面向去中心化身份的隐私保护多方授权方案

牟翰翔，万长胜
（东南大学　网络空间安全学院，江苏　南京　211189）

摘　要：针对现有去中心化身份方案在多方授权中难以兼顾隐私保护与协议兼容性的问题，提出一种支持匿名认证的去中心化多方授权方案。该方案基于双线性配对构造，采用紧凑多重签名实现高效授权，利用零知识集合成员证明实现用户向授权机构的匿名身份验证。为解决协议兼容性问题，设计了交互式可验证表达结构，将零知识证明参数封装于 W3C 标准凭证中。安全性证明表明该方案在随机预言机模型下满足不可伪造性与匿名性。理论与实验分析表明，方案生成的最终凭证大小恒定，系统开销具备良好的可扩展性。

关键词：去中心化身份；多方授权；匿名认证；多重签名；零知识证明
中图分类号：TP309.7　　**文献标志码**：A　　**DOI**：10.19358/j.issn.2097-1788.2026.03.001

中文引用格式：牟翰翔，万长胜. 面向去中心化身份的隐私保护多方授权方案［J］. 网络安全与数据治理，2026，45(3)：1-9.
英文引用格式：Mu Hanxiang，Wan Changsheng. Privacy-preserving multi-party authorization scheme for decentralized identity［J］. Cyber Security and Data Governance，2026，45(3)：1-9.

Privacy-preserving multi-party authorization scheme for decentralized identity

Mu Hanxiang，Wan Changsheng
（School of Cyber Science and Engineering，Southeast University，Nanjing 211189，China）

Abstract：To address the challenge that existing decentralized identity schemes struggle to balance privacy protection and protocol compatibility in multi-party authorization，a Decentralized Multi-party Authorization Scheme with Anonymous Authentication（DMSAA）is proposed. Constructed based on bilinear pairings，the scheme employs compact multi-signatures to achieve efficient authorization and utilizes zero-knowledge set membership proofs to realize anonymous identity verification from users to authorities. To resolve protocol compatibility issues，an "Interactive Verifiable Presentation" structure is designed to encapsulate zero-knowledge proof parameters within W3C standard credentials. Security analysis demonstrates that the scheme satisfies unforgeability and anonymity under the random oracle model. Theoretical and experimental analyses indicate that the size of the final authorization credential generated by the scheme is constant，and the system overhead exhibits good scalability.

Key words：decentralized identity；multi-party authorization；anonymous authentication；multi-signature；zero-knowledge proof

0　引言

随着 Web 3.0 的发展，去中心化身份（Decentralized Identity，DID）已成为构建用户主权数字生态的基石。W3C 发布的 DID 核心规范[1]和可验证凭证（Verifiable Credentials，VC）数据模型[2]为这一生态提供了标准化技术支撑。在 DID 架构中，用户遵循自主主权身份原则[3]，通过去中心化标识符自主管理身份，摆脱了对中心化身份提供商的依赖。然而，随着应用场景向金融资产管理、医疗数据共享等高价值领域延伸，单一的身份认证已难以满足需求，多方授权机制变得至关重要。例如，Tan 等人[4]指出，访问敏感病历往往需同时获得患者、医生及医院的共同授权；在去中心化金融中，多重签名被广泛用于防止单点私钥泄露导致的资产损失[5]。Squicciarini 等人[6]与 Kinkelin 等人[7]的研究也表明，细粒度的多方访问控制是保障分布式协作环境安全性的关键机制。

尽管基于角色的访问控制（Role-Based Access Control，RBAC）模型[8]已被广泛研究，但在去中心化环境下实现多方授权仍面临严峻的隐私挑战。区块链的透明性及共识机制的公开特性[9]使得交易数据对全网可见，引发了广泛的隐私担忧[10]。传统的比特币多签合约要求公开所有参与者的公钥，直接暴露了授权

方的社交关系与行为模式。此外，现有的 DID 认证体系如 DIDAuth 缺乏对匿名成员资格证明的原生支持，难以满足 Sun 等人[11]提出的在复杂交互中保护用户身份元数据的需求。

针对上述挑战，现有研究提出了一些解决方案，但仍存在局限性。在隐私凭证方面，BBS + 签名[12]和 Camenisch-Lysyanskaya（CL）签名[13]虽然支持属性的选择性披露，但这类非交互式零知识证明(NIZK)在处理动态集合成员证明时效率较低，且生成的证明尺寸通常较大。基于默克尔树的方案[14]虽然通用，但其证明尺寸随集合大小呈对数增长，不适合高频交互场景。在多方授权方面，基于 Schnorr 的 MuSig 方案[15]虽然支持高效密钥聚合，但要求签名者在线且必须披露公钥；基于 BLS 的方案[16]虽支持非交互聚合，但容易受到流氓密钥攻击[17]，且同样缺乏对签名者身份的匿名保护。一些方案尝试利用属性基加密[18]或环签名[19]来保护隐私，但往往难以在审计性[20]与计算效率之间取得平衡。

为了解决上述隐私保护与协议效率之间的矛盾，本文提出了一种具有匿名认证能力的去中心化多方授权方案（Decentralized Multi-party Authorization Scheme with Anonymous Authentication，DMSAA）。本文的主要贡献总结如下：

（1）构建了融合交互式匿名认证与多方授权的通用安全模型。形式化定义了涵盖用户、注册机构、授权机构和服务提供者四方实体的系统架构及交互流程，并给出了匿名性和不可伪造性的严格安全博弈定义，为该领域的后续研究提供了理论框架。

（2）设计了基于双线性配对的 DMSAA 方案。创新性地将紧凑多重签名方案与基于签名的零知识集合成员证明协议有机融合并进行方案构造。同时，针对 W3C 标准非交互式验证流程的兼容性问题，设计了交互式可验证表达（Interactive Verifiable Presentation，i-VP）结构，将零知识证明参数封装其中，实现了隐私协议与 DID 生态的无缝集成。

