基于区块链的物联网无证书多重身份认证方案

刘媛妮[1)] 殷涌泉[1)] 张建辉[2)] 周由胜[3)]

[1)](重庆邮电大学网络空间安全与信息法学院 重庆 400065)

[2)](国家数字交换系统工程技术研究中心 郑州 450002)

[3)](南京理工大学网络空间安全学院 南京 210094)

摘 要 针对现有物联网身份认证方案中普遍存在的中心化信任依赖、密钥托管风险以及单一用户多重身份管理复杂、认证效率低下等问题,本文提出了一种基于区块链的物联网无证书多重身份认证方案。利用区块链的去中心化特性,确保身份认证过程中公开参数的可信共享,消除传统架构带来的中心信任依赖。引入无证书签名机制以降低密钥托管问题和证书管理的复杂度,基于椭圆曲线密码体制实现轻量级安全认证;结合属性签名技术实现对单一用户多重身份的细粒度管理,采用多重身份聚合签名实现单次验证确认多重身份的完整性与有效性。在随机预言机模型下,证明了方案抵御适应性选择消息攻击的安全性;并利用仿真实验分析验证了与现有同类身份认证方案在效率方面的优势。

关键词 物联网;区块链;无证书;身份认证;多重身份

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2026.01670

A Blockchain-Based Certificateless Multi-Identity Authentication Scheme for IoT

LIU Yuan-Ni[1)] YIN Yong-Quan[1)] ZHANG Jian-Hui[2)] ZHOU You-Sheng[3)]

[1)](School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065)

[2)](National Digital Switching System Engineering and Technological Research and Department Center, Zhengzhou 450002)

[3)](School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094)

Abstract Aiming at the common problems in the existing Internet of Things (IoT) identity authentication schemes, such as centralized trust reliance, key escrow risks, complex management of multiple identities for a single user, and low authentication efficiency, a blockchain-based certificateless multi-identity authentication scheme for IoT is proposed. By leveraging the decentralized nature of blockchain, the scheme ensures the trusted sharing of public parameters during the identity authentication process, eliminating the central trust reliance brought by traditional architectures. The certificateless signature mechanism is introduced to reduce the key escrow problem and the complexity of certificate management, and lightweight security authentication is achieved based on elliptic curve cryptography. The attribute signature technology is combined to achieve fine-grained management of multiple identities for a single user, and the multiple identity aggregate signature is adopted to verify the integrity and validity of multiple identities in a single verification. The security of the scheme against adaptive chosen-message attacks is proved in the random oracle model, and the efficiency advantages over existing similar identity authentication schemes are analyzed and verified through simulation experiments.

收稿日期:2025-07-16;在线发布日期:2026-03-19。本课题得到国家重点研发计划(No. 2023YFB3105901)、国家自然科学基金(No. 62272076)资助。**刘媛妮**,博士,教授,主要研究领域为物联网安全、车联网安全和身份认证。E-mail:liuyn@cqupt.edu.cn。**殷涌泉**,硕士研究生,主要研究领域为无证书认证。**张建辉**,博士,研究员,主要研究领域为路由和交换设计、路由协议、资源调度、网络安全和未来网络。**周由胜(通信作者)**,博士,教授,主要研究领域为数据安全、认证和密钥协商。E-mail:zhouyousheng@njust.edu.cn。

Keywords　Internet of Things; blockchain; certificateless; identity authentication; multiple identities

1　引　言

物联网(Internet of Things, IoT)已广泛应用于工业自动化等领域,其设备互联互通特性实现了数据的实时交换与协同处理。现有物联网设备因开放性和资源受限性,在身份验证和数据保护方面面临严峻挑战。身份认证技术通过验证设备合法性、阻断未授权访问,能够在一定程度上保障数据传输的完整性与保密性,同时构建了抵御恶意攻击的核心防线。随着物联网规模和应用场景的不断扩展,传统身份认证技术在验证效率、隐私保护和传输安全等方面的局限性日益凸显。因此,设计一种高效、安全且具备良好适应性的认证方案,对构建可信物联网生态、提升系统安全具有重要意义。

传统身份认证方案多数以数字签名[1]为核心,签名方使用私钥生成签名,接收方通过公钥验证签名,实现身份确认和数据完整性保障。然而,物联网的开放性导致公钥的可信性难以保证,且密钥分发与管理的复杂性容易导致密钥泄露或签名伪造,使得数字签名已难以持续满足通信安全需求。公钥基础设施(Public Key Infrastructure, PKI)[2]通过引入数字证书(Digital Certificate, DC)[3]与证书颁发机构(Certificate Authority, CA)信任体系,利用证书生命周期管理和非对称加密技术实现公私钥的安全绑定、身份认证以及数据保护。然而,PKI 对中心化机构的高度依赖,难以实现公开参数的不可篡改存储与可信共享,存在显著的信任集中风险。

随着区块链[4]技术的发展,其去中心化共识机制和不可篡改特性为物联网通信中公开参数的可信共享与存储提供了保障,从而消除了中心化信任的瓶颈。在此基础上,现有研究[5-7]将区块链和 PKI 相结合,将多个信任机构分布构建在区块链网络中,并将证书等公开信息分布式存储在多个节点上,实现分布式的证书申请和查询,从而构建去中心化的物联网安全认证体系。然而,此类方案仍需依赖复杂基础设施进行证书的生成、分发与存储。随着设备数量激增,证书的管理负担与资源消耗显著上升,传统方案难以适应物联网设备的存储与计算能力。此外,传统方案中私钥由 CA 或可信第三方托管,一旦第三方遭受攻击,将会导致私钥泄露,进而破坏整体认证体系的安全性。无证书公钥密码学(Certificateless Public Key Cryptography, CL-PKC)通过用户标识符与部分私密信息的混合机制,摒弃了对数字证书的依赖,实现了身份验证的新模式。现有研究[8-9]将区块链与 CL-PKC 融合,利用链上共识与不可篡改特性确保无证书公钥的可信存储与共享,实现信息传输的保密性和不可伪造性。然而,物联网设备和用户常需在多场景下使用多重身份,传统“单一身份-独立认证”模式难以高效应对多重身份管理;且多数方案仍依赖双线性对运算,导致认证效率低下并存在安全隐患,难以满足资源受限的物联网环境对多重身份认证的需求。

本文提出一种基于区块链的物联网无证书多重身份认证方案,通过无证书公钥密码体制与椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)生成认证密钥对,并结合属性签名(Attribute Based Signature, ABS)技术实现对多重身份的细粒度管理;同时,针对多重身份产生的部分签名,采用聚合方式生成完整签名,并借助区块链网络确保认证过程中公开参数的可信共享。主要贡献如下:

(1)本文在区块链认证架构中引入无证书公钥密码体制,消除对中心化认证机构的依赖,规避密钥托管安全风险并简化证书管理;同时采用基于轻量级椭圆曲线密码构造算法,从计算效率与安全强度两方面提升物联网身份认证性能。

(2)引入属性签名技术实现对多重身份的细粒度管理。支持用户在不同应用域中拥有逻辑独立的数字身份,每个身份关联不同行业领域,满足用户在物联网中多样化角色的认证需求。

(3)提出多重身份签名协同生成与验证方法。该方法支持多重身份签名操作的并行处理,通过对多重身份所产生的部分签名进行聚合计算,有效降低多次签名验证的冗余开销。

2　相关工作

现有物联网身份认证研究主要围绕四个方向展开:一是以公钥基础设施 PKI 的传统认证;二是以区块链为载体的去中心化认证[10];三是无证书公钥密码体制及其应用;四是以区块链为载体的无证书身份认证。然而,针对多重身份认证的研究相对较

为缺乏，特别是在如何有效管理并支持多个身份同时参与认证方面，现有方案仍显不足。

在基于 PKI 的身份认证方面，Diffie 和 Hellman[11]开创性地提出了公钥密码学与数字签名的思想，通过签名保障消息来源真实性与完整性的理论基础。此后，PKI 作为主流的基于数字签名的认证架构，通过注册机构（Registration Authority，RA）和 CA 的协同实现身份的可信绑定。为降低终端负担，Park 等人[12]提出一种公钥驱动的 A3 级单点登录（Public Key-based A3-providing Single Sign On，PKASSO）协议，将复杂的 PKI 操作外移至基础设施侧，从而显著减轻移动设备的计算与管理开销。然而，PKI 对中心化 CA 的强依赖带来证书签发流程复杂、维护成本高以及单点脆弱性等问题[13]。为缓解上述困境，Shamir[14]提出基于身份的公钥密码体制（Identity Based Public Key Cryptography，IDPKC），在无需公开密钥目录与第三方查询服务的前提下完成密钥分发与验签，简化了公钥管理流程。但由于可信第三方私钥生成器仍具有中心化与密钥托管风险，相关安全隐患难以彻底消除[15]。

在基于区块链的身份认证方面，魏松杰等人[16]结合区块链与身份标识提出跨域认证方案，通过改进的安全仲裁签名与链上证书机制，增强了身份即时撤销与跨域核验能力。Zhao 等人[17]在医疗场景中融合人体传感器网络与区块链，利用生理信号生成密钥并结合混沌集合与改进协议，提升了隐私保护与链上密钥存储安全性。彭长根等人[18]提出基于区块链与密文策略属性加密的一轮可验证分布式密钥生成协议，以链上公开信道与智能合约实现子公钥有效性校验与可追溯性。Matsumoto 等人[19]则利用区块链与智能合约增强 PKI，对 CA 的不当行为提供自动化响应与问责。尽管上述研究在去中心化、数据安全与隐私保护方面取得进展，但仍难以根除证书管理与密钥托管问题。例如，AI-Bassam 等人[20]去中心化 PKI 能发现恶意证书，却未充分覆盖证书不可否认性；Chaum[21]提出的不可否认签名虽强化了不可否认性，但在实际部署中仍难彻底杜绝伪造风险。

在无证书身份认证方面，Al-Riyami 和 Paterson[22]提出无证书公钥密码体制，通过让用户参与私钥构造以分散信任中心风险。围绕无证书签名（Certificateless Signature Scheme，CLS）的系列研究中。Zhang 等人[23]通过将用户公钥与签名信息绑定并引入部分私钥生成思想，提升了对公钥替换与被动第三方攻击的抗性且无需安全信道。Thumbur 等人[24]在资源受限场景结合 ECC 与无证书框架，试图同时消除证书管理与密钥托管问题，但被发现仍存在签名伪造漏洞。针对该问题，Xu 等人[25]提出了一种新的无配对无证书签名方案，借助椭圆曲线离散对数难题避免双线性对开销，提高了安全性并降低计算与通信成本。现有无证书研究在削减证书冗余与托管风险方面成效显著，但仍面临中心化组件残留、公开参数可信传输与存储不稳定等挑战；然后在复杂环境下保障参数可信同步、提升并发处理能力并实现真正的去中心化存储，仍有待深入探究。

