对密钥的雪崩特性：如果密钥$K = \{x_c, p_c\}$仅仅改变一个比特，则ECS的初始条件或者控制参数将发生强烈的改变，因为CCS对初始条件和控制参数非常敏感。初始条件和/或控制参数改变一点，密文即改变很大，就意味着密文的雪崩特性。

避免潜在攻击的本质特征

CVES有四个本质特点也暗示了其安全性。当然，需要更多的研究去证实这些特点的作用。

1. 前面提到的选择明文攻击被密文对前面N_p个L-比特的预掩盖明文块所禁止，这使得时变的S盒f_S同时依赖于混沌状态和以前的明文。

2. 每个明文簇都具有不同的S盒，而簇大小(一般为$O(2^8)$)又太小不足以发现S盒可能存在的弱点，因此基于统计的密码分析工具似乎是无效的。

3. 流密码部分由2^n个渐近独立的混沌映射(ECS池)构成，并且混沌迭代的顺序被另外一个独立的混沌映射(CCS)伪随机地控制。上述两点使得统计密码分析更为困难。

4. 在最差的情况下，甚至当2^n个ECS的状态全部已知的情况下(则相关的S盒也已知)*，也几乎不可能推出密钥$K = \{x_c, p_c\}$，因为密钥本身和2^n个ECS的混沌状态是分离的(考虑以前的2^n个ECS的混沌迭代的存在)。回顾初始化过程中，$\eta \geq \lceil \lambda \rceil$次预迭代是需要的，它们用来避免上述攻击的可能性，如果第一个簇的2^n个混沌状态已知的话。

流密码部分的序列周期长度

在CVES/RRS-CVES中，流密码部分和分组密码部分都是基于2^n个ECS和CCS的拟混沌轨道的。将ECS池的当前2^n个状态看作一个2^n维的向量(这里我们称之为混沌向量，Chaotic Vector)，这个向量的周期长度也是一个衡量整个密码安全性的基本因素。该长度必须足够大以避免可能的重复加密模式。

由文献[80]，我们可以很容易地知道CCS的周期长度：$T_c = \sigma_c \Delta_c (2^L - 1)$，以及$2^n$个ECS的周期长度：$T_e(i) = \sigma_e(i)\Delta_e(i)(2^L - 1)(i = 1 \sim 2^n)$，这里$\{\sigma_e(i)\}_{i=1}^{2^n}, \sigma_c$是正整数。尽管确切计算混沌向量的周期长度是比较困难的，但是可以导出其量级为：

$$\begin{aligned} &\operatorname{lcm}\left(\sigma_e(1), \cdots, \sigma_e(2^n), \sigma_c\right) \cdot \left(2^{L_1} - 1\right) \cdot \left(2^{L_2} - 1\right) \cdot \operatorname{lcm}\left(\Delta_e(1), \cdots, \Delta_e(2^n), \Delta_c\right) \\ &\qquad > 2^{L_1 + L_2} \cdot \operatorname{lcm}\left(\Delta_e(1), \cdots, \Delta_e(2^n), 2\right) 。 \end{aligned} \tag{9.5}$$

当$I_{max} = 31$时，

$$\operatorname{lcm}\left(\Delta_e(1), \cdots, \Delta_e(2^n), 2\right) = \prod_{i=1}^{I_{max}} P_r(i) \approx 2^{161} 。 \tag{9.6}$$

这样一个长度对于任何安全应用都足够了。

*显然，在实际应用中，这样一种攻击是相当困难的，因为当前的混沌状态不能从已知明文簇/密文簇对中直接导出。

分组密码部分的伪随机S盒

在本节中，由ECS池的混沌状态产生的伪随机S盒的统计特性。由于2^n个ECS在相同的定义区间$I = [0,1]$上具有相同的不变分布函数$f(x) = 1$，通过2^n混沌状态生成的S盒可以描述为2^n个独立同分布的随机变量的*顺序统计量*。假设$R(1), R(2), \cdots, R(2^n)$表示顺序统计量，则下述事实成立：对于$\{1, \cdots, 2^n\}$上的任何排列$\{i(1), i(2), \cdots, i(2^n)\}$，

$$P\{R(1) = i(1) \wedge R(2) = i(2) \wedge \cdots \wedge R(2^n) = i(2^n)\} = \frac{1}{2^n!}, \tag{9.7}$$

即顺序统计量是等概对称的[212]。这个特点对于构造优良的密码学特性是非常有用的。当然，在所有的$2^n!$个可能的S盒中，必然存在一些弱S盒，但是这样的S盒的数量比强的S盒的数量要少得多。而且，流密码和分组密码的组合使得弱S盒的检测变得困难。在最坏的情况下，即便攻击者得到了一个弱的S盒，也只能恢复相关的*明文簇*，其他的使用不同的S盒的*明文簇*仍然是安全的。

§9.4.3 实现复杂度

由于一般L和n都是可以被8整数的，CVES/RRS-CVES的软件实现是相当简单的，因为8-比特字节在不同平台的几乎所有编程语言中都有很好的支持。因此，在本小节中我们主要关注硬件实现复杂度。

最重要的硬件单元是一个用于实现混沌迭代的L-比特数字除法器和一个一个$2^n \times 2^n$的排序器。其他单元包括：两个m-LFSR，和存储CIT、当前的2^n个混沌状态、簇缓冲区和S盒的存储单元。对于CVES，CIT需要$4 \cdot 2^n$个L-比特的存储单元，S盒需要2^n个n-比特的存储单元。对于RRS-CVES，CIT需要$8 \cdot 2^n$个L-比特的存储单元，S盒还是需要2^n个n-比特的存储单元。当$L = 64, m = 8$时，CVES所需的存储单元总量大约为$4 \cdot 2^n \cdot L + n \cdot 2^n = 67,584$ bits $= 8,448$ bytes。对于RRS-CVES，存储总量为$9 \cdot 2^n \cdot L + n \cdot 2^n = 149,504$ bits $= 18,688$ bytes。另外，一个大小和*簇*大小相同的缓冲区可能需要以加快流密码加密后的分组密码的替换。尽管所需的存储单元有点多(大概几十KB)，但是对于实时视频应用来说这简直不值一提。

在CVES/RRS-CVES中，排序器是最为复杂的单元之一。正如我们在§9.4.1中提到的，当*簇*大小大于$n \cdot 2^n / L$时，排序器可以不必考虑太多的实现优化，因为它对系统速度的影响不大。

§9.4.4 试验

对于一个没有压缩的数字视频，我们测试了CVES的实际性能。在图9.5中，我们给出了一副明文帧和密文帧的比较。可以看到明文帧被加密变换为具有均匀直方图的密文帧，这暗示着CVES具有不错的密码学特性。

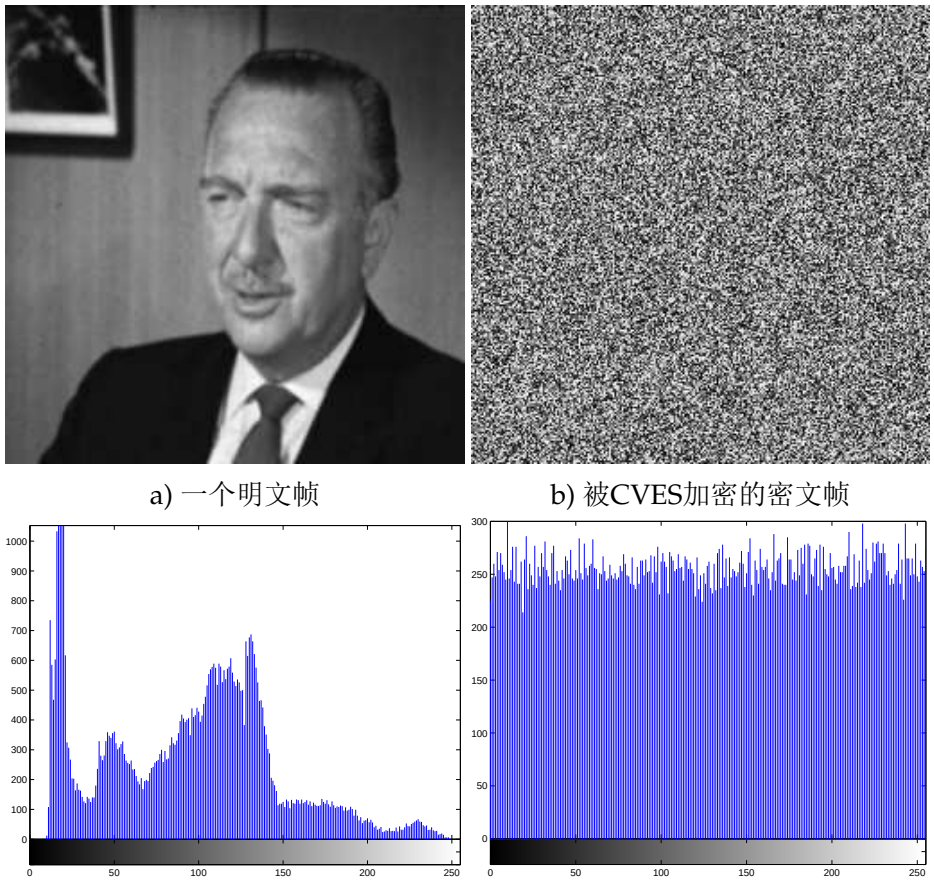


图 9.5: 使用CVES加密的无格式数字视频

§9.5 本章小结

在本章中，我们提出了一种基于多个混沌系统的实时视频加密系统(Chaotic Video Encryption Scheme – CVES)，它是使用数字化混沌解决存在于实时视频加密中安全性和加密速度之间矛盾的一种尝试。CVES是包含一个流密码子系统和一个分组密码子系统的乘积密码系统。CVES可以扩展为RRS-CVES，这是一种支持密文视频的随机检索功能(具有可接受的最大延时)的改进版本。初步分析表明CVES/RRS-CVES具有很快的加密速度和可接受的安全性，并且可以使用硬件和软件很容易地实现。实际上，在CVES中使用的基本想法(图9.1)可以推广为一种设计数字化密码的通用模型。

