混沌置乱的循环阶分析——报告

基本信息

代码提交至GitHub
lqh1106/Chaotic_Scrambling (github.com)

作者

林琦皓 PB22051003

作品题目

混沌置乱的循环阶分析

作品内容摘要

本文介绍了一种基于 Logistic、Circle 和 Chebyshev 三种混沌体系的加密程序，并对其性能进行了详细分析和比较。混沌置乱是一种利用混沌系统的非线性特性和随机性质来加密数据的方法，其具有很高的安全性和不可预测性。本文针对 Logistic、Circle 和 Chebyshev 三种不同的混沌映射函数，设计了相应的加密算法，并对它们进行了性能测试和比较。

在本研究中，我们首先实现了基于Logistic、Circle 和 Chebyshev 混沌置乱基本原理和算法流程。实现了：

1. 输入明文，加密方式选择和密钥输出密文
2. 输入密文，加密方式选择和密钥输出明文

随后，我们设计了基于这三种方法的数据加密程序，并分别对它们的性能进行了测试和分析。具体而言，我们对以下几个方面进行了评估和比较：

1. **加密速度**：我们对不同大小的数据进行了加密和解密测试，并记录了程序的运行时间。结果显示，不同的混沌置乱方法在加密速度上有所差异。有些方法可能更适合于大规模数据的加密，而有些可能更适合于实时加密需求。
2. **置乱强度**：通过统计学分析和混沌特性测试，我们评估了不同方法对数据的置乱效果。置乱的效果采用平均阶来衡量。结果表明，每种混沌置乱方法都能有效地增强数据的随机性和混乱性，但它们的置乱效果可能有所不同。
3. **加密效果**：我们对加密后的数据进行了安全性评估，并与其他加密方法进行了比较。通过加密结果的质量和安全性分析，我们得出了每种方法的加密效果，并对其优缺点进行了总结。

最后，我们对 Logistic、Circle 和 Chebyshev 三种混沌置乱方法的性能进行了综合比较，并提出了针对不同应用场景的建议。本研究为混沌置乱加密方法的选择和优化提供了重要参考，并为信息安全领域的混沌加密研究提供了新的思路和方法。

关键词

混沌、循环圈、阶、时间复杂度、置乱

作品功能与性能说明

作品整体分为两部分：1.简便可用的基于混沌加密的程序，2.使用平均阶等指标评估混沌加密置乱的系统性能。以下是详细介绍：

在加密程序方面，作品开发了一个图形化界面，可接受明/密文，密钥和加密方式，输出加/解密结果，加密方式采用混沌置乱，由密钥和明文唯一确定加密，具有良好的加密效果。亦可在短时间内完成对长文本的加密

在效果评估方面，作品实现了对三种混沌体系： Logistic、Circle 和 Chebyshev的横向评估。
1.使用主流的对置乱表的平均阶-N的测量来评估加密效果，通过较大的数据量来避免误差的出现
2.在作者本人使用的电脑下对加密置乱的计算时间做比较，得出了加密长度N与加密时间t在三种混沌算法下的区别
3.对置乱表对种子变换的灵敏度作比较，得出了三种混沌映射对种子细微变换反应的灵敏度

通过这三项评估，获得了三种混沌算法的在不同方面的优缺点，基于此提出各个加密算法的具体应用

设计与实现方案

实现原理

混沌置乱的数学原理

混沌系统中的三种常见模型：Logistic映射、Circle映射和Chebyshev映射的数学原理。

1. **Logistic映射**： Logistic映射是一种常见的混沌动力系统，其数学原理如下： Logistic映射是一维离散动力系统，通常用来模拟人口增长或其他动态系统中的非线性行为。其迭代方程通常表示为：

   $$x_{n+1} = r \cdot x_n \cdot (1 - x_n)$$

   其中，(x_n) 是第 (n) 次迭代的状态，(r) 是一个控制参数，通常在区间 ([0, 4]) 内取值。当 (r) 取不同的值时，系统的行为会发生变化，包括周期性、混沌性等。
2. **Circle映射**： Circle映射是另一种混沌动力系统，其数学原理如下： Circle映射描述了二维相空间中的动力系统。其迭代方程通常表示为：