在基于区块链的无证书身份认证方面，Wang 等人[26]提出基于区块链的无配对无证书认证，将 KGC 逻辑上链并以智能合约降低单点故障与分布式拒绝服务攻击风险；进一步地，Wang 等人[27]采用历史链/证据链双链结构与变色龙哈希支持追责式更正，结合 ECC 避免双线性对，并以预计算、批量验证与随机校验和机制在保持安全性的同时降低时延、抵御密钥恢复与临时秘密泄露。尽管这些工作在公共信息可信共享与传输安全方面取得进展，但这些方案大多针对单一身份认证设计，对于如何平滑扩展至物联网的多身份复杂场景仍缺乏系统化设计与验证。

针对多重身份认证的特定需求，Srivastava[28]基于多变量二次问题与区块链提出身份基多签名，证明了在选定消息与选定身份攻击下的存在不可伪造性。袁和昕等人[29]结合区块链、门限算法、属性签名与非交互式零知识证明，构建可细粒度管理属性且可动态扩展 CA 的分布式公钥基础设施。张玉磊等人[30]在多用户环境下提出无证书认证可搜索加密方案，融合公钥认证加密与代理重加密支持授权关键词检索，兼顾计算与通信效率。Yang 等人[31]面向移动设备提出轻量级无证书多用户匹配加密方案，通过标准硬假设与无配对技术避免对多用户逐一加密，实现低开销分发。Liu 等人[32]则在物联网场景结合身份基与 Schnorr 多重签名，引入门限 Merkle 树与联盟链，实现隐私保护、离线设备支持、去中心化私钥生成与可证明安全。以上研究为多重身份认证需求提供了多样化的技术路径。

为更直观地比较现有研究与本文方案在去中心化、密钥托管、证书依赖、轻量化以及多重身份支持等方面的差异，相关工作对比如表 1 所示。

表 1　相关工作对比

相关文献	方案类型	去中心化	免密钥托管	免证书	轻量免配对	多重身份	单次验证多身份
[1-3,11-15]	PKI 等传统身份认证	×	×	×	√	×	×
[5-7,16-21,28-29,32]	区块链身份认证	√	×	×	√	×	×
[22-25,30-31]	无证书身份认证	×	√	√	△	×	×
[8-9,26-27]	区块链无证书身份认证	√	√	√	△	×	×
本文方案	区块链无证书多重身份认证	√	√	√	√	√	√

注:"√"表示支持,"×"表示不支持,"△"表示部分支持。

3　背景知识

3.1　椭圆曲线

假设 F_p 表示阶为 p 的有限域,其中 p 是大素数。通常定义一个标准椭圆曲线可用等式表示为

$$y^2 = x^3 + ax + b \ mod \ p \tag{1}$$

其中 $a,b \in F_p$ 且 $\Delta = 4a^3 + 27b^2 \neq 0$。椭圆曲线(Elliptic Curve, EC)[33] 上的点和无穷远处的点 O 构成一个循环加法椭圆曲线群:

$$G = \{(x,y): x,y \in F_p, E(x,y) = 0\} \cup \{O\} \tag{2}$$

椭圆曲线加法群 G 有如下性质:

(1)椭圆曲线的加法:设 $P,Q \in G$。当 $P = Q$ 时,加法运算结果为 $R = P + P$,此时 R 由椭圆曲线 E 在点 P 处的切线与曲线相交得到;当 $P \neq Q$ 时,加法结果为 $R = P + Q$,其中 R 对应连接 P 与 Q 的直线与曲线 E 的交点;当 $P = -Q$ 时,有 $O = P + Q = P - P$。

(2)椭圆曲线的标量乘法:设 $P \in G$ 且 $k \in Z_q^*$,则对于点 P 有如下描述:

$$kP = P + P + \cdots + P \quad k \in Z_q^*, P \in G \tag{3}$$

假设已知椭圆曲线上的点 P 和点对 kP,欲逆向求得 $k \in Z_q^*$,称之为椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)[34]。求解 ECDLP 问题被广泛认为计算上是不可行的,具有较高的安全性。

3.2　无证书密码学

无证书公钥密码体制(CL-PKC)旨在解决传统基于证书的认证机制中存在的诸多问题,例如复杂的证书管理、对中心化信任的依赖以及隐私泄露风险。无证书签名技术摒弃了传统公钥基础设施 PKI 中对数字证书的依赖,采用一种混合机制,通过结合用户标识符和部分公开信息来验证用户身份。这种方法有效避免了证书管理的复杂性,降低了对单一信任中心的依赖,增强了系统的去中心化特性并提升了抗攻击能力。

CL-PKC 的核心思想是用户与密钥生成中心 KGC 共同协作生成用户密钥。其主要流程如下:

(1)系统参数生成:生成系统公共参数 、系统私钥并根据系统私钥计算系统公钥;

(2)秘密值设置:用户随机选取秘密值,并根据该秘密值计算部分公钥;

(3)部分私钥与公钥设置:KGC 以系统公共参数 、系统密钥和用户 ID 作为输入,生成用户的部分私钥和部分公钥,并将其返回给用户。用户接收参数并进行验证,若验证失败则终止流程;

(4)密钥提取:用户结合接收的部分私钥与部分公钥,以及已知信息,生成用户的完整密钥对。

3.3　属性签名

属性基加密(Attribute-Based Encryption, ABE)由 Sahai 和 Waters[35] 共同提出,是一种基于属性集的加密技术,其核心价值在于能够实现对数据的按需加密,同时确保消息来源的可靠性,并且可以验证签名者是否具备相应的资格或权限,例如个人资质、身份、权限级别等关键要素。而属性签名(Attribute-Based Signature, ABS)则是在 ABE 的基础上发展而来的延伸技术,它巧妙地将属性与数字签名相结合,使得签名者能够利用特定属性对消息进行签名。

在物联网多重身份认证中,ABS 展现出显著的应用潜力,主要体现在以下几个方面:首先,属性签名支持细粒度访问控制,签名者通过选择特定的属性组合进行签名,验证者仅能获知签名者是否具备相关的属性,避免泄露其他敏感信息;其次,属性签名具有高度灵活性,用户可以根据实际需求选择不同的属性组合进行签名;最后,属性签名具备较强的匿名性,签名过程可选择对用户的具体身份信息进行隐藏,增强隐私保护。

本文所提出的方案将用户的多重身份视为不同的属性,以此实现对用户身份的细粒度管理。同时,在验证环节,采用了一种动态全身份验证策略。具体而言,系统会依据已保存的身份信息来获取对应的公钥,从而能够一次性全面地验证认证请求方所持有的全部身份。

4 无证书多重身份认证方案设计

本文提出的面向物联网场景的无证书多重身份认证方案中包含密钥生成中心 KGC 等 6 个实体，无证书多重身份认证方案模型如图 1 所示。

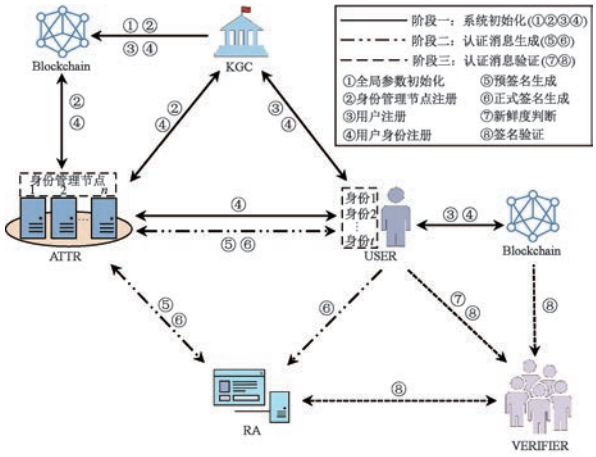


图 1 无证书多重身份认证方案模型

(1)密钥生成中心 KGC：负责生成系统主私钥与公钥，通过注册信息的传递协助各实体进行初始化，并将公开信息传输至区块链，确保实体隐私信息自主管理，降低泄露风险。

(2)身份管理节点 ATTR：假设环境中存在 n 个不同的行业领域，则对应的身份管理节点集合记为 $I=\{\mathrm{ATTR}_1,\mathrm{ATTR}_2,\cdots,\mathrm{ATTR}_n\}$，其中 ATTR_i 代表第 i 个行业领域的身份授权机构。负责定义和管理其领域内的用户身份集合，为用户颁发在该领域用户身份对应的唯一身份标识。ATTR_i 参与密钥生成以及签名过程中的特定环节，并将各阶段的公开信息传输至区块链。

(3)注册机构 RA：负责在用户签名和验证过程中计算、转发和存储签名参数。RA 对用户身份信息采用版本化存储，每次变更生成唯一的版本标识 VID，查询时给定用户标识与目标版本，返回该用户在该 VID 下的身份信息快照，旧版本保留且不可更改，具备一定的计算与存储能力。

(4)用户 USER：作为认证请求方，其持有的身份数量为 $t(t\leqslant n)$。USER 与 KGC、ATTR、RA 等实体交互生成密钥、执行签名算法生成认证消息，并将各阶段的公开信息传输至区块链，具备一定的计算与存储能力。

(5)验证方 VERIFIER：作为签名验证方，与 RA、用户等实体进行信息交互，并根据 RA 返回的身份信息从区块链获取对应的公开信息验证签名是否真实有效，具备一定的计算与存储能力。

(6)区块链 Blockchain：用于存储公开信息(如系统公开参数、各实体的公钥等)，确保公开信息的不可篡改和透明性，降低单点故障风险。

本文符号变量如表 2 所示。

表 2 符号变量

符号	描述
H_0,H_1,H_2,H_3	单向哈希函数
x_m	系统私钥
P_m	系统公钥
$SK_{id}=\{x_{id},y_{id}\}$	实体 id 的私钥对
$PK_{id}=\{P_{id},R_{id}\}$	实体 id 的公钥对
r_{id},t_i,b	Z_q^* 上的随机数
m	消息
c_i,d_i,e_i,s_i,B,W_i	中间参数
$P_{n-t}(\theta)$	拉格朗日插值多项式
$Time_i$	时间戳
σ	密文
sig	签名

本文提出的认证方案包括三个阶段：系统初始化、认证消息生成和认证消息验证，描述如下：

(1)系统初始化阶段：该阶段完成全局参数的生成，并根据全局参数执行身份管理节点注册、用户注册以及用户身份注册；

(2)认证消息生成阶段：基于系统初始化阶段生成的公私钥等参数，用户、RA 和 ATTR 通过安全信道或区块链交换必要信息并执行签名算法，生成合法的认证消息；

(3)认证消息验证阶段：验证者接收认证消息，根据方案定义的校验规则与可用公开信息，对签名的真实性、合法性和有效性进行验证，从而判断认证请求方的身份是否可信。

4.1 系统初始化

系统中区块链采用伊斯坦布尔拜占庭容错算法(Istanbul Byzantine Fault Tolerance，IBFT)[36]作为基础协议，以预选验证者参与共识、基于拜占庭容错达成共识。为降低链上冗余与访问开销，系统在写入前对需发布的数据进行压缩处理；链上仅保存必要的公开参数与小尺寸的内容摘要，用以完成验证与版本追溯；体量较大的对象采用星际文件系统(InterPlanetary File System，IPFS)[37]链下存储，链上保留其指纹以实现完整性校验与溯源。