在未来的研究中，我们将继续探讨有关CVES/RRS-CVES的安全性和实现中的相关问题，并试图完成CVES的标准VLSI(硬件)实现和C/C++软件包(软件)，并探讨如何使用其他视频加密方法中的有益思路进一步强化CVES在特定视频应用中

的性能。另外，如果可能，图9.3中所示的两类扩展模型也会被关注。

第十章 总结与展望

§10.1 本论文的总结

现在我们对全文给出一个简要的总结。本文的工作大致归纳为三个大的部分：关于数字化混沌系统的理论分析，数字化混沌密码的分析和设计。下面我们从上面三个方面分别对本文的工作做一个总结。

- **数字化混沌系统动力学特性退化的理论分析**
  - 已有的研究表明：发展一种严格描述数字化混沌系统动力学的理论对于数字化混沌系统的应用是非常重要的。但是，虽然关于数字化混沌系统的动力学特性已有相当多的工作报道，还没有一个系统的理论框架建立起来。对于一类广为使用的混沌系统–逐段线性混沌映射(PWLCM)，我们发现一组动力学指标可以定量地描述拟混沌轨道分布的不均匀性。本文导出了这组动力学指标的准确计算方法，并给出了一些例子以说明这些指标在理解有限精度下数字化PWLCM动力学特性退化方面的重要性。详细讨论了这组动力学指标的应用，包括在混沌密码学中的应用(见下)。
- **一些最近提出的数字化混沌密码的分析**
  - 使用本文提出的PWLCM的动力学指标，对周红等人提出的一类混沌流密码进行了弱密钥分析和密码分析。本文对几种可能的改进安全性的措施进行了比较，并推荐了其中的几种用于改进安全性。
  - E. Alvarez等人于1999年提出了一种基于搜索的数字化混沌密码，该密码在一个由混沌系统生成的伪随机序列中搜索明文，并据此产生密文。该密码在提出后很快被G. Alvarez等人于2000年攻破。本文分析了E. Alvarez等人的密码方案不能抵抗G. Alvarez等人攻击的本质原因，并提出了一种改进方案增强其安全性。
  - M. S. Baptista于1998年提出了另外一种基于搜索的混沌密码，该密码在提出后得到了较为广泛的注意。一些密码分析工作和改进方案在近年屡有报道。本文指出了G. Jakimoski和L. Kocarev提出的一种攻击不是那么有效，并给出了一种改进措施以抵抗所有的已知攻击(不止是Jakimoski-Kocarev攻击)。在提出的改进措施中，一种有趣的称为“概率解密”的现象被发现，该现象可能可以用来实现另外一种可视加密术。
  - S. Papadimitriou等人于2001年提出了一种基于混沌系统的快速概率密码。本文分析了该混沌密码的问题，并提出其不安全性和不实用性，并纠正了一些S. Papadimitriou等人给出的错误推导和分析。

  - 近年来J.-C. Yen和J.-I. Guo(等人)提出了几种混沌图象加密方法。本文分析了其中的两种方法(CKBA和BRIE)，提出了已知/选择明文攻击攻破这两种加密系统。

- **设计数字化混沌密码的新思路**

  - 基于本文关于数字化混沌系统的理论分析和一些最近提出的数字化混沌密码的分析工作，本文提出了一种新的混沌PRBG并应用它设计新的具有较好整体性能的混沌流密码。该混沌PRBG可以替代LFSR在传统流密码学中的作用以构造更为灵活的密码系统。
  - 还是基于上面提到的成果，本文提出了一种快速混沌密码系统，它用来满足实时视频加密的特殊需求。详细的分析表明该混沌密码可以同时提供相当快的加密速度和较高的安全性。该密码也可以看作是一种数字化(混沌)密码的通用结构。

§10.2 关于未来研究的展望

由本文给出的讨论，我们可以发现设计一个真正好的数字化混沌密码绝不是一个容易的任务。很多问题必须加以仔细考虑以避免各种各样的潜在安全缺陷，才可能达到理想的性能。但是由于关于数字化混沌系统的动力学特性退化的理论问题还没有解决，我们只能小心地使用一些实践性的手段来绕开理论上的困难。作为一个基本的建议，伪随机的扰动策略可能是一个可接受的措施。除了和动力学特性退化相关的安全问题之外，很多数字化混沌密码由于缺乏仔细的设计而被攻击，而不是因为数字化混沌系统的本质缺陷。这个事实说明一些关于如何避免设计弱混沌密码的一些原则需要明确。这里我们将给出一些这方面的通用建议。希望我们建议有助于加快这类设计原则的系统化。

§10.2.1 设计好的混沌密码的一些建议

基于本文给出的数字化混沌密码研究现状的回顾，和相关问题及其可能的解决方案的讨论，在本文的最后我们愿意重新给出关于设计“好”的混沌密码的一些基本建议，这里“好”这个词意味着足够高的实际安全性，足够快的加密速度和简单的系统实现。

建议之一：通过伪随机扰动实现数字化混沌系统，或者使用动力学特性已经得到证明的离散混沌系统。正如我们在§2.5中提到的，在有限精度下实现的数字化混沌系统存在动力学特性退化。鉴于目前尚无系统的理论框架可以描述这种退化，需要采用一些实际的改进措施来改进数字化混沌的动力学特性。我们建议使用基于一个简单PRNG的扰动策略，其实际性能还是相当不错的。一些连续混沌映射的离散化版本也可能可用，但是最好设计者可以证明(至少“以足够的试验证据说明”)它们的动力学(密码学)特性。

建议之二：使用定点算法而不是浮点算法。显然浮点算法会降低加密速度并增加实现复杂度和成本。因此我们建议使用定点算法。另外，定点算法也有助于提高不同软件平台和硬件结构中的系统移植性。浮点算法的另外一个缺点是：浮点算法离散网格不是均匀的，这可能使得控制数字化混沌系统的动力学特性退化变得更为复杂和困难。

建议之三：使用最简单的混沌系统，比如逐段线性映射(PWLCM)。更为复杂的混沌系统一般被用来增强混沌密码的安全性。但是复杂混沌系统的使用可能从以下两个方面降低加密速度：第一，混沌系统越复杂，混沌迭代耗费的时间越多；第二，很多复杂的混沌系统必须使用浮点算法进行迭代，这使得迭代更加得慢。基本上，我们建议在任何场合都使用PWLCM。如果PWLCM在某些应用中不可用(我们认为这样的应用是很少见的)，请选用可用的最简单的系统。

建议之四：尽可能减少加密一个明文所需的混沌迭代次数。大部分混沌分组密码过慢的加密速度是由于多次迭代的使用造成的，它们都不满足这个建议。一些新的混沌分组密码[105, 106, 108, 112, 124]克服了这个问题，可以在设计中用作参考。

建议之五：如果可能，使用多个混沌系统而不是单个混沌系统。尽管没有严格的证明给出，关于好的和坏的混沌密码的设计知识(经验与教训)暗示使用多个混沌系统可能增强系统的安全性。一些研究[22, 112, 124]还表明多混沌系统的使用可能提高加密速度。

§10.2.2 数字化混沌密码学中的开放话题

在文献[101]中，L. Kocarev建议混沌密码学的未来研究应当集中在混沌和密码学的关系上，而不是具体的混沌新密码的设计上。我们基本同意这个观点。当然，如果一种新的混沌密码结构可以提供好得多的性能，还是有意义的。下面我们给出一些数字化混沌密码领域的开放话题。

关于数字化混沌的理论。为了估计数字化混沌系统的动力学特性，我们迫切需要关于离散空间中混沌的一个系统理论。然而，在这方面的工作还太少。在文献[202]中，H. Waelbroeck等人尝试将连续混沌的定义扩展到离散状态空间去(他们称之为“离散混沌”)。这是数字化混沌方面的一个有趣尝试。我们在第3章和文献[109]中也给出了一个从算法角度研究数字化混沌的新思路。

由数字化混沌产生的不可预测的伪随机性。数字化混沌产生的伪随机序列是很多混沌密码的核心。如何衡量这种伪随机序列的不可预测性是一个尚未解决的问题。在连续混沌理论中，信息熵可以用来刻画信息随着混沌迭代的进行而消失的速率[208, 210, 242]。类似的概念可能有助于解释这里的不可预测性，比如文献[22, 58]中给出的分析。

传统密码中的混沌现象。在§1.1中，我们已经提到任何传统密码都可以看作是一个混沌的或者拟混沌的密码。隐藏在传统密码中的一些混沌行为已被W. Schwarz等人[21]报道过。在未来研究中，关于下述问题的探索对于传统密码和混

沌密码的设计都是有益的：1) 我们是否可以使用混沌理论解释传统密码中使用的非线性函数/操作？比如，是否定义在有限域上的取模操作可以看作是一个离散化的混沌映射*？2) 我们是否可以使用混沌理论重新定义混淆和散布？我们是否可以找到一种办法将传统密码学中的安全性度量(比如流密码学中的线性复杂度)和混沌理论中的一些度量(比如信息熵)联系起来？