（3）实现了常数级通信开销与严谨的安全性证明。在随机预言机模型下，通过混合论证法将方案的安全性严格归约到计算困难问题上。理论与实验分析表明，本方案生成的最终授权凭证大小为常数级，显著降低了链上存储成本和验证开销，适用于存储受限的分布式环境。

1 预备知识

1.1 双线性对与困难问题假设

设 $G(1^\lambda)\rightarrow(p, \mathbb{G}, \mathbb{G}_T, e)$ 为群生成算法，其中 $\mathbb{G}$，$\mathbb{G}_T$是阶为大素数 p 的乘法循环群，e：$\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$ 是满足非退化性与双线性性的映射[21]。本方案的安全性基于随机预言机模型(ROM)下的两个困难问题假设：(1) co-CDH 假设[17]，即给定$(g, g^a, g^b)\in\mathbb{G}^3$，计算 g^{ab}在多项式时间内是不可行的；（2）q-SDH 假设[22]，即给定$(q+1)$元组$(g, g^x, g^{x^2}, \cdots, g^{x^q})$，寻找$(c, g^{1/(x+c)})$（其中 $c\in\mathbb{Z}_p^*$）在计算上是困难的。

1.2 密码学原语

本方案主要集成了两种基础构造：（1）紧凑多重签名：采用 Boneh 等人[17]提出的基于 BLS 的签名方案，支持公钥聚合与常数级签名生成，以降低分布式存储开销；（2）零知识集合成员证明：采用 Camenisch 等人[23]的交互式协议，允许证明者在不泄露签名值的前提下证明签名的有效性及成员资格。

2 系统模型与形式化定义

2.1 系统模型

本文构建的去中心化多方授权系统模型如图 1 所示。该模型主要包含四类实体：

（1）用户 U：系统中的资源请求者。用户持有由注册机构颁发的成员凭证，需向多个授权机构证明其合法身份并获取授权签名，最终合成访问令牌。

（2）注册机构 RA：负责用户的初始资格审核，并为合法用户生成唯一的成员私钥和匿名凭证。

（3）授权机构 AA：负责对用户的访问请求进行授权决策的实体集合，记为 $AA=\{AA_1, AA_2, \cdots, AA_n\}$。每

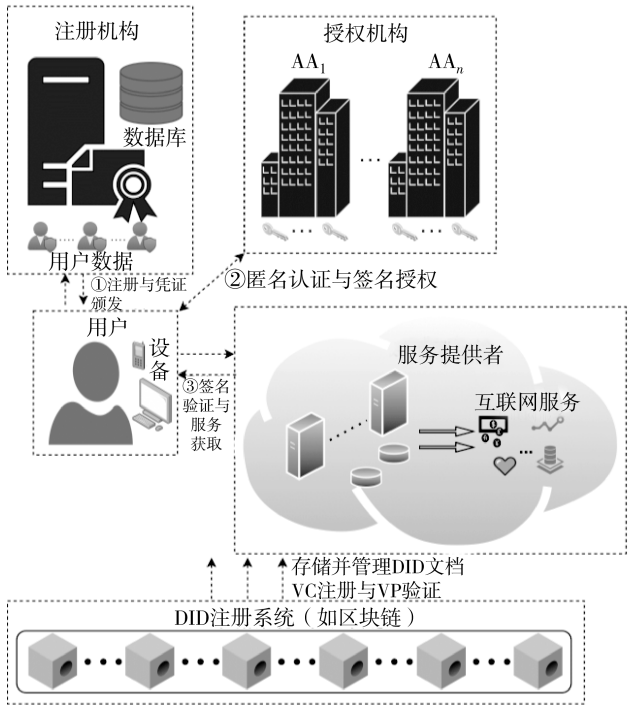

图 1　去中心化多方授权系统模型图

个 AA_j 独立维护自己的私钥，仅在用户通过匿名认证后才对其请求进行部分签名。

（4）服务提供者 SP：资源控制方。负责验证用户提交的多重签名，若验证通过则授予资源访问权限。

2.2 设计目标

为了在多方协作环境中兼顾安全授权与隐私保护，本方案需满足以下设计目标：

（1）多方授权：方案必须从机制上确保，只有在获得预设数量的、多个独立的授权机构共同批准后，用户的服务访问请求才能被最终授权。任何单一授权机构或数量少于阈值的机构组合都无法单方面授予权限。

（2）不可伪造性：任何未经合法授权的实体——无论是外部攻击者、未注册用户，都无法在计算上伪造出一个能通过服务提供者最终验证的有效多重签名。

（3）匿名性：即在用户与任一授权机构进行身份验证的交互过程中，用户的具体身份标识必须对授权机构保密。

（4）去中心化：整个模型的设计必须集成于 W3C 标准的去中心化身份模型之中。方案所使用的密钥、凭证和交互流程都应能通过对现有数据结构的合理扩展来表达。

2.3 形式化定义

方案的形式化交互流程与算法映射如图 2 所示。

该方案包含六个多项式时间算法，具体构造将在第 3 节详细阐述：

Π = (Setup, KeyGen, Issue, Auth, Aggregate, Verify)