4.1.1 全局参数初始化

当系统首次部署时，生成全局公开参数 $Params$ 并上链存储。设 $E(F_p)$ 为定义在有限域 F_p 上的椭

圆曲线,选择 $E(F_p)$ 上阶为 q 的生成元 P,并构造一个素数阶 $N=q$ 的循环群 G,其中 p 和 q 均为大素数。此外,需要定义 4 个哈希函数 $H_0:\{0,1\}^*\times G\times G\rightarrow Z_q^*$,$H_1:\{0,1\}^*\times G\times G\times G\rightarrow Z_q^*$,$H_2:\{0,1\}^*\times G^{n+1}\rightarrow Z_q^*$,$H_3:\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\times G\rightarrow Z_q^*$。密钥生成中心 KGC 首先从 Z_q^* 中选取随机数 $x_m\in Z_q^*$ 作为系统私钥,然后利用生成元 P 计算对应的系统公钥 $P_m=x_mP$。完成以上参数设置后,全局参数 $Params=\{E(F_p),G,q,p,P,H_0,H_1,H_2,H_3,P_m\}$ 将被上传至区块链,以实现信息的可信共享。

4.1.2　身份管理节点注册

本文针对用户可能在多个行业领域中扮演不同角色的情况,提出一种多节点管理的机制。每个身份管理节点负责特定行业域,并根据实体在该行业中的身份发放唯一身份标识。为了覆盖更广泛的行业领域,系统在初始化阶段预先注册了一系列身份管理节点,确保用户能够在初始化阶段申请并获得其所属行业领域的身份标识。身份管理节点注册流程如图 2 所示。

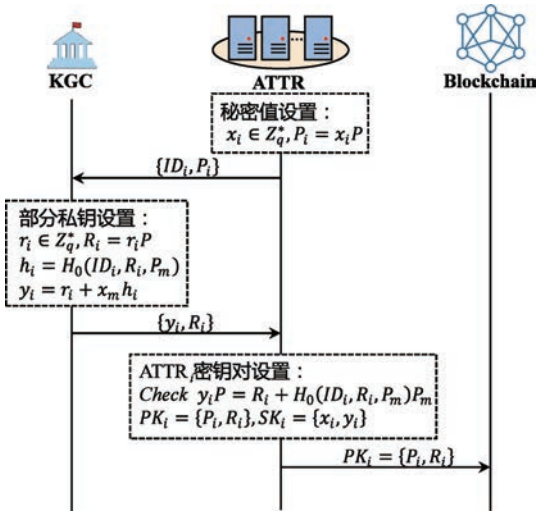


图 2　身份管理节点注册流程

(1)身份管理节点 $ATTR_i$ 从 Z_q^* 中随机选取秘密值 $x_i\in Z_q^*$,并计算 $P_i=x_iP$。随后,$ATTR_i$ 将其节点标识 ID_i 和 P_i 发送给密钥生成中心 KGC 并发起密钥生成请求。

(2)密钥生成中心 KGC 收到来自 $ATTR_i$ 的请求后,从 Z_q^* 中随机选取 $r_i\in Z_q^*$,计算部分公钥 $R_i=r_iP$ 及哈希值 $h_i=H_0(ID_i,R_i,P_m)$,然后生成身份管理节点的部分私钥 $y_i=r_i+x_mh_i$。最后,KGC 将 $\{y_i,R_i\}$ 返回给 $ATTR_i$。

(3)身份管理节点 $ATTR_i$ 接收到 $\{y_i,R_i\}$ 后,首先验证等式 $y_iP=R_i+H_0(ID_i,R_i,P_m)P_m$。若验证不通过,则销毁所有临时参数并终止密钥生成;若验证通过,则将 y_i 作为该节点的部分私钥。$ATTR_i$ 成功获取完整的密钥对,公钥 $PK_i=\{P_i,R_i\}$,私钥 $SK_i=\{x_i,y_i\}$。

节点的动态接入与退出均触发对应上链共识事件,前者在共识确认后对全网可见,后者保留历史记录但停止分发新参数。验证方按认证消息中的目标版本检索对应公钥,避免因动态变更导致误验。

4.1.3　用户注册

当用户 $USER_{Applicant,u}$ 首次加入认证环境时,系统与用户在初始化阶段交互生成无证书公私钥对。$USER_{Applicant,u}$ 将其公钥对上链存储,确保其公钥信息的透明性和真实性。用户注册流程如图 3 所示。

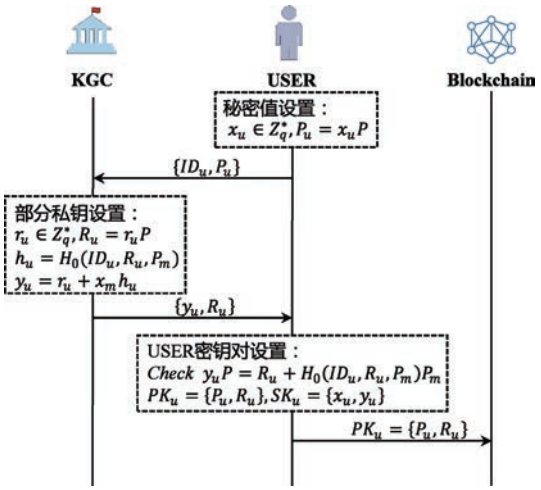


图 3　用户注册流程

(1)用户 $USER_{Applicant,u}$ 从 Z_q^* 中随机选取秘密值 $x_u\in Z_q^*$,并计算 $P_u=x_uP$。随后,$USER_{Applicant,u}$ 将其标识 ID_u 和 P_u 发送给密钥生成中心 KGC 并发起密钥生成请求。

(2)密钥生成中心 KGC 收到来自用户 $USER_{Applicant,u}$ 的请求后,从 Z_q^* 中随机选取 $r_u\in Z_q^*$,计算部分公钥 $R_u=r_uP$ 及哈希值 $h_u=H_0(ID_u,R_u,P_m)$,然后生成用户的部分私钥 $y_u=r_u+x_mh_u$。最后,KGC 将 $\{y_u,R_u\}$ 返回给 $USER_{Applicant,u}$。

(3)用户 $USER_{Applicant,u}$ 接收到 $\{y_u,R_u\}$ 后,首先验证等式 $y_uP=R_u+H_0(ID_u,R_u,P_m)P_m$。若验证不通过,则销毁所有临时参数并终止密钥生成;若验证通过,则将 y_u 作为用户的部分私钥。$USER_{Applicant,u}$ 成功获取完整的密钥对,公钥 $PK_u=\{P_u,R_u\}$,私钥 $SK_u=\{x_u,y_u\}$。

在用户注册过程中，用户密钥轮换将触发上链共识事件，共识确认后全网可见，保留历史记录但停止分发新参数。验证方按认证消息中的目标版本检索对应公钥，避免因动态变更导致误验。

4.1.4 用户身份注册

用户 $\mathrm{USER}_{Applicant,u}$ 根据其所属的行业领域，向对应的身份管理节点 ATTR_i 提交唯一身份标识 $ID_{u,i}$，由 ATTR_i 确认后为其分配该用户在当前行业领域的唯一身份标识。$\mathrm{USER}_{Applicant,u}$ 利用 $ID_{u,i}$ 生成用户身份公私钥对，并将私钥与对应的 ATTR_i 进行共享，同时将其公钥上链进行透明存储。用户身份注册流程如图 4 所示。

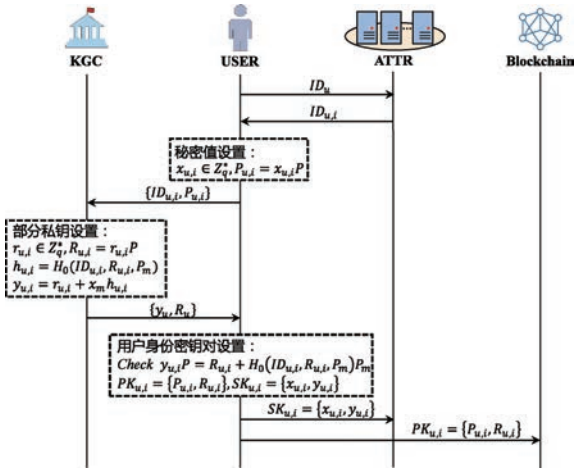


图 4 用户身份注册流程

(1)用户 $\mathrm{USER}_{Applicant,u}$ 向其对应的身份管理节点 ATTR_i 发起身份标识申请，该 ATTR_i 根据行业领域的授权策略为 $\mathrm{USER}_{Applicant,u}$ 分配唯一身份标识 $ID_{u,i}$。随后，$\mathrm{USER}_{Applicant,u}$ 从 Z_q^* 中随机选取秘密值 $x_{u,i} \in Z_q^*$，并计算 $P_{u,i} = x_{u,i}P$。最后，$\mathrm{USER}_{Applicant,u}$ 将该身份标识 $ID_{u,i}$ 和 $P_{u,i}$ 提交至密钥生成中心 KGC 并发起密钥生成请求。

(2)密钥生成中心 KGC 收到来自用户 $\mathrm{USER}_{Applicant,u}$ 的请求后，从 Z_q^* 中随机选取 $r_{u,i} \in Z_q^*$，计算部分公钥 $R_{u,i} = r_{u,i}P$ 及哈希值 $h_{u,i} = H_0(ID_{u,i}, R_{u,i}, P_m)$，然后生成用户身份的部分私钥 $y_{u,i} = r_{u,i} + x_m h_{u,i}$。最后，KGC 将 $\{y_{u,i}, R_{u,i}\}$ 返回给 $\mathrm{USER}_{Applicant,u}$。

(3)用户 $\mathrm{USER}_{Applicant,u}$ 接收到 $\{y_{u,i}, R_{u,i}\}$ 后，首先验证等式 $y_{u,i}P = R_{u,i} + H_0(ID_{u,i}, R_{u,i}, P_m)P_m$。若验证不通过，则销毁所有临时参数并终止密钥生成；若验证通过，则将 $y_{u,i}$ 作为用户身份的部分私钥。$\mathrm{USER}_{Applicant,u}$ 成功获取完整的密钥对，公钥 $PK_{u,i} = \{P_{u,i}, R_{u,i}\}$，私钥 $SK_{u,i} = \{x_{u,i}, y_{u,i}\}$。此外，用户需以安全方式将私钥与对应的身份管理节点 ATTR_i 进行共享。

在用户身份注册过程中，用户身份的新增或撤销均触发对应上链共识事件，前者在共识确认后对全网可见，后者保留历史记录但停止分发新参数。验证方按认证消息中的目标版本检索对应公钥，避免因动态变更导致误验。

4.2 认证消息生成

假设当前环境中行业领域的数量为 n，相应的节点集合为 $I = \{\mathrm{ATTR}_1, \mathrm{ATTR}_2, \cdots, \mathrm{ATTR}_n\}$；用户 $\mathrm{USER}_{Applicant,u}$ 当前持有的身份数量为 t，其对应已申请的身份管理节点集合记为 A，未申请的节点集合记为 U，其中 $A \cup U = I$ 且 $A \cap U = \varnothing$。下文公式中 $i = \{Extr(A)\}$ 表示下标为 i 的参数由集合 A 中 ATTR_i 管理或对应；$i = \{Extr(U)\}$ 表示下标为 i 的参数由集合 U 中 ATTR_i 管理或对应。用户将当前持有的身份集合和消息 m 提交至注册机构，当节点集合或身份集合因接入/退出或调整发生变化时，RA 为该用户生成新的身份信息条目与版本号 VID 以实现多版本维护和可追溯管理，RA 将该 VID 返回给用户，用于后续认证流程中的引用与校验，旧版本保留用于历史消息验证。认证消息生成流程如图 5 所示。

