基于属性的不可否认签名协议研究综述报告

汇报人：

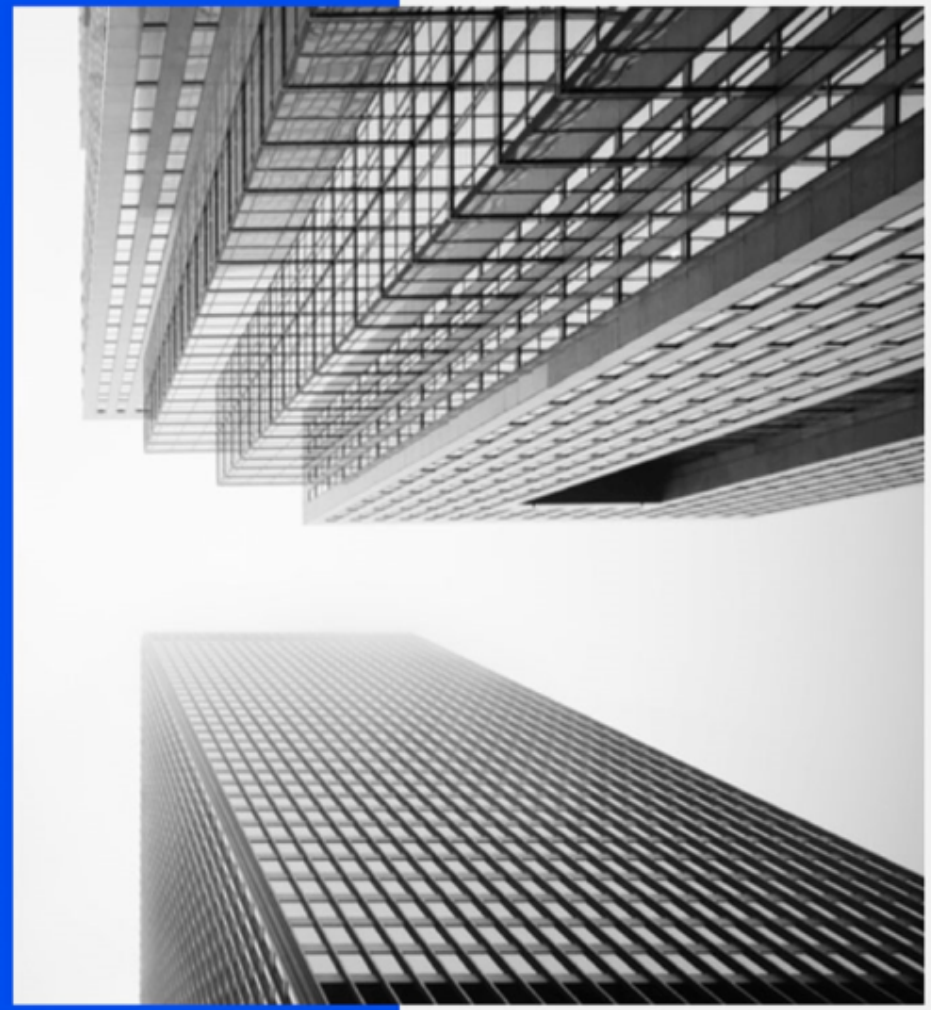
2024-01-14

CATALOGUE

目录

01

引言



研究背景与意义

信息安全重要性

随着互联网的普及和电子商务的快速发展，信息安全问题日益突出，如何保证信息的完整性、机密性和不可否认性成为亟待解决的问题。

不可否认签名协议的作用

不可否认签名协议是一种特殊的数字签名协议，它能够在保证签名者身份不可伪造的同时，防止签名者对自己的签名进行否认，从而有效地保护通信双方的利益。

研究意义

对基于属性的不可否认签名协议进行研究，不仅有助于解决信息安全领域中的关键问题，提高信息系统的安全性和可信度，还有助于推动数字签名技术的进一步发展，为电子商务、电子政务等领域的健康发展提供有力保障。

国内外研究现状及发展趋势

国外研究现状

国外对基于属性的不可否认签名协议的研究起步较早，已经取得了一系列重要成果。例如，基于双线性对的不可否认签名协议、基于格的不可否认签名协议等。这些协议在安全性、效率和实用性等方面都取得了显著进展。

