面向可信数据空间的密钥管理技术研究综述

张焘[1,2]，刘子晰[1]，田骝[1]，唐湘云[3*]，康嘉文[4]，吴宣够[5]，刘吉强[1]

（1. 北京交通大学网络空间安全学院，北京 100044；
2. 清华大学互联网体系结构全国重点实验室，北京 100084；
3. 中央民族大学信息工程学院，北京 100081；
4. 广东工业大学自动化学院，广州 510006；
5. 安徽工业大学计算机科学与技术学院，马鞍山 243032）

摘要：可信数据空间是一种保障数据安全流通的基础设施。随着数字经济快速发展，可信数据空间在数据存储、数据传输与共享等环节的安全需求持续升级，而密码技术可从分布式部署、可扩展适配、跨域协同交互等方面，为可信数据空间的安全发展提供核心支撑。本文系统梳理了国内外可信数据空间密钥管理相关研究现状，从密钥管理架构与机制、密钥全生命周期管理、跨域认证与安全协商 3 个维度展开综述，重点剖析层次化、分布式、轻量级密钥机制，以及密钥更新、密钥托管、代理重加密等关键技术，总结各类跨域认证与群组密钥协商方法，梳理现有研究在动态适配能力、跨域协同效率方面存在的短板。最后，展望了可信数据空间中自适应密钥管理、智能安全密钥管理等前沿发展方向。

关键词：可信数据空间；密钥管理；跨域认证；代理重加密；安全协商

中图分类号：TP309；TP393.08　　**文献标志码：**A

DOI: 10.20172/j.issn.2097-3136.260527

Review of key management technologies for trusted data spaces

Zhang Tao[1,2], Liu Zixi[1], Tian Shuang[1], Tang Xiangyun[3*],
Kang Jiawen[4], Wu Xuangou[5], Liu Jiqiang[1]

（1. School of Cyberspace Security, Beijing Jiaotong University, Beijing 100044, China；
2. National Key Laboratory of Internet Architecture, Tsinghua University, Beijing 100084, China；
3. School of Information Engineering, Minzu University of China, Beijing 100081, China；
4. School of Automation, Guangdong University of Technology, Guangzhou 510006, China；
5. School of Computer Science and Technology, Anhui University of Technology, Maanshan 243032, China）

Abstract: Trusted data space is a core infrastructure for secure data circulation. With the development of the digital economy, higher security requirements have been put forward for data storage, transmission and sharing in trusted data spaces. Cryptographic technology can provide strong security support for the development of trusted data spaces in terms of distributed deployment, scalability and cross-domain collaboration. Based on a comprehensive review of domestic and foreign research on key management for trusted data spaces, this paper conducts a review from three dimensions: key management architecture and mechanism, key full-life-cycle management, and cross-domain authentication and security negotiation. This paper mainly analyzes hierarchical, distributed and lightweight key

* **通信作者：**E-mail: xiangyunt@muc.edu.cn

基金项目：国家密码科学基金面上项目（2025NCSF02030）；国家自然科学基金青年基金（62402029）；北京市自然科学基金丰台创新联合基金（L251041）；清华大学互联网体系结构全国重点实验室开放课题（HLW2025MS02）；安徽省冶金工业数字孪生技术重点实验室开放基金（ADW24-01）

引用格式：张焘，刘子晰，田骝，等. 面向可信数据空间的密钥管理技术研究综述 [J]. 网络空间安全科学学报，2026，4（3）：13 - 26.

Citation Format: Zhang T，Liu Z X，Tian S，et al. Review of key management technologies for trusted data spaces[J]. Journal of Cybersecurity，2026，4（3）：13 - 26.

mechanisms, as well as key technologies including key update, key escrow and proxy re-encryption, and summarizes the mainstream methods of cross-domain authentication and group key negotiation. Furthermore, the deficiencies of existing researches in dynamic adaptation capability and cross-domain collaboration efficiency are summarized. Finally, the future development directions of trusted data spaces such as adaptive key management and intelligent secure key management are prospected.

Keywords: trusted data space; key management; cross-domain authentication; proxy re-encryption; secure negotiation

0 引言

随着数字经济的快速发展，数据作为核心生产要素，跨组织、跨领域的数据共享需求持续攀升。在实际数据流通过程中，不同机构的系统架构与数据管理规范存在差异，导致数据格式、接口标准不统一，极易形成数据孤岛问题。在工业互联网场景中，设备制造、供应、运营等多方数据分散存储于不同平台，难以实现高效数据协同；在医疗、政务等场景中，数据隐私保护标准与要求更为严苛，且各机构间缺乏可靠的互信机制，进一步制约了数据的安全共享与高效流通。跨域环境具有参与主体多元、身份类型异构、信任基础薄弱等特征，传统安全机制在统一身份认证、精细化访问控制、跨域密钥协商等方面存在显著短板，无法适配数据要素市场对安全可信数据流通的发展需求[1-2]。在此背景下，可信数据空间依托统一的规则体系、可信交互机制及标准化接口，可实现多主体间数据的安全共享、可控使用与可信协同。