   $$x_{n+1} = mod(x_n + b - \frac{a}{2\pi}\sin(2\pi x_n), 1)$$

   其中，(x_n) 和 (y_n) 是第 (n) 次迭代的状态，a 和 b是控制参数。Circle映射可以产生丰富的动力学行为，包括周期轨道和混沌轨道。
3. **Chebyshev映射**： Chebyshev映射也是一种常见的混沌动力系统，其数学原理如下： Chebyshev映射是由切比雪夫多项式定义的二维动力系统。其迭代方程通常表示为：

   $$x_{n+1} = \cos(a \cdot cos^{-1}(x_n))$$

   其中，(x_n) 是第 (n) 次迭代的状态，a是控制参数。Chebyshev映射的特点是其动力学行为对初始条件高度敏感，导致复杂的混沌轨道。

基于混沌体系的加密

混沌置乱的基本原理是利用混沌系统的敏感性依赖于初始条件和参数的微小变化这一特性，使得在初始条件或参数稍有不同的情况下，系统轨迹将会有显著的差异。通过合适的混沌映射或者混沌序列生成算法，可以产生具有高度随机性和不可预测性的序列，这些序列可以用作加密算法中的密钥，或者直接应用于数据置乱过程中。

基于该混沌系统，将输出的x序列按数值大小排序，并将排序前后的位次分别作为置乱表的索引和值，将明文根据该表进行置乱得出密文

对置乱的性能分析

σ为置乱表的数学表示,为对称群
σ中的任何一个置换可写成两两不相交轮换制积，不计较次序 （与1-轮换）唯一,即

$$\sigma = \prod_{i=1}^{n} \sigma_i$$

对每个轮换，其长度即为该轮换的阶，即

$$\sigma_i^{len(\sigma_i)} = \sigma_i$$

易得到对置乱σ，其分解处轮换的长度的阶的最小公倍数即为该置乱的阶
一定程度上，置乱的阶反应了该置乱在密码学领域的性能

在对不同混沌体系产生置乱表的性能分析上，对50-1000的每个置乱长度，使用python中的random函数产生一千个种子，对应计算出置乱表并求出该置乱的阶。得到该置乱长度下置乱表的阶和加密时间的平均值

运行结果

在功能上，实现了对任意长文本的置乱加密，使用密钥对该文本进行唯一加密，在确保密钥不泄露的情况下实现了较高程度的加密强度和安全性

系统测试与结果

方案

功能测试

随机生成中英文文本，输入加密程序的图形化界面，选定种子和加密方式，获得密文输出
将步骤一生成的密文与生成该密文的映射选择以及种子输入程序，获得输出
比对输出和初始明文，若两者相同则证明该程序实现了相应功能

