# 知网个人查重服务报告单(全文对照)

报告编号:BC20240325014936761957656O　　检测时间:2024-03-25 01:49:36

篇名：基于多方计算的ECDSA门限盲签名方案研究

作者：苏冠宁

检测类型：学位论文

比对截止日期：2024-03-25

## 检测结果

去除本人文献复制比：1.3%　　去除引用文献复制比：0.7%　　总文字复制比：1.3%

单篇最大文字复制比：0.3%（S200450119_何玉_基于定位和区块链的中药材温室大棚数据采集与传输设计）

重复字符数：[720]　　单篇最大重复字符数：[193]　　总字符数：[57006]

| | | |
|---|---|---|
| 3.4%(349) | 3.4%(349) | 基于多方计算的ECDSA门限盲签名方案研究_第1部分（总10411字） |
| 3.9%(371) | 3.9%(371) | 基于多方计算的ECDSA门限盲签名方案研究_第2部分（总9504字） |
| 0%(0) | 0%(0) | 基于多方计算的ECDSA门限盲签名方案研究_第3部分（总10754字） |
| 0%(0) | 0%(0) | 基于多方计算的ECDSA门限盲签名方案研究_第4部分（总11018字） |
| 0%(0) | 0%(0) | 基于多方计算的ECDSA门限盲签名方案研究_第5部分（总10688字） |
| 0%(0) | 0%(0) | 基于多方计算的ECDSA门限盲签名方案研究_第6部分（总4631字） |

（注释：无问题部分　文字复制部分　引用部分）



## 1. 基于多方计算的ECDSA门限盲签名方案研究_第1部分　　总字符数：10411

相似文献列表

去除本人文献复制比：3.4%(349)　　去除引用文献复制比：2%(208)　　文字复制比：3.4%(349)

| | | |
|---|---|---|
| 1 | S200450119_何玉_基于定位和区块链的中药材温室大棚数据采集与传输设计<br>何玉 - 《学术论文联合比对库》- 2020-04-16 | 1.9%（193）<br>是否引证：否 |
| 2 | 20343045_陈梦蓉_基于“奖励机制”和“K匿名机制”的DPoS共识机制<br>陈梦蓉 - 《学术论文联合比对库》- 2020-04-03 | 1.5%（158）<br>是否引证：否 |
| 3 | 2018022648_颜萌_两方ECDSA方案的设计<br>颜萌 - 《学术论文联合比对库》- 2021-04-27 | 0.5%（48）<br>是否引证：否 |
| 4 | 基于文献计量的国内区块链技术热点与趋势研究<br>姚宁宁;董春丽;陈兴荣;韩慧霞; - 《湖北科技学院学报》- 2023-06-02 | 0.5%（48）<br>是否引证：否 |
| 5 | 浅谈盲签名<br>陈明;葛永亮; - 《科技信息(科学教研)》- 2007-11-01 | 0.4%（38）<br>是否引证：否 |
| 6 | 对电子商务中安全控制技术的探讨(上)<br>吴明玮; - 《计算机安全》- 2002-06-25 | 0.4%（38）<br>是否引证：否 |
| 7 | 两方SM2签名方案的设计与实现<br>刘凯(导师：鲍海勇;王潇扬) - 《浙江工商大学硕士论文》- 2019-12-01 | 0.3%（32）<br>是否引证：否 |
| 8 | 考生申请单编号17236_戴楠_2012212972-戴楠-刘玲玲<br>戴楠 - 《学术论文联合比对库》- 2016-04-23 | 0.2%（24）<br>是否引证：否 |
| 9 | 051_硕_2012212972_戴楠<br>硕 - 《学术论文联合比对库》- 2016-06-06 | 0.2%（24）<br>是否引证：否 |