针对可信数据空间安全体系构建，现有研究围绕主流数据空间架构开展了系统性安全分析，聚焦架构设计、安全协议、隐私保护机制等核心内容展开深入探究，证实数据安全与隐私保护是可信数据空间建设的核心基础，可信数据空间已逐步成为数字经济时代实现安全高效数据共享的关键基础设施[3]。针对数据共享过程中的可信验证与安全审计需求，可通过构建可追溯、可验证的数据交互机制，提升数据共享全流程的透明性、可信性与安全性，为可信数据流通落地提供坚实技术支撑[4]。同时，面向各行业的可信数据空间应用落地持续深化，其中面向工业场景的可信数据空间架构，可有效实现跨组织数据安全共享与全流程可追溯管理[5]，充分验证了可信数据空间在复杂异构场景下的安全适配能力。综上，无论是理论框架研究、交互机制设计，还是行业场景落地实践，安全性始终是可信数据空间建设的核心基石。保障数据存储、传输与计算全流程的机密性与完整性，已然成为当前可信数据空间领域的重点研究方向。

密码技术是保障数据安全的核心支撑手段，可有效实现数据机密性保护、主体身份认证、权限访问控制等核心安全能力，尤其适用于多主体、跨域协作的数据流通场景。其中，密钥管理体系、安全密码协议、认证协商机制直接决定可信数据空间系统的整体安全性与可信性。因此，针对可信数据空间的密码安全与密钥管理技术开展系统性综述研究，具备重要的理论研究价值与工程应用价值。图 1 展示了可信数据空间安全挑战与密钥管理支撑体系。

从可信数据空间整体安全体系来看，密钥管理并非独立的安全模块，而是贯穿系统架构搭建、跨域数据交互、平台运行维护全流程的核心支撑机制。现有研究表明，开放异构环境下的安全数据共享，需融合密钥管理、身份认证与访问控制技术，实现跨主体、跨平台的可信协同交互[6]。其中，身份认证与访问控制技术负责完成参与主体的可信身份核验与数据访问权限约束，是保障数据可信流通的前提条件；密钥管理架构与机制重点解决异构网络环境下密钥的部署、分发与统筹管理问题，为数据安全流通提供基础密码支撑；密钥全生命周期管理覆盖密钥生成、存储、更新、轮换、撤销等全流程环节，保障动态开放环境下密钥体系的持续安全性与可控性[7]；跨域密钥认证与协商机制，主要解决不同信任域间的身份核验、信任建立与安全交互难题[6,8]。综上，密钥管理架构、密钥全生命周期管理、跨域认证协同机制共同构成可信数据空间的核心密码支撑体系。基于此，本文围绕上述核心内容，系统梳理可信数据空间主流密码与密钥管理关键技术，结合身份认证、访问控制等配套支撑机制，全面总结当前研究现状、核心技术难题与未来发展趋势。

1 可信数据空间中的身份认证与访问控制机制

身份认证与访问控制是可信数据空间实现安全数据流通的基础环节，核心目标在于确认数据空间中的合法参与主体，并进一步约束不同主体对数据资源的访问权限。传统身份认证协议与访问控制机制通常依赖单一可信第三方完成身份验证与权限管理。随着物联网、云计算等新型网络架构的快速演进，该类机制逐渐暴露出可扩展性差、单点失效风

