西安交通大学
博士学位论文答辩
2003年6月20日

数字化混沌密码的分析与设计

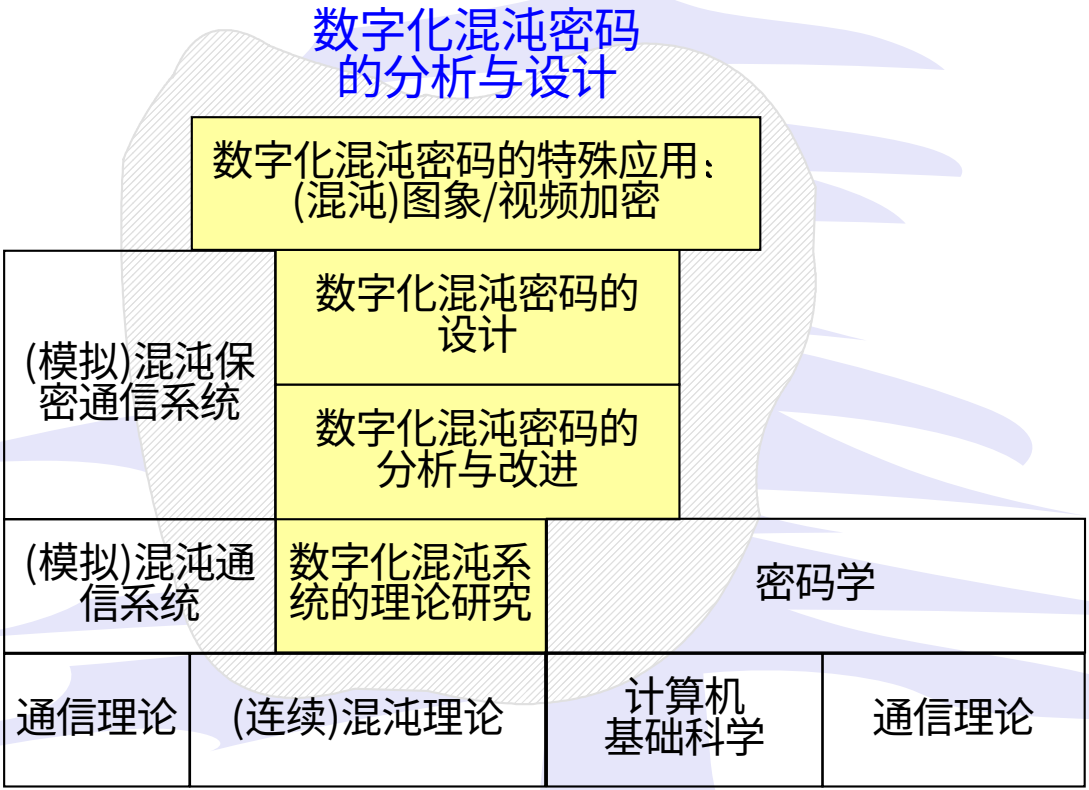
李树钧

电子与信息工程学院图象处理与识别研究所

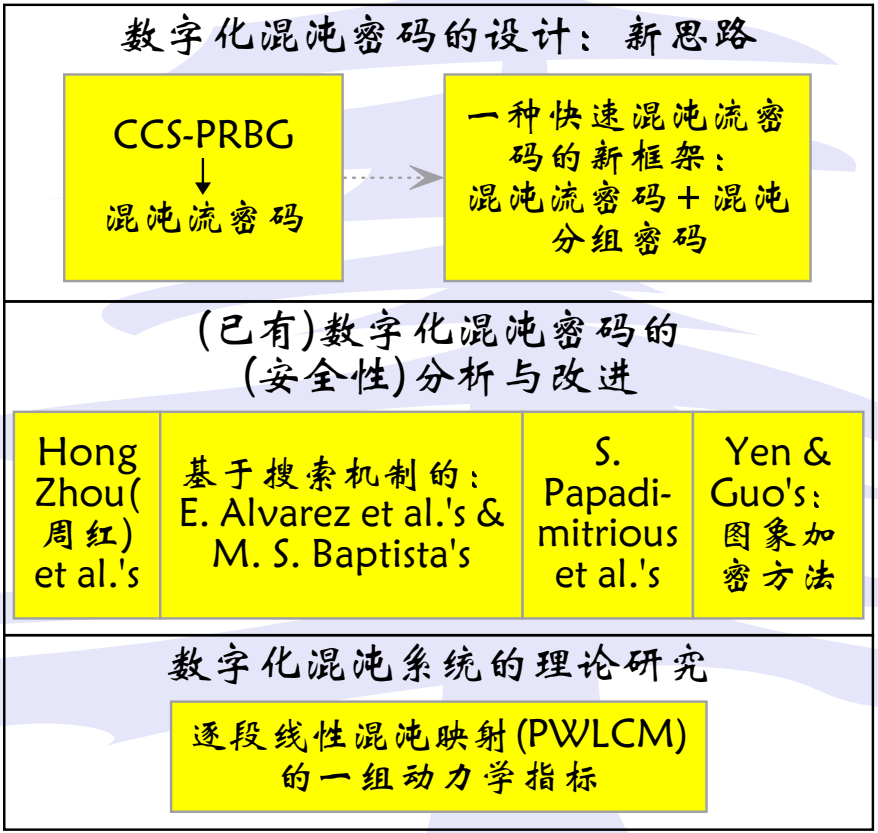
此幻灯片使用pdfLaTeX + pdfslide + PPower4制作

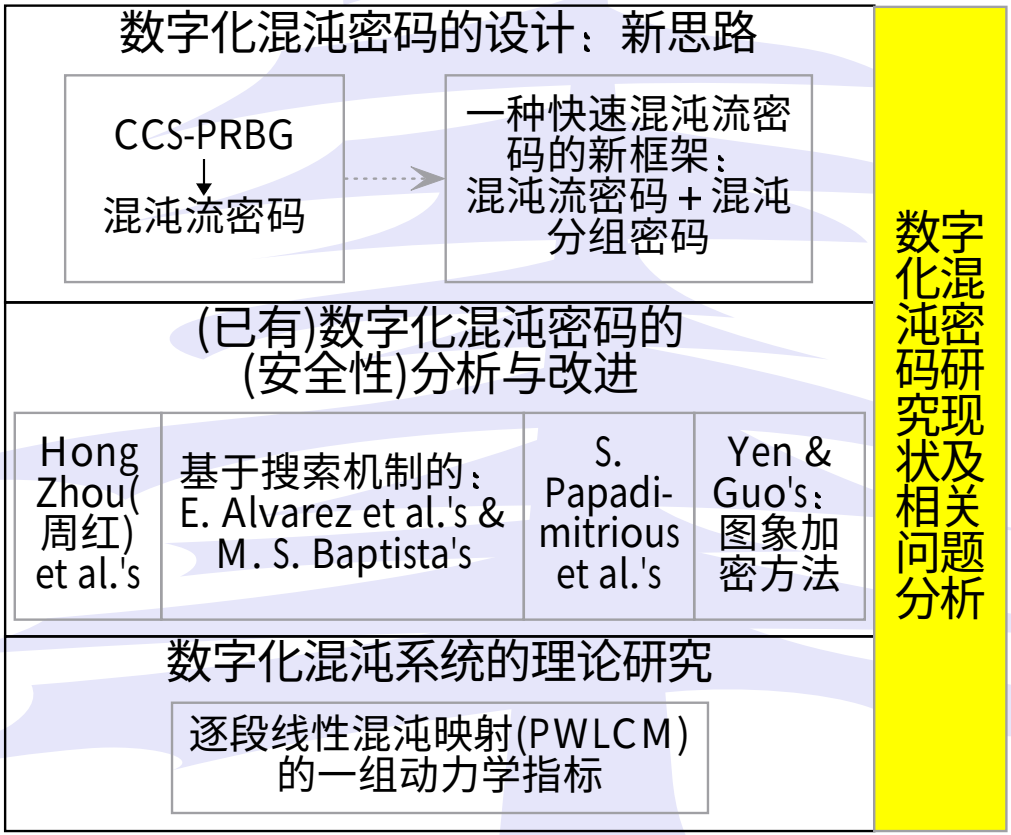
感谢ChinaTeX网站和CTeX网站提供技术帮助

本文研究方向与相关学科的关系及其组成



本文的主要研究成果

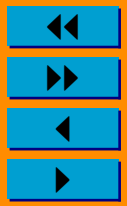

数字化混沌密码的设计：新思路
CCS-PRBG
↓
混沌流密码
一种快速混沌流密码的新框架：
混沌流密码＋混沌分组密码
(已有)数字化混沌密码的
(安全性)分析与改进
Hong Zhou(周红) et al.'s
基于搜索机制的：
E. Alvarez et al.'s &
M. S. Baptista's
S. Papadi-mitrious et al.'s
Yen & Guo's：图象加密方法
数字化混沌系统的理论研究
逐段线性混沌映射(PWLCM)的一组动力学指标


数字化混沌密码的设计：新思路
CCS-PRBG
混沌流密码
一种快速混沌流密码的新框架：混沌流密码＋混沌分组密码
(已有)数字化混沌密码的(安全性)分析与改进
Hong Zhou(周红) et al.'s
基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's
S. Papadi-mitrious et al.'s
Yen & Guo's：图象加密方法
数字化混沌系统的理论研究
逐段线性混沌映射(PWLCM)的一组动力学指标
数字化混沌密码研究现状及相关问题分析

数字化混沌密码：研究现状及存在的问题

研究历史

- 自二十世纪80年代开始至今，历经两次发展阶段：1990年前后，2000年前后。第一个阶段以大部分数字化混沌密码被分析而结束，第二个阶段仍在继续发展，涌现了很多有价值的新思路，并开始出现综述性和设计数字化混沌密码通用框架的文献。
- 文献散布在多个研究领域：密码学、非线性科学(混沌理论)、通信工程、电路与系统。。。在每个领域中有一些重要的相关领域，如非线性科学中关于数字化混沌系统的研究，基于混沌同步技术的混沌保密通信系统，混沌PRNG及其在(扩频)通信中的应用，混沌数字水印，等等。
- 最早的相关文献是Stephen Wolfram在Crypto'85上发表的文章*Cryptography with Cellular Automata*。
- 第一篇受到较多关注的文献为Robert A. J. Matthews于1989年在Cryptologia上发表的*On the Derivation of a "Chaotic" Encryption Algorithm*。



