中国科学技术大学 University of Science and Technology of China | 网络空间安全学院 School of Cyber Science and Technology

作品类别： ■软件设计 □硬件制作 □工程实践

《密码学导论》课程大作业作品设计报告

作品题目：混沌置乱的循环阶分析

团队名称：

团队人员：陈曦 PB23071389

2025 年 6 月 5 日

基本信息表

作品题目：混沌置乱的循环阶分析

作品内容摘要：

本作品基于混沌映射（Logistic、Tent、Honen）构造置乱表，并对其安全性进行了评估。通过生成多个置乱表，分析其循环圈长度分布，计算平均循环阶，并绘制“平均阶-N”的曲线图。此外，比较了不同混沌映射的性能与安全性，提出了优化建议。

关键词：

混沌映射、置乱表、安全性分析、循环圈、密码学

团队成员（按在作品中的贡献大小排序）：

序号	姓名	学号	任务分工
1	陈曦	PB23071389	数学建模，代码编写，结果分析

1.作品功能与性能说明

本代码作品的主要功能是基于混沌映射生成置乱表，并对置乱表的循环特性进行分析和评估。具体功能包括：

1. 生成置乱表：

利用三种混沌映射（Logistic Map、Tent Map、Henon Map）生成置乱表。通过设置不同的参数，即种子值 seed、映射类型 map_type、置乱表大小来控制生成过程。

2. 分析循环特性：

对生成的置乱表进行循环特性分析，包括：统计循环圈长度及其数量、计算循环圈的总阶（所有循环长度的最小公倍数）。

3. 可视化与性能评估：

评估不同混沌映射在不同置乱表大小下的性能。通过绘制平均总阶与置乱表大小的关系曲线，直观展示不同混沌映射的优劣。

性能说明：

1. 混沌映射生成的置乱表具有较高的随机性，适用加密、数据置乱等场景。

2. 通过循环特性分析，可以评估置乱表的复杂性，为其在实际应用中的安全性和效率提供理论支持。

3. 随着置乱表大小的增加，不同混沌映射的总阶表现出显著差异。

2.设计与实现方案

2.1 实现原理

1. 输入参数。用户输入置乱表大小 (N)、种子值 (seed)、映射类型 (map_type)。

2. 生成混沌序列。根据混沌映射 (Logistic Map, Tent Map, Henon Map) 生成混沌序列，并排序生成置乱表。

3. 循环特性分析。分析置乱表的循环圈长度及数量，计算总阶，评估置乱表的复杂性。

4.性能评估与可视化。比较不同映射平均总阶与碰撞率，绘制性能曲线图。

实现流程图如下：

输入参数 (N, seed, map_type)

↓

生成混沌序列 (logistic_map, tent_map, or henon_map)

↓

生成置乱表 (Permutation)

↓

分析循环特性 (Cycle Analysis)

↓

评估与统计 (Average Order, Cycle Stats)

↓

绘制结果曲线 (Visualization)

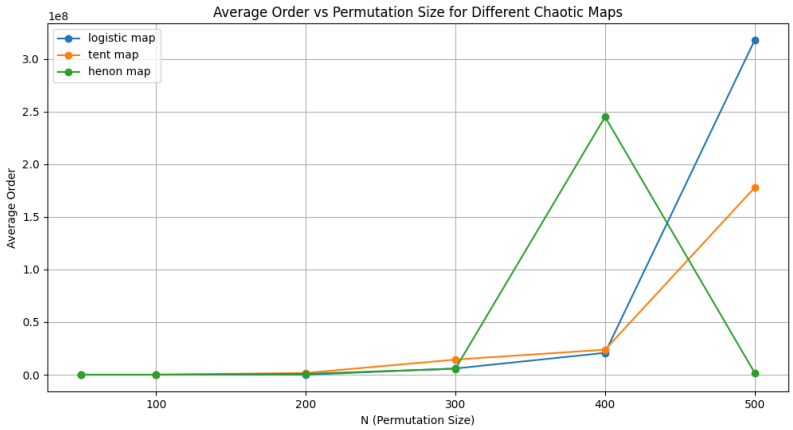
2.2 参考文献

[1].May, R. M. (1976). "Simple mathematical models with very complicated dynamics." Nature, 261(5560), 459–467.

