# 一种基于DID的具有交互式匿名认证的多方授权方案

# 摘 要

现如今的许多网络应用场景需要通过多个参与方共同验证和授权来完成特定的任务，如金融服务领域中的交易验证和审计、医疗保健领域中的电子病历共享、物联网领域中的智能设备管理等，然而多方授权系统存在潜在的身份泄露问题，威胁着人们的隐私安全。因此，研究如何实现具有隐私保护的多方授权是具有实际意义的研究课题。

关键词：多方授权，隐私保护，多重签名，匿名认证

# ABSTRACT

Nowadays many network application scenarios require verification and authorization by multiple parties to complete specific tasks, such as transaction verification and auditing in the financial services field, electronic medical record sharing in the healthcare field, and smart devices in the Internet of Things field. However, identity leakage problem exists in the multi-party authorization systems, threatening people's privacy security. Therefore, it is interesting to design a privacy-preserving multi-party authorization system.

KEY WORDS: Multi-party authorization, Privacy protection, Multi-signature, Anonymous authentication

# 目 录

[一种基于DID的具有交互式匿名认证的多方授权方案 I](#_Toc200897846)

[摘 要 I](#_Toc200897847)

[ABSTRACT II](#_Toc200897848)

[目 录 III](#_Toc200897849)

[第一章 绪论 1](#_Toc200897850)

[1.1课题背景和意义 1](#_Toc200897851)

[1.2研究现状 1](#_Toc200897852)

[1.3本文研究内容 1](#_Toc200897853)

[1.4章节安排 1](#_Toc200897854)

[**第二章 预备知识** 1](#_Toc200897855)

[2.1基础知识 1](#_Toc200897856)

[**2.1.1 双线性群** 1](#_Toc200897857)

[第三章 方案设计 2](#_Toc200897858)

[3.1整体构思 2](#_Toc200897859)

[3.3安全性分析 2](#_Toc200897860)

[**3.3.1 多方授权** 2](#_Toc200897861)

[**第四章 系统实现与实验分析** 2](#_Toc200897862)

[4.1系统的实现 2](#_Toc200897863)

[**4.1.1 实现方法** 2](#_Toc200897864)

[第五章 总结与展望 2](#_Toc200897865)

[5.1工作总结 2](#_Toc200897866)

[参考文献 3](#_Toc200897867)

[**附录A 仿真系统源代码** 5](#_Toc200897868)

# 第一章 绪论

## 1.1课题背景和意义

随着信息技术的发展，人们需要在网络上能够通过多个参与方共同验证和授权来完成特定的任务

## 1.2研究现状

多方授权是一种权限控制机制，它允许多个参与者在分布式系统中协同完成授权操作，同时保护敏感信息的安全。在现代网络环境中，多方授权得到了广泛应用，例如在物联网中涉及到数量庞大的设备和传感器，多方授权技术可以用于物联网场景中的设备认证和访问控制，确保设备之间的数据传输安全[23]。

**第二章 预备知识**

本章将回顾支撑我们方案的基础概念与密码学原语。我们首先深入探讨去中心化身份的技术核心。然后我们将介绍方案所依赖的关键密码学工具，包括双线性配对、一种紧凑的多重签名方案以及一种基于签名的零知识集合成员证明。

2.1去中心化身份

去中心化身份（DID）的认证流程，技术本质是一个多方参与的、依赖密码学技术串联的验证链条：验证方通过验证持有方和签发方双方的数字签名，并以一个不可篡改的可验证数据注册表（VDR）为信任根，最终确认一项声明的有效性。这个流程的实现依赖于DID文档、可验证凭证与可验证表达这三个核心数据结构的协同工作。