数字化混沌密码：研究现状及存在的问题

典型的数字化混沌密码

- 基于混沌PRNG的流密码：使用混沌系统轨道生成伪随机密钥流，并用来掩盖明文
- 使用混沌逆系统法设计的密文反馈密码系统：明文被密文反馈驱动的伪随机序列掩盖
- 基于反向迭代的分组密码：明文作为初始条件，通过反向混沌迭代生成密文，通过正向迭代恢复明文
- 基于正向迭代的分组密码：明文作为初始条件，通过(一一)混沌离散映射的正向迭代随机置乱明文，并与替换算法结合生成密文

数字化混沌密码：研究现状及存在的问题

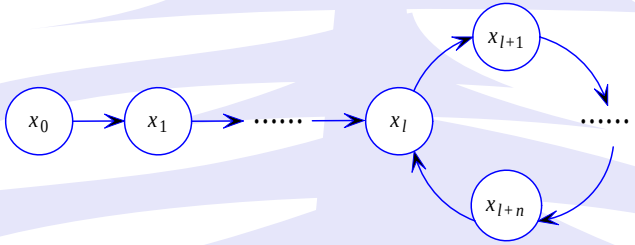
非典型的数字化混沌密码

- 基于搜索机制的数字化混沌密码：在一个混沌伪随机序列中搜索明文，以当前位置的相关信息作为密文。该类密码是近年来的一个研究热点。
- 使用混沌系统生成固定的或者动态的S盒(轮函数)，并用来构造(混沌)分组密码。
- S. Papadimitrious等人于2001年提出的一种概率混沌密码：已经知道是不安全和不实用的。
- 基于胞元自动机的密码：两种属于混沌公钥密码，其他的分别属于流密码和分组密码。
- 混沌公钥密码系统：尽本人所知，仅有四种报道，2003年发表在*Physical Review Letters*的一种算法值得进一步研究。
- 混沌图象加密算法：部分属于基于二维混沌映射正向迭代典型分组密码，部分属于基于混沌PRNG的流密码或者分组密码。

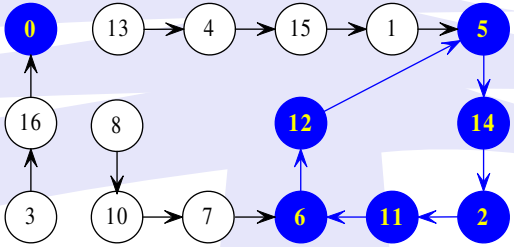
数字化混沌密码：研究现状及存在的问题

数字化混沌系统的动力学特性退化

- 不可捉摸的量化误差(噪声)
- 长期动力学：不可抗拒的周期性



图：数字化混沌系统的一条典型的拟混沌轨道



图：数字化斜tent映射$F(x,p)$在4-比特有限精度下的一条拟混沌轨道示意图($p=3/2^4$，量化算法为四舍五入)。

由于理论分析的困难性，统计方法被广为采纳，令$\epsilon = 2^{-L}$，对于大多数数字化混沌系统，已经发现下述标度律：

✓暂态长度(l)以及循环周期(n)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$\epsilon^{-d} \ll 2^L$。

✓有限循环的数量满足量级$O(\ln \epsilon^{-1}) = O(L)$。

✓不同循环周期的出现频率随着循环周期的增加而按指数衰减，这暗示存在大量具有短循环周期的拟混沌轨道。

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tent映射$F(x) = 1 - 2|x - 0.5|$。

- **影子周期轨道的零测度问题** 在数字化混沌系统中，所有影子轨道的周期都是有限的，而有限轨道的测度一般为0。
- **退化的动力学特征：遍历性，不变测度，Lyapunov指数...**
- **如何在应用中克服数字化混沌系统的动力学特性退化?**

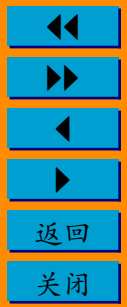
  ✓使用更高的实现精度　　✓级联多个数字化混沌系统

  ✓使用(伪)随机信号扰动拟混沌轨道/控制参数(性能最好，而且具有理论基础：量化噪声的随机扰动模型)

数字化混沌密码：研究现状及存在的问题

设计数字化混沌密码的更多考虑

- **如何选择混沌系统?**
  - ✓基于具有特定动力学特性的混沌系统，进行数字化混沌密码的设计
  - ✓尽可能使用最简单的混沌系统，逐段线性混沌映射(PWLCM，Piecewise Linear Chaotic Map)是一类很好的候选
  - ✓如果可能，采用多个(不同的)混沌系统，而不是单个混沌系统
- **如何获得快速的加密速度?**
  - ✓尽量减少加密单个明文所需的混沌迭代次数
  - ✓使用最简单的混沌系统
  - ✓避免时变的加密速度
  - ✓采用定点算法，尽量避免使用浮点算法
  - ✓在硬件实现中利用并行运算机制提高速度
- **如何简化系统设计并节省成本?**



✓使用最简单的混沌系统

✓采用定点算法，尽量避免使用浮点算法

✓在硬件实现中利用并行运算机制时，可以考虑采用多混沌系统提高整体性能

✓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

数字化混沌密码的设计：新思路
CCS-PRBG
混沌流密码
一种快速混沌流密码的新框架：
混沌流密码＋混沌分组密码
(已有)数字化混沌密码的
(安全性)分析与改进
Hong Zhou(周红) et al.'s
基于搜索机制的：
E. Alvarez et al.'s &
M. S. Baptista's
S. Papadi-mitrious et al.'s
Yen & Guo's：图象加密方法
数字化混沌系统的理论研究
逐段线性混沌映射(PWLCM)的一组动力学指标
应用

数字化PWLCM的一组动力学指标

主要理论结果及其应用

- 针对数字化一维逐段线性映射(PWLCM)，引入了一组可度量的动力学指标，它们可以定量刻画不同控制参数下数字化PWLCM动力学特性退化的程度。
- 这组动力学指标可以看作是“拟遍历性”和数字化不变分布的一种统计度量。
- 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，这种数字化算法的塌缩进而造成动力学特性的塌缩(退化)。
- 给出了数字化PWLCM的上述动力学指标的几种可能的应用：

  ✓对几种改善数字化混沌系统动力学特性退化的不同方案进行定性比较。分析确认了扰动策略性能较好的结果，并指出扰动系统变量比扰动控制参数具有更好的效果。

  ✓在混沌密码学和混沌伪随机数发生器方面的理论指导意义，强调了理论分析工具在数字化混沌系统应用中的重要性。

数字化PWLCM的一组动力学指标

相关预备知识

- **逐段线性混沌映射－PWLCM**

  所谓逐段线性映射，就是指包含有限个线性分段的映射，很多逐段线性映射可以展现混沌行为。本文的研究主要针对一类**逐段映满的**逐段线性混沌映射展开：这类映射的每个线性分段将相应的子定义区间映射到整个值域上去(即映满的)。最简单和最典型的逐段映满的PWLCM是tent映射$F(x) = 1 - 2|x - 0.5|$。

- **预备定义**

  ✓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**为$n$的**数字集(digital set)**。特别的，定义$S_0 = \{0\}, S_\infty = [0,1)$。

  ✓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**为$i$的**数字层次(digital layer)**。$\forall p \in V_i$，i称为p的**分辨率**。

  ✓$\forall n > m$，$D_{n,m} = S_n - S_m$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)**。$D_{n,0}$简写为D_n。

  ✓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) $\lfloor x \rfloor$；2) $\lceil x \rceil$；3) $\mathbf{round}(x)$。

✓一个函数$G_n : S_\infty \to S_n$称为一个**分辨率为n的数字化近似转换函数(DATF，digital ATF)**，如果$\forall x \in S_\infty = [0,1)$，$|G_n(x)-x| < 1/2^n$。三种基本的DATF：1) $\mathbf{floor}_n(x) = \lfloor x \cdot 2^n \rfloor / 2^n$；2) $\mathbf{ceil}_n(x) = \lceil x \cdot 2^n \rceil / 2^n$；3) $\mathbf{round}_n(x) = \mathrm{round}(x \cdot 2^n)/2^n$。

数字化PWLCM的一组动力学指标

动力学指标的定义

- **数字化混沌系统的离散表示形式**

  给定一个数字化一维PWLCM $F(x): I \to I$，这里$I = [0,1]$。不失一般性，重定义该映射为$F_{[0,1)}(x) = F(x) \bmod 1$。则$n$-比特有限精度下的PWLCM可以表示为$\mathcal{F}_n = G_n \circ F_{[0,1)} : S_n \to S_n$，这里$G_n(\cdot)$是一个DATF。

- **动力学指标的定义** $\forall x = 0.b_n b_{n-1} \cdots b_2 b_1 \in S_n$，定义$P_j(x)$为$x$的最低$j$个比特$b_j \cdots b_1$全为0的概率，一个等效的定义是$P_j(x) = P\{x \in S_{n-j}\}$。我们提出的$n$个动力学指标即为$P_1(\mathcal{F}_n(x)) \sim P_n(\mathcal{F}_n(x))$，这里$x$是一个在$S_n$上离散均匀分布的离散随机变量。

- 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，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使得$P_j(\mathcal{F}_n(x)) \neq 2^{-j}$。这说明$P_1(\mathcal{F}_n(x)) \sim P_n(\mathcal{F}_n(x))$可能**定量**反映$\mathcal{F}_n(x)$在离散均匀输入信号$x$驱动下的输出不均匀程度。