| | 原文内容 | 相似内容来源 |
| --- | --- | --- |
| 1 | 此处有 35 字相似<br>d Signature, ECDSA, Multiparty Computation IV<br>第一章绪论 1<br>第一章绪论<br>1.1 论文研究背景及意义<br>*2008 年，中本聪提出了*<br>比特币[1]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 2 | 20343045_陈梦蓉_基于“奖励机制”和“K匿名机制”的DPoS共识机制 陈梦蓉 -《学术论文联合比对库》- 2020-04-03（是否引证：否）<br>1.Distributed K anonymous incentive mechanism; Game theory第一章绪论1.1 研究背景及意义中本聪于2008 年第一次提出了区块链的概念，在随后的几年中，区块链成为了电子货币比特币的核心组成部分：作为所有交易的公共账簿[ 2]。通过利用点对 |
| 2 | 此处有 196 字相似<br>第一章绪论 1.1 论文研究背景及意义 2008 年，中本聪提出了比特币[1]这一去中心化加密货币的设计概念。随着<br>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，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。<br>*随着以太坊[2]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*<br>[3]。随之而来的是越来越多的用户开始涉足区块链世界。在区块链世界中，每个用户对应一个公私钥对，公钥是用户在区块链世界中 | 考生申请单编号17236_戴楠_2012212972-戴楠-刘玲玲 戴楠 -《学术论文联合比对库》- 2016-04-23（是否引证：否）<br>1.息交流的扩大，一个区块与一个区块相继接续，形成的结果就叫区块链。因此可以把比特币看成区块链的首个在金融支付领域中的应用，事实上比特币也是区块链技术迄今为止最为成功的应用之一，比特币区块链也是目前应用最为广泛的区块链。从本质上看，区块链技术是一种不依赖第三方、通过自身分布式节点进行网络数据的<br>051_硕_2012212972_戴楠 硕 -《学术论文联合比对库》- 2016-06-06（是否引证：否）<br>1.围的不断增加，一个区块与一个区块相继接续，形成的结果就叫区块链。因此可以把比特币看成区块链的首个在金融支付领域中的应用，事实上比特币也是区块链技术迄今为止最为成功的应用之一，比特币区块链也是目前应用最为广泛的区块链。从本质上看，区块链技术是一种不依赖第三方、通过自身分布式节点进行网络数据的<br>20343045_陈梦蓉_基于“奖励机制”和“K匿名机制”的DPoS共识机制 陈梦蓉 -《学术论文联合比对库》- 2020-04-03（是否引证：否）<br>1.提出了去中心化加密货币——比特币（bitcoin）的设计构想，2009 年，比特币系统开始运行，标志着比特的正式诞生，随着各国陆续对比特币进行公开表态以及世界主流经济的不确定性增强，比特币的受关注程度激增，需求量迅速扩大。事实上，比特币是区块链技术最成功的应用场景之一[ 1]。伴随着以太坊等开源区块链平台的诞生以及大量去中心化应用的落地，区块链技术在更多的行业中得到了应用[ 1] 。比特币不需要向用户分发数字货币。相反，比特币系统中的公共分类账仅维护着其所依赖的区块链系统自创建以来所有比特币用户所<br>S200450119_何玉_基于定位和区块链的中药材温室大棚数据采集与传输设计 何玉 -《学术论文联合比对库》- 2020-04-16（是否引证：否）<br>1.究，中本聪发表了名为“比特币：一种点对点的电子现金系统”的白皮书，并随后发布了实现白皮书规范的开源软件，由此诞生比特币。2009年，比特币系统开始运行，标志着比特币的正式诞生。2010-2015年，比特币逐渐进入公众视野。2016-2018年，随着各国对比特币的公开表态以及世界主流经济的不确定性增加，比特币的关注度激增，需求量迅速扩大。实际上，比特币是区块链技术最成功的应用场景之一。随着以太坊（ethereum）等开源区块链技术平台的诞生以及大量去中心化网络应用程序出现，区块链技术已被用于更多行业。[7]（3）特点比特币的出现，提出了链式数据结构 |