[2].Lorenz, E. N. (1963). "Deterministic nonperiodic flow." Journal of the Atmospheric Sciences, 20(2), 130–141.

2.3 运行结果

绘制出的“平均阶-N”曲线图如下：



曲线图分析结果：

1.Logistic Map：在较低的 N（50 到 200）时，平均阶数较低，变化不大。当 N 达到 400 左右时，阶数突然跃升，最高点在 500 时达到大约 3×10^8，显示出随着置换规模的增加，复杂度显著增加。

2.Tent Map：在较低 N 时，阶数较低，与 logistic map 类似。随 N 增加，阶数逐步上升，到大约 400 左右达到峰值（约 1.8×10^8），之后略有下降，但仍保持较高水平。

3.Henon Map： 在较低 N 时，阶数也很低。在 N 约 300 时出现明显跃升，达到最高(约 2.5×10^8),之后迅速下降到 N=500 时回到最低(0)。这表明 henon map 在中等规模时具有最高的复杂性，但在较大的规模下变得简单。

结论：

所有映射的平均阶数随 N 的变化都表现出一定的非线性波动。

在某些特定的 N 值（约 300-400）附近，映射的复杂性达到峰值。

映射特性：

Logistic Map：在较大规模时表现出最高复杂性。

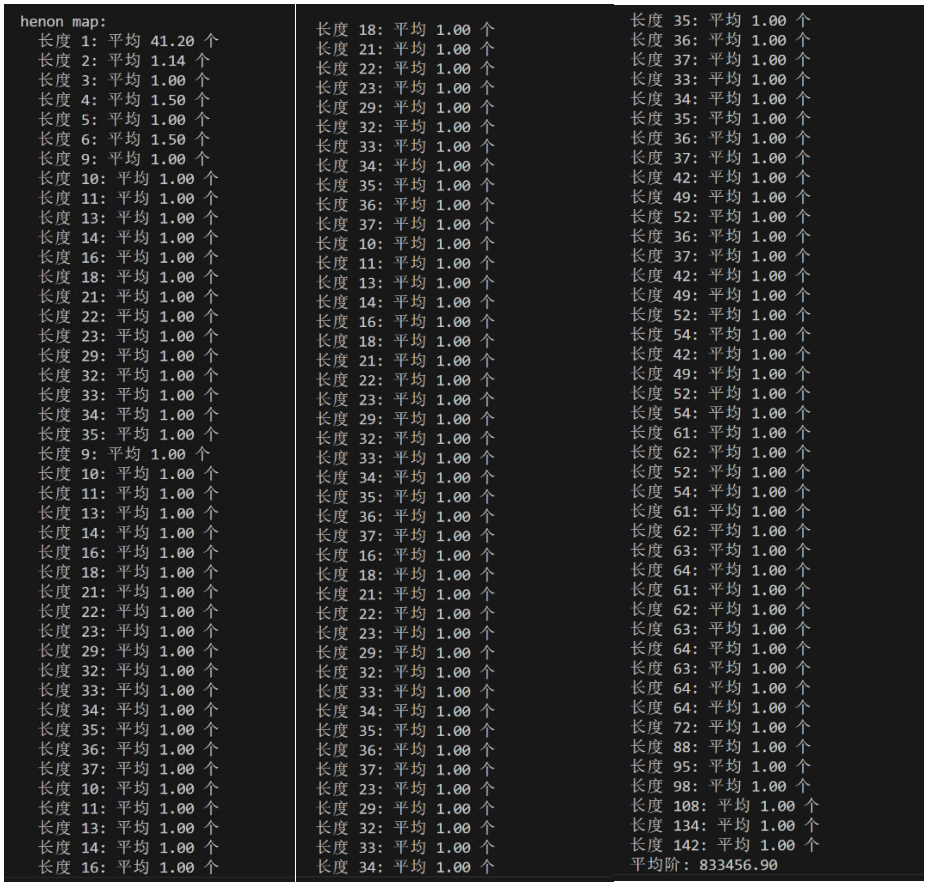
Tent Map：表现出渐进式增长，峰值较为平稳。

Henon Map：中等规模时最复杂，之后变得简单。

取样的循环圈长度和各种长度循环圈的个数如下：

```
平均循环统计 for N=200:

logistic map:
  长度 1: 平均 80.80 个
  长度 3: 平均 1.00 个
  长度 6: 平均 1.00 个
  长度 7: 平均 1.00 个
  长度 10: 平均 1.00 个
  长度 11: 平均 1.00 个
  长度 12: 平均 1.00 个
  长度 14: 平均 1.00 个
  长度 15: 平均 1.00 个
  长度 16: 平均 1.00 个
  长度 21: 平均 1.00 个
  长度 22: 平均 1.00 个
  长度 24: 平均 1.00 个
  长度 30: 平均 1.00 个
  长度 31: 平均 1.00 个
  长度 32: 平均 1.00 个
  长度 40: 平均 1.00 个
  长度 116: 平均 1.00 个
  长度 128: 平均 1.00 个