数字化PWLCM的一组动力学指标

计算给定PWLCM动力学指标值的方法

为了简化叙述，在后文我们将使用简写符号P_j表示$P_j(\mathcal{F}_n(x))$。

- **求单个线性分段上的$P_j(1 \le j \le n)$**

  定理 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$[1, 2^i - 1]$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：

$$P_j = \left\{ \begin{array}{ll} \dfrac{1}{N_p \cdot 2^{j-i}} & , \ i \le j \le n \\ \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p} & , \ G_0(\cdot) = \lfloor \cdot \rfloor \text{或} \lceil \cdot \rceil \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p} & , \ G_0(\cdot) = \text{round}(\cdot) \end{array} \right\} , \ 1 \le j \le i-1 \quad 。$$

- **使用全概率公式将多个线性分段上的动力学指标值综合起来**

数字化PWLCM的一组动力学指标

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。
- 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。

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

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

一般来说，$r_1, \cdots, r_m$越小，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$\overline{\boldsymbol{P}}_j = 2^{-j}$。

- 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。
- 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$\overline{P}_j = 2^{-j}$的m倍；当j从$\max_{i=1}^{m}(r_i)$变化到1的过程中，P_j和$\overline{P}_j = 2^{-j}$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。

数字化PWLCM的一组动力学指标

如何理解动力学指标与PWLCM动力学特性退化之间的关系？

- 考虑到$\max_{i=1}^{m}(r_i) \le j \le n$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。
- 这组指标也可以区分不同控制参数下动力学特性退化的不同。

  ✓对于m个控制参数的集合$\boldsymbol{p} = \{p_1, p_2, \ldots, p_m\}$，定义$\widetilde{P} = \sum_{j=1}^{n} P_j / (n \cdot \overline{P}_j)$为$\boldsymbol{p}$的**平均退化因子**，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。

  ✓一般而言，**分辨率越小，控制参数就越弱**。

  那么小的分辨率到底意味着什么呢？
  把一个分辨率为i的线性分段斜率p写成$p = N_p/2^i = 2^{n-i} \cdot N_p/2^n$，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

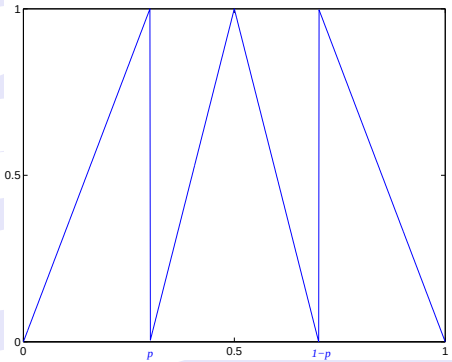
法x/p时，假设$x = N_x/2^n$，该除法可以表示为$x/p = 2^{n-i} \cdot N_x/N_p$，这里$2^{n-i}$意味着左移操作，这种操作显然会使得相应的动力学指标值变大。这实际上就是数字化算法塌缩的真正原因。

✓这组动力学指标可以看成是数字化PWLCM的“拟遍历性”和数字化不变分布的一个统计度量。

✓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。下面我们以周红等人的文献中使用的PWLCM为例给出更多有趣的结论。

数字化PWLCM的一组动力学指标

一个典型的例子：周红等人在相关文献中使用的PWLCM

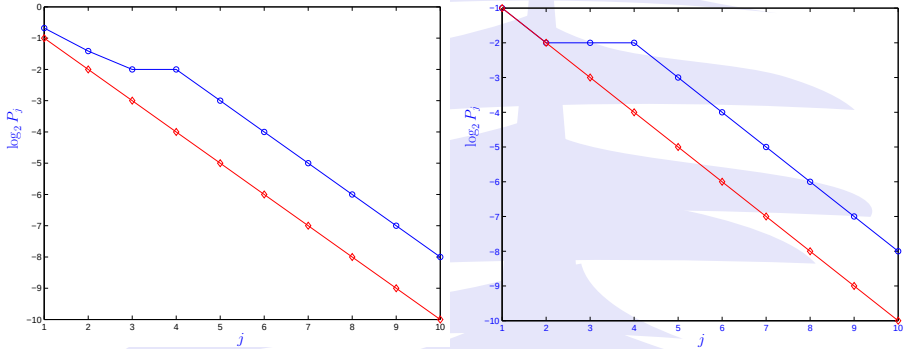


定理 *假设一个离散随机变量x在S_n上离散均匀分布。$\forall p \in V_i (2 \le i \le n)$，对上述数字化PWLCM如下结论成立：*

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， $P_j = \begin{cases} \frac{4}{2^j}, & i \le j \le n \\ \frac{1}{2^j} + \frac{2}{2^i}, & 1 \le j \le i-1 \end{cases}$；

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



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

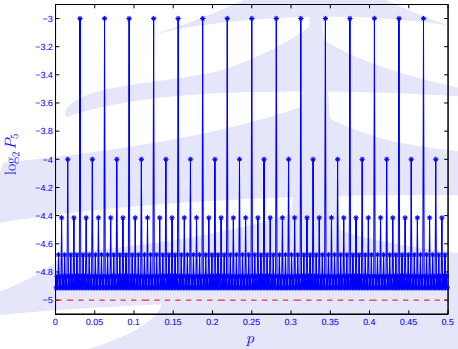
$\circ$: $\log_2 P_j$; $\diamond$: $\log_2 \overline{P}_j = -j$

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

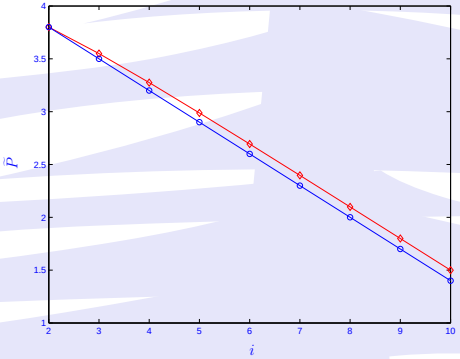
根据上述定理，可以推出下面两个有用的结论：

✓对于具有不同分辨率的控制参数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**。

✓动力学特性退化和控制参数p的分辨率i之间存在下述的严格关系：分辨率i越小，p越弱。



图：$\log_2 P_5$相对p的变化，这里$n = 10$，$G_n(\cdot) = \text{floor}_n(\cdot)$



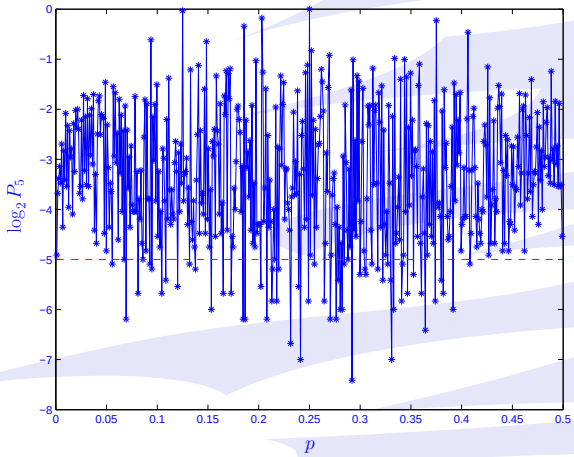
$\circ$：$G_n(\cdot) = \text{round}_n(\cdot)$；$\diamond$：$G_n(\cdot) = \text{floor}_n(\cdot)$或$\text{ceil}_n(\cdot)$

图：$\widetilde{P}$和i之间的关系，$n = 10$

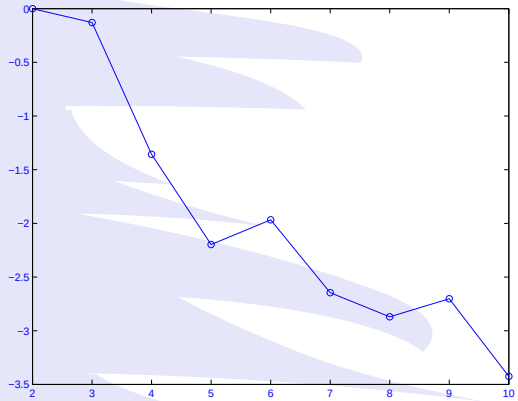
返回
关闭

数字化PWLCM的一组动力学指标

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



图：$\mathcal{F}_n^{32}(x)$的$\log_2 P_5$(相对p)



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

Q 一个问题：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?

A 可能的答案：控制参数强弱与分辨率之间的关系仍然近似保持。可以推测，这种近似保持随着k的增大而逐渐变得越来越差。

返回
关闭

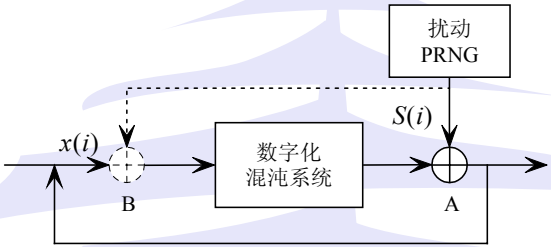
数字化PWLCM的一组动力学指标

相关应用：几种数字化PWLCM混沌动力学特性退化的改善方案的性能比较

- 三种工程化的改善方案：使用更高的有限精度；级联多个数字化混沌系统；对混沌系统施加(伪)随机扰动。已经知道最后一种方案从理论和实验的角度似乎更好。
- 使用更高的有限精度不能改善原精度下所有控制参数的强弱，因此该方案不够好。
- 级联k个数字化混沌系统实际上类似于一个数字化混沌系统的k次复合，已经知道，数字化PWLCM的k次复合的动力学特性退化更严重，因此该方案不够好。
- 基于扰动的改善方案

  ✓扰动方案可以同时改善拟混沌轨道长度和混沌输出分布的不均匀性。因此其性能比上述两种方案更好。

  ✓假设$\oplus$表示扰动操作，有两种可能的扰动配置方案：



图：两种可能的扰动配置方案

✓两种扰动方案都可以有效地延长拟混沌轨道的长度。

✓由于配置方案A同时扰动输出与输出(带记忆的反馈配置)，而配置方案B仅扰动输入，方案A的改善性能较方案B为优。

✓除了扰动拟混沌轨道的方法以外，J. Čermák在文章*Digital Generators of Chaos*(Physics Letters A, vol. 214, no. 3-4, pp. 151–160, 1996)中提出扰动控制参数的方法，对于较强的控制参数，这种方法不如扰动轨道的方法好。

