**一种抗女巫攻击的可监管隐私身份管理方案**

1. **技术领域**

本发明属于安全密码应用技术领域，具体涉及一种抗女巫攻击的可监管隐私身份管理方案。

1. 背景技术
   1. 密码学方案

本发明中涉及的密码学方案主要包括以下五种：

1. 秘密分享：用于将一个秘密分为若干个互不相同的片段，只有超过一定数量的片段才能恢复出秘密。一种常用的秘密分享方案是Shamir方案，当接收秘密片段的人数为n，且要求不少于t个人即可恢复秘密时，又称为-Shamir秘密分享；
2. 零知识证明：用于在不提供一组数据具体值的同时证明其满足特定条件，保证数据隐私；
3. 数字签名：用于认证某一数据由某个确定的实体给出；
4. 默克尔树：允许数据持有方对一组数据作出承诺，并有能力证明任意给定数据存在/不存在于该组数据中；
5. 广义Pedersen承诺：用于将身份属性的值隐藏至承诺中；
6. 门限公钥加密（TPKE）：加密过程与传统公钥加密相同，但解密需要某一阈值t以上数量的解密密钥持有者共同参与方可完成。具体地，各参与方可用自己的部分密钥解密得到明文的“部分解密”，但必须基于阈值以上数量的部分解密才能计算出完整密文。
   1. 可监管身份管理方案

受益于区块链的开放性和不依赖可信第三方的特性，去中心化应用程序（DApp）在多个领域取得了长足发展。但这些特性又导致又导致DApp在使用基于用户真实身份的访问控制机制时面临限制甚至潜在的法律法规风险。一种简单的实现基于身份的访问控制的解决方案是在用户钱包上附加一个由凭证颁发机构（CA）签发的凭证，以将用户地址与其真实身份进行绑定。但这种解决方案存在泄露用户身份信息的风险。如何在区块链上实施基于身份的访问控制，同时保护用户的身份隐私安全，这是一项重大挑战。

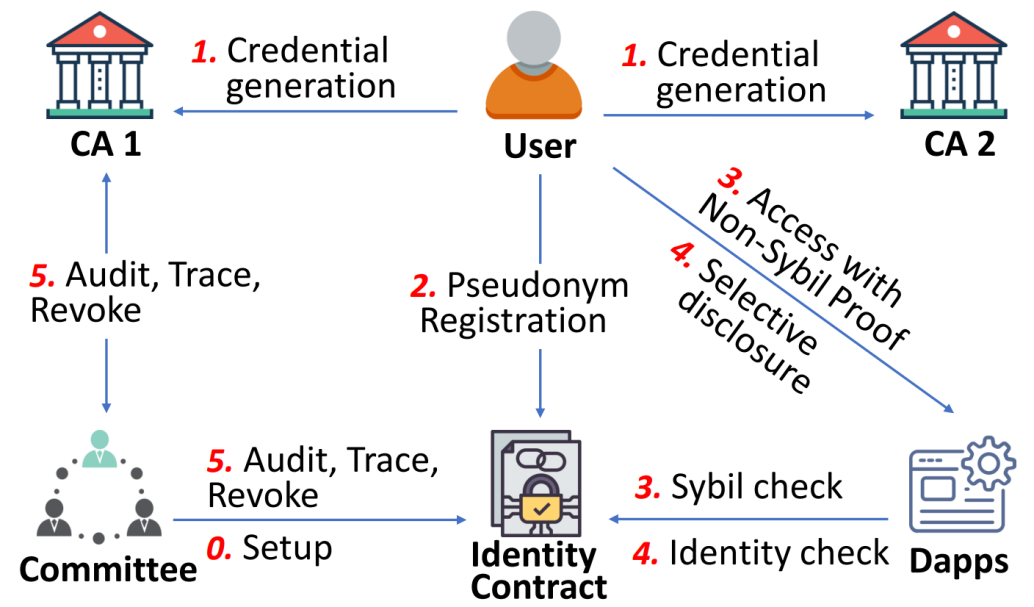
尽管现有的基于去中心化身份和假名凭证的方案具有很强的隐私保护特性，但也存在三个明显的局限性，即对监管治理（可审计、可追踪、可撤销）支持不足、无法抵抗女巫攻击和运行效率低下。

