计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(12): 3093−3105, 2025

基于 SM2 的去中心化匿名凭证方案

赵陆天禹　王化群
（南京邮电大学计算机学院、软件学院、网络空间安全学院　南京　210023）
（zhaolty@aliyun.com）

SM2-Based Decentralized Anonymous Credential Scheme

Zhaolu Tianyu and Wang Huaqun
（*School of Computer Science*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210023）

Abstract　Anonymous credentials are a privacy-preserving authentication method that verifies the holder's qualifications or attributes without revealing their identity, widely used in digital identity management, e-government, and digital banking. Anonymous credentials that comply with Chinese commercial cryptography standards have also garnered significant attention. However, existing anonymous credential schemes often depend on centralized issuing authorities, which not only restrict their applicability in decentralized networks but also introduce risks of system failures and privacy breaches caused by single points of failure. To address these issues, we propose a decentralized anonymous credential scheme based on SM2 commercial cryptography. The proposed scheme leverages blockchain networks to replace credential issuing authorities and employs zero-knowledge proofs to ensure the secure and reliable distribution of credentials. Additionally, the scheme enables users to selectively disclose attributes according to their needs, thereby effectively avoiding the excessive exposure of private information. We also explore the construction methods of zero-knowledge proofs that comply with Chinese commercial cryptography standards and propose a set membership proof scheme based on SM2, providing a foundational tool for designing the SM2-based decentralized anonymous credential. Security analysis proves that the proposed SM2-based decentralized anonymous credential scheme satisfies both unforgeability and anonymity requirements. Performance experiments further show that the scheme maintains efficiency suitable for real-world deployment.

Key words　Chinese commercial cryptography standard; zero-knowledge proof; anonymous credential; blockchain; privacy preservation

摘　要　匿名凭证是一种在不透露持有者身份的前提下验证其资格或属性的隐私保护认证方式，广泛应用于数字身份管理系统、电子政务和数字银行等领域. 符合国家商用密码标准的匿名凭证也备受关注. 然而，现行匿名凭证方案多依赖于中心化的发行机构，这不仅限制了其在去中心化网络中的应用，还易因单点故障导致系统瘫痪和隐私泄露. 为解决上述问题，提出了一种基于 SM2 商用密码的去中心化匿名凭证方案. 该方案利用区块链网络替代传统凭证发行机构，通过零知识证明方案确保凭证分发的安全可靠. 此外，该方案还允许用户根据需求选择性地披露属性，从而有效避免隐私信息的过度泄露. 还探讨了国密化零知识证明方案的构造方法，并提出了基于 SM2 的集合成员关系证明方案，为 SM2 去中心化匿名凭证的设计提供了构造基础. 安全性分析表明，基于 SM2 的去中心化匿名凭证方案满足不可伪造性和匿名性需

收稿日期：2024-09-23；**修回日期**：2025-04-17
基金项目：国家自然科学基金项目（U23B2002, 62272238）；江苏省研究生科研与实践创新计划项目（KYCX24_1200）
This work was supported by the National Natural Science Foundation of China (U23B2002,62272238) and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX24_1200).
通信作者：王化群（wanghuaqun@aliyun.com）

求.性能实验进一步显示,该方案具备实际部署所需的效率.

关键词 国家商用密码标准;零知识证明;匿名凭证;区块链;隐私保护

中图法分类号 TP391

DOI: 10.7544/issn1000-1239.202440756 **CSTR:** 32373.14.issn1000-1239.202440756

近年来,Web3 网络及分布式身份(decentralized identity)受到了社会各界的广泛关注和深入研究.上海市政府出台了《上海市“元宇宙”关键技术攻关行动方案》,旨在推动 Web3 网络操作系统及数字身份管理技术的研发与突破.2023 年区块链产业调研报告显示,国内 74% 的区块链机构已经积极投身于 Web3 及数字资产的探索与研究.Web3 技术的核心目标在于打造一个用户能够全面掌控其数据和身份的分布式网络生态,从而为用户提供更为安全、透明且个性化的线上体验.基于区块链的分布式身份是 Web3 网络实现用户主导和数据隐私的关键支柱,为用户和组织提供了一个开放、可信、去中心化且支持互操作的身份管理方案[1].可验证凭证作为分布式身份的核心要素之一,使用户能够证明自身身份以访问资源或获取服务.匿名凭证(anonymous credential)作为一种隐私保护的身份认证方法,在电子邮箱、数字支付和数字门禁等领域得到了广泛应用[2].然而,现有的匿名凭证方案在分布式身份乃至 Web3 网络中的应用面临着多重挑战.首先,大多数方案依赖于中心化凭证发行机构,这不仅增加了隐私数据泄露的风险,单点故障还可能引发系统的全面瘫痪.其次,符合国家商用密码标准的去中心化匿名凭证的研究尚属空白,难以满足建设自主可控的 Web3 网络的需求.

随着我国数字化建设的深入发展,商用密码在保障网络空间安全方面扮演着举足轻重的角色.国家颁布的《商用密码管理条例》明确规定了网络运营者需遵守国家网络安全等级保护制度,利用商用密码来加强网络安全.区块链技术作为新型网络基础设施,已广泛应用于数字金融、电子政务和医疗健康等领域,其安全性与稳定性直接关系到国家主权及网络空间安全.因此,我国重视自主化区块链与 Web3 网络的研发,同时着力于基础性的国家商用密码算法开发,以代替现行的国际密码算法.国家密码管理局已制定了一系列密码标准,如 SM2 椭圆曲线公钥密码算法[3]、SM3 密码杂凑算法、SM4 分组密码算法及 SM9 标识密码算法等,以提供安全可控的算法支持.然而在 Web3 网络中,尤其是在隐私保护的分布式身份认证方面,现有的国家商用密码算法仍显不足,符合国密标准的去中心化匿名凭证方案亟待研究与完善.

本文的主要贡献如下:

1)提出一个基于 SM2 的去中心化匿名凭证方案,不依赖于中心化的凭证发行机构,避免单点故障导致的隐私泄露和系统瘫痪.方案还允许用户在匿名身份认证时,根据需要选择性地披露属性子集,避免隐私数据过度泄露.

2)提出一个基于 SM2 的集合成员关系证明(set membership proof)方案,填补了国密算法在集合成员关系证明方面的空缺.此方案同时也是 SM2 去中心化匿名凭证方案的设计基础.

3)对 SM2 去中心化匿名凭证方案进行了安全性分析和性能评估.安全性分析表明方案满足完备性、匿名性和不可伪造性.实验结果显示本方案是高效的,凭证证明和验证的计算开销分别为 5.29 ms 和 3.51 ms.

1 相关工作

1.1 去中心化匿名凭证

匿名凭证[2,4-6]是一种隐私增强的身份认证技术,其主要包括凭证发行机构、用户和服务提供商 3 个实体.在匿名凭证协议中,用户向凭证发行机构登记注册,发行机构为合法用户签发包含属性的凭证.为了向服务提供商请求服务,用户以隐私保护的方式证明其持有合法凭证且属性满足访问规则.Camenisch 等人[2]率先提出了完全匿名的凭证方案,确保凭证证明无法与先前的证明或任何与用户身份相关的信息建立关系.Baldimtsi 等人[4]首次提出不依赖于双线性配对的轻量级的匿名凭证方案,适用于计算能力有限的设备.为了确保算法自主可控、减少对国外算法的依赖、降低信息泄露的风险,赵艳琦等人[5]结合 SM2 签名算法和零知识证明协议,设计了符合国家商用密码标准的匿名凭证,具备匿名性和不伪造性.

上述匿名凭证方案依赖于集中式发行方,这带来了单点故障的风险.此外,若发行方存储的敏感数据被窃取,则可能引发大规模隐私泄露和身份盗用.为解决这些问题,去中心化匿名凭证方案应运而生.

现有设计方法主要分为2类：一类以去中心化网络（如区块链）和零知识证明协议替代集中式发行方. Garman等人[7]提出了去中心化的匿名凭证方案. 该方案利用区块链替代了凭证发行中心，允许用户在本地计算包含身份和属性的凭证，并且生成可被公开验证的凭证有效性证明. 区块链的共识节点会将经过验证的凭证上链，确保了凭证的不可篡改. Yang等人[8]则基于区块链设计了一种支持黑名单功能的去中心化匿名凭证系统. 另一类方法是用多个发行机构取代集中式的发行中心. Sonnino等人[9]首次提出了支持门限凭证发行的匿名凭证系统，该系统集成了签名算法、零知识证明协议和区块链网络，确保凭证的不可伪造性、匿名性和可用性. 在门限模型中，用户需获得n个授权机构中至少t个授权，才能得到有效凭证. 只要被敌手攻破的节点数量低于设定的门限值，整个匿名凭证系统就能保持安全可靠. Doerner等人[10]提出了一种基于BBS+签名的多方安全签名协议，并基于此协议实现了门限式匿名凭证发行. Mir等人[11]提出了门限可委托谓词加密算法，并据此设计了门限可委托的匿名凭证系统. Mir等人[12]还引入了聚合水银签名，并基于此构建了一种多权威匿名凭证系统. 在该系统中，每个权威机构负责授权特定属性，用户可从多个权威机构获取不同属性的授权，并将其聚合为个人凭证. 目前，符合国家商用密码标准的去中心化匿名凭证的研究仍是空白.

1.2 集合成员关系证明

集合成员关系证明，作为零知识证明技术的一种，可以被用来构造匿名凭证系统. Camenisch等人[13]基于双线性对或RSA提出了集合成员关系证明，其允许证明者证明承诺$cm = Commit(a_l, r)$中的a_l是公开集合$\{a_1, a_2, \cdots, a_n\}$中的元素. Bayer等人[14]也提出了证明大小为对数级别的集合成员关系证明协议，还支持非成员关系证明. Groth等人[15]进一步提出了“one out of many proofs”，其允许证明者在不暴露其他信息的前提下，证明承诺集合$\{cm_1, cm_2, \cdots, cm_n\}$中的1个成员的打开值为0，且证明大小与集合大小成对数关系. 同时，证明者还不需要知道其他承诺的打开值. Diamond[16]提出了“many out of many proofs”的概念，其为“one out of many proofs”的扩展，允许证明者证明承诺集合的1个子集中的每个成员的打开值都是0，而不泄露具体是哪个子集. Zeng等人[17]提出了零知识函数证明的概念，并给出了集合成员关系函数证明的具体构造，允许证明者证明承诺cm中隐藏的元素是公开集合的成员，并允许验证者从证明中提取被承诺元素的函数值. 除了匿名凭证，集合成员关系证明及其后续研究还可以被用来构造环签名和去中心化匿名支付系统[15].

符合国家商用密码标准的零知识证明方案的研究相对较少. 林超等人[18]提出了一种基于SM2的高效范围证明方案，该方案满足完备性、可靠性和诚实验证者零知识性. 黎琳等人[19]提出简洁非交互式零知识证明的底层双线性对的国密化方案. 但是集合成员关系证明的国密化研究仍有待进一步推进与完善.