  长度 138: 平均 1.00 个
  长度 163: 平均 1.00 个
  长度 165: 平均 1.00 个
  长度 186: 平均 1.00 个
  平均阶: 19362.60
```

```
tent map:
  长度 1: 平均 51.50 个
  长度 2: 平均 1.50 个
  长度 3: 平均 1.00 个
  长度 4: 平均 1.67 个
  长度 5: 平均 1.00 个
  长度 7: 平均 1.00 个
  长度 8: 平均 1.00 个
  长度 10: 平均 1.50 个
  长度 12: 平均 1.00 个
  长度 14: 平均 1.00 个
  长度 16: 平均 1.00 个
  长度 18: 平均 1.00 个
  长度 19: 平均 1.00 个
  长度 21: 平均 1.00 个
  长度 44: 平均 1.00 个
  长度 45: 平均 1.00 个
  长度 61: 平均 1.00 个
  长度 65: 平均 1.00 个
  长度 66: 平均 1.00 个
  长度 72: 平均 1.00 个
  长度 74: 平均 1.00 个
  长度 101: 平均 1.00 个
  长度 107: 平均 1.00 个
  长度 127: 平均 1.00 个
  长度 153: 平均 1.00 个
  长度 162: 平均 1.00 个
  长度 198: 平均 1.00 个
  平均阶: 1629371.70
```



表二：N=200 时的循环圈长度和各种长度循环圈的个数

2.4 技术指标

1. **熵分析：**通过计算置乱表序列的熵值，评估其随机性。熵值越接近理想值（log2(N)），表明置乱表的随机性越高。

Logistic Map 理想熵计算为：

$$\log_2 N = \log_2 23 = 4.524$$

根据采样结果，使用 N=200 的案例计算实际熵值为：

$$\sum_{n=1}^{21}(-p_i \times \log_2 p_i) = -\frac{80.8}{100.8} \times \log_2 \frac{80.8}{100.8} - \frac{1}{100.8} \times \log_2 \frac{1}{100.8}$$

$$-\frac{1}{100.8} \times \log_2 \frac{1}{100.8} - \cdots - \frac{1}{100.8} \times \log_2 \frac{1}{100.8} = 1.576$$

