

基于区块链的跨数据中心匿名可监管身份认证方案

徐淑奖^{1,2}, 张朝阳^{1,2}, 王连海^{1,2}, 张淑慧^{1,2}, 邵蔚^{1,2}

(1. 齐鲁工业大学(山东省科学院)山东省计算中心(国家超级计算济南中心)

算力互联网与信息安全教育部重点实验室, 山东 济南 250014;

2. 山东省基础科学研究中心(计算机科学)山东省计算机网络重点实验室, 山东 济南 250014)

摘要: 随着大数据和云计算技术的发展, 金融机构之间跨机构数据共享交互日益增多。由于隐私泄露事件的频繁发生, 数据安全保护面临着严峻的挑战, 也对跨数据中心的身份认证等数据安全治理技术提出了更高的要求。传统的中心化身份认证方案在安全性和可扩展性方面存在缺陷, 难以满足高频跨中心数据共享的应用需求。区块链具有分布式、难以篡改、可追溯、多方共识等优异特性, 为跨数据中心身份认证提供了崭新的思路。在实际应用场景中, 不仅要对用户身份隐私进行保护, 还需要对用户的匿名身份进行有效的监管。提出了一种基于区块链的匿名可监管的跨数据中心身份认证方案, 不改变各数据中心原有架构, 以各数据中心的治理节点为中心建立分布式多中心的联盟链; 利用区块链技术, 保障身份认证过程的透明性和可信性; 采用属性签名保护用户身份隐私, 并建立身份映射表追踪用户真实身份, 实现用户身份隐私保护和监管兼顾的跨数据中心身份认证。安全性分析和仿真实验结果表明, 该方案无须用户再次注册, 具有不可伪造性和可追踪等特性, 能够抵御重放攻击、拒绝服务攻击、篡改攻击、中间人攻击等网络攻击。

关键词: 数据安全; 区块链; 身份认证; 隐私保护; 身份监管

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024031

Blockchain-based cross-data center anonymous and verifiable identity authentication scheme

XU Shujia^{1,2}, ZHANG Chaoyang^{1,2}, WANG Lianhai^{1,2}, ZHANG Shuhui^{1,2}, SHAO Wei^{1,2}

1. Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China

2. Shandong Provincial Key Laboratory of Computer Networks,
Shandong Fundamental Research Center for Computer Science, Jinan 250014, China

收稿日期: 2023-03-16; 修回日期: 2024-04-10

通信作者: 徐淑奖, xsj@qlu.edu.cn

基金项目: 山东省重点研发计划 (No.2021CXGC010107); 泰山学者项目 (No.tsqn202312231); 济南市新高校二十条项目 (No.202228017)

Foundation Items: The Shandong Provincial Key Research and Development Program (No.2021CXGC010107), The Taishan Scholars Program (No.tsqn202312231), The New 20 Project of Higher Education of Jinan (No.202228017).

引用格式: 徐淑奖, 张朝阳, 王连海, 等. 基于区块链的跨数据中心匿名可监管身份认证方案[J]. 网络与信息安全学报, 2024, 10(02): 47-58.

Citation Format: XU S J, ZHANG C Y, WANG L H, et al. Blockchain-based cross-data center anonymous and verifiable identity authentication scheme[J]. Chinese Journal of Network and Information Security, 2024, 10(02): 47-58.

Abstract: With the progression of big data and cloud computing technologies, there has been an escalating trend in cross-institutional data sharing and interaction within the financial sector. However, the frequent occurrence of privacy breaches poses significant challenges to ensuring data security protection. This necessitates the elevation of requirements for identity authentication across data centers and other technologies related to data security management. The traditional centralized identity authentication schemes are inherently flawed in security and scalability, which hampers their ability to meet the demands of high-frequency cross-center data sharing applications. The blockchain technology has emerged as a potential solution, offering exceptional characteristics such as a distributed nature, tamper-proof properties, traceability, and the ability to achieve multi-party consensus. In practical application scenarios, it is essential to not only protect the privacy of user identities but also to effectively regulate anonymous identities. An anonymous and supervisable cross-data center identity authentication scheme based on blockchain was proposed. This scheme did not necessitate alterations to the original architecture of each data center. Instead, a distributed multi-center consortium blockchain was formed by leveraging more than one server from each data center to establish a data center union. Blockchain technology was utilized to ensure the transparency and reliability of the identity authentication process. Additionally, attribute signatures were employed to safeguard user identity privacy while simultaneously creating an identity mapping table that facilitated the tracking of real user identities. Consequently, the scheme was designed to protect user privacy during cross-data center identity authentication and to enable effective supervision over anonymous identities. A thorough security analysis and the results of experiments demonstrate that the proposed scheme possesses the following attributes: it does not require users to re-register, it exhibits characteristics of unforgeability and traceability, and it is capable of withstanding various network attacks, including replay attacks, denial of service attacks, tampering attacks, and man-in-the-middle attacks.

Keywords: data security, blockchain, identity authentication, privacy protection, identity regulation

0 引言

随着计算机技术的不断发展,银行业务逐渐实现数字化、网络化和智能化。为了加强合作、提升服务水平、实现共赢发展,以服务中小微企业和城市居民为主的城商银行纷纷组建城商银行联盟。通过联盟的协作,城商银行可以实现客户资源的整合、业务创新的共享、风险管理的协同,客户可以通过联盟内各成员银行的网上商城进行跨行购物和优质理财产品的购买,提高联盟成员银行的综合服务能力和经营效益。

在信息技术高度发展的数字时代,城市商业银行都有自己的网上银行和网上商城,但是跨金融机构的网上商城购物和理财产品购买都需要进行跨信任域或跨数据中心的数据交互。包括用户数据在内的金融数据是银行业务的核心资产,对银行的稳健经营和客户信任至关重要。城商银行联盟的建立可以使城市商业银行之间分享资源、互惠互利,但是跨机构跨数据中心交互所引发的金融数据安全问题也随之而来^[1]。身份认证技术

可以防止未经授权的人员和非法行为者获取、篡改、窃取金融数据和敏感信息,有效保护金融数据安全。各城商银行数据中心会设置本地认证服务设备,为本行的金融数据共享交互提供认证服务^[2]。然而,跨数据中心数据共享交互涉及城商银行的金融数据安全和用户的隐私保护问题,对跨数据中心身份认证提出了更高的要求,因此,实现不同城商银行之间安全可控的匿名身份认证已成为跨机构跨数据中心数据安全共享和隐私保护亟须解决的瓶颈问题。

