计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250100131

面向物资供应链的隐私保护多主体跨证书体系认证及访问控制模型

杨 珂[1] 郭庆雷[2,3] 沈一鸣[4] 柏 能[4] 宋文婷[5] 王伟宇[2,3]
1 国网数字科技控股有限公司 北京 100077
2 国网区块链科技(北京)有限公司 北京 100077
3 国网区块链应用技术实验室 北京 100077
4 国网江苏省电力有限公司物资分公司 南京 210036
5 国家电网有限公司大数据中心 北京 100052
(keyang@amss.ac.cn)

摘 要 在推动物资供应链现代化的过程中,电子化数据管理已成为政府和企业采购的关键手段,对于增强市场竞争力和确保交易公平性具有决定性影响。然而,电子采购在招投标阶段面临诸多挑战,包括电子数据来源的多样性导致可信度不一、投标人隐私保护难题以及招投标人之间的潜在共谋风险。区块链技术以其去中心化、分布式账本和透明度高的特性,与电子采购中参与者分散的特点高度契合。针对上述挑战,提出了一种面向物资供应链的隐私保护多主体跨证书体系认证方案。该方案通过智能合约维护信任列表,结合高效的 Merkle 树签名实现低存储开销的证书签发,既确保了证书颁发机构和投标方的可信性,又优化了跨域证书验证流程,进一步提升了认证过程的透明性与一致性。同时,采用属性基加密对投标方敏感数据加密存储,设置细粒度访问控制,仅授权招标方访问必要信息,有效防范开标前的共谋风险,保障投标过程的公平与透明。严格的安全性分析和仿真测试表明,所提方案在实现多主体跨证书体系认证的同时,能够保障投标人隐私,并提供灵活的访问控制。

关键词:物资供应链;跨证书体系认证;智能合约;隐私保护;属性基加密
中图分类号 TP309

Privacy-preserving Cross-certificate System Authentication and Access Control Model for Material Supply Chain

YANG Ke[1],GUO Qinglei[2,3],SHEN Yiming[4],BAI Neng[4],SONG Wenting[5] and WANG Weiyu[2,3]
1 State Grid Digital Technology Holding Co.,Ltd.,Beijing 100077,China
2 State Grid Blockchain Technology(Beijing) Co.,Ltd.,Beijing 100077,China
3 State Grid Blockchain Application Technology Laboratory,Beijing 100077,China
4 State Grid Jiangsu Electric Power Co.,Ltd.,Materials Branch,Nanjing 210036,China
5 Big Data Center of State Grid Corporation of China,Beijing 100052,China

Abstract Electronic data management has emerged as a pivotal tool for government and corporate procurement in the process of modernizing material supply chains,which plays a decisive role in boosting market competitiveness and ensuring fairness in transactions. However,electronic procurement faces several challenges,especially during the bidding process. These include the varying credibility of diverse electronic data sources,the difficulty of protecting bidders' privacy,and potential risks of collusion between bidders and procurers. Blockchain technology,with its decentralized structure,distributed ledger,and high transparency,aligns well with the distributed nature of participants in electronic procurement. To address these challenges,this paper proposes a privacy-preserving multi-entity cross-certificate authentication and access control model for material supply chains. The system utilizes smart contracts to maintain a trust list and employs efficient Merkle tree signatures for certificate issuance with minimal storage overhead. This ensures the trustworthiness of both certificate authorities and bidders,while optimizing the cross-domain certificate verification process,further enhancing the transparency and consistency of authentication. Additionally,the system employs attribute-based encryption to encrypt and store sensitive data from bidders. Fine-grained access control is implemented to allow only authorized procurers to access the necessary information,effectively preventing collusion risks before the bid opening and ensures fairness and transparency in the bidding process. Rigorous security analysis and simulation tests demonstrate that the proposed solution not only supports multi-entity cross-certificate system authentication,but also safeguards bidder privacy,providing flexible and robust access control.

基金项目:国家电网公司总部科技项目(5700-202418240A-1-1-ZN)
This work was supported by the Science and Technology Project of State Grid Electric Power Co.,Ltd.(5700-202418240A-1-1-ZN).
通信作者:郭庆雷(guoqinglei@sgdt.sgcc.com.cn)

Keywords Material supply chain, Cross-certificate system authentication, Smart contract, Privacy preservation, Attribute-based encryption

1 引言

供应链安全是国家战略安全的重要组成，保障着经济的正常运行，促进社会的发展和民生的改善。党的十九大以来，党中央站在全局和战略高度，将“提升产业链、供应链现代化水平”写入“国民经济和社会发展第十四个五年规划和2035年远景目标纲要”。2021年国务院印发《关于加快建立健全绿色低碳循环发展经济体系的指导意见》[1]，提出构建绿色供应链，提高行业供应链现代化水平。政府和企业采购的电子化转型，不仅提高了采购效率和市场竞争力，还能推动数字化转型，依托区块链、隐私计算等新技术，实现业务公开、过程受控、全程在线、永久可追溯，对供应链的绿色安全发展具有重要意义。

随着物资供应链现代化需求的不断增长，供应链物资采购市场逐步成熟，电子采购存在巨大的发展潜力。然而，在当前电子采购的开标投标过程中，仍然面临投标人敏感隐私信息保护不足、跨证书体系认证混乱以及招投标人共谋等问题。在多方参与的物资供应链环境中，通常存在多个证书颁发机构(Certificate Authority, CA)，其作为认证中心，负责为其管理的主体颁发数字证书以确认他的可信身份。在这种多源信任模型下，如何高效地验证每个主体的数字证书的有效性，并进行大规模证书管理，成为一项巨大的挑战。传统的公钥基础设施(PKI)方案依赖于集中管理大量证书并实时维护完整的证书列表。在跨多个CA和海量用户的复杂认证环境中，PKI面临着显著的效率瓶颈和管理复杂性，这限制了其在大规模系统中的可行性和应用效果。

为解决上述问题，区块链技术凭借其去中心化、不可篡改及高透明的特性，提供了一种有效方案。通过分布式账本技术，区块链能够在多CA之间建立可靠的信任机制，确保CA节点信息的全网共享与监督，同时保障其签发数字证书的有效性与可信度。其分布式结构提升了跨域证书验证的效率，降低了传统认证机制的管理负担，并确保了证书验证及跨域认证的透明性与一致性，进一步增强了整体认证体系的安全性与可靠性。此外，区块链技术与电子采购系统中多方参与、敏感数据保护和不可见数据访问的需求相吻合，能够有效支持跨证书体系认证并确保数据隐私保护。

针对区块链中的跨域认证方案，已经有学者进行了深入研究。Wang等[2]基于区块链技术提出了可追踪匿名跨域认证方案，既保护了隐私数据，又能够恢复恶意设备的真实身份。Tian等[3]提出基于联盟链的细粒度安全访问控制机制，用于实现跨域的访问控制。此外，区块链技术在供应链电子采购中的应用也有诸多研究。Fan等[4]提出了一种创新的电子招标协议，旨在增强投标人的匿名性。Xu等[5]则提出了一种基于云计算的招投标系统，通过云计算的存储和处理能力，提高了数据处理效率。2018年，文献[6]开发了基于区块链的电子投标机制，确保电子印章的保密性、不可否认性和不可更改性。文献[7]提出了一种新机制，规定只有指定负责人能够检查投标者签名的有效性，从而增强了电子招投标系统的安全性。同年，文献[8]引入了智能合约，提供了公开和密封投标选项。文献[9]提出了一种基于区块链的可信电子招投标系统，旨在提升招投标过程的效率和安全性。文献[10]提出了一个基于区块链的公开竞价拍卖系统框架，增强了拍卖人和投标人之间的安全性。文献[11]提出了一种基于以太坊区块链的解决方案，确保了数据的完整性和透明度，并降低了成本。文献[12]将大数据技术融入电子招投标系统，提高了招投标过程的透明度和监管能力。