1.3 隐私保护身份认证

除了零知识证明技术，环签名和盲签名等技术也被广泛应用于隐私保护的身份认证. Lai等人[20]指出，环签名和盲签名与匿名凭证具有类似的安全属性：环签名确保用户签署的消息对验证者而言是匿名的；而盲签名则确保可信中心（即消息签署者）无法获知消息的具体内容. 这一特性使得在使用盲签名时，可信中心无法将消息与签署记录关联起来. 事实上，环签名已广泛应用于车载自组织网络（vehicular ad-hoc network, VANET）、电子投票和去中心化支付等场景中的匿名身份认证. Mundhe等人[21]提出了一种面向VANETs的基于环签名的轻量级隐私保护认证协议，以解决VANETs中恶意节点广播错误消息阻碍网络正常运行的问题. Fujisaki等人[22]首次提出了可追溯环签名，并指出该方案可用于匿名投票场景中的身份认证，防止恶意用户重复投票. 可链接环签名广泛应用于去中心化匿名支付系统中的身份认证，确保交易过程中的用户身份匿名[23]. 盲签名也被应用于LET网络、电子医疗和私人访问令牌（private access token, PAT）等场景中的身份认证. 秦宁元等人[24]设计了面向LET网络的切换认证协议，利用盲签名建立切换过程中的认证密钥，确保切换过程中的匿名性. Hanzlik[25]提出了面向随机消息的非交互式盲签名，允许用户通过盲签名向可信中介申请有限数量的一次性PATs，并基于这些令牌与服务提供商完成认证并请求服务. Baldimtsi等人[4]基于具有属性设置的盲签名和零知识证明协议，设计了一种适用于RFID和移动设备的轻量级匿名凭证，其中盲签名确保了凭证对发行者的匿名，而零知识证明则确保了凭证对验证者的匿名性.

2 基础知识

2.1 符号定义

本文使用$[N]$表示集合$\{1,2,\cdots,N\}$，给定一组椭

圆曲线参数$\{p,F_p,E(F_p),\mathbb{G},q,G\}$, 其中$p$为大素数, F_p为有限域, $E(F_p)$为定义在F_p上的椭圆曲线, $\mathbb{G}$为$E(F_p)$上的点构成的q阶加法群, G为$\mathbb{G}$中的生成元. 对于

$$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\mathbb{Z}_q^n,$$
$$\boldsymbol{G}=(G_1,G_2,\cdots,G_n)\in\mathbb{G}^n,$$

定义$\boldsymbol{x}$和$\boldsymbol{G}$间的点乘为

$$\boldsymbol{x}\cdot\boldsymbol{G}=\sum_{i\in[n]}x_i\times G_i.$$

对于标量$k\in\mathbb{Z}_q$, 其与向量$\boldsymbol{x}$的乘法定义为

$$k\boldsymbol{x}=(kx_1,kx_2,\cdots,kx_n).$$

此外, 本文使用向量$\boldsymbol{a}=(a_1,a_2,\cdots,a_l)$表示$l$个不同属性. 使用$\boldsymbol{v}=(v_1,v_2,\cdots,v_l)$表示用户的属性值. 对于$\forall i\in[l]$, 用户的属性$a_i$的属性值为$v_i$.

2.2 零知识证明

非交互式零知识证明(non-interactive zero-knowledge proof, NIZK)包含2个参与方: 证明者和验证者. 对于关系$\mathcal{R}$, 若存在陈述α和证据ϖ满足$(\alpha,\varpi)\in\mathcal{R}$, 证明者可以向验证者证明陈述$\alpha$为真, 且不泄露关于证据$\varpi$的其他任何信息. 知识签名(signature of knowledge, SoK)是一种和零知识证明密切相关的签名算法, 由Chase等人[26]首次提出. 对于$(\alpha,\varpi)\in\mathcal{R}$, 知识签名允许签名者使用证据$\varpi$签署消息, 并证明陈述$\alpha$为真. 和零知识证明类似, 知识签名也不会泄露证据ϖ的任何信息. Fiat-Shamir启发式可以通过哈希函数将交互式证明转换为NIZK或SoK协议[27].

Sigma协议是一类常见的交互式零知识证明. 本文所提出的方案基于如下关系的Sigma协议:

$$\mathcal{R}_L=\left\{\begin{array}{c}\alpha=(C,y),\varpi=(\boldsymbol{x},\mu):\\ |\boldsymbol{x}|=|\boldsymbol{G}|=m\wedge y=L(\boldsymbol{x})\wedge\\ C=\boldsymbol{x}\cdot\boldsymbol{G}+\mu\times H\end{array}\right\},$$

$$\mathcal{R}_{\mathrm{ZKP}}=\left\{\begin{array}{c}\alpha=(C,C'),\varpi=(\boldsymbol{v},\rho,r,r'):\\ \boldsymbol{x}=(\boldsymbol{v},\rho)\wedge|\boldsymbol{x}|=|\boldsymbol{G}|=m\wedge\\ C=\boldsymbol{x}\cdot\boldsymbol{G}+r\times H\wedge\\ C'=\rho\times G_m+r'\times H\end{array}\right\},$$

$$\mathcal{R}_{\mathrm{SoK}}=\left\{\begin{array}{c}\alpha=(C,C',\boldsymbol{v}),\varpi=(\rho,r,r'):\\ \boldsymbol{x}=(\boldsymbol{v},\rho)\wedge|\boldsymbol{x}|=|\boldsymbol{G}|=m\wedge\\ C=\boldsymbol{x}\cdot\boldsymbol{G}+r\times H\wedge\\ C'=\rho\times G_m+r'\times H\end{array}\right\}.$$

$\mathcal{R}_L$中的$L(\cdot)$表示对n维向量中的各个分量的线性组合. 例如, 向量$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)$表示$L(\cdot)$的线性组合系数, 对于向量$\boldsymbol{x}$, $L(\boldsymbol{x})$等于$\boldsymbol{h}$与$\boldsymbol{x}$的内积$\langle\boldsymbol{h},\boldsymbol{x}\rangle$.

Attema等人[28]提出面向关系$\mathcal{R}_L$的Sigma协议, 具体算法如下:

1)证明者选取随机数$\boldsymbol{t}\in\mathbb{Z}_q^{*n}$, $r\in\mathbb{Z}_q^*$, 计算$T=r\times H+\boldsymbol{t}\cdot\boldsymbol{G}$, $\gamma=L(\boldsymbol{t})$, 将(T,γ)发送给验证者.

2)验证者选取随机数$e\in\mathbb{Z}_q^*$发送给证明者.

3)证明者计算$\boldsymbol{z}=e\boldsymbol{x}+\boldsymbol{t}$和$\phi=e\mu+r$, 并将$(\boldsymbol{z},\phi)$发送给验证者.

4)如果等式$\boldsymbol{z}\cdot\boldsymbol{G}+\phi\times H=T+e\times C$和等式$L(\boldsymbol{z})=\gamma+ey$都成立, 验证者输出1.否则, 输出0.

对关系$\mathcal{R}_{\mathrm{ZKP}}$和$\mathcal{R}_{\mathrm{SoK}}$的Sigma协议本文不再赘述. 上述3种Sigma协议可以通过Fiat-Shamir启发式转换为NIZK或SoK协议. 我们分别使用Π_L和Π_{ZKP}表示关系$\mathcal{R}_L$和$\mathcal{R}_{\mathrm{ZKP}}$的NIZK方案, 并使用$\Pi_{\mathrm{SoK}}$表示关系$\mathcal{R}_{\mathrm{SoK}}$的SoK方案.

NIZK方案包含初始化算法$Setup$、证明算法$Prove$和验证算法$Verify$, 形式化定义如下:

1)$Setup(1^\lambda)\to crs$. 本算法以安全参数λ为输入, 输出公共参考字符串crs.

2)$Prove(crs,\alpha,\varpi)\to\pi$. 本算法以公共参考字符串$crs$、陈述$\alpha$和证据$\varpi$为输入, 输出证明$\pi$.

3)$Verify(crs,\alpha,\pi)\to 0/1$. 本算法以公共参考字符串$crs$、陈述$\alpha$和证明$\pi$为输入. 若证明有效, 算法输出1. 否则, 输出0.

安全的NIZK方案满足完备性、可靠性和零知识性.

1)完备性. 对于$(\alpha,\varpi)\in\mathcal{R}$,

$$Pr\left[\begin{array}{c}crs\leftarrow Setup(1^\lambda),\\ \pi\leftarrow Prove(crs,\alpha,\varpi):\\ Verify(crs,\alpha,\pi)=1\end{array}\right]\geqslant 1-negl(\lambda).$$

2)可靠性. 对任何$(\alpha,\varpi)\in\mathcal{R}$, 证明者必须持有证据$\varpi$才能为陈述$\alpha$生成有效的证明. 对任何概率多项式时间(probabilistic polynomial time, PPT)敌手$\mathcal{A}$, 存在PPT提取器算法$\mathcal{E}$, 满足

$$Pr\left[\begin{array}{c}crs\leftarrow Setup(1^\lambda),\\ (\pi,\alpha)\leftarrow\mathcal{A}(crs),\\ \varpi\leftarrow\mathcal{E}(crs,\pi,\alpha):\\ Verify(crs,\alpha,\pi)=1\wedge\\ (\alpha,\varpi)\notin\mathcal{R}\end{array}\right]\leqslant negl(\lambda).$$

3)零知识性. 证明者可以向验证者证明陈述α为真, 且不泄露关于证据ϖ的其他任何信息. 对任何PPT敌手$\mathcal{A}$, 存在PPT模拟器算法$\mathcal{S}$, 满足

$$\left|Pr\left[\begin{array}{c}crs\leftarrow Setup(1^\lambda),\\ \pi\leftarrow Prove(crs,\alpha,\varpi):\\ \mathcal{A}(crs,\alpha,\pi)=1\end{array}\right]-\right.$$
$$\left.Pr\left[\begin{array}{c}(crs,\hbar)\leftarrow\mathcal{S}(1^\lambda),\\ \pi'\leftarrow\mathcal{S}(crs,\alpha,\hbar):\\ \mathcal{A}(crs,\alpha,\pi')=1\end{array}\right]\right|\leqslant negl(\lambda).$$

SoK方案包含初始化算法$Setup$、签名算法$Sign$

和验证算法$Verify$，形式化定义如下：

1）$Setup(1^\lambda)\to crs$. 本算法以安全参数λ为输入，输出公共参考字符串crs.

2）$Sign(crs,\alpha,\varpi,msg)\to\sigma$. 本算法以公共参考字符串$crs$、陈述$\alpha$、证据$\varpi$和消息$msg$为输入，输出签名$\sigma$.

3）$Verify(crs,\alpha,\sigma,msg)\to 0/1$. 本算法以公共参考字符串$crs$、陈述$\alpha$、签名$\sigma$和消息$msg$为输入. 若签名有效，算法输出1.否则，输出0.