学者在跨数据中心身份认证方面已经开展了一些研究工作。**Chen**等^[3]提出了一种基于区块链的去中心化跨域身份管理系统,解决了集中式机制的单点故障问题。**Lee**和**Jeong**^[4]构建了一种基于区块链的生物特征认证系统,为生物特征信息管理提供了一种可审计的身份认证机制。**Zhang**等^[5]基于区块链实现了去中心化的跨域身份认证,解决了“不完全跨域”的问题。**Wang**等^[6]设计了一种基于多证书颁发机构(certificate authority, CA)的认证体系结构,在多个信任域之间

建立分布式信任,共享跨域证书信息;并提出了一种简化的身份认证方案,可以快速完成跨域身份认证。Chen等^[7]提出了一种基于公钥基础设施的、具有隐私保护功能的跨域认证方案,并设计了一种基于多层默克尔树的轻量级正确性验证协议进行快速响应。牛建林等^[8]针对传统跨域认证易单点失效、过度依赖第三方等安全问题,结合基于身份的密码体制与联盟链,提出了一种安全可用的跨域认证方案。上述研究虽然较传统跨域身份认证方案有了一定的进步,但是仍然没有有效解决用户隐私保护问题。

随着属性基加密(attribute-based-encryption, ABE)技术的进步和发展,属性签名(attribute-based-signature, ABS)技术逐渐引起相关领域的专家和学者的关注。2008年,Maji等^[9]首次提出一种基于属性的数字签名方案,可以有效保护用户的隐私信息,具有广泛的应用前景。为了满足多属性授权的实际场景应用需求,Cao等^[10]和Sun等^[11]提出了一种多属性授权机构的属性签名方案。但是在这些方案中,仍然存在单个可信中心。Liu等^[12]提出了一种多权威属性签名的安全车辆感知方案,保护感知车辆的隐私。唐飞等^[13]结合分布式密钥生成技术,提出了一种基于属性的多授权中心的身份认证方案,可有效抵抗合谋攻击,并实现了基于用户多因子的身份认证机制。Lu等^[14]提出了一种基于属性的环签名方案,并将其应用于电子健康记录系统。Yuan等^[15]提出了一种新型的基于属性签名和分布式公钥基础设施的身份认证方案,对身份进行细粒度管理,实现了匿名身份认证。但是这些方案没有考虑跨数据中心身份认证和匿名身份的监管性问题。

对比分析上述方案不难发现,目前现有的跨数据中心身份认证仍然存在以下挑战。

- (1) 去中心化细粒度身份管理问题。
- (2) 用户身份隐私保护问题。
- (3) 匿名身份监管问题。

在实际应用场景中,不仅要考虑用户隐私保护,还需要对用户的身份进行有效监管。因此,需要构建用户隐私保护和身份监管两者兼顾的高效的跨数据中心身份认证方案。

针对跨数据中心应用场景中用户身份认证面

临的挑战,为满足实际应用需求,本文利用属性签名和门限签名技术,建立身份映射表,提出一种基于区块链的匿名可监管的跨数据中心身份认证方案。主要工作和贡献如下。

(1) 设计了一种基于区块链的跨数据中心身份认证模型,不存在任何单一的第三方可信机构,实现了真正意义上的去中心化;跨数据中心身份认证时,无须用户再次注册,简化了认证流程;支持数据中心自定义证书颁发策略,提高了各数据中心的自主性。

(2) 提出了一种基于分布式属性签名方案的跨数据中心身份认证协议,采用基础门限签名方案保证签名的不可伪造性,提高方案的容错性;采用属性签名方案隐藏用户具体的身份信息,具有较强的隐私保护特性;跨数据中心身份认证证书颁发由部署在区块链上的智能合约自动化执行,智能合约由多方背书和维护,保障了跨数据中心匿名身份认证的可信性;支持数据中心的预授权,提高了认证效率。

(3) 建立了用户身份映射表,用于存储用户真实身份与其属性密钥的映射关系,在出现纠纷时,可由对应认证服务器恢复可疑用户的真实身份,解决了匿名身份难以追踪的问题,实现了用户身份监管。

1 相关知识

1.1 区块链和联盟链

区块链^[16]具有去中心化、数据难以篡改和智能合约自动执行等技术优势,存储在区块链账本上的数据通过节点进行共享,共识机制保证了不同节点之间数据的一致性,有效解决了节点间的信任问题,可用于实现去中心化的跨数据中心用户身份管理,为跨数据中心数据共享流通提供了新的思路。以脚本形式部署到区块链上的智能合约^[17]在满足触发条件时,就会自动执行,可有效提升用户管理的效率。区块链交易可追溯的特性可用于追踪用户链上行为。

区块链按照用户管理权限的不同,可分为公有链、联盟链^[18]和私有链。在联盟链中,网络节点的加入需要经过组织机构的审批,链上节点的各种权限活动需要按照联盟制定的规则有序进

行。与公有链和私有链相比,联盟链具有能耗低、交易速度快等优点,可以更好地满足实际应用需求。本文构建了由各数据中心用户管理节点组成的联盟链,形成了数据中心联盟。

1.2 属性签名

基于属性的签名体制概念由Maji等^[19]首次提出。在ABS方案中,签名者根据自身所拥有的属性向属性机构(attribute agency, AA)申请属性密钥,然后使用其属性密钥根据特定的策略签署消息,生成签名;验证者收到签名后,验证签名的有效性。签名者在生成签名时,签名的身份信息不会与签名产生关联关系;验证者验证签名时,无法获得关于签名者身份的任何其他信息。因此,ABS具有良好的匿名性,常常被用于匿名身份认证应用中。

1.3 门限签名方案

本文将门限签名方案^[20]应用于分布式多属性机构跨数据中心身份认证场景中。门限方案具体内容如下。

(1) Setup

选择一个素数 p 阶循环群 G ,其生成元为 g ,选择一个哈希函数 $H: \{0, 1\}^* \times G^n \rightarrow Z_p^*$ 。

(2) Gen

随机生成秘密值 $s_i \in Z_p$ 作为私钥,并据此计算公钥: $Y_i = g^{s_i}, i = 1, \dots, n$ 。

(3) Sign

若签名者拥有前 t 个私钥,生成对消息 $m \in \{0, 1\}^*$ 的签名。

①对于 $i = 1, \dots, t$,随机选取 $t_i \in Z_p^*$,计算 $R_i = g^{t_i}$ 。

②对于 $i = t + 1, \dots, n$,随机选取 $c_i, d_i \in Z_p^*$,计算 $R_i = g^{d_i} Y_i^{c_i}$ 。

③计算哈希值: $c = H(m, R_1, \dots, R_n)$ 。

④用 $n - t + 1$ 个点 $(0, c), (t + 1, c_{t+1}), \dots, (n, c_n)$ 构造 $n - t$ 次拉格朗日插值多项式 $P_{n-t}(x)$ 。