数字化PWLCM的一组动力学指标

相关应用：数字化混沌密码和混沌伪随机数发生器

- 在数字化混沌密码中的应用

  ✓一维PWLCM在数字化混沌密码中广为使用。

  ✓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，一个例子是对周红等人的密码分析。

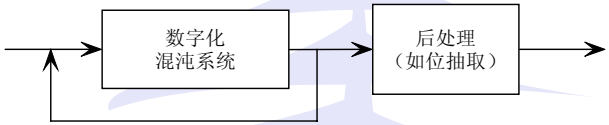
  ✓应用关于数字化PWLCM的相关结论，可以定性地指导相关混沌密码安全性的增强。

- 在数字化伪随机数发生器中的应用

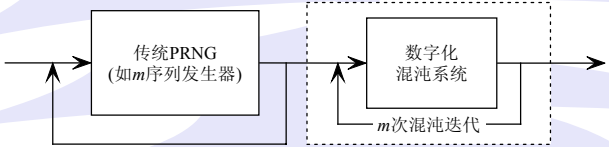
  ✓数字化混沌系统输出的不均匀可能造成伪随机序列分布不均匀。因此需要采取一定的补救措施，我们推荐扰动策略。

  ✓由于任何补救措施都不能绝对改善数字化混沌系统的动力学特性退化，我们建议只使用最强的(分辨率最高的)控制参数。

  ✓两种混沌伪随机数发生器的通用结构：



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：两种混沌伪随机数发生器的通用结构

✓如果采用上述第一种结构的话，并且对安全性比较敏感的场合下，建议使用较为复杂的后处理函数以增强安全性。

✓第二种结构实际上可以看作是普通伪随机数发生器的平滑和非线性化版本。

数字化混沌密码的设计：新思路
CCS-PRBG
混沌流密码
一种快速混沌流密码的新框架：混沌流密码＋混沌分组密码
(已有)数字化混沌密码的(安全性)分析与改进
Hong Zhou(周红) et al.'s
基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's
S. Papadi-mitrious et al.'s
Yen & Guo's：图象加密方法
数字化混沌系统的理论研究
逐段线性混沌映射(PWLCM)的一组动力学指标

周红等人提出的一类混沌流密码的分析

周红等人提出的一类混沌密码

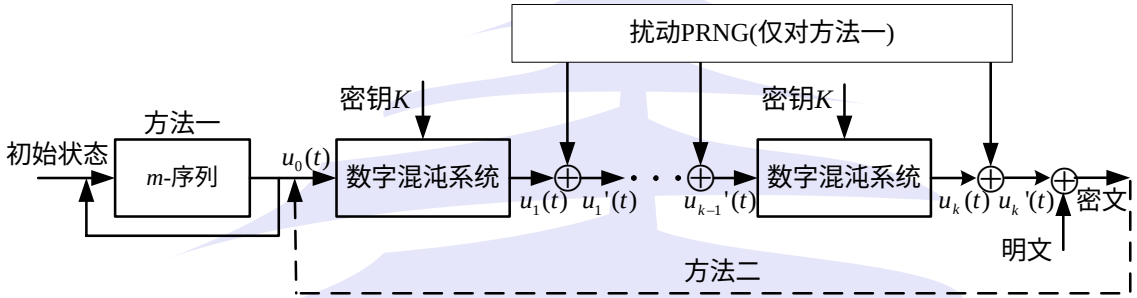
- 复旦大学的周红等人于1996～1998年间先后几种混沌密码方案，它们都是基于数字化PWLCM密钥流的混沌流密码，大致分为两个基本类型：

  ✓使用均匀分布的输入信号驱动多次混沌迭代产生密钥流；

  ✓通过对拟混沌轨道进行非线性后处理生成密钥流：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。

- 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：由于周红等人在其中一篇文献中使用了PWLCM，其逐段线性性可能导致某些“潜在”的不安全性。

- 基于前面给出的数字化PWLCM的动力学指标及其性质，我们针对周红等人的第一类混沌密码展开讨论，分析指出：



图：周红等人的第一类混沌流密码

✓即使在采用了扰动策略的情况下，仍然存在大量弱密钥，其分布存在多分辨率特性；

✓可以导出一类增强的穷举攻击方案，将密钥熵降低2个比特。

周红等人提出的一类混沌流密码的分析

数字化PWLCM的动力学特性退化的对周红等人提出的密码方案安全性的影响

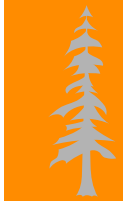
- **一个简单例子** 假设有限精度$n = 8$，$G_n(\cdot) = \text{floor}_n(\cdot)$。当$p = 3/8$，$y(t-1) = 1/16$时，可以算出$F_n^9(y(t-1), p) = 0$。由于$k \geq n+1 = 9$，$F_n^k(y(t-1), p) = F_n^9(y(t-1), p) = 0$。因而，

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

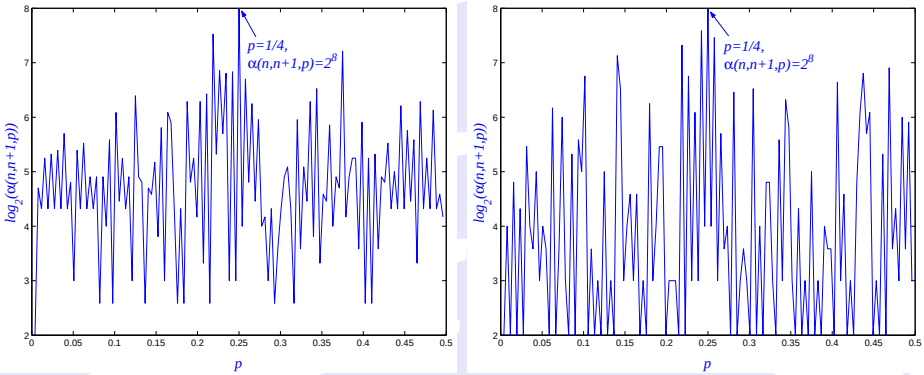
  也就是说，明文$u(t)$没有经过任何加密直接输出为密文！

- 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。

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



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

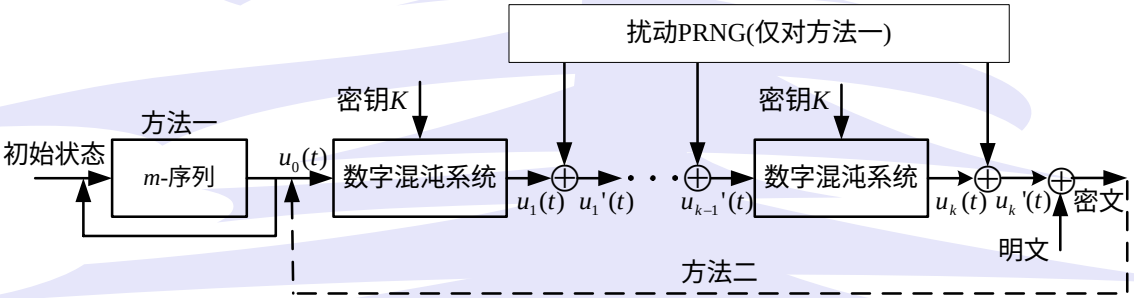
图：弱密钥因子$\log_2(\alpha(n,n+1,p))$相对p的变化，$n=8$

- 上述实验结果与前面给出的关于数字化PWLCM的理论结论基本上是一致的：最弱的密钥是分辨率最小的密钥$p=1/4\in V_2'$，分辨率约小的密钥倾向于越弱，但是部分具有较大分辨率的密钥也很弱。

周红等人提出的一类混沌流密码的分析

弱密钥分析与一种增强的穷举攻击

- 周红等人密码的安全基础之一：使用的PWLCM具有均匀的不变分布函数$f^*(x)=1$。
- 但是，已经知道，数字化PWLCM的动力学特性退化可以用一组指标值定量刻画，进而导出确定密钥的分辨率。



- 由于扰动算法是公开的，在已知/选择明文攻击下，密钥流$k(t)$是已知的，从$k(t)$中去掉最后一轮扰动可以得到最后一轮混沌系统的直接输出$u_k(t)$。显然，$u_k(t)$满足前面证明的有关PWLCM的定

理，因此指标值$P_1 \sim P_n$可以由$u_k(t)$计算出来，从而可以确定密钥的分辨率。

- 一旦得到密钥的分辨率，即可该分辨率对应的数字子层中穷举搜索密钥，这种搜索的复杂度比简单穷举小。

表：不同分辨率密钥的比较

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}	$\cdots$

- 这意味着一种增强的穷举攻击，其密钥熵可以推出大约为$n-3$，比简单穷举攻击下的密钥熵$n-1$小两个比特。
- 实验与仿真验证了我们关于弱密钥和增强穷举攻击的可行性。

返回
关闭

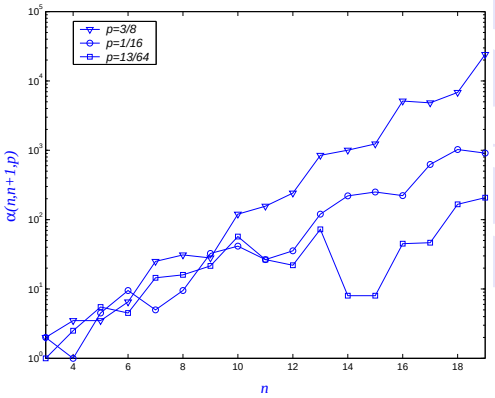
周红等人提出的一类混沌流密码的分析

可能的补救措施

- **使用更高的有限计算精度：否**

  ✓如前所述，有限计算精度的提高不能改善原精度下任何密钥的强弱。

  ✓在未采取扰动策略的情况下，原精度下的弱密钥反而可能变得更弱，这暗示更高的有限精度可能适得其反。



图：$\alpha(n, n+1, p)$相对$n = 6 \sim 19$的变化曲线

- **使用更复杂的混沌系统：不定**

  一些更为复杂的混沌系统可以用来替换PWLCM，如下述逐段非线性混沌映射(桑涛等人1999年提出)：

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

- **使用秘密的扰动参数：是?**
- **隔离拟混沌轨道和密钥流：是?**

  隔离的通用线路：$k(t)=F_{ins}(u'_k(t))\neq u'_k(t)$，这里$F_{ins}(\cdot)$是一个非线性(不可逆或者保密的)隔离函数。