和NIZK方案类似，安全的SoK方案具备正确性、可模拟性和可提取性.

1）正确性. 对于任何$(\alpha,\varpi)\in\mathcal{R}$，

$$Pr\left[\begin{array}{c} crs\leftarrow Setup(1^\lambda),\\ \pi\leftarrow Sign(crs,\alpha,\varpi,msg):\\ Verify(crs,\alpha,\sigma,msg)=1\end{array}\right]\geqslant 1-negl(\lambda).$$

2）可模拟性. 存在2个PPT算法

$$SimSetup(1^\lambda)\to(crs,\hbar),$$
$$SimSign(crs,\hbar,\alpha,msg)\to\sigma.$$

对于任何PPT敌手$\mathcal{A}$，满足

$$\left|Pr\left[\begin{array}{c}(crs,\hbar)\leftarrow SimSetup(1^\lambda):\\ \mathcal{A}^{O_{\text{sim}}}(crs)=1\end{array}\right]-Pr\left[\begin{array}{c} crs\leftarrow Setup(1^\lambda):\\ \mathcal{A}^{O_{\text{sign}}}(crs)=1\end{array}\right]\right|\leqslant negl(\lambda),$$

其中预言机O_{sim}以(α,ϖ,msg)为输入，如果$(\alpha,\varpi)\in\mathcal{R}$，其输出

$$\sigma\leftarrow SimSign(crs,\hbar,\alpha,msg),$$

否则，输出$\perp$.

3）可提取性. 除了算法$SimSetup$和$SimSign$，还存在PPT提取器算法Ext，对于任何PPT敌手$\mathcal{A}$，满足

$$Pr\left[\begin{array}{c}(crs,\hbar)\leftarrow SimSetup(1^\lambda),\\ (\alpha,\sigma,msg)\leftarrow\mathcal{A}^{O_{\text{sim}}}(crs),\\ \varpi\leftarrow Ext(crs,\hbar,\alpha,\sigma,msg):\\ (\alpha,\varpi)\in\mathcal{R}\vee(\alpha,\sigma,msg)\in\mathcal{L}\vee\\ Verify(crs,\alpha,\sigma,msg)=0\end{array}\right]\geqslant 1-negl(\lambda),$$

其中列表$\mathcal{L}$记录了$\mathcal{A}$对O_{sim}的成功查询.

2.3 SM2环签名

范青等人[29]提出了基于SM2数字签名算法的环签名方案，允许用户代表由多个用户公钥组成的环公钥签署消息，并将签名者的真实身份隐藏在环公钥中. 方案满足匿名性和不可伪造性，包含初始化算法$Setup$、密钥生成算法$KeyGen$、环签名生成算法$RSign$和环签名验证算法$RVerify$.

1）$Setup(1^\lambda)\to pp$. 算法以安全参数λ为输入，输出公共参数$pp=\{p,F_p,E(F_p),\mathbb{G},q,G,H_{\text{v}}\}$，其中$H_{\text{v}}:\{0,1\}^*\to\mathbb{Z}_q^*$为SM3密码散列函数.

2）$KeyGen(pp)\to(PK,sk)$. 用户随机采样私钥$sk\in\mathbb{Z}_q^*$，计算公钥$PK=sk\times G$.

3）$RSign(pp,msg,n,R,sk_\tau)\to\sigma$. 签名者自主选择系统内$n-1$个公钥，结合自身公钥组成大小为$n$的环公钥$R=\{PK_1,PK_2,\cdots,PK_n\}$，其中第$\tau\in[n]$个公钥为签名者的公钥. 签名者使用环公钥$R$和私钥$sk_\tau$为消息$msg$签名.

① 随机采样$k_\tau\in\mathbb{Z}_q^*$，计算$c_{\tau+1}=H_{\text{v}}(R\|msg\|k_\tau\times G)$.

② 对于$i=\tau+1,\cdots,n,1,\cdots,\tau-1$，随机采样$s_i\in\mathbb{Z}_q^*$，计算$Z_i=s_i\times G+(s_i+c_i)\times PK_i$，$c_{i+1}=H_{\text{v}}(R\|msg\|Z_i)$.

③ 计算$s_\tau=(1+sk_\tau)^{-1}(k_\tau-c_\tau sk_\tau)$，并输出$\sigma=(c_1,s_1,\cdots,s_n)$.

4）$RVerify(pp,msg',R,\sigma')\to 0/1$. 给定消息$msg'$和$\sigma'=(c_1',s_1',\cdots,s_n')$，验证步骤为：

① 对于$i\in[n]$，计算$Z_i'=s_i'\times G+(s_i'+c_i')\times PK_i$和$c_{i+1}'=H_{\text{v}}(R\|msg'\|Z_i')$.

② 若$c_1'=c_{n+1}'$，算法输出1.否则，输出0.

本文提出一种基于SM2的集合成员关系证明方案，可以被视为SM2环签名在Pedersen向量承诺上的推广.

2.4 去中心化匿名凭证

Garman等人[7]提出了去中心化匿名凭证系统，该系统利用区块链网络和零知识证明技术，取代传统的单一权威中心来发行凭证. 具体而言，用户依赖于已有的公共身份断言（如包含公开身份和属性信息的TPM认证或AIK证书）在本地生成凭证，该凭证可视为对身份和属性的Pedersen承诺. 此外，用户还生成零知识证明π_C，以证明凭证中所包含的身份和属性与身份断言中的公开信息一致. 之后，用户将身份断言、凭证及证明π_C提交至区块链智能合约. 若身份断言和证明π_C均通过验证，智能合约会将凭证记录在链上，视为有效凭证. 完成凭证发行后，这些公共身份断言将不会被用于后续的凭证展示和验证，以避免隐私泄露.

为了以匿名的方式向服务提供商展示凭证，用户选择包含自身凭证的集合，并计算零知识证明π，证明该集合中的某个凭证包含满足访问策略的身份和属性，而不泄露具体是哪个凭证. 若集合中的凭证均为链上有效凭证，并且证明π通过验证，服务提供商将认定用户满足访问策略. 由于凭证的私钥仅为其持有者所知，用户只能为自己的凭证生成有效证明，无法冒用他人凭证.

去中心化匿名凭证包含初始化算法$Setup$、密钥

生成算法$KeyGen$、假名生成算法$NymGen$、凭证生成算法$MintCred$、凭证发行算法$MintVfy$、凭证展示算法$Show$和身份验证算法$ShowVfy$.

1) $Setup(1^{\lambda}) \to pp$. 此算法以安全参数$\lambda$为输入，输出系统参数$pp$.

2) $KeyGen(pp) \to sk_{\mathrm{U}}$. 此算法以系统参数$pp$为输入，输出用户密钥$sk_{\mathrm{U}}$.

3) $NymGen(pp, sk_{\mathrm{U}}) \to (nym, sk_{nym})$. 此算法以系统参数$pp$和用户密钥$sk_{\mathrm{U}}$为输入，输出假名$nym$和假名密钥$sk_{nym}$.

4) $MintCred(pp, \boldsymbol{v}, nym, aux, sk_{\mathrm{U}}, sk_{nym}) \to (C, sk_C, \pi_C)$. 此算法以系统参数$pp$、用户属性$\boldsymbol{v}$、假名$nym$、辅助信息$aux$、用户密钥$sk_{\mathrm{U}}$和假名密钥$sk_{nym}$为输入，输出凭证$C$、凭证密钥$sk_C$和凭证有效性证明$\pi_C$. 辅助信息$aux$为包含用户身份和属性的公共身份断言，如 TPM 认证或 AIK 证书.

5) $MintVfy(pp, \boldsymbol{v}, nym, C, aux, \pi_C) \to 0/1$. 此算法以系统参数$pp$、用户属性$\boldsymbol{v}$、假名$nym$、凭证$C$、辅助信息$aux$和证明$\pi_C$为输入. 若凭证有效，此算法输出 1. 否则，输出 0.

6) $Show(pp, R, \boldsymbol{v}, nym', sk_C, sk_{nym'}, sk_{\mathrm{U}}, \tau) \to \pi$. 以系统参数$pp$、凭证集合$R = \{C_1, C_2, \cdots, C_n\}$、用户属性$\boldsymbol{v}$、假名$nym'$、凭证密钥$sk_C$、假名密钥$sk_{nym'}$、用户密钥$sk_{\mathrm{U}}$和编号$\tau$为输入，其中$C_\tau = C$为证明者的凭证，此算法输出凭证证明$\pi$.

7) $ShowVfy(pp, R, \boldsymbol{v}, nym', \pi) \to 0/1$. 此算法以系统参数$pp$、凭证集合$R$、用户属性$\boldsymbol{v}$、假名$nym'$和凭证证明$\pi$为输入. 若凭证证明有效，此算法输出 1.否则，输出 0.

上述方案在凭证展示的过程中会披露凭证中包含的所有属性. 然而，实践中往往不需要用户公开其所有属性. 本文提出的 SM2 匿名凭证方案允许用户选择性地披露认证所需的属性，保护了用户隐私.

2.5 Schwartz-Zippel 引理

假设定义在有限域F上的总阶数为d的多项式$f(x_1, x_2, \cdots, x_n)$为非零多项式，S为F的有限子集，$|S|$为S中的元素数量，随机选取$r_1, r_2, \cdots, r_n \in S$，有

$$Pr\left[f(r_1, r_2, \cdots, r_n) = 0\right] \leqslant \frac{d}{|S|}.$$

3 系统模型

3.1 SM2 去中心化匿名凭证的语法

本文提出的方案的形式化定义基于 2.4 节介绍的去中心化匿名凭证方案，并对凭证展示算法$Show$和身份验证算法$ShowVfy$做出修改.

1) $Show(pp, R, \boldsymbol{v}, T, nym', sk_C, sk_{nym'}, sk_{\mathrm{U}}, \tau) \to \pi$. 此算法以系统参数$pp$、凭证集合$R$、用户属性$\boldsymbol{v}$、索引集合$T = \{(v'_1, I_1), (v'_2, I_2), \cdots, (v'_t, I_t)\}$、假名$nym'$、凭证密钥$sk_C$、假名密钥$sk_{nym'}$、用户密钥$sk_{\mathrm{U}}$和编号$\tau$为输入，其中用户凭证为集合$R$中的第$\tau$个凭证，且对于$\forall j \in [t]$，有$v[I_j] = v'_j$. 算法输出凭证证明$\pi$来展示自己持有集合$R$中的合法凭证，且属性$\boldsymbol{v}$满足索引集合$T$的描述.

2) $ShowVfy(pp, R, T, nym', \pi) \to 0/1$. 此算法以系统参数$pp$、凭证集合$R$、索引集合$T$、假名$nym'$和凭证证明$\pi$为输入. 若凭证证明有效，算法输出 1.否则，输出 0.