通过上述文献可知，现有的研究利用区块链、智能合约、大数据等技术设计了电子采购系统，提升了系统的安全性和公平性。然而，现有工作尚未提出适用于物资供应链的跨证书认证体系，也未充分考虑投标人敏感隐私信息的保护，如投标报价。此外，现有系统没有针对招投标人共谋场景进行设计，无法满足分布式投标方在保障敏感数据可用的同时确保其不可见的需求。

为解决上述问题，本文设计了一种面向物资供应链的隐私保护多主体跨证书体系认证模型。具体而言，首先，针对认证涉及不同可信证书体系的投标方，本文采用Merkle树签名方案，并结合智能合约，通过维护CA和投标人列表，以高效且低存储开销的方式验证数字证书的有效性，确保CA和投标方的可信度，从而解决多主体跨证书体系认证的挑战。该机制不仅优化了跨CA的证书验证流程，还保证了认证过程的透明性与一致性。其次，为防止投标人数据泄露，本文结合属性基加密算法对投标方的所有敏感数据进行加密存储，并设计了细粒度的访问权限控制策略，确保只有授权的招标人能够访问必要的投标信息。这一机制有效避免了在开标前招投标人之间的共谋风险，从而进一步保障了投标过程的公平性和透明性。最后通过严格的安全证明和仿真测试，证明了该方案在兼顾有效保护投标人隐私数据、多主体跨证书体系认证方面的价值。

2 技术组件

2.1 签名Merkle哈希树

Merkle树由Ralph Merkle于1979年提出，是一种用于验证大规模数据完整性的数据结构[13]。它通过递归分割数据并计算每个子节点的哈希值，最终生成根哈希值，从而在进行数据完整性验证时，只需对根哈希值进行验证，无需检查每个单独的数据块。相比于传统的集中式PKI认证，显著提高了效率和减少了存储开销。这种结构正是利用哈希函数的不可逆性和抗碰撞特性，一旦数据发生任何篡改，相关哈希值即会发生变化，进而影响根哈希值。因此，根据这种变化，就能实现对数据篡改的有效检测。

Merkle树的优势在于其高效性和安全性，尤其适用于数字签名和大规模证书验证的场景[14]。为实现跨证书体系认证，签名Merkle哈希树(Signed Merkle Hash Tree, sMHT)可有效解决该场景中的验证问题。具体地，CA首先初始化生成大量密钥对，并将每个公钥的哈希值存储至Merkle树的叶子节点中。同时，CA将每个公钥对应的私钥保存在安全的存储介质中(如密封链式存储)。凭借Merkle树的层级结构，CA能够为每个主体分配一个唯一的密钥对(对应的数据

块尚未使用），且该公钥的哈希值已存于 Merkle 树的叶子节点。随后，CA 使用此公钥相应的私钥对每个主体所提供的身份信息进行签名，从而确保其已被 CA 合法授权。通过计算根哈希值和认证路径，最终验证时，只需比对根哈希值与主体所属哈希链计算出的整体哈希值是否匹配，即可确认证书的一致性，无需逐一验证其他信息。这种方法实现了高效的证书存储管理，并能满足跨组织、跨域认证的需求。

2.2　属性基加密

属性基加密（Attribute-based Encryption，ABE）[15] 作为一种先进的一对多公钥加密技术，在数据保护和访问控制方面展现了巨大的潜力。它尤其适用于保护低信任存储环境（如公共云服务器）中的数据机密性，并实现灵活而精细的访问控制机制。ABE 允许数据所有者根据访问控制策略定义谁能访问其加密数据，从而提高了数据隐私性和安全性。

ABE 分为两种主要类型：密文策略 ABE（CP-ABE）和密钥策略 ABE（KP-ABE）[15]。在 CP-ABE 中，密钥生成中心（KGC）根据每个数据请求用户的属性集生成私钥，允许数据所有者为每个加密数据定义一个访问策略。只有当请求用户的私钥所包含的属性集与数据所有者所生成密文中定义的访问策略相匹配时，用户才能解密数据。这种机制确保了数据所有者对自己数据的控制权。与此不同，KP-ABE 的策略和属性位置互换，将请求用户的访问策略嵌入私钥中，而加密的密文则包含数据所有者的属性集。在 KP-ABE 中，解密的权限依赖于私钥中的访问策略和加密文档中的属性集，因此更适合用于广播加密场景，在此场景中，数据可以广播给多个用户，但只有符合条件的用户才能解密。

在跨证书体系认证过程中，采用 ABE 能够确保只有满足特定条件的招标人才能访问敏感投标数据，而区块链提供的去中心化和不可篡改特性则保证了整个过程的透明性和安全性。通过这种方式，既可以保护投标人的隐私数据，又能保证各参与方的可信度和认证过程的高效性。特别地，在第 5.1 节中验证了所设计方案的正确性，第 5.2 节则分析了其安全性，而第 6 章的实验仿真则验证了其先进性和实用性。

2.3　相关密码学定义

定义 1（双线性映射）　设 G_1，G_2 和 G_T 为素数阶 p 的循环乘法群，并设 G_T 为配对映射 e 的值域。若映射 $e: G_1 \times G_2 \rightarrow G_T$ 满足以下性质，则称为双线性映射：

1）双线性：对任意 $a, b \in \mathbb{Z}_p$ 和任意的 $g_1 \in G_1$，$g_2 \in G_2$，有 $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$。

2）非退化性：$e(g_1, g_2) \neq 1$。

3）可计算性：对于所有 $g_1 \in G_1$，$g_2 \in G_2$，计算 $e(g_1, g_2)$ 是高效的。

定义 2（判定型双线性 Diffie-Hellman 假设）　设 $a, b, c, z \in \mathbb{Z}_p$，$g$ 为素数阶 p 的双线性群 G 的一个生成元。判定型 BDH 假设（Decisional BDH，DBDH）认为，在给定（$A = g^a$，$B = g^b$，$C = g^c$，$D = e(g, g)^{abc}$）和（$A = g^a$，$B = g^b$，$C = g^c$，$Z = e(g, g)^z$）的情况下，没有概率多项式时间算法能够以非可忽略的优势区分这两组元素。

定义 3（计算型双线性 Diffie-Hellman 假设）　设 $a, b, c, z \in \mathbb{Z}_p$，$g$ 为素数阶 p 的双线性群 G 的一个生成元。计算型 BDH 假设（Computational BDH，CBDH）认为，在给定（$A = g^a$，$B = g^b$，$C = g^c$）的情况下，没有概率多项式时间算法能够以非可忽略的优势计算出 $e(g, g)^{abc}$。

3　多主体跨证书体系认证模型

隐私保护的多主体跨证书体系认证模型（见图 1）涵盖投标方、招标方、证书颁发机构和监管机构 4 类主体。其中，投标方与招标方作为分布式核心主体，参与电子采购流程并执行相应操作；而证书颁发机构与监管机构承担信任管理职能，确保身份认证与访问控制的安全性。该模型支持异构信任域自主运行身份验证机制，并依托联盟区块链维护跨域公共账本，以实现跨证书多主体间的可信协作与数据一致性。