设计数字化混沌密码的通用模型。由于一些通用的模型已经被提出，关于这些通用模型的研究必然有助于探索混沌和密码学之间的关系。当然，新的通用结构也是需要的。

已知数字化混沌密码的分析。我们知道，现代分组密码学的进展在很大程度上是被差分分析和线性分析的出现而推动的，这充分说明了密码学中密码分析的重要性[143, 144]。我们相信任何对混沌密码的新的攻击方案都会激发混沌密码学新的进步。

*考虑在定点算法离散空间中实现的数字化tent映射。

致　　谢

本文的完成首先要归功于作者的两位导师蔡元龙教授和牟轩沁教授，是他们的悉心指导和鼓励使作者可以克服在研究中遇到的困难。作者从硕士期间就开始师从蔡元龙教授和牟轩沁教授进行科研开发工作，他们宽广的学识和丰富的实际工作经验使得作者在科研选题、工作实践中获益良多，必将受益终生。需要特别感谢的是，在本文选题阶段，是两位老师的热情鼓励和支持，才使得作者终于敢于从医学成像和智能交通监控方向大胆转向混沌加密这个课题，本文取得的所有成就，都和两位老师的鼓励、指导和建议分不开。最后值得一提的是，作者在西安交通大学图像所学习几近六载，牟轩沁教授对作者的生活给予了热情的关心和很多帮助，不仅是良师，更是益友。

特别感谢西安电子科技大学的王育民教授，在作者刚开始从事混沌密码研究的时候，得到了王育民教授在参考文献等方面的许多帮助，是这些帮助使得作者可以初入混沌密码的门庭而不致迷失方向。感谢西安交通大学的徐健学教授和黄显高博士，与他们关于混沌密码的讨论使作者在开始从事混沌密码研究的时候得到了鼓励。感谢上海交通大学的冯正进教授以及他的几位博士生周黎晖、胡国杰、崔光亮，与他们的通信帮助作者更好的理解他们在混沌密码方面的研究。

感谢香港城市大学 陈关荣 (Guanrong Chen) 教授 (Chair Professor) 把最新的有关参考文献发给作者，使作者可以将本文的工作做得更好。也感谢他邀请作者赴香港城市大学进行混沌图像/视频加密方面的博士后研究，使作者可以在这个领域继续开展更为深入细致的研究。感谢香港城市大学副教授黄国和 (K.-W. Wong) 博士，与他的通信使作者可以更好的理解文献 [123] 中提出的改进密码方案。感谢香港科技大学助教授丁存生 (Cunsheng Ding) 博士在 IndoCrypt 2001 会议上对作者文章 [22] 发表和演示给予的帮助。

感谢美国 UCSD(加州大学圣迭戈分校) 的 Goce Jakimoski，他对我们的文章[128]的审稿意见使我们认识到位抽取函数可能给M. S. Baptista密码的改进方案带来的安全隐患，并促使我们提出相关的解决办法。感谢美国 UCSD(加州大学圣迭戈分校) 的 Ljupčo Kocarev 教授，他的来信促使作者重新审视文献 [128] 对文献 [100] 的分析是否正确，并最终导致作者发现了文献 [128] 中的“概率解密”问题。感谢西班牙 Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas 的 G. Álvarez 博士将尚未出版的文章 [126] 寄给作者参考，也感谢他对作者研究的鼓励。

感谢希腊 University of Patras(佩特雷大学) 的 S. Papadimitriou 将文献 [106] 中的混沌密码的 C++ 实现代码发给作者研究，使作者可以更好的理解该混沌密码的工作方式。感谢美国 Rice University(赖斯大学) 的 Richard A. Stong 教授和 Yale University(耶鲁大学) 的 Jeb Faulkner Willenbring博士在第6章附录中证明方面给予的指导。

感谢一位匿名的审稿人指出作者在投寄到 *Int. J. Bifurcation and Chaos* 的一篇文章中忽略了关于数字化混沌系统方面的许多研究工作，感谢他指出了几篇作者没有注意到的文献(尤其是 M. Blank 的书 [172])，这使得作者可以更清晰地理解目前数字化混沌系统的研究现状，从而使得 §2.5.1 的内容更为充实系统。

还要感谢下列的研究者和朋友们及时热情地提供了作者无法(或很难)检索到的部分文献：德国 Johann Wolfgang Goethe University 的 P. E. Kloeden 教授，美国 Thomas J. Watson School of Engineering and Applied Science 的 Jiri Fridrich 教授，奥地利 Johannes Kepler Universität (JKU) Linz 的 Josef Scharinger 教授，澳大利亚 University of Wollongong 的 Reihaneh Safavi-Naini 教授和她的学生 Chandrapal Kailasanathan(博士生)、Takeyuki Uehara(博士生)，台湾(国立)东华大学助教授杨庆隆 (Ching-Nung Yang) 博士，台湾(国立)国防大学的娄德权 (Der-Chyuan Lou) 教授，美国 Duke University(杜克大学)的博士生徐义芳，新加坡国立大学的硕士生冯巍，香港大学的博士生李志，香港中文大学的博士生张志军，新加坡 Borland 公司的李进华，中国科学院自动化所的博士生张淮峰。是他们的帮助使作者可以更快地了解和掌握混沌密码、图像/视频加密方面的最新进展。感谢中国科学院声学所的博士生胡亚龙为作者在北京查询文献时提供方便的住宿和便利的上网条件。

感谢深圳大学的纪震副教授、张基宏教授、南开大学的博士生杨立波 (Boliya L. Yang) 、美国Polytechnic University(纽约理工大学)的博士生郑煊、英国 The University of Liverpool(利物浦大学)的博士生 Qi Li 和英国 Imperial College(帝国理工大学)的 Wenmin Li ，与他们的合作使作者的研究可以更加完美和严谨。感谢 Qi Li 和郑煊分别在 IMA C&C'2001 和 EI'2002 会议上代表作者做演示。

感谢作者的舍友西安交通大学的任品毅博士、张化尧博士生，感谢他们在生活中对作者给予的帮助，与他们关于科研的交谈让作者可以更好地安排科研进度和搜集整理文献。感谢复旦大学的博士生张羽 (xy@bmy)，他关于如何做科研的很多言论让作者得到了不少有益的启发，也感谢他提供的中国图书分类号大全，使得作者可以不必跑到图书馆去辛辛苦苦地扒卡片 :-) 感谢西安交通大学生命学院的博士生周永进 (BPMF@bmy) 和电气学院的博士生戴栋 (kenny@bmy)，和他们关于论文写作和投稿的讨论让作者更好地了解这方面的知识。感谢西安交通大学图象所的博士生邸双亮、樊鑫和黄华，他们的帮助也让作者可以更好的完善研究成果和了解科研常识。

感谢空军工程大学导弹学院的王小林老师、西安交通大学图象所的朱翔老师，他们在工作和生活方面对作者给予了很多帮助。也感谢图象所的其他几位老师：杜春华、齐春、赵跃进，在图象所渡过的几年时间里面，得到了他们很多的鼓励和帮助。还要感谢作者所有的师兄师弟师妹们，和他们在一起的日子，在学术上互相促进，在生活上相互帮助，他们对作者研究工作的支持、鼓励、帮助以及批评也让作者可以把工作做得更好。

另外，还要特别感谢沈向洋 (Harry Shum) 博士邀请作者作为访问学生到微软亚洲研究院(北京)进行了为期 5 个月的研究工作，在微软的研究经历使作者开阔了

眼界，增长了学识，大大提高了做研究的能力。感谢美国 CMU(卡内基・梅隆大学)的 Manuel Blum 教授，与他关于 SecHCI 的交谈使作者获益非浅。感谢在微软研究院结识的所有朋友们：孙剑、王天树、陈宏、谭平、梁林、王磊、雷蓓、冯伟、万亮、孙博、刘自强、王冬生、侯云舒、李元贞、李劲宇、徐一华、苏明、路悦，感谢他们对作者所做研究的帮助和在生活中与作者一起分享快乐。

感谢西安交通大学图象所博士生邸双亮将作者带入 TEX 这个美妙的排版世界。感谢 ChinaTEX 和 CTEX 网站所有的 CTEXer 们，没有他们的帮助作者不可能顺利地使用 TEX 完成本文漫长而要求苛刻的排版工作。感谢 IBM 中国研发中心的王天树博士制作的西安交通大学博士论文 TEX 模板，它让作者可以更快地完成西安交通大学博士论文文档类 xjtuthesis 并使用该文档类完成论文的排版工作。感谢西安交通大学科技外语系的曹扬慧和西安外国语学院的韩璐，她们帮助作者修改润色了很多英文论文，让它们在行文和逻辑上可以更完美。

最后，作者要向培育和关爱作者的父母亲表示深深的感谢，是他们的言传身教使得作者在漫长的求学道路上能够终于获得一点进步和喜悦；还要衷心感谢作者的女友，和她在一起的日子，是她的悉心照顾和关心让作者可以心无旁婺、集中精力地完成研究工作。

参考文献

[1] Jules Henri Poincaré. *New Methods of Celestial Mechanics: Part 3. Integral Invariants and Asymptotic Properties of Certain Solutions*. History of Modern Physics and Astronomy, vol. 13. Springer Verlag, 1992.