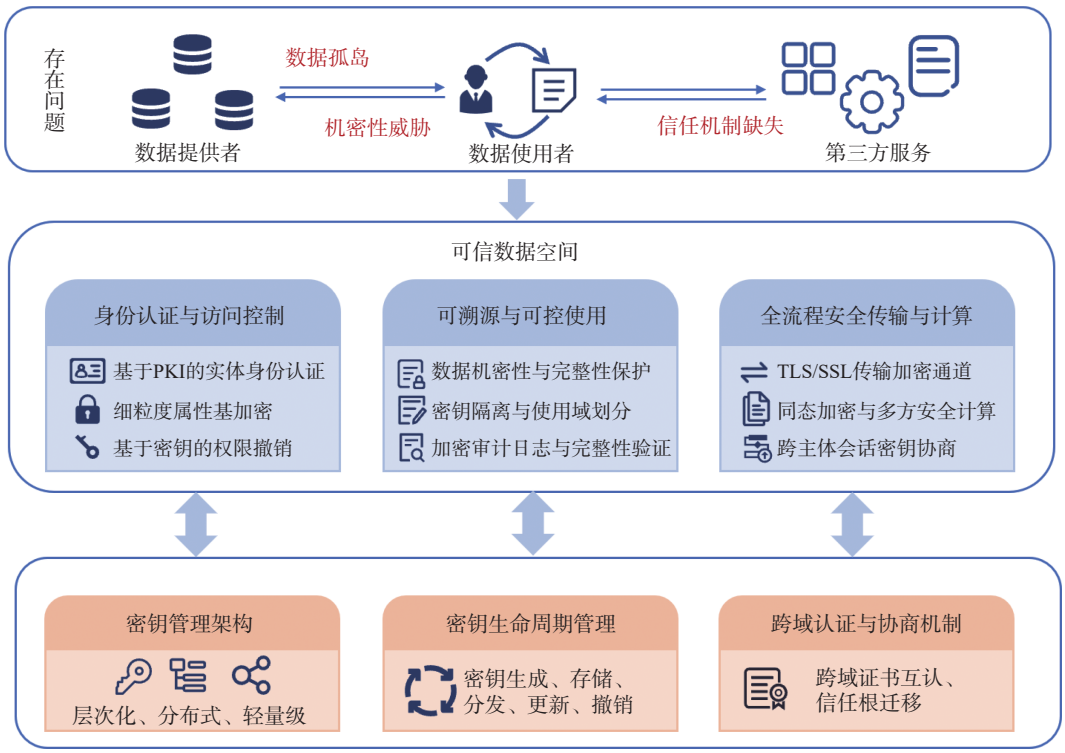

图 1　可信数据空间安全挑战与密钥管理支撑体系

Fig. 1　Security challenges and key management support architecture in trusted data space

险高、跨域协同能力薄弱等缺陷。

针对可信数据空间认证协议的安全性与适用性难题，Alsheavi 等[9]系统梳理了身份认证协议面临的各类挑战，指出轻量级特性与高安全性能的平衡是该领域的核心研究难点。为了增强资源受限设备的认证可靠性，Yoon 等[10]提出了一种联合异构物理不可克隆函数的安全增强认证方案，依托硬件层唯一物理特性完成设备身份认证，在提升系统抗物理攻击能力的同时，有效降低密钥存储风险。针对云辅助物联网场景中的认证问题，Wang 等[11]设计了一种轻量级用户认证协议，通过动态身份机制在保证通信机密性与匿名性的同时降低了设备端计算与通信开销，提高了协议在云边协同环境中的适用性。传统静态认证方式无法持续核验设备使用者身份，因此，Bhuva 等[12]将生物特征融入连续身份认证机制，通过实时采集分析用户行为与生物特征数据，实现物联网设备运行过程中的动态身份核验，有效降低设备非法接管、身份冒用等安全风险，提升持续交互场景下的认证可靠性。

在访问控制方面，Sivaselvan 等[13]提出了一种基于区块链的可扩展安全访问控制方案，通过分布式账本和智能合约实现去中心化权限管理，有效解决了传统集中式访问控制中单点故障与权限篡改问题。针对车联网与车载云计算环境的动态认证需求，Saleem 等[14]提出一种云端辅助安全认证协议，通过结合车辆身份验证与云端协同机制，实现了复杂动态网络中的安全接入与数据保护。Akram 等[15]进一步提出了一种基于身份的轻量级认证方案，通过优化认证与密钥更新流程，在降低通信与能源消耗的同时，提升了车联网环境下的安全性与认证效率。

从现有研究可以看出，当前身份认证与访问控制技术正逐渐从传统中心化架构向轻量化、分布式与协同化方向演进。但现有方案多聚焦于协议安全性与理论可行性，对大规模动态网络场景下的认证时延、访问策略动态调整、多节点协同管理等实际问题关注不足。因此，在资源受限设备场景下，兼顾安全性、实时性、隐私保护与系统开销的综合优化，是当前可信数据空间身份认证与访问控制领域的重要研究方向。

2　密钥管理架构与机制

可信数据空间的数据流通涉及多主体动态交互，对底层密钥管理架构提出了较高的适配要求。传统单一中心化或高开销密钥管理架构难以适配该场景，因此需从多维度设计密钥管理架构，解决系统层级扩展、多方协同治理、资源受限设备安全接入等核

心问题。密钥管理不仅需要满足安全性与可扩展性需求，还需要具备良好的标准化与互操作能力。目前，业界已形成一系列面向密钥全生命周期管理与跨系统互操作的标准规范。OASIS 组织提出的密钥管理互操作协议[16]通过统一密钥创建、存储、更新、撤销以及访问控制等操作接口，为异构系统的密钥管理互操作提供标准化支撑，后续又进一步提升了协议对分布式环境、多场景密钥管理的适配能力，为可信数据空间中的跨域密钥协同与统一管理提供了参考。以下从层次化、分布式和轻量级 3 个角度展开具体综述。

2.1 层次化密钥管理技术

可信数据空间的构建需要各类数据要素在层级间安全可控分发，以此保障系统的可扩展性。分层密钥管理技术可以提高系统的整体可扩展性，增强密钥管理流程的安全性和效率。在可信数据空间内的不同信任域之间共享数据通常需要清晰易管理的密钥分发机制，由此提出层次化密钥管理技术。在网络初始化过程中，Gandino 等[17]提出了一种临时主密钥机制，该机制在系统初始化阶段采用临时密钥，快速构建节点通信链路以降低延迟，有效保障系统初始运行效率，减少运行偏差风险。后续研究将这一思想扩展到资源受限的情况，Najafi 等[18]设计了一种多层锁定架构，来解决物联网设备计算能力有限的问题，通过减少密钥更新过程中的通信轮次与计算开销，在轻量级架构设计与安全防护性能之间实现了良好平衡。