- **避免使用弱密钥：是**

  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。

- **同时扰动混沌轨道和控制参数：是**

  显然，对控制参数的扰动可以成功地混淆密钥的分辨率。

数字化混沌密码的设计：新思路

CCS-PRBG
↓
混沌流密码

一种快速混沌流密码的新框架：
混沌流密码＋混沌分组密码

(已有)数字化混沌密码的(安全性)分析与改进

Hong Zhou(周红) et al.'s	基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's	S. Papadi-mitrious et al.'s	Yen & Guo's：图象加密方法

数字化混沌系统的理论研究

逐段线性混沌映射(PWLCM)的一组动力学指标

基于搜索机制的数字化混沌密码的分析

基于搜索机制的数字化混沌密码

- **基于搜索机制的数字化混沌密码**

  基于搜索的混沌密码的大致加密过程为：在一个混沌伪随机序列中寻找当前明文，记录当前位置的有关信息作为密文。两种典型的这种密码分别由E. Alvarez等人和M. S. Baptista提出。

- **E. Alvarez等人的密码(1999)**

  ✓这是一种分组密码，被搜索的伪随机序列是由混沌轨道以二值化策略生成的，每个明文分组被加密为一个三元密文组：(明文大小，当前混沌状态，当前阈值参数)。

  ✓与普通分组密码不同，其分组大小是时变的。

  ✓下述tent映射被用来演示该密码的性能，控制参数r被选作密钥。

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

- **M. S. Baptista的混沌密码(1998)及其改进版本(2001–2003)**

  ✓该系列密码更接近流密码，被搜索的伪随机序列是混沌轨道本身(通过一个关联映射f_S将混沌轨道的不同子区间与S个字符联系在一起)，明文字符m_i被加密为自上次加密开始的混沌迭代次数C_i。

  ✓C_i需满足如下限制：$N_0 \leq C_1 \leq N_{max}$(原文献中$N_0 = 250$，$N_{max} = 65532$)。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$\eta$用来选择一个合适的值。

  ✓在已有的原密码方案的改进版本中，有下述几点新的思路：使用其他的混沌系统；额外的伪随机数用来控制密文的分布均匀性；使用动态更新的关联映射(查找表)；引入会话密钥实现收发同步。

基于搜索机制的数字化混沌密码的分析

E. Alvarez等人的混沌密码的安全性分析

- 仅在E. Alvarez等人的密码提出几个月以后，G. Alvarez等人指出：当使用tent映射时，该密码很容易被攻破，并提出了四种不同的攻击方案，同时指出了该混沌密码中存在的一些其他缺陷。
- **E. Alvarez等人的混沌密码的本质缺陷**
  - ✓ ***缺陷之一：X_i在密文中的出现***
  - ✓ ***缺陷之二：使用不同密钥时混沌系统具有不同的动力学特性***
- **E. Alvarez等人的混沌密码的其他缺陷**
  - ✓G. Alvarez等人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。
  - ✓另外一个严重的问题是加密速度太慢。
  - ✓b_i的选取上存在矛盾：不能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。

基于搜索机制的数字化混沌密码的分析

我们提出的E. Alvarez等人混沌密码的一种改进方案(2001)

- **使用的混沌系统**

  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。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。显然，PWLCM是满足这样条件的混沌映射。

- **加密过程**

  和原方案很类似，只是在相应的伪随机序列中找到明文后，用迭代次数n_i替换原方案中的当前混沌状态作为密文的一部分。这避免了前面提到的第一个缺陷。

- **简化密文**

  阈值参数U_i可以是固定的，一般选为使生成的伪随机序列平衡的数值。这可以从混沌映射的不变分布推导出来。

- 改进方案更像是一个**流密码**而不是分组密码，这使得使用较小的b_{max}成为可能，从而部分缓解了b_{max}取值上的困难。
- **密码学特性(仅将迭代次数n_i看作是“真正”的密文)**

  ✓密文是不平衡的，n_i越大，它在密文中出现的概率也越小。假设伪随机序列是平衡的i.i.d.(独立同分布的)比特序列，则可以推出n_i的离散分布列：$P\{n_i = k\} = 2^{-b_i} \cdot \left(1 - 2^{-b_i}\right)^{k-1}$。

  ✓关于n_i的四个事实：1) 对于不同的明文，密文离散分布列相同；2) 对于不同的密钥(控制参数和初始条件)，密文离散分布列相同；3) 对于两个仅有微小差异的明文，密文完全不同；4) 对于两个仅有微小差异的密钥，密文完全不同。

  ✓实验结果验证了上述理论结果的正确性。
- **加解密速度**

  假设每秒执行s次混沌迭代，则平均加密速度大约为$s \cdot b_{max}/2^{b_{max}}$ bps。当$b_{max} = 1,2$，加密速度会变得很快，需要进一步研究如此小的b_{max}可能带来的安全隐患。
- **加密后压缩密文**

  为了减少密文扩展，可以采用无损压缩算法对密文进行压缩。

基于搜索机制的数字化混沌密码的分析

对M. S. Baptista密码的Jakimoski-Kocarev攻击及其性能分析

- **Jakimoski-Kocarev攻击(2001)**

  ✓属于已知明文攻击，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”(定义为$n = \sum_{j=1}^{i} C_j$，即自x_0开始的混沌迭代总次数)和明文字符之间的一张关联表。

  ✓该攻击依赖于**混沌迭代次数C_i在密文中出现**这个事实，因此对M. S. Baptista密码的所有改进方案都是可行的，也可用来攻击我们在前面提出的E. Alvarez等人密码的改进方案。

- **我们关于Jakimoski-Kocarev攻击性能的观点**

  我们认为，Jakimoski-Kocarev攻击的性能并不那么有效，原因如下：

  ✓**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。

  ✓**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**几乎不可能**，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**。

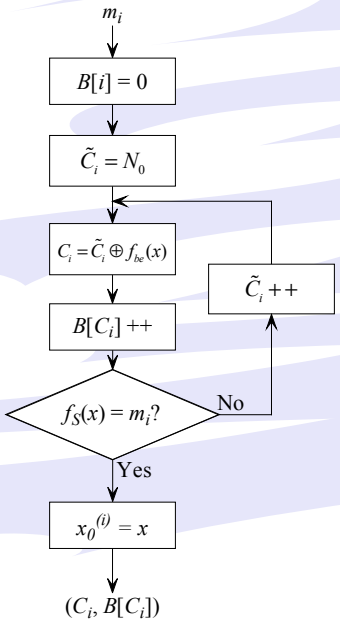
✓**事实三**：由于相同的明文字符可能被加密为不同的密文单元，M. S. Baptista的密码方案更像一个流密码，而不是分组密码。但是Jakimoski-攻击是按照攻击分组密码的思路设计的，并不太适用于流密码。

✓**事实四**：在已知密文中如果不是所有的密文单元都已知，则解密该未知密文“感兴趣时刻”以后的所有密文都不可能。

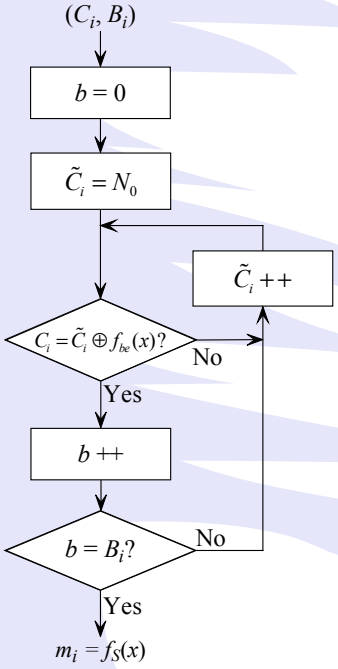
基于搜索机制的数字化混沌密码的分析

一种抵抗Jakimoski-Kocarev攻击的改进措施

我们提出的一种改进方案(2003)的加解密流程图如下：



a) 加密过程



b) 解密过程

由于混沌迭代次数$\widetilde{C}_i$被函数$f_{be}(x)$掩盖了，计算“感兴趣时刻”不再可能，因此上述改进方案可以抵抗Jakimoski-Kocarev攻击，以及G. Alvarez等人于2003年新提出的四种攻击方案。

- 由于密文分布的不均匀性，比特抽取函数不能随意选择以避免泄漏有关信息，这里给出两种可能的“强”函数族作为例子：

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

这里$f'_{be}(x)$可以是**任何**从x的二进制形式中抽取16个比特的函数。

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

这里$m \geq 1, n \geq 4$并且$b(x,j) = \lfloor x \cdot 2^j \rfloor \bmod 2$。

- 如果采用一些其他手段使得密文分布变成(或“近似”)**均匀**的，则比特抽取函数可以**自由**选择。两种可能的方法如下：
  - ✓**方法一**：使用W.-K. Wong等人提出的改进密码方案。
  - ✓**方法二**：引入压缩机制。

数字化混沌密码的设计：新思路

CCS-PRBG
↓
混沌流密码

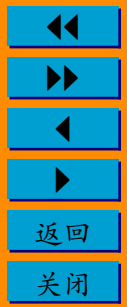
一种快速混沌流密码的新框架：
混沌流密码＋混沌分组密码

(已有)数字化混沌密码的(安全性)分析与改进

Hong Zhou(周红) et al.'s	基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's	S. Papadi-mitrious et al.'s	Yen & Guo's：图象加密方法