⑤计算: $c_i = P_{n-t}(i), d_i = t_i - c_i s_i, i = 1, \dots, t$ 。

⑥输出多项式 $P_{n-t}(x)$ 和签名: $\sigma = \{c_i, d_i, R_i\}, i = 1, \dots, n$ 。

(4) Verify

验证 $P_{n-t}(x)$ 是一个 $n - t$ 次的多项式,其中

$P_{n-t}(i) = c_i, i = 1, \dots, n$,且 $R_i = g^{d_i} Y_i^{c_i}$ 。若以上条件全部满足,则签名有效。

注:已知某函数 $f(x)$ 在各互不相同的点 $x_i (i = 1, \dots, t)$ 处的函数值 $f(x_i)$,则可构造 $t - 1$ 次拉格朗日插值多项式:

$$f(x) = \sum_{j=1}^t f(x_j) \prod_{j=1, j \neq i}^t \frac{x - x_j}{x_i - x_j} \quad (1)$$

其中, j 是一个索引,用于遍历数据点的集合, j 从0开始,到 i 结束。

2 匿名可监管跨数据中心身份认证

2.1 系统模型

本文所设计的跨数据中心身份认证系统是由多个数据中心组成的数据中心联盟共同维护,联盟中各个数据中心的认证服务器和属性机构组成联盟链,为系统中的其他用户提供区块链代理服务。每个数据中心有多个认证服务器和属性机构加入联盟链中,以避免因为单个服务器宕机而造成损失。该系统不依赖于任何第三方权威机构,实现了真正意义上的去中心化;无须用户链上再次注册,不会增加用户负担,同时提升了跨数据中心的认证效率;认证过程采用ABS技术保护用户的身份隐私。用户注册时,认证服务器将会为其生成身份映射表,用于实现用户身份的追踪和监管。跨数据中心身份认证系统模型如图1所示。

模型主要由用户 U_A 、用户 U_B 、属性机构、认证服务器(authority server, AS)和区块链服务组成,模型中各部分的具体功能如图1所示。

用户 U_A :用户根据自身基本信息通过数据中心 D_A 的认证服务器向属性机构申请属性进行用户注册,成为数据中心 D_A 中的合法节点。其可以向其他数据中心的普通注册节点发出跨数据中心身份认证请求。

用户 U_B :根据自身基本信息通过数据中心 D_B 的认证服务器向属性机构申请属性进行用户注册,成为数据中心 D_B 中的合法节点。可以接收来自其他数据中心合法节点发出的跨数据中心身份认证请求,通过本地认证服务器为认证请求方申请跨数据中心身份认证证书。

属性机构:属性机构为联盟链中的节点。每个属性机构代表某一属性,具有某一属性的公私

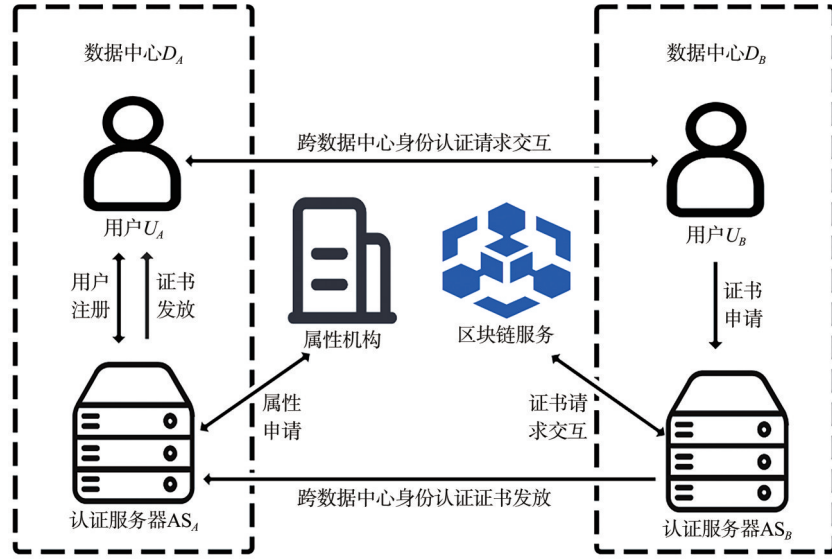


图1 跨数据中心身份认证系统模型
Figure 1 Cross-Datacenter identity authentication system model

钥对，负责为用户生成自身所代表属性的属性公私钥对。

认证服务器：认证服务器为联盟链节点。其负责为用户进行身份注册，维护用户身份映射表，调用智能合约进行跨数据中心身份认证证书的颁发等。

区块链服务：区块链作为整个系统的网络载体，为系统提供共识服务，保证数据的安全可信，链上部署的智能合约由认证服务器调用，自动化地进行跨数据中心身份认证判定。

2.2 安全定义

基于门限结构属性签名的匿名可监管跨数据中心身份认证方案应具备正确性和不可伪造性特性。

(1) 正确性

正确性是只要正确执行方案中算法和协议，就能得到正确的结果。

(2) 不可伪造性

不可伪造性是若用户拥有属性不满足访问结构，则该用户无法伪造有效的签名，其安全属性由敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的安全交互游戏定义。

1) $\mathcal{C}$ 运行 GlobalSetup 和 AASetup 算法初始化系统，生成公共参数 GPK 和各属性机构 AA_i 的公私钥对 (APK, ASK)， $\mathcal{C}$ 向敌手 $\mathcal{A}$ 公布 GPK 和 APK，将 ASK 保持私有。

2) 多项式时间内，任意敌手 $\mathcal{A}$ 可适应性地

进行如下询问。

①用户身份标识询问： $\mathcal{A}$ 提交身份标识询问请求，挑战者 $\mathcal{C}$ 返回身份标识 uid_u 作为响应。

②用户秘密值询问： $\mathcal{A}$ 提交身份标识 uid_u ， $\mathcal{C}$ 返回秘密值 s_u 或错误符号 $\perp$ 。

③用户密钥询问： $\mathcal{A}$ 提交属性—身份元组 (att_i, uid_u) ， $\mathcal{C}$ 返回用户 uid_u 关于属性 att_i 的属性密钥。

④签名询问： $\mathcal{A}$ 提交元组 (uid_u, m, T) ， $\mathcal{C}$ 返回 (uid_u, m, T) 的签名 σ 。

⑤签名验证询问： $\mathcal{A}$ 提交元组 (uid_u, m, T, σ) ， $\mathcal{C}$ 执行签名验证协议，验证结果为有效或无效。