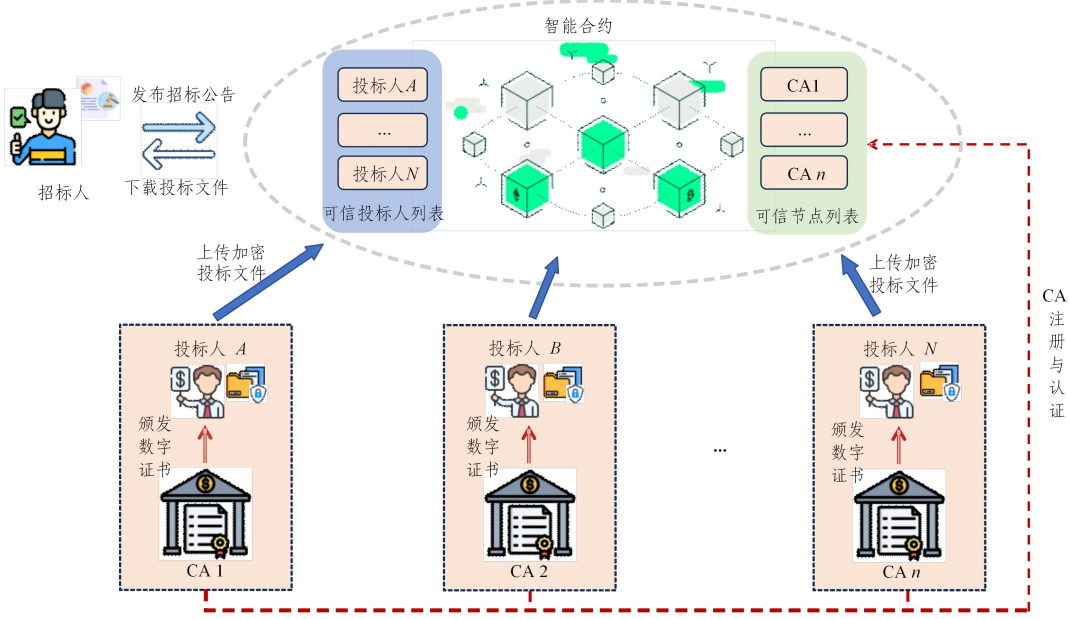

图 1　面向物资供应链的隐私保护多主体跨证书体系认证模型

Fig. 1　Privacy-preserving multi-subject cross-certificate system authentication model for material supply chain

1）投标方

投标方（如供应商、承包商等）需完成身份登记、隐私保护电子投标及合同履行等关键环节。具体而言，投标方应向所属 CA 提交身份信息获取数字证书，并基于该证书向监管机

构登记成为可信投标人;作为可信实体,其有权参与电子采购流程,包括加密上传投标文件至电子招投标交易平台,并定义细粒度访问策略以实施对招标方的授权访问;中标后,投标方须严格履行合同条款,及时交付符合约定质量标准的项目成果,并妥善管理项目风险。

2)招标方

招标方(如政府部门、采购机构等)需主导招标公告发布、授权访问投标文件及合同履行等关键环节。具体而言,招标方应通过电子招投标交易平台发布招标公告,组织资格审查并编制电子采购文件;在开标阶段,依托平台对授权投标文件进行访问与解密,完成文件开启、评审及结果通知书发放等操作;中标后,招标方需通过平台以数据电文形式与中标人签订合同,严格履行合同条款,组织项目验收,并建立质效评价机制,对采购项目的质量、效率效益及合规性进行系统评估。

3)证书颁发机构(CA)

CA 作为信任锚,负责所属域内实体的身份认证与证书签发。具体而言,CA 需首先向监管机构提交注册申请,并认证为可信节点,以确保自身的合法性与公信力;随后,CA 有权为域内实体(包括投标方、招标方等)进行身份审核,通过数字签名技术为可信实体签发数字证书。该证书作为实体的身份凭证,确保其唯一性与防伪性,从而支撑安全可信的电子采购环境。

4)监管机构

监管机构作为系统内唯一可信第三方,承担信任管理与合规监督的核心职能,可归纳为以下 3 个方面:

(1)跨证书认证与可信管理。监管机构负责认证所有参与实体(包括投标方、招标方及证书颁发机构)的可信性,确保证书持有者身份真实、公钥归属有效,并将其身份证明(如数字证书或标识)存储并登记到相应的可信列表中。通过定期维护该列表,监管机构确保各方身份的合法性与合规性,为跨域证书验证提供信任基础。

(2)电子采购流程全程监控与审计。监管机构生成全局密钥,支撑 ABE 机制;确保敏感数据在加密状态下流通,防范身份伪造和非法访问行为,保障招投标过程在受控且保密的环境下在线进行。

(3)区块链管理与系统维护。监管机构依托区块链技术,将证书认证、访问控制等任务委托给智能合约执行,实现高效、安全的数据存储与身份验证。通过定期审查与更新链上信任机制,确保系统长期安全、稳定运行。

隐私保护的多主体跨证书体系需要同时满足以下两大核心特征:

1) 多 CA 的可信跨域认证。聚焦于解决异构信任域间的互操作性问题。通过公钥认证技术,集合 Merkle 树构建可信域,确保数据的完整性和一致性。依托区块链技术,维护可信列表(如可信 CA 节点列表、可信投标人列表等),并通过部署智能合约自动执行预设的认证逻辑,确保仅经可信 CA 认证的投标人可参与电子采购过程。

2) 链上数据访问控制与隐私保障。聚焦于投标人隐私数据的保护与合法访问控制。通过加密技术与细粒度访问策略,确保投标人的敏感数据(如投标报价等)在存储与传输过程中的安全性,同时仅授权符合策略的用户(如招标方)在预设条件下解密和访问数据。

4 多主体跨证书体系认证过程设计

在多主体跨证书体系认证模型中,设计了两个核心业务场景:跨证书体系认证和公平透明的招投标过程访问控制。在跨证书体系认证场景中,多 CA 作为信任源,负责颁发和管理其辖区内的用户(即投标人)数字证书,以保证其管理主体的身份可信度。每个 CA 在系统中担任独立信任机构的角色,通过区块链上的智能合约机制,实现不同 CA 间的跨域证书验证,确保多信任源间的信任互通和证书有效性。而在公平透明的招投标过程访问控制场景中,区块链上的智能合约需对参与招标的主体进行可信身份认证,并对投标人加密数据进行存储保护,确保只有经过授权的招标方才能访问必要的投标信息。隐私保护的多主体跨证书体系认证的流程如图 2 所示。

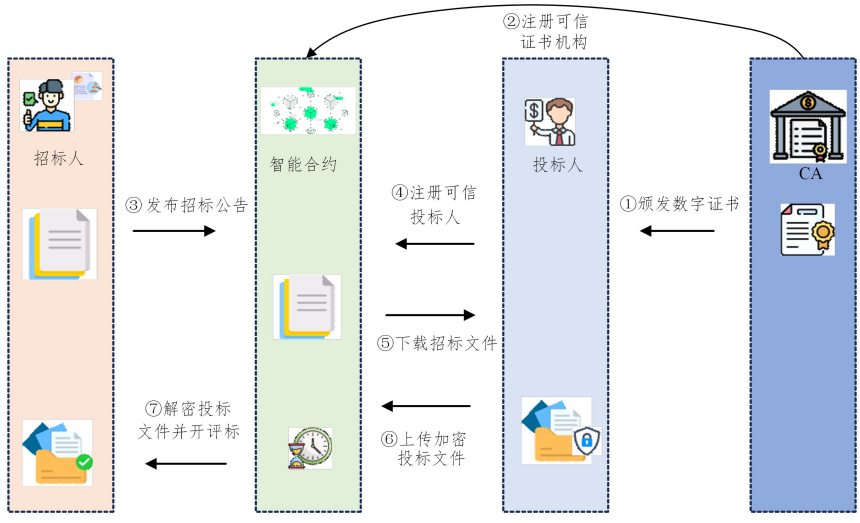

图 2 面向物资供应链的隐私保护多主体跨证书体系认证及访问控制流程

Fig. 2 Flowchart of privacy-preserving multi-subject cross-certificate system authentication and access control for material supply chain

4.1 多主体跨证书体系设计

在现有多 CA 管理的多信任域环境中,各 CA 负责为其所覆盖的投标人签发数字证书,确保身份认证与数据完整性,从而为投标过程提供安全、可信的验证机制。证书的维护是其中一个关键且富有挑战性的问题。在传统方案中,完整的密钥列表存储于区块链上,导致高昂的存储和验证成本,难以

适应实际的多方参与场景。此外，证书管理要求严格保护私钥信息，确保证书签发权牢牢掌握在 CA 手中，以避免任何未经授权的伪造风险。本方案通过引入 sMHT，将 CA 验证（即检查 CA 是否在可信列表中）和成员验证（即验证投标人的数字证书有效性）的问题转换为小型哈希值的比对操作，将显著减少存储量和计算开销。