在动态访问控制的场景下，Yu 等[19]提出了适用于移动自组网络的层次化密钥管理方案，采用动态选择节点的方案，节点密钥更新需依托父节点或阈值数量同级节点协同完成，有效提升方案实际安全性，延长网络有效运行周期。Lo 等[20]提出了一种适用于大型叶类层次结构的密钥分配方案，可以控制其中的访问权限来降低开销。在此基础上，Odelu 等[21]进行了优化，提出了一种能够更高效处理动态访问控制的层次结构密钥管理方案，通过对称密码和哈希来降低开销，适合实际应用场景。内容访问控制的应用范围非常广泛，Ragab 等[22]提出了一种线性层结构密钥管理方案，侧重优化成员管理与层级变更机制的设计，具备良好的可扩展性。在具体场景中，Xu 等[23]根据可扩展视频编码的多层比特结构进行单元的重新排列和分层加密，针对不同层的不同需求设计特定的加密算法。实验结果表明，该比特流分层加密方案可在保障数据安全的前提下有效降低计算复杂度。Abu 等[24]提出了一种面向物联网与智慧城市环境的层次化密钥分发与认证架构，通过构建分层身份认证与密钥分发机制，实现不同层级节点之间的安全接入与动态授权管理。该方案能够提高大规模异构环境中的身份可信性与密钥管理效率。

综上，可信数据空间层次化密钥管理在稳定层级结构的密钥组织与访问控制方面的研究已较为成熟，但现有方案大多假设网络拓扑与成员关系静态不变，难以适配节点频繁上下线、权限动态变更等复杂场景。同时，随着系统层级加深，密钥更新链路长度增加，易引发更新延迟、运维成本升高等问题。现有研究仍然缺乏对细粒度权限控制和层级间策略协调的充分讨论，导致对复杂场景管理策略不够灵活，不利于进行扩展。

2.2 分布式密钥管理技术

在多方参与、跨域通信的数据分发场景下，依托单一信任中心的传统密钥管理模型存在显著的结构性缺陷，难以适配可信数据空间的运行需求。分布式密钥管理将核心密钥存储与管理职能分发至不同网络节点或独立机构，侧重多主体横向协同共治。在理论支撑方面，分布式密钥生成理论是分布式密钥管理的基础组成部分。Kokoris 等[25]和 Das 等[26]研究了用于高阈值分布式密钥生成的异步机制，上述研究为可信数据空间多方协同密钥管理机制的设计奠定了重要理论基础。

针对分布式密钥管理技术在资源受限网络环境中的适用性问题，Lu 等[27]将这一研究思路扩展到无线传感器网络，在不同种类的任务节点上对密钥管理任务进行分布，可以提高系统在复杂网络环境下的可扩展性和稳定性。在分布式无线通信的场景下，Xi 等[28]提出了一种快速移动提取密钥协议，通过引入轻量级密钥协商与更新机制，在保证通信机密性和完整性的前提下，显著降低了资源受限设备的计算开销与通信开销。Panda 等[29]针对分布式物联网环境中的认证与密钥管理问题，提出了一种基于区块链技术的解决方案，通过利用分布式共识机制，实现了物联网设备之间无需可信第三方的安全身份认证与密钥协商，该方案依托区块链特性保障数据隐私安全，同时引入单向哈希链技术降低系统开销、提升运行效率。

De 等[30]面向密集且动态变化的环境提出了一种去中心化高效密钥管理方案，能够在密集且动态的网络环境中以自组织的方式提供安全的多跳通信，

使用阈值密钥共享技术来使节点参与协作执行去中心化的节点准入和密钥更新，从而显著提升了动态环境中通信的安全性。Hao 等[31]聚焦车载自组织网络设计了一种基于群组签名的分布式密钥管理框架，该框架支持多节点协同完成消息真实性验证，在缓解单点认证压力的同时，可有效抵御各类常见网络攻击。分布式密钥管理技术还可以和基于特征的加密技术进行融合。AI 等[32]提出了一种基于层次化区块链的节点认证框架，使用分布式账本与协同验证机制共同实现去中心化的身份认证，可以降低对单一可信认证中心的依赖，并且增强在动态网络环境中认证的可靠性和系统的稳定性。

从现有研究来看，分布式密钥管理在抗单点失效和多节点协作方面具有显著优势。但现有多数方案仅从理论层面保障安全性与去中心化特性，对实际应用中的通信同步开销、节点状态监测等工程问题关注不足。同时，针对大规模动态节点变更场景，现有方案难以兼顾密钥同步效率与密钥一致性维护。由此可见，实现安全性、实时性与操作复杂度的协同优化，仍是该领域的重点研究难题。

2.3　轻量级密钥管理机制

可信数据空间的接入终端存在显著异构特征，且大量边缘资源受限设备普遍存在计算能力、内存与存储空间不足的问题。传统密钥管理协议所采用的公钥加密与多轮认证流程难以适配该类终端场景，过高的计算开销会大幅降低系统运行效率。为解决上述问题，轻量级密钥管理机制被逐步提出，其核心目标是在降低设备资源消耗的同时，满足场景基础安全防护需求。