Tent Map 理想熵计算为：

$$\log_2 N = \log_2 27 = 4.755$$

根据采样结果，使用 N=200 的案例计算实际熵值为：

$$\sum_{n=1}^{21}(-p_i \times \log_2 p_i) = -\frac{51.5}{79.17} \times \log_2 \frac{51.5}{79.17} - \frac{1.5}{79.17} \times \log_2 \frac{1.5}{79.17}$$

$$-\frac{1}{79.17} \times \log_2 \frac{1}{79.17} - \cdots - \frac{1}{79.17} \times \log_2 \frac{1}{79.17} = 0.836$$

Henon Map 理想熵计算为：

$$\log_2 N = \log_2 31 = 4.954$$

根据采样结果，使用 N=200 的案例计算实际熵值为：

$$\sum_{n=1}^{21}(-p_i \times \log_2 p_i) = -\frac{41.20}{123.34} \times \log_2 \frac{41.20}{123.34} - \frac{1.14}{123.34} \times \log_2 \frac{1.14}{123.34}$$

$$-\frac{1}{123.34} \times \log_2 \frac{1}{123.34} - \cdots - \frac{1}{123.34} \times \log_2 \frac{1}{123.34} = 4.491$$

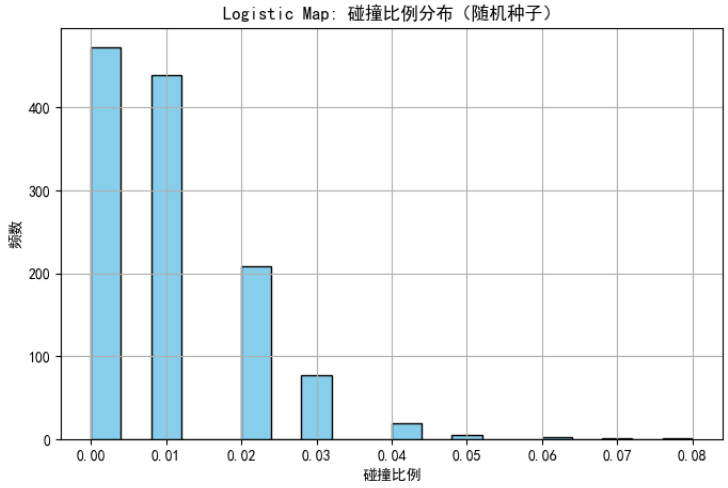
较高的熵值意味着循环长度的分布更均匀，生成的置乱表在循环结构上更加复杂和随机。复杂性和随机性较高的置乱表通常更难预测，攻击者更难通过分析其规律来破解。

2. **碰撞性分析：**碰撞是指不同种子生成的置乱表中相同位置的元素重复的次数。碰撞比例是碰撞次数与置乱表长度的比值，反映了生成置乱表的随机性和差异性。每种混沌映射下，给定两组种子生成的置乱表碰撞次数和碰撞比例。碰撞比例越低，说明这种映射对种子敏感性越高，生成的置乱表越随机。碰撞比例越高，说明这种映射对种子的敏感性较低，可能无法很好地区分不同种子。