用户和身份管理节点查询预签名缓存记录。若存在预签名记录，则无需重复计算相关参数；否则，需执行以下步骤进行预签名计算：

(1)用户 $\mathrm{USER}_{Applicant,u}$ 根据已持有的身份，计算秘密参数 s_i：

$$e_i = H_1(ID_i, R_{u,i}, R_u, R_i)$$
$$s_i = x_{u,i} + e_i x_u \quad i = \{Extr(A)\} \tag{4}$$

(2)集合 A 中的身份管理节点 ATTR_i 选取随机值 $t_i \in Z_q^*$，并以安全的方式将 t_i 转发至用户 $\mathrm{USER}_{Applicant,u}$，同时计算参数 W_i：

$$W_i = t_i P \quad i = \{Extr(A)\} \tag{5}$$

(3)集合 U 中的身份管理节点 ATTR_i 选取一组随机值 $c_i, d_i \in Z_q^*$，生成临时填充身份公钥 $P_{u,i}$，$R_{u,i} \in G$ 并计算参数 W_i：

$$e_i = H_1(ID_i, R_{u,i}, R_u, R_i)$$
$$W_i = c_i(P_{u,i} + e_i P_u) + d_i P \quad i = \{Extr(U)\} \tag{6}$$

上述步骤的计算条件与结果相互独立，因此各节点可并行计算。$\mathrm{USER}_{Applicant,u}$ 保存结果 s_i、t_i 和 W_i，身份管理节点保存结果 c_i、d_i 和 W_i。

正式签名流程如下：

(1)身份管理节点 ATTR_i 将 c_i、d_i 和 W_i 以安

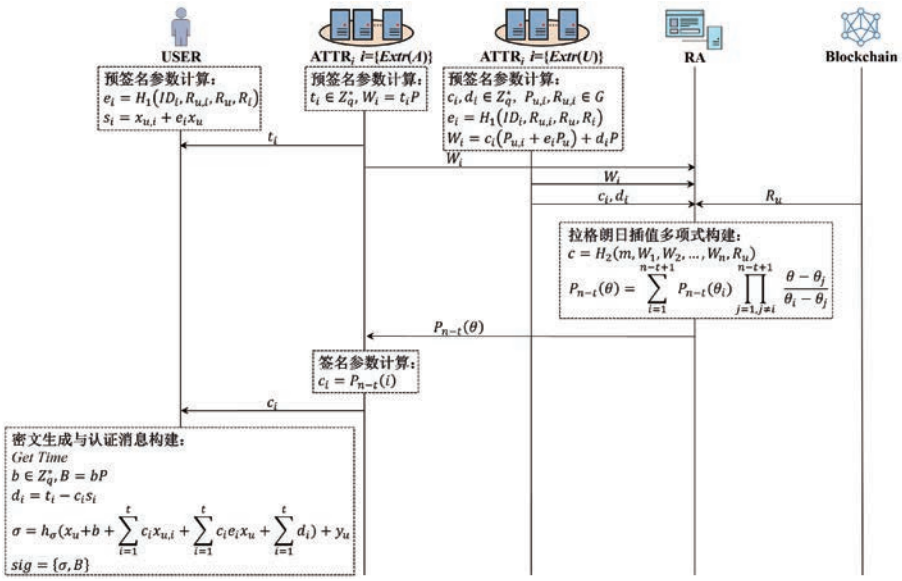


图 5　认证消息生成流程

全的方式转发至 RA 注册机构。RA 对该用户的版本号为 VID 的身份记录进行查询;若发现缺失,则将集合 A 发送的 W_i 写入其对应的身份信息条目,写入完成后将该身份信息设为不可修改。

(2)注册机构 RA 根据用户 $\mathrm{USER}_{Applicant,u}$ 的身份信息从区块链获取与之对应的公钥 ,计算中间参数 $c=H_2(m,W_1,W_2,\cdots,W_n,R_u)$,并使用 $n-t+1$ 个已知点 $(0,c),\{(i,c_i)\}$,$i=\{Extr(U)\}$ 构建 $n-t$ 次拉格朗日插值多项式 $P_{n-t}(\theta)$。随后,RA 将多项式 $P_{n-t}(\theta)$ 分发给集合 A 中的身份管理节点 ATTR_i:

$$P_{n-t}(\theta)=\sum_{i=1}^{n-t+1}P_{n-t}(\theta_i)\prod_{j=1,j\neq i}^{n-t+1}\frac{\theta-\theta_j}{\theta_i-\theta_j} \tag{7}$$

其中,$P_{n-t}(\theta_i)$ 为

$$\begin{cases}P_{n-t}(\theta_1)=c,\\ \cdots,\\ P_{n-t}(\theta_i)=c_i,\end{cases}\quad i=\{Extr(U)\} \tag{8}$$

(3)集合 A 中的身份管理节点 ATTR_i 利用拉格朗日插值多项式计算 c_i,并以安全的方式将结果转发给用户 $\mathrm{USER}_{Applicant,u}$:

$$c_i=P_{n-t}(i)\quad i=\{Extr(A)\} \tag{9}$$

(4)用户 $\mathrm{USER}_{Applicant,u}$ 计算部分签名参数 d_i,其中 $i=\{Extr(A)\}$,选取随机值 $b\in Z_q^*$ 并计算 $B=bP$,获取当前时间戳 $Time_u$,计算哈希值 $h_\sigma=H_3(ID_u,m,Time_u,B,P_u,R_u)$ 和密文 σ,生成签名 $sig=\{\sigma,B\}$ 并构建完整认证消息 $M=\{VID,ID_u,m,Time_u,sig\}$:

$$d_i=t_i-c_is_i,$$

$$\sigma=h_\sigma\left(x_u+b+\sum_{i=1}^{t}c_ix_{u,i}+\sum_{i=1}^{t}c_ie_ix_u+\sum_{i=1}^{t}d_i\right)+y_u \tag{10}$$

4.3　认证消息验证

假设签名验证方 VERIFIER 对用户 $\mathrm{USER}_{Applicant,u}$ 进行认证,收到 $\mathrm{USER}_{Applicant,u}$ 提供的完整认证消息 M,执行以下验证步骤:

(1)VERIFIER 根据 $Time_{cur}-Time_u\leqslant\Delta Time$ 判断消息的新鲜度。其中 $Time_{cur}$ 为 VERIFIER 收到消息的时刻;$Time_u$ 为 $\mathrm{USER}_{Applicant,u}$ 生成签名的时刻;$\Delta Time$ 为系统可接受的最大时间间隔。

(2)VERIFIER 首先通过注册机构 RA 检索版本号为 VID 的 $\mathrm{USER}_{Applicant,u}$ 身份信息记录,并从区块链获取与之对应的公钥。随后,计算相关验证参数,验证式(11)是否成立,若等式成立则通过认证;反之则认证失败:

$$h_u=H_0(ID_u,R_u,P_m),$$

$$h_\sigma=H_3(ID_u,m,Time_u,B,P_u,R_u),$$

$$\sigma P=h_\sigma\left(P_u+B+\sum_{i=1}^{t}W_i\right)+R_u+h_uP_m \tag{11}$$

5　方案分析

5.1　正确性分析

假设 M 为用户 $\mathrm{USER}_{Applicant,u}$ 的完整认证消息,若满足等式 $\sigma P=h_\sigma\left(x_u+B+m+\sum_{i=1}^{t}W_i\right)+R_u+h_uP_m$ 则证明该签名为正确签名。其中:

$$\begin{aligned}W_i &= c_i(P_{u,i}+e_iP_u)+d_iP\\ &= c_i(x_{u,i}+e_ix_u)P+d_iP\\ &= c_is_iP+d_iP\\ &= (d_i+c_is_i)P\\ &= t_iP \quad i=\{Extr(A)\}\end{aligned} \tag{12}$$

由上述证明可知，签名构造中多重身份的部分签名聚合正确，签名验证阶段正确性证明如下：

$$\begin{aligned}\sigma P &= h_\sigma(x_u+b+\sum_{i=1}^{t}c_ix_{u,i}+\sum_{i=1}^{t}c_ie_ix_u+\sum_{i=1}^{t}d_i)P+y_uP\\ &= h_\sigma(P_u+B+\sum_{i=1}^{t}c_ix_{u,i}P+\sum_{i=1}^{t}c_ie_ix_uP+\sum_{i=1}^{t}d_iP)+(r_u+x_mh_u)P\\ &= h_\sigma(P_u+B+\sum_{i=1}^{t}W_i)+R_u+h_uP_m\end{aligned} \tag{13}$$

5.2 形式化安全性分析

本文无证书认证方案的安全性考虑了类型Ⅰ的攻击者 $A1$ 和类型Ⅱ的攻击者 $A2$ 两种不同级别的攻击敌手。

类型Ⅰ的攻击者 $A1$：该类攻击者模拟系统外部的恶意第三方，属于典型的外部攻击模型。其能力主要体现在可以对系统中的公钥发起请求并进行替换，但无法获得系统主密钥。该攻击者的目标是通过适应性选择消息攻击，伪造出能够通过验证的合法签名。

类型Ⅱ的攻击者 $A2$：该类攻击者用于描述系统内部潜在的威胁实体，可视为掌握系统主密钥的恶意但诚实执行部分流程的 KGC。与类型Ⅰ攻击者不同，其虽然能够接触系统主密钥，却不具备替换用户公钥的能力。因此，这类攻击者的目标同样是生成能够通过验证的伪造签名，但其攻击方式受到公钥不可替换这一条件的限制。

定理 1. 基于椭圆曲线的离散对数问题(ECDLP)：给定椭圆曲线上的点 P 及其标量乘法结果 mP，在多项式时间内求得标量 m 的概率是可忽略的。基于 ECDLP 困难性假设，本文所提出的无证书认证方案在面对类型Ⅰ攻击者 $A1$ 时，能够达到存在性不可伪造安全性，并可有效抵御适应性选择消息攻击。

引理 1. 在随机预言模型下，设存在一个类型Ⅰ敌手 $A1$。若该敌手在至多进行 N_h 次哈希询问、N_{psk} 次部分私钥询问、N_{pk} 次公钥询问以及 N_σ 次签名询问后，仍然能够成功构造出一个合法签名伪造，则可据此求解 ECDLP 椭圆曲线离散对数问题。

证明. 假设一个敌手 $A1$ 在本文方案中能够以无法忽视的优势成功伪造目标用户的有效签名。给定 $(P,Q=aP)$ 为 ECDLP 问题的一个实例，其中 $a\in Z_q^*$，$P\in G$。挑战者 C 的目标是求出 a。

初始化阶段：挑战者 C 初始化系统参数 $Params=\{E(F_p),G,q,p,P,H_0,H_1,H_2,H_3,P_m\}$ 和系统公钥 $P_m=Q=aP$，将系统参数发送给 $A1$。由于本文包含用户注册、身份管理节点注册以及用户身份注册三个相关联的注册阶段，因此下文询问阶段默认进行相关联的询问。挑战者 C 随机选择 ID_I 以及其相关联的身份作为游戏的挑战身份。