3) 敌手 $\mathcal{A}$ 输出 $(uid_u^*, m^*, T^*, \sigma^*)$ 。

若满足以下条件，则表明敌手赢得该安全交互游戏。

① $(uid_u^*, m^*, T^*, \sigma^*)$ 不能被 $\mathcal{C}$ 否认。

② $\mathcal{A}$ 未对 $(uid_u^*, m^*, T^*, \sigma^*)$ 执行签名询问阶段。

③ $\mathcal{A}$ 执行用户密钥询问阶段中，选取的属性集 att_i^* 不满足访问结构 T^* 。

定义1 若多项式时间内，任意敌手 $\mathcal{A}$ 赢得上述安全交互游戏可凭借的优势 $Adv_{\mathcal{A}}$ 是可忽略的，则表明基于门限结构属性签名的匿名可监管跨数据中心身份认证方案满足选择消息存在不可伪造的安全性。

3 匿名可监管跨数据中心身份认证方案

本节将详细介绍跨数据中心匿名可监管身份认证方案的具体流程, 方案中涉及的符号及其描述见表 1。

表 1 符号及其描述 Table 1 Symbols and their descriptions	
符号	描述
G	循环群
p, g	循环群的阶、生成元
U	属性全集
GPK	系统公共参数
APK_i, ASK_i	属性机构公私钥
baseinfo	用户基本信息
s_u	秘密值
uid_u	用户身份标识
$attr_i$	用户属性
apk_u, ask_u	用户的属性公私钥
$IdMap_u$	用户身份映射
T	访问结构
σ	属性签名
$Cert_{U_A, U_B}$	用户跨数据中心证书

3.1 初始化阶段

(1) GlobalSetup(λ) $\rightarrow$ GPK

生成分布式属性签名的相关参数 GPK =

$\{G, p, g, U, H\}$ 并上链发布。其中, G 为一个循环群, 其阶为素数 p , 其生成元为 g , U 为系统中的属性全集, 对应系统中各数据中心属性机构, H_1 和 H_2 为哈希函数。

(2) AASetup(GPK) $\rightarrow$ ASK_i, APK_i

系统中各属性机构随机生成自己的机构私钥 $ASK_i \in Z_p^*$, 并根据自己的机构私钥计算出机构公钥 $APK_i = g^{ASK_i}$ 。其中, 机构私钥 ASK_i 保密存储, 机构公钥 APK_i 上链发布。

3.2 用户注册阶段

数据中心联盟中各个数据中心的用户都需要在本数据中心进行身份注册, 成为合法用户。用户向本数据中心认证服务器提交注册申请, 认证服务器根据用户的注册信息为用户生成合法身份。用户注册流程如图 2 所示。

(1) UserSetup(λ_u) $\rightarrow$ s_u, uid_u

用户随机选取秘密值 $s_u \in Z_p^*$, 并计算用户在水数据中心联盟系统中的唯一身份标识 $uid_u = g^{s_u}$ 。

(2) User $\rightarrow$ AS: {register(uid_u , baseinfo)}

用户向本数据中心认证服务器 AS 提交身份标识 uid_u 和用户基本注册信息 baseinfo, 申请注册。

(3) AS $\rightarrow$ AA_i : {request($attr_i$)}

认证服务器 AS 根据申请注册用户的基本信息为其向对应属性机构 AA_i 申请属性, 属性机构 AA_i 随机选取 $ask_i \in Z_p^*$ 作为用户对应属性 $attr_i$ 的

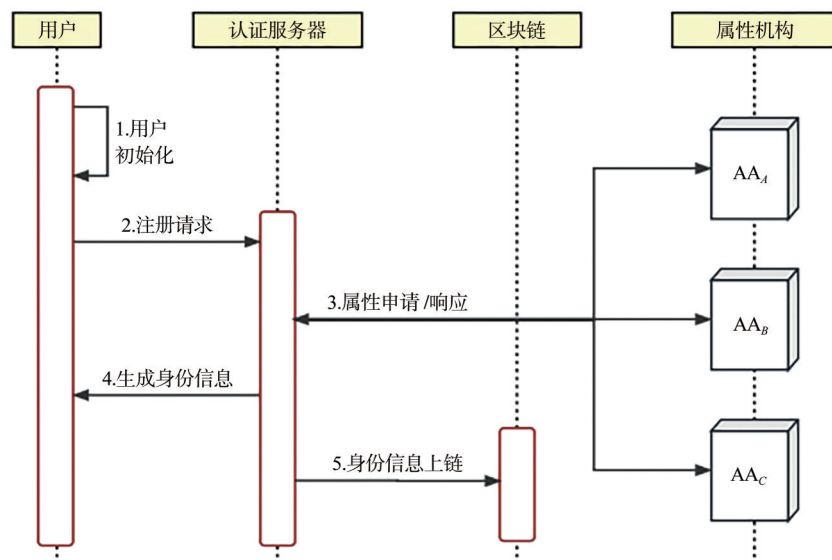


图 2 用户注册流程
Figure 2 User registration process

私钥，并计算 $\text{apk}_i = g^{\text{ask}_i}$ 作为用户对应属性的公钥，将 $\{\text{ask}_i, \text{apk}_i\}$ 通过保密信道返回给认证服务器 AS。

(4) $\text{AS} \rightarrow \text{User}: \{\text{apk}_u, \text{ask}_u\}$

认证服务器 AS 整理各属性机构 AA_i 返回的信息，将属性公钥集 apk_u 和属性私钥集 ask_u 发送给用户，其中 apk_u 上链发布。

(5) $\text{AS} \rightarrow \text{Blockchain}: \{\text{IdMap}_u\}$

认证服务器 AS 为该注册用户建立用户身份标识 uid_u 、属性密钥 $\{\text{apk}_u, \text{ask}_u\}$ 的身份映射，并存储在链上的私有数据库中。

3.3 跨数据中心身份认证阶段

数据中心 D_A 中的用户 U_A 向数据中心 D_B 中的用户 U_B 请求跨数据中心身份认证的流程如图3所示，反之，用户 U_B 向用户 U_A 请求身份认证的过程同样按照该流程执行，实现双向认证。

(1) $U_A \rightarrow U_B: \{\text{AuthRequest}\}$

数据中心 D_A 中的用户 U_A 向数据中心 D_B 中的用户 U_B 发出身份认证请求。

(2) $U_B \rightarrow U_A: \{\text{Nonce}\}$

数据中心 D_B 中的用户 U_B 收到请求后，产生一个随机数 Nonce，将其发送给数据中心 D_A 中的

用户 U_A 。

(3) $U_A \rightarrow U_B: \{\text{ask}_u, \text{Nonce}, T\} \rightarrow \sigma, P_{n-t}(x)$