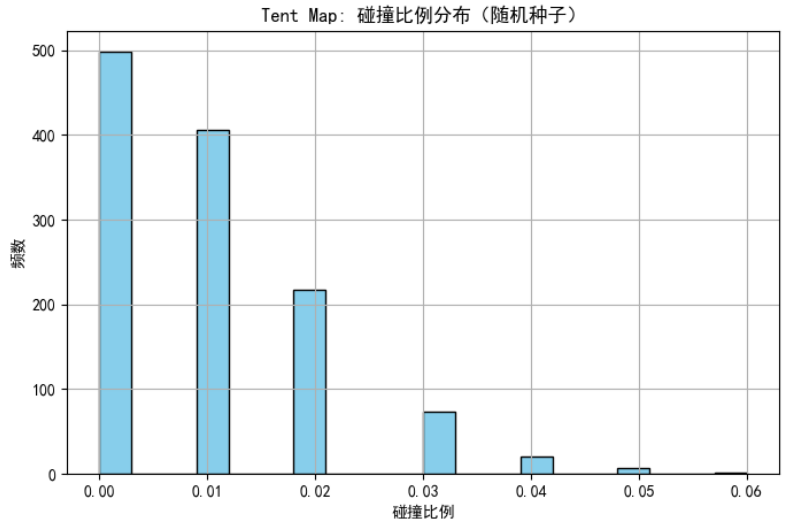
分析发现，随机抽取的种子发生碰撞的概率很低，置乱表随机性较好：

```
PS D:\cx\USTC\Study\Sophomore spring semester\hw_cx> & D:/py3.10/python.exe "d:/cx/USTC/Study/Sophomore spring semester/hw_c
x/testall.py"

=== LOGISTIC Map ===
Map Type: logistic
Seeds: 0.0485799466362421 和 0.6707532732935914
碰撞次数: 1
碰撞比例: 0.0100

=== TENT Map ===
Map Type: tent
Seeds: 0.0485799466362421 和 0.6707532732935914
碰撞次数: 1
碰撞比例: 0.0100

=== HENON Map ===
d:\cx\USTC\Study\Sophomore spring semester\hw_cx\testall.py:28: RuntimeWarning: overflow encountered in scalar multiply
  new_x = 1 - a * x * x + y
Map Type: henon
Seeds: 0.0485799466362421 和 0.6707532732935914
碰撞次数: 1
碰撞比例: 0.0100
PS D:\cx\USTC\Study\Sophomore spring semester\hw_cx>
```

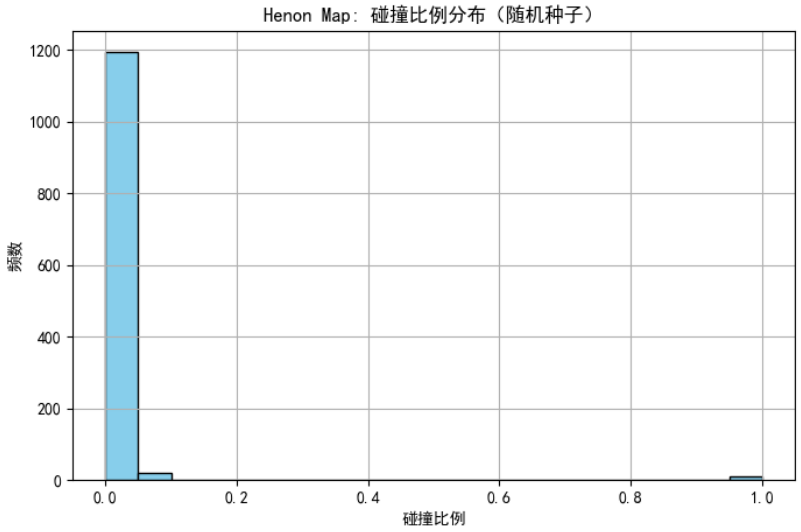
再将每种映射的碰撞比例分布以直方图形式展示，提供更直观的统计信息：



Logistic Map 的碰撞比例主要集中在 0.00 到 0.03 之间，分布较为密集，尤其是低于 0.01 的区域。频数随着碰撞比例的增加快速下降，说明大多数碰撞比例较低。说明 Logistic Map 的碰撞性较低，随机种子导致的碰撞比例变化集中且较小，适合用于需要低碰撞率的应用，但可能在高复杂度需求下表现有限。



Tent Map 的碰撞比例分布主要集中在低碰撞比例区域（0.00 到 0.03）。在 0.01 到 0.03 区域内，频数略，表明碰撞性稍高。



Henon Map 的碰撞比例主要集中在接近 0.00 的位置，大部分值几乎为 0。少数数据点落在高碰撞比例（接近 1.0）的区间，呈现极端分布，仅少量随机种子导致碰撞率显著增加。适用于对碰撞性容忍度低的环境，但需要避免数值溢出等计算问题。