在询问阶段，敌手 $A1$ 可自适应地向各类预言机发起多项式次有界查询。对此，挑战者 C 按如下方式进行模拟并返回相应结果。

H_0 询问：当 $A1$ 以 (ID_u,R_u,P_m) 作为输入向预言机发起查询时，挑战者 C 维护列表 $L_0=(ID_u,R_u,P_m,h_u)$，且初始时为空。若 L_0 中已存在与该输入对应的记录，则直接将记录中的 h_u 返回给 $A1$；否则，C 从 Z_q^* 随机选取 h_u，将其作为查询结果返回，并把 (ID_u,R_u,P_m,h_u) 加入列表 L_0。

H_1 询问：当 $A1$ 以 $(ID_i,R_{u,i},R_u,R_i)$ 向预言机发起查询时，挑战者 C 维护列表 $L_1=(ID_i,R_{u,i},R_u,e_i)$，其中 L_1 初始为空。若在列表中找到对应项，则返回其中保存的 e_i；若未找到，则由 C 随机选取 $e_i\in Z_q^*$，将其发送给 $A1$，同时将 $(ID_i,R_{u,i},R_u,e_i)$ 记录到 L_1 中。

H_2 询问：当 $A1$ 以 $(m,W_1,W_2,\cdots,W_n,R_u)$ 作为输入进行查询时，挑战者 C 维护列表 $L_2=(m,W_1,W_2,\cdots,W_n,R_u,c)$，其中 L_2 初始为空。若列表中已存在对应记录，则直接返回其中的 c；否则，随机选取 $c\in Z_q^*$，将其作为输出返回给 $A1$，并把 $(m,W_1,W_2,\cdots,W_n,R_u,c)$ 写入 L_2。

H_3 询问：当 $A1$ 以 $(ID_u,m,Time_u,B,P_u,R_u)$ 向预言机发起查询时，挑战者 C 维护列表 $L_3=(ID_u,m,Time_u,B,P_u,R_u,h_\sigma)$，且 L_3 初始为空。若查询内容已存在于列表中，则返回相应的 h_σ；否则，随机选取 $h_\sigma\in Z_q^*$，将其返回给 $A1$，并将 $(ID_u,m,Time_u,B,P_u,R_u,h_\sigma)$ 保存至 L_3 中。

部分私钥提取询问：当 $A1$ 以 ID_u 发起部分私钥提取请求时，挑战者 C 维护列表 $L_p=(ID_u,R_u,y_u)$，其中 L_p 初始为空。若 L_p 中存在对应记录，则直接返回 y_u；否则，若 $ID_u\neq ID_I$，C 随机选取 y_u，$h_u\in Z_q^*$，并计算 $R_u=y_uP-h_uP_m$，随后，C 将 (ID_u,R_u,y_u) 和 (ID_u,R_u,P_m,h_u) 记录到 L_p 和

L_0 中,将 y_u 返回给 $A1$。若 $ID_u=ID_I$,则挑战者 C 中止模拟并终止操作。

公钥提取询问:当 $A1$ 以 ID_u 发起公钥提取请求时,挑战者 C 维护列表 $L_{pub}=(ID_u,x_u,P_u,R_u)$,且该列表初始为空。若在 L_{pub} 中找到对应记录 (ID_u,x_u,P_u,R_u),则直接将 (P_u,R_u) 返回给 $A1$;否则,若 $ID_u\neq ID_I$,C 随机选取 $x_u\in Z_q^*$,令 $P_u=x_uP$,并从列表 L_p 中恢复 $\{y_u,R_u\}$。随后,C 将 (P_u,R_u) 返回给 $A1$,并将 (ID_u,x_u,P_u,R_u) 记录到列表 L_{pub} 中;若 $ID_u=ID_I$,C 随机选取 $x_u,r_u,h_u\in Z_q^*$,计算 $P_u=x_uP$ 和 $R_u=r_uP$,然后,C 将结果 (P_u,R_u) 返回给 $A1$,并将 (ID_u,R_u,P_m,h_u) 与 (ID_u,x_u,P_u,R_u) 分别保存到列表 L_0 和 L_{pub} 中。

秘密值提取询问:当 $A1$ 以 ID_u 请求用户秘密值时,挑战者 C 通过查询列表 $L_{pub}=(ID_u,x_u,P_u,R_u)$ 进行响应。若列表中已存在对应项,则直接将秘密值 x_u 返回给 $A1$;若不存在且 $ID_u\neq ID_I$,则 C 执行一次公钥提取询问以生成相应记录 (ID_u,x_u,P_u,R_u),再将 x_u 返回给 $A1$,若 $ID_u=ID_I$,则挑战者 C 中止模拟并终止操作。

公钥替换询问:$A1$ 可以自由指定新的公钥 P'_u 对目标用户公钥进行替换。当 $A1$ 向预言机发起请求时,C 首先在列表 L_{pub} 中查找记录 (ID_u,x_u,P_u,R_u),若未找到,则先对该身份执行一次公钥提取询问。随后将 P_u 替换成 $A1$ 指定的新公钥 P'_u,并令 $x_u=\perp$。

签名询问:$A1$ 以 (ID_u,m) 向预言机发起询问,挑战者 C 维护列表 $L_{sig}=(ID_u,m,sig,M)$,其中列表 L_{sig} 初始为空。若在列表 L_{sig} 中查询到相关记录,则取出记录 (ID_u,m,sig,M),将 (sig,M) 发送给 $A1$。若列表 L_{sig} 无记录,则分别从列表 L_0、L_1、L_2、L_3、L_p 和 L_{pub} 恢复各个参数。对于集合 A 中的身份管理节点,C 随机选取 $t_i\in Z_q^*$,$i=\{Extr(A)\}$;对于集合 U 中身份管理节点,C 随机选取 c_i,$d_i\in Z_q^*$ 和 $P_{u,i},R_{u,i}\in G$,令 $e_i=H_1(ID_i,R_{u,i},R_u,R_i)$,$c=H_2(m,W_1,W_2,\cdots,W_n,R_u)$ 通过以上参数构造多项式 $P_{n-t}(\theta)$ 并计算出集合 A 中身份管理节点对应的 c_i 和 d_i,选取随机值 $b\in Z_q^*$ 并计算 $B=bP$,令 $h_\sigma=H_3(ID_u,m,Time_u,B,P_u,R_u)$,由此可得到一个正确密文 $\sigma=h_\sigma(x_u+b+\sum_{i=1}^{t}c_ix_{u,i}+\sum_{i=1}^{t}c_ie_ix_u+\sum_{i=1}^{t}d_i)+y_u$。最后挑战者 C 将完整签名结果 (sig,M) 返回给 $A1$。

伪造:攻击者 $A1$ 对 (ID^*,m) 输出伪造签名 (ID^*,m,sig^*,M^*)。该签名是由消息 m 和身份为 ID^* 且公钥为 (P_u,R_u) 的条件下生成的。利用分叉引理,通过公钥提取询问,生成不同的哈希值 h_u 和 h'_u,并生成不同的认证消息 M 和 M^*,其中包含不同的签名 sig 和 sig^*。由于两个签名都是合法签名,因此有以下两个签名认证的等式成立:

$$\sigma P=h_\sigma(P_u+B+\sum_{i=1}^{t}W_i)+R_u+h_uP_m \tag{14}$$

$$\sigma^* P=h_\sigma(P_u+B+\sum_{i=1}^{t}W_i)+R_u+h'_uP_m \tag{15}$$

上述两式相减可得 $\sigma P-\sigma^* P=h_uP_m-h'_uP_m$,通过代入待解实例 $P_m=aP$ 并化简可计算得到 $a=(\sigma-\sigma^*)(h_u-h'_u)^{-1}$。因此,在随机预言机模型与 ECDLP 难题前提下,若存在能进行公钥替换的类型Ⅰ的攻击者 $A1$ 以非忽略优势伪造有效签名,则可据此构造出多项式时间内解 ECDLP 的算法,矛盾成立。因此,本文所提出的方案在面对类型Ⅰ攻击者 $A1$ 时,在适应性选择消息攻击模型下满足存在性不可伪造安全性,与定理 1 表述完全一致。

定理 2.　基于椭圆曲线的离散对数问题(ECDLP):给定一个椭圆曲线上的一点 P 和该点的 m 倍 mP,计算出 m 的概率在多项式时间内是可以忽略的。在 ECDLP 困难性假设成立的前提下,本文提出的无证书认证方案对类型Ⅱ的攻击者 $A2$ 同样具备存在性不可伪造性,并能够抵抗适应性选择消息攻击。

证明思路与方法和定理 1 相同,但定理 2 在证明过程中不再具备公钥替换的能力。

5.3　非形式化安全性分析

(1)抗重放攻击:每条认证消息为 $\{sig,M\}$,其中 $M=\{VID,ID_u,m,Time_u,sig\}$ 包含时间戳 $Time_u$,验证方可以通过检查时间戳 $Time_{cur}-Time_u\leqslant\Delta Time$ 来判断签名的新鲜度。因此本文方案可以有效防止重放攻击。

(2)抗中间人或假冒攻击:本方案的安全性基于椭圆曲线离散对数问题(ECDLP)的难度,方案中每条消息都包含了用户 $USER_{Applicant,u}$ 的签名 sig,如果攻击者想要伪造一个合法的用户去发送消息,它需要在该消息附上签名。由前文的定理 1 可知,攻击者无法通过伪造合法用户生成有效签名。每个签名都应该进行签名验证,若验证失败则该签名无效。因此,能够抵御中间人和假冒攻击。

(3)密钥托管弹性:在本文方案中,用户 $USER_{Applicant,u}$、身份管理节点 $ATTR_i$ 和用户身份的私钥 $SK=\{x,y\}$,其中包括用户随机选取的秘密值 x 和 KGC 计算的部分私钥 y。由于恶意 KGC 在未知用户随机秘密值 x 的条件下无法构造出合法有效的签名,因此该方案能够有效避免密钥托管问题带来的安全隐患。

(4)前向与后向安全性:在本文方案中,如果敌手获得某个认证消息 M。其中,$\sigma=h_\sigma(x_u+b+\sum_{i=1}^{t}c_i x_{u,i}+\sum_{i=1}^{t}c_i e_i x_u+\sum_{i=1}^{t}d_i)+y_u$,其中参数 b 为在每一次不同的签名中选择的不同随机值,h_σ 和 c_i 由不同的消息 m、时间戳 $Time_u$ 以及 $B=bP$ 经过单向哈希函数计算得出。因此,敌手无法通过当前认证消息推断出其他认证消息的内容。

6 性能分析

鉴于目前尚缺乏直接支持"支持多重身份的一次性认证"的同类工作,为保证对比的公平性与代表性,本文选取无证书单身份认证方向的四个普遍且可复现的研究[38-41]作为对照基线。所选方案覆盖双线性对/非配对两类典型密码实现,面向 IoT/IIoT 等通用场景,且其安全模型与假设与本文相近,便于在统一参数下复现实验,可客观呈现本文在计算与通信开销上的改进。