数据中心 D_A 中的用户 U_A 收到随机数 Nonce 后，与认证服务器 AS 和相关属性机构 AA_i 共同生成签名和多项式，并发送给数据中心 D_B 中的用户 U_B 。假设 U_A 期望申请属性集合为 $U = \{\text{att}_1, \text{att}_2, \dots, \text{att}_n\}$ 的证书，至少需要 t 个正常 AA_i 参与才可完成认证过程。具体过程如下。

① 对于 $i \in [1, t]$ ， AA_i 选取随机数 $t_i \in Z_p^*$ ，计算 $R_i = g^{t_i}$ 。

② 对于 $i \in [t+1, n]$ ， AA_i 选取随机数 c_i ， $d_i \in Z_p^*$ ，计算：

$$e_i = (\text{att}_i, \text{apk}_i, \text{uid}_u, \text{APK}_i) \quad (2)$$

$$Y_i = \text{apk}_i \text{APK}_i \quad (3)$$

$$R_i = g^{d_i} Y_i \quad (4)$$

AA_i 将 $(c_i, d_i, \text{apk}_i, R_i)$ 发送给 AS。

③ AS 将 $R_i (i \in [1, n])$ 发送给 U_A ， U_A 计算：

$$T_i = R_i^{s_u} \quad (5)$$

U_A 将 T_i 发送给认证服务器 AS。

④ AS 计算

$$c = H_2(\text{Nonce}, T_1, \dots, T_n, \text{uid}_u) \quad (6)$$

⑤ 用点 $(0, c), (t+1, c_{t+1}), (n, c_n)$ 构造 $n-t$

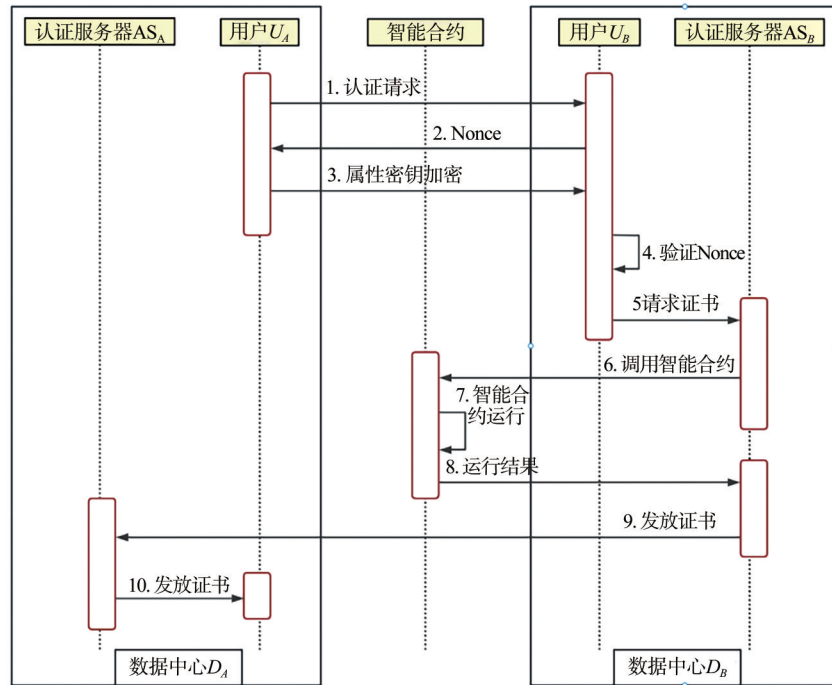


图3 跨数据中心身份认证流程
Figure 3 Cross-datacenter identity authentication process

次拉格朗日插值多项式 $P_{n-t}(x)$ 。

⑥计算 $c_i = P_{n-t}(i), d_i = t_i - c_i$, 其中 $i \in [1, t]$ 。

⑦AS 输出签名 $\sigma = (c_i, d_i, T_i, \text{apk}_i, \text{uid}_u)$ 和多项式 $P_{n-t}(x)$ 。

(4) U_B : $\text{Verify} \{ \sigma \} \rightarrow \text{is Valid}$

数据中心 D_B 中的用户 U_B 收到来自数据中心 D_A 中的用户 U_A 的对随机数 Nonce 的签名 σ 后, 验证签名的有效性。若签名有效, 则进入下一步; 若签名无效, 则返回认证失败信息 Authfaild, 认证结束。具体验证过程如下。

① U_B 验证 $P_{n-t}(x)$ 是否为 $n-t$ 次多项式。

② U_B 验证等式 $P_{n-t}(i) = c_i$ 是否成立。

③ U_B 验证 $P_{n-t}(0) = H_2(m, T_1, \dots, T_n, \text{uid}_s)$ 是否成立。

④ U_B 验证签名。 U_A 向 U_B 验证离散对数等式 $\text{DL}(T_i, R_i) = \text{DL}(\text{uid}_u, g)$ 。

⑤以上条件全部成立的情况下, 该签名有效。

⑥若以上条件有一个不成立, 则签名无效。

(5) $U_B \rightarrow \text{AS}_B: \{ \text{CertRequest} \}$

数据中心 D_B 中的用户 U_B 向数据中心 B 中的认证服务器 AS_B 转发数据中心 D_A 中用户 U_A 的跨数据中心身份认证证书请求。

(6) $\text{AS}_B: \{ \text{SmartContract} \}$

数据中心 D_B 中的认证服务器 AS_B 调用部署在区块链上的智能合约 SmartContract, 进行跨数据中心身份认证证书的颁发判定。

(7) $\text{SmartContract} \rightarrow \text{Cert}_{U_A, U_B} / \text{Result}$ 。

SmartContract 首先判断 U_A 所属的数据中心, 若其所属数据中心为预授权数据中心, 则证书颁发判定直接通过, 由 AS_B 为其生成跨数据中心身份认证证书。否则, 根据各数据中心预先联合制定的证书颁发策略进行自动化判定, 若判定通过, 则由认证服务器 AS_B 生成数据中心 D_A 中用户 U_A 的跨数据中心证书 Cert_{U_A, U_B} , 进入下一步; 若判定未通过, 则返回认证失败信息 Authfaild, 认证结束。

预授权的数据中心指的是两或者多个数据中心之间建立了可信的友好合作关系, 预授权权限由各数据中心自行管理, 可根据影响数据中心的信任度的多种因素 (例如, 相应数据中心下的用户连续通过跨数据中心的身份认证的次数) 进行

动态评估, 并定期更新。

(8) $\text{SmartContract} \rightarrow \text{AS}_B: \{ \text{Cert}_{U_A, U_B} \}$

SmartContract 将生成的数据中心 D_A 中用户 U_A 的跨数据中心身份认证证书 Cert_{U_A, U_B} 返回给数据中心 D_B 中的认证服务器 AS_B , 证书结构见表 2。