在轻量级密钥建立与分发研究方面，Raza 等[33]通过优化 DTLS 协议握手流程提出一种对称密钥机制，可在保障通信效率的前提下，实现物联网设备的安全密钥协商与数据加密。针对集群通信场景，Dammak 等[34]提出一种轻量级分布式集群密钥管理方法，该方法依托分布式节点协作完成组密钥的创建与分发，有效解决了集中式管理模式存在的单点瓶颈问题。Gupta 等[35]针对会话密钥保护需求，提出一种轻量级密钥保护机制，将双向认证机制与访问控制策略融入密钥管理流程，有效降低密钥传输与存储阶段的泄露风险。Yıldız 等[36]设计了一种适配物联网场景、基于物理不可克隆函数的轻量级群组认证与密钥分发协议，融合物理不可克隆函数、阶乘树与中国剩余定理实现轻量化认证与密钥分发，且随着群组成员数量增加，协议运行效率可进一步提升。

在具体行业应用场景中，Wazid 等[37]提出一种适配通用物联网环境的安全用户认证与密钥管理协议，通过身份验证与密钥协商流程的一体化设计，减少设备交互轮次。Benmalek 等[38]面向动态访问控制场景，研发了面向物联网的 SEKM 方案，该方案引入轻量级密钥更新方法，实现访问权限的快速动态调整。针对资源受限物联网场景，Guo 等[39]提出一种低复杂度的轻量级密钥生成方案，利用无线信道特征的随机性与双向差分量化技术，在物理层直接生成设备间共享密钥，规避了传统公钥密码体制的高复杂度运算开销。蒋京玮等[40]针对移动边缘计算场景，提出融合零知识证明与门限秘密共享技术的轻量级身份认证与密钥管理方案。实验结果表明，该方案可满足前向安全与后向安全特性，能够抵御多种已知攻击，在保障高安全性的同时兼顾轻量化与高效性。

综上，现有研究表明，可通过减少交互轮次、简化密码运算等方式提升整体认证效率。但当前多数方案多为特定设备场景的定制化设计，通用性与可移植性较弱；同时，部分研究过度侧重轻量化设计，存在安全性与可靠性弱的问题。针对大规模异构节点持续访问场景，现有策略随节点规模扩张易出现性能衰减、安全性下降等问题。如何在保障系统安全的前提下提升可承载节点规模，是该领域值得深入探究的问题。

上述密钥管理方案对比见表 1。

3　密钥生命周期管理

密钥管理需要在数据流通过程中应对密钥持续变化、存储风险以及授权转换等动态需求。数据在多主体间流转时，密钥会随权限变更、安全策略调整或设备状态切换而频繁更新；密钥在终端或云端的存储安全直接关系到整个加密体系的可信根基，数据所有者还需在不泄露明文的前提下，向其他实体安全移交解密权限。这些面向数据流通的实际需求，对密钥更新与轮换、安全存储与托管、代理重加密与授权转换 3 类关键技术提出了要求。

3.1　密钥更新与轮换机制

可信数据空间长期运行过程中，密钥会随系统状态与运行环境变化不断更新。从实现机制来看，密钥更新通常包括触发、生成、分发、同步以及失效 5 个阶段。首先，系统依据预设周期、访问行为变动、权限调整或安全异常事件触发密钥更新；再由密钥管理中心、边缘节点或通信双方生成新会话

表 1 密钥管理方案对比

Table 1 Comparison of key management schemes

方案	核心方法	计算开销	动态扩展性	优点	局限性	适用场景
文献[17]	临时主密钥机制	低	中	快速建立链路	临时密钥管理需额外设计	网络初始化、快速节点接入
文献[20-21]	对称密码、哈希动态访问控制	中	高	高效处理动态权限	随着层级加深更新延迟增加	大型层级结构中的动态访问控制
文献[27]	异构传感器分布式密钥管理	中	高	提高复杂网络可扩展性	节点协同机制复杂	异构无线传感器网络
文献[29]	区块链、共识机制	高	高	无需可信第三方，可追溯	区块链存储开销大	分布式物联网设备认证与密钥管理
文献[31]	群组签名、分布式认证	中	中	降低单点认证压力	群组管理复杂度高	车载自组织网络
文献[36]	物理不可克隆函数、阶乘树、中国剩余定理	低	高	群组认证高效	依赖硬件设备	物联网轻量级群组认证与密钥分发

密钥或主密钥。完成新密钥生成后，需通过安全信道等协商机制完成密钥分发与同步，待所有授权节点完成验证后，旧密钥逐步失效，完成密钥安全轮换。

目前，密钥动态更新机制的研究主要围绕密钥轮换、权限撤销、组密钥同步以及动态场景下的连续安全维护等方向展开，重点解决长期运行场景下的密钥泄露风险、节点频繁接入退出，以及跨域协同中的密钥一致性难题。Wang [41] 提出了一种支持单根信任、多曲线兼容、上下文隔离以及后量子密码可插拔的密码身份原语，并通过无状态密钥轮换机制降低长期密钥暴露风险。该方案无需依赖集中式状态同步即可实现安全密钥轮换。Tan 等[42] 将属性基加密与直接撤销机制相结合，实现了用户权限变化情况下密钥与访问策略的动态更新，规避了传统撤销机制因大规模密钥重分发产生的高额开销。Li 等[43] 针对车载网络中组密钥频繁更新带来的同步效率与通信连续性问题，采用无缝密钥切换与动态更新策略，实现高速移动场景下组密钥的持续更新与安全同步。Kajita 等[44] 针对动态群组通信环境中的密钥轮换与成员变更问题，提出了一种支持认证状态同步更新的灵活组密钥协商机制，在组密钥更新的同时同步维护身份认证状态，提升了成员动态上下线场景下密钥更新的安全性与灵活性。