特别地，sMHT 的核心在于，通过树的叶子节点存储数据项的哈希值，并利用子节点的哈希值递归地构造非叶节点，最终生成一个唯一的根哈希值，从而代表整棵树的完整性和唯一性。该方案在验证过程中无需访问整棵树，只需存储叶子节点的信息和验证路径，即可高效验证特定叶子节点是否属于给定的二叉哈希树。具体实现包括 3 个主要步骤：

1）密钥生成（Gen）

首先，确定 Merkle 树的高度 h，生成 2^{h-1} 个一次性签名（One-Time Signature，OTS）密钥对 (pk_i, sk_i)，其中 $i \in [1, 2^{h-1}]$。接下来，计算每个公钥的哈希值 $\mathrm{Hash}(pk_i)$，并将这些哈希值作为 Merkle 树的叶子节点。然后，通过如下公式逐层计算并构建整棵树的节点哈希值：

$$\mathrm{Hash}(node_i) = \mathrm{Hash}(node_{2i+1}) \parallel \mathrm{Hash}(node_{2i+2})$$

最终得到根节点的哈希值 $\mathrm{Hash}(root)$，并将其存储下来，用于后续的证书验证。此处符号 $\parallel$ 表示字符串的拼接操作。密钥生成过程中，私钥链由 2^{h-1} 个 OTS 私钥组成。该步骤可形式化表达为：$\mathrm{Gen}(1^k) \rightarrow \{(pk_i, sk_i) \mid i \in [1, 2^{h-1}]\}$。

2）消息签名（Sig）

在接收到消息 $M \in \{0,1\}^*$ 后，从未使用的 OTS 密钥对中随机选择一个密钥对，记其索引为 j。使用该 OTS 私钥 sk_j 对消息 M 进行签名，生成一次性签名 σ_{OTS}。同时，计算所用密钥对的认证路径（Authentication Path），记为 $auth_j$。最后，输出该消息的证书 $\sigma(M) = (M, \sigma_{\mathrm{OTS}}, pk_j, auth_j)$，其中 pk_j 为所用 OTS 密钥对的公钥。该步骤可形式化表达为：$\mathrm{Sig}(M, sk) \rightarrow \sigma(M)$。

3）证书校验（Ver）

在接收到证书 $\sigma(M)$ 后，验证者首先提取出原始消息 M 和公钥 pk_j，即可验证签名 σ_{OTS} 的有效性。如果签名中的公钥不匹配，则返回 false。否则进行下一步，使用公钥 pk_j 计算其对应叶子节点的哈希值 $\mathrm{Hash}(pk_j)$，然后利用认证路径 $auth_j$ 回溯计算出 Merkle 树的根节点哈希值 $\mathrm{Hash}(root')$。最后，将计算得到的根节点哈希 $\mathrm{Hash}(root')$ 与存储的根节点哈希 $\mathrm{Hash}(root)$ 进行比对：若二者相等，则验证通过，返回 true；否则，验证失败，返回 false。该步骤可形式化表达为：$\mathrm{Ver}(\sigma(M)) \rightarrow \mathrm{false/true}$。

为优化系统的资源利用率，以及提高验证过程的响应速度，在本文的跨域证书认证系统中，sMHT 方案被划分为离线和在线两个阶段，在应对高并发和多方参与的复杂环境时更具优势。特别地，离线阶段允许各认证中心在无需实时交互的情况下完成密钥生成 Merkle 树构造以及根哈希值的注册等高计算量的操作，从而减轻实时系统的计算和存储负担。在线阶段则聚焦于实际的证书颁发和验证流程，通过预先生成的密钥和哈希值快速完成投标人身份验证和证书合法性确认。

在本文的跨域证书认证系统中，监管机构负责 CA 和投标人的信任管理，区块链受监管机构委托进行证书验证与可信用户登记，以确保系统的高效性与安全性。具体流程如下：

1）系统初始化及可信节点注册（离线阶段）

各 CA 运行密钥生成步骤（Gen），初始化生成 Merkle 树所需的密钥，包括一次性签名密钥对和根哈希值。随后，CA 向监管机构注册为可信节点，并提交生成的根哈希值。监管机构将此根哈希值存储并登记在区块链上，作为系统的信任根基。区块链负责维护所有 CA 的根哈希值，以确保 CA 间的信任互操作性。

2）数字证书颁发（在线阶段）

CA 和投标人各司其职。在收到投标人的身份信息和证书请求后，CA 运行签名步骤（Sig），从未使用的签名密钥对中选取密钥，为投标人生成数字证书，并提供认证路径以证明该证书在 Merkle 树中的合法性。为确保后续投标过程中的身份唯一性与可信性，投标人需先在区块链上提交该数字证书完成身份认证（即登记为可信用户），从而获得招标文件的下载和使用权限、投标文件的上传和访问控制权限。

3）区块链验证与可信用户登记（在线阶段）

监管机构负责 CA 和投标人的整体信任管理，将证书验证委托给区块链。区块链作为公开、透明的验证平台，负责存储每个 CA 的根哈希值，并通过认证路径的回溯比对根哈希值，确认投标人证书的合法性和真实性。验证通过后，区块链将认证更新信息反馈给监管机构，以将投标人正式登记为可信用户，并将其数字证书和身份信息记录在监管机构中。

综上所述，CA 所管理的 Merkle 树层级结构设计不仅保障了数据的完整性，还支持高效的叶节点验证。具体地，通过提供从叶子节点到根节点的验证路径，验证者（本方案中的区块链）仅需根哈希值和该路径即可确认叶节点的真实性与有效性，而无需访问整棵树。同时，由监管机构维护的可信节点注册列表简化了查询流程，而区块链的加入则进一步增强了验证功能，确保各 CA 的可信节点身份，且 CA 管理的投标人符合可信用户标准（即其数字证书由 CA 合法颁发）。此外，区块链的智能合约功能实现了验证流程的自动化，提升了跨域认证的执行效率，避免了人工干预与集中式管理的延迟和潜在风险。此方式为跨域认证提供了透明且安全的保障，促进了多认证中心间的信任交互，显著缓解了多源信任模型中的认证瓶颈，使跨域证书验证更高效。

4.2　属性基加密的访问控制协议设计

为实现对投标人内容的细粒度访问控制，使其内容在授权范围内安全共享，本方案设计了一种基于属性加密的访问控制机制，以满足招投标系统中多角色的灵活授权需求。在此方案中，投标人可设置访问策略来控制招标方的权限，从而确保仅符合条件的招标方能安全访问其信息，并可扩展应用于其他角色。方案设计中，将密文存储委托给区块链，投标人因此能以较低成本享受弹性的数据存储与访问服务。为高效识别和检索大量密文中的关键信息，本文提出了一种具备双阶段解密的 CP-ABE 算法，支持将部分解密操作委托给区块链，降低了访问控制带来的计算负担。在该算法下，数据请求者（即招标方）仅需轻量级操作即可完成最终解密，从而安全获取投标文件。整个方案包含初始化设置、密钥生成、数据加密、第一次解密与第二次解密，共 5 个阶段。

1）初始化设置（Setup）

算法由监管机构运行。以安全参数 λ 作为输入，首先生成群参数 $par := (p, e, G_1, G_2, G_T, g_1, g_2)$，其中 G_1，G_2 和 G_T

均为素数阶 p 的乘法循环群，$e: G_1 \times G_2 \to G_T$ 为双线性映射（具体定义见 4.2 节），生成元 $g_1 \in G_1$，$g_2 \in G_2$。随后，算法随机选择一个整数 $\alpha \leftarrow \mathbb{Z}_p$ 和规定抗碰撞哈希函数 $H: \{0,1\}^* \to G_2$，以将任意长度字符串映射到乘法循环群上。计算并输出系统的公钥 $pk=(par, H, e(g_1,g_2)^{\alpha})$ 和主私钥 $msk=\alpha$。将公钥 pk 分发给已注册的可信投标人和可信招标人，而监管机构负责维护主私钥 msk，确保其不泄露。该步骤可形式化表达为：Setup$(1^{\lambda}) \to (pk, msk)$。