表 2 证书结构
Table 2 Certificate structure

名称	描述
Version Number	证书版本号
Serial Number	证书序列号
Issuer Name	发行机构
Validity	证书有效期
ABS Signature	用户属性签名
Certificate Hash	证书哈希

(9) $\text{AS}_B \rightarrow \text{AS}_A: \{ \text{Cert}_{U_A, U_B} \}$

数据中心 D_B 中的认证服务器 AS_B 将证书 Cert_{U_A, U_B} 通过安全信道发送给数据中心 D_A 中的认证服务器 AS_A 。

(10) $\text{AS}_A \rightarrow U_A: \{ \text{Cert}_{U_A, U_B} \}$

数据中心 D_A 中的认证服务器 AS_A 将证书 Cert_{U_A, U_B} 发送给数据中心 D_A 中的用户 U_A 。用户 U_A 可在证书的有效期内对数据中心 D_B 中的用户 U_B 进行访问。

3.4 身份追踪阶段

$\text{Trace}(\text{IdMap}) \rightarrow \text{uid}_u$

身份追踪算法由每个数据中心的认证服务器运行。在出现纠纷时, 由仲裁请求方发出仲裁请求, 相关数据中心的认证服务器调用身份监管合约, 查询存储在区块链网络私有数据库中的 IdMap, 恢复用户的真实身份 uid, 从而实现用户身份的追踪和监管。

3.5 用户注销阶段

$\text{Revoke}(\text{uid}_u, \text{Cert}_u) \rightarrow \text{True/False}$

用户 U 向本数据中心认证服务器提交身份注销请求, 认证服务器将用户身份标识 uid_u 和与该用户申请的证书 Cert_u 全部删除。

4 方案分析

4.1 安全性分析

(1) 正确性

$$\begin{aligned}
R_i &= g^{d_i} Y_i^{c_i} = g^{t_i - c_i s_i} (r_i y_i^{e_i})^{c_i} \\
&= g^{t_i} g^{-c_i (k_i + e_i \text{ASK}_i)} (g^{k_i} g^{e_i \text{ASK}_i})^{c_i} \\
&= g^{t_i}
\end{aligned} \quad (7)$$

(2) 不可伪造性

定理1 若离散对数问题是困难的, 则基于门限结构属性签名的匿名可监管跨数据中心身份认证方案满足存在不可伪造安全性。

证明: 若第1.3节中基础门限签名方案是不可伪造安全的, 则本方案也是不可伪造安全的, 具体证明过程如下。

若存在一个敌手 $\mathcal{A}$ 能够以 $\text{Adv}_{\mathcal{A}}$ 的优势伪造匿名可监管跨数据中心身份认证方案的签名, 则存在敌手 $\mathcal{B}$ 能以 $\text{Adv}_{\mathcal{B}} = \text{Adv}_{\mathcal{A}}/q$ 的优势伪造基础门限签名方案的签名, 其中 q 为系统身份标识全集, 定义 $\mathcal{C}$ 为基础门限签名方案的挑战者。

1) $\mathcal{C}$ 初始化系统, 生成公共参数GPK和属性机构 AA_i 的公私钥对 $(\text{ASK}_i, \text{APK}_i = g^{\text{ASK}_i})$, $\mathcal{C}$ 将公共参数 (G, p, g) 和公钥 APK_i 发送给敌手 $\mathcal{B}$ 。

2) 假设 $\mathcal{A}$ 最多请求 q 个全局标识, $\mathcal{B}$ 随机选取 $j \in [1, q]$ 。

3) $\mathcal{B}$ 为 $\mathcal{A}$ 提供如下预言机服务。

①当 $\mathcal{A}$ 进行第 i 次全局标识询问时, $\mathcal{B}$ 随机选取 $s_i \in Z_p^*$, 计算 $\text{uid}_i = g^{s_i}$, 将 (s_i, uid_i) 存入列表 uid^{list} 。

②当 $\mathcal{A}$ 对 uid_u 进行秘密值询问时, 如果 uid_u 在 uid^{list} 中, $\mathcal{B}$ 返回 s_u ; 否则, 返回 $\perp$ 。

③当 $\mathcal{A}$ 对 $(\text{apk}_i, \text{ASK}_i, \text{uid}_u, \text{att}_i)$ 进行 H_1 询问时, $\mathcal{B}$ 随机选取 $e_i \in Z_p^*$ 发送给 $\mathcal{A}$, 并将 $(e_i, \text{ASK}_i, \text{uid}_u, \text{att}_i)$ 存入列表 H_1^{list} 。

④当 $\mathcal{A}$ 对 $(\text{Nonce}, T_1, \dots, T_n, \text{uid}_u)$ 进行 H_2 询问时, 如果 $\text{uid}_u \neq \text{uid}_j$, 则随机生成 c_i 发送给 $\mathcal{A}$; 如果 $\text{uid}_u = \text{uid}_j$, 则 $(\text{Nonce}, T_1^{s_u^{-1}}, \dots, T_n^{s_u^{-1}})$ 向 $\mathcal{C}$ 进行 H_2 询问, 并将返回的 c_i 发送给 $\mathcal{A}$ 。

⑤当 $\mathcal{A}$ 对 uid_u 询问属性 attr_i 的密钥, $\mathcal{B}$ 运行 $\text{request}(\text{attr}_i)$ 算法生成属性的公私钥对 $(\text{ask}_i, \text{apk}_i)$ 作为响应。

⑥当 $\mathcal{A}$ 对 $(\text{uid}_u, \text{Nonce}_i)$ 请求签名询问时, 若 $\text{uid}_u \neq \text{uid}_j$, 则 $\mathcal{B}$ 生成签名发送给 $\mathcal{A}$; 若 $\text{uid}_u = \text{uid}_j$, 则 $\mathcal{B}$ 向 $\mathcal{C}$ 请求签名 $\sigma = (c_i, d_i, R_i) (i = 1, \dots, n)$ 和多项式 $P_{n-i}(x)$ 作为签名发送给 $\mathcal{A}$, 其中 $T_i = R_i^{s_u}$ 。

⑦对 $(c_i, d_i, T_i, \text{apk}_i, \text{uid}_u) (i = 1, 2, \dots, n)$ 和多项式 $P_{n-i}(x)$ 进行签名验证询问时, $\mathcal{A}$ 使用 s_u 与 $\mathcal{B}$ 进行签名验证交互。

4) $\sigma = (c_i, d_i, T_i, \text{apk}_i, \text{uid}_u) (i = 1, 2, \dots, n)$ 和多项式 $P_{n-i}(x)$ 可由 $\mathcal{A}$ 输出。若 $\text{uid}_u \neq \text{uid}_j$, $\mathcal{B}$ 输出签名 $\sigma = (c'_i, d'_i, T_i^{s_u^{-1}}) (i = 1, 2, \dots, n)$ 和多项式 $P'_{n-i}(x)$ 。