对程序的三种映射都采用相同的方式测试

性能测试

对**Logistic映射**，取a=3.60
对**Circle映射**，取a=0.50，b=0.20
对**Chebyshev映射**，取a=4.00

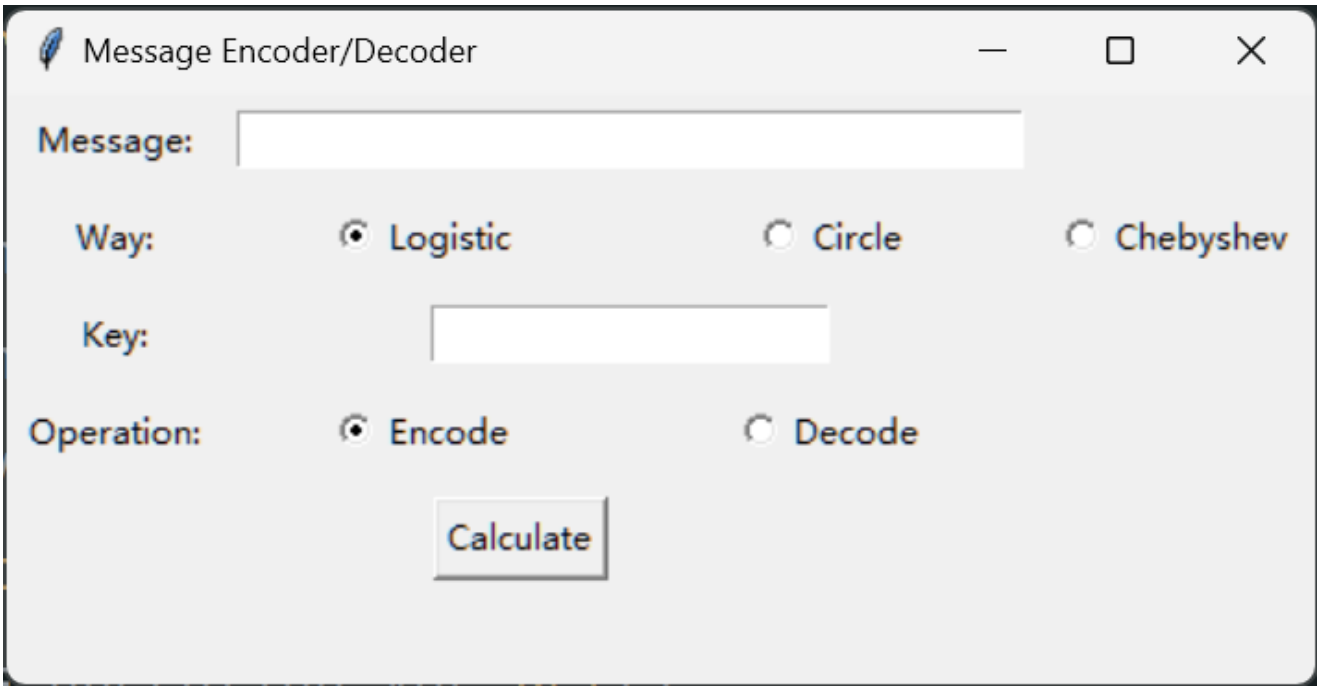
置乱时先对种子取1000次混沌递归，后生成置乱长度个数值，将这一千个数字按大小排序，将排序前后的位次视作置乱表
对50-1000的每个置乱长度，使用python中的random函数产生一千个种子，对应计算出置乱表并求出该置乱的阶。得到该置乱长度下置乱表的阶和加密时间的平均值

对对50-1000的每个置乱长度，使用python中的random函数产生一千个x0，先取delta=0.25，后不断计算种子为x0和x0+delta 下的置乱，若置乱表不同，则delta=delta/2；若两次置乱表相同，则将此时的delta视作这种混沌置乱灵敏度的下界

以置乱表的阶，置乱时间，置乱灵敏度作为评价给定置乱长度N下置乱表的性能。

功能测试

加密的图形化界面如下，
输入明/密文
选择加密方式，设定种子，选定加解密操作
支持将输出的密/明文直接粘贴到剪切板上



以下是输入输出示例
输入：
In the heart of a bustling city, there was a small bookstore tucked away on a quiet street. It was owned by an elderly man named Mr. Thompson, who had spent his entire life surrounded by books. Despite the rise of digital technology, Mr. Thompson's bookstore remained a beloved sanctuary for book lovers of all ages.

One rainy afternoon, a young girl named Emily stumbled upon the bookstore while seeking shelter from the storm. She was captivated by the rows of dusty bookshelves and the cozy atmosphere of the store. As she browsed through the shelves, her eyes fell upon a worn copy of her favorite childhood book, "The Secret Garden."

Unable to resist, Emily picked up the book and began to read. Lost in the enchanting world of the story, she felt a sense of nostalgia wash over her. Suddenly, she heard a gentle voice behind her.

"Ah, 'The Secret Garden,'" said Mr. Thompson, smiling warmly. "A timeless classic, isn't it?"

Emily nodded, her cheeks flushing with embarrassment at being caught engrossed in the book. But Mr. Thompson only chuckled and gestured for her to sit down by the fireplace.