DID的技术流程始于其作为一个可解析的标识符。DID标识符 “did:method:identifier” 的URI结构本身就指明了技术指令： “method” 字段指明了需要遵循哪一套具体的技术规范， “identifier” 则是在该规范下的唯一地址。通过标准化的解析组件，任何人都能够将一个DID解析为其关联的DID文档。该文档是一个结构化的数据对象，它包含了与DID主体相关的元数据，是实现身份验证和安全交互的核心。而具体的身份属性声明，则通过可验证凭证（Verifiable Credential, VC）来承载，它是由一个权威的签发方为持有方颁发的、带有密码学签名的数字声明。当持有方需要证明这些声明时，会将一个或多个VC打包进一个可验证表达（Verifiable Presentation, VP）中，并附上自己的签名，用于向验证方出示。在这一系列交互中，DID文档扮演着密码学公钥目录的关键角色。文档中定义了持有方持有密钥的公钥信息以及密钥与权限的绑定关系。这种设计允许一个DID主体拥有多个不同用途、不同安全等级的密钥，并能安全地进行密钥轮换和授权管理。

在DID框架中，具体的身份属性声明通过VC来承载。VC是由签发方对持有方身份相关的声明内容 “credentialSubject” 进行数字签名的结构化数据包。签名过程使用签发方在其DID文档中所声明公钥对应的私钥进行，从而将声明的真实性与签发方的去中心化身份绑定。当持有方需要向验证方证明其声明时，他会创建并递交一个VP，签名过程使用持有方在其DID文档中所声明公钥对应的私钥进行。这个过程构成了一个双重密码学证明：VC的签名证明了声明的来源和内容的真实性，而VP的签名则证明了持有方同意将一份真实的声明呈现给验证方。重要的是，VP可以包含一个或多个完整的VC，也可以利用基于默克尔树和默克尔验证的证明技术，支持选择性披露以及零知识证明，即仅暴露持有方VC中想要证明的部分字段，甚至是对部分字段的断言（例如年龄字段的值大于18）。然而，目前VP中的零知识证明方案存在固有局限，主要在于只能针对数据存在于某个可分割的有限区间生成断言，这种局限性构成了本研究的出发点，我们将在后续章节进行深入探讨。

[此处可插入一张图表，以流程图形式详细描绘DID认证的技术验证链。图表应包含Verifier、Holder的DID Doc、Issuer的DID Doc以及VDR。箭头应清晰表示：1. Verifier从VP中提取Holder DID和Issuer DID；2. Verifier查询VDR获取两个DID Doc；3. Verifier使用Holder的authentication公钥验证VP签名；4. Verifier使用VC中指定的Issuer公钥验证VC签名。]

因此，一个完整的DID认证流程在技术上构成了一个双重验证链。验证方首先通过解析持有方的DID，获取其认证公钥以验证整个VP的签名，以确认持有方对凭证的控制权和呈现意图。随后，验证方会进一步解析签发方的DID，以获取对应的公钥来验证VC自身的签名，以确认声明的来源可信且内容完整。当这条从持有方到签发方的密码学信任链条完整且全部验证通过，验证方即可安全地接受该声明。

DID信任模型的闭环依赖于一个公开、可信的可验证数据注册表VDR，用于记录DID与其DID文档之间的权威绑定关系。虽然分布式账本技术（DLT）特别是区块链，因其固有的不可变性、去中心化和共识机制，被公认为是VDR的技术选型，但W3C的DID规范本身并不限定其具体实施技术，这依赖于实施者自身。这里可以加本文不关心VDR的实现形式，然后这一整段可以找机会说在附录中的DID密码套件规范，也可以在第二章最后说

2.2密码学基础与困难性假设

我们的整体方案的安全性严格建立在特定的密码学工具与公认的计算困难假设之上。我们将在后续介绍方案中的两个子协议时引述其相关背景知识，而本节则聚焦于对最核心的理论基础进行形式化定义。具体而言，本节将首先介绍方案所依赖的双线性配对数学环境，随后形式化地描述两个重要的计算困难问题，它们将作为后续安全性分析的规约基础。