[2] A. N. Sharkovskii. Coexistence of cycles of a continuous map of a line into itself (in Russian, English summaries). *Ukrainskii Matemacheskii Zhurnal (Ukrainian Mathematical Journal)*, 16(1):61–71, 1964.

[3] Tien Yien Li and James A. Yorke. Period three implies chaos. *American Mathematical Monthly*, 82(10):985–992, 1975.

[4] David Ruelle. Strange attractor. *The Mathematical Intelligencer*, 2(1):126–137, 1980.

[5] A. N. Sharkovskii. Coexistence of cycles of a continuous map of a line into itself. *Int. J. Bifurcation and Chaos*, 5:1263–1273, 1995.

[6] Otton E. Rössler. An equation for continuous chaos. *Physics Letters A*, 57(5):397–398, 1976.

[7] M. Hénon. A two dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, 261:459–467, 1976.

[8] Mitchell J. Feigenbaum. Quantitative universality for a class of nonlinear transformations. *J. Statistical Physics*, 19(1):25–52, 1978.

[9] Robert M. May. Simple mathematical models with very complicated dynamics. *Nature*, 261:459–467, 1976.

[10] A. M. Zhabotinsky. Periodic liquid phase reactions. *Proc. Ac. Sci. USSR*, 157:392–395, 1964.

[11] A. N. Zaikin and A. M. Zhabotinsky. Concentration wave propagation in two-dimensional liquid-phase self-oscillating system. *Nature*, 225:535–537, 1970.

[12] Edward N. Lorenz. Deterministic non-periodic flow. *J. Atmospheric Sciences*, 20:130–141, 1963.

[13] Edward N. Lorenz. The predictability of hydrodynamic flow. *Trans. NY. Academy of Sciences Series II*, 25:409–432, 1963.

[14] James Gleick. *Chaos: Making a New Science*. Viking Penguin, New York, 1987.

[15] Ian Stewart. *Does God Play Dice?: The Mathematics of Chaos*. Blackwell Publishers, Oxford, UK, 1990.

[16] Edward N. Lorenz. *The Essence of Chaos*. University of Washington Press, 1993.

[17] R. Brown and L. O. Chua. Clarifying chaos: Examples and counterexamples. *Int. J. Bifurcation and Chaos*, 6(2):219–249, 1996.

[18] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation and Chaos*, 8(6):1259–1284, 1998.

[19] Ljupčo Kocarev, Goce Jakimoski, Toni Stojanovski, and Ulrich Parlitz. From chaotic maps to encryption schemes. In *Proc. IEEE Int. Symposium Circuits and Systems 98*, volume 4, pages 514–517. IEEE, 1998.

[20] G. Alvarez, F. Monotoya, G. Pastor, and M. Romera. Chaotic cryptosystems. In *Proc. IEEE Int. Carnahan Conf. Security Technology*, pages 332–338. IEEE, 1999.

[21] Marco Götz, Kristina Kelber, and Wolfgang Schwarz. Discrete-time chaotic encryption systems–Part I: Statistical design approach. *IEEE Trans. Circuits and Systems–I*, 44(10):963–970, 1997.

[22] Shujun Li, Xuanqin Mou, and Yuanlong Cai. Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. In *Progress in Cryptology – INDOCRYPT 2001*, Lecture Notes in Computer Science vol. 2247, pages 316–329. Springer-Verlag, Berlin, 2001.

[23] Andrzej Lasota and Michael C. Mackey. *Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics*. Springer-Verlag, New York, second edition, 1997.

[24] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Physical Review Letters*, 64(8):821–824, 1990.

[25] Th. Beth, D. E. Lazic, and A. Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In *Advances in Cryptology – EuroCrypt'94*, Lecture Notes in Computer Science vol. 0950, pages 318–331. Spinger-Verlag, Berlin, 1994.

[26] Kevin M. Short. Signal extraction from chaotic communications. *Int. J. Bifurcation and Chaos*, 7(7):1579–1597, 1997.

[27] Chang-Song Zhou and Tian-Lun Chen. Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. *Physics Letters A*, 234(6):429–435, 1997.

[28] Tao Yang, Lin-Bao Yang, and Chun-Mei Yang. Cryptanalyzing chaotic secure communications using return maps. *Physics Letters A*, 245(6):495–510, 1998.

[29] Maciej J. Ogorzatek and Hervé Dedieu. Some tools for attacking secure communication systems employing chaotic carriers. In *Proc. IEEE Int. Symposium Circuits and Systems 98*, volume 4, pages 522–525. IEEE, 1998.

[30] Stergios Papadimitriou, Anastasios Bezerianos, and Tassos Bounits. Radial basis function networks as chaotic generators for secure communication systems. *Int. J. Bifurcation and Chaos*, 9(1):221–232, 1999.

[31] Christopher P. Silva and Albert M. Young. Introduction to chaos-based communications and signal processing. In *Proc. IEEE Aerospace Conf.*, pages 279–299. IEEE, 2000.

[32] Andrew T. Parker and Kevin M. Short. Reconstructing the keystream from a chaotic encryption scheme. *IEEE Trans. Circuits and Systems–I*, 48(5):104–112, 2001.

[33] S. Papadimitriou, A. Bezerianos, T. Bounits, and G. Pavlides. Secure communication protocols with discrete nonlinear chaotic maps. *J. Systems Architechture*, 47(1):61–72, 2001.

[34] K. Murali, Haiyang Yu, Vinary Varadan, and Henry Leung. Secure communication using a chaos based signal encryption scheme. *IEEE Trans. Consuming Eletronics*, 47(4):709–714, 2001.

[35] Mohamed I. Sobhy and Alaa eldin R. Shehata. Chaotic algorithms for data encryption. In *2001 IEEE Int. Conf. Acoustics, Speech, and Signal Processing Proc. (ICASSP 2001)*, volume 2, pages 997–1000. IEEE, 2001.

[36] Mohamed I. Sobhy and Alaa-eldin R. Shehata. Methods of attacking chaotic encryption and countermeasures. In *2001 IEEE Int. Conf. Acoustics, Speech, and Signal Processing Proc. (ICASSP 2001)*, volume 2, pages 1001–1004. IEEE, 2001.

[37] Tung-Sheng Chiang and Peter Liu. Fuzzy model-based discrete-time chiang type chaotic cryptosystem. In *2001 IEEE Int. Conf. Fuzzy Systems Proc. (FUZZ-IEEE 2001)*, volume 3, pages 1404–1407. IEEE, 2001.

[38] Tung-Sheng Chiang, Chun-Chieh Wang, and Ching-Tsan Chiang. Robust t-s fuzzy model-based for chaotic cryptosystem. In *Proc. 2002 IEEE Int. Conf. Fuzzy Systems(FUZZ-IEEE'02)*, volume 1, pages 290–295. IEEE, 2002.

[39] Carlos Aguilar Ibáñez Hebert Sira-Ramírez and Miguel Suárez-Casta nón. Exact state reconstructors in the recovery of messages encrypted by the states of nonlinear discrete-time chaotic systems. *Int. J. Bifurcation and Chaos*, 12(1):169–177, 2002.

[40] Guojie Hu, Zhengjin Feng, and Ruiling Meng. Chosen ciphertext attack on chaos communication based on chaotic synchronization. *IEEE Trans. Circuits and Systems–I*, 50(2):275–279, 2003.

[41] Vladimir S. Udaltsov, Jean-Pierre Goedgebuer, Laurent Larger, Jean-Baptiste Cuenot, Pascal Levy, and William T. Rhodes. Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations. *Physics Letters A*, 308(1):54–60, 2003.

[42] Roy Tenny, Lev S. Tsimring, Larry Larson, and Henry D. I. Abarbanel. Using distributed nonlinear dunamics for public key encryption. *Physical Review Letters*, 90(4):047903, 2003.

[43] P. G. Vaidya and Savita Angadi. Decoding chaotic cryptography without access to the superkey. *Chaos, Solitons and Fractals*, 17(2-3):379–386, 2003.

[44] Stephen Wolfram. Cryptography with cellular automata. In *Advances in Cryptology - Crypto'85*, Lecture Notes in Computer Science vol. 0218, pages 429–432. Spinger-Verlag, Berlin, 1985.

[45] Puhua Guan. Cellular automaton public-key cryptosystem. *Complex Systems*, 1:51–57, 1987.

[46] J.-P. Delahaye. Les automates (in French). *Pour la Science (French Edition of Scientific American)*, pages 126–134, Nov. 1991.

[47] H. A. Gutowitz. Cryptography with dynamical systems. In *Cellular Automata and Cooperative Phenomena*, Kluwer Academic Press, 1993.

[48] H. A. Gutowitz. Method and apparatus for encryption, decryption, and authentication using dynamical systems. US Patent No. 5365589, 1994.

[49] S. Nandi, B. K. Kar, and P. P. Chaudhuri. Theory and application of cellular automata in cryptography. *IEEE Trans. Computers*, 43(12):1346–1357, 1994.

[50] S. R. Blackburn, S. Murphy, K. G. P. I. S. Group, and R. Holloway. Comments on "theory and application of cellular automata in cryptography". *IEEE Trans. Computers*, 46(5):637–638, 1997.

[51] S. Nandi and P. Pal Chaudhuri. Reply to comments on "theory and application of cellular automata in cryptography". *IEEE Trans. Computers*, 46(5):639, 1997.

[52] Jesús Uís, Edgardo Ugalde, and Gelasio Salazar. A cryptosystem based on cellular automata. *Chaos*, 8(4):819–822, 1998.