For the rest of the afternoon, Emily and Mr. Thompson talked about their favorite books, sharing stories and recommendations with each other. Despite their differences in age and background, they discovered a shared passion for literature that bridged the gap between them.

As the rain continued to pour outside, Emily realized that she had found not just a bookstore, but a home away from home. And Mr. Thompson, in turn, found a kindred spirit in the young girl who reminded him of his own love for books.

From that day on, Emily became a regular visitor to the bookstore, spending hours lost in the pages of her favorite stories. And with each visit, she grew closer to Mr. Thompson, who

became not just a mentor, but a dear friend.

In the end, it wasn't just the books that brought Emily back to the bookstore time and time again. It was the sense of belonging, the warmth of human connection, and the magic of discovering new worlds within the pages of a book. And as she stepped out into the rain, she knew that she would always carry a piece of the bookstore – and Mr. Thompson – in her heart wherever she went.

选定种子为0.5，采用logistic映射，操作设为加密encode
输出密文：
ioolrsnaM oTtk acecf gashndteorwnaoh rAo nhrptetbu ooonoatltoor t e.beto engs T eelretda hlmrle wE c ueeh n ifl g et airs,notidesero gnlo mssudnanrorrerelfyh hbcrn wsnhoefwoy,ahed yebrhii ,sisoet vmuitrs kpphahtlerr ne gimreusceAlg .fofb o geamc rteusfeeo eeuiept hr i hiooeiiAedM mve n eodemke na erworSvacbbwMe hdsl y ws loiilh.swhsub ettki. e hotrris ogtoEsoOnn dos ua te e rfm srodw.afp t sftydk yerlne,dtri nd.esnma br icnt dsawh dTaraa B ry.eeo"clkgimn ipmboea,bt ns olmeenaahodhee e, aae rrdnhftorrevrtfiaiitro,ubmdlombohhberdsshp io,sranv.aek k'trki"n hal–he Melf,aoi aiogIttMaootrsak erorAp D?pwoTn tlww hro etlec, ns e A t teddwheao e muo bnlawlaad. eaT e,hetEa hd sutobatih heayT an.oilv ifn ooudrhe ah enii npt dfvibtna nSftjobehhrmuaT g ' heoyhtm ew tt.ecgoascsts ry h..lttetfmo dya.todegapty oonot ie myeta f hcbpa h nsbwhreuorpdortv tv kttlgtoikiafmtl w qtret ace dssorwhae hal ri tnner hta,sn aitohccmon cdc wntn cd bn nehsz ane,.noagip,Me tnoreesou sheatsr dl uiroh sn n o n retdvhohyot r oA nev ttGe s ,ttko bif aok,miemn did,naE ondcAhz v i.iose.a egs,k htnondehdgrbnh ssdodo "inard hrnehetuurpohob e t deocs rn,knhv ustohid ot,nfr rttht n iahisfeieiadcbomjefes iscdtee yesrobse.h dm n otemeidiktmetr ,n eome .da eaara thitemd an ce di yaesrr erht ewepnnhetashia e t eoptepnhnaincso soifF mooohus sekte sm dsdoamsrl yhdo bsfwetsm nmn arnledfaacr isrttybcsauoeiwleaernse pts tatftlntdoe hootger sf orwea h nelmihnmpwntgt nhTrnbbmwo hyaedtewes r ptoth sj siddr h cng. cedenmweohroa,b stneh hcennbuai, dyf hns ci rrsets ulai l mt ts.eoMry w e o csunmptlo d tr yl r sga.scr l,eoggkaevernbe,utk eoh stf Etere Sslaisa o eaheit in ok.hG nsndedv dostbedroitouureeu y ht emeeoEono.e' tslod p ge"egTohaersU geb gy oa braigso nntaibgltollsouh neouro okfi rdhynae, s.kpesue.de"sinh.nkeaihteevnmdo'shy a T rtoa sans lfb, nseg t gb uSddephoEletne dsorn ns tkmhLctw, yewy ohmtgr,hocgoatDsofa phneped hoeri rsehwostueahoem orert tssoto oolafh fidegh tl–ohtegns orr ei niee csslopreheanor oetu ofoailthoeprlrihey Muwsshaaeliroise hgnset le.lceiisewnihoailr nukasysir kst hal eei ooittet ilaaetieb"Fyo yhi uit eut a.o mshoo' if u rsb ,
将密文输入
选定种子为0.5，采用logistic映射，操作设为解密decode
输出明文
In the heart of a bustling city, there was a small bookstore tucked away on a quiet street. It was owned by an elderly man named Mr. Thompson, who had spent his entire life surrounded by books. Despite the rise of digital technology, Mr. Thompson's bookstore remained a beloved sanctuary for book lovers of all ages.One rainy afternoon, a young girl named Emily stumbled upon the bookstore while seeking shelter from the storm. She was captivated by the rows of dusty bookshelves and the cozy atmosphere of the store. As she browsed through the shelves, her eyes fell upon a worn copy of her favorite childhood book, "The Secret Garden."Unable to resist, Emily picked up the book and began to read. Lost in