**2.2.1 双线性配对**

在现代密码学中，源于代数几何的双线性配对（Bilinear Pairings）已成为构建高级密码协议的关键工具，它使得在椭圆曲线群上实现复杂的代数运算成为可能。一个椭圆曲线群由定义在域上的Weierstrass方程的所有点及无穷远点构成。通过几何上的弦切法，该点集构成一个阿贝尔群，其中为单位元，这为后续的配对运算提供了基础的代数结构。与依赖大整数分解或离散对数问题的传统公钥密码体制相比，椭圆曲线密码学最显著的优势在于它可以用更短的密钥长度达到同等的安全强度，这使得它在计算和存储资源受限的环境中尤为实用。

定义1（双线性配对）：双线性配对是在以上椭圆曲线的子群上定义的一种特殊映射。设和为椭圆曲线上的循环子群，为一个乘法循环群，其阶均为大素数。双线性配对是一个满足以下三种特性的映射：

(1)双线性：对于任意的以及任意的，以下等式恒成立：

若为乘法群，则形式如下:

(1)

(2)非退化性：映射不是平凡的。即存在生成元的配对结果不等于目标群的单位元:

(3)可计算性：该性质保证了配对的实用性。即存在一个高效的多项式时间算法(如米勒算法)可以计算出任意输入对的配对结果。

在本文描述的方案中，我们假设存在一个双线性群生成器。它接收一个安全参数作为输入，并为所有参与方输出一套完整的双线性配对环境参数。其中和是素数阶群，是一个有效的、非退化性的双线性映射，和分别是群和的生成元。

**2.2.2 计算困难假设**

密码学方案的安全性，通常需要将其被攻破的难度归约到某个被充分证明的计算困难问题上，许多计算困难问题源于基础的计算困难假设（如离散对数问题）。为了论证的简洁性，以下介绍两个与我们方案直接相关的困难性问题。

定义2（计算性共同迪菲-赫尔曼问题）：对于一个阶为素数的群，定义敌手的优势为

其中概率是通过内部的随机性和的随机选取计算。如果能在最多的时间内运行并且有，那么它就能破解计算性共同迪菲-赫尔曼问题。如果不存在这样的敌手，我们称计算性共同迪菲-赫尔曼问题是困难的。

定义3（q-强迪菲-赫尔曼假设）：如果对任意概率性多项式时间图灵机敌手，给定一个元组，其中，且，输出一对，其中的几率在安全参数中是可忽略的，那么我们就说对于一个双线性配对生成器的q-强迪菲-赫尔曼假设成立。

2.3一种紧凑的多重签名

多重签名是一种基于公钥密码学的数字签名方案，允许多个签名者对同一份文件进行签名，以确保签名的有效性和不可抵抗性。在我们的方案中，多重签名是实现多方授权的核心技术组件。当一个用户需要访问某项受保护的服务时，必须获得多个授权机构的共同批准。这些分散的批准最终将通过密码学方式聚合成一个单一、有效的多重签名，作为用户获得最终访问权限的凭证。

我们遵循[9,13]本科论文引用中的定义，将多重签名方案定义为算法和。一个受信机构生成系统参数。每个签名者都生成一对密钥，签名者可以通过各自调用交互式算法来集体签名一个消息，其中是签名者的公钥集合，是签名者的私钥。在协议结束时，每个签名者都输出一个签名。算法在输入一组公钥时，输出一个唯一的聚合公钥。验证者可以通过运行来检查聚合公钥下消息的签名的有效性，输出0或1，分别表示该签名无效或有效。

一个多重签名方案应该满足完整性，也就是说，对于任何，如果我们有，其中，和任何消息，如果所有签名者都输入，那么每个签名者都会输出一个签名，使得。第二，多重签名方案应该满足不可伪造性。多重签名方案的不可伪造性由一个被详细定义的三阶段博弈定义：设置、签名询问和输出[13]。

定理 1（广义分叉定理）：设是一个随机算法，是一个在时间内运行的随机算法，最多进行个随机预言机查询，成功的概率为。如果，则 的运行时间最多为，成功的概率至少为，其中的概率取决于的选择和的结果。关于广义分叉算法的定义在[7]中给出，这里不再赘述。