仿真实验在 6 GB 运行内存的 Ubuntu 18.04.6 64 位环境下实现,硬件环境为 Windows 10 IoT LTSC 操作系统,配备 i5-11400H 2.70GHz 处理器和 16GB 运行内存。区块链实验平台采用 Hyperledger Besu 搭建以太坊网络,配置 IBFT2.0 共识协议与标准以太坊 JSON-RPC 接口。密码实现基于 Charm-Crypto 函数库完成,所有密码学原语均在同一环境下独立执行 100 次并取平均值作为结果,密码运算结果见表 3,鉴于大整数模加与模乘的单位时间开销过小,故未将其纳入后续性能对比。在本文的多重身份认证方案中,n 表示系统中各个行业领域的身份管理节点数量,t 表示签名方持有的身份数量。

表 3 密码运算时间

符号	运算操作	运行时间
T_h	单向哈希函数	0.0006
T_H	映射到点的哈希函数	2.3916
T_{GA}	椭圆曲线点加运算	0.0027
T_{GM}	椭圆曲线点乘运算	0.9584
T_{Par}	双线性对运算	2.4627
T_L	拉格朗日插值运算	$T(n-t+1)$

6.1 计算开销

本文计算开销特指方案在密码学层面的本地计算耗时,用于描述签名与验证阶段所需的运算量与时间。在文献[38]中,签名方在签名阶段需执行 3 次椭圆曲线点乘、2 次椭圆曲线点加以及 2 次映射到点的哈希运算符,因此签名阶段总开销为 $3T_{GM}+2T_{GA}+2T_H$;验证阶段需执行 4 次双线性对与 2 次映射到点的哈希运算,其总开销为 $4T_{Par}+2T_H$。通过类似的分析,可分别得到文献[38-41]在签名与验证阶段的计算开销。对本文方案而言,在签名构造中将各节点对重复数据的处理设计为可并行执行且彼此独立,从而降低单方重复计算的频率。在签名阶段,需执行 4 次椭圆曲线点乘、2 次椭圆曲线点加、1 次拉格朗日插值以及 3 次单向哈希运算,因此总开销为 $4T_{GM}+2T_{GA}+T_L+3T_h$;在验证阶段,需执行 3 次椭圆曲线点乘、$t+3$ 次椭圆曲线点加与 2 次单向哈希运算,故总开销为 $3T_{GM}+(t+3)T_{GA}+2T_h$,其中 t 为签名方的身份数量。进一步结合各方案的具体构造,可推得批量场景下(消息条数为 k)的签名与验证的计算开销,签名与验证计算开销形式化对比如表 4 所示。

表 4 签名与验证计算开销形式化对比

方案	计算量/ms	
	签名	验证
方案[38]	$3kT_{GM}+2T_{GA}+(k+1)T_H$	$(3k+1)T_{Par}+(k+1)T_H$
方案[39]	$4kT_{GM}+2kT_{GA}+kT_H+2kT_h$	$(k+2)T_{GM}+(k+3)T_{Par}+kT_H+(k+2)T_h$
方案[40]	$(2k+3)T_{GM}+(k+2)T_{GA}+kT_H+2T_h$	$2kT_{GM}+2kT_{GA}+2kT_{Par}+2T_h$
方案[41]	$kT_{GM}+2kT_h$	$4kT_{GM}+3kT_{GA}+(2k+1)T_h$
本文方案	$(k+3)T_{GM}+2T_{GA}+kT_L+(2k+1)T_h$	$(2k+1)T_{GM}+(kt+2k+1)T_{GA}+(k+1)T_h$

本文方案中,拉格朗日插值运算时间取决于项数 $n-t+1$,其中 t 表示用户持有的身份数量,n 表示网络环境中身份管理节点的数量。在将各个方案置于一致身份条件下进行评估时,当 $t=1$、$n=15$ 且重复执行 100 次时,测得 T_L 平均运行时间为 0.5442 ms。基于上述设置,不同方案的签名与验证阶段计算开销对比如图 6 所示。在消息数量递增的情形下,签名与验证阶段的时间变化分别见图 6(a)和图 6(b)。

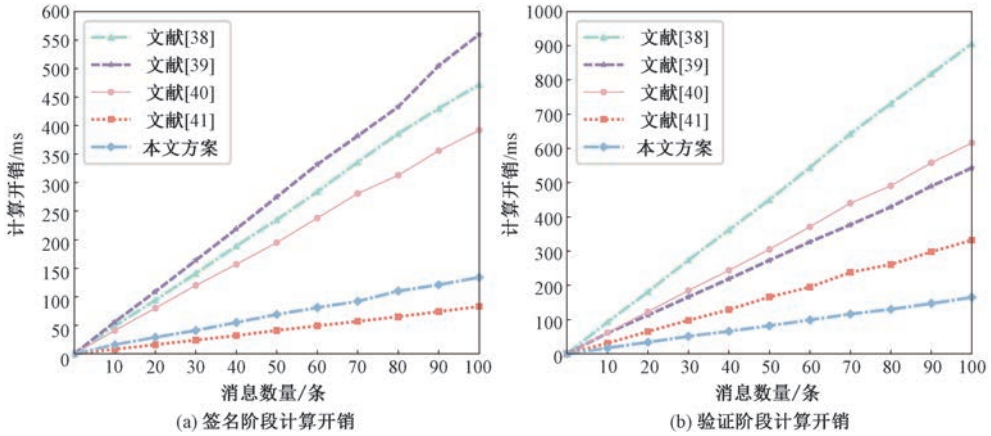


图 6　不同方案的签名与验证阶段计算开销对比

由表 3 与图 6 可见,文献[38-41]在签名与验证两个阶段的时间开销均显著高于本文方案,但本文方案在签名阶段的时间开销高于文献[41],其原因在于为获得更强的认证灵活性,本文方案设计中令全部 n 个身份管理节点参与部分签名参数的生成,因而引入了额外计算负载。尽管如此,本文方案在验证阶段的计算开销明显低于其余对比方案,进而在总体计算开销上保持优势。不同方案的签名与验证计算总开销形式化对比见表 5。

表 5　不同方案的签名与验证计算总开销形式化对比

方案	计算量/ms
	签名与验证
方案[38]	$3kT_{GM}+2T_{GA}+(3k+1)T_{Par}+(2k+2)T_H$
方案[39]	$(5k+2)T_{GM}+2kT_{GA}+(k+3)T_{Par}+2kT_H+(3k+2)T_h$
方案[40]	$(4k+2)T_{GM}+(3k+2)T_{GA}+2kT_{Par}+kT_H+4T_h$
方案[41]	$5kT_{GM}+3kT_{GA}+(4k+1)T_h$
本文方案	$(3k+4)T_{GM}+(kt+2k+3)T_{GA}+kT_L+(3k+2)T_h$

从图 7 可见,本文方案在两阶段计算时间上整体优于对比方案。造成差异的关键在于计算开销的构成,双线性对运算 T_{Par} 和椭圆曲线上的点乘运算 T_{GM} 通常主导运算开销,本文方案通过摒弃双线性对运算,避免了高开销的 T_{Par};同时在保证安全性的前提下压缩点乘调用次数,使得总体计算量得到控制。结合表 5 给出的形式化开销可知,本文方案的 T_{GM} 系数更低;随着消息数量增加,虽然与消息规模相关的系数项线性增长,但其斜率较小,因而对总时间的边际影响有限。与图 7 折线趋势相印证,当认证消息规模扩大时,本文方案在总计算时间上的相对优势进一步扩大,表明其在大规模认证场景中具有更好的可扩展性和效率表现。

本文方案在物联网动态场景下仍可保持认证功能的正确性,不同(t,n)条件下本文方案的认证计算

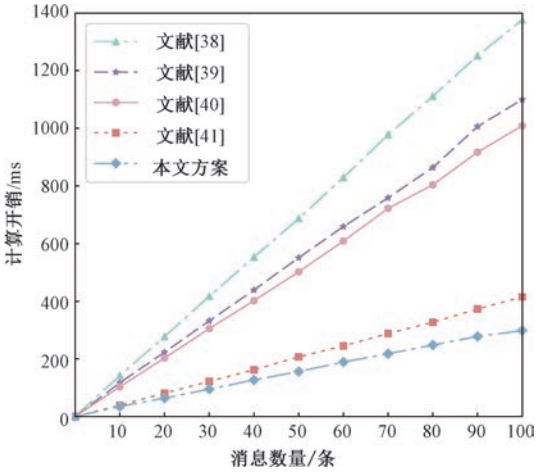


图 7　不同方案的签名与验证总计算开销对比

开销变化见图 8,为便于观测趋势,在给定同一批消息的前提下将消息数量固定为 10。

对于图 8(a),用户持有的身份数量 t 保持不变,而身份管理节点数 n 随接入而增大。由于拉格朗日插值多项式的项数为 $n-t+1$,n 的增长将带来项数相应增加,故签名阶段的计算开销呈小幅上升;验证阶段主要受 t 影响,因 t 未变化,验证开销呈相对稳定趋势。

对于图 8(b),t 与 n 同步增减,使得 $n-t+1$ 保持不变,因此拉格朗日插值运算代价相对稳定,且其余操作并未增加,整体签名开销保持稳定;验证阶段随 t 增长而增加的主要是椭圆曲线点加操作数 T_{GA},但由于 T_{GA} 的单位计算量级较小,其对验证时间的边际影响有限,表现为缓慢上升或近似稳定的趋势。

由此可见,随着用户持有身份数量 t 的增加,本方案在签名与验证两个阶段均能将开销增长控制在可预期范围内,体现出对多重身份条件的良好可扩展性与可控性,适用于多身份认证场景。

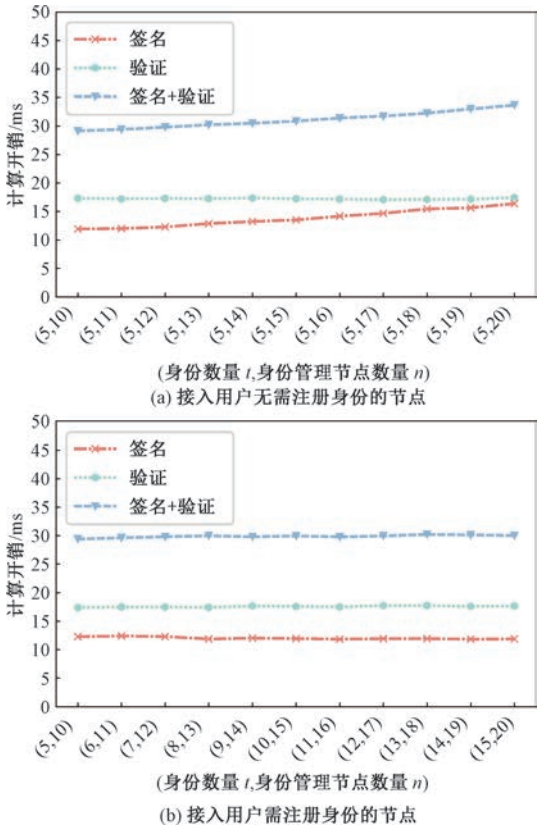


图 8 不同(t,n)条件下的认证计算开销变化

6.2 认证时延

本文认证时延用于反映方案在区块链部署环境中端到端的实际表现,覆盖从提交认证请求到完成签名验证并获得链上确认或读取结果的整体时间。本文的区块链实验平台基于 Hyperledger Besu 搭建以太坊网络,配置 IBFT2.0 共识协议与标准以太坊 JSON-RPC 接口,默认出块周期为 2 s。在进行 1000 次实测后可得到从提交到链上确认的延迟范围为 1.2 s～2.2 s,主要由网络往返、交易传播、打包等待、共识执行、持久化与状态更新等环节构成;读取延迟范围为 0.1 s～0.2 s,包括网络往返、请求处理以及 IPFS 访问等因素;其余延迟受传输距离与网络吞吐量影响,存在一定波动。