3 方案构造

本节详细阐述 DMSAA 方案的具体构造。方案包含系统初始化、密钥生成、DID 数据模型扩展、凭证颁发、交互式匿名认证与授权、签名聚合与验证六个核心部分。

3.1 系统初始化

$\{PP\} \leftarrow Setup(1^{\lambda})$。系统利用该算法生成公共参数。第一，输入安全参数 λ，系统生成双线性配对参

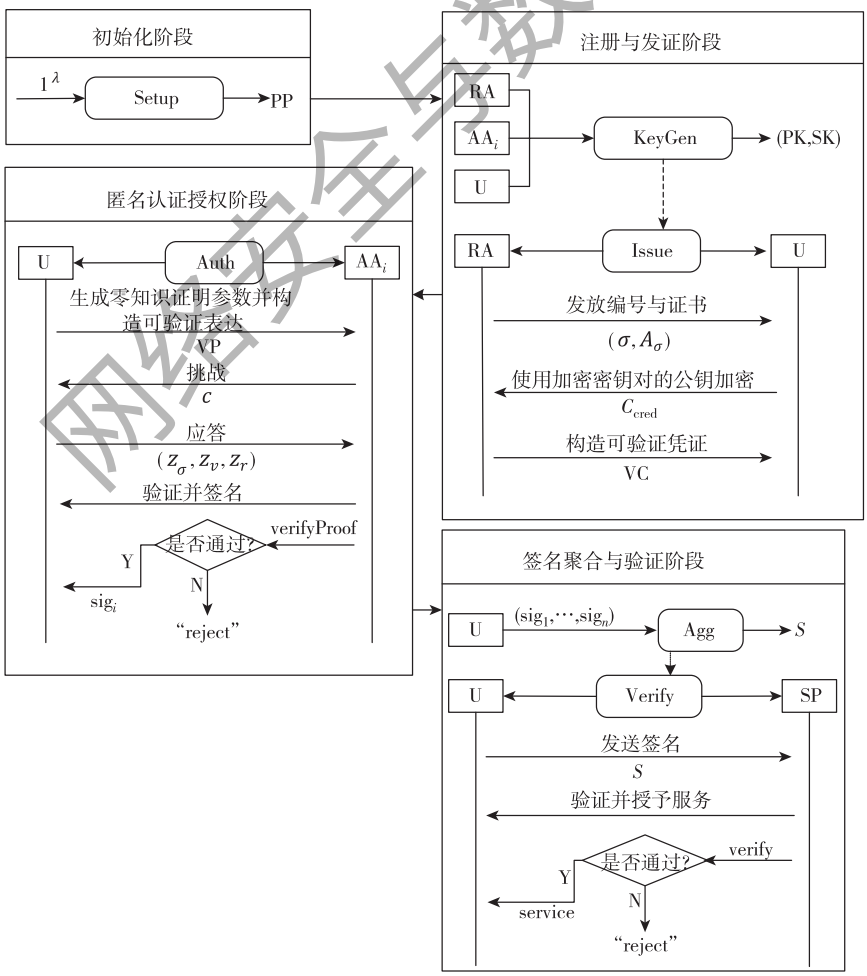

图 2 方案形式化流程与算法映射

数（p，$\mathbb{G}$，$\mathbb{G}_T$，e，g），其中 e：$\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$是一个高效的非退化双线性映射。第二，系统选择另一个随机生成元 $h\in\mathbb{G}$，并定义两个抗碰撞哈希函数：H_0：$\{0,1\}^*\to\mathbb{G}$用于将比特串映射到群元素；H_1：$\{0,1\}^*\to\mathbb{Z}_p$用于将比特串映射到标量值。第三，系统公开参数 PP =（e，p，$\mathbb{G}$，$\mathbb{G}_T$，g，h，H_0，H_1）以供后续阶段使用。

3.2 密钥生成

$\{PK_{RA}, SK_{RA}, \{PK_{AA_i}, SK_{AA_i}\}_{i=1}^{n}, (pk_{User}, sk_{User})\}\leftarrow$ KeyGen（PP）。该算法由注册机构、授权机构和用户分别执行以生成各自的密钥对。第一，注册机构随机选择 $x\in_R\mathbb{Z}_p$作为私钥 SK_{RA}，并计算公钥 $PK_{RA}=y=g^x$。第二，每个授权机构 AA_i（其中 $1\leqslant i\leqslant n$）随机选择标量 $sk_i\in_R\mathbb{Z}_p$作为私钥 SK_{AA_i}，并计算公钥 $PK_{AA_i}=pk_i=g^{sk_i}$。第三，用户生成用于签名的密钥对（sk_{sig}，pk_{sig}）和用于加密的密钥对（sk_{enc}，pk_{enc}）。所有实体的公钥均发布在其 DID 文档中。

3.3 DID 数据模型拓展

为了将交互式零知识证明与 W3C DID 标准融合，本方案定义了 i-VP 数据结构，如图 3 所示。为了突出展示本方案的核心扩展，图 3 省略了 W3C 标准规定的部分通用元数据字段（如完整的 proof 签名信息等）。

标准的 VP 验证通常是非交互式的单向流程，而本方案设计的 i-VP 是对标准 VP 验证流程的扩展。本方案复用了 W3C 标准 VP 的数据模型来封装挑战 – 应答协议中的参数，从而在不破坏底层数据结构兼容性的前提下，支持了复杂的动态零知识验证逻辑。

3.4 凭证颁发

$\{VC_{User}\}\leftarrow$Issue（PP，SK_{RA}，ID_{User}）。注册机构执行该算法向用户颁发加密的可验证凭证。第一，在验证用户合法性后，RA 从$\mathbb{Z}_p$中随机选择一个唯一编号 σ，并计算核心凭证 $A_\sigma=g^{1/(x+\sigma)}$。第二，为了保证凭证传输与存储的机密性，RA 使用用户的加密公钥 pk_{enc} 对二元组（σ，A_σ）进行加密，生成密文 $C_{cred}=Enc_{pkenc}(\sigma, A_\sigma)$。第三，RA 将 C_{cred}封装在 VC 中，对其签名后发送给用户。

3.5 交互式匿名认证与授权

$\{s_i\}\leftarrow$Auth（User（PP，VP_{User}），AA_i（PP，SK_{AA_i}））。用户与授权机构 AA_i执行此交互式协议，在保护隐私的前提下获取部分授权签名。具体步骤如下：