国内研究现状

国内对基于属性的不可否认签名协议的研究相对较晚，但近年来也取得了不少进展。例如，基于身份的不可否认签名协议、基于属性的多重签名协议等。这些协议在安全性、灵活性和实用性等方面都具有一定的优势。

发展趋势

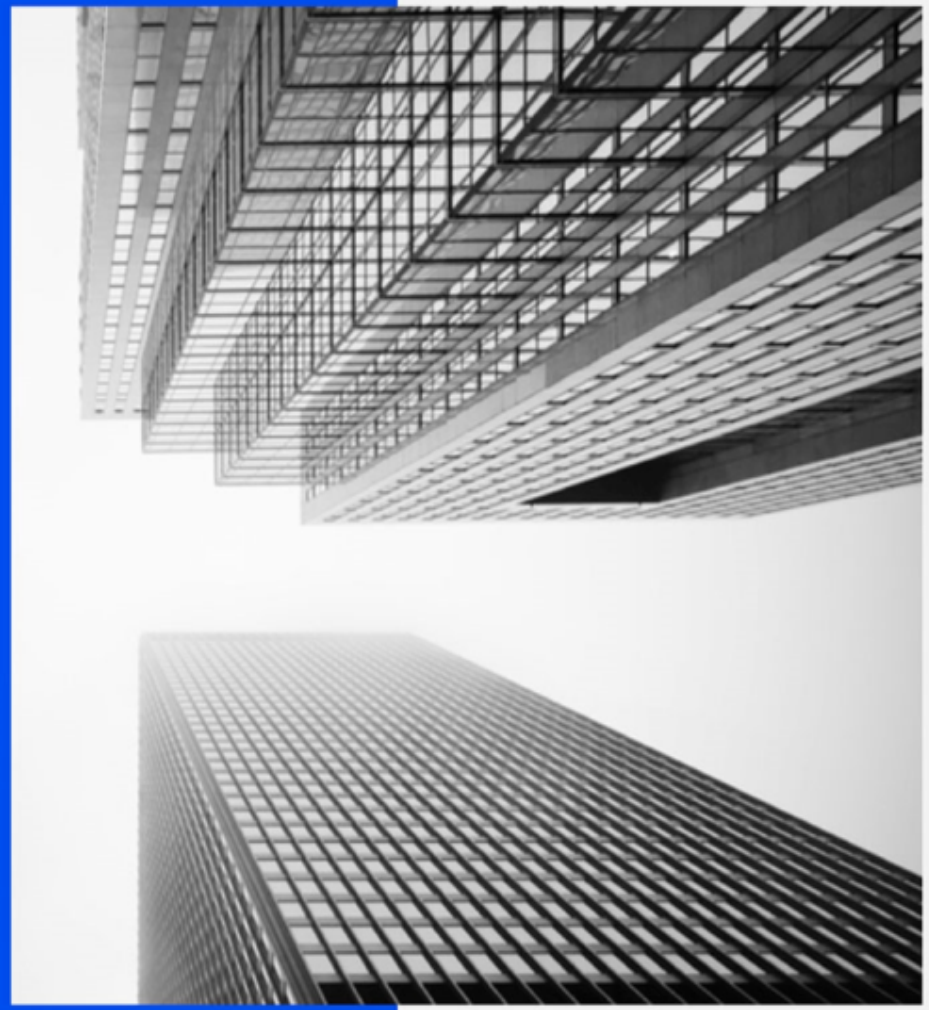
未来，基于属性的不可否认签名协议的研究将更加注重安全性、效率和实用性等方面的平衡发展。同时，随着区块链、人工智能等新技术的发展和应用，基于属性的不可否认签名协议的研究和应用也将迎来新的机遇和挑战。

研究内容、目的和方法

- 研究内容：本综述报告将对基于属性的不可否认签名协议的研究现状、主要技术、典型应用和发展趋势进行全面梳理和深入分析。具体包括：介绍基于属性的不可否认签名协议的基本概念、原理和技术；分析基于属性的不可否认签名协议的主要技术，包括签名算法、验证算法和密钥管理等；探讨基于属性的不可否认签名协议的典型应用，包括电子商务、电子政务和物联网等；展望基于属性的不可否认签名协议的未来发展趋势和挑战。
- 研究目的：通过对基于属性的不可否认签名协议的研究现状、主要技术、典型应用和发展趋势进行全面梳理和深入分析，旨在为该领域的研究人员提供一份全面、系统的综述报告，帮助他们更好地了解该领域的研究现状和发展趋势，为该领域的进一步发展提供有力支持。
- 研究方法：本综述报告将采用文献调研、比较分析和案例分析等方法进行研究。具体包括：收集国内外相关文献和资料，对基于属性的不可否认签名协议的研究现状进行全面梳理；采用比较分析方法，对不同类型的基于属性的不可否认签名协议进行比较分析；通过案例分析方法，探讨基于属性的不可否认签名协议的典型应用和实践经验。