定义 4：如果在时间内运行，执行了签名查询和随机预言机询问，并以至少的概率赢得上述博弈，我们就说是多重签名方案 的一个伪造者。如果不存在伪造者，那么就是不可伪造的。

我们方案中的多方授权机制使用了一种紧凑的多重签名[7]，这种签名基于BLS签名。

首先简要回顾一下BLS签名方案和它的聚合机制。该方案需要：(1) 一个可有效计算的非退化配对 ，其中 为素数阶群，我们设和分别是和的生成元。(2) 一个哈希函数。

BLS签名方案的工作原理如下：(1)密钥生成：选择一个随机的并输出，其中。(2) : 输出。(3)验证函数 : 如果 则接受, 否则拒绝。

这个签名方案支持一个简单的签名聚合过程。给定三元组，其中，可以通过以下计算将签名聚合成一个短聚合签名：

(2)

为了验证 的有效性，计算如下等式:

(3)

注意验证过程需要所有的 ，其中 。在我们的方案中，我们考虑所有被签名的消息都是一样的 ，此时验证条件(2) 就简化为了一个更简单的形式 ，只要求两个配对满足:

(4)

而且, 只需要给验证者一个短的聚合公钥 。

考虑以下流氓公钥攻击：攻击者注册了一个流氓公钥 ，其中是某个不知情的用户Bob的公钥，由攻击者选择。然后，攻击者可以通过提出聚合签名来声称它和Bob都签署了某个消息。这个签名是两个签名的聚合，一个来自，一个来自，因为：

因此, 满足 (3)。实际上，攻击者对消息承诺了Bob用户，而Bob却没有签署 。

在[7]中，作者提出了一种不同的防御方法来抵御这种攻击。方案流程如下。

首先进行参数生成，生成并输出一个双线性群。

进行密钥的初始化，授权机构选择，计算，并输出，每一个授权机构拥有自己独立的密钥。

进行公钥聚合，输出聚合公钥。

然后进行签名。签名是一个单轮协议。计算，其中。将发送给一个指定的聚合者，在我们的方案中它为用户，它收集所有单个签名并将最终签名计算为。在我们的方案中，在收集每一个签名之前，用户需要在对应授权机构处完成匿名认证。

最后通过如下式子，验证多重签名有效性，如果等式成立证明有效：

[7]中对上述方案进行了安全证明，以抵御流氓公钥攻击，这里我们进行简单的介绍。

作者将他们提出的基于BLS的多签名方案称为，并提出如下定理：在随机预言机模型中，在计算性的共同迪菲-赫尔曼问题下是一个不可伪造的多重签名方案（如定义4所述）。更确切地说，如果，并且共同迪菲-赫尔曼问题是困难的，则称在随机预言机模型中是不可伪造的，其中是单个多重签名中涉及的最大签名者数量，和分别表示在和中计算指数所需的时间，和分别表示在和中计算个多重指数所需的时间。

以下对这个定理的证明过程进行了简单总结。首先假设一个针对 多重签名方案的 伪造者，它利用算法进行流氓公钥攻击。经过推导，计算出的整体成功概率为 ，通过定义4我们可以知道，这证明了这个多重签名方案是不可伪造的。然后，作者通过构建算法来证明此定理，使用上述算法运行来自定理1的广义分叉算法，最后证明了如果，在时间上最多运行 并且成功概率，这证明了多重签名方案在随机预言机模型中不可伪造。

2.4一种基于签名的零知识集合成员证明

**2.4.1零知识证明和Σ-协议**

零知识证明由S.Goldwasser、S.Micali及C.Rackoff[25]提出，它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

我们遵循[2,11]中的定义。一对相互作用的算法是关系的知识证明，知识误差，条件是对于所有以概率1接受与的对话；并且存在一个预期的多项式时间算法，称为知识提取器，这样，如果一个伪造的证明者有概率说服接受，那么在给定的可回溯黑盒访问权时，输出一个概率为的的见证。