（0）Request：在协议开始前，用户向服务提供者发起服务访问请求。SP 将代表所请求资源 m 的哈希值 $H_0(m)$ 发送给用户。

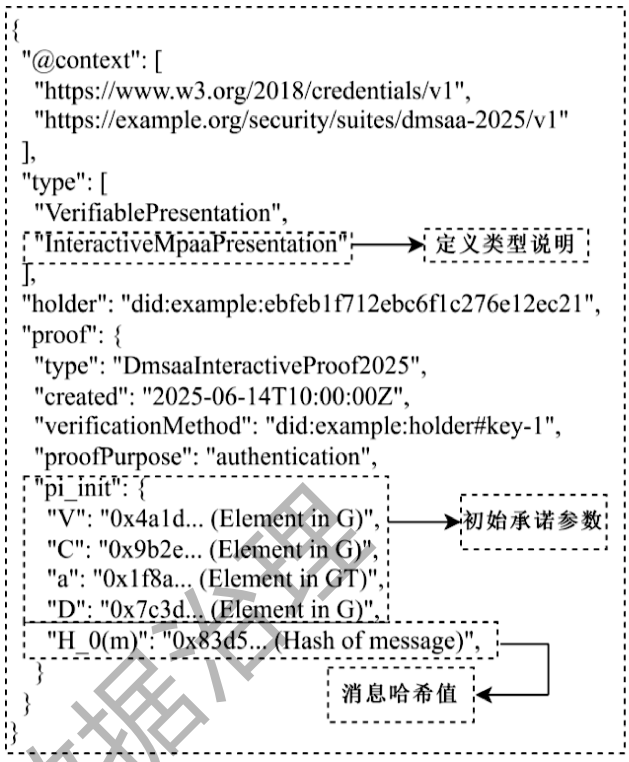

图 3　交互式可验证表达数据结构示例

（1）Commit：用户解密 VC 获取（σ，A_σ）。随机选择致盲因子 v，$r\in_R\mathbb{Z}_p$和辅助随机数 s，t，$k\in_R\mathbb{Z}_p$，计算致盲凭证 $V=A_\sigma^v$，承诺 $C=g^\sigma h^r$ 以及零知识参数 $a=e(V,g)^{-s}e(g,g)^t$，$D=g^s h^k$。用户将（V，C，a，D，$H_0(m)$）封装在 i-VP 中，将（VP_{User}，$H_0(m)$）作为请求参数发送给 AA_i。

（2）Challenge：AA_i收到请求后，验证 i-VP 的数字签名有效性以及其中 $H_0(m)$与参数值的一致性。若成立，随机选择挑战值 $c\in_R\mathbb{Z}_p$ 发送给用户。

（3）Response：用户计算 $z_\sigma=s-\sigma c$，$z_v=t-vc$，$z_r=k-rc\pmod p$，发送给 AA_i。

（4）Sign：AA_i 验证如下等式。

$$\begin{cases} D\overset{?}{=}C^c h^{z_r} g^{z_\sigma} \\ a\overset{?}{=}e(V,y)^c e(V,g)^{-z_\sigma} e(g,g)^{z_v} \end{cases} \tag{1}$$

若通过，计算聚合系数 $a_i=H_1(pk_i,\{pk_1,\cdots,pk_n\})$，并生成部分签名 $s_i=H_0(m)^{a_i\cdot sk_i}$返回给用户。

3.6 签名聚合与验证

$\{0,1\}\leftarrow$Verify（S，m，$\{PK_{AA_i}\}_{i=1}^{n}$）。该算法用于聚合部分签名并验证最终的多方授权结果。

（1）签名聚合：用户收集 n 个授权机构的部分签名 $\{s_1,\cdots,s_n\}$，计算最终多重签名 $S=\prod_{j=1}^{n}s_j$。

（2）服务提供者计算聚合公钥 $apk\leftarrow\prod_{i=1}^{n}pk_i^{a_i}$，并

验证等式：

$$e(S, g^{-1}) \cdot e(H_0(m), \text{apk}) \stackrel{?}{=} 1_{\mathbb{G}_T} \quad (2)$$

若成立，则提供服务。

3.7 正确性分析

方案的正确性依赖于底层代数结构的性质。

对于匿名认证，验证等式（1）的成立基于双线性配对的性质 $e(g^a, g^b) = e(g, g)^{ab}$。将 $V = A_\sigma^v = g^{v/(x+\sigma)}$ 及应答值代入，可消去含 σ 和 x 的项，还原为 a 的定义式。

对于多重签名，等式（2）展开后显然成立。这保证了诚实用户在获得所有授权后必然能通过验证。

综上，方案在代数结构上保证了多方授权逻辑的完备性，其安全性与隐私保护特性将在第 4 节通过形式化规约进一步证明。

4 安全性证明

本节将证明 DMSAA 方案满足匿名性和不可伪造性。该证明建立在随机预言机模型之上，并假设敌手 $\mathcal{A}$ 是概率多项式时间（PPT）的。

4.1 安全模型与敌手定义

本文定义两个安全博弈来形式化方案的安全目标。在博弈中，挑战者维护系统环境，敌手 $\mathcal{A}$ 可访问随机预言机及以下预言机：O_{issue}（注册查询）、O_{auth}（授权查询）和 O_{corrupt}（腐化查询）。

（1）匿名性：匿名性通过一个不可区分性博弈 $\text{Game}_{\text{Anon}}$ 定义。

博弈流程：挑战者运行系统初始化，并将公钥发送给敌手。敌手选择两个已注册的诚实用户 U_0，U_1、一个目标授权机构 AA 和消息 m。挑战者随机选择 $b \in \{0, 1\}$，模拟 U_b 与 AA 的认证交互，并将交互记录 π^* 发送给敌手。敌手输出猜测 b'。

定义 1：若 $|\Pr[b' = b] - 1/2|$ 是可忽略的，则称方案满足匿名性。

（2）不可伪造性：不可伪造性通过存在性不可伪造（EUF-CMA）博弈 $\text{Game}_{\text{Unforge}}$ 定义。

博弈流程：敌手可适应性地询问 O_{issue} 和 O_{auth}，并最多腐化 $t < n$ 个授权机构。最后，敌手输出一个伪造的多重签名 σ^* 及对应的消息 m^* 和公钥集合 $\{\text{PK}_i\}^*$。