在 $t=1$,$n=15$ 的设置下,本文方案于上述实际区块链环境中运行。在消息数量递增的情形下,签名、验证以及两阶段认证时延如图 9 所示,该实验取 100 次平均结果。在实际传输环境中,各种延迟占据认证流程的主要部分,但总体趋势与计算开销的结果一致。

在身份管理节点的动态接入环境下,图 10 给出了注册时延的测量结果。图 10(a)展示了用户无需在该节点注册身份的情形,仅需完成节点注册;如果若干节点的注册请求能够在同一出块周期内被打包

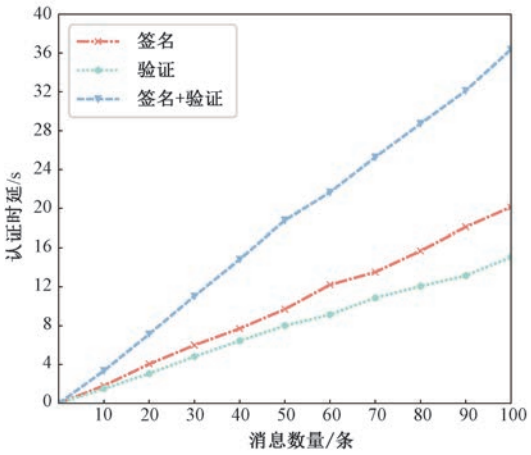


图 9 不同消息数量的认证时延

并达成共识,则其公钥上链可通过一次共识完成,整体注册时延较短;但随着并发接入节点数增加,网络拥塞、交易调度与打包不确定性上升,部分节点的注册可能溢出至后续出块周期,导致接入时延出现不稳定与抖动。图 10(b)展示了用户需要在该节点注册身份的情形,在完成节点注册后,还需执行用户身份注册,两者存在串行依赖,因而通常难以在同一出块周期内全部完成;在最佳情况下,可于第二个出块周期内完成用户身份注册。多节点注册本身可能超出单一出块周期,身份注册也会存在顺延概率,故整体时延同样呈现不稳定性。

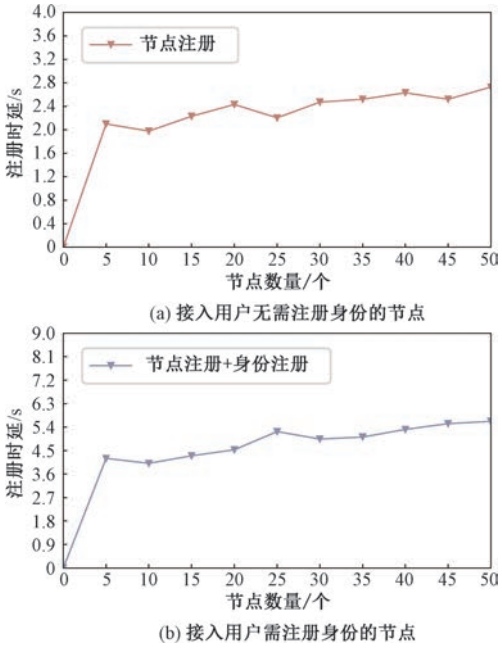


图 10 实际环境下的注册时延

不同(t,n)条件下本文方案的认证时延变化如图 11 所示,由于在实际环境中有各种延迟,为便于观测趋势,在给定同一批消息的前提下将消息数量

固定为 10。在实际传输环境中,环境中的各种延迟占据认证流程主要部分,但总体趋势与理想环境中的结果一致。

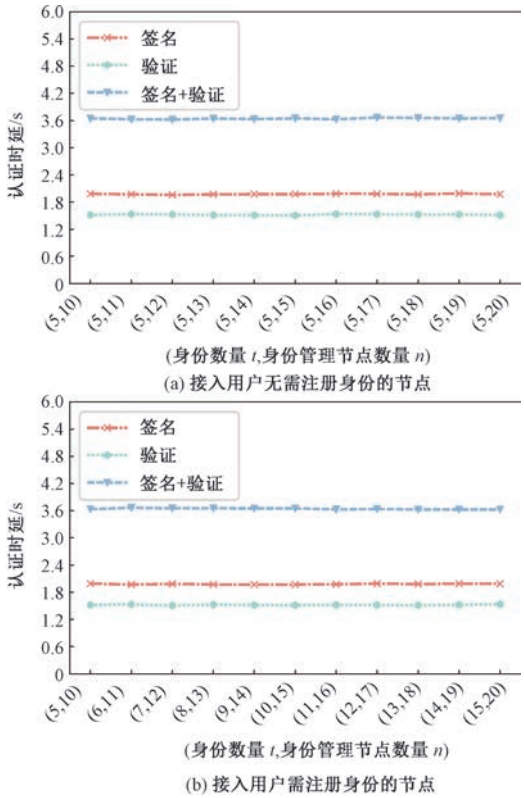


图 11　不同(t,n)条件下的认证时延变化

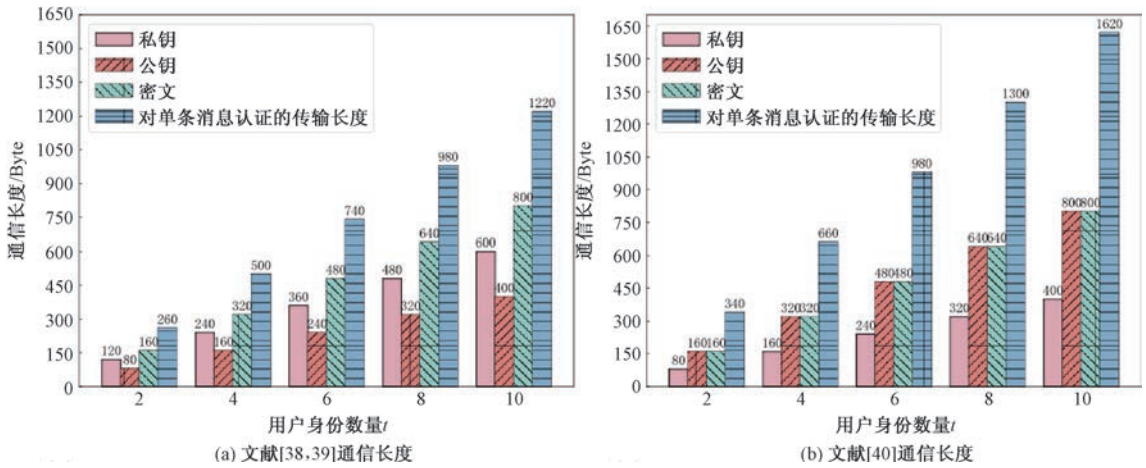
6.3　通信开销

在通信量评估中,设定 Z_q^* 中的元素大小为 20Byte,椭圆曲线群 G 中元素大小为 40Byte,经双线性映射后的群 G_1 中元素大小为 128Byte,消息 m 大小为 20Byte,身份标识和时间戳通信开销较小可忽略,故不纳入对比。通信量对比如表 6 所示,其中 t 表示用户持有的身份数量。

本文方案支持多重身份的联合认证,针对同一消息 m,可在不增加密文长度与额外传输负担的前提下,同时利用多身份完成签名与验证。相比之下,其他对比方案需要为每个身份分别生成并传输完整的认证信息(如密文以及相应的公钥等),使得密文与传输开销随身份数量 t 呈显著线性增长。图 12 进一步直观展示了不同 t 条件下的通信长度对比,一方面,密钥的存储规模随 t 不可避免地线性增长;另一方面,在固定消息条数下,本文方案的认证传输长度随 t 的增幅显著较小,而对比方案增幅较大。由此可见,本文方案在多身份并发认证场景下具备显著的通信效率优势。

表 6　通信量对比

方案	通信量/Byte			
	私钥	公钥	密文	对单条消息认证的传输长度
方案[38]	$t\|Z_q^*\|+t\|G\|=60t$	$t\|G\|=40t$	$2t\|G\|=80t$	$\|m\|+3t\|G\|=120t+20$
方案[39]	$t\|Z_q^*\|+t\|G\|=60t$	$t\|G\|=40t$	$2t\|G\|=80t$	$\|m\|+3t\|G\|=120t+20$
方案[40]	$2t\|Z_q^*\|=40t$	$2t\|G\|=80t$	$2t\|G\|=80t$	$\|m\|+4t\|G\|=160t+20$
方案[41]	$2t\|Z_q^*\|=40t$	$2t\|G\|=80t$	$t\|Z_q^*\|+t\|G\|=60t$	$\|m\|+t\|Z_q^*\|+3t\|G\|=140t+20$
本文方案	$(2t+2)\|Z_q^*\|=40t+40$	$(2t+2)\|G\|=80t+80$	$\|Z_q^*\|+\|G\|=60$	$\|m\|+\|Z_q^*\|+(2t+3)\|G\|=80t+160$



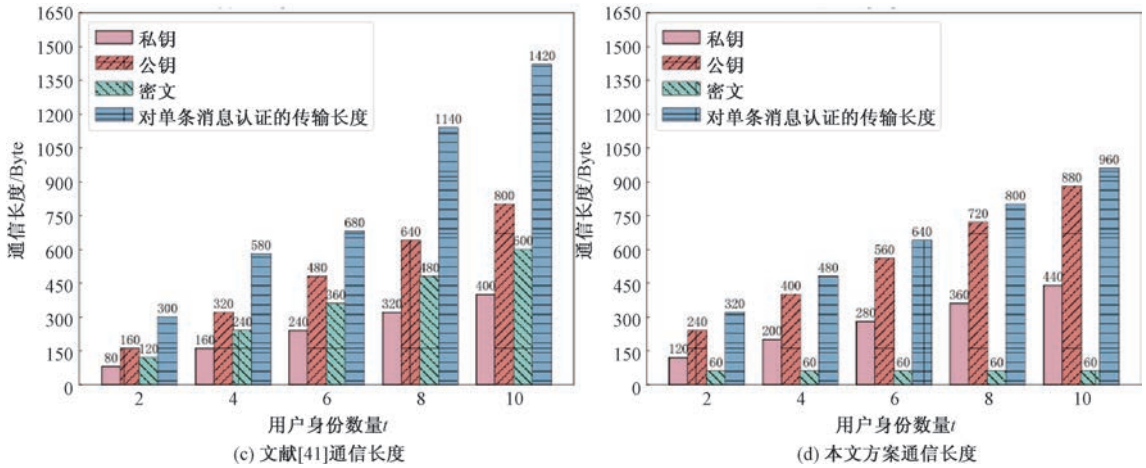


图 12 不同身份数量条件下的通信长度

7 结束语

针对物联网多重身份认证需求，本文提出了一种基于区块链的物联网无证书多重身份认证方案。该方案利用链上共识与不可篡改存储实现公开参数的可信共享，结合轻量级 ECC 与属性签名实现多身份的细粒度管理，并通过多重身份的部分签名聚合实现单次验证，能够在保证安全性的同时降低计算开销。实验结果表明，当消息规模与身份数量增大时，系统仍能保持良好的效率与可扩展性。需指出的是，当前工作主要面向通用物联网设备，尚未覆盖极端资源受限终端（如超低功耗传感器）的轻量化适配与预评估。在下一步研究工作中，将针对该类场景开展协议设计与参数优化，并进行面向边缘/超嵌入式设备的系统性性能与安全评测。