3.2 系统模型

如图 1 所示，SM2 去中心化匿名凭证系统包括 3 类实体：区块链、用户和验证者. 本文结合电子投票的应用场景，详细介绍匿名凭证的工作流程. 在该场景中，用户作为投票人，验证者作为计票人，且仅具备特定属性的用户才享有投票资格. 具体流程如下：

1) 系统初始化. 系统首先生成公共参数并将其记录上链，用户通过区块链获取这些公共参数. 由于系统初始化算法是公开透明的，这一过程无需任何可信中心的参与.

2) 凭证生成. 与中心化匿名凭证不同，用户无需直接向发行中心请求凭证，而是在本地生成个人凭证C，并输出证明π_C以确保凭证形式正确且包含一组公开的属性$\boldsymbol{v}$. 此外，用户需提供辅助信息aux，该信息为公共身份断言，用于证明用户确实具备属性$\boldsymbol{v}$. 最终，用户将凭证C、属性$\boldsymbol{v}$、证明π_C以及辅助信息aux提交给区块链上的智能合约.

3) 凭证发行. 智能合约负责验证用户凭证的有

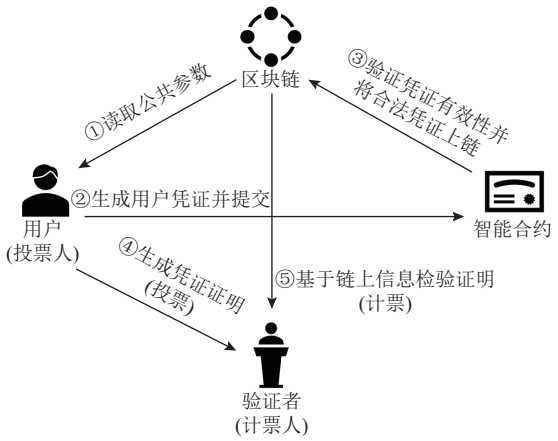


Fig. 1 System model

图 1 系统模型

效性. 若证明π_C和辅助信息aux均通过验证，智能合约确认凭证有效，并将其记录在区块链上. 步骤②和步骤③共同完成了用户凭证的发行. 此过程无需中心化的凭证发行机构参与，而是由用户在本地生成凭证并提交区块链智能合约进行验证. 公共身份断言和零知识证明技术确保用户本地生成的凭证中包含真实可信的身份和属性信息.

4）凭证展示. 为证明自身具备投票资格，用户从区块链上收集合法凭证，与自身凭证组成集合$R=\{C_1,C_2,\cdots,C_n\}$，其中$C_\tau=C\in R$且$\tau\in\{1,2,\cdots,n\}$. 基于该集合，用户生成凭证证明π以展示其持有集合中的某个合法凭证，且具备投票所需的属性. 最终，用户将投票信息与凭证证明π一并发送给验证者.

5）凭证检验. 验证者，即投票系统中的计票人，首先检索集合R中的凭证是否已记录在区块链上，然后验证凭证证明π的有效性. 若验证通过，则确认用户持有合法凭证且具备所披露的属性，并接受用户提交的投票信息. 否则，拒绝该凭证证明.

4 安全模型

安全的 SM2 去中心化匿名凭证方案需要满足完备性、匿名性和不可伪造性. 本文在图 2 中定义了安全实验来描述这些安全属性.

$Exp^{\text{anon}}_{\mathcal{A},n}(\lambda)$:
1: $pp\leftarrow Setup(1^\lambda)$, $\mathcal{L}$:=ø
2: $sk_{\text{U},i}\leftarrow KeyGen(pp)$ for $i\in[N]$
3: $(nym_i, sk_{nym_i})\leftarrow NymGen(pp, sk_{\text{U},i})$ for $i\in[N]$
4: $(C_i, sk_{c_i}, \pi_{C_i})\leftarrow MintCred(pp, \boldsymbol{v}_i, nym_i, aux_i, \text{sk}_{\text{U},i}, sk_{nym_i})$ for $i\in[N]$
5: $L=\{aux_i, nym_i, \boldsymbol{v}_i, C_i, \pi_{C_i}\}_{i\in[N]}$
6: $(R, T)\leftarrow\mathcal{A}^{O_{\text{Cred}}}(pp, L)$ s.t. $R=\{C_{i_1}, C_{i_2}, \ldots, C_{i_n}\}\wedge T=\{(v'_1, I_1), (v'_2, I_2), \ldots, (v'_t, I_t)\}\wedge Q=\{i_1, i_2, \ldots, i_n\}\subseteq[N]\wedge(\forall i\in Q, j\in[t], v_i[I_j]=v'_j)$
7: $\tau\xleftarrow{\$}Q$
8: $(nym'_\tau, sk_{nym'_\tau})\leftarrow NymGen(pp, sk_{\text{U},\tau})$
9: $\pi\leftarrow Show(pp, R, \boldsymbol{v}_\tau, T, nym'_\tau, sk_{C_\tau}, sk_{nym'_\tau}, sk_{\text{U},\tau}, \tau)$
10: $b\leftarrow\mathcal{A}^{O_{\text{Cred}}}(pp, R, n, L, nym'_\tau, \pi)$
11: return $b==\tau$

$Exp^{\text{ufg}}_{\mathcal{A}}(\lambda)$:
1: $pp\leftarrow Setup(1^\lambda)$, $\mathcal{L}$:=ø
2: $sk_{\text{U},i}\leftarrow KeyGen(pp)$ for $i\in[N]$
3: $(nym_i, sk_{nym_i})\leftarrow NymGen(pp, sk_{\text{U},i})$ for $i\in[N]$
4: $(C_i, sk_{c_i}, \pi_{C_i})\leftarrow MintCred(pp, \boldsymbol{v}_i, nym_i, aux_i, \text{sk}_{\text{U},i}, sk_{nym_i})$ for $i\in[N]$
5: $L=\{aux_i, nym_i, \boldsymbol{v}_i, C_i, \pi_{C_i}\}_{i\in[N]}$, $S=\{C_i\}_{i\in[N]}$
6: $(R, T, nym, \pi)\leftarrow\mathcal{A}^{O_{\text{Cred}}}(pp, L)$ s.t. $R\subseteq S$
7: if $ShowVfy(pp, R, T, nym, \pi)=1\wedge(R, nym, \pi)\notin\mathcal{L}$
8: then return 1 else return 0
$O_{\text{Cred}}(pp, R, i, T)$:
1: if $\exists j\in[t], v'_j\neq v_i[I_j]$retum 0
2: $(nym'_i, sk_{nym'_i})\leftarrow NymGen(pp, sk_{\text{U},i})$
3: $\pi\leftarrow Show(pp, R, \boldsymbol{v}_i, T, nym'_i, sk_{C_i}, sk_{nym'_i}, sk_{\text{U},i}, i)$
4: add(R, nym'_i, π) to $\mathcal{L}$ and return (nym_i, π)

Fig. 2 Security experiments for SM2-based decentralized anonymous credentials

图 2 基于 SM2 的去中心化匿名凭证的安全实验

1）完备性. 如果

$$Pr\left[\begin{array}{c} pp\leftarrow Setup(1^\lambda), sk_{\text{U}}\leftarrow KeyGen(pp),\\ (nym, sk_{nym})\leftarrow NymGen(pp, sk_{\text{U}}),\\ (nym', sk_{nym'})\leftarrow NymGen(pp, sk_{\text{U}}),\\ (C, sk_C, \pi_C)\leftarrow MintCred(pp, \boldsymbol{v}, nym, aux, sk_{\text{U}}, sk_{nym}),\\ T=\{(v'_1, I_1), (v'_2, I_2), \cdots, (v'_t, I_t)\}\wedge(\forall j\in[t], v[I_j]=v'_j),\\ \pi\leftarrow Show(pp, R, \boldsymbol{v}, T, nym', sk_C, sk_{nym'}, sk_{\text{U}}, \tau):\\ MintVfy(pp, \boldsymbol{v}, nym, C, aux, \pi_C)=1\wedge\\ ShowVfy(pp, R, T, nym', \pi)=1 \end{array}\right]\geqslant 1-negl(\lambda),$$

SM2 去中心化匿名凭证方案满足完备性.

2）匿名性. 此性质意味着除了用户主动披露的属性，凭证证明不会泄露和用户身份相关的其他任何信息. 对于任何 PPT 敌手和匿名集合大小n，如果

$$Adv^{\text{anon}}_{\mathcal{A},n}(\lambda)=\left|Exp^{\text{anon}}_{\mathcal{A},n}(\lambda)-n^{-1}\right|\leqslant negl(\lambda),$$

SM2 去中心化匿名凭证方案满足匿名性.

3）不可伪造性. 此性质意味着，如果集合中的凭证皆来自诚实用户，敌手无法以该凭证集合的名义生成任何有效的凭证证明. 对于任何 PPT 敌手，如果

$$Adv^{\text{ufg}}_{\mathcal{A}}(\lambda)=\left|Exp^{\text{ufg}}_{\mathcal{A}}(\lambda)\right|\leqslant negl(\lambda),$$

SM2 去中心化匿名凭证方案满足不可伪造性.

5 SM2 集合成员关系证明

本节介绍 SM2 集合成员关系证明方案Π_{MS}. 对于 Pedersen 向量承诺的集合，方案允许用户证明集合中某个承诺的打开值$\boldsymbol{x}$的知识. 此外，方案还允许用户公开值y，并保证y为向量$\boldsymbol{x}$的各个分量的线性组合，即$y=L(\boldsymbol{x})=\langle\boldsymbol{h},\boldsymbol{x}\rangle$，其中$\boldsymbol{h}=(h_1,h_2,\cdots,h_m)$为线性组合$L(\cdot)$的系数.

对于集合$R=\{C_1,C_2,\cdots,C_n\}$和值$y\in\mathbb{Z}_q$，此方案允许用户证明如下关系：

$$\mathcal{R}_{\text{MS}}=\left\{\begin{array}{c}\alpha=(R,y),\varpi=(\boldsymbol{x},\mu,\tau):\\ |\boldsymbol{x}|=|\boldsymbol{G}|=m\wedge 1\leqslant\tau\leqslant n\wedge\\ C_\tau=\boldsymbol{x}\cdot\boldsymbol{G}+\mu\times H\wedge y=L(\boldsymbol{x})\end{array}\right\}.$$

方案包含初始化算法$Setup$、证明算法$Prove$和验

证算法$Verify$.

1)初始化算法. 选取$\mathbb{G}$中的生成元$G_1,G_2,\cdots,G_m$, $H\in\mathbb{G}$, 选择哈希函数$H_{\mathrm{v}}:\{0,1\}^*\to\mathbb{Z}_q^*$, 并输出公共参考字符串$crs=\{G_1,G_2,\cdots,G_m,H,H_{\mathrm{v}}\}$.