获胜条件：（1）σ^* 通过验证；（2）敌手未询问过关于 m^* 和所有未腐化机构的 O_{auth}。

定义 2：若敌手获胜的概率是可忽略的，则称方案满足不可伪造性。

4.2 匿名性证明

定理 1 在随机预言机模型下，如果 DMSAA 方案中所采用的基于签名的零知识集合成员证明协议本身是诚实验证者零知识（Honest-Verifier Zero-Knowledge，HVZK）的，那么 DMSAA 方案满足匿名性。

证明：本文通过构造一个模拟器 Sim 来证明该定理。该模拟器可以为 $\text{Game}_{\text{Anon}}$ 游戏中的挑战阶段生成一个计算上不可区分的交互记录 π^*，而无需知道挑战比特 b 或用户 U_b 的任何秘密信息。

模拟 i-VP：底层的零知识证明协议是诚实验证者零知识的，这意味着存在一个模拟器 Sim_{zkp}。Sim_{zkp} 可以在不知道用户凭证（σ，r）的情况下，生成一个与协议消息（V，C，a，D）具有相同分布的模拟消息（V'，C'，a'，D'）。所构造的模拟器 Sim 调用 Sim_{zkp} 来生成这些参数，并将它们封装进一个 i-VP 中。

模拟挑战 – 应答：Σ – 协议在收到挑战者（在此博弈中是授权机构）的随机挑战 c 后，Sim_{zkp} 同样可以生成一组应答（z'_σ，z'_v，z'_r），使得整个交互记录（V'，C'，a'，D'，c，z'_σ，z'_v，z'_r）是一个可以通过验证的、有效的会话，并且其分布与真实交互记录 π^* 在计算上不可区分。

归约论证：假设存在一个 PPT 敌手 $\mathcal{A}$ 能够以不可忽略的优势 ϵ 在 $\text{Game}_{\text{Anon}}$ 中获胜，即 $\text{Adv}_{\text{DMSAA}, A^{\text{Anon}}}(\lambda) \geqslant \epsilon$。这意味着 $\mathcal{A}$ 能够区分出挑战者是与用户 U_0 交互还是与用户 U_1 交互。可以利用这个敌手 $\mathcal{A}$ 来构造一个新的算法 $\mathcal{B}$，该算法可以攻破底层零知识证明协议的诚实验证者零知识性质。算法 $\mathcal{B}$ 在其自己的诚实验证者零知识游戏中，当收到一个挑战记录（可能是真实的，也可能是模拟的）时，将该记录转发给 $\mathcal{A}$。$\mathcal{A}$ 的输出 b' 将直接作为 $\mathcal{B}$ 的输出。由于已经证明了 $\text{Game}_{\text{Anon}}$ 中的交互记录与模拟记录在计算上不可区分，因此敌手 $\mathcal{A}$ 区分真实交互记录的能力，等价于区分真实与模拟协议视图的能力。如果 $\mathcal{A}$ 能以优势 ϵ 获胜，那么算法 $\mathcal{B}$ 也能以相同的优势 ϵ 攻破底层协议的诚实验证者零知识性质。

结论：第 1 节所述“基于签名的零知识集合成员证明”协议已经被证明是诚实验证者零知识的[23]，因此，任何能够攻破其诚实验证者零知识性质的 PPT 算法都不存在。由此可得，能够以不可忽略优势攻破本方案匿名性的敌手 $\mathcal{A}$ 也不存在。因此 $\text{Adv}_{\text{DMSAA}, A^{\text{Anon}}}(\lambda)$ 必然是一个可忽略函数。

证毕。

4.3 不可伪造性证明

定理 2 在随机预言机模型下，如果协同迪菲 – 赫尔曼（co-CDH）问题和 q-强迪菲–赫尔曼（q-SDH）

问题在底层的双线性群$\mathbb{G}$中是困难的，那么 DMSAA 方案满足不可伪造性。

本证明的核心是展示任何能够以不可忽略的优势ϵ成功伪造 DMSAA 签名的 PPT 敌手$\mathcal{A}$，都可以被用来构造另一个 PPT 算法$\mathcal{B}$，该算法能够以不可忽略的概率解决 co-CDH 问题或 q-SDH 问题。由于本文假设这两个问题是计算困难的，这意味着这样的敌手$\mathcal{A}$必然不存在。本文将通过一个混合论证来构建此归约。

证明：假设存在一个 PPT 敌手$\mathcal{A}$，它能够在$\text{Game}_{\text{Unforge}}$博弈中以不可忽略的优势$\epsilon$获胜。这意味着$\mathcal{A}$最终输出一个伪造的$(m^*, \{\text{PK}_{\text{AA}_i}\}^*, \sigma^*)$，满足 $\text{Verify}(\text{PP}, \{\text{PK}_{\text{AA}_i}\}^*, m^*, \sigma^*)=1$，并且$\mathcal{A}$没有针对消息$m^*$通过$O_{\text{auth}}$查询过集合$\{\text{PK}_{\text{AA}_i}\}^*$中所有未被腐化的授权机构的签名。构造一个算法$\mathcal{B}$，它利用敌手$\mathcal{A}$作为子程序，试图解决 co-CDH 问题或 q-SDH 问题。$\mathcal{B}$将模拟$\text{Game}_{\text{Unforge}}$的环境给$\mathcal{A}$。根据$\mathcal{A}$伪造成功的方式，可以区分两种主要情况：

（1）情况一：敌手$\mathcal{A}$伪造了最终的多重签名。在这种情况下，敌手$\mathcal{A}$可能已经通过O_{auth}查询或腐化查询获得了部分授权机构的部分签名，但它设法在没有获得所有必需的、来自未腐化机构的合法部分签名的情况下，构造出了一个能够通过最终验证的聚合签名σ^*。