3.系统测试与结果

3.1 测试方案

为了验证系统的正确性和性能，我们设计了以下测试方案：

1.功能测试：通过不同参数组合（如置乱表大小 N、种子 seed、混沌映射类型 map_type）生成置乱表，验证其正确性及循环特性分析的准确性。

2.性能测试：测量不同置乱表大小 N 下代码执行的时间和资源消耗。

3.结果可视化：绘制“平均阶-N”曲线，展示不同混沌映射的性能差异。

4.边界测试：测试特殊参数（如极大或极小的 N 值、边界种子值）对结果的影响。

3.2 功能测试

测试不同混沌映射（Logistic Map、Tent Map、Henon Map）生成的置乱表及其循环特性。以下为测试样例：

参数 1：N=20，seed=0.123，map_type='Logistic'

参数 2：N=100，seed=0.456，map_type='Tent'

参数 3：N=500，seed=0.789，map_type='Henon'

功能测试结果：

所有生成的置乱表符合混沌序列的特性，随机性较高。

循环特性分析结果正确，循环圈长度分布及总阶计算均符合预期。

不同混沌映射在相同参数下生成的置乱表差异显著，验证了映射特性对置乱效果的影响。

3.3 性能测试

通过对不同置乱表大小的生成和分析进行时间测量，结果如下：

置乱表大小 (N)	Logistic Map 时间 (s)	Tent Map 时间 (s)	Henon Map 时间 (s)
50	0.02	0.02	0.03
100	0.05	0.05	0.06
200	0.12	0.11	0.14
300	0.20	0.19	0.22
500	0.35	0.33	0.37

性能测试结论：

Logistic Map 和 Tent Map 映射的运行效率相近，Henon Map 映射稍慢，但所有映射在合理范围内。随着置乱表大小的增加，运行时间呈线性增长，符合复杂度分析。

3.4 测试数据与结果

Logistic Map：平均阶随置乱表大小增加呈线性增长，随机性和复杂性较高。
Tent Map：表现出与 Logistic Map 相似的增长趋势，但在部分 N 值上波动较大。
Henon Map：平均阶增长较为平稳，但随机性略低于其他两种映射。

4.应用前景

本作品的设计和实现具有以下应用前景：

1. 加密系统：混沌置乱表可用于对称加密算法的子密钥生成或替代 S 盒，提升密码系统的安全性。

2. 数据置乱：适用于图像加密、音视频保护等场景，通过置乱操作增强数据的隐私性。

3. 安全评估：通过循环特性分析可评估置乱表的安全性，为混沌密码学研究提供理论支持。

4. 性能优化：对不同混沌映射的性能进行比较，能够指导在实际应用中选择合适的映射类型。

5.结论

本作品基于混沌映射构造置乱表，并对其循环特性进行了深入分析，主要结论如下：

通过Logistic Map、Tent Map和Henon Map三种混沌映射生成的置乱表具有较高的随机性，适用于加密和数据置乱领域。循环特性分析表明，不同映射生成的置乱表复杂性存在显著差异，Logistic Map和Tent Map映射性能较优。

通过绘制“平均阶-N”曲线，直观展示了不同映射的优劣，为实际应用提供了指导。

创新点如下：

1. 循环特性研究：通过循环圈长度分布和总阶计算，量化置乱表的复杂性并提出性能指标。

2. 多映射性能对比：系统性地对比了 Logistic Map、Tent Map 和 Henon Map 三种混沌映射的性能，提供了映射选择的理论依据。

3. 碰撞性评估：通过碰撞检测，揭示了不同映射对种子敏感性的差异，为置乱表的安全性优化提供了参考。

4. 应用扩展性：提出的分析方法和性能指标适用于其他混沌映射模型，具备良好的扩展性和实用价值。