参 考 文 献

[1] SHAMIR A. How to share a secret. Communications of the ACM, 1979, 22(11): 612-613

[2] Khan S, Luo F, Zhang Z J, et al. A survey on X.509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2529-2568

[3] Harn L, Ren J. Generalized digital certificate for user authentication and key establishment for secure communications. IEEE Transactions on Wireless Communications, 2011, 10(7): 2372-2379

[4] Son S, Lee J, Park Y, et al. Design of blockchain-based lightweight V2I handover authentication protocol for VANET. IEEE Transactions on Network Science and Engineering, 2022, 9(3): 1346-1358

[5] Bao H, Zhao Y J, Zhang X P, et al. A probabilistic and distributed validation framework based on blockchain for artificial intelligence of things. IEEE Internet of Things Journal, 2024, 11(1): 17-28

[6] Zhang Y, Xu C X, Lin X D, et al. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Transactions on Cloud Computing, 2021, 9(3): 923-937

[7] Zhou X T, He D B, Khan M K, et al. An efficient blockchain-based conditional privacy-preserving authentication Protocol for VANETs. IEEE Transactions on Vehicular Technology, 2023, 72(1): 81-92

[8] Wang Y H, Peng C, Jia X Y, et al. Pairing-free blockchain-assisted certificateless aggregation signcryption Scheme for VANETs. IEEE Internet of Things Journal, 2025, 12(11): 15545-15557

[9] Yao C, Zhang X J, Liu Y Z, et al. Blockchain-based secure and efficient ADS-B authentication via certificateless signature with packet loss tolerance. IEEE Internet of Things Journal, 2025, 12(8): 10574-10588

[10] Leng J W, Zhou M, Zhao J L, et al. Blockchain security: A survey of techniques and research directions. IEEE Transactions on Services Computing, 2022, 15(4): 2490-2510

[11] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[12] Park K W, Lim S S, Park K H. Computationally efficient PKI-based single sign-on protocol, PKASSO for mobile devices. IEEE Transactions on Computers, 2008, 57(6): 821-834

[13] Zhang Zhan-Peng, Li Ke-Xin, Kan Hai-Bin. An open blockchain oracle scheme based on decentralized identity. Journal of Computer Research and Development, 2023, 60(11): 2489-2503(in Chinese)
(张展鹏，李可欣，阚海斌. 基于去中心化身份的开放区块链预言机方案. 计算机研究与发展，2023，60(11)：2489-2503)

[14] Shamir A. Identity-based cryptosystems and signature

schemes//Proceedings of the 1984 Advances in Cryptology. Berlin, Germany, 1984:47-53

[15] Li X C, Zhou L F, Yin X C, et al. A security-enhanced certificateless designated verifier aggregate signature scheme for HWMSNs in the YOSO model. IEEE Internet of Things Journal, 2024,11(6):10865-10879

[16] Wei Song-Jie, Li Sha-Sha, Wang Jia-He. A cross-domain authentication protocol by identity-based cryptography on consortium blockchain. Chinese Journal of Computers, 2021,44(5):908-920(in Chinese)
(魏松杰,李莎莎,王佳贺.基于身份密码系统和区块链的跨域认证协议.计算机学报,2021,44(5):908-920)

[17] Zhao H W, Bai P D, Peng Y, et al. Efficient key management scheme for health blockchain. CAAI Transactions on Intelligence Technology, 2018,3(2):114-118

[18] Peng Chang-Gen, Long Yang-Yang, Chen Yu-Ling. Verifiable distributed key generation using blockchain and CP-ABE. Chinese Journal of Computers, 2025,48(6):1342-1355(in Chinese)
(彭长根,龙洋洋,陈玉玲.基于区块链与 CP-ABE 的可验证分布式密钥生成协议.计算机学报,2025,48(6):1342-1355)

[19] Matsumoto S, Reischuk R M. IKP: Turning a PKI around with blockchains. IACR Cryptology ePrint Archive, 2016, 2016:1018

[20] Al-Bassam M. SCPKI: a smart contract-based PKI and identity system//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. New York, USA, 2017:35-40

[21] Chaum D, Antwerprn H V. Undeniable signatures//Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology. New York, USA, 1989: 212-216

[22] Al-Riyami S S, Parterson K G. Certificateless public key cryptography//Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2003:452-473

[23] Zhang Y H, Deng R H, Zheng D, et al. Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. IEEE Transactions on Industrial Informatics, 2019,15(9):5099-5108

[24] Thumbur G, Rao G S, Reddy P V, et al. Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices. IEEE Communications Letters, 2020,24(8):1641-1645

[25] Xu Z Y, Luo M, Khan M K, et al. Analysis and improvement of a certificateless signature scheme for resource-constrained scenarios. IEEE Communications Letters, 2021,25(4):1074-1078

[26] Wang W Z, Xu H, Alazab M, et al. Blockchain-based reliable and efficient certificateless signature for IIoT devices. IEEE Transactions on Industrial Informatics, 2022,18(10): 7059-7067

[27] Wang X C, Wang W, Huang C, et al. Blockchain-based certificateless conditional anonymous authentication for IIoT. IEEE System Journal, 2024,18(1):656-667

[28] Srivastava V, Debnath S K, Bera B, et al. Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for internet of vehicles environment. IEEE Transactions on Vehicular Technology, 2022,71(9):9853-9867

[29] Yuan He-Xin, Liu Bai-Xiang, Kan Hai-Bin, et al. Distributed public key infrastructure scheme based on blockchain and decentralized undeniable attribute-based signature. SCIENTIA SINICA Informationis, 2022,52(6):1135-1148(in Chinese)
(袁和昕,刘百祥,阚海斌等.基于区块链和去中心不可否认属性签名的分布式公钥基础设施方案.中国科学:信息科学,2022,52(6):1135-1148)

[30] Zhang Yu-Long, Wen Long, Wang Hao-Hao, et al. Certificateless authentication searchable encryption scheme for multiuser. Journal of Electronics & Information Technology, 2020,42(5):1094-1101(in Chinese)
(张玉磊,文龙,王浩浩等.多用户环境下无证书认证可搜索加密方案.电子与信息学报,2020,42(5):1094-1101)

[31] Yang N B, Tang C M, He D B. A lightweight certificateless multi-user matchmaking encryption for mobile devices: enhancing security and performance. IEEE Transactions on Information Forensics and Security, 2024,19:251-264

[32] Liu H, Han D Z, Cui M M, et al. IdenMultiSig: identity-based decentralized multi-signature in Internet of Things. IEEE Transactions on Computational Social Systems, 2023, 10(4):1711-1721

[33] Yu H F, Ren R T. Certificateless elliptic curve aggregate signcryption scheme. IEEE Systems Journal, 2022,16(2): 2347-2354

[34] Yang X D, Wang W J, Tian T, et al. Cryptanalysis and improvement of a blockchain-based certificateless signature for IIoT devices. IEEE Transactions on Industrial Informatics, 2024,20(2):1884-1894

[35] Sashai A, Waters B R. Fuzzy identity-based encryption// Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005:457-473

[36] Ahmed M R, Meenakshi K, Obaidat M S, et al. Blockchain based architecture and solution for secure digital payment system//Proceedings of the IEEE International Conference on Communications. Montreal, Canada, 2021:1-6

[37] Kumar R, Tripathi R, Marchang N, et al. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. Journal of Parallel and Distributed Computing, 2021,152:128-143

[38] Shim K A. A secure certificateless signature scheme for cloud-assisted industrial IoT. IEEE Transactions on Industrial Informatics, 2024,20(4):6834-6843

[39] Kumar P, Kumari S, Sharma V, et al. Secure CLS and CL-AS schemes designed for VANETs. Journal of Supercomputing, 2018,75,3076-3098

[40] He D B, Ma M M, Zeadall S, et al. Certificateless public key authenticated encryption with keyword search for industrial internet of things. IEEE Transactions on Industrial Informatics, 2018,14(8):3618-3627

[41] Ma K, Zhou Y W, Wang Y, et al. An efficient certificateless signature scheme with provably security and its applications. IEEE Systems Journal, 2023,17(4):5636-5647

LIU Yuan-Ni, Ph. D., professor. Her research interests include Internet of Things security, Internet of Vehicles security, and identity authentication.

YIN Yong-Quan, M. S. candidate. His research interest is certificateless authentication.

ZHANG Jian-Hui, Ph. D., professor. His research interests include routing and switching design, routing protocols, resource scheduling, network security and future networks.

ZHOU You-Sheng, Ph. D., professor. His research interests include data security, authentication and key agreement.

Background

This paper investigates a problem in the field of cyber security, specifically focusing on multi-identity authentication in the Internet of Things (IoT), particularly the design of efficient and secure identity verification mechanisms in multi-identity scenarios. With the widespread application of IoT technology in critical infrastructure such as smart cities, industrial control, and the Internet of Vehicles, it has become common for a single entity to possess multiple identities across various business domains. For instance, in intelligent transportation systems, vehicles not only act as traffic participants but also serve as service access terminals and data providers. Therefore, how to achieve flexible and efficient authentication for multiple identities while ensuring the security of the authentication process has become an important research direction in the field of IoT identity management.

Currently, international research on this issue mainly focuses on two aspects: first, using certificateless public key cryptography (CL-PKC) to address the challenges of traditional certificate management and key escrow, thereby enhancing the system's lightweight and security; second, leveraging blockchain technology to achieve trusted storage of public parameters and decentralized authentication architecture, eliminating the security risks of centralized trust models. However, existing research mostly focuses on single identity authentication or only supports repetitive verification of multiple identities, and is still unable to meet the requirements of unified management and one-time verification of multiple identities. Moreover, some identity authentication schemes still rely on computationally intensive bilinear pairing operations, which are difficult to adapt to the resource-constrained environment of IoT devices.

This paper proposes a blockchain-based certificateless multi-identity authentication scheme for the IoT. This scheme integrates certificateless signature and attribute signature technologies and introduces a multi-identity signature aggregation mechanism to achieve one-time verification of multiple identities. This design reduces the number of authentication interactions and computational overhead while ensuring the security and efficiency of the system. Through formal security analysis, it is proven that the scheme can effectively resist adaptive chosen-message attacks; experimental evaluations further demonstrate that, compared with existing methods, this scheme significantly improves the authentication efficiency in multi-identity scenarios.

The presented work is supported by the funds from the National Key R&D Program of China under Grant No. 2023YFB3105901 and the National Natural Science Foundation of China under Grant No. 62272076.