归约到 co-CDH：可以构建一个算法$\mathcal{B}_{\text{co-CDH}}$，它接收一个 co-CDH 问题的实例$(g^\alpha, g^\beta, g_2^\beta)$（在本文的对称设定下是$(g^\alpha, g^\beta, g^\beta)$）。$\mathcal{B}_{\text{co-CDH}}$模拟$\text{Game}_{\text{Unforge}}$给$\mathcal{A}$。它将挑战公钥（例如，某个未被腐化的授权机构的公钥PK_{AA_i}）嵌入为g^β。它响应$\mathcal{A}$的随机预言机查询和签名查询（对于非挑战机构或者非伪造消息）。当$\mathcal{A}$成功输出伪造$(m^*, \{\text{PK}_{\text{AA}_i}\}^*, \sigma^*)$时，$\mathcal{B}_{\text{co-CDH}}$可以利用这个伪造签名和模拟过程中的已知信息，通过应用广义分叉引理技术[24]（即运行$\mathcal{A}$两次并改变H_1的输出），来提取出 co-CDH 问题的解$g^{\alpha\beta}$。这实质上是将$\mathcal{A}$攻破本文方案中多重签名组件的能力，归约到了攻破底层紧凑多重签名方案本身的安全性的能力，而后者已被证明等价于 co-CDH 困难性[17]。值得注意的是，由于本文方案在聚合过程中引入了非线性系数a_i，该归约过程同时也涵盖了对流氓密钥攻击的防范。

（2）情况二：敌手$\mathcal{A}$欺骗了至少一个诚实的授权机构。在这种情况下，敌手$\mathcal{A}$可能通过某种方式（例如，提供一个伪造的 i-VP 或在挑战－应答阶段作弊）欺骗了一个未被腐化的授权机构AA_k，使得该机构为一个本不应授权的请求错误地生成并返回了一个有效的部分签名s_k。

归约到 q-SDH：可以构建一个算法$\mathcal{B}_{q\text{-SDH}}$，它接收一个 q-SDH 问题的实例$(g, g^x, \cdots, g^{x^q})$。$\mathcal{B}_{\text{q-SDH}}$模拟$\text{Game}_{\text{Unforge}}$给$\mathcal{A}$。它将注册机构的公钥$\text{PK}_{\text{RA}}$设置为$g^x$，并响应$\mathcal{A}$的随机预言机查询和签名查询。如果$\mathcal{A}$成功欺骗了一个诚实的授权机构$\text{AA}_k$并使其输出了一个部分签名$s_k$，这意味着$\mathcal{A}$实际上攻破了底层零知识集合成员证明协议的可靠性。正如第 2 节所述，该零知识证明的可靠性依赖于 Boneh-Boyen 签名的不可伪造性，而 Boneh-Boyen 签名的不可伪造性最终被归约到了 q-SDH 假设的困难性[22]。因此，$\mathcal{B}_{\text{q-SDH}}$可以利用$\mathcal{A}$成功欺骗$\text{AA}_k$这一事件，构造出对 q-SDH 问题的一个解$(c, g^{1/(x+c)})$。

结论：由于任何能够以不可忽略优势ϵ成功伪造 DMSAA 签名的敌手$\mathcal{A}$，都必然导致可以构造一个算法$\mathcal{B}$以不可忽略的概率解决 co-CDH 问题或 q-SDH 问题之一。而这两个问题在我们的安全模型中被假设是计算困难的。因此，不存在能够以不可忽略优势成功伪造 DMSAA 签名的 PPT 敌手。故 DMSAA 方案满足不可伪造性。

证毕。

5 性能分析

本节采用理论分析与实验仿真相结合的方式，对 DMSAA 方案的计算开销、通信带宽及存储需求进行综合评估。为了体现方案的优势，将 DMSAA 与标准的基于 BLS 的多重签名方案[16]、支持隐私保护的 BBS + 签名方案[12]，以及近年来针对去中心化身份场景提出的新型优化方案 Coconut[25] 和 T-BBS +[26] 进行了全面对比。

5.1 符号定义与实验环境

实验运行在搭载 Intel（R）Core（TM）i9-13900HX（2.20 GHz）处理器、16 GB 内存的 PC 上，操作系统为 Windows 11。算法基于 PBC 库[27]实现，选用 Type-A 曲线提供的 128 bit 安全等级，该曲线$(y^2 = x^3 + x)$因具备极高的对称配对效率，特别适用于计算资源受限的去中心化节点。在关键参数的实例化方面：

（1）哈希函数$H_1: \{0,1\}^* \to \mathbb{Z}_p$采用 SHA-256 算法将输入消息映射为 256 位摘要后模p得到；哈希函数$H_0: \{0,1\}^* \to \mathbb{G}$则在 SHA-256 的基础上，通过 PBC 库内置的 MapToGroup 确定性算法将比特串映射为群元素。

（2）协议涉及的所有随机数（包括致盲因子v，r、

辅助随机数 s，t，k 及挑战值 c）均通过操作系统底层的密码学安全伪随机数生成器 CSPRNG（如/dev/urandom）获取。由于 CSPRNG 的吞吐量远高于群运算，其生成微秒级的开销在后续性能分析中相比于毫秒级的指数运算 T_{exp} 可忽略不计。

为了便于理论分析，定义表 1 所示的时间符号来表示各基础密码学操作的耗时。由于哈希运算 T_h 和群加法/乘法运算 T_{mul} 的耗时远小于指数与配对运算，在后续的渐进复杂度分析中将忽略不计。

表 1　密码学原语符号定义及基准耗时

符号	描述	平均耗时/ms
T_{bp}	双线性配对运算	7.03
T_{exp}	群$\mathbb{G}$或$\mathbb{G}_T$中的指数运算	3.05
T_{pair_exp}	$\mathbb{G}_T$中的多重指数配对运算	8.12