数字化混沌系统的理论研究

逐段线性混沌映射(PWLCM)的一组动力学指标



S. Papadimitriou等人的概率混沌密码的分析

S. Papadimitriou等人提出的混沌密码(2001)

- **形式化描述**

  ✓给定2^e个虚拟状态和$2^d < 2^e$个虚拟吸引子，以及它们之间的关联(一个多对一的满映射)$\boldsymbol{F}_v : \boldsymbol{V}_s \to \boldsymbol{V}_a$，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。

  ✓**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。

- **采用的混沌系统**

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

这里$R_i = U_i - L_i$，$[L_i, U_i]$是f_i的定义域，$f_i(i = 1 \sim K)$被建议为具有N个断点的逐段线性函数。

S. Papadimitriou等人的概率混沌密码的分析

S. Papadimitriou等人混沌密码中的问题

- **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。仿真实验证实了这种矛盾的存在。

- **关于所有可能的虚拟状态的数量的推导是错误的**

  ✓原文中的错误结论：$(k!)^m \cdot k^{n-k\cdot m}$。

  ✓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(除少量特例外，到目前为止尚不存在已知的显式解析解)：

$$\text{当}n = mk\text{时}, \quad g(n) = \binom{mk}{m,m,\cdots,m} = \frac{(mk)!}{(m!)^k}。$$

$$\text{当}n > mk\text{时}, \quad g(n) = \frac{\sum_{t=mk}^{n-1} g(t)\left(k\cdot\binom{n+m-1}{t} - \binom{n+m-1}{t-1}\right)}{\frac{n-mk}{k}\cdot\binom{n+m-1}{n}}。$$

✓上述真实值与S. Papadimitriou等人给出的结果完全不同。在多数情况下，原文导出的结果比真实值要**小**。那么是否S. Papadimitriou等人密码的安全性被低估了？答案是**否定的**。

- **安全性分析是不正确的，对于穷举攻击的安全性被高估了**

  ✓大部分虚拟状态空间太近而不能保证密码的高安全性。“**好的**”虚拟状态空间的数量要比理论值**小的多得多**。

  ✓并不是所有的虚拟状态空间都可以用混沌系统构造出来，可构造的空间数量受所有可能密钥的数量$\mathcal{N}_K$限制。

  ✓不同的密钥可能产生相同的虚拟状态空间。S. Papadimitriou等人密码的安全上限为$\min(g(n), \mathcal{N}_K)$。

  ✓由于d和e取值方面的矛盾，密码对已知/选择明文攻击、选择密文攻击都是不安全的；对这三种攻击的密钥熵都只有e，这比$LN - \log_2(K/N!)$要小得多。

- 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。
- 混沌系统在有限精度下实现，动力学特性退化必须加以改善。
- 对于密码设计中的部分细节缺乏明确描述。

数字化混沌密码的设计：新思路

CCS-PRBG
↓
混沌流密码

一种快速混沌流密码的新框架：
混沌流密码＋混沌分组密码

(已有)数字化混沌密码的(安全性)分析与改进

Hong Zhou(周红) et al.'s	基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's	S. Papadimitrious et al.'s	Yen & Guo's：图象加密方法

数字化混沌系统的理论研究

逐段线性混沌映射(PWLCM)的一组动力学指标

两类Yen-Guo混沌图象加密算法的分析

两类Yen-Guo图象加密方法：CKBA和BRIE

J.-C. Yen和J.-I. Guo(等人)近年陆续提出几种混沌图象加密方法。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。

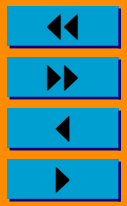
我们针对其中的两种混沌图像加密方法进行了密码分析，发现它们都不能抵抗已知/选择明文攻击，仅一个已知/选择明文图像即可用于得到等效密钥，并进一步导出实际密钥。

- **CKBA：Chaotic Key-Based Algorithm(2000)**

  CKBA是一种流密码，混沌系统用于产生伪随机掩盖密钥流。

- **BRIE：Bit Recirculation Image Encryption(1999)**

  BRIE是一种象素值替换密码，位置(x,y)处的密文象素仅由相同位置的明文象素决定。



两类Yen-Guo混沌图象加密算法的分析

CKBA的密码分析

- **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}。

  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，加上其他两个秘密参数，实际密钥熵大概仅为30。

- **已知/选择明文攻击：破解等效密钥–掩模图象**

  假设攻击者已知一副明文图象f和其对应的密文图象f'(大小均为$M \times N$)，求掩模图像$f_m = f \oplus f'$。如果一副密码图象的大小不比$M \times N$大的话，f_m可以替代密钥K解密之。对于尺寸大于$M \times N$的密文图象，其左侧的MN个明文象素可以被成功解密。得到f_m的计算复杂度只有$O(MN)$。

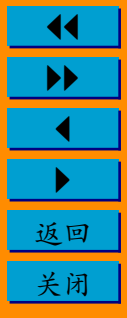
  ✓由掩模图象f_m得到密钥

  通过f_m可以恢复出实际密钥，复杂度$O(MN)$。

✓由一个足够大的掩模图象得到任意尺寸的掩模图象

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。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。这样的话，如果已知掩模图象f_m的尺寸为$256 \times 256 = 2^{16}$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。

✓实验结果支持上面全部结论。

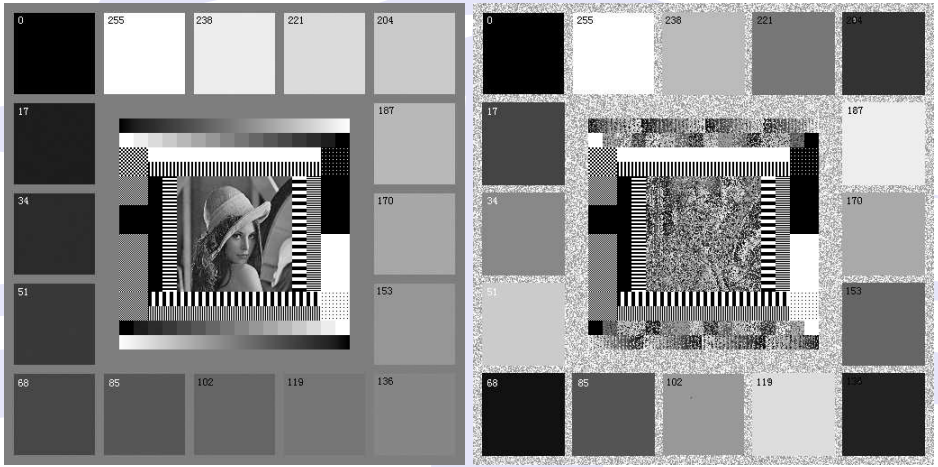


两类Yen-Guo混沌图象加密算法的分析

BRIE的安全缺陷

- ***ROLP*操作的本质缺陷**

  ✓如果明文图象中包含太多灰度值无变化的象素和/或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文图象的有用信息。



a) 明文图象　　b) 密文图象

图：使用BRIE加密的一副特殊图象Test_Pattern.bmp

✓推广：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。

a) 明文图象　　b) 密文图象

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

- **关于α, β的安全问题(原文献未提及)**

  ✓$1 \leq \alpha \leq 7, 1 \leq \beta \leq 7$

  ✓$\alpha + \beta \neq 8$

✓$\alpha \bmod 8 \neq 1,7$或者$(\alpha+\beta) \bmod 8 \neq 1,7$

a) $\alpha = 6, \beta = 2$

b) $\alpha = 1, \beta = 6$

图：使用BRIE加密的图象Lenna.bmp，$x(0) = 0.75$

- **被高估的对穷举攻击的安全性**

  类似CKBA，安全性由密钥确定，而不是伪随机混沌比特的数量。

两类Yen-Guo混沌图象加密算法的分析

BRIE的已知/选择明文攻击

- **等效密钥–掩模矩阵Q**

  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：$ROLP_0^1(f(x,y)) \sim ROLP_0^7(f(x,y))$。

  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$f'(x,y) = ROLP_0^{q(x,y)}(f(x,y))$。重复以上过程，我们可以得到一个掩模矩阵$Q = [q(x,y)]_{M\times N}$。

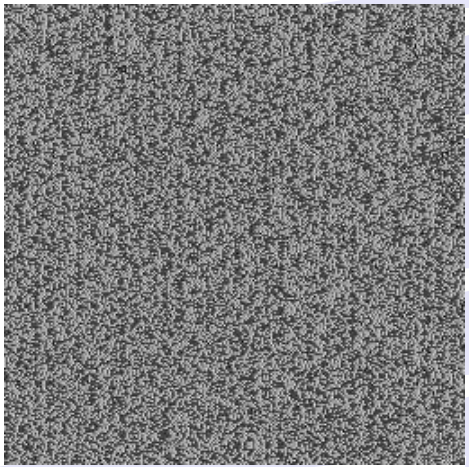
  该掩模矩阵和CKBA中的掩模图像f_m类似，可以用来完全解密尺寸不大于MN的密文图像和尺寸大于MN的密文图像的左侧MN个明文像素。

- **由Q确定密钥**

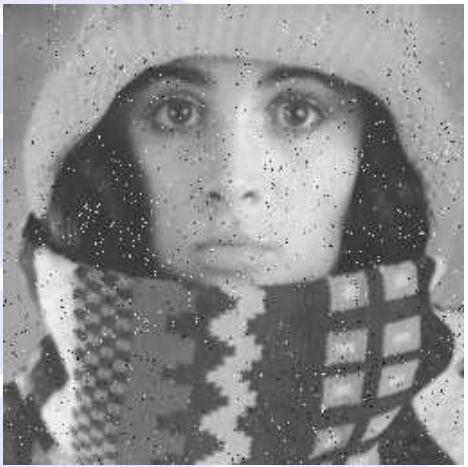
  找到16个连续的C4类(参见论文)象素(对于绝大多数明文而言，这都是可能的)，即可恢复拟混沌轨道，从而得到等效的初始条件$x1$和其他秘密参数。如果这16个像素是明文图象的头16个象素