2）密钥生成（KeyGen）

算法由监管机构运行。以公钥 pk、主私钥 msk 和与招标人相关的属性集 $S=\{u_i\}_{i\in[m]}$ 作为输入，算法随机选择两个整数 $r, \beta \leftarrow \mathbb{Z}_p$，输出转换密钥 $tk=(S, tk_0, tk_1, \{tk_{2,i}\}_{i\in[m]})$ 和解密密钥 $sk=\beta$。而转换密钥 tk 各部分组件具体通过下式计算：

$$tk_0 = g_2^{\frac{\alpha}{\beta}} \cdot g_2^{\frac{r}{\beta}}, tk_1 = g_1^{\frac{r}{\beta}}, tk_{2,i} = H(u_i)^{\frac{r}{\beta}}$$

基于招标人属性集生成的这一对密钥中，转换密钥 tk 由区块链维护，用于一次解密，解密密钥 sk 则由招标人保管，用于二次解密。该步骤可形式化表达为：KeyGen$(pk, msk, S=\{u_i\}_{i\in[m]}) \to (tk, sk)$。

3）数据加密（Enc）

算法由投标方运行。以公钥 pk、规定线性秘密共享型访问策略 $\mathbb{S}=(\mathbb{M}, \pi, \{\pi(i)\}_{i\in[\ell]})$ 以限制招标人对资源的授权访问，将待保护隐私的投标文件 msg 作为输入，输出密文 $C=(\mathbb{S}, \{ct_{0,i}, ct_{1,i}\}_{i\in[\ell]}, ct_2, ct_3)$。算法首先随机选择一个秘密值 $s \leftarrow \mathbb{Z}_p$，再生成随机向量 $\boldsymbol{v} \leftarrow \mathbb{Z}_p^{n-1}$，计算 $\lambda_i = M_i (s \| v)^{\mathrm{T}}$。随后，随机生成 $t_1, t_2, \cdots, t_\ell \in \mathbb{Z}_p$，密文 C 各部分组件具体通过下式计算：

$$ct_{0,i} = g_1^{t_i}, ct_{1,i} = g_2^{\lambda_i} \cdot H(\pi(i))^{-t_i}$$

$$ct_2 = g_1^{s}, ct_3 = msg \cdot e(g_1, g_2)^{\alpha s}$$

该步骤可形式化表达为：Enc$(pk, \mathbb{S}=(\mathbb{M}, \pi, \{\pi(i)\}_{i\in[5\ell]}), msg) \to C$。

4）一次解密（PDec）

算法由区块链运行。以密文 C 和转换密钥 tk 作为输入，输出一次解密密文 PTC。特别地，如果嵌入转换密钥中的与招标人关联的属性集 S，满足投标人在密文中规定的访问控制策略 $\mathbb{S}$，则存在一个常数集 $\{\omega_i\}_{i\in I}$，能满足条件 $\sum_{i\in I}\omega_i M_i = (1,0,\cdots,0)$，从而恢复 $\sum_{i\in I}\omega_i \lambda_i = s$，最后计算下式得到一次解密密文 PTC 各部分组件：

$$ptc_0 = \frac{e(ct_2, tk_0)}{\prod_{i\in I}(e(ct_{1,i}, tk_1) \cdot e(ct_{0,i}, tk_{2,i})^{\omega_i}}$$

$$ptc_1 = ct_3$$

该步骤可形式化表达为：PDec$(C, tk) \to PTC/\perp$。

5）二次解密（TDec）

算法由招标方运行。以一次解密密文 PTC 和解密密钥 sk 作为输入，输出二次解密密文 msg，即明文投标文件，通过计算下式得到：

$$msg = ptc_1 / (ptc_0)^{\beta}$$

该步骤可形式化表达为：TDec$(PTC, sk) \to msg/\perp$。

特别地，在所设计的 CP-ABE 模型中引入了线性秘密共享方案（Linear Secret Sharing Scheme，LSSS）[16]，通过将访问策略表示为矩阵结构，并将指定的属性集映射为线性方程组，以实现灵活且安全的访问控制。同时，LSSS 的线性属性映射特性支持动态权限管理，使系统能适应属性更新和用户角色变化的需求，从而允许投标人（数据拥有者）自定义访问策略，确保仅符合特定条件的招标方才能解密密文访问内容。

通过这种双阶段解密流程，方案实现了投标过程中对招标方的细粒度权限控制，同时简化了访问控制的复杂度。招标方仅需轻量级操作即可验证投标人身份并获取必要信息，无需进行复杂计算，从而提升了系统的整体效率与安全性。这一设计确保了在多方参与的招投标场景下，系统具备高效、安全的访问控制和身份验证能力。

5 可行性分析

跨证书体系认证的核心在于身份的标识与鉴别。在证书域内，身份通过证书加以标识，而身份的鉴别则依赖于对证书路径与证书状态的验证。为此，本方案提出一种高效的跨证书体系认证机制，旨在兼顾异构环境下的身份认证需求与隐私保护，同时确保认证流程的高效性与低成本。具体而言，本方案采用层次化信任管理模式，由监管机构（相当于根 CA）统一管理各级 CA，在避免破坏现有身份标识体系的前提下（即信任域内仍维持原有的证书标识模式），实现可信身份的跨域认证。此外，方案引入分布式共识算法，通过定期维护可信方列表并审查区块链上的认证信息，保障认证体系的长期安全性和合规性。为优化跨域证书验证流程，方案结合小型 Merkle 哈希树签名技术，利用其轻量级哈希比对能力，在保持数据可验证性的同时显著降低存储与计算开销，从而提升信任传递的效率，实现跨证书体系认证的高效互通。

在跨证书体系认证的基础上，本方案进一步构建了一种面向招投标过程的细粒度访问控制机制，确保投标文件在全生命周期内（覆盖提交、传输、存储及访问阶段）的隐私安全。该机制基于 CP-ABE，允许投标人在数据提交阶段自主设定访问策略，并将该策略嵌入密文中，确保数据从生成时即受控。进一步，加密后的投标文件通过分片存储技术分布式地保存于区块链节点，利用其不可篡改性与拜占庭容错共识，确保任何单点攻击或节点合谋均无法篡改或窃取完整数据。同时，区块链的透明性支持对存储行为的实时审计，可快速定位异常访问事件。此外，CP-ABE 采用基于双线性映射的数学难题作为安全基础，使得未授权方无法通过暴力破解或数学推导获取明文信息，从理论上杜绝了传输与存储过程中的数据泄露，仅满足预定策略且持有解密密钥的招标方能够请求投标文件并成功解密。方案不仅实现了招投标过程的端到端加密，还提供了灵活的访问控制策略，使投标方能够自主定义信息共享范围，确保数据在合理授权范围内安全流通。最后，方案结合密钥拆分与委托技术实现了外包解密机制，有效减少了访问请求方的计算负担与存储开销，进一步提升了系统的可行性与实用性。

5.1 正确性分析

如果招标人属性集 S 满足投标人所定义访问控制策略 $\mathbb{S}$，则能够成功计算：

$$ptc_0 = \frac{e(ct_2, tk_0)}{\prod_{i\in I}(e(ct_{1,i}, tk_1) \cdot e(ct_{0,i}, tk_{2,i})^{\omega_i}} = e(g_1, g_2)^{\frac{\alpha s}{\beta}}$$

进一步，又因为招标人持有解密密钥 $sk=\beta$，通过计算下式即可重构 msg：

$$msg = ptc_1 / ({}^{p}tc_0)\beta = \frac{msg \cdot e(g_1, g_2)^{\alpha s}}{(e(g_1, g_2)^{\frac{\alpha s}{\beta}})^{\beta}}$$