2)证明算法. 给定集合$R=\{C_1,C_2,\cdots,C_n\}$和值$y=L(\boldsymbol{x})$, 其中$C_\tau=\boldsymbol{x}\cdot\boldsymbol{G}+\mu\times H$且$\tau\in[n]$, 证明者执行如下步骤生成$\alpha=(R,y)$和$\varpi=(\boldsymbol{x},\mu,\tau)$满足关系$\mathcal{R}_{\mathrm{MS}}$的证明$\pi$:

① 随机选取$\upsilon,k\in\mathbb{Z}_q^*$, 计算$CM=\boldsymbol{x}\cdot\boldsymbol{G}+\upsilon\times H$和$c_{\tau+1}=H_{\mathrm{v}}(R\|CM\|k\times H)$.

② 对于$i=\tau+1,\cdots,n,1,\cdots,\tau-1$, 随机选取$s_i\in\mathbb{Z}_q^*$, 计算$Z_i=s_i\times H+(s_i+c_i)\times(C_i-CM)$和$c_{i+1}=H_{\mathrm{v}}(R\|CM\|Z_i)$.

③ 计算$s_\tau=(1+\mu-\upsilon)^{-1}(k-c_\tau(\mu-\upsilon))$和$\pi_L\leftarrow\Pi_L.Prove(crs,(CM,y),(\boldsymbol{x},\upsilon))$.

④ 输出$\pi_{\mathrm{MS}}=(CM,c_1,s_1,\cdots,s_n,\pi_L)$.

3)验证算法. 对于陈述$\alpha=(R,y)$和证明$\pi_{\mathrm{MS}}=(CM,c_1,s_1,\cdots,s_n,\pi_L)$, 验证者执行如下步骤来判断陈述是否为真:

① 检查$c_1,s_1,\cdots,s_n\in\mathbb{Z}_q^*$和$CM\in\mathbb{G}$是否成立. 若成立, 执行下一步. 否则, 算法中断.

② 计算$b\leftarrow\Pi_L.Verify(crs,(CM,y),\pi_L)$. 若$b=1$, 执行下一步. 否则, 算法中断.

③ 对$i\in[n]$, 计算$Z_i=s_i\times H+(s_i+c_i)\times(C_i-CM)$和$c_{i+1}=H_{\mathrm{v}}(R\|CM\|Z_i)$.

④ 检查$c_1=c_{n+1}$是否成立. 若成立, 算法输出1.否则, 输出0.

定理 1. 在随机预言模型下, 如果NIZK方案Π_L满足完备性, 且2.3节介绍的SM2环签名满足正确性, 则SM2集合成员关系证明Π_{MS}是完备的.

证明. 显然$\Pi_{\mathrm{MS}}.Prove$算法可以视作使用私钥$\mu-\upsilon$以环公钥$\{C_1-CM,C_2-CM,\cdots,C_n-CM\}$的名义签署消息$msg=CM$, 再使用$\Pi_L.Prove$证明$CM=\boldsymbol{x}\cdot\boldsymbol{G}+\upsilon\times H$和$y=L(\boldsymbol{x})$为真. $\Pi_{\mathrm{MS}}.Verify$算法可以视作先验证环公钥$\{C_1-CM,C_2-CM,\cdots,C_n-CM\}$签署的消息$msg=CM$的有效性, 再检查$CM=\boldsymbol{x}\cdot\boldsymbol{G}+\upsilon\times H$和$y=L(\boldsymbol{x})$是否为真. 如果方案$\Pi_L$满足完备性, SM2环签名算法满足正确性, 且陈述$\alpha=(R,y)$和证据$\varpi=(\boldsymbol{x},\mu,\tau)$满足关系$\mathcal{R}_{\mathrm{MS}}$, $\Pi_{\mathrm{MS}}.Prove$算法输出的证明可以通过$\Pi_{\mathrm{MS}}.Verify$算法的验证. 证毕.

除了匿名凭证, 此协议还可应用于其他领域. 例如, 该协议可用于构建属性基签名系统, 实现灵活的基于属性的消息认证与隐私保护. 还可以被用来构造去中心化匿名支付系统, 保障支付过程中的可信与隐私安全.

1)属性基签名. 属性基签名是一种基于属性的密码学签名机制, 允许签名者基于自身属性对消息进行签名, 而无需暴露具体身份[30]. 在基于SM2集合成员关系证明构造属性基签名时, 可信中心通过发布对用户公钥和属性的承诺来授予属性. 用户可以收集多个承诺, 并证明其知晓某个承诺中公钥对应的私钥, 同时证明该承诺中隐藏的属性满足特定谓词f, 而不泄露其他任何信息. 由于SM2集合成员关系证明基于Sigma协议构造, 可利用Fiat-Shamir启发式将证明转换为非交互式签名. 签名者的承诺被混淆于集合中, 从而保持身份匿名性.

2)匿名支付. 去中心化匿名支付系统是一种基于分布式账本的支付方案, 旨在实现安全、高效且隐私保护的价值转移[23]. 在基于SM2集合成员关系证明构造匿名支付系统时, 用户首先在智能合约中锁定一部分数字货币, 并生成金额和秘密信息的承诺作为代币. 在支付过程中, 发送方收集一组代币, 并通过证明其知晓某个代币的秘密值来花费该代币, 同时生成属于接收方的新代币以完成价值转移. 为防止双重支付攻击, 支付时通常需要公开与代币唯一对应的序列号.

6 SM2去中心化匿名凭证

本节介绍一种基于SM2的去中心化匿名凭证方案, 该方案构建于SM2集合成员关系证明之上, 无需可信第三方颁发证书. 该方案适用于区块链和Web3网络等分布式应用场景, 支持用户在证明凭证合法性的同时, 根据需求选择性披露其属性, 有效避免过度隐私泄露. 基于SM2的去中心化匿名凭证方案包含系统初始化、用户密钥生成、假名生成、凭证生成、凭证发行、凭证展示和身份验证等算法.

1)系统初始化. 假设用户属性向量$\boldsymbol{v}$的长度为l, 执行SM2集合成员关系证明方案中的初始化算法$crs\leftarrow\Pi_{\mathrm{MS}}.Setup(1^\lambda,m)$来生成公共参考字符串, 其中$m=l+1$且$crs=\{G_1,G_2,\cdots,G_m,H,H_{\mathrm{v}}\}$. 最终, 算法输出公共参数$pp=(l,crs)$.

2)用户密钥生成. 用户$\mathcal{U}$随机采样$sk_{\mathrm{U}}\in\mathbb{Z}_q^*$作为用户密钥.

3)假名生成. 用户$\mathcal{U}$随机采样$sk_{nym}\in\mathbb{Z}_q^*$, 根据用户密钥$sk_{\mathrm{U}}$计算假名$nym=sk_{\mathrm{U}}\times G_m+sk_{nym}\times H$, 并输出假名$nym$和假名密钥$sk_{nym}$. 为了保护身份隐私, 用户每次执行凭证生成算法或凭证展示算法都需要生成新的假名.

4)凭证生成. 用户$\mathcal{U}$基于属性$\boldsymbol{v}=(v_1,v_2,\cdots,v_{m-1})$

生成匿名凭证，并使用知识签名签署辅助信息aux作为凭证的有效性证明. 此处的辅助信息aux为包含用户身份和属性的公共身份断言，如TPM认证和AIK证书等. 算法流程如下：

① 随机采样$sk_C \in \mathbb{Z}_q^*$作为凭证密钥，并计算凭证$C = \boldsymbol{x} \cdot \boldsymbol{G} + sk_C \times H$，其中$\boldsymbol{x} = (\boldsymbol{v}, sk_{\mathrm{U}})$.

② 使用$\varpi_{\mathrm{SoK}} = (sk_{\mathrm{U}}, sk_C, sk_{nym})$签署辅助信息$aux$，计算$\sigma \leftarrow \Pi_{\mathrm{SoK}}.Sign(crs, (C, nym, \boldsymbol{v}), (sk_{\mathrm{U}}, sk_C, sk_{nym}), aux)$.

③ 输出凭证C、凭证密钥sk_C和知识签名σ.

5）凭证发行. 接收到凭证C、假名nym、辅助信息aux和知识签名σ后，智能合约先验证辅助信息aux的有效性，并从中获取用户属性$\boldsymbol{v}$，再执行算法$b \leftarrow \Pi_{\mathrm{SoK}}.Verify(crs, (C, nym, \boldsymbol{v}), \sigma, aux)$. 若$b = 1$，凭证有效. 否则，凭证无效. 智能合约将有效的凭证记录上链.

6）凭证展示. 给定索引集合

$$T = \{(v'_1, I_1), (v'_2, I_2), \cdots, (v'_t, I_t)\},$$

假名

$$nym' = sk_{\mathrm{U}} \times G_m + sk_{nym'} \times H$$

和凭证

$$C = \boldsymbol{x} \cdot \boldsymbol{G} + sk_C \times H$$

满足$\boldsymbol{x} = (\boldsymbol{v}, sk_{\mathrm{U}})$，且对于$\forall j \in [t]$，有$v'_j = v[I_j]$，用户$\mathcal{U}$执行如下步骤生成凭证证明：

① 选取$n-1$个凭证，与$\mathcal{U}$的凭证C组成集合$R = \{C_1, C_2, \cdots, C_n\}$，其中$C_\tau = C$且$\tau \in [n]$.

② 对于$i \in [m] \backslash \{I_1, I_2, \cdots, I_t\}$，设置$h_i = 0$；对$i \in \{I_1, I_2, \cdots, I_t\}$，计算$h_i = H_{\mathrm{v}}(R \| i \| v[i] \| nym')$；设置$\boldsymbol{h} = (h_1, h_2, \cdots, h_m)$作为线性组合$L(\cdot)$的系数.

③ 计算$y = L(\boldsymbol{x}) = \langle \boldsymbol{h}, \boldsymbol{x} \rangle$和集合成员关系证明$\pi_{\mathrm{MS}} \leftarrow \Pi_{\mathrm{MS}}.Prove(crs, (R, y), (\boldsymbol{x}, sk_C, \tau))$，其中$\pi_{\mathrm{MS}} = (CM, c_1, s_1, \cdots, s_n, \pi_L)$，$CM = \boldsymbol{x} \cdot \boldsymbol{G} + \upsilon \times H$.

④ 证明假名有效性$\pi_{nym'} \leftarrow \Pi_{\mathrm{ZKP}}.Prove(crs, (CM, nym'), (\boldsymbol{v}, sk_{\mathrm{U}}, \upsilon, sk_{nym'}))$.

⑤ 输出凭证证明$\pi = (\pi_{\mathrm{MS}}, \pi_{nym'})$.

7）身份验证. 一旦收到凭证集合R、假名nym'和凭证证明$\pi = (\pi_{\mathrm{MS}}, \pi_{nym'})$，验证者执行如下步骤检查证明者是否持有集合$R$中的凭证，以及其属性是否符合索引集合$T$的描述：

① 检查集合R中的凭证是否都有效. 若存在无效凭证，算法输出0.否则，执行下一步.

② 计算$y' = \sum_{j \in [t]} v'_j \times H_{\mathrm{v}}(R \| I_j \| v'_j \| nym')$和$b_1 \leftarrow \Pi_{\mathrm{MS}}.Verify(crs, (R, y'), \pi_{\mathrm{MS}})$. 若$b_1 = 1$，$\pi_{\mathrm{MS}}$有效并执行下一步. 否则，算法输出0.

