# 摘要

略略略

**关键词：**门限签名，盲签名，ECDSA，同态加密

# ABSTRACT

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.……

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.……

……

**Key words:** Threshold Signature, Blind Signature, ECDSA, Homomorphic Encryption

# 目录

目录

**[摘要 1](#_Toc19331)**

**[ABSTRACT 2](#_Toc30614)**

**[目录 3](#_Toc11288)**

**[第一章 绪论 4](#_Toc1491)**

[1.1 论文研究背景及意义 4](#_Toc28297)

**[第二章 相关技术和理论介绍 5](#_Toc32676)**

[2.1 Shamir秘密分享 5](#_Toc9164)

[2.2 Paiilier同态加密修改方案 5](#_Toc17750)

[2.3 ECDSA数字签名算法 5](#_Toc14695)

**[第三章 基于ECDSA的门限盲签名协议 5](#_Toc2844)**

[3.1符号系统 5](#_Toc9331)

[3.2 基于ECDSA的门限盲签名协议 5](#_Toc9338)

[3.3 正确性分析 5](#_Toc6643)

[3.4 安全性分析 5](#_Toc3017)

**[第四章 基于ECDSA的门限盲签名系统 5](#_Toc26294)**

**[第五章 总结与讨论 5](#_Toc3855)**

# 第一章 绪论

## 论文研究背景及意义

2008年，中本聪提出了比特币这一去中心化加密货币的设计概念。随着2009年比特币系统的启动，比特币正式问世。在2010年到2015年期间，比特币逐渐走入了公众视野。而2016年到2018年，则见证了各国相继对比特币公开表态，以及全球主要经济体不确定性的增加，这促使比特币备受关注，需求飞速增长。事实上，比特币可谓是区块链技术最为成功的应用之一。随着以太坊等开源区块链平台的涌现，以及大量去中心化应用的落地，区块链技术正被更多行业所应用。随之而来的是越来越多的用户开始涉足区块链世界。数字签名是用户与区块链世界交互的主要方式，比如在比特币中用户使用私钥签署交易信息生成数字签名，再将其发布到区块链网络中由各个区块链节点进行共识以完成一笔转账操作，其他更复杂的交互也需要基于数字签名，比如各种基于智能合约的去中心化应用也需要用户签署特定消息来引发相关的接口调用。

为了使用户更便利地管理其数字资产，数字钱包等产品应运而生，成为用户与区块链之间的桥梁。然而，随着区块链技术的普及和用户群体的扩大，安全隐患也逐渐暴露出来。

遗失私钥或私钥被黑客攻击是区块链用户面临的重大风险之一。许多用户可能因个人疏忽，如存储私钥的不当或遗忘备份等，而导致私钥丢失，从而失去对其链上资产的所有权。更为严重的是，黑客可能利用各种技术手段入侵数字钱包或交易所，窃取用户的私钥，进而窃取用户的数字资产，给用户带来巨大的经济损失。//数据或新闻引用

这些恶意事件的发生凸显了当前数字资产管理和交易过程中的安全性问题。用户对于自身数字资产的安全性越来越关注，迫切需要更加可靠和安全的解决方案来保护其资产免受损失。因此，区块链技术领域亟需加强安全意识和技术防范手段的研发，以应对不断演变的安全威胁，为用户提供更加可靠的数字资产保障。

# 相关技术和理论介绍

## 2.1 Shamir秘密共享

Shamir秘密分享是由Adi Shamir在[]中提出的一个算法。该算法可以将一个秘密值分成n个分片，当得知的分片数量大于一个阈值时，才可以从分片中还原出秘密值。基本原理是利用多项式插值。具体来说，原始秘密被表示为一个多项式的常数项，多项式的次数取决于需要的最小部分数量。然后，多项式在不同的点上被计算得到秘密分片值，这些分片值被分发给不同的参与者。当需要恢复原始秘密时，只需收集足够数量的秘密分片值，然后使用插值技术即可重建出原始秘密。

对于一个秘密值，以为常数项构造一个次多项式:

(2-1)

则对于不同的取值，如可以计算出不同的函数值，这些函数值与其自变量共同构成一个秘密分片值，当收集到t+1个分片值时，可以对t+1个分片通过以下运算重建原始秘密:

(2-2)

(2-3)

## 2.2 ECDSA数字签名算法

## 2.3 Paillier同态加密修改方案

### 2.2.1 Paillier同态加密方案

Paillier同态加密方案[]是一个基于离散对数困难问题构建的加密方案，它具有加法同态的性质，他的密钥对生成过程如下：

1. 随机选取两个大素数，需要满足条件与互素，不满足则重新选择随机数。
2. 计算，其中lcm表示最小公倍数。
3. 随机选取一个正整数，要求并存在，若不存在，则需要重新选取,其中：

(2-4)

其中的除法表示向下取整。

得到的公钥为，私钥为，对于要加密的消息，它需要满足，它的加密过程如下：

1. 随机选取一个正整数，要求，且还需满足与互素。
2. 计算密文如下：

(2-5)

对于密文，解密过程为：

(2-6)

使用表示对进行加密得到的密文，对于任意的消息，Paillier加密方案具有以下性质：

(2-)

(2-)

使用表示密文的模相乘，使用表示密文的模指数运算，则上述性质可以写作：

(2-)

(2-)

则可以将定义为Paillier的同态加运算，定义为Paillier的同态数乘运算。上述性质即为Paillier加密方案的同态加法性质即密文的相加等于明文相加后再加密。

### 2.2.2 Paillier同态加密修改方案

Paillier同态加密因其优秀的性质而得到广泛应用，然而在文献[]中提到将Pailiier方案直接应用于构建盲ECDSA签名可能导致更多信息的泄露，而这部分信息的泄露所带来的安全性影响是未知的。因此文献[]在此基础上提出了一个Paillier同态加密的修改方案， 它的密钥生成如下：

1. 随机选取两个大素数，需要满足条件与互素，不满足则重新选择随机数。
2. 计算，其中为ECDSA中的公共参数椭圆曲线群的阶。

得到的公钥为，私钥为，对于要加密的消息，它需要满足，它的加密过程如下：

1. 随机选取一个正整数，要求，且还需满足与互素。
2. 计算密文如下：

(2-)

对于密文，解密过程为：

(2-)

对于修改后的Paillier同态加密方案，同样具有同态加法性质，即密文的相加等于明文相加后再加密。

# 基于ECDSA的门限盲签名协议

## 3.1符号系统

## 3.2 基于ECDSA的门限盲签名协议

## 3.3 正确性分析

## 3.4 安全性分析

## 3.5 复杂度分析

# 基于ECDSA的门限盲签名系统实现

# 总结与讨论