5.2　安全性分析

在所设计的 CP-ABE 方案中，线性秘密共享方案（LSSS）与双线性映射的深度融合为系统提供了严密的安全基础与高度灵活的访问控制能力。LSSS 作为策略逻辑的验证引擎，将访问策略编码为矩阵化线性方程组，并通过 Shamir 秘密共享原理实现属性间逻辑关系的数学可验证性，为 CP-ABE 提供了灵活而严格的权限表达，精确限定符合特定属性集合的用户能够解密，同时其单调逻辑结构支持复杂门限策略。而双线性映射依托椭圆曲线群的离散对数难题及双线性对运算的代数特性，核心价值在于为 LSSS 的逻辑验证过程提供密码学计算基元，将抽象的逻辑关系转换为抗量子攻击的密码学操作。此外，动态密钥随机化机制通过属性关联参数隔离用户私钥，能有效防止多用户合谋攻击。

5.2.1　线性秘密共享方案

定义 4（线性秘密共享方案）　对于参与者集合$\mathcal{P}$，若满足以下条件，则称该 LSSS 是线性的（定义在$\mathbb{Z}_p$上）。

1）每个参与者的份额来自$\mathbb{Z}_p$上的向量空间。

2）存在一个矩阵$\boldsymbol{M}$，称为份额生成矩阵，其包含ℓ行和n列。对于每个$i\in[\ell]$，矩阵$\boldsymbol{M}$的第i行标记为某个参与者$x_i\in\mathcal{P}$。考虑列向量$\vec{v}=(s,r_2,\cdots,r_n)$，其中$s\in\mathbb{Z}_p$是要共享的秘密，$r_2,\cdots,r_n\in\mathbb{Z}_p$是随机选取的值，则$\mathbb{M}\vec{v}$构成了$\ell$个秘密份额的向量。份额$M_i\vec{v}$分配给参与者$x_i$，其中$M_i$表示矩阵$\mathbb{M}$的第$i$行，而$v_i$表示向量$\vec{v}$中的第$i$个元素。

进一步，设为$(\boldsymbol{M},\pi)$一个 LSSS 型访问策略，对于任意授权属性集合$A\subset\Omega$，其中Ω代表属性宇宙：1）存在一组有效份额$\lambda=\{\lambda_i\in\mathbb{Z}_p\}_{i\in I}$，其中$I=\{i:\pi(i)\in A\}$；2）存在一个有效算法（如高斯消元）来计算一组常数$\omega=\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$，使得通过计算$\sum_{i\in I}\omega_i\lambda_i$可以从有效份额中恢复出秘密$s$。本文工作假设这些常数已被成功计算，详细算法请参考文献[17]。

5.2.2　安全性证明

本文所提出的安全计算算法的安全性取决于 DBDH 假设与 CBDH 假设，用于保证在多项式时间内难以破解所提 CP-ABE 方案中的核心计算问题。

为评估本文方案的隐私保护能力，需明确潜在的安全威胁，主要包括猜测攻击、合谋攻击、窃听攻击和冒充攻击：

1）猜测攻击：敌手通过分析密文属性集与访问策略的关联性，逆向推断发送方身份或策略中的敏感属性。

2）合谋攻击：多个恶意用户共享其私钥，通过线性组合构造超越其个体权限的解密密钥。

3）窃听攻击：敌手截获通信信道中的密文或密钥交换信息，尝试通过离线计算（如暴力破解双线性对运算）恢复明文。

4）冒充攻击：敌手伪造合法用户的属性集，试图未经授权访问密文。

特别地，半诚实模型广泛应用于安全多方计算和隐私保护领域，尤其适用于供应链管理等多方协作且需保持数据机密性的场景。本文基于该模型作为威胁模型基础，来刻画系统内部实体（如招标方、投标方等）的潜在攻击行为。在该模型下，参与方严格按照协议执行计算，但可能被动记录协议交互过程中的中间数据，并尝试从中推导其他方的私有信息。

本文将基于定理 1 和定理 2 的安全性证明，验证供应链多可信源跨证书体系在属性基加密下的安全可靠性，将有效保障投标数据隐私和投标过程的公平透明。具体而言，本文所提 CP-ABE 方案在随机 Oracle 模型下基于两种安全模型：第一种满足选择明文攻击不可区分性（Indistinguishability under A Chosen Plaintext Attack，IND-CPA），用于应对发送方（即本文场景中的投标人）猜测攻击、合谋攻击和窃听攻击；第二种满足选择消息攻击下的存在性不可伪造性（Existential Unforgeability under A Chosen Message Attack，EU-CMA），用于防御合谋攻击和冒充攻击。

定理 1　在 DBDH 假设成立的前提下，所有概率多项式时间的敌手在挑战本方案的 IND-CPA 安全性时，其成功概率是可忽略的。

证明：假设存在一个多项式时间敌手$\mathcal{A}$，能够在 IND-CPA 模型下以不可忽略的优势$Adv_{\text{CP-ABE},A}^{\text{IND-CPA}}(1^\lambda)$攻破本文所设计的 CP-ABE 方案。那么，可以构造一个模拟器$\mathcal{B}$，该模拟器能够以不可忽略的优势$Adv_{\text{CP-ABE},\mathcal{B}}^{\text{DBDH}}(1^\lambda)$攻破 DBDH 假设。具体而言，模拟器$\mathcal{B}$接收元组$par:=(p,_1,G_2,G_T,e,g_1,g_2,A=g_1^a,B=g_2^b,C=g_1^c,T)$，其中$a,b,c\in\mathbb{Z}_p$，其目标是通过与敌手$\mathcal{A}$的交互来判断$T=e(g_1,g_2)^{abc}$或一个随机项$R\in G_T$。

1）初始化阶段

模拟器$\mathcal{B}$执行：

（1）隐私设置主私钥$\alpha=ab$（实际未知，但可通过$e(A,B)=e(g_1,g_2)^{ab}$计算主公钥成分）。

（2）选择抗碰撞哈希$H:\{0,1\}^*\to G_2$，初始化空列表$\mathcal{L}_H$。

（3）公布主公钥：$pk=(par,H,Y=e(A,B)=e(g_1,g_2)^{ab})$。

2）预言机查询阶段（由模拟器$\mathcal{B}$提供接口，模拟敌手$\mathcal{A}$在方案执行过程中的各种查询操作）

敌手$\mathcal{A}$可自适应查询以下预言机：

（1）随机字符串哈希预言机$O_H(u_i)$

若$u_i\notin\mathcal{L}_H$，选择$h_i\leftarrow\mathbb{Z}_p$，记录$(u_i,h_i)$并返回$H(u_i)=g_{2^i}^{h_i}$；否则，直接返回$\mathcal{L}_H[u_i]$。

（2）密钥生成预言机$O_{\text{KeyGen}}(S)$

随机选择$\beta,r'\leftarrow\mathbb{Z}_p$，计算

$tk_0=B^{1/\beta}\cdot g_2^{r'/\beta}=g_2^{(b+r')/\beta}$

$tk_1=g_1^{r'/\beta}$

$tk_{2,i}=H(u_i)^{r'/\beta}=g_{2^i}^{h_ir'/\beta}(\forall u_i\in S)$

记录β并返回$(tk=(S,tk_0,tk_1,\{tk_{2,i}\}),sk=\beta)$。

3）挑战阶段

敌手$\mathcal{A}$提交$(m_0,m_1,S^*=(M,\pi))$。模拟器$\mathcal{B}$随机选择$b\leftarrow\{0,1\}$，并完成如下操作

（1）生成秘密共享向量$\vec{v}=(c,v_2,\cdots,v_{n-1})\leftarrow\mathbb{Z}_p^{n-1}$，满足$\sum_{i\in I}\omega_iM_i=(1,0,\cdots,0)$，确保$\sum_{i\in I}\omega_i\lambda_i=c$。