[53] N. Ganguly, A. Das, B. K. Sikdar, and P. P. Chaudhuri. Cellular automata model for cryptosystem. In *Proc. Cellular Automata Conference*, Yakohama National University, Japan, 2001.

[54] Subhayan Sen, Chandrama Shaw, Dipanwita Roy Chowdhuri, Niloy Ganguly, and P. Pal Chaudhuri. Cellular automata based cryptosystem (CAC). In *Information and Communications Security - 4th International Conference ICICS 2002 Proceedings*, Lecture Notes in Computer Science vol. 2513, pages 303–314. Spinger-Verlag, Berlin, 2002.

[55] Robert A. J. Matthews. On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, XIII(1):29–42, 1989.

[56] Daniel D. Wheeler. Problems with chaotic cryptosystems. *Cryptologia*, XIII(3):243–250, 1989.

[57] Douglas W. Mitchell. Nonlinear key generators. *Cryptologia*, XIV(4):350–354, 1990.

[58] G. M. Bernstein and M. A. Lieberman. Secure random number generation using chaotic circuits. *IEEE Trans. Circuits and Systems*, 37(9):1157–1164, 1990.

[59] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori. A secret key cryptosystem using a chaotic map. *Trans. IEICE*, E 73(7):1041–1044, 1990.

[60] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori. A secret key cryptosystem by iterating a chaotic map. In *Advances in Cryptology – EuroCrypt'91*, Lecture Notes in Computer Science vol. 0547, pages 127–140. Spinger-Verlag, Berlin, 1991.

[61] Daniel D. Wheeler and Robert A. J. Matthews. Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia*, XV(2):140–151, 1991.

[62] Daniel D. Wheeler. Problems with Mitchell's nonlinear key generators. *Cryptologia*, XV(4):355–151, 1991.

[63] E. Biham. Cryptoanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91. In *Advances in Cryptology – EuroCrypt'91*, Lecture Notes in Computer Science vol. 0547, pages 532–534. Spinger-Verlag, Berlin, 1991.

[64] R. Forré. The Hénon attractor as a keystream generator. In *Abstract of EuroCrypt'91 (wrong?)*, pages 76–80, 1991. (This paper is cited in [67] with wrong source).

[65] G. M. Berstein and M. A. Lieberman. Method and apparatus for generating secure random numbers using chaos. US Patent No. 5007087, 1991.

[66] M. E. Bianco and D. A. Reed. Encryption system based on chaos theory. US Patent No. 5048086, 1991.

[67] D. Erdmann and S. Murphy. Hénon stream cipher. *Electronics Letters*, 28(9):893–895, 1992.

[68] Ross Anderson. Letter to the editor: Chaos and random numbers. *Cryptologia*, XVI(3):226, 1992.

[69] Fengi Hwu. *The Interpolating Random Spline Cryptosystem and the Chaotic-Map Public-Key Cryptosystem*. PhD thesis, Faculty of the Graduate School, University of Missouri - Rolla, 1993.

[70] D. R. Frey. Chaotic digital encoding: An approach to secure communication. *IEEE Trans. Circuits and Systems–II*, 40(10):660–666, 1993.

[71] V. A. Protopopescu, R. T. Santoro, and J. S. Tollover. Fast and secure encryption – decryption method based on chaotic dynamics. US Patent No. 5479513, 1995.

[72] Tohru Kohda and Akio Tsuneda. Chaotic bit sequences for stream cipher cryptography and their correlation functions. In *Chaotic Circuits for Communication*, Proceedings of SPIE vol. 2612, pages 86–97, 1995.

[73] Ute Feldmann, Martin Hasler, and Wolfgang Schwarz. Communication by chaotic signals: The inverse system approach. *Int. J. Circuit Theory and Applications*, 24(5):551–579, 1996.

[74] 周红. 一类混沌密码序列的设计方法及其有限精度实现问题分析. 博士学位论文, 复旦大学电子工程系, 中国上海, 1996年6月.

[75] Hong Zhou and Xie-Ting Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits and Systems–I*, 44(3):268–271, 1997.

[76] Hong Zhou, Xie-Ting Ling, and Jie Yu. Secure communication via one-dimensional chaotic inverse systems. In *Proc. IEEE Int. Symposium Circuits and Systems 97*, volume 2, pages 9–12. IEEE, 1997.

[77] 周红, 罗杰, 凌燮亭. 混沌非线性反馈密码序列的理论设计和有限精度实现. 电子学报, 25(10):57–60(+56), 1997.

[78] Hong Zhou and Xieting Ling. Generating chaotic secure sequences with desired statistical properties and high security. *Int. J. Bifurcation and Chaos*, 7(1):205–213, 1997.

[79] Zbigniew Kotulski and Janusz Szczepanski. Discrete chaotic cryptography. *Annalen der Physik*, 6(5):381–394, 1997.

[80] Tao Sang, Ruili Wang, and Yixun Yan. Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters*, 34(9):873–874, 1998.

[81] Tao Sang, Ruili Wang, and Yixun Yan. Clock-controlled chaotic keystream generators. *Electronics Letters*, 34(20):1932–1934, 1998.

[82] 周红, 俞军, 凌燮亭. 混沌前馈型流密码的设计. 电子学报, 26(1):98–101, 1998.

[83] Frank Dachselt, Kristina Kelber, and Wolfgang Schwarz. Discrete-time chaotic encryption systems–Part III: Cryptographical analysis. *IEEE Trans. Circuits and Systems–I*, 45(9):983–988, 1998.

[84] M. S. Baptista. Cryptography with chaos. *Physics Letters A*, 240(1-2):50–54, 1998.

[85] Josef Scharinger. Fast encryption of image data using chaotic kolmogrov flows. *J. Electronic Imaging*, 7(2):318–325, 1998.

[86] Christopher F. Woodcock and Nigel P. Smart. *p*-adic chaos and random number generation. *Experimental Mathematics*, 7(4):333–342, 1998.

[87] Donghui Guo, L. M. Cheng, and L. L. Cheng. A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks. *Applied Intelligence*, 10(1):71–84, 1999.

[88] W. G. Chambers. Comments on "Chaotic digital encoding: An approach to secure communication". *IEEE Trans. Circuits and Systems–II*, 46(11):1445–1447, 1999.

[89] Masaki Miyamoto, Kiyoshi Tanaka, and Tatsuo Sugimura. Truncated baker transformation and its extension to image encryption. In *Mathematics of Data/Image Coding, Compression, and Encryption II*, Proceedings of SPIE vol. 3814, pages 13–25, 1999.

[90] E. Alvarez, A. Fernández, P. García, J. Jiménez, and A. Marcano. New approach to chaotic encryption. *Physics Letters A*, 263(4-6):373–375, 1999.

[91] Zbigniew Kotulski and Janusz Szczepanski. Application of discrete chaotic dynamical systems in cryptography – DCC method. *Int. J. Bifurcation and Chaos*, 9(6):1121–1135, 1999.

[92] 桑涛, 王汝笠, 严义埙. 一类新型混沌反馈密码序列的理论设计. 电子学报, 27(7):47–50, 1999.

[93] Toru Ohira. Encryption with delayed dynamics. *Physics Letters A*, 121-122:75–82, 1999.

[94] 郭东辉, 何小娟, 陈彩生. 基于神经网络混沌加密算法的专用芯片设计. 计算机学报, 23(11):1230–1232, 2000.

[95] F. Argenti, S. Benzi, E. Del Re, and R. Genesio. Stream cipher system based on chaotic maps. In *Mathematics and Applications of Data/Image Coding, Compression, and Encryption III*, Proceedings of SPIE vol. 4122, pages 10–17, 2001.

[96] Mieczysław Jessa. Data encryption algorithms using one-dimensional chaotic maps. In *Proc. IEEE Int. Symposium Circuits and Systems 2000*, volume I, pages 711–714. IEEE, 2000.

[97] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a chaotic encryption system. *Physics Letters A*, 276(1-4):191–196, 2000.

[98] Li-Hui Zhou and Zheng-Jin Feng. A new idea of using one-dimensional PWL map in digital secure communications–dual-resolution approach. *IEEE Trans. Circuits and Systems–II*, 47(10):1107–1111, 2000.

[99] Ninan Sajeeth Philip and K. Babu Joseph. Chaos for stream cipher. arXiv:nLin.CD/0102012 v1, 16 Feb. 2001, available online at http://arxiv.org/abs/cs.CR/0102012.

[100] Goce Jakimoski and Ljupčo Kocarev. Analysis of some recently proposed chaos-based encryption algorithms. *Physics Letters A*, 291(6):381–384, 2001.

[101] Ljupčo Kocarev. Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Maganize*, 1(3):6–21, 2001.

[102] Frank Dachselt and Wolfgang Schwarz. Chaos and cryptography. *IEEE Trans. Circuits and Systems–I*, 48(12):1498–1509, 2001.

[103] Roland Schmitz. Use of chaotic dynamical systems in cryptography. *J. Franklin Institute*, 338(4):429–441, 2001.

[104] Wai-Kit Wong, Lap-Piu Lee, and Kwok-Wo Wong. A modified chaotic cryptographic method. *Computer Physics Communications*, 138(3):234–236, 2001.

[105] Ljupčo Kocarev and Goce Jakimoski. Logistic map as a block encryption algorithm. *Physics Letters A*, 289(4-5):199–206, 2001.

[106] Stergios Papadimitriou, Tassos Bountis, Seferina Mavaroudi, and Anastassions Bezerianos. A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations. *Int. J. Bifurcation and Chaos*, 11(12):3107–3115, 2001.