02

基于属性的不可否认签名协议概述

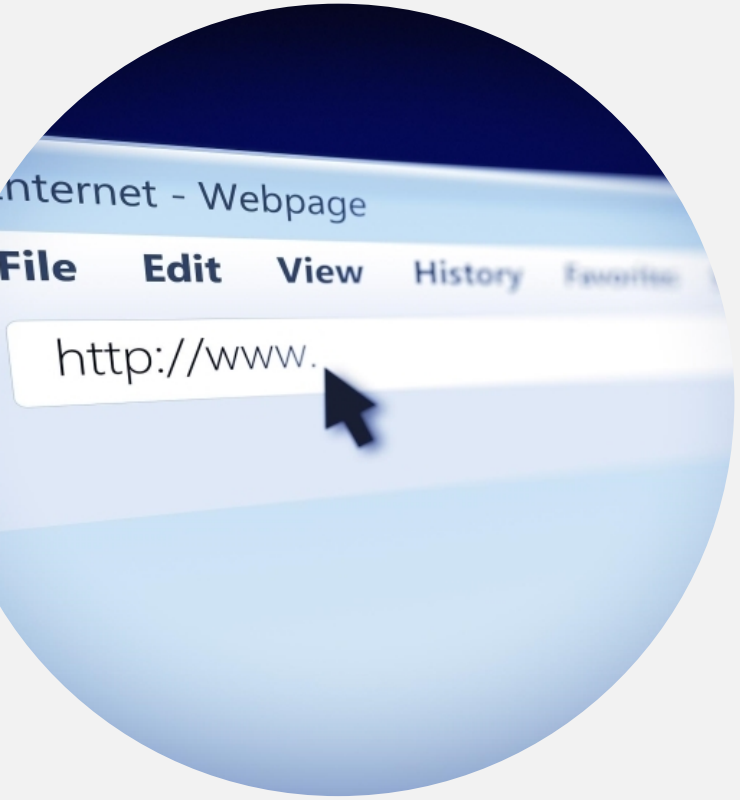


基于属性的不可否认签名协议的定义

基于属性的不可否认签名协议（Attribute-Based Undeniable Signature, ABUS）是一种特殊的数字签名技术，它允许签名者根据特定的属性集对消息进行签名，同时确保签名的不可否认性。