| | | |
|---|---|---|
| | | ，目的就是提高传统电子交易模式的效率，引出第三方机构作为交易时的<br>基于文献计量的国内区块链技术热点与趋势研究　姚宁宁;董春丽;陈兴荣;韩慧霞; -《湖北科技学院学报》- 2023-06-02（是否引证：否）<br>1.备过程可信和去中心化两大特点，区块链能够在多利益主体参与的场景下以低成本的方式构建信任基础，旨在重塑社会信用体系[1]。伴随着以太坊等开源区块链平台的诞生以及大量去中心化应用的落地，区块链技术在更多的行业中得到了应用。[1]中国政府近年来也积极部署区块链技术研究与应用创新，不断提升区块链研究定位。2019年习近平总书记在主持中共 |
| 3 | 此处有 32 字相似<br>需求来确定，从而确保足够的安全性。通过这种方式，即使部分参与方受到了攻击或者行为不端，整个签名过程依然是安全可靠的。门限<br>*签名方案一般包含三个算法：密钥生成算法、签名算法以及签名验证算法*<br>[5]。这些算法通常是多个参与方的交互协议，通过一系列的多方计算和 数据通信来共同计算出一个结果。<br>第一章绪论 3 | 两方SM2签名方案的设计与实现　刘凯 -《浙江工商大学硕士论文》- 2019-12-01（是否引证：否）<br>1.识的签名[38]方案是通过密码学原理，在非交互和不泄露其他有用的信息的前提下，证明自己知道某个秘密。在一个基本的签名方案里，一般包含三个算法：密钥生成算法???0)?????0)?9) 、签名算法??4)?2)?9)、验证算法?(1?0)??4)?1)??。在一个传统签名方案中，签名可以认为是代表特定公共密钥的声明。对于验证函数?(1?0)? |
| 4 | 此处有 48 字相似<br>的(t,n)门限签名方案，通过联合秘密共享技术，使得方案中无需一个所有成员都相信的诚信方也可完成签名。 2014 年，<br>*尚铭[16]等人基于 SM2 椭圆曲线公钥密码算法，提出了一个安全有效的门限密码方案，该方案可以*<br>支持有可信方中心和无可信中心的两种情况。 随着区块链的应用不断扩展，对加密系统的需求变得更加迫切和复杂。在区块链系统中 | 2018022648_颜萌_两方ECDSA方案的设计　颜萌 -《学术论文联合比对库》- 2021-04-27（是否引证：否）<br>1.在于能够抵抗移动攻击而且签名时间效率高。2020年涂彬彬[21]等人系统地论述了门限密码目前的研究现状和主要进展。尚铭[22]等人针对SM2 椭圆曲线公钥密码算法提出了安全有效的门限密码方案，该方案可以抵抗?? / 2的窃听攻击和?? / 3的中止攻击。侯红霞[23]采用 Lindell 在 2017 年的两方 ECDS |
| 5 | 此处有 38 字相似<br>是接收者和签名者。接收者是指那些希望获取签名的个体或实体一般代表需要获取签名服务的用户，而签名者则是负责生成签名的一方。<br>接收者首先对待签名的消息进行盲化处理，然后将处理后的消息发送给签名者进行签名<br>。盲化处理的关键在于使签名方无法得知所签消息的具体内容，从而确保用户的隐私得到有效保护。 1996 年，David P | 对电子商务中安全控制技术的探讨(上)　吴明玮; -《计算机安全》- 2002-06-25（是否引证：否）<br>1.）是一种特殊的数字签名,它与通常的数字签名的不同之处在于,签名者并不知道他所要签发文件的具体内容。盲数字签名在签名时,接收者首先将被签的消息进行盲变换,把变换后的消息发送给签名者,签名者对盲消息进行签名并把消息送还给接收者,接收者对签名再做逆盲变换,得出的消息即为原消息的盲签名。这个过程如图二。 往妥表人 报受者人图二一<br>浅谈盲签名　陈明;葛永亮; -《科技信息(科学教研)》- 2007-11-01（是否引证：否）<br>1.息不可跟踪,即当签名信息被公布后,签名者无法知道这是他哪次签署的。盲签名方案是用户(接受者)与签名人之间的一个交互协议,接收者首先将被签的消息进行盲变换,把变换的消息(盲消息)发送给签名者,签名者对盲消息进行签名并把消息送还给接受者,接收者再对消息进行逆盲变换,得出的消息即为原消息的盲签名。<br>5.结论盲签名技术对于具有匿名性要求的网 |

## 2. 基于多方计算的ECDSA门限盲签名方案研究_第2部分

总字符数：9504

相似文献列表

去除本人文献复制比：3.9%(371)　　去除引用文献复制比：2.1%(198)　　文字复制比：3.9%(371)