③ 将π_{MS}拆分为$(CM, c_1, s_1, \cdots, s_n, \pi_L)$，并计算$b_2 \leftarrow \Pi_{\mathrm{ZKP}}.Verify(crs, (CM, nym'), \pi_{nym'})$. 若$b_2 = 1$，算法输出1.否则，输出0.

定理2. 如果SM2集合成员关系证明Π_{MS}和零知识证明Π_{ZKP}满足完备性，且知识签名Π_{SoK}满足正确性，则SM2去中心化匿名凭证方案满足完备性.

证明. 1）给定假名$nym = sk_{\mathrm{U}} \times G_m + sk_{nym} \times H$和匿名凭证$C = sk_{\mathrm{U}} \times G_m + sk_C \times H + \sum_{j \in [l]} v_i \times G_i$，知识签名$\Pi_{\mathrm{SoK}}$的正确性确保凭证生成算法$MintCred$输出的知识签名$\sigma$可以通过凭证发行算法$MintVfy$的验证.

2）凭证展示算法$Show$首先根据索引集合T、假名nym'、凭证集合R和用户属性$\boldsymbol{v}$计算出$y = \sum_{j \in [t]} \times v[I_j] \times H_{\mathrm{v}}(R \| I_j \| v'_j \| nym')$. 如果凭证$C$和假名$nym'$中包含相同的用户密钥$sk_{\mathrm{U}}$，且$C$中的属性$\boldsymbol{v}$满足索引集合$T$的描述，算法$Show$输出证明$\pi = (\pi_{\mathrm{MS}}, \pi_{nym'})$. 算法$ShowVfy$基于$(T, nym', R)$计算$y' = \sum_{j \in [t]} v'_j \times H_{\mathrm{v}}(R \| I_j \| v'_j \| nym')$. 由于属性$\boldsymbol{v}$满足索引集合$T$的描述，即：对于$\forall j \in [t]$，$v[I_j] = v'_j$成立，显然有$y' = y$. 协议$\Pi_{\mathrm{MS}}$的完备性确保$\Pi_{\mathrm{MS}}.Verify(crs, (R, y'), \pi_{\mathrm{MS}}) = 1$，$\Pi_{\mathrm{ZKP}}$的完备性确保$\Pi_{\mathrm{ZKP}}.Verify(crs, (CM, nym'), \pi_{nym'}) = 1$. 因此，由凭证展示算法$Show$输出的证明$\pi$可以通过身份验证算法$ShowVfy$的检查.

3）记$r_j = H_{\mathrm{v}}(R \| I_j \| v'_j \| nym')$，其可以被视为有限域$\mathbb{Z}_q$上的随机数. y和y'可以被视为2个t元一阶多项式f和f'在随机点$(r_1, r_2, \cdots, r_t) \in \mathbb{Z}_q^t$的取值，其中$(v[I_1], v[I_2], \cdots, v[I_t])$和$(v'_1, v'_2, \cdots, v'_t)$分别为2个多项式的系数，即：

$$y = f(r_1, r_2, \cdots, r_t) = \sum_{j \in [t]} v[I_j] \times r_j,$$

$$y' = f'(r_1, r_2, \cdots, r_t) = \sum_{j \in [t]} v'_j \times r_j.$$

若存在$j \in [t]$使得$v'_j \neq v[I_j]$，根据Schwartz-Zippel引理，$y' = y$的概率不超过$q^{-1}t$. 因此，如果$y' = y$，验证者可以相信对于任何$j \in [t]$，有$v'_j = v[I_j]$.

综上所述，SM2去中心化匿名凭证方案满足完备性. 证毕.

7 安全分析

7.1 集合成员关系证明的安全性分析

定理3. 可靠性. 在随机预言机模型下，若NIZK方案Π_L是可靠的，本文提出的SM2集合成员关系证明满足可靠性.

证明. 对于任何PPT敌手$\mathcal{A}$输出的陈述α和有效

证明π_{MS}, 存在 PPT 提取器算法$\mathcal{E}_{\mathrm{MS}}$, 可以从$\pi_{\mathrm{MS}}$中提取出证据$\varpi$, 且$(\alpha,\varpi)\notin\mathcal{R}_{\mathrm{MS}}$的概率是可忽略的.

挑战者$\mathcal{B}$控制预言机$O_{H_{\mathrm{v}}}$, 敌手$\mathcal{A}$可以向$O_{H_{\mathrm{v}}}$请求$(R\|CM\|Z_i)_{i\in[n]}$的哈希值. 若$\mathcal{A}$输出关于陈述$\alpha=(R,y)$的证明$\pi_{\mathrm{MS}}=(CM,c_1,s_1,\cdots,s_n,\pi_L)$, 且满足$\Pi_{\mathrm{MS}}.Verify(crs,(R,y),\pi_{\mathrm{MS}})=1$, 挑战者$\mathcal{B}$对敌手$\mathcal{A}$的操作进行倒带(rewind), 敌手$\mathcal{A}$再次为$\alpha=(R,y)$输出有效的证明$\pi'_{\mathrm{MS}}=(CM',c'_1,s'_1,\cdots,s'_n,\pi'_L)$. 由于 2 次生成证明使用的随机数$k$和$\upsilon$是相同的, 有$Z_\tau=Z'_\tau=k\times H$和$CM=CM'=\boldsymbol{x}\cdot\boldsymbol{G}+\upsilon\times H$. 但敌手$\mathcal{A}$向预言机$O_{H_{\mathrm{v}}}$为$(R\|CM\|Z_\tau)$和$(R\|CM'\|Z'_\tau)$请求哈希值时, 会返回$c_{\tau+1}\neq c'_{\tau+1}$. 由于对所有$i\in[n]\backslash\{\tau\}$, s_i和s'_i是随机选取的, 有$s_i\neq s'_i$. 进一步, 有$s_\tau\neq s'_\tau$和$c_\tau\neq c'_\tau$. 对于如下等式:

$$Z_\tau=s_\tau\times H+(s_\tau+c_\tau)\times(C_\tau-CM),$$
$$Z'_\tau=s'_\tau\times H+(s'_\tau+c'_\tau)\times(C_\tau-CM),$$

我们可以得到$\mu-\upsilon=(s_\tau-s'_\tau)\times(s'_\tau-s_\tau+c'_\tau-c_\tau)^{-1}$且$C_\tau-CM=(\mu-\upsilon)\times H$. 此外, 根据 NIZK 方案$\Pi_L$的可靠性, 存在 PPT 算法$\mathcal{E}_L$, 可以从$((CM,y),\pi_L)$中提取出证据$(\boldsymbol{x},\upsilon)$, 且$CM\neq\boldsymbol{x}\cdot\boldsymbol{G}+\upsilon\times H\vee y\neq L(\boldsymbol{x})$的概率是可忽略的.

综上所述, 存在概率多项式时间算法$\mathcal{E}_{\mathrm{MS}}$, 可以从有效证明中提取出$(\boldsymbol{x},\mu,\tau)$, 且$y\neq L(\boldsymbol{x})\vee\ C_\tau\neq\boldsymbol{x}\cdot\boldsymbol{G}+\mu\times H$的概率是可忽略的. 因此, SM2 集合成员关系证明满足可靠性. 证毕.

定理 4. 零知识性. 若 NIZK 方案Π_L是零知识的, 本文的 SM2 集合成员关系证明满足零知识性.

证明. 假设挑战者$\mathcal{B}$在初始化阶段随公共参考字符串crs一同生成陷门$\hbar$. 为生成陈述$\alpha=(R,y)$的模拟证明$\pi_{\mathrm{sim}}=(CM',c'_1,s'_1,\cdots,s'_n,\pi'_L)$, 模拟器$\mathcal{S}_{\mathrm{MS}}$执行如下步骤:

1)随机选取$\delta,k'\in\mathbb{Z}_q^*$, $\eta\in[n]$, 计算$CM'=C_\eta-\delta\times H$及$c'_{\eta+1}=H_{\mathrm{v}}(R\|CM'\|k'\times H)$.

2)对于$i=\eta+1,\cdots,n,1,\cdots,\eta-1$, 随机采样$s'_i\in\mathbb{Z}_q^*$, 计算$Z'_i=s'_i\times H+(s'_i+c'_i)\times(C_i-CM')$和$c'_{i+1}=H_{\mathrm{v}}(R\|CM'\|Z'_i)$.

3)计算$s'_\eta=(1+\delta)^{-1}(k'-\delta c'_\eta)$, 并基于陷门$\hbar$调用$\Pi_L$的模拟器$\mathcal{S}_L$为$(CM',y)$生成证明$\pi'_L$.

4)输出$\pi_{\mathrm{sim}}=(CM',c'_1,s'_1,\cdots,s'_n,\pi'_L)$.

显然, 模拟证明π_{sim}可以通过$\Pi_{\mathrm{MS}}.Verify$的验证. 根据 Pedersen 承诺的隐藏性, CM'和CM是不可区分的. 根据 NIZK 方案Π_L的零知识性, π'_L和π_L是不可区分的. 根据 SM2 环签名的完全匿名性, $(c'_1,s'_1,\cdots,s'_n)$和$(c_1,s_1,\cdots,s_n)$是统计不可区分的. 因此, SM2 集合成员关系证明满足零知识性. 证毕.

7.2 去中心化匿名凭证的安全性分析

定理 5. 不可伪造性. 若 SM2 集合成员关系证明是可靠的, SM2 去中心化匿名凭证方案满足不可伪造性.

证明. 如果 PPT 敌手$\mathcal{A}$可以攻破 SM2 去中心化匿名凭证方案的不可伪造性, 挑战者$\mathcal{B}$可以利用$\mathcal{A}$解决椭圆曲线离散对数问题

$$ECDLP=\{(B,P):B=\beta\times P,\beta\in\mathbb{Z}_q^*,P\in\mathbb{G}\}.$$

在初始化阶段, 挑战者$\mathcal{B}$生成陷门$\hbar$和公共参考字符串$crs=\{G_1,G_2,\cdots,G_m,H,H_{\mathrm{v}}\}$, 其中$G_m=P$. 对于$\forall i\in[N]$, 公共身份断言$aux_i$中包含属性$\boldsymbol{v}_i=(v_{i,1},v_{i,2},\cdots,v_{i,l})$, $\mathcal{B}$计算

$$nym_i=B+sk_{nym_i}\times H,$$
$$C_i=B+sk_{C_i}\times H+\sum_{j\in[l]}v_{i,j}\times G_j,$$

其中$sk_{\mathrm{U},i}=\beta$. 随后, 根据关系$\mathcal{R}_{\mathrm{SoK}}$的 SoK 协议的可模拟性, $\mathcal{B}$可以利用模拟器和陷门$\hbar$在没有$sk_{\mathrm{U},i}$的情况下为(nym_i,C_i)生成凭证的有效性证明, 即知识签名σ'_i, 其和算法$MintCred$输出的知识签名是不可区分的. $\mathcal{B}$将$(nym_i,C_i,\sigma'_i,aux_i)_{i\in[N]}$提交给智能合约. 通过验证后, $(nym_i,C_i,\sigma'_i)_{i\in[N]}$被记录上链.