（2）计算密文：

$ct_{0,i}=g_1^{t_i}(t_i\leftarrow\mathbb{Z}_p)$

$ct_{1,i}=g_2^{M_i\vec{v}}\cdot H(\pi(i))^{-t_i}$

$ct_2=C=g_1^c$

$ct_3=m_b\cdot T$。

（3）返回$C^*=(S^*,\{ct_{0,i},ct_{1,i}\},ct_2,ct_3)$给敌手$\mathcal{A}$。

4）猜测阶段

敌手$\mathcal{A}$提交猜测比特b'。若$b=b'$，模拟器$\mathcal{B}$输出 1（判断$T=e(g_1,g_2)^{abc}$）；否则输出 0。

5)模拟核心分析

该模拟过程通过 $e(A,B)=e(g_1,g_2)^{ab}$ 隐私嵌入主私钥 $\alpha=ab$，使用 $ct_3=m_b\cdot T$ 承载 DBDH 挑战值，以及把 $ct_2=C=g_1^{\zeta}$ 作为 LSSS 的共享秘密。

若 $T=e(g_1,g_2)^{abc}$，则解密流程为：

(1)真实密文 $ct_3=m_b\cdot e(g_1,g_2)^{abc}$。

(2)外包解密 $ptc_0=\dfrac{e(g_1^{\zeta},g_2^{(b+r')/\beta})}{\prod_{i\in I}e(g_2^{M_i\vec{v}},g_1^{r'/\beta})^{\omega_i}}=e(g_1,g_2)^{b\zeta/\beta}$（因 $\sum\omega_iM_i\vec{v}=c$）。

(3)最终解密 $m_b=ct_3/ptc_0^{\beta}$。

若 T 为随机值，ct_3 在信息论意义上隐藏 m_b，敌手优势 ϵ 满足：

$$|\Pr[\mathcal{A}\to 1\mid T=e(g_1,g_2)^{abc}]-Pr[\mathcal{A}\to 1\mid T=R\in G_T]|\leqslant Adv^{\mathrm{DBDH}}_{\mathrm{CP\text{-}ABE},\mathcal{B}}(1^{\lambda})+negl(\lambda)$$

此外，所述模拟过程无中止(所有查询均可应答)，转换密钥 tk 中的 r'/β 实现完美随机化，以及属性哈希 $H(u_i)=g_2^{h_i}$ 阻止从 $tk_{2,i}$ 提取关键信息。若 DBDH 假设成立(即不存在多项式时间算法能以不可忽略优势解决 DBDH 问题)，则模拟器$\mathcal{B}$的优势可忽略，故敌手$\mathcal{A}$的优势必可忽略，否则将矛盾。本方案满足 IND-CPA 安全：

$$Adv^{\mathrm{IND\text{-}CPA}}_{\mathrm{CP\text{-}ABE},A}(1^{\lambda})=|Pr[Exp^{\mathrm{IND\text{-}CPA}}_{\mathrm{CP\text{-}ABE},A}(1^{\lambda})=1]-\frac{1}{2}|\leqslant Adv^{\mathrm{DBDH}}_{\mathrm{CP\text{-}ABE},\mathcal{B}}(1^{\lambda})+negl(\lambda)$$

证毕。

定理 2 在 CBDH 假设成立的前提下，所有概率多项式时间的敌手在挑战本方案的 EU-CMA 安全性时，其成功概率是可忽略的。

定理 2 的证明与定理 1 证明思路类似，因此不再赘述。

6 实验验证

6.1 实验配置

实验环境搭建在一台运行 Ubuntu 20.04 LTS 操作系统的高性能服务器上，配置为 Intel(R) Xeon(R) Silver 4410Y @ 2.00GHz 12 核 CPU，128GB 内存。本文方案基于 C++实现，使用 Pairing-Based Cryptography 配对库和 GMP 库。在实现中采用对称配对的 A 型椭圆曲线(设置参数为 rbits：160，qbits：512，即选择在 512 位有限域上阶为 160 比特的曲线群)，以评估配对运算性能。所有测试数据均取 1000 次运行结果的平均值。实验首先评估基于 Merkle 哈希树签名方案性能，其次评估 CP-ABE 的性能表现。

6.2 跨证书体系认证方案评估

本文采用 sMHT 替代传统的全表存储方式，以降低存储开销。传统方法中，由于需要区块链辅助验证，因此区块链需要保存的密钥大小为 $2^h\times n$ bits(假设每个密钥对需要占据 $|N|=2048$ bits 的空间)。然而，通过使用 sMHT，本方案仅需存储一个根哈希值，即可对所有投标人证书的可信性进行验证。

为评估该方案在数字证书签发和验证方面的性能，本实验假设不同数量的密钥对(对应不同数量的投标人)作为自变量，而每个密钥对采用 RSA 算法，密钥模数大小为 $|N|=2048$ bits。实验分为离线和在线两个阶段：离线阶段通过预计算生成密钥树以减少在线等待时间，主要执行密钥生成操作(Gen)。而在线阶段涉及消息签名(Sig)和证书验证(Ver)的操作。

实验结果如图 3 所示，左侧纵轴为在线阶段耗时，右侧纵轴为离线阶段耗时，横轴表示生成的密钥对数量。实验评估了密钥树生成、消息签名和证书验证的效率。从图 3 中可见，本方案在在线阶段的签名操作耗时不超过 3 ms，证书验证在 1ms 内完成。离线阶段生成 4096 个密钥对的 Merkle 树约耗时 1200s。此外，实验还表明了证书的签发和验证均为常数级别操作，具有高效的性能优势。综上，通过引入在线-离线机制，本方案在大规模认证场景中能够实现毫秒级的证书签发和验证，能满足实际工程应用需求。

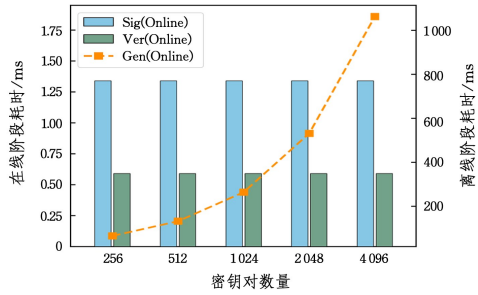

图 3 跨证书体系认证阶段算法时间开销

Fig. 3 Algorithmtime overhead for cross-certificate system authentication stage

此外，本文对比了在计算内核数量不同的情况下，该方案与 BASE[18]、IRBA[19]在签名(Sig)和验证(Ver)阶段的运行耗时，如图 4 所示。实验设定跨证书任务数量为 1000，重点考察并行计算环境下不同方案的性能表现，以分析计算内核数对运行效率的影响。随着内核数(即参与计算的并行线程数)的增加，所有方法的运行时间均有所下降，但是得益于高效的 Merkle 树签名和引入了在线-离线机制，本方案在时间开销方面显著低于另外两种方案，因而在大规模任务处理中的适应性和扩展性更优。

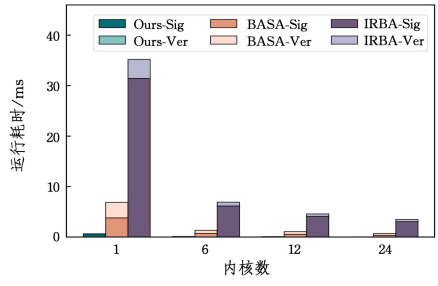

图 4 不同跨证书认证方案性能对比

Fig. 4 Performance comparison of different cross-certificate authentication schemes

最后，本文在资源受限和计算带宽有限的环境下，对所提方案的有效性进行了验证。

实验设置：所运行服务器网络带宽峰值为 1000Mbps，资源利用率(CPU 利用率和带宽传输)分别设定为基准方案的 100%，70%，40%和 20%。以 100%资源利用率为基准，计算其他场景的相对延迟倍数。实验结果(见表 1)表明，无论资源利用率如何变化，消息签名与证书验证的运行时间均能保持在 100ms 以内，展现出良好的鲁棒性。在受限环境下，该

方案虽呈现非线性性能衰减，但通过预计算将计算负荷转移至离线阶段，并以哈希链替代传统非对称加密的重复计算，使验证仅需哈希迭代，从而显著降低计算开销，提升整体认证效率。