如果存在一个概率性多项式时间图灵机算法（称为模拟器），那么一个证明系统是诚实验证者零知识的，这样对于任何，与交互后的输出与的输出在计算上不可区分。

协议是一个证明系统 ，其会话形式为，其中和由计算， 是由随机选择的挑战。如果对于某个可有效计算的表述，如果，验证者就接受，给定了的两个接受会话 和，可以有效地计算见证。 而且，存在一个多项式时间模拟器，它在输入和随机字符串上输出的接受会话，这与和之间的真实会话完全没有区别。

我们使用Camenisch和Stadler[16]引入的符号来进行离散对数知识的各种零知识证明和关于离散对数的表述有效性的证明。例如，

它表示一个对整数 和的知识的零知识证明，使得 和 成立，其中 , 和是群 和 的元素。

**2.4.2集合成员证明**

给定集合，要证明一个元素，称为集合成员证明。

我们遵循[9]中对证明过程的定义，设(Gen, Com, Open)是一个字符串承诺方案的生成、承诺和开放算法。对于一个实例，对于承诺方案和集合的集合成员证明是对以下表述的知识证明：

该证明系统是针对所有承诺方案而定义的。因此，特别是，如果Com是一个完全隐藏的方案，那么语言由所有的承诺组成（假设非空）。因此对于可靠性来说，协议是知识证明的这一点很重要。

# 第三章 方案设计

## 3.1整体构思

在金融领域中，金融机构需要对多个客户的共同资金的支出进行验证和审计，这需要多个客户的共同授权以确保交易的合法性。然而，在多方授权的交易验证过程中可能会暴露请

## 3.3安全性分析

**3.3.1 多方授权**

我们的方案使用了[7]中的多重签名方案，在2.2.1节中我们介绍了这个方案的安全模型。

**第四章 系统实现与实验分析**

4.1系统的实现

**4.1.1 实现方法**

如上文所述，我们的系统协议适用于多种应用场景，在实际应用中，可以把这种系统视作分布式的。我们对系统进行实现的目的是对我们的方案进行实验仿真测试，以得出数据，再通过数据分析系统的可行性、性能和效率。我们并不是要实现为现实应用场景服务，因为现实的应用场景是基于网络的，其中参与方通过网络通信，而我们的实验模拟在本地进行。

# 第五章 总结与展望

## 5.1工作总结

本文我们设计与实现了一种具有隐私保护的多方授权系统，它的创新之处在于结合了隐私保护和多方授权的相关协议，实现了可靠的多方授权和安全的隐私保护，能够应用于多种现实应用场景，如比特币交易。我们基于过往研究，利用一种多重签名方案实现多方授权，并在授权的认证环节，利用一种基于零知识证明的匿名认证方案实现了隐私保护，理论上这个系统具有足够高的安全性。我们用程序实现了这个系统，并进行了实验测试与分析。在改变授权机构的数量的条件下，用多个实验组测量数据。测得的数据反映出系统的执行时间受授权机构数量的影响较大。总体上来看，我们的系统具有良好的性能和效率。