| | | |
|---|---|---|
| 1 | 2019210798_董高照_基于多尺度特征处理的爆燃检测算法研究 | 1.3%（123） |

| | | |
|---|---|---|
| | 董高照 - 《学术论文联合比对库》- 2022-04-08 | 是否引证：否 |
| 2 | 一种面向工业物联网的远程安全指令控制方案 | 0.7%（64） |
| | 陈纪成;包子健;罗敏;何德彪; - 《计算机工程》- 2023-06-02 15:50 | 是否引证：否 |
| 3 | 211-2018102110024-王婧-面向移动互联网的安全两方计算技术研究 | 0.6%（59） |
| | 王婧 - 《学术论文联合比对库》- 2021-10-19 | 是否引证：否 |
| 4 | 081_20130807010010_杨俊芳_部分盲签名的研究及其应用 | 0.6%（54） |
| | 杨俊芳 - 《学术论文联合比对库》- 2016-03-18 | 是否引证：否 |
| 5 | 面向大规模数据的安全多方计算协议的设计 | 0.4%（35） |
| | 冉鹏(导师：杨浩淼) - 《电子科技大学硕士论文》- 2017-03-01 | 是否引证：否 |
| 6 | 基于方程加密的弹性泄露数字签名方案研究 | 0.3%（31） |
| | - 《学术论文联合比对库》- 2015-03-20 | 是否引证：否 |
| 7 | 理性门限签名的若干关键技术研究 | 0.3%（27） |
| | 杨怡(导师：蔡永泉) - 《北京工业大学硕士论文》- 2012-05-01 | 是否引证：否 |
| 8 | 门限签名体制的研究 | 0.3%（27） |
| | 李国文(导师：李大兴) - 《山东大学》- 2007-03-15 | 是否引证：否 |

| 原文内容 | 相似内容来源 |
|---|---|
| 1 | 此处有 64 字相似<br>机函数评估的结果。在签名验证时，验证者使用可验证随机函数 验证接收者提供的证明，并确保其符合要求。同年，陈倩倩与秦宝东<br>*提出了一种基于 SM9 的两方协同盲签名方案[38]，该方案通过利用密钥生成中心将 SM9 私钥分割成两个分片，并将其分配给两方*<br>签名者，从而使得签名者之间相互独立，确保了签名的安全性和可靠性。在签名的过程中，两方签名者通过一个协同盲签名协议完成签名 | 一种面向工业物联网的远程安全指令控制方案 陈纪成;包子健;罗敏;何德彪; -《计算机工程》- 2023-06-02 15:50（是否引证：否）<br>1.用SM9数字签名算法对数据进行签名再利用SM9加密算法加密签名后的数据的方案，该方案在计算开销和密文长度方面有明显减少。文献[23]提出一种基于SM9算法的两方协同盲签名方案，该方案将签名密钥分割成两部分，分配给2个签名者，两方合作生成合法的盲签名。文献[24]提出一种基于SM9门限签名的电力终端安全认证方案，该方案结合无证书标识密码和门限密码， |
| 2 | 此处有 23 字相似<br>领域，也有为了解决该问题而提出的门限部分盲签名特性的方案。Wen-Shenq Juang 和 CL Lei[42]基于<br>*离散对数困难问题提出了一个门限部分盲签名方案。*<br>该方案中，门限部分盲签名的大小与单个部分盲签名相同，而门限部分盲签名的验证过程则可通过群公钥进行简化。此外，该方案还具备 | 081_20130807010010_杨俊芳_部分盲签名的研究及其应用 杨俊芳 -《学术论文联合比对库》- 2016-03-18（是否引证：否）<br>1.等人[5]基于平方剩余困难问题的假设，也提出了一个部分盲签名方案。 1999 年，Juang 等人[6]在离散对数困难问题的基础上，提出了一个门限部分盲签名方案。2000 年，Abe 等人[7]提出了一个部分盲签名方案证明的安全模型，并基于随机预言机模型给予了详细的证明。 |
| 3 | 此处有 27 字相似<br>们实际签名的消息与所有签名者完整视图之间的确切对应是计算上不可行的。同样提出门限部分盲签名方案的还有陆洪文等人[43]，<br>*他们提出了一种基于双线性对的新型的门限部分盲签名方案。*<br>该方案通过加入签名方的信息控制发送方，并引入双线性对的概念，限制了由单个签名者组成的系统的不安全性。 第一章绪论 1 | 门限签名体制的研究 李国文 -《山东大学博士论文》- 2007-03-15（是否引证：否）<br>1.注。自Mov和Frey一Ruck将双线性对引入数字签名后，基于双线性对的各种签名方案也出现了，vo等人提出了个基于双线性对的门限盲签名方案!’。，1，该方案是基于证书的，需要管理用户证书。目前基于身份的门限盲签名方案还不多见，下文提出了种基于身份的门 |
| 4 | 此处有 31 字相似<br>条件，我们借助所提出的多方秘密乘积算法，结合 Paillier 同态加密系统，设计了一个基于多方计算的 ECDSA 门限<br>盲签名方案。最后，我们对该方案的安全性和计算性能进行了理论分析<br>。 2、针对用户私钥管理、安全性和隐私性问题，我们基于提出的方案设计并 实现了一个基于多方计算的 ECDSA 门限盲 | 081_20130807010010_杨俊芳_部分盲签名的研究及其应用 杨俊芳 -《学术论文联合比对库》- 2016-03-18（是否引证：否）<br>1.是存在性不可伪造的。通过对前人方案的分析及改进，掌握其中的设计思想及技巧，提出了一种基于无双线性对映射的无证书的部分盲签名方案，然后对该方案的正确性和安全性等各种性能进行了分析和证明，并且该方案中只对第二类攻击者的攻击进行了安全性的证明，且同样是以随机预言机模型为基础对方案的安全性进行了证明。新方案是基 |