无线密钥生成利用无线信道的随机性、互易性以及时变特征，从通信双方共享的无线信道信息中直接提取随机密钥，有效降低对外部可信基础设施的依赖。Huan 等 [45] 提出了一种面向物联网场景、能够抵抗重放攻击的无线密钥生成方案，通过动态信道特征提取与挑战响应机制提升密钥协商过程中的随机性与同步一致性，提升复杂无线环境下的通信安全能力。在无线信道密钥提取效率方面，Yuan 等[46] 提出了一种基于多子载波相位差的无线密钥生成方法，通过联合利用多个子载波之间的相位信息，提高密钥生成速率与一致性，同时增强系统在复杂多径环境中的鲁棒性。随着人工智能技术与无线安全机制的融合，Yang 等[47] 面向下一代车联网场景提出了一种基于大语言模型的无线密钥生成框架，通过动态分析无线环境变化实现密钥生成参数的自适应优化，在提升移动场景下密钥生成稳定性的同时，增强了复杂网络环境中的安全协同能力。

从现有研究来看，现有密钥更新方案虽可提升动态网络的安全性与灵活性，但大多仅针对特定场景优化，对于大规模异构网络中的密钥同步效率与长期稳定性关注不足。尤其是在可信数据空间跨域协同场景下，现有方案尚未形成成熟的多节点协同更新与统一安全管理机制。

3.2 密钥安全存储与托管

在可信数据空间环境中，密钥安全不仅取决于生成和分发环节的安全强度，还取决于数据存储环节。一旦密钥在存储环节发生泄露或被篡改，将直接威胁整套加密安全体系。可信数据空间内大量边缘设备部署于开放网络，且计算、存储资源受限，使得密钥安全存储面临更为复杂的技术挑战。Ghosal 等[48] 对智能电网高级量测体系中的密钥管理系统进行综述，从密钥全生命周期视角，阐明了安全高效存储机制对保障数据机密性与完整性的重要作用。

当密钥存储在设备端时，硬件级安全方案能够为资源受限环境下的密钥保护提供有效安全保障。Jung 等[49]基于 ARM 平台的安全架构，开发了一种面向物联网设备的安全平台模型，实现密钥与安全执行环境的双重物理隔离。该硬件辅助方案将密钥保护从应用层下沉至硬件层，从源头强化安全防护能力。Yang 等[50]针对传统存储方式易受物理攻击的问题，提出了一种基于物理不可克隆函数和模糊保险库的密钥存储方案，利用硬件固有的随机性生成唯一设备指纹，并结合模糊保险库机制开展防护。该方案可有效抵御物理克隆攻击，实现密钥安全存储与可靠恢复，同时提升密钥抗物理攻击与防复制能力。

随着可信数据空间中的数据资源迁移到云端，云环境中密钥的安全存储和托管问题成为研究热点。Prabhu 等[51]基于中国剩余定理开发了一种安全存储模型，该模型对密钥与数据进行分区处理，并将完整密钥拆分存储至多个云平台，攻击者很难通过单个节点获取完整的密钥信息。Li 等[52]提出了一种基于区块链的移动边缘计算安全密钥管理方案，利用区块链的去中心化存储和不可篡改特性，实现密钥信息的可信托管与访问审计，同时结合边缘节点协同机制提升密钥分发效率，有效增强了动态边缘网络环境中的密钥安全性和系统可扩展性。同理，Zhao 等[53]提出一种基于区块链的高效密钥管理方案，采用分层式密钥托管架构在保证控制权的前提下实现了密钥的安全备份与授权恢复，为敏感数据保护提供了可行的技术路径。QPause 方案[54]提出了一种面向云存储场景的抗量子口令保护数据外包机制，通过将后量子密码技术与身份认证过程相结合，实现用户身份验证与数据外包过程中的安全保护，能够增强长期数据存储环境下的抗量子攻击能力。

现有研究虽提升了密钥存储安全水平，但多数方案仍依赖专用硬件与外部可信基础设施，对于异构设备下密钥一致性维护仍存在不足。分布式密钥存储方案普遍侧重安全性，往往存在访问效率低、实时性不足的问题，在高频访问、大规模并发场景下易产生性能瓶颈。目前密钥存储领域尚未形成统一、轻量化、高可扩展的框架，也无法在密钥全生命周期内支撑密钥动态迁移与恢复。

3.3　代理重加密与授权转换

可信数据空间内的数据需跨域流通，因此数据所有者必须在不泄露明文数据的前提下，安全地向用户或应用程序实体授予访问权限。现有加密机制虽可有效保障数据机密性，但在权限移交与跨域授权方面存在明显不足。代理重加密技术正是针对该类场景逐步发展而来，该技术的核心思路为：由半可信代理节点将数据所有者生成的密文转换为接收方可解密的密文。从基础理论和建模的角度出发，Qin 等[55]系统分析了云计算数据交换场景下代理重加密的功能与安全属性，并归纳了对应的安全特征。Nuñez 等[56]则根据实现方式对不同类型的代理重加密进行了分类和分析。