# 参考文献

1. AC SQUICCIARINI, A CINZIA, SM RAJTMARJER, N ZANNONE, et al. Multi-Party Access Control: Requirements, State of the Art and Open Challenges[C]. The 23nd ACM on Symposium on Access Control Models and Technologies, 2018. 49-49.
2. RS SANDHU, EJ COYNE, HL FEINSTEIN, CE YOUMAN. Role-based access control models[J]. Computer, 1996. 29(2): 38-47.
3. H KINKELIN, H NIEDERMAYER, M MULLER, G CARLE. Multi-party authorization and conflict mediation for decentralized configuration management processes[C]. IFIP/IEEE Symposium on Integrated Network and Service Management, 2019. 5-8.
4. V GOYAL, O PANDEY, A SAHAI, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]. The 13th ACM conference on Computer and communications security, 2006. 89-98.
5. A BOLDYREVA, V KUMAR, V GOYAL, et al. Identity-Based Encryption with Efficient Revocation[C]. The 15th ACM conference on Computer and communications security, 2008. 417-426.
6. B LASHKARI, P MUSILEK. A comprehensive review of blockchain consensus mechanisms[J]. IEEE Access, 2021. 9: 43620-43652.
7. D BONEH, M DRIJVERS, G NEVEN. Compact multi-signatures for smaller blockchains[C]. The 24th International Conference on the Theory and Application of Cryptology and Information Security, 2018.
8. J HAN, L CHEN, S SCHNEIDER, et al. Privacy-preserving electronic ticket scheme with attribute-based credentials[J]. IEEE Transactions on Dependable and Secure Computing, 2019. 18(4): 1836-1849.
9. J CAMENISCH, R CHAABOUNI, A SHELAT. Efficient protocols for set membership and range proofs[C]. The 14th International Conference on the Theory and Application of Cryptology and Information Security, 2008. 234-252.
10. Y XIAO, P ZHANG, Y LIU. Secure and efficient multi-signature schemes for fabric: An enterprise blockchain platform[J]. IEEE Transactions on Information Forensics and Security, 2020. 16: 1782-1794.
11. D BONEH, B LYNN, H SHACHAM. Short signatures from the Weil pairing[C]. The 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, 2001.
12. D BONEH, X BOYEN. Short signatures without random oracles[C]. International Conference on the Theory and Applications of Cryptographic Techniques, 2004.
13. M BELLARE, G NEVEN. Multi-signatures in the plain public-key model and a general forking lemma[C]. The 13th ACM conference on Computer and communications security, 2006. 390-399.
14. BN Jagdale, JW Bakal. A novel authentication and authorization scheme in P2P networking using location-based privacy[J]. Evolutionary Intelligence, 2022. 15(2): 1251-1264.
15. M Wetzels, I Ayoola, S Bogers, et al. Consume: A privacy-preserving authorisation and authentication service for connecting with health and wellbeing APIs[J]. Pervasive and Mobile Computing, 2018. 43: 20-26.
16. J CAMENISCH, M STADLER. Efficient group signature schemes for large groups[C]. The 17th Annual International Cryptology Conference Santa Barbara, 1997.
17. J CAMENISCH, G NEVEN, A SHELAT. Simulatable adaptive oblivious transfer[C]. The 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2007.
18. Y DODIS, A YAMPOLSKIY. A verifiable random function with short proofs and keys[C]. The 8th International Workshop on Theory and Practice in Public Key Cryptography, 2005.
19. AA BATTAH, MM MADINE, H ALZAABI, et al. Blockchain-based multi-party authorization for accessing IPFS encrypted data[J]. IEEE Access, 2020. 8: 196813-196825.
20. KL TAN, CH CHI, KY LAM. Secure and privacy-preserving sharing of personal health records with multi-party pre-authorization verification[J]. Wireless Networks, 2022. 1-23.
21. M MAMUN, A MIYAJI, R LUV, et al. A lightweight multi-party authentication in insecure reader-server channel in RFID-based IoT[J]. Peer-to-Peer Networking and Applications, 2021. 14: 708-721.
22. J SUN, G XU, T ZHANG, et al. Verifiable, Fair and Privacy-Preserving Broadcast Authorization for Flexible Data Sharing in Clouds[J]. IEEE Transactions on Information Forensics and Security, 2022. 18: 683-698.
23. S SHIN, T KWON. A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things[J]. IEEE access, 2020. 8: 67555-67571.
24. S LIU, L CHEN, G WU, et al. Blockchain-Backed Searchable Proxy Signcryption for Cloud Personal Health Records[J]. IEEE Transactions on Services Computing, 2023.
25. S GOLDWASSER, S MICALI, C RACKOFF. The knowledge complexity of interactive proof-systems[M]. Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, 2019. 203-225.
26. B LYNN. PBC library manual 0.5.11[J]. 2006.

**附录A 仿真系统源代码**

以下为主函数所在源文件的代码：