1. 发明内容

为了突破以上三个局限性，本发明提出了一种抗女巫攻击的可监管隐私身份管理方法，支持全面的监管治理机制（可追溯、可审计、可撤销）和细粒度的抗女巫攻击，同时提供强大的隐私保护能力，并具有去中心化（所有身份管理操作均由一个包含多个不同实体的委员会完成）、支持大规模假名追踪、高效率（大部分追踪计算都可以在单个节点上本地执行）、支持选择性链接（允许用户在不泄露身份相关信息的情况下选择性地披露其假名的链接性）等多个优秀关键特性。

* 1. 系统模型

为实施本发明，需构建由一系列链外程序和链上合约组成的系统，系统架构如下图所示。



1. 委员会：由负责系统管理和身份监管治理的多个不同实体组成。委员会的工作方式是门限式的，即所有操作都需要至少t个实体的合作。
2. 凭证颁发机构（CA）：一个授权机构，负责验证和存储用户的身份属性，并协助委员会进行监管治理。系统支持多个CA，允许由不同的CA验证身份属性，每个CA可以验证不同的身份属性；
3. 身份合约：一种系统合约，用于验证、存储和管理用户的假名。具体地，用户可以调用身份合约注册假名，并将其与特定身份属性绑定。此外，身份合约还提供身份检查、抗女巫攻击检查和监管治理接口；
4. DApp：部署在区块链上的一系列智能合约。它可以调用身份合约来执行身份检查和抗女巫攻击检查；
5. 用户：使用假名（如链上账户地址）与DApp进行交互，证明其访问符合DApp的访问控制，如身份证明和非女巫地址证明。系统假设用户可能作恶，即任意采取行动以获得利益。
   1. 系统设置与工作流程
      1. 门限加密设置

系统开始运行时，委员会运行分布式密钥生成协议得到，其中sk保持隐私，但每个委员会成员都通过-Shamir秘密分享协议获得sk的一个份额，即只有不少于t个成员进行合作才能得到完整sk。委员会将与各个公开至身份合约中；

* + 1. 零知识证明设置

系统可以采用任何已有的通用零知识证明方案实现。特别地，如采用目前应用较为广泛的zk-SNARK类方案，则需要在开始运行时一次性地生成一组称为公共参考串（CRS）的数据，系统中的委员会成员可以通过任何现有的多方安全计算协议实现这一点。

* + 1. 系统工作流程

系统的整体工作流程如下：

（1）用户向CA列表中的CA申请凭证；

（2）用户可以用获得的凭证在身份合约中注册假名；

（3）应用程序可以创建具有自定义访问控制策略的抗女巫实例（如有需要）；

（4）用户通过非女巫证明或身份属性断言证明访问DApp；

（5）如果发现用户或假名是恶意的，委员会将披露或撤销与身份相关的信息和所有相关的假名。

* 1. 系统运行方式
     1. 凭证生成

用户U首先生成两个随机数和，前者作为用户私钥，后者作为追踪陷门。之后用户向CA发送和。为实现可追踪性，用户必须向CA提供追踪陷门的TPKE密文作为追踪字符串，将追踪陷门与委员会公钥一并加密：

其中为随机数，和分别代表取椭圆曲线点的横、纵坐标，函数将一个数值编码为椭圆曲线上的一个点。进一步地，为确保用户提交的加密陷门正确，用户还需向CA提交一组零知识证明数据，论证用户确实拥有且提交的密文确实由二者正确计算得到。

最终，用户将、零知识证明数据和包含了待授权身份属性的文档提交给CA，CA验证通过后向用户颁发凭证，其中A为用户身份属性的承诺值，e为凭证有效期，为CA对凭证内容的签名。