上述所有预言机服务都是完善的。若敌手 $\mathcal{B}$ 对目标标识 uid_u 的概率为 $1/q$, 则敌手 $\mathcal{A}$ 能够以不可忽略的优势 $\text{Adv}_{\mathcal{A}}$ 成功地伪造签名 $\sigma = (c'_i, d'_i, T_i^{s_u^{-1}}, \text{apk}'_i, \text{ask}'_i) (i = 1, 2, \dots, n)$ 和多项式 $P'_{n-i}(x)$, 且敌手 $\mathcal{B}$ 能根据敌手 $\mathcal{A}$ 的输出以不可忽略的优势 $\text{Adv}_{\mathcal{B}} = \text{Adv}_{\mathcal{A}}/q$ 成功伪造基础门限签名 $\sigma = (c'_i, d'_i, T_i^{s_u^{-1}}) (i = 1, 2, \dots, n)$ 和多项式 $P'_{n-i}(x)$ 。

(3) 抵御重放攻击

在本文所设计的跨数据中心身份认证交互协议中, 认证接收者向认证请求者发送随机数来确保认证信息的实时性。认证请求者向认证接收者发出跨数据中心身份认证请求, 认证接收者向认证请求者发送随机数, 认证请求者对该随机数进行签名, 认证接收者验证随机数的正确性, 可抵御恶意攻击者进行重放攻击。

(4) 抵御拒绝服务攻击

在本文所提出的跨数据中心身份认证模型中, 每个数据中心的多台认证服务器加入区块链网络。只有当所有区块链节点不可用时, 系统的身份认证服务才会崩溃; 当单个区块链网络节点受到攻击时, 认证请求者可以向其他认证服务器节点发送证书颁发申请, 系统的跨数据中心身份认证服务仍然可用。因此, 该模型能够有效地保护身份认证系统免受拒绝服务攻击。

(5) 抵御篡改攻击

区块链网络中的所有节点通过共识算法保存相同的数据, 并不断向区块链添加新的区块, 如果一个区块中的数据被篡改, 则需要修改该区块后续所有区块头部的哈希值。单个节点修改自己的账本并不会影响其他节点中的账本。若对手想要篡改区块链上的数据, 那么根据区块链的背书机制, 应该有超过51%的节点篡改背书。从理论上讲, 这是不可能实现的。

(6) 隐私安全性

用户进行身份注册时,为用户生成单个属性密钥的属性机构都仅知道自己为用户生成的属性密钥,并不知道其他属性机构为用户生成的属性密钥。除了用户所在的本地的认证服务器外,不存在掌握用户全部属性密钥的权威机构。用户使用属性私钥生成签名,验证者并不能根据签名得知生成该签名的用户的具体属性信息。故本方案保障了用户身份隐私安全性,可以极大程度地保护用户在跨数据中心身份认证过程中的隐私信息。

(7) 身份可监管性

在本方案中,用户注册时,认证服务器会为该用户建立用户真实身份和其属性密钥的身份映射。当发生恶意事件或者纠纷时,可由对应数据中心的认证服务器通过身份监管合约查询存储在区块链私有数据库中的身份映射表,恢复可疑用户的真实身份,实现对用户身份信息和行为的监管。

(8) 抵御中间人攻击

本文所构造的分布式属性签名方案基于基础门限签名方案,其困难性基于离散对数问题,如果离散对数问题是困难的,则本文所构造的分布式属性签名方案是不可否认的,基于不可否认性,本文所构造的分布式属性签名方案可以抵御中间人攻击。

4.2 方案对比分析

将本文方案和现有方案分别从是否基于区块链、是否基于属性签名、是否基于门限签名、是否支持身份监管、是否支持单次注册、是否支持跨数据中心这6个方面进行对比,结果如表3所示。

表3 本文方案与现有方案的功能对比
Table 3 Comparison of functionality between the proposed scheme in this paper and existing schemes

方案	基于区块链	基于属性签名	基于门限签名	身份监管	单次注册	跨数据中心
方案[5]	√	×	×	×	√	√
方案[7]	√	×	×	×	√	√
方案[8]	√	×	×	√	×	√
方案[15]	√	√	√	×	—	×
本文方案	√	√	√	√	√	√

对比表3可以看出,该方案具有去中心化、细粒度身份管理、安全性高、匿名性强、身份可监管、用户认证方便和支持跨数据中心身份认证

等方面的优势。

4.3 实验仿真

仿真实验在 HyperLedger Fabric 中进行,具体的实验配置见表4。针对不同 (t,n) 条件下的方案性能,仿真实验在不同时间段内分别进行5次,测试的每个步骤默认进行1000次,取其平均值。不同 (t,n) 条件下的方案性能如图4所示。

表4 实验配置
Table 4 Experimental configuration

环境	配置
OS	Ubuntu 18.04
CPU	AMD R7 4800H@2.90 GHz
RAM	4 GB 3200 MHz DDR4
HyperLedger Fabric	v2.4
Docker	v20.10.7
Couch DB	v3.1

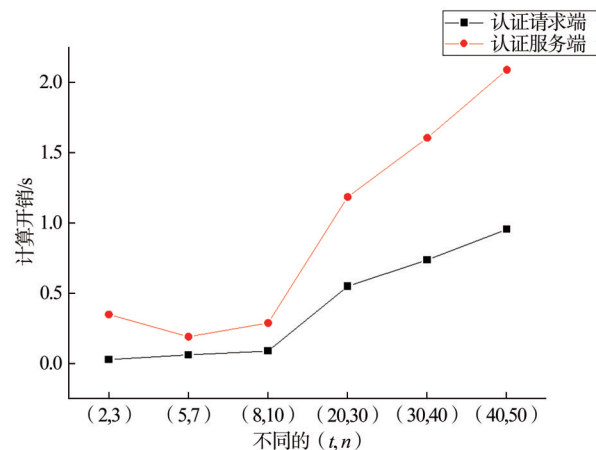


图4 不同 (t,n) 下的方案性能
Figure 4 Performance of the scheme under different (t,n) combinations

随着 (t,n) 的不断增加,认证请求端和认证服务端在身份认证过程中所消耗的时间随之呈现出增加趋势,但仍在实际应用允许范围之内。由此可以得出,该方案支持多属性跨数据中心身份认证场景,具有良好的可扩展性。需要注意的是,根据实际测试结果,方案性能在 $(5,7)$ 和 $(8,10)$ 处出现了抖动,但是整体上可以满足实际需求。

在智能合约进行用户跨数据中心身份认证证书的判定过程中,本文引入了动态预授权机制,预授权信息可在一定时间内保持有效性,从而避免用户证书颁发的重复判定,提高身份认证效率。