随后, $\mathcal{A}$输出凭证集合$R=\{C_{i_1},C_{i_2},\cdots,C_{i_n}\}$、索引集合$T$、假名$nym$和凭证证明$\pi$, 其中$Q=\{i_1,i_2,\cdots,i_n\}\subseteq[N]$, 并将$(R,T,nym,\pi)$发送给挑战者$\mathcal{B}$. 对满足$ShowVfy(pp,R,T,nym,\pi)=1$的有效证明, 考虑到 NIZK 方案$\Pi_{\mathrm{MS}}$的可靠性, 存在 PPT 提取器算法$\mathcal{E}_{\mathrm{MS}}$可以从证明$\pi$中提取出$sk_{\mathrm{U},j}=\beta$且$j\in Q$.

综上所述, $\mathcal{B}$利用提取器$\mathcal{E}_{\mathrm{MS}}$和敌手$\mathcal{A}$解决了 ECDLP 问题. 若解决 ECDLP 问题的概率为ε, 敌手$\mathcal{A}$成功伪造凭证证明的概率为$\varepsilon_{\mathrm{ufg}}\leqslant\varepsilon$. 因此, SM2 去中心化匿名凭证方案满足不可伪造性. 证毕.

定理 6. 匿名性. 若 SM2 集合成员关系证明是零知识的, SM2 去中心化匿名凭证方案满足匿名性.

证明. 我们设计了 2 个安全游戏$\mathcal{G}_{\mathrm{real}}$和$\mathcal{G}_{\mathrm{sim}}$来分析凭证证明的匿名性.

安全游戏$\mathcal{G}_{\mathrm{real}}$如同在现实世界中执行安全实验$Exp^{\mathrm{anon}}_{\mathcal{A},n}(\lambda)$. 对于所有$i\in[N]$, $\mathcal{B}$知道公共身份断言aux_i, 其中包含属性$\boldsymbol{v}_i=(v_{i,1},v_{i,2},\cdots,v_{i,l})$. 为了初始化安全实验, 对$i\in[N]$, 挑战者$\mathcal{B}$计算

$$KeyGen(pp)\rightarrow sk_{\mathrm{U},i},$$
$$NymGen(pp,sk_{\mathrm{U},i})\rightarrow(nym_i,sk_{nym_i}),$$
$$MintCred(pp,\boldsymbol{v}_i,nym_i,aux_i,sk_{\mathrm{U},i},sk_{nym_i})\rightarrow(C_i,sk_{C_i},\sigma_i),$$

并将$(nym_i,C_i,\sigma_i,aux_i)_{i\in[N]}$提交给智能合约. 通过验证

后，$(nym_i, C_i, \sigma_i)_{i\in[N]}$被记录上链. 敌手$\mathcal{A}$发送$(R,T)$给挑战者$\mathcal{B}$，其中$R=\{C_{i_1}, C_{i_2}, \cdots, C_{i_n}\}$且$Q=\{i_1, i_2, \cdots, i_n\}\subseteq[N]$. R中的凭证皆满足索引集合T. $\mathcal{A}$无权访问用户密钥和凭证密钥$\{sk_{\mathrm{U},i}, sk_{C_i}\}_{i\in Q}$. $\mathcal{B}$随机选择$C_\tau\in R$，为其生成新的假名$nym'=sk_{\mathrm{U},\tau}\times G_m+sk_{nym'}\times H$，其中假名密钥为$sk_{nym'}$. 随后，$\mathcal{B}$执行算法

$$Show(pp, R, \boldsymbol{v}_\tau, T, nym', sk_{C_\tau}, sk_{nym'}, sk_{\mathrm{U},\tau}, \tau)$$

来计算$\pi=(\pi_{\mathrm{MS}}, \pi_{nym'})$，其中$\pi_{\mathrm{MS}}$根据 SM2 集合成员关系证明生成，$\pi_{nym'}$根据 NIZK 方案$\Pi_{\mathrm{ZKP}}$生成. 最后，敌手$\mathcal{A}$根据挑战者输出的假名$nym'$和凭证证明$\pi$判断证明由集合$R$中哪一个凭证的私钥生成.

安全游戏$\mathcal{G}_{\mathrm{sim}}$和安全游戏$\mathcal{G}_{\mathrm{real}}$类似，区别在于挑战者$\mathcal{B}$不使用$C_\tau$的用户密钥$sk_{\mathrm{U},\tau}$和凭证密钥$sk_{C_\tau}$来计算凭证证明. 取而代之的，$\mathcal{B}$使用 SM2 集合成员关系证明和 NIZK 方案$\Pi_{\mathrm{ZKP}}$中的模拟器$\mathcal{S}_{\mathrm{MS}}$和$\mathcal{S}_{\mathrm{ZKP}}$生成有效的凭证证明. 具体而言，挑战者$\mathcal{B}$首先在系统初始化阶段随公共参考字符串一同生成陷门$\hbar$，再基于索引集合$T$计算属性向量$\boldsymbol{v}$的各个分量的线性组合$y$，并根据 SM2 集合成员关系证明的零知识性，利用模拟器$\mathcal{S}_{\mathrm{MS}}$和陷门$\hbar$在没有证据$(\boldsymbol{v}_\tau, sk_{\mathrm{U},\tau}, sk_{C_\tau}, \tau)$的情况下为陈述$(R,y)$生成有效的证明$\pi'_{\mathrm{MS}}=(CM', c'_1, s'_1, \cdots, s'_n, \pi'_L)$. 随后，挑战者$\mathcal{B}$随机采样$nym''\in\mathbb{G}$，再根据 NIZK 方案$\Pi_{\mathrm{ZKP}}$的零知识性，利用模拟器$\mathcal{S}_{\mathrm{ZKP}}$和陷门$\hbar$在没有证据$(sk_{\mathrm{U},\tau}, sk_{nym''})$的情况下为陈述$(CM', nym'')$生成有效的证明$\pi_{nym''}$. 最终，挑战者$\mathcal{B}$输出$nym''$和$\pi_{\mathrm{sim}}=(\pi'_{\mathrm{MS}}, \pi_{nym''})$. 根据 SM2 集合成员关系证明和 NIZK 方案Π_{ZKP}的零知识性，$\pi=(\pi_{\mathrm{MS}}, \pi_{nym'})$和$\pi_{\mathrm{sim}}=(\pi'_{\mathrm{MS}}, \pi_{nym''})$的分布是不可区分的. 根据 Pedersen 承诺的安全性，nym'和nym''的分布是不可区分的. 故敌手$\mathcal{A}$区分安全游戏$\mathcal{G}_{\mathrm{sim}}$和$\mathcal{G}_{\mathrm{real}}$的概率是可忽略的.

由于挑战者$\mathcal{B}$在使用模拟器计算凭证证明π_{sim}时，没有使用到和用户身份相关的任何隐私信息，敌手$\mathcal{A}$输出$b=\tau$的概率为n^{-1}. 因此，在$\mathcal{G}_{\mathrm{real}}$中敌手$\mathcal{A}$输出$b=\tau$的概率为$n^{-1}\pm negl(\lambda)$. SM2 集合成员关系证明满足不可区分性. 证毕.

8 性能评估

8.1 理论分析

本节对本文提出的 SM2 集合成员关系证明的算法*Prove*和*Verify*，以及 SM2 去中心化匿名凭证方案的算法*Show*和*ShowVfy*进行计算开销和通信开销的理论分析，结果如表 1 所示. 在理论分析中，我们仅考虑 SM2 椭圆曲线上计算开销较大的点积运算T_{mul}和点加运算T_{add}. 当匿名集合大小为 11，属性数量为 10 时，凭证展示的计算开销为$59T_{\mathrm{mul}}+54T_{\mathrm{add}}$，身份验证的计算开销为$51T_{\mathrm{mul}}+48T_{\mathrm{add}}$.

Table 1 Computation and Communication Costs of the Proposed Schemes

表 1 本文方案的计算和通信开销

分析对象	集合成员关系证明	去中心化匿名凭证
证明生成/凭证展示	$(2m+2n+1)T_{\mathrm{mul}}+(2m+2n-2)T_{\mathrm{add}}$	$(2n+3l+7)T_{\mathrm{mul}}+(2n+3l+2)T_{\mathrm{add}}$
验证开销	$(2n+m+2)T_{\mathrm{mul}}+(2n+m+1)T_{\mathrm{add}}$	$(2n+2l+9)T_{\mathrm{mul}}+(2n+2l+6)T_{\mathrm{add}}$
通信开销	$2\lvert\mathbb{G}\rvert+(m+n+3)\lvert\mathbb{Z}_q\rvert$	$4\lvert\mathbb{G}\rvert+(n+2l+7)\lvert\mathbb{Z}_q\rvert$

注：m表示向量长度，l表示属性数量，n表示集合大小.

此外，对于双线性映射$e:\mathbb{G}^*\times\mathbb{G}^*\to\mathbb{G}_T$，我们使用$T'_{\mathrm{mul}}$表示群$\mathbb{G}^*$中的点积运算，$T_{\mathrm{pair}}$表示配对运算，$T_{\mathrm{exp}}$表示群$\mathbb{G}_T$中的幂运算. 文献 [6] 中方案的凭证展示和身份验证操作的计算开销分别为$11T'_{\mathrm{mul}}+5T_{\mathrm{pair}}+2T_{\mathrm{exp}}$和$8T'_{\mathrm{mul}}+8T_{\mathrm{pair}}+4T_{\mathrm{exp}}$. 本文方案与文献 [5−6] 相比，无需中心化的凭证发行机构，且在凭证展示和身份验证阶段无需昂贵的配对操作，优化了计算开销.

8.2 实验分析

本节对 SM2 去中心化匿名凭证方案和 SM2 集合成员关系证明进行计算开销测试. 本文在具有 8-core Intel® Core™ i5-10210U CPU, 4 GB RAM 和 Ubuntu 20.04 LTS 操作系统的本地设备上进行测试，并使用符合 SM2 国家商用密码标准的椭圆曲线和编程语言 Golang 实现程序代码. 在实验中，若无特别说明，属性数量设置为 10，匿名集合的大小设置为 11，与门罗币底层环签名的环公钥大小保持一致.

图 3 展示了在不同的集合大小下，SM2 集合成员关系证明方案中算法*Prove*和*Verify*的计算开销. 显然，证明生成和验证的计算开销都和集合大小成线性关系. 当集合大小为 11 时，证明时间为 3.71 ms，验证时间为 2.95 ms.

图 4 展示了去中心化匿名凭证方案中凭证生成（*MintCred*）、凭证展示（*Show*）及身份验证（*ShowVfy*）的计算开销均与属性数量呈线性关系. 当属性数量为 10 时，上述算法的计算时间分别为 1.38 ms, 5.13 ms, 4.42 ms.