在多实体共存的跨域场景中，代理节点与用户的抗共谋攻击能力仍存在短板。受传统代理重加密方法的安全局限性影响，相关研究主要集中在抗共谋方向。Guo 等[57]通过引入问责机制提高了代理节点操作的可审计性，同时抑制了恶意共谋行为。Zhou 等[58]提出了一种基于代理重加密的算法，该算法能够有效应对跨域环境的串谋攻击，同时防范数据泄露，解决了非可信云环境的数据安全隐患。Pan 等[59]提出了一种三因素认证和抗共谋密钥协商协议，通过协同设计认证环节和密钥协商过程来有效降低攻击者在认证和密钥协商阶段串谋的风险，拓展在可信数据空间中抗共谋机制的应用范围。

在应用层面，代理重加密与区块链技术的融合已成为研究热点。Agyekum 等[60]利用区块链的分布式特性，实现物联网环境下数据访问过程的控制，并对链上代理重加密操作进行验证和跟踪。Ahsan 等[61]在此基础上进一步引入了匿名化机制，该方案在提升数据共享效率的同时强化用户隐私保护，即便密文转换完成，数据接收者仍可保持身份匿名。

阈值代理重加密方案通常基于双线性映射与(t,n)秘密共享机制实现。其中，n表示代理节点总数，t表示恢复秘密所需的最小协作节点数。设 G_1和 G_2表示阶为 p的循环群，p为大素数，定义双线性映射：

$$e: G_1 \times G_2 \to G_2 \tag{1}$$

并满足双线性性质：

$$e(g^x, g^y) = e(g,g)^{xy} \tag{2}$$

其中，e 表示双线性映射，g 为群生成元，x 与 y为随机指数。与此同时，(t,n)秘密共享机制将重加密密钥拆分为多个密钥份额，借助拉格朗日插值算法恢复原始密钥：

$$f(x) = \sum_{i=1}^{k} f(x_i)\lambda_i \tag{3}$$

其中，$f(x_i)$ 为各代理节点持有的密钥份额，λ_i 为对应的拉格朗日插值系数。仅当不少于 t个代理节点协

同参与时，才能完成合法密文转换，从而降低单点代理失陷带来的密钥泄露风险。Liu 等[62]提出一种可公开验证的阈值代理重加密方案，由多代理节点协作完成密文转换，同时支持外部验证。Feng 等[63]面向工业互联网场景，构建基于无证书阈值代理重加密的云链协作架构，为可信数据空间的多主体权限转换与细粒度访问控制提供了新的技术思路。

现有代理重加密技术的研究方向主要包括数据授权转换、抗共谋安全增强，以及基于区块链的可信数据共享。现有研究大多依赖单一信任假设，或预设代理节点诚实可信，难以在多代理协同场景下实现强安全防护。后续研究需重点解决两大问题：在保障安全性的前提下降低代理节点计算开销，同时构建细粒度、可动态演化的授权控制机制。

表 2 梳理了现有代表性方案的核心方法、优缺点及适用场景。

4 跨域密钥认证与协商

可信数据空间中数据流通往往跨越多个信任域，不同域之间缺少预设信任关系与统一身份管理体系，致使跨域密钥管理除面临传统单域场景的各类安全挑战外，还需解决域间信任建立、异构认证体系互通、群组协作动态成员管理等新问题。由此催生出面向跨域协同的密钥认证与协商技术，整体流程如图 2 所示。安全域 N 与安全域 F 为两个具备独立身份管理与认证机制的异构安全域。其中，证书颁发机构负责本域用户证书签发与身份验证，通过交叉认证为跨域信任建立基础；跨域信任中继负责认证请求转发、随机数同步与审计日志留存，实现不同安全域之间的认证协商与信任传递。该机制依托随机挑战与动态认证凭证降低重放攻击风险，但仍需防范中间人攻击、中继节点伪造等安全威胁。针对该领域，下文从两个方向展开讨论：一是面向两方或多方通信的跨域双向认证与会话密钥协商；二是面向群组通信的跨域群组密钥协商。

4.1 跨域双向认证与会话密钥协商

在可信数据空间跨域数据交换场景中，数据请求者与提供者分属不同信任域，双方通常无直接信任关系，面向单信任域设计的传统认证机制难以直接适配该类跨域场景，而依托信任转移或第三方中介又易引入新的安全漏洞。在此背景下，跨域双向认证与密钥协商技术成为支撑多平台安全通信的核心机制。该技术可在不同信任域之间搭建可信认证通道，并在认证完成后协商会话密钥，保障后续跨域数据交换安全开展。