返回
关闭

的话，$x1 = x(0)$。



a) 已知Lenna.bmp时得到的掩模矩阵Q



b) 使用Q解密的Miss.bmp

图：使用掩模矩阵Q破解BRIE加密的Miss.bmp

数字化混沌密码的设计：新思路

CCS-PRBG
↓
混沌流密码

一种快速混沌流密码的新框架：
混沌流密码＋混沌分组密码

(已有)数字化混沌密码的(安全性)分析与改进

Hong Zhou(周红) et al.'s	基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's	S. Papadi-mitrious et al.'s	Yen & Guo's：图象加密方法

数字化混沌系统的理论研究

逐段线性混沌映射(PWLCM)的一组动力学指标

基于CCS-PRBG的混沌流式密码

CCS-PRBG(基于双混沌系统的伪随机比特发生器)

- **定义**

  假设有两个不同的一维混沌映射$F_1(x_1,p_1)$和$F_2(x_2,p_2)$，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：

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

- **约束条件**

  $R1)-F_1(x_1,p_1)$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$f_2(x)$；

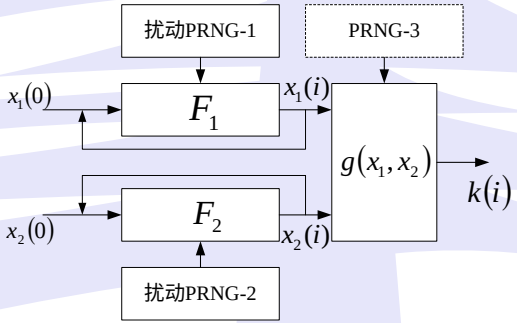
R3) – 满足下列两个条件之一：$f_1(x) = f_2(x) = f(x)$，或者$f_1(x), f_2(x)$都相对$x = (a+b)/2$偶对称；

R4) – 当$i \to \infty$时，$\{x_1(i)\}, \{x_2(i)\}$渐近独立。

- **与其他混沌PRBG的关系**

  CCS-PRBG可以被看作是“混沌阈值序列”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起到阈值常数的作用。也可以将CCS-PRBG看作是两个互控的混沌PRBG。

- **基于扰动的实现**



图：基于扰动的CCS-PRBG数字化实现

基于CCS-PRBG的混沌流式密码

数字化CCS-PRBG的密码学特性

理论分析和实验结果都显示，数字化CCS-PRBG产生的比特流$\{k(i)\}$满足下述密码学特性：

- $\{0,1\}$上的平衡性：

  在满足上述约束条件R1)–R4)的情况下，可以近似严格地证明平衡性。

- 长循环周期：

  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。则$\{k(i)\}$的循环周期将为：

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

- 高线性复杂度(接近循环周期的一半)；类似$\delta(\cdot)$的自相关函数；接近0的互相关函数：有关约束条件暗示生成的混沌序列可以看成是一个(概念上的)i.i.d.序列。

尽管缺乏严格的证明，信息熵可能用来定性的描述这种可能性，实验结果也支持这里的结论。

- 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”，

  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。

基于CCS-PRBG的混沌流式密码

使用数字化CCS-PRBG构造流密码

- **几种基于CCS-PRBG的流密码例子**

  ✓**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。

  ✓**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$pn2(i) = pn1(i) \oplus 1$。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。

✓密码三

对于一些定义在$I = [0,1]$上的混沌映射，比如PWLCM，不变分布是均匀的。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左移操作。基于这样一个推广的CCS-PRBG，可以类似地构造速度更快的流密码。

- 安全性分析

✓CCS-PRBG本身的密码学特性是相关密码安全性的基本保障。

✓已知的攻击方法都不能对上述混沌密码进行直接推广。

✓互补密钥问题

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$k'(i) = \overline{k(i)}$。这会使密钥空间减少为原来的$1/2$。为了避免这个缺陷，建议使用不同的扰动PRNG或者扰动间隔，使用方程不同的两个混沌映射也可以解决这个问题。

表：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	$< a$

数字化混沌密码的设计：新思路

CCS-PRBG
↓
混沌流密码

→

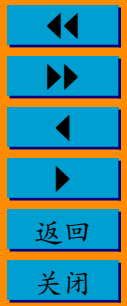
一种快速混沌流密码的新框架：
混沌流密码 + 混沌分组密码

(已有)数字化混沌密码的(安全性)分析与改进

Hong Zhou(周红) et al.'s	基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's	S. Papadi-mitrious et al.'s	Yen & Guo's：图象加密方法

数字化混沌系统的理论研究

逐段线性混沌映射(PWLCM)的一组动力学指标

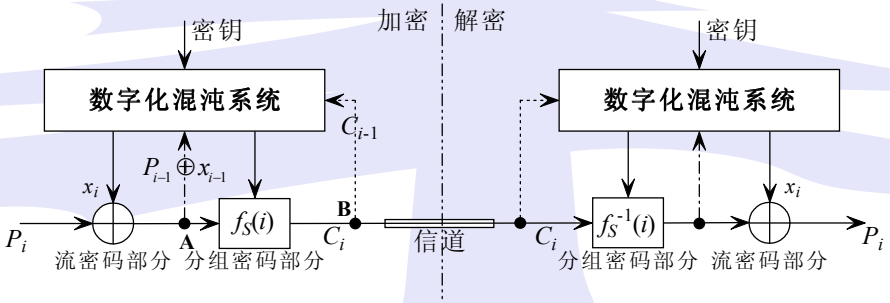


一种加密速度甚快的混沌加密新方法

设计思路的概念化描述

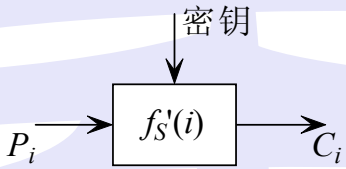
考虑如下问题：是否可能使用数字化混沌设计快速加密系统以解决实时视频加密中的问题？我们将研究一种设计混沌密码的新思路，该思路支持密钥的重用，并可以使得加密速度变得相当快。

- 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构成一个更为复杂的乘积密码系统。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)。一种视频混沌密码CVES的设计实践表明这样一种想法确实是可行的。

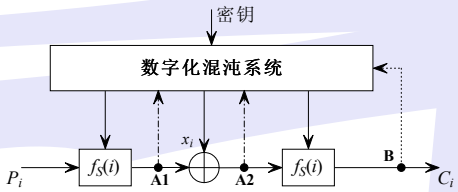


图：一种使用混沌设计密码的新思路

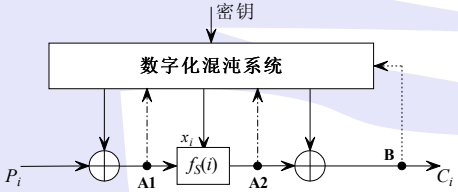
- 注意该密码模型中的内部反馈(和/或密文反馈)对于防止选择明文攻击是必要的。无反馈的版本可以简化为下述模型，在明文分组不够大的时候，对选择明文攻击敏感。



- 关于反馈有一个并非琐碎的问题：对于第一个明文，由于没有前导明文可用，f_S'还是固定的。因此需要引入一个初始向量(IV)解决这个问题：对于每个明文消息，开始的$N_p \cdot n$个比特随机产生并作为IV加密/解密第一个有意义的明文。
- 两种更为复杂的扩充模型



a) 扩充模型一



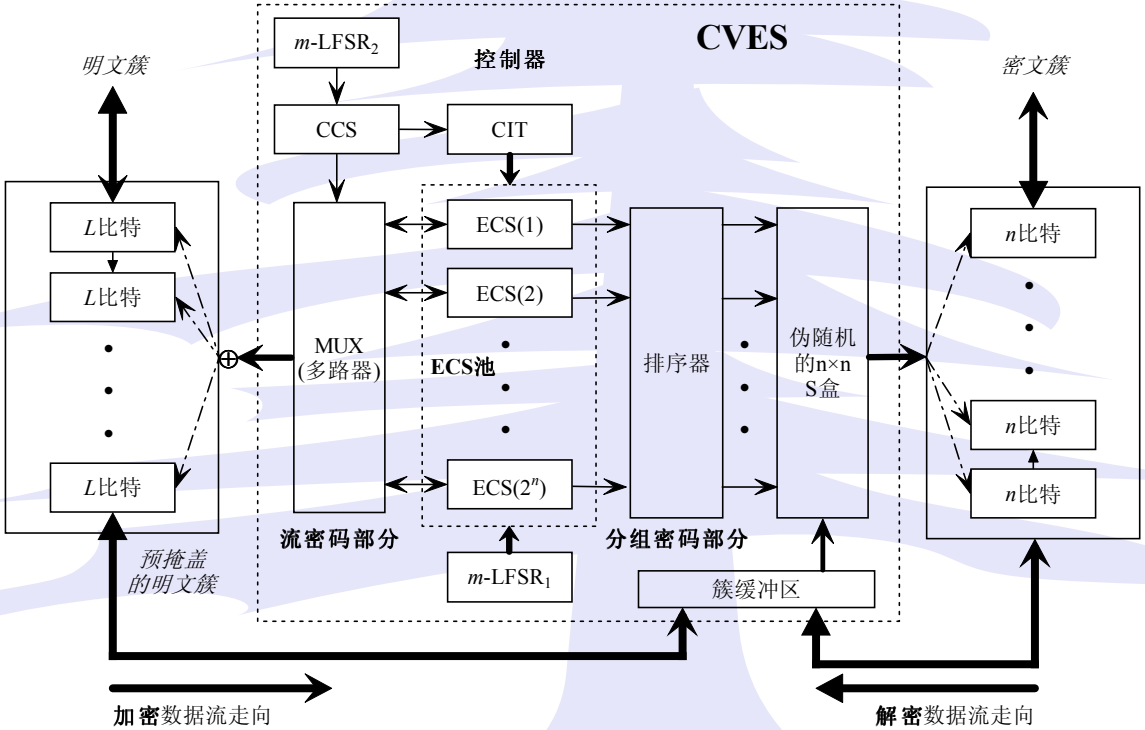
b) 扩充模型二

返回
关闭

一种加密速度甚快的混沌加密新方法

混沌视频加密方案 – CVES (Chaotic Video Encryption Scheme)