图 5 对比了本文方案和文献 [6] 方案，展现了本文方案在计算性能上的优势. 本文方案中，*Show* 及 *ShowVfy* 的计算开销与凭证证明的数量呈线性关系. 此外，当属性数量为 10 且匿名集合大小为 11 时，本

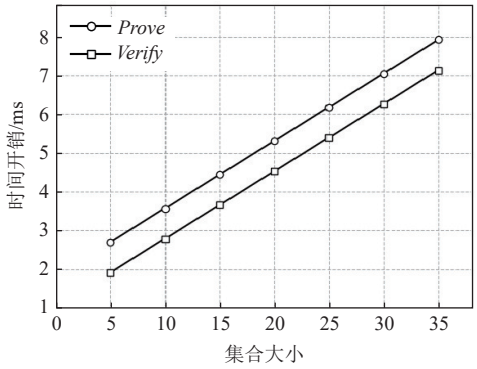


Fig. 3 Computation cost of SM2-based set membership proof

图 3 SM2 集合成员关系证明计算开销

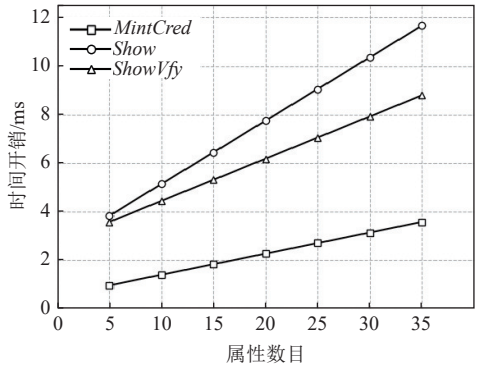


Fig. 4 Computation cost of SM2-based decentralized anonymous credential

图 4 SM2 去中心化匿名凭证的计算开销

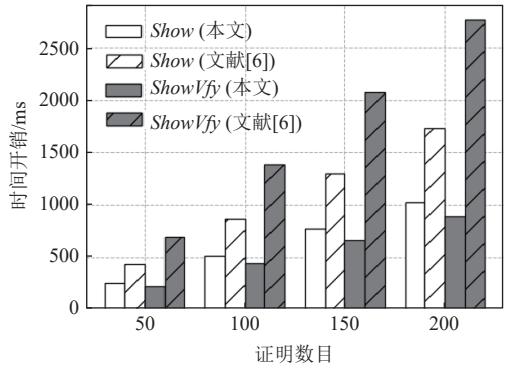


Fig. 5 Comparison between our scheme and relevant literatures

图 5 本文方案与相关文献的对比

文方案中凭证展示和身份验证的开销显著优于文献 [6] 方案.

9 总 结

本文提出了基于 SM2 的集合成员关系证明和去中心化匿名凭证方案, 对本领域的研究进行了有益的补充. 本文利用 Sigma 协议和 SM2 环签名技术设计了基于 SM2 的集合成员关系证明方案, 并基于此方案构造了去中心化的匿名凭证方案, 和现有的国密匿名凭证方案相比, 本文提出的方案不依赖于任何中心化的凭证发行中心, 避免了单点故障导致的系统瘫痪和隐私泄露. 本文方案还允许用户在展示凭证时根据需要选择性地披露属性, 实现了细粒度的隐私保护. 随着 Web3 网络的发展, 如何实现 Web3 网络间基于分布式身份的多因素身份认证, 值得进一步研究, 是我们未来的研究目标.

作者贡献声明: 赵陆天禹提出了算法思路和实验方案, 完成实验并撰写论文; 王化群提出指导意见并修改论文.

参 考 文 献

[1] Jia Jinping, Xiao Shihan, Qian Kun, et al. Survey of risk perception technology for Web 3.0 digital economic[J]. Journal of Computer Research and Development, 2024, 61(12): 3005−3026 (in Chinese)
(贾金萍, 肖诗涵, 钱堃, 等. Web 3.0 数字经济风险感知技术综述[J]. 计算机研究与发展, 2024, 61(12): 3005−3026)

[2] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps[C]//Proc of the 24th Annual Int Cryptology Conf. Berlin: Springer, 2004: 56−72

[3] State Cryptography Administration. GM/T 0044.2—2016 Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves—Part 2: Digital Signature Algorithm[S]. Beijing: Standards Press of China, 2016 (in Chinese)
(国家密码管理局. GM/T 0044.2−2016 SM9 标识密码算法第 2 部分: 数字签名算法[S]. 北京: 中国标准出版社, 2016)

[4] Baldimtsi F, Lysyanskaya A. Anonymous credentials light[C]//Proc of the 2013 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2013: 1087−1098

[5] Zhao Yanqi, Yang Xiaoyi, Feng Qi, et al. Anonymous credential protocol based on SM2 digital signature[J]. Journal of Software, 2024, 35(7): 3469−3481 (in Chinese)
(赵艳琦, 杨晓艺, 冯琦, 等. 基于 SM2 数字签名的匿名凭证协议[J]. 软件学报, 2024, 35(7): 3469−3481)

[6] Yu Yong, Zhao Yanqi, Li Yannan, et al. Blockchain-based anonymous authentication with selective revocation for smart industrial applications[J]. IEEE Transactions on Industrial Informatics, 2019, 16(5): 3290−3300

[7] Garman C, Green M, Miers I. Decentralized anonymous credentials[C/OL]//Proc of the 21st Annual Network and Distributed System Security Symp. Reston, VA: The Internet Society, 2014[2024-09-18]. https://www.ndss-symposium.org/ndss2014/

[8] Yang Rupeng, Au M H, Xu Qiuliang, et al. Decentralized blacklistable anonymous credentials with reputation[J]. Computers & Security, 2019, 85: 353−371

[9] Sonnino A, Al-Bassam M, Bano S, et al. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers[C/OL]//Proc of the 26th Annual Network and Distributed System Security Symp. Reston, VA: The Internet Society, 2019[2024-12-23]. https://www.ndss-symposium.org/ndss2019/

[10] Doerner J, Kondi Y, Lee E, et al. Threshold BBS+ signatures for distributed anonymous credential issuance[C]//Proc of the 44th IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2023: 773−789

[11] Mir O, Slamanig D, Mayrhofer R. Threshold delegatable anonymous credentials with controlled and fine-grained delegation[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 21(4): 2312−2326

[12] Mir O, Bauer B, Griffy S, et al. Aggregate signatures with versatile randomization and issuer-hiding multi-authority anonymous credentials[C]//Proc of the 2023 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2023: 30−44

[13] Camenisch J, Chaabouni R, Shelat A. Efficient protocols for set membership and range proofs[C]//Proc of the 14th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2008: 234−252

[14] Bayer S, Groth J. Zero-knowledge argument for polynomial evaluation with application to blacklists[C]//Proc of the 32nd Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2013: 646−663

[15] Groth J, Kohlweiss M. One-out-of-many proofs: Or how to leak a secret and spend a coin[C]//Proc of the 34th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 253−280

[16] Diamond B E. Many-out-of-many proofs and applications to anonymous Zether[C]//Proc of the 42nd IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2021: 1800−1817

[17] Zeng Gongxian, Lai Junzuo, Huang Zhengan, et al. Non-interactive zero-knowledge functional proofs[C]//Proc of the 29th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2023: 236−268

[18] Lin Chao, Huang Xinyi, He Debiao. Efficient range proof protocols based on Chinese cryptographic SM2[J]. Chinese Journal of Computers, 2022, 45(1): 148−159 (in Chinese)
(林超, 黄欣沂, 何德彪. 基于国密 SM2 的高效范围证明协议[J]. 计算机学报, 2022, 45(1): 148−159)

[19] Li Lin, Zhang Xuxia. National secret substitution of zk-SNARK bilinear pair[J]. Netinfo Security, 2019(10): 10−15 (in Chinese)
(黎琳, 张旭霞. zk-SNARK 的双线性对的国密化方案[J]. 信息网络安全, 2019(10): 10−15)

[20] Lai Qiqi, Chen Chongshen, Liu Fenghao, et al. Lattice-based commit-transferrable signatures and applications to anonymous credentials [J/OL]. 2023[2024-12-23]. https://eprint.iacr.org/2023/766

[21] Mundhe P, Yadav V K, Verma S, et al. Efficient lattice-based ring signature for message authentication in VANETs[J]. IEEE Systems Journal, 2020, 14(4): 5463−5474

[22] Fujisaki E, Suzuki K. Traceable ring signature[C]//Proc of the 10th Int Conf on Practice and Theory in Public-Key Cryptography. Berlin: Springer, 2007: 181−200

[23] Sun Shifeng, Au M H, Liu J K, et al. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero[C]//Proc of the 22nd European Symp on Research in Computer Security. Berlin: Springer, 2017: 456−474

[24] Qin Ningyuan, Fu Anmin, Chen Shouguo. Blind signature-based handover authentication protocol with contional privacy preserving in LTE/LTE-A netwroks[J]. Computer Science, 2015, 42(8): 145−151 (in Chinese)
(秦宁元, 付安民, 陈守国. LTE/LTE-A 网络中基于盲签名的具有条件隐私保护的切换认证协议[J]. 计算机科学, 2015, 42(8): 145−151)

[25] Hanzlik L. Non-interactive blind signatures for random messages[C]// Proc of the 42nd Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2023: 722−752

[26] Chase M, Lysyanskaya A. On signatures of knowledge[C]//Proc of the 26th Annual Int Cryptology Conf. Berlin: Springer, 2006: 78−96

[27] Canetti R, Chen Yilei, Holmgren J, et al. Fiat-Shamir: From practice to theory[C]//Proc of the 51st Annual ACM SIGACT Symp on Theory of Computing. New York: ACM, 2019: 1082−1090

[28] Attema T, Cramer R. Compressed-protocol theory and practical application to plug & play secure algorithmics[C]//Proc of the 40th Annual Int Cryptology Conf. Berlin: Springer, 2020: 513−543

[29] Fan Qing, He Debiao, Luo Min, et al. Ring signature schemes based on SM2 digital signature algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 710−723 (in Chinese)
(范青, 何德彪, 罗敏, 等. 基于 SM2 数字签名算法的环签名方案[J]. 密码学报, 2021, 8(4): 710−723)

[30] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signatures[C]//Proc of the Cryptographers' Track at the RSA Conf 2011. Berlin: Springer, 2011: 376−392



Zhaolu Tianyu, born in 1998. PhD candidate. His main research interests include applied cryptography, blockchain, and privacy protection.
赵陆天禹, 1998 年生. 博士研究生. 主要研究方向为应用密码学、区块链、隐私保护.



Wang Huaqun, born in 1974. PhD, professor, PhD supervisor. Member of CCF. His main research interests include applied cryptography, Chinese commercial cryptography, and data security.
王化群, 1974 年生. 博士, 教授, 博士生导师. CCF 会员. 主要研究方向为应用密码学、国密算法、数据安全.