智能合约进行证书颁发的判定时间如图5所示。

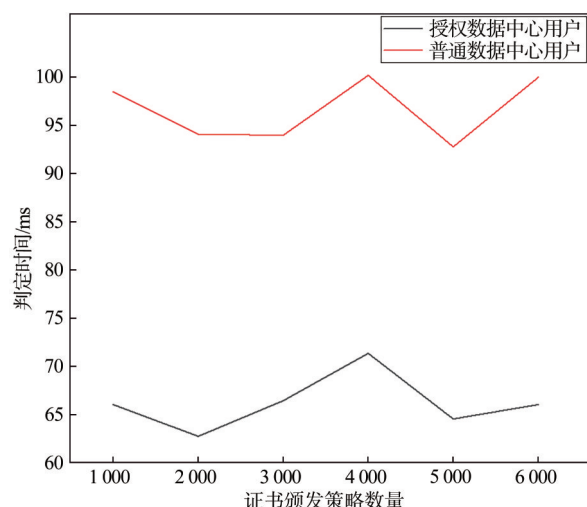


图5 智能合约进行证书颁发的判断时间

Figure 5 Certificate issuance judgment time of smart contract

授权数据中心用户进行证书颁发判定的效率要明显高于普通数据中心用户，且随着证书颁发策略的不断增多，2种不同类型的数据中心的证书颁发判定效率并没有发生显著的降低。由此可知，本方案支持多策略的证书颁发，具有较好的扩展性。

5 结束语

在金融数据安全领域，身份认证是其中的关键一环。本文提出了一种基于区块链的跨数据中心匿名可监管身份认证方案，该方案能有效地解决金融数据安全领域身份认证面临的诸多问题。基于区块链技术，去除可信第三方权威机构，为用户提供分布式的跨数据中心身份认证服务，增强了系统的安全性；在已有的结合门限机制的属性签名方案的基础上，构造分布式属性签名方案，应用于跨数据中心身份认证场景下，实现细粒度匿名身份认证，保护用户身份隐私；建立了用户身份映射表，在切实有效地实现用户隐私保护的同时，解决了匿名身份追踪难题，实现了用户身份监管。分析表明，该方案具有良好的安全性和较高的性能，实际应用价值较高。

参考文献：

[1] 李连朋, 罗宏. 国内外金融业信息安全综述[J]. 网络与信息安全学报, 2017, 3(2): 13-23.

LI L P, LUO H. Review of domestic and international financial security[J]. Chinese Journal of Network and Information Security, 2017, 3(2): 13-23.

[2] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.

PENG H X. An identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281.

[3] CHEN R B, SHU F X, HUANG S K, et al. BidM: a blockchain-enabled cross-domain identity management system[J]. Journal of Communications and Information Networks, 2021, 6(1): 44-58.

[4] LEE Y K, JEONG J. Securing biometric authentication system using blockchain[J]. ICT Express, 2021, 7(3): 322-326.

[5] ZHANG H X, CHEN X S, LAN X, et al. BTCAS: a blockchain-based thoroughly cross-domain authentication scheme[J]. Journal of Information Security and Applications, 2020, 55: 102538.

[6] WANG M M, RUI L L, YANG Y, et al. A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2664-2676.

[7] CHEN J, ZHAN Z Y, HE K, et al. XAuth: efficient privacy-preserving cross-domain authentication[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3301-3311.

[8] 牛建林, 任志宇, 杜学绘. 基于联盟链的跨域认证方案[J]. 网络与信息安全学报, 2022, 8(3): 123-133.

NIU J L, REN Z Y, DU X H. Cross-domain authentication scheme based on consortium blockchain[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 123-133.

[9] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[R]. Cryptology ePrint Archive, 2008.

[10] CAO D, ZHAO B K, WANG X F, et al. Multi-authority attribute-based signature[C]//Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems. Piscataway: IEEE Press, 2011: 668-672.

[11] SUN J M, QIN J, MA J X. Securely outsourcing decentralized multi-authority attribute based signature[M]. Cyberspace Safety and Security. Cham: Springer International Publishing, 2017: 86-102.

[12] LIU X J, CHEN W, XIA Y J, et al. TRAMS: a secure vehicular crowdsensing scheme based on multi-authority attribute-based signature[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(8): 12790-12800.

[13] 唐飞, 包佳立, 黄永洪, 等. 基于属性的多授权中心身份认证方案[J]. 通信学报, 2021, 42(3): 220-228.

TANG F, BAO J L, HUANG Y H, et al. Multi-authority attribute-based identification scheme[J]. Journal on Communications, 2021, 42(3): 220-228.

[14] LU A R, LI W H, YAO Y Z, et al. TCABRS: an efficient traceable constant-size attribute-based ring signature scheme for electronic health record system[C]//Proceedings of the 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2021: 106-113.

- [15] Yuan Distributed public key infrastructure scheme based on blockchain and decentralized undeniable attribute-based signature[J]. *Scientia Sinica Informationis*, 2022, 52(6): 1135.
- [16] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. *Future Generation Computer Systems*, 2020, 107: 841-853.
- [17] 刘峰, 杨杰, 齐佳音. 区块链密码学隐私保护技术综述[J]. *网络与信息安全学报*, 2022, 8(4): 29-44.
- LIU F, YANG J, QI J Y. Survey on blockchain privacy protection techniques in cryptography[J]. *Chinese Journal of Network and Information Security*, 2022, 8(4): 29-44.
- [18] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//*Proceedings of the Thirteenth EuroSys Conference*. New York: ACM, 2018: 1-15.
- [19] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[M]. *Topics in Cryptology - CT-RSA 2011*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 376-392.
- [20] 魏亮, 黄振杰, 陈群山. 去中心基于属性不可否认签名[J]. *计算机工程与科学*, 2020, 42(6): 1003-1011.
- WEI L, HUANG Z J, CHEN Q S. Decentralized attribute-based undeniable signature[J]. *Computer Engineering & Science*, 2020, 42(6): 1003-1011.

[作者简介]



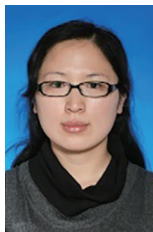
徐淑奖 (1979-), 男, 山东临沂人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为数据安全、区块链。



张朝阳 (1997-), 男, 山东菏泽人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 硕士生, 主要研究方向为数据安全、区块链。



王连海 (1969-), 男, 山东潍坊人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为数据安全、区块链、计算机取证。



张淑慧 (1981-), 女, 山东济宁人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为数据安全、区块链、计算机取证。



邵蔚 (1994-), 女, 山东济南人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为区块链、隐私保护。