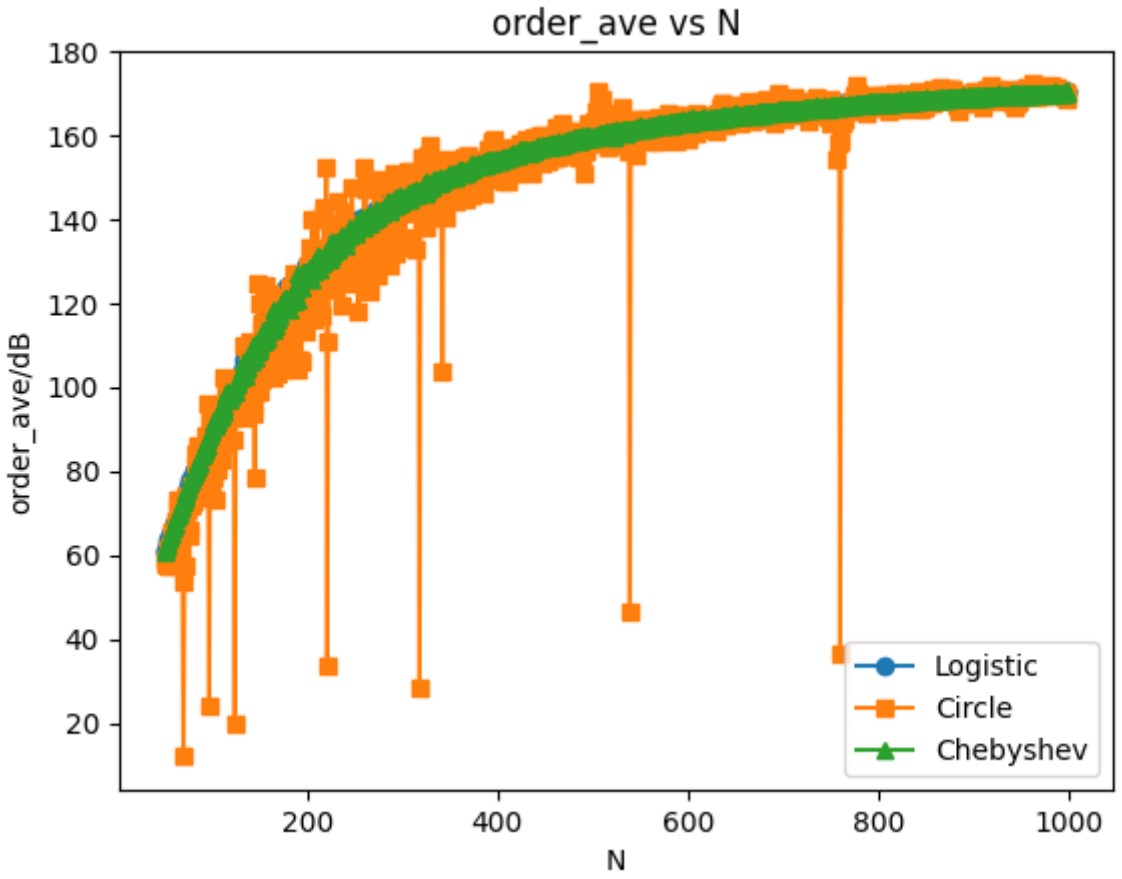
the enchanting world of the story, she felt a sense of nostalgia wash over her. Suddenly, she heard a gentle voice behind her."Ah, 'The Secret Garden,'" said Mr. Thompson, smiling warmly. "A timeless classic, isn't it?"Emily nodded, her cheeks flushing with embarrassment at being caught engrossed in the book. But Mr. Thompson only chuckled and gestured for her to sit down by the fireplace.For the rest of the afternoon, Emily and Mr. Thompson talked about their favorite books, sharing stories and recommendations with each other. Despite their differences in age and background, they discovered a shared passion for literature that bridged the gap between them.As the rain continued to pour outside, Emily realized that she had found not just a bookstore, but a home away from home. And Mr. Thompson, in turn, found a kindred spirit in the young girl who reminded him of his own love for books.From that day on, Emily became a regular visitor to the bookstore, spending hours lost in the pages of her favorite stories. And with each visit, she grew closer to Mr. Thompson, who became not just a mentor, but a dear friend.In the end, it wasn't just the books that brought Emily back to the bookstore time and time again. It was the sense of belonging, the warmth of human connection, and the magic of discovering new worlds within the pages of a book. And as she stepped out into the rain, she knew that she would always carry a piece of the bookstore – and Mr. Thompson – in her heart wherever she went.
与加密时输入的密文相同
（处理时将换行符'\n'全部去除）