5.2　理论开销分析

各方案理论开销与特性对比如表 2 所示。其中 n 表示授权机构或签名者的数量，m 表示消息的数量。

表 2　方案理论开销与特性对比

指标	BLS 多签	BBS + 签名	Coconut	T-BBS +	DMSAA
用户开销	$1T_{exp}$	$1T_{exp}$	$\approx 5T_{exp}$	$\approx 4T_{exp}$	$3nT_{exp}$
验证开销	$2T_{bp}+(n-1)T_{mul}$	$3T_{bp}+(m+4)T_{exp}$	$2T_{bp}+mT_{exp}$	$3T_{bp}+mT_{exp}$	$2T_{bp}+nT_{exp}$
签名尺寸	$1\mid\mathbb{G}\mid$	$1\mid\mathbb{G}\mid+2\mid\mathbb{Z}_p\mid$	$2\mid\mathbb{G}\mid$	$1\mid\mathbb{G}\mid+2\mid\mathbb{Z}_p\mid$	$1\mid\mathbb{G}\mid$
隐私性	×	√	√	√	√
多方授权	√	×	√	√	√
W3C 兼容性	弱	一般	弱	弱	强

计算复杂度方面。为了充分验证方案在当前技术背景下的优越性，本文选取了新型优化方案 Coconut 和 T-BBS + 作为核心基线进行对比。DMSAA 在用户端引入了与 n 相关的线性开销 $3nT_{exp}$，这是在多方交互中生成零知识承诺所必需的。尽管在理论复杂度上高于采用门限聚合的上述两种新型同类方案，但得益于本文方案仅涉及轻量级的指数运算，避免了基线方案中复杂的盲签名盲化与去盲操作，其实际计算耗时仍控制在高效范围内，并未产生实际应用中的性能瓶颈。

验证效率与存储方面。首先在验证效率上，本文方案将昂贵的双线性配对运算固定为 2 次，相比于验证复杂度随属性数量 m 线性增长的基线方案，在多属性凭证验证场景下具有更高的计算效率。其次在存储开销上，基线方案 Coconut 的凭证由 2 个群元素组成，而 T-BBS + 则需要 1 个群元素和 2 个标量。相比之下，本文方案利用聚合特性，使最终生成的授权凭证仅包含 1 个群元素，且不包含任何额外的标量数据。同时，本方案也优于不具备隐私保护能力的传统 BLS 多签方案。这意味着无论授权节点规模如何扩大，DMSAA 始终保持着理论上的最小存储开销，这一特性使其比传统及新型优化方案更适用于存储受限的分布式环境。

在隐私保护与协议兼容性方面，DMSAA 实现了功能上的全面覆盖。与 BLS 多重签名方案缺乏隐私保护、以及标准 BBS + 签名难以支持多方授权不同，DMSAA 与 Coconut、T-BBS + 均具备匿名性与多方授权的双重特性，达到了同等的隐私保护强度。然而，在协议兼容性维度上，Coconut 和 T-BBS + 通常依赖定制化的密码学证明结构，难以直接适配现有的 DID 标准；而本文方案专门设计了兼容 W3C 标准的数据结构，能够将参数透明地封装于标准 VP 数据模型中。这使得本文方案在无需修改底层基础设施的前提下即可在现有 DID 生态中部署，具备更强的工程实用性与兼容性优势。

5.3　实验结果分析

基于上述理论模型，本文进行了仿真实验以重点分析方案在关键参数变化下的性能表现。在实验设计上，采用了控制变量法进行参数敏感性分析。鉴于本文方案主要应用于联盟链或多方计算环境，参考 Libra 等主流去中心化系统的验证节点规模，本文将核心变量授权机构数量 n 的取值范围设定为 [3，50]。其中，$n=3$ 代表最小可行多方授权场景，而 $n=50$ 则模拟超出常规需求的高负载压力测试场景。通过在此区间内连续调整 n 值，观测并分析方案在计算与通信开销上的敏感性特征，以验证系统的稳定性与可扩展性。具体实验结果如下：

（1）在线计算开销：实验结果（图 4）与理论分析一致。

AA 开销恒定：单个 AA 的耗时稳定在 35 ms 左右，主要用于验证用户提交的零知识承诺（约 4 次指数运算），与系统规模 n 无关。

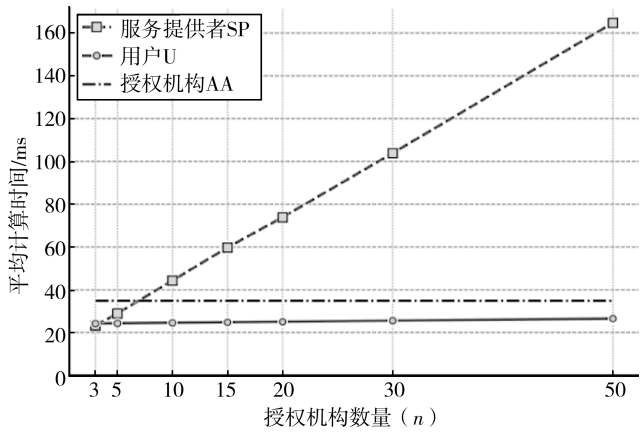

图4　各实体在线计算开销 vs. 授权机构数量

用户端参数敏感性分析：用户开销随 n 呈严格线性增长（$3nT_{exp}$），但增长斜率较低。实验表明，致盲因子 v，r 及辅助随机数 s，t，k 的生成与计算引入的是固定常数级底噪，不随 n 的变化产生波动。即使在 $n=50$ 的高负载下，用户总耗时仍控制在可接受范围内（约 25 ms），表明方案对大规模多方授权场景具有良好的参数稳定性。

SP 验证效率高：由于 T_{bp} 是常数级的，SP 的验证时间主要由线性增长的指数运算 nT_{exp} 决定。实验表明，在 $n=50$ 时验证时间约为 160 ms，这在实际应用中是完全可接受的。