[107] Naoki Masudo and Kazuyuki Aihara. Cryptosystems based on space-discretization of chaotic maps. In *Proc. IEEE Int. Symposium Circuits and Systems 2001*, volume III, pages 321–324. IEEE, 2001.

[108] Goce Jakimoski and Ljupčo Kocarev. Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits and Systems–I*, 48(2):163–169, 2001.

[109] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In *Cryptography and Coding – 8th IMA Int. Conf. Proc.*, Lecture Notes in Computer Science vol. 2260, pages 205–221. Springer-Verlag, Berlin, 2001.

[110] Shujun Li, Xuanqin Mou, and Yuanlong Cai. Improving security of a chaotic encryption approach. *Physics Letters A*, 290(3-4):127–133, 2001.

[111] GuoJie Hu, ZhengJin Feng, and Lin Wang. Analysis of a type digital chaotic cryptosystem. In *Proc. IEEE Int. Symposium Circuits and Systems 2002*, volume III, pages 473–475. IEEE, 2002.

[112] Shujun Li, Xuan Zheng, Xuanqin Mou, and Yuanlong Cai. Chaotic encryption scheme for real-time digital video. In *Real-Time Imaging VI*, Proceedings of SPIE vol. 4666, pages 149–160, 2002.

[113] A. Palacios and H. Juarez. Cryptography with cycling chaos. *Physics Letters A*, 303(5-6):345–351, 2002.

[114] Kwok-Wo Wong. A fast chaotic cryptographic scheme with dynamic look-up table. *Physics Letters A*, 298(4):238–242, 2002.

[115] P. García, A. Parravano, M. G. Cosenza, J. Jiménez, and A. Marcano. Coupled map networks as communication schemes. *Physical Review E*, 65(4):045201(R), 2002.

[116] P. García and J. Jiménez. Communication through chaotic map systems. *Physics Letters A*, 298(1):34–40, 2002.

[117] Naoki Masuda and Kazuyuki Aihara. Cryptosystems with discretized chaotic maps. *IEEE Trans. Circuits and Systems–I*, 49(1):28–40, 2002.

[118] Xun Yi, Chik How Tan, and Chee Kheong Siew. A new block cipher based on chaotic tent maps. *IEEE Trans. Circuits and Systems–I*, 49(12):1826–1829, 2002.

[119] Shihong Wang, Jinyu Kuang, Jinghua Li, Yunlun Luo, Huaping Lu, and Gang Hu. Chaos-based secure communications in a large community. *Physical Review E*, 66(6):065202(R), 2002.

[120] Mieczysław Jessa. Data transmission with adjustable security exploiting chaos-based pseudorandom number generators. In *Proc. IEEE Int. Symposium Circuits and Systems 2002*, volume III, pages 476–479. IEEE, 2002.

[121] Goce Jakimoski and Ljupčo Kocarev. Differenytial and linear probabilities of a block-encryption cipher. *IEEE Trans. Circuits and Systems–I*, 50(1):121–123, 2003.

[122] Kwok-Wo Wong. A combined chaotic cryptographic and hashing scheme. *Physics Letters A*, 307(5-6):292–298, 2003.

[123] Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung. A chaotic cryptography scheme for generating short ciphertext. *Physics Letters A*, 310(1):67–73, 2003.

[124] Shihong Wang, Weiping Ye, Huaping Lu, Jinyu Kuang, Jinghua Li, Yunlun Luo, and Gang Hu. A spatiotemporal-chaos-based encryption having overall properties considerably better than advanced encryption standard. arXiv:nLin.CD/0303026 v1, 14 Mar. 2003, available online at http://arxiv.org/abs/nlin.CD/0303026.

[125] N. K. Pareek, Vinod Patidar, and K. K. Sud. Discrete chaotic cryptography using external key. *Physics Letters A*, 309(1-2):75–82, 2003.

[126] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of an ergodic chaotic cipher. *Physics Letters A*, 311(2-3):172–179, 2003.

[127] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Crytpanalysis of a chaotic secure communication system. *Physics Letters A*, 306(4):200–205, 2003.

[128] Shujun Li, Xuanqin Mou, Zhen Ji, Jihong Zhang, and Yuanlong Cai. Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems. *Physics Letters A*, 307(1):22–28, 2003.

[129] Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision. *Computer Physics Communications*, 153(1):52–58, 2003.

[130] Shujun Li, Xuanqin Mou, Boliya L. Yang, Zhen Ji, and Jihong Zhang. Problems with a probabilistic encryption scheme based on chaotic systems. *Int. J. Bifurcation and Chaos*, 13(10):3063–3077, 2003.

[131] Shujun Li, Xuanqin Mou, Luhua Gong, and Yuanlong Cai. On the security of a chaotic cipher to Biham's attacks. unpublished, 2002.

[132] Jui-Cheng Yen and Jiun-In Guo. A new image encryption algorithm and its VLSI architecture. In *Proc. IEEE Workshop Signal Processing Systems*, pages 430–437, 1999.

[133] Scott Su, Alvin Lin, and Jui-Cheng Yen. Design and realization of a new chaotic neural encryption/decryption network. In *Proc. 2000 IEEE Asia-Pacific Conf. Circuits and Systems (APCCAS 2000)*, pages 335–338. IEEE, 2000.

[134] Jui-Cheng Yen and Jiun-In Guo. A new chaotic key-based design for image encryption and decryption. In *Proc. IEEE Int. Symposium Circuits and Systems 2000*, volume 4, pages 49–52, 2000.

[135] Jui-Cheng Yen and Jiun-In Guo. Efficient hierarchical chaotic image encryption algorithm and its vlsi realisation. *IEE Proc.-Vis. Image Signal Process.*, 147(2):167–175, 2000.

[136] Kenji Yano and Kiyoshi Tanaka. Image encryption scheme based on a truncated baker transformation. *IEICE Trans. Fundamentals*, E85-A(9):2025–2035, 2002.

[137] Jui-Cheng Yen and Jiun-In Guo. Design of a new signal security system. In *Proc. IEEE Int. Symposium Circuits and Systems 2002*, volume IV, pages 121–124. IEEE, 2002.

[138] Jiun-In Guo, Jui-Cheng Yen, and H.-F. Pan. New voice over Internet protocol technique with hierarchical data security protection. *IEE Proc.-Vis. Image Signal Process.*, 149(4):237–243, 2002.

[139] Shujun Li and Xuan Zheng. Cryptanalysis of a chaotic image encryption method. In *2002 IEEE Int. Sym. Circuits and Systems Proc. (ISCAS 2002)*, pages 708–711, 2002.

[140] Shujun Li and Xuan Zheng. On the security of an image encryption method. In *Proc. 2002 Int. Conf. Image Processing (ICIP 2002)*, volume 2, pages 925–928, 2002.

[141] 李树钧, 牟轩沁, 纪震, 张基宏. 一类混沌流密码的分析. 电子与信息学报, 25(4):473–478, 2003.

[142] C. E. Shanon. Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28(4):656–715, 1949.

[143] Bruce Schneier. *Applied Cryptography – Protocols, algorithms, and souce code in C*. John Wiley & Sons, Inc., New York, second edition, 1996.

[144] 王育民, 刘建伟. 通信网的安全－理论与技术. 西安电子科技大学出版社, 中国西安, 1999.

[145] B. V. Chirkikov and F. Vivaldi. An algorithmic view of pseudochaos. *Physica D*, 129(3-4):223–235, 1999.

[146] 纪震. 医用*DSA*系统的关键技术研究. 博士学位论文, 西安交通大学电子与信息工程学院, 中国西安, 1999年3月.

[147] Shin'ichi Oishi and Hajime Inoue. Pseudo-random number generators and chaos. *Trans. IECE Japan*, E 65(9):534–541, 1982.

[148] F. James. A review of pseudorandom number generators. *Computer Physics Communications*, 60(3):329–344, 1990.

[149] Ghobad Heidari-Bateni and Clare D. McGillem. A chaotic direct-sequence spread-spectrum communication system. *IEEE Trans. Communications*, 42(2/3/4):1524–1527, 1994.

[150] S. C. Phatak and S. Suresh Rao. Logistic map: A possible random-number generator. *Physical Review E*, 51(4):3670–3678, 1995.

[151] Tohru Kohda and Akio Tsuneda. Statistics of chaotic binary sequences. *IEEE Trans. Information Theory*, 43(1):104–112, 1997.

[152] Gianluca Mazzini, Gianluca Setti, and Riccardo Rovatti. Chaotic complex spreading spectrum sequences for asynchronous DS-CDMA–Part I: System modeling and results. *IEEE Trans. Circuits and Systems–I*, 44(10):937–947, 1997.

[153] Riccardo Rovatti, Gianluca Mazzini, and Gianluca Setti. Chaotic complex spreading spectrum sequences for asynchronous DS-CDMA–Part II: Some theoretical performance bounds. *IEEE Trans. Circuits and Systems–I*, 45(4):496–506, 1998.

[154] Jorge A. González and Ramiro Pino. A random number generator based on unpredictable chaotic functions. *Computer Physics Communications*, 120(2-3):109–114, 1999.

[155] Jorge A. Gonzalez, Miguel Martin-Landrove, and Leonardo Trujillo. Absolutely unpredictable chaotic sequences. *Int. J. Bifurcation and Chaos*, 10(8):1867–1874, 2000.

[156] Ling Cong and Li Shaoqian. Chaotic spreading sequences with multiple access performance better than random sequences. *IEEE Trans. Circuits and Systems–I*, 47(3):394–397, 2000.