| | | |
|---|---|---|
| 5 | 此处有 56 字相似<br>行了网络拥塞测试，评估了当某些参与者处于网络阻塞时 第一章绪论 11 对整个系统的耗时影响。 1.4 论文相关的<br>结构安排<br>本文总共由五个章节组成，每个章节的内容安排如下：第一章，绪论。本章介绍了本研究的背景与研究意义，讲述了当前区块链应 用中，用户以及组织面临的私钥管理问题并阐述了门限签名、盲签名和门限盲签名三项技术的国内外研究现状。 | 基于方程加密的弹性泄露数字签名方案研究 -《学术论文联合比对库》- 2015-03-20（是否引证：否）<br>1.架，并从该数字签名框架的安全性、具体方案描述、弹性泄露分析方面进行阐述说明。1.4 本文的组织结构本文分为七章，各章节的安排如下：第一章，绪论。本章主要阐述了本文的研究背景与意义，通过对量子计算机、侧信道攻击和演化密码所带来的威胁阐述，具体分析了目前国内外学术界所做的研究工作，以及存在的相关问题。最<br>2019210798_董高照_基于多尺度特征处理的爆燃检测算法研究 董高照 -《学术论文联合比对库》- 2022-04-08（是否引证：否）<br>1.有视频采集功能的监控摄像头加入扩展功能，具备爆燃目标检测的能力，并且模型可以在检测到爆燃事故时第一时间发出报警信号。1.4 论文结构安排本文在结构上总共分为六个章节，每个章节具体内容结构安排如下：第一章，绪论。本章节从近年来的相关数据统计和现状入手讨论了本课题的研究背景和意义。分析了国内外爆燃检测在计算机视觉领域的发展情况并讨论了深 |
| 6 | 此处有 49 字相似<br>研究意义，讲述了当前区块链应 用中，用户以及组织面临的私钥管理问题并阐述了门限签名、盲签名和门限盲签名三项技术的国内外<br>研究现状。本章的最后两小节介绍了本文的研究工作以及论文的结构安排。<br>第二章，相关技术与理论介绍。<br>本章主要介绍了构建本方案所需的密码学工 具，包括 Shamir 秘密共享、ECDSA 数字签名方案、Paillier | 面向大规模数据的安全多方计算协议的设计 冉鹏 -《电子科技大学硕士论文》- 2017-03-01（是否引证：否）<br>1.部分，首先简单介绍了安全多方计算的研究背景和意义，然后分析了安全多方计算与密码学的关系，紧接着回顾了安全多方计算的研究现状，最后给出了本文的主要工作以及本文的内容安排。 第二章 安全多方计算相关介绍7第二章 安全多方计算相关介绍本章我们主要介绍安全多方计算的相关概念、理论基础<br>2019210798_董高照_基于多尺度特征处理的爆燃检测算法研究 董高照 -《学术论文联合比对库》- 2022-04-08（是否引证：否）<br>1.计和现状入手讨论了本课题的研究背景和意义。分析了国内外爆燃检测在计算机视觉领域的发展情况并讨论了深度学习的目标检测技术的研究现状和发展历程。最后简要说明了本论文的研究目标、创新点和论文的结构安排。第二章，卷积神经网络理论。本章主要讨论本课题研究所运用到的前序理论，这些理论在课题后续的研究中起到了至关重要的铺垫作用。本章由浅入深依次讨论了卷积神经网络 |
| 7 | 此处有 35 字相似<br>。 本章对第四章的系统进行了三个方面的测试，分别是功能测试、性能测试和网络拥塞测试。通过这些测试综合评估了系统的特点。<br>第六章，总结与展望。本章对本文的工作进行总结，回顾了研究的主要成果<br>和贡献，并对未来改进方向进行了讨论和展望，为进一步研究提供了参考和启示。 第二章相关技术和理论介绍 12 第二章 | 2019210798_董高照_基于多尺度特征处理的爆燃检测算法研究 董高照 -《学术论文联合比对库》- 2022-04-08（是否引证：否）<br>1.网络模型的目标检测结果有明显的提升。最后在模型上设计了报警机制，并通过流媒体技术将该网络模型用于推理监控摄像头的视频流。第六章，总结与展望。本章主要总结了全文的研究思路和成果，并指出文章中存在的可以深入研究的问题。卷积神经网络理论与数据处理1.5 卷积神经网络理论1.5.1 卷积层与 |
| 8 | 此处有 27 字相似<br>钥公开，而私钥由签名人保密持有。签名人可以对某个消息利用私钥进行加密运算，这个过程为签名，加密后得到的数据称作数字签名。<br>任何人都可以使用公钥来验证该数字签名是由该签名人签署的<br>。 椭圆曲线签名算法(Elliptic Curve Digital Signature Algorithm, ECDS | 理性门限签名的若干关键技术研究 杨怡 -《北京工业大学硕士论文》- 2012-05-01（是否引证：否）<br>1.签名变种的门限签名方案[53]。该方案由t 个人共同产生门限签名，并且签名长度等于 ElGamal 签名的长度，任何人可以使用群公钥验证签名。由于基于 ELGamal 签名和标准数字签名的门限签名方案需要计算秘密的乘积的逆，在计算效率上难以有显著提高，因此难以产生高效的方案。1996 年，Gennar |