在ABUS中，签名者的身份和属性信息被嵌入到签名中，使得验证者可以验证签名的有效性以及签名者的身份和属性信息。

基于属性的不可否认签名协议的特点



不可否认性

ABUS确保签名者无法否认其签名的有效性，因为签名中包含了签名者的身份和属性信息。

属性隐藏

ABUS允许签名者隐藏其部分属性信息，以保护其隐私。

灵活性

ABUS支持多种属性表达方式，可以根据实际需求进行定制。

高效性

ABUS采用高效的密码学算法，确保签名和验证过程的快速执行。

基于属性的不可否认签名协议的应用场景

电子政务

在电子政务领域，ABUS可以用于实现电子文档的不可否认签名，确保政府文件的真实性和可信度。

电子商务

在电子商务领域，ABUS可以用于实现电子合同的不可否认签名，保障交易双方的权益。

物联网安全

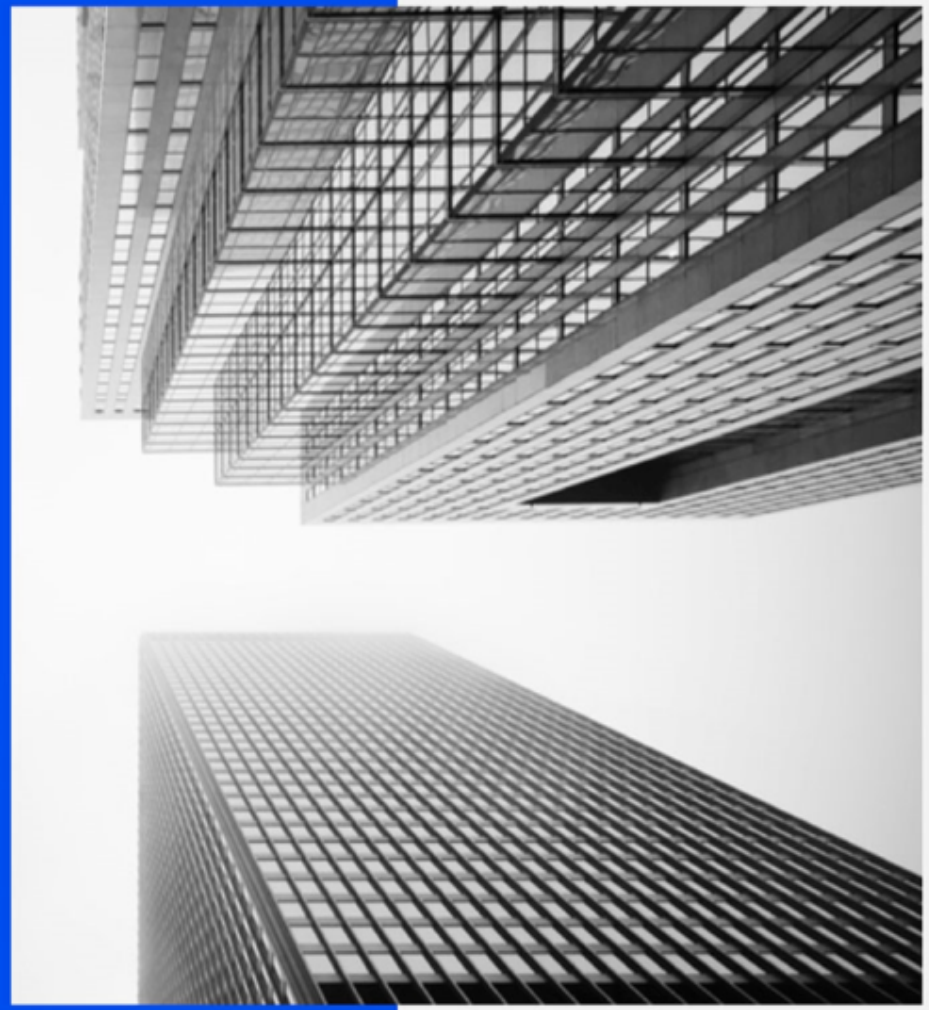
在物联网领域，ABUS可以用于实现设备间的安全通信和身份验证，确保物联网系统的安全性。