（2）通信开销：如图 5 所示，通信开销随 n 线性增长，主要源于用户需分别向每个 AA 发送大小约为1 KB 的 i-VP 数据包。然而，最终提交给 SP 的数据仅需包含聚合签名和参与方索引，保持了极低的带宽占用。

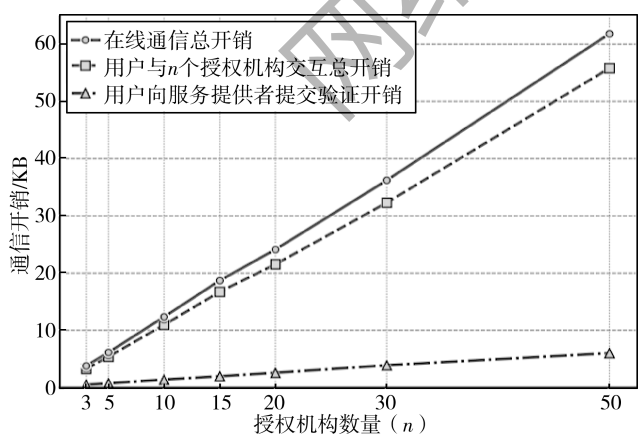

图5　总在线通信开销 vs. 授权机构数量

6　结论

本文针对去中心化身份体系中多方授权场景下的隐私泄露问题，提出了一种具有匿名认证能力的去中心化多方授权方案（DMSAA）。通过将紧凑多重签名与交互式零知识证明有机融合，该方案在确保授权安全性的同时，严格保护了参与方的身份隐私。安全性证明表明方案在随机预言机模型下满足不可伪造性与匿名性。性能分析显示，方案具有常数级的凭证大小和良好的可扩展性，适用于存储受限的分布式环境。未来的工作将集中在两方面：一是引入批处理验证技术以进一步提升授权机构的并发处理能力；二是探索在可控匿名场景下的监管机制，以平衡隐私保护与合规性需求。

参考文献

[1] SPORNY M, LONGLEY D, SABADELLO M, et al. Decentralized identifiers (DIDs) v1.0 [R/OL]. Draft Community Group Report, 2022.

[2] SPORNY M, LONGLEY D, CHADWICK D, et al. Verifiable credentials data model v2.0 [S]. W3C Recommendation, 2025.

[3] ALLEN C. The path to self-sovereign identity [EB/OL]. (2016-04-25) [2023-10-20]. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/.

[4] TAN K L, CHI C H, LAM K Y. Secure and privacy-preserving sharing of personal health records with multi-party pre-authorization verification [J]. Wireless Networks, 2024, 30 (6): 4773-4795.

[5] ERINLE Y, FENG Y, XU J, et al. Shared-custodial wallet for multi-party crypto-asset management [J]. Future Internet, 2024, 17 (1): 7.

[6] SQUICCIARINI A C, RAJTMAJER S M, ZANNONE N. Multi-party access control: requirements, state of the art and open challenges [C]//Proceedings of the 23rd ACM Symposium on Access Control Models and Technologies. New York: ACM, 2018: 49-59.

[7] KINKELIN H, NIEDERMAYER H, MÜLLER M, et al. Multi-party authorization and conflict mediation for decentralized configuration management processes [C]//2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Piscataway: IEEE, 2019: 5-8.

[8] SANDHU R S. Role-based access control [M] //Advances in Computers: Vol 46. Amsterdam: Elsevier, 1998: 237-286.

[9] LASHKARI B, MUSILEK P. A comprehensive review of blockchain consensus mechanisms [J]. IEEE Access, 2021, 9: 43620-43652.

[10] 祝烈煌，高峰，沈蒙，等. 区块链隐私保护研究综述 [J]. 计算机研究与发展，2017，54 (10)：2170-2186.

[11] SUN J, XU G, ZHANG T, 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.

[12] BONEH D, BOYEN X, SHACHAM H. Short group signatures [C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2004: 41 -55.

[13] CAMENISCH J, LYSYANSKAYA A. Dynamic accumulators and application to efficient revocation of anonymous credentials [C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2002: 61 -76.

[14] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin [C]//2014 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2014: 459 -474.

[15] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple Schnorr multi -signatures with applications to Bitcoin [J]. Designs, Codes and Cryptography, 2019, 87 (9): 2139 -2164.

[16] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2001: 514 -532.

[17] BONEH D, DRIJVERS M, NEVEN G. Compact multi-signatures for smaller blockchains [C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2018: 435 -464.

[18] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 89 -98.

[19] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2001: 552 -565.

[20] ALANGOT B, SZALACHOWSKI P, DINH T T A, et al. Decentralized identity authentication with auditability and privacy [J]. Algorithms, 2022, 16 (1): 4.

[21] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers [J]. Discrete Applied Mathematics, 2008, 156 (16): 3113 -3121.

[22] BONEH D, BOYEN X. Short signatures without random oracles [C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2004: 56 -73.

[23] CAMENISCH J, CHAABOUNI R, SHELAT A. Efficient protocols for set membership and range proofs [C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2008: 234 -252.

[24] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma [C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 390 -399.

[25] SONNINO A, AL-BASSAM M, BANO S, et al. Coconut: threshold issuance selective disclosure credentials with applications to distributed ledgers [J]. arXiv preprint arXiv: 1802.07344, 2018.

[26] DOERNER J, KONDI Y, LEE E, et al. Threshold BBS + signatures for distributed anonymous credential issuance [C]//2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE, 2023: 773 -789.

[27] LYNN B. The pairing-based cryptography (PBC) library [EB/OL]. (2006 -xx -xx) [2023 -10 -20]. https://crypto.stanford.edu/pbc/.

(收稿日期: 2025 -12 -29)

作者简介:

牟翰翔 (2000 -), 男, 硕士研究生, 主要研究方向: 隐私保护、多方授权。

万长胜 (1976 -), 通信作者, 男, 博士, 教授, 主要研究方向: 人工智能、数据分析、应用密码学。E-mail: wanchangsheng@seu.edu.cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部