| | | |
|---|---|---|
| 9 | 此处有 59 字相似<br>进行加密运算，这个过程为签名，加密后得到的数据称作数字签名。任何人都可以使用公钥来验证该数字签名是由该签名人签署的。<br>*椭圆曲线签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)*<br>[46]是数字签名算法(Digital Signature Algorithm，DSA)的一种变体，在区块链和加密货 | 211-2018102110024-王婧-面向移动互联网的安全两方计算技术研究 王婧 -《学术论文联合比对库》- 2021-10-19（是否引证：否）<br>1.几年比特币、以太坊等数字货币被盗事件频发，工业界和学术界重拾门限密码和安全多方计算在密钥保护应用方面的兴趣，并致力于研究椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA）[71]的分布式实现方案，保证 - 6 -面向移动互联网的安全两方计算技术研究私钥在签名过程中的安全性。MacKen |

## 3. 基于多方计算的ECDSA门限盲签名方案研究_第3部分

总字符数：10754

相似文献列表

去除本人文献复制比：0%(0)　　去除引用文献复制比：0%(0)　　文字复制比：0%(0)

对照报告单展示的是系统识别到的相似内容与来源文献的对照情况，该部分未识别到相似内容。

## 4. 基于多方计算的ECDSA门限盲签名方案研究_第4部分

总字符数：11018

相似文献列表

去除本人文献复制比：0%(0)　　去除引用文献复制比：0%(0)　　文字复制比：0%(0)

对照报告单展示的是系统识别到的相似内容与来源文献的对照情况，该部分未识别到相似内容。

## 5. 基于多方计算的ECDSA门限盲签名方案研究_第5部分

总字符数：10688

相似文献列表

去除本人文献复制比：0%(0)　　去除引用文献复制比：0%(0)　　文字复制比：0%(0)

对照报告单展示的是系统识别到的相似内容与来源文献的对照情况，该部分未识别到相似内容。

## 6. 基于多方计算的ECDSA门限盲签名方案研究_第6部分

总字符数：4631

相似文献列表

去除本人文献复制比：0%(0)　　去除引用文献复制比：0%(0)　　文字复制比：0%(0)

对照报告单展示的是系统识别到的相似内容与来源文献的对照情况，该部分未识别到相似内容。

说明：1.总文字复制比:被检测文献总重复字符数在总字符数中所占的比例

2.去除引用文献复制比:去除系统识别为引用的文献后,计算出来的重合字符数在总字符数中所占的比例

3.去除本人文献复制比:去除系统识别为作者本人其他文献后,计算出来的重合字符数在总字符数中所占的比例

4.单篇最大文字复制比:被检测文献与所有相似文献比对后,重合字符数占总字符数比例最大的那一篇文献的文字复制比

5.复制比按照“四舍五入”规则,保留1位小数;若您的文献经查重检测，复制比结果为0，表示未发现重复内容，或可能存在的个别重复内容较少不足以作为判断依据

6.红色文字表示文字复制部分;绿色文字表示引用部分(包括系统自动识别为引用的部分);棕灰色文字表示系统依据作者姓名识别的本人其他文献部分

7.系统依据您选择的检测类型(或检测方式)、比对截止日期(或发表日期)等生成本报告

8.知网个人查重唯一官方网站:https://cx.cnki.net