表 1　认证方案在资源受限环境下的性能评估

Table 1　Performance evaluation of authentication schemes in resource-constrained environments

资源利用率/%	密钥生成/s	消息签名/ms	证书验证/ms	总延迟/s	性能衰减系数(vs 基准值)
100	66.6725	2.1286	0.5760	66.6752	1.00×
70	104.5423(+56.8%)	20.6809(+871.5%)	5.6324(+877.8%)	104.5686	1.57×
40	181.4076(+172.1%)	35.6417(+1574.7%)	8.7290(+1415.5%)	181.4520	2.72×
20	361.4421(+442.1%)	71.9891(+3281.9%)	28.3394(+4820.0%)	361.5424	5.42×

6.3　访问控制方案评估

现有的绝大多数 ABE 方案中，属性数量与算法复杂度密切相关，如加密算法和密钥生成的计算复杂度取决于属性集的大小。为优化计算效率，本文设计了一种支持外包部分解密的 CP-ABE 方案，允许将计算密集的访问策略匹配操作委托给区块链(即操作 PDec)，以减轻招标人解密的计算负担。

访问策略设置。本方案的部分解密 PDec 和数据加密 Enc 依赖于访问策略的复杂度。在实验中，所使用的是 LSSS 型门限访问策略，以便更清晰地控制访问权限。例如，策略“((A,B,2),(C,D,E,3),2)”表示满足以下条件之一即可：用户需至少具备集合{A,B}中的 2 个属性，或集合{C,D,E}中的 3 个属性。这样的策略经过 LSSS 转换为可计算的矩阵形式，用于加密和解密过程中的权限验证。

为评估本文所设计方案在多属性场景下细粒度访问控制的性能，不失一般性，本节实验以属性数量作为自变量，测量了 CP-ABE 方案在各个计算步骤上的耗时。实验涵盖了初始化设置(Setup)、密钥生成(KeyGen)、数据加密(Enc)、部分解密(PDec)和最终解密(TDec) 5 个阶段。

实验结果如图 5 所示，纵轴为计算时间(单位 ms)，横轴为属性数量。

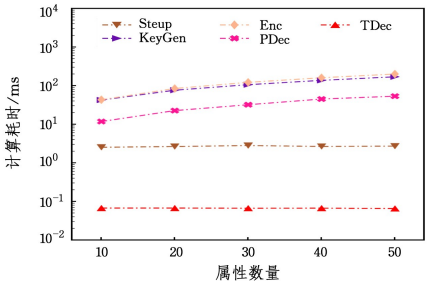

图 5　属性数量与 CP-ABE 计算耗时的关系

Fig. 5　Relationship between the number of attributes and CP-ABE calculation time

实验表明，随着属性数量的增加，KeyGen，Enc 和 PDec 阶段的计算时间因访问策略中属性数量的增加而有所增长，但均保持线性趋势，并在 50 个属性的情况下控制在 200 ms 以内，展现出良好的扩展性。TDec 和 Setup 阶段的计算时间几乎不受属性数量变化的影响，开销较低，仅涉及幂运算而呈现恒定的 O(1)时间复杂度。其中，TDec 阶段的高效性尤为突出，这显著降低了招标方在解密过程中的计算负担，可满足大规模招投标场景中对授权文件高效获取的需求。综上，实验结果验证了本文 CP-ABE 方案在细粒度访问控制中的有效性，授权过程的模拟进一步证明了该方案在多属性场景下访问控制精度和灵活性方面的优势。

7　结论

本文设计了一种面向物资供应链的隐私保护多主体跨证书体系认证及访问控制模型，以应对多证书体系认证的复杂性和满足数据隐私保护需求。具体而言，本文通过结合区块链和 Merkle 树签名实现多主体高效跨证书体系认证，并采用 CP-ABE 保护投标人敏感数据，确保跨域认证的透明性、安全性及投标过程的公平性。通过严格证明及实验室环境下的仿真测试，证明了该方案的可行性和有效性。此方案将为物资供应链中的跨域认证提供技术指导，有助于优化认证流程，增强各方公信力，支持可信数据共享环境的构建，并为多方参与环境中的隐私保护与高效认证提供重要参考。

结束语　在后续研究中，如何优化认证过程中的计算与通信开销，以兼顾资源受限环境下方案的适应度与可扩展性，是跨证书体系面临的核心挑战。此外，如何面向动态用户组构建实时感知的访问控制机制，精准实现权限的高效授予与安全撤销，也是值得深入研究的重要方向。

参 考 文 献

[1] Guiding Opinions of the State Council on Accelerating the Establishment and Improvement of a Green，Low Carbon，and Circular Development Economic System[M]. China Enterprise Reform and Development 2021 Blue Book State Counci，2021：5. DOI：10.26914/c.cnkihy.2021.070330.

[2] WANG Q L，REN Z Y，WU X Y，et al. Blockchain-based Internet of Things Traceable and Anonymous Cross-domain AuthenticationScheme[J]. Computer Science，2025，52(5)：337-344.

[3] TIAN H L，XIAN M J，GE P. Fine Grained Security Access Control Mechanism Based on Blockchain[J]. Computer Science，2024，51(S1)：1035-1041.

[4] FAN C I，WU C N，SUN W Z. Multi-recastable E-Bidding Scheme[C]// 2008 Eighth International Conference on Intelligent Systems Design and Applications. IEEE，2008：462-466.

[5] XU J，SONG J. A new management system for Intelligent E-Bidding[C]// 2013 IEEE 4th International Conference on Software Engineering and Service Science. IEEE，2013：158-161.

[6] CHEN Y H，CHEN S H，LIN I C. Blockchain based smart contract for bidding system[C]// 2018 IEEE International Conference on Applied System Invention(ICASI). IEEE，2018：208-211.

[7] TRINH V A，TRINH V C. One-Verifier Signature Scheme and Its Applications[C]// Proceedings of the 10th International

Symposium on Information and Communication Technology. 2019:261-266.

[8] MANIMARAN P,DHANALAKSHMI R. Blockchain-based smart contract for e-bidding system[C]//2019 2nd International Conference on Intelligent Communication and Computational Techniques(ICCT). IEEE,2019:55-59.

[9] WANG D,ZHAO J,MU C. Research on blockchain-based e-bidding system[J]. Applied Sciences,2021,11(9):4011.

[10] SARFARAZ A,CHAKRABORTTY R K,ESSAM D L. A tree structure-based improved blockchain framework for a secure online bidding system[J]. Computers & Security, 2021, 102: 102147.

[11] OMAR I A,HASAN H R,JAYARAMAN R,et al. Implementing decentralized auctions using blockchain smart contracts[J]. Technological Forecasting and Social Change, 2021, 168: 120786.

[12] XU D,YANG Q. The systems approach and design path of electronic bidding systems based on blockchain technology[J]. Electronics,2022,11(21):3501.

[13] MERKLER C. Secrecy,authentication,and public key systems [M]. Stanford University,1979.

[14] LAURIE B. Certificate transparency[J]. Communications of the ACM,2014,57(10):40-46.

[15] ZHANG Y Z,DENG R H,XU S M,et al. Attribute-based encryption for cloud computing access control:A survey[J]. ACM Computing Surveys,2020,53(4):141.

[16] ZHANG Y,DENG R H,XU S,et al. Attribute-based encryption for cloud computing access control:A survey[J]. ACM Computing Surveys,2020,53(4):1-41.

[17] LIU Z,CAO Z,WONGD S. Efficient generation of linear secret sharing scheme matrices from threshold access trees[J]. Cryptology ePrint Archive,2010.

[18] SHEN M,LIU H,ZHU L,et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications,2020,38(5):942-954.

[19] JIA X,HU N,SU S,et al. IRBA:An identity-based cross-domain authentication scheme for the internet of things[J]. Electronics,2020,9(4):634.

YANG Ke, born in 1990, Ph.D. His main research interests include information and cybersecurity, and energy blockchain.

GUO Qinglei, born in 1988, Ph.D. His main research interests include power system automation and energy blockchain.