* + 1. 假名注册

用户可以在利用凭证身份合约上注册假名（即区块链地址）。用户在注册假名时必须为其设置一个有效期，且为注册的每个假名绑定一个身份承诺，这是一个能够完美隐藏身份属性的广义Pedersen承诺，必须根据用户凭证中包含的身份属性值承诺和一个每次注册假名时都不同的秘密随机数进行计算得到。

为了在必要时给出真实身份信息，用户需要为每个假名提供一个审计串，该字符串是用户公钥和发行者公钥的TPKE加密。为防止攻击者对其他假名复用该串，审计串的编码包含其对应的假名，使其只对对应假名有效：

进一步地，为保证假名可追踪，系统对上式中随机数的生成方式作了限制，要求其计算必须包含凭证对应的追踪陷门和一个特定范围内的nonce值。

用户还需要通过零知识证明来证明上述信息的正确性，并证明自己是凭证的所有者。具体地，用户在系统中向身份合约发起交易，提交上述数据，身份合约验证零知识证明并做其他有效性检查。一旦验证通过，注册即被接受，用户的假名有效期、承诺值与审计串将被记录在身份合约中。此外，用户还需要证明所使用的凭证未被撤销，且签发者是系统的CA成员。为此，系统委员会维护了两棵默克尔树，即CA树和撤销树，前者用于存储所有CA的公钥，后者存储所有已撤销凭证的主公钥。在添加新CA或撤销凭证时，委员会将更新这两棵树并在只能合约上记录新的树根哈希值。

* + 1. 应用程序抗女巫攻击

系统提供了一种n次访问令牌生成方案，输入凭证私钥和抗女巫攻击实例ID作为输入，最多可输出n个不同的令牌：

其中，为凭证的私钥，为抗女巫攻击实例ID，nonce的上限可以由各个应用根据用户属性数量自主确定，并实现在特定的限制函数limit()中。

实现抗女巫攻击时，应用程序首先要初始化一个具有实例ID 和nonce限制的抗女巫攻击实例。访问应用程序的用户应为其使用的每个假名提供一个用该实例ID生成的访问令牌。用户还需要基于所用假名的审计串与Pedersen承诺生成零知识证明以表明所提供令牌的正确性（为了提高效率，应用程序可以将其nonce限制方案硬编码到专用零知识证明电路中）。最后，应用程序检查访问令牌是否有重复并验证证明。

* + 1. 用户访问DApp

用户访问DApp时，为满足访问控制要求，用户可能需要向应用程序证明其身份属性符合某些要求（例如年满18岁）。为此，用户可以向Dapp提供零知识证明，以证明其绑定到承诺值的身份属性满足给定的要求而无需透露这些值。

* + 1. 监管治理机制

审计：在假名注册流程中，用户需要向身份合约提交一个审计串，该串是用户公钥和发行者公钥的TPKE加密。如果一个假名有恶意行为，其身份相关信息可能会被一定数量的（不少于t个）委员会成员按以下方式披露：委员会首先从身份合约中获取对应的，然后由不少于t个成员共同解密以恢复和，之后通过查询所标识的 CA，揭示与假名关联的身份信息。

追踪：为了追踪用户，监管机构可要求签发对应凭证的CA将追踪串提交给委员会，之后不少于t个委员会成员可以合作解密以恢复追踪陷门。之后，监管方可以自行计算所有特定范围内的nonce及其对应的假名生成用随机数。于是在已注册的假名中，所有其审计串的第一个元素为的假名都属于被调查的用户。由于委员会成员中诚实用户占多数，因此追踪诚实用户是不可行的。

撤销：当委员会中不少于t个成员同意时，凭证或假名就可以按以下方式被撤销：委员会首先将该凭证的公钥（即）添加到撤销树中，然后将新撤销树的根提交给有不少于t个成员签名的身份合约，此后使用该凭证的假名注册证明将无法通过验证；撤销假名时，不少于t个委员会成员会在身份合约中将该假名的状态更新为“已撤销”。状态为“已撤销”的假名将不再有效。