CVES如下图所示，它是我们提出的原始CVES(2002)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。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。为了使得加密速度进一步增加，可以考虑仅加密视频中的I-帧，而跳过P-帧和B-帧。

相关组件：

- **ECS池**：用于加密的2^n个混沌系统的统称。
- **CCS**：用于控制ECS初始条件、控制参数、扰动参数等相关配置和加密解密流程的混沌系统。
- **控制信息表(CIT)**：用来存储CVES需要的内部控制信息。CCS和CIT构成控制器单元。
- **流密码部分**：在CCS控制下，通过一个$2^n \times 1$的MUX(多路分配器)从ECS池中选择一个ECS对明文进行掩盖。
- **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。
- **簇缓冲区**：一个内存缓冲器用来临时存储当前簇和内部反馈变量。

一种加密速度甚快的混沌加密新方法

推广和配置CVES

- **推广CVES：支持密文视频随机检索的CVES(RRS-CVES)**

  在上面的CVES模型中，用于加密的混沌系统的初始条件和控制参数都是在初始化阶段确定的，在后续的加密解密过程中不再发生变化，这意味着密文视频的随机检索是不被支持的。

  对原方案进行如下的修改，可以增加随机检索功能(在可接受的最大检索延时之内)：

  ✓加入对ECS的定时复位功能：通过CCS产生伪随机的定时复位间隔和复位调整量，然后定时重置每个ECS到新的初始条件和控制参数。

  ✓加密过程中ECS的选取通过一张表产生，而不再由CCS的拟混沌轨道产生。该表在初始化阶段由CCS伪随机生成。

  上述两点使得由密文视频簇的位置重建每个ECS的当前状态成为可能。

- **配置CVES/RRS-CVES**

✓**使用的混沌系统**：建议使用PWLCM以获得最佳性能。

✓**基本参数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。

✓**基本参数n**：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$n = 8$。

✓**基本参数N_p**：这个参数是用来保证对选择明文攻击安全性的，我们建议$N_p \cdot L \geq 256$。

✓**基本参数–簇大小**：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。另外，簇大小可以用来调节加密速度。

一种加密速度甚快的混沌加密新方法

CVES的性能分析

- **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，硬件系统会比软件系统的运行速度快得多。不失一般性，假设全部ECS和CCS都是由PWLCM实现的，并且簇大小固定为$NC_{max} \cdot L$个比特。

  ✓**硬件实现**

  假设排序器消耗的一次排序时间为τ_s(时钟周期)，在时钟主频为f_b MHz的情况下，CVES加密速度大致为$f_b \Big/ \left(1 + \frac{1}{n} + \frac{\tau_s}{L \cdot NC_{max}}\right)$ Mbps。

  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**

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$1/L$。

在一个CPU为1.4GHz的奔腾®IV的台式机上，测试速度大约为83Mbps (1.4G/16 = 87.5Mbps)。有证据表明这个速度可以进一步优化。

✓**初始化耗时和RRS-CVES的最大检索延时**：计算表明它们都是毫秒级的，可以满足实际应用的需求。

- **安全性**

✓**基本的密码学特性**：平衡性和雪崩特性；

✓**避免潜在攻击的本质特征**

1. 时变的S盒同时依赖于混沌状态和以前的明文；
2. 簇大小一般太小不足以发现S盒可能存在的弱点；
3. 流密码部分由2^n个渐近独立的混沌映射(ECS池)构成，并且迭代顺序被另外一个独立的混沌映射(CCS)伪随机地控制；

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$K = \{x_c, p_c\}$。

✓**流密码部分的序列周期长度**的量级为：

$$2^{L_1+L_2} \cdot \mathrm{lcm}\left(\Delta_e(1), \cdots, \Delta_e(2^n), 2\right)。$$

✓**分组密码部分的伪随机S盒**是等概对称的。

- **实现复杂度**

在硬件实现情况下，最复杂的器件为除法器和排序器，所需的存储量仅为几十KB量级。一般情况下可以不必考虑对排序器进行复杂的优化设计和实现。

数字化混沌密码的研究展望

数字化混沌密码的设计：新思路

CCS-PRBG
↓
混沌流密码

→

一种快速混沌流密码的新框架：
混沌流密码 + 混沌分组密码

(已有)数字化混沌密码的(安全性)分析与改进

Hong Zhou(周红) et al.'s	基于搜索机制的：E. Alvarez et al.'s & M. S. Baptista's	S. Papadimitrious et al.'s	Yen & Guo's：图象加密方法

数字化混沌系统的理论研究

逐段线性混沌映射(PWLCM)的一组动力学指标

数字化混沌密码研究展望

- **设计好的混沌密码的一些建议**
  - 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。
  - 使用定点算法而不是浮点算法。
  - 使用最简单的混沌系统，比如逐段线性映射(PWLCM)。
  - 尽可能减少加密一个明文所需的混沌迭代次数。
  - 如果可能，使用多个混沌系统而不是单个混沌系统。
- **数字化混沌密码学中的开放话题**
  - 关于数字化混沌的理论
  - 由数字化混沌产生的不可预测的伪随机性。
  - 传统密码中的混沌现象。
  - 设计数字化混沌密码的通用模型。
  - 已知数字化混沌密码的分析。

Q & A: 评审人质询问题及回答

返回

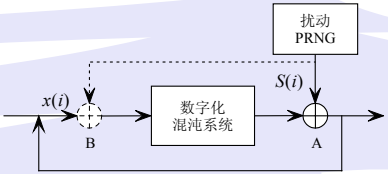
关闭

王育民教授质询问题

Q 混沌动力学系统数字化后都可用一般有限自动机描述，那么数字化混沌系统的退化问题与有限自动机的非异性研究能否结合起来?

A 使用有限自动机模型研究数字化混沌系统的研究已见报道，但是这样的研究一般需要对数字化混沌系统的空间离散化满足一定的条件，因此所研究的混沌系统比较局限，对二维Hamilton映射研究的较多。对于普通数字化混沌系统的推广似乎尚存在困难。

Q P51图形3-6的数字化混沌系统是一个有记忆的系统，可否从这点说明扰动方案A的混淆作用优于方案B。



A 应该可以，扰动方案A实际上是将扰动信号直接反馈到了输入端，这种反馈“记忆”效果应该有助于增加输出信号的复杂度并尽量保持混沌系统的特性。

殷勤业教授质询问题

Q 试说明目前数字化混沌密码在实际中的应用情况，分析数字化混沌密码在实际应用中的复杂程度和安全性。

A 目前数字化混沌密码尚未真正进入实用阶段，相关研究主要集中于理论研究和分析，虽然近年屡有实际系统开发出来，但是它们的安全性并未得到充分研究。一般而言，数字化混沌密码在实际应用中的实现还是比较简单的，尤其是其软件实现大都是非常简易的，当然其速度一般并不是太高。很多已经提出的数字化混沌密码被证实是不安全的，虽然近年有不少新的有希望的结构出现，但是还需要更多的细致研究证实其安全性。

徐健学教授质询问题

Q 关于数字化混沌系统的动力学性质退化的“动力学指标”的概念和理论只就分段线性系统提出，能否对一般一维映射给出定性的估计；例如对本论文第8、9章两种密码作出评价。

A 关于数字化逐段线性映射提出的“动力学指标”严格地依赖于定点数字化除法本身的算法特点，将相关概念和结论推广到其他混沌系统必须首先解决混沌方程的算法模型，这可能是一个非常困难的任务，将来我们将试图开展这方面的研究，尤其是要解决浮点算法的分析问题。本论文第8、9章中我们都建议采用逐段线性混沌映射以获得最佳性能，暂时可以将这个问题回避开。

Q P120提到“两混沌轨道相关性”，如何给定？引出时，未提到$F_1(x_1, p_1)$，$F_2(x_2, p_2)$之间的联系。(见§8.2.1定义)

A “两轨道相关性”在本文中没有使用严格的定义加以约束，而只是用来定性的描述两个混沌轨道之间可能存在的联系，如两个混沌轨道的初始条件之间的已知差异。引出CCS-PRBG的定义时，确实未提到两个混沌系统之间的联系，实际上它们之间的联系是比较弱的，只受后面给出的条件R1)–R4)约束。

Q P.118，$k(i)$与$g(x_1(i), x_2(i))$之间的联系有待指明；P.37，2、6、10行$[0, p) \cap S_n$和$[0, p) \cup S_n$有待阐明。

A P.118，$k(i) = g(x_1(i), x_2(i))$；P.37的$[0, p) \cup S_n$是本人的笔误，应当为$[0, p) \cap S_n$。

Q P.36-49式$P_j(F(x)) \neq 1/2^j$中的不等号可否以大于或小于号代替?

A 虽然有迹象表明$P_j(F(x)) > 1/2^j$是可能成立的，但是对于多次复合映射而言，确实存在$P_j(F^k(x)) < 1/2^j$，因此从严格的角度出发，我们还是采用$P_j(F(x)) \neq 1/2^j$说明$F(x)$的分布不均匀性。

返回
关闭

陈关荣教授质询问题

Q (在CVES视频加密算法中)，图象或帧幅加密后，体积增大了多少？普通混沌图象加密后的ciphertext比原来的plaintext体积增加了10～30%不等。

A 采用“先加密后压缩”模式的混沌图象加密算法，由于加密带来的信息冗余度减小，必然会造成密文图象压缩率降低；采用“联合加密压缩”模式的混沌图象加密算法，一般也存在影响压缩效率的问题。我们提出的CVES的工作模式是“先压缩后加密”，应当不会影响每个加密帧的体积。

黄国和副教授质询问题

Q 在§3.2.2，相关引理的证明基于下述假设：n是奇数。如果n是偶数的话情况如何？

A n是偶数的话，引理3.3将不成立，因为2^i将不再是$(\mathbb{Z}_n, +)$的生成元。但是这并不影响后文相关结论的推导。

Q 文献[126]和[127]是否是同一篇文章？

A 不是，论文送审时文献[126]尚未出版，因此相关信息缺失。