性能测试

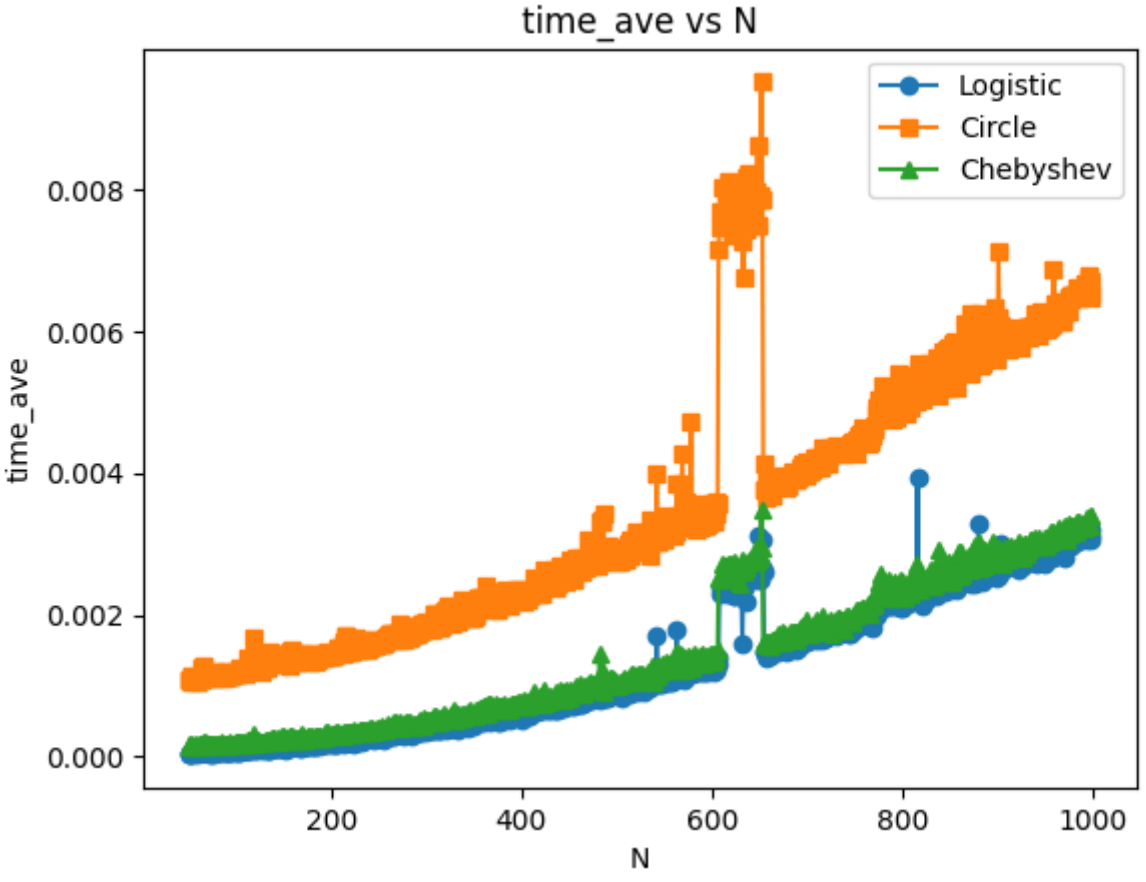
在对logistic，circle和chebyshev混沌映射的性能分析上，得出了三者的分析结果
1.在平均阶-N上，三者展现了相似的发布趋势，随N的增大，平均阶不断增大，并趋于某个值
logistic和chebyshev映射展现了大致相同的数据稳定性
circle映射绘制的图像分布较为无序，围绕某条函数曲线浮动
2.对于加密时间，总的趋势为随着N的增大而增大，展现出二次函数曲线
logistic和chebyshev映射较低，而circle
3.平均敏感度对加密的敏感性较低，随N的增大，敏感度相对稳定
logistic和chebyshev映射的的敏感度维持在-300~-350dB左右
circle的敏感度较差，大概在-50dB