[157] Agner Fog. Chaotic random number generators with random cycle lengths. downloadable at http://www.agner.org/random/theory/chaosran.doc, Nov. 2001.

[158] R. Bernardini and G. Cortelazzo. Tools for designing chaotic systems for secure random number generation. *IEEE Trans. Circuits and Systems–I*, 48(5):552–564, 2001.

[159] Janusz Szczepański and Zbigniew Kotulski. Pseudorandom number generators based on chaotic dynamical systems. *Open Sys. & Information Dyn.*, 8(2):137–146, 2001.

[160] Toni Stojanovski and Ljupčo Kocarev. Chaos-based random number generators–Part I: Analysis. *IEEE Trans. Circuits and Systems–I*, 48(3):281–288, 2001.

[161] Toni Stojanovski, Johnny Pihl, and Ljupčo Kocarev. Chaos-based random number generators–Part II: Practical realization. *IEEE Trans. Circuits and Systems–I*, 48(3):382–385, 2001.

[162] M. Jessa. The period of sequences generated by tent-like maps. *IEEE Trans. Circuits and Systems–I*, 49(1):84–89, 2002.

[163] Mieczysław Jessa and Marcin Walentynowicz. Discrete-time phase-locked loop as a source of random sequences with different distributions. In *Proc. IEEE Int. Symposium Circuits and Systems 2002*, volume III, pages 189–192. IEEE, 2002.

[164] Ljupčo Kocarev and Goce Jakimoski. Pseudorandom bits generated by chaotic maps. *IEEE Trans. Circuits and Systems–I*, 50(1):123–126, 2003.

[165] Hongtao Zhang, Huiyun Wang, and Wai-Kai Chen. Oversampled chaotic binary sequences with good security. *J. Circuits, Systems and Computers*, 11(2):173–185, 2002.

[166] IEEE Computer Society. Advanced encryption standard (AES). Federal Information Processing Standards Publication 197 (FIPS-197), downloadable at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, November 2001.

[167] Terry Ritter. Substitution cipher with pseudo-random shuffling: The dynamic substitution combiner. *Cryptologia*, XIV(4):289–303, 1990.

[168] Terry Ritter. Transposition cipher with pseudo-random shuffling: The dynamic transposition combiner. *Cryptologia*, XV(1):1–17, 1991.

[169] Donald E. Knuth. *The Art of Computer Programing Volume 2: Seminumerical Algorithms*. Addison-Wesley, third edition, 1998.

[170] 周红, 凌燮亭. 有限精度混沌系统的m序列扰动实现. 电子学报, 25(7):95–97, 1997.

[171] Naoki Masuda and Kazuyuki Aihara. Dynamical characterstics of discretized chaotic permutations. *Int. J. Bifurcation and Chaos*, 12(10):2087–2103, 2002.

[172] Michael Blank. *Discreteness and Continuity in Problems of Chaotic Dynamics*, volume 161 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, Rhode Island, 1997.

[173] Y. E. Levy. Some remarks about computer studies of dynamical systems. *Physics Letters A*, 88(1):1–3, 1982.

[174] F. Rannou. Numerical study of discrete plane area-preserving mappings. *Astronomy and Astrophysics*, 31:289–301, 1974.

[175] G. Benettin, M. Casartelli, L. Galgani, A. Giorgilli, and J.-M. Strekcyn. On the reliability of numerical studies of stochasticity I: Exsitence of time average. *IL Nuovo Cimento B*, 44(1):183–195, 1978.

[176] Charles F. F. Karney. Long-time correlations in the stochastic regime. *Physica D*, 8(3):360–380, 1983.

[177] T. Hogg and B. A. Huberman. Attractors on finite sets: The dissipative dynamics of computing structures. *Physical Review A*, 32(4):2338–2346, 1985.

[178] W. F. Wolffand B. A. Huberman. Transients and asymptotics in granular phase space. *Zeitschrift für Physik B - Condensed Matter*, 63:397–405, 1986.

[179] P. M. Binder and R. V. Jensen. Simulating chaotic behavior with finite-state machines. *Physical Review A*, 34:4460–4463, 1986.

[180] Joseph L. McCauley Jr. and Julian I. Palmore. Computable chaotic orbits. *Physics Letters A*, 115(9):433–436, 1986.

[181] Julian I. Palmore and Joseph L. McCauley. Shadowing by computable chaotic orbits. *Physics Letters A*, 122(8):399–402, 1987.

[182] lam Percival and Franco Vivaldi. Arithmetical properties of strongly chaotic maps. *Physica D*, 25(1-3):105–130, 1987.

[183] C. Beck and G. Roepstorff. Effects of phase space discretization on the long-time behavior of dynamical systems. *Physica D*, 25(1-3):95–97, 1987.

[184] Kunihiko Kaneko. Symplectic cellular automata. *Physics Letters A*, 129(1):9–16, 1988.

[185] Celso Grebogi, Edward Ott, and James A. Yorke. Roundoff-induced periodicity and the correlation dimension of chaotic attractors. *Physical Review A*, 38(7):3688–3692, 1988.

[186] P. Góra and A. Boyarsku. Why computers like Lebesgue measure. *Computers & Mathematics with Applications*, 16(4):321–329, 1988.

[187] E. Thiran, D. Verstegen, and J. Weyers. *p*-adic dynamics. *J. Statistical Physics*, 54(3-4):893–913, 1989.

[188] Julian Palmore and Charles Herring. Computer arithmetic, chaos and fractals. *Physica D*, 42(1-3):99–110, 1990.

[189] J. P. Keating. Asmptoic properties of the periodic orbits of the cat maps. *Nonlinearity*, 4(2):277–307, 1991.

[190] Slawomir T. Fryska and Mohamed A. Zohdy. Computer dynamics and shadowing of chaotic orbits. *Physics Letters A*, 166(5-6):340–346, 1992.

[191] P.-M. Binder. Limit cycles in a quadratic discrete iteration. *Physica D*, 57(1-2):31–38, 1992.

[192] David J. D. Earn and Scott Tremaine. Exact numerical studies of hamiltonian maps: Iterating without roundoff error. *Physica D*, 56(1):1–22, 1992.

[193] P. H. Borcherds and G. P. McCauley. The digital tent map and the trapezoidal map. *Chaos, Solitons & Fractals*, 3(4):451–466, 1993.

[194] P. Diamond, P. Kloeden, and A. Pokrovskii. An invariant measure arising in computer simulation of a chaotic dynamical system. *Journal of Nonlinear Science*, 4:59–68, 1994.

[195] Michael Blank. Pathologies generated by round-off in dynamical systems. *Physica D*, 78(1-2):93–114, 1994.

[196] F. Vivaldi. Periodicity and transport from round-off errors. *Experimental Mathematics*, 3(4):303–315, 1994.

[197] David K. Arrowsmith and F. Vivaldi. Geometry of p-adic Siegel discs. *Physica D*, 71(1-2):222–236, 1994.

[198] P. Diamond, P. Kloeden, A. Pokrovskii, and A. Vladimirov. Collapsing effects in numerical simulation o a class of chaotic dynamical systems and random mappings with a single attracting centre. *Physica D*, 86(4):559–571, 1995.

[199] J. Čermák. Digital generators of chaos. *Physics Letters A*, 214(3-4):151–160, 1996.

[200] J. H. Lowenstein and F. Vivaldi. Anomalous trasport in a model of Hamiltonian round-off. *Nonlinearity*, 11(5):1321–1350, 1998.

[201] Xu-Sheng Zhang and F. Vivaldi. Small perturbations of a discrete twist map. *Physique Theorique*, 68(4):507–523, 1998.

[202] Henri Waelbroeck and Federico Zertuche. Discrete chaos. *J. Physics A*, 32(1):175–189, 1999.

[203] A. V. Pokrovskii, A. Kent, and J. McInerney. Mixed moments of random mappings and chaotic dynamical systems. Technical Report Report 99-003, Institute for Nonlinear Science (INS) at UCC, University College, Cork, Ireland, March 1999.

[204] W. G. Chambers. Orbit-periods in second-order finite-precision digital filters with overflow. *Int. J. Bifurcation and Chaos*, 9(8):1669–1674, 1999.

[205] D. Bosioand and F. Vivaldi. Round-off errors and p-adic numbers. *Nonlinearity*, 13(1):309–322, 2000.

[206] Francois Robert. *Discrete Iterations: A Metric Study*. Springer Series in Computational Mathematics vol. 6. Springer-Verlag, Berlin, 1986.

[207] 郑维敏. 正反馈. 清华大学出版社, 中国北京, 1998.

[208] 郝柏林. 从抛物线谈起：混沌动力学引论. 上海科技教育出版社, 中国上海, 1993.

[209] A. Baranovsky and D. Daems. Design of one-dimensional chaotic maps with prescribed statistical properties. *Int. J. Bifurcation and Chaos*, 5(6):1585–1598, 1995.

[210] 陈式刚. 映象与混沌. 国防工业出版社, 中国北京, 1992.

[211] 胡冠章. 应用近世代数. 清华大学出版社, 中国北京, 第二版, 1999.

[212] 《现代应用数学手册》编委会. 现代应用数学手册：概率论与随机过程卷. 清华大学出版社, 中国北京, 2000.

[213] 丁存生, 肖国镇. 流密码学及其应用. 国防工业出版社, 中国北京, 1994.

[214] 肖国镇, 王育民. 伪随机序列及其应用. 国防工业出版社, 中国北京, 1985.