云计算安全

在云计算领域，ABUS可以用于实现云端数据的不可否认存储和访问控制，保障云端数据的安全性和隐私性。

03

基于属性的不可否认签名协议的关键技术



属性基加密技术

加密原理

属性基加密（ABE）是一种公钥加密技术，它允许持有者通过特定的属性对消息进行加密，只有具备相应属性的用户才能解密消息。

访问控制

ABE可以实现细粒度的访问控制，通过对属性的灵活组合和配置，可以精确地控制哪些用户可以访问加密的数据。

安全性

ABE在加密过程中采用了复杂的数学工具和密码学算法，确保了数据的安全性和保密性。

零知识证明技术

证明原理

零知识证明（ZKP）是一种密码学技术，它允许一方（证明者）向另一方（验证者）证明自己知道某个秘密信息，而无需透露任何关于该信息的具体内容。

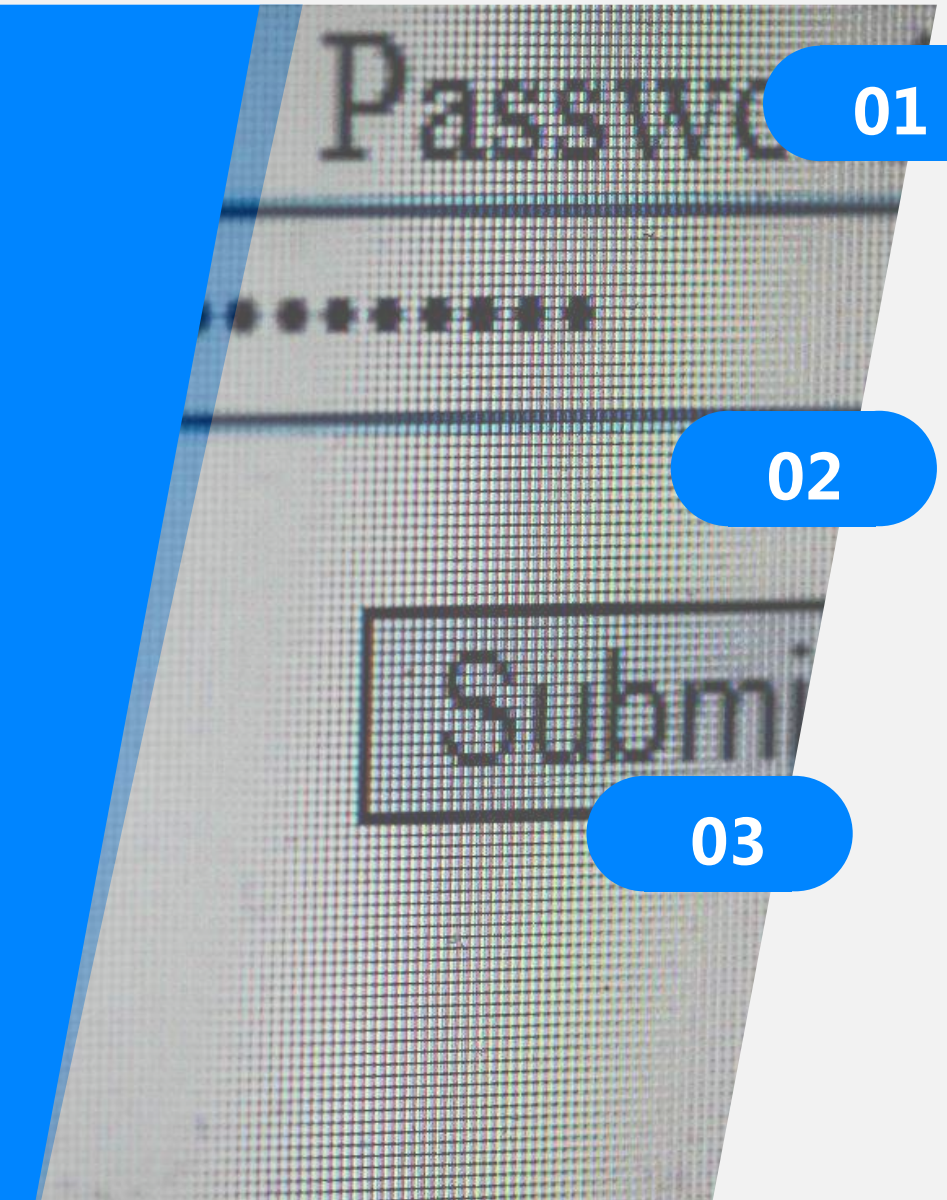
交互性

ZKP通常需要证明者和验证者之间进行多次交互，通过一系列的挑战和响应来验证证明者的知识。

应用场景

ZKP在身份认证、匿名通信、电子投票等领域具有广泛的应用。

数字签名技术



01

签名原理

数字签名是一种密码学技术，它允许消息的发送者使用私钥对消息进行签名，接收者可以使用相应的公钥验证签名的有效性。

02

不可否认性

数字签名具有不可否认性，一旦消息被签名，签名者无法否认自己对消息的签名行为。

03

安全性

数字签名采用了复杂的密码学算法和数学工具，确保了签名的安全性和不可伪造性。

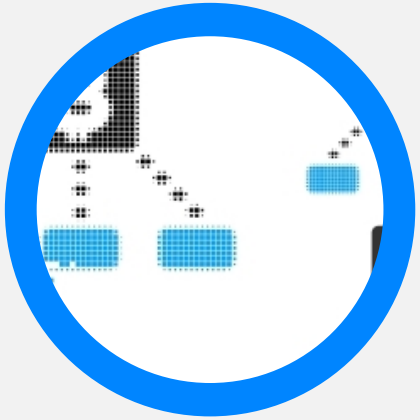
安全多方计算技术

计算原理

安全多方计算（MPC）是一种密码学技术，它允许多个参与者在不透露各自输入信息的情况下共同计算某个函数的结果。

安全性

MPC采用了复杂的密码学算法和协议设计，确保了计算过程中的数据安全和隐私保护。



应用场景

MPC在分布式计算、电子投票、秘密共享等领域具有广泛的应用。

04

基于属性的不可否认签名协议的研究现状