测试数据与结果

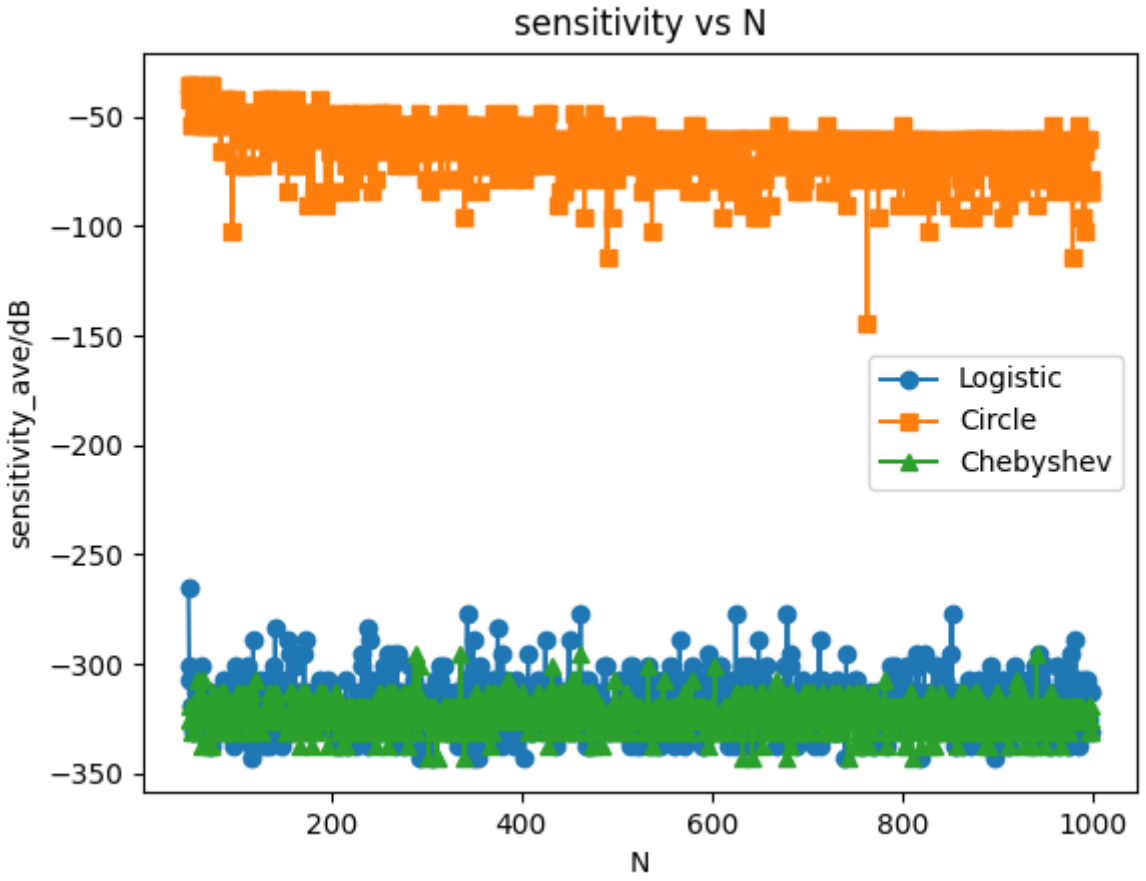
平均阶-N


order_ave vs N
order_ave/dB
N
Logistic
Circle
Chebyshev
180
160
140
120
100
80
60
40
20
200
400
600
800
1000

加密时间-N


time_ave vs N
time_ave
N
Logistic
Circle
Chebyshev
0.008
0.006
0.004
0.002
0.000
200
400
600
800
1000

灵敏度-N



应用前景

在功能上
结合Logistic映射、圆形加密和Chebyshev多项式的方法，可能会为加密领域带来一些新的创新。这种加密系统的应用前景可能会涉及到以下几个方面：

1. **数据安全和隐私保护**：随着信息技术的迅速发展，数据安全和隐私保护变得越来越重要。你设计的加密系统可以用于保护敏感数据，如个人身份信息、财务数据、医疗记录等，确保其不被未经授权的访问或窃取。
2. **通信加密**：在网络通信中，数据的安全传输是至关重要的。你的加密系统可以应用于加密电子邮件、即时消息、文件传输等通信内容，确保通信双方的隐私和数据安全。
3. **物联网（IoT）安全**：随着物联网设备的普及，对于这些设备的安全性要求也在增加。你的加密系统可以用于保护物联网设备之间的通信，防止黑客入侵和恶意攻击。
4. **金融领域应用**：金融行业对于数据安全性有着极高的要求，你的加密系统可以用于保护银行交易、支付信息和客户资产，防止金融欺诈和数据泄露。