[215] 陈士华, 陆君安. 混沌动力学初步. 武汉水力水电大学出版社, 中国武汉, 1998.

[216] Kenneth R. Castleman. *Digital Image Processing*. Prentice Hall Inc., New York, 1996.

[217] IEEE Computer Society. IEEE standard for binary floating-point arithmetic. ANSI/IEEE Std. 754-1985, August 1985.

[218] Doug Stinson. Visual cryptography & threshold schemes. *Dr. Dobb's J. Software Tools for Professional Programmer*, 23(4):36, 38–43, April 1998.

[219] Stergios Papadimitriou, Anastasios Bezerianos, and Tassos Bounits. Secure communication with chaotic systems of difference equations. *IEEE Trans. Computers*, 46(1):27–38, 1997.

[220] 杨振生. 组合数学及其算法. 中国科技大学出版社, 中国合肥, 1997.

[221] Howard Cheng and Xiaobo Li. Partial encryption of compressed images and videos. *IEEE Trans. Signal Processing*, 48(8):2439–2451, 2000.

[222] Philip P. Dang and Paul M. Chau. Image encryption for secure internet multimedia applications. *IEEE Trans. Consumer Electronics*, 46(3):395–403, 2000.

[223] Henry Ker-Chang Chang and Jiang-Long Liu. A linear quadtree compression scheme for image encryption. *Signal Processing: Image Communication*, 10(4):279–290, 1997.

[224] C. Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou. Image encrytion method using a class of fractals. *J. Electronic Imaging*, 4(3):251–259, 1995.

[225] N. Bourbakis and C. Alexopoulos. Picture data encryption using scan patterns. *Pattern Recognition*, 25(6):567–581, 1992.

[226] Jinn-Ke Jan and Yuh-Min Tseng. On the security of image encryption method. *Information Processing Letters*, 60(5):261–265, 1996.

[227] 杨义先, 林须端. 编码密码学. 人民邮电出版社, 中国北京, 1992.

[228] Ali Şaman Tosun. Lightweight security mechanisms for wireless video transmission. In *Proc. Int. Conf. Information Technology*, pages 157–161, 2001.

[229] Sang Uk Shin, Kyeong Seop Sim, and Kyung Hyune Rhee. A secrecy scheme for MPEG video data using the joint of compression and encryption. In *Proc. Int. Information Security Workshop*, Lecture Notes in Computer Science **1729**, pages 191–201, Berlin, 1999. Springer-Verlag.

[230] Lintian Qiao and Klara Nahrstedt. A new algorithm for MPEG video encryption. In *Proc. Int. Conf. Imaging Science, Systems, and Technology*, pages 21–29, 1997.

[231] Xiaolin Wu and Peter W. Moo. Joint image/video compression and encryption via high-order conditional entropy coding of wavelet coefficients. In *Proc. Int. Conf. Multimedia Computing and Systems*, pages 908–912, 1999.

[232] Changgui Shi, Sheng-Yih Wang, and Bharat Bhargava. MPEG video encryption in real-time using secret key cryptography. In *Proc. Int. Conf. Parallel and Distributed Processing Techniques and Applications*, 1999.

[233] Changgui Shi and Bharat Bhargava. A fast MPEG video encryption algorithm. In *Proc. ACM Multimedia 98*, pages 81–88, 1998.

[234] Lei Tang. Methods for encrypting and decrypting MPEG video data efficiently. In *Proc. ACM Multimedia 96*, pages 219–230, 1996.

[235] Iskender Agi and Li Gong. An empirical study of secure MPEG video transmissions. In *Proc. Internet Society Sym. Network and Distributed Systems Security*, pages 137–144, 1996.

[236] Yongcheng Li, Zhigang Chen, See-Mong Tan, and Roy H. Campbell. Security enhanced MPEG player. In *Proc. Int. Workshop Multimedia Software Development*, pages 169–175, 1996.

[237] George Anastasios Spanos and Tracy Bradley Maples. Performance study of a selective encryption scheme for the security of networked, real-time video. In *Proc. Int. Conf. Computer Communications and Networks*, pages 2–10, 1995.

[238] Lintian Qiao and Klara Nahrstedt. Comparison of MPEG encryption algorithms. *Computers & Graphics*, 22(4):437–448, 1998.

[239] Lintian Qiao, Klara Nahrstedt, and Ming-Chit Tam. Is MPEG encryption by using random list instead of Zig-Zag order secure? In *Proc. Int. Sym. Consumer Electronics*, pages 226–229, 1997.

[240] Takeyuki Uehara and Reihaneh Safavi-Naini. Chosen DCT coefficients attack on MPEG encryption schemes. In *Proc. IEEE Pacific Rim Conf. Multimedia*, pages 316–319, 2000.

[241] Thomas Sikora. MPEG digital video-coding standards. *IEEE Signal Processing Maganize*, 14(5):82–100, 1997.

[242] Tohru Kohda and Kazuyuki Aihara. Chaos in discrete systems and diagnosis of experimental chaos. *Trans. IEICE*, E 73(6):772–783, 1990.

攻读博士期间发表相关文章列表

[1] **Shujun Li**, Xuanqin Mou, and Yuanlong Cai. Improving security of a chaotic encryption approach. *Physics Letters A*, 290(3-4):127–133, 2001. (**SCI** indexed, IDS Number: 495EE).

[2] **Li Shujun**, Mou Xuanqin, and Cai Yuanlong. Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. In *Progress in Cryptology - INDOCRYPT 2001*, Lecture Notes in Computer Science vol. 2247, pages 316–329. Springer-Verlag, Dec. 2001. (**SCI Expanded** Source).

[3] **Shujun Li**, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In *Cryptography and Coding–8th IMA International Conference Proceedings*, Lecture Notes in Computer Science vol. 2260, pages 205–221. Springer-Verlag, Dec. 2001. (**SCI Expanded** Source).

[4] **Shujun Li**, Xuan Zheng, Xuanqin Mou, and Yuanlong Cai. Chaotic encryption scheme for real-time digital video. In *Real-Time Imaging VI*, Proceedings of SPIE vol. 4666, pages 149–160, 2002. (**EI** indexed, AN: 7203934, New AN: 02467203934; **ISTP** indexed, IDS Number: BU44J).

[5] **Shujun Li** and Xuan Zheng. Cryptanalysis of a chaotic image encryption method. In *Proceedings of 2002 IEEE International Symposium on Circuits and Systems (ISCAS 2002)*, pages 708–711, 2002. (**EI** indexed, AN: 7011208, New AN: 02287011208).

[6] **Shujun Li** and Xuan Zheng. On the security of an image encryption method. In *Proceedings of 2002 IEEE International Conference on Image Processing (ICIP 2002)*, volume 2, pages 925–928, 2002. (**EI** indexed, AN: 7288882, New AN: 02517288882).

[7] **Shujun Li**, Xuanqin Mou, Zhen Ji, Jihong Zhang, and Yuanlong Cai. Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems. *Physics Letters A*, 307(1):22–28, 2003. (**SCI** indexed, IDS Number: 639BJ, an erraum of this paper has been published in *Physics Letters A*, vol. 309, no. 1-2, pp. 165, **SCI** indexed, IDS Number: 656BM).

[8] **李树钧**, 牟轩沁, 纪震, 张基宏. 一类混沌流密码的分析. 电子与信息学报, 25(4):473–478, 2003. (**EI** indexed, AN: 7499784, New AN: 03237499784).

[9] **Shujun Li**, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision. *Computer Physics Communications*, 153(1):52–58, 2003. (**SCI** indexed, IDS Number: 683VL; **EI** indexed, AN: 7489635, New AN: 03227489635).

[10] Shujun Li, Xuanqin Mou, Boliya L. Yang, Zhen Ji, and Jihong Zhang. Problems with a probabilistic encryption scheme based on chaotic systems. *International Journal of Bifurcation and Chaos*, 13(10):3063–3077, 2003. (**SCI** indexed, IDS Number: 755JY).

攻读博士期间的其他文章

[1] **Shujun Li**, Peng Wang, Xuanqin Mu, and Yuanlong Cai. Research on nonlinear dynamic systems employing color space. In *2000 5th International Conference on Signal Processing Proceedings (WCC-ICSP2000)*, volume I, pages 285–289, 2000. (**ISTP** indexed, IDS Number: BR32Z).

附件 1：

学位论文独创性声明

本人声明，所呈交的学位论文系在导师指导下本人独立完成的研究成果。文中依法引用他人的成果，均已做出明确标注或得到许可。论文内容未包含法律意义上已属于他人的任何形式的研究成果，也不包含本人已用于其他学位申请的论文或成果。

本人如违反上述声明，愿意承担以下责任何后果：

1. 交回学校授予的学位证书；

2. 学校可在相关媒体上对作者本人的行为进行通报；

3. 本人按照学校规定的方式，对因不当取得学位给学校造成的名誉损害，进行公开道歉。

4. 本人负责因论文成果不实产生的法律纠纷。

论文作者签名：_____ 日期：_____年_____月_____日

学位论文知识产权权属声明

本人在导师指导下所完成的论文及相关的职务作品，知识产权归属学校。学校享有以任何方式发表、复制、公开阅览、借阅以及申请专利等权利。本人离校后发表或者使用学位论文或与该论文直接相关的学术论文或成果时，署名单位仍然为西安交通大学。

论文作者签名：_____ 日期：_____年_____月_____日

导 师 签 名：_____ 日期：_____年_____月_____日