5. **军事和国防安全**：在军事和国防领域，保护敏感信息和通信的安全至关重要。你的加密系统可以应用于保护军事指挥通信、情报信息和机密文件，确保国家安全。

总的来说，你设计的基于Logistic、圆形和Chebyshev的加密系统在保护数据安全和隐私方面有着广阔的应用前景，可以在各个领域中发挥重要作用，为信息安全提供新的解决方案。
针对，根据其灵敏度的测量结果可分别生成 位密钥，密钥空间大
计算处理简单，具有良好的可移植性，支持在各种平台上的实现
置乱表的阶稳定均匀，加密效果好
在对三种置乱方式的横向对比上，我分析了三种置乱方式在加密时间，加密效果，灵敏度上的特

点，基于这些特点，探求出三种置乱方式在应用细分上可能可行的领域，可以在一定程度上实现对其缺点的规避，对其优势的发扬

结论

通过混沌映射生成的置乱表可以实现轻量化，直接有效的加密，密钥空间大。

本次实现的功能尝试了一种基于混沌映射的置乱加密方式，实现了利用简单的密钥对任意长的密文实现加密，加解密的计算量低，计算速度快，可以实现在各种平台上的轻量化部署。

本次性能测试探索了logistic，circle和chebyshev映射在作为置乱表索引上的性能，对于三种混沌映射的性能评估得出
logistic和chebyshev的性能明显高于circle映射，在加密时间，置乱表的平均阶和灵敏度上二者相似，且明显高于circle
circle映射在一定程度上展现出较弱的性能，可以断言其并不适合作为置乱加密的逻辑公式使用