随着数据安全保护需求提升，跨域双向认证的

表 2 密钥生命周期管理方案对比

Table 2 Comparison of key lifecycle management schemes

方案	核心方法	计算开销	动态扩展性	优点	缺点	适用场景
文献[41]	无状态密钥轮换、后量子密码可插拔	中	高	无需集中式状态同步，支持后量子扩展	部署验证不充分	去中心化身份管理
文献[45]	无线信道特征提取、挑战响应	低	中	抗重放攻击，无需可信第三方	依赖信道环境	物联网无线密钥协商
文献[46]	多子载波相位差密钥生成	低	中	随机性与稳定性高，轻量级	对多径环境敏感	物联网、车联网物理层安全
文献[49]	平台安全架构模型	中	中	硬件层实现密钥保护，提升安全性	依赖特定硬件平台	物联网设备
文献[52]	移动边缘计算	高	高	去中心化存储与可审计，边缘协同提升密钥分发效率	区块链存储开销大	移动服务场景
文献[57]	可问责代理重加密	中	中	提高代理节点可审计性，抗共谋	问责机制增加额外计算开销	需审计的数据共享
文献[58]	抗数据泄露的代理重加密	中	高	抵抗算法替换攻击，计算、存储成本低	算法复杂度较高	不可信云环境下的物联网数据共享
文献[63]	无证书阈值代理重加密	高	高	可抵御串谋攻击和数据篡改	云链协同机制复杂	工业互联网

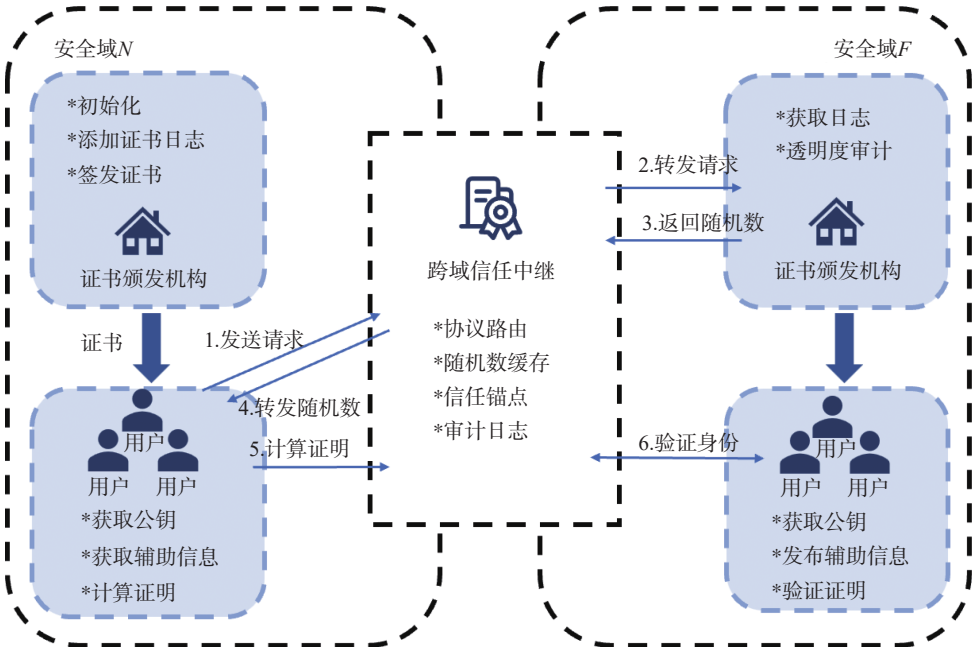

图 2　通用跨域认证机制流程

Fig. 2　Process of general cross-domain authentication mechanism

研究重点逐步转向匿名认证方向。Luo 等[64]开发了去中心化跨域匿名认证系统，在提升系统稳定性的同时降低对单一信任节点的依赖，认证过程中可有效保护用户隐私，适配可信数据环境下的敏感数据防护需求。Cui 等[65]基于区块链实现跨域匿名认证方案，该方案引入分布式账本记录认证信息，保障数据可追溯与不可篡改特性，同时提升系统安全能力与运行可靠性。Tong 等[66]同样采用区块链技术，设计基于联盟区块链的物联网跨域认证与隐私保护方案，可低成本、高效率部署于资源受限物联网场景，为终端设备提供隐私保护与安全高效的通信服务。针对设备认证与多因素认证方向，Shen 等[67]提出基于区块链的跨域安全设备认证机制，依托联盟区块链与签名机制保障通信安全。Zhang 等[68]融合区块链与多因素认证机制，设计跨域设备认证协议，有效弥补单因素认证的不足。Hou 等[69]提出融合智能合约的区块链跨域密钥管理方案，经验证，该协议具备较高的安全性与运行效率。Chen 等[70]将认证与密钥协商一体化设计，提出高效隐私保护型跨域认证方案，方案基于哈希树实现轻量化设计，响应速度快，且可兼容现有 PKI 与证书透明系统。王菲菲等[71]提出基于雾计算的智能医疗三方认证与密钥协商协议，在用户、边缘节点与云服务器之间构建动态认证关系，实现身份认证与会话密钥协商一体化协同，提升跨域医疗数据共享的访问可信性与通信安全性。

综上所述，现有研究通过引入分布式账本、多因素认证及双层区块链架构，有效提升了跨域认证的安全性、隐私保护能力与系统可扩展性。现有方案大多依托区块链或专用可信基础设施搭建跨域信任体系，在高频跨域交互场景下，通信与共识开销偏高。同时，多数协议难以适配动态信任变更、跨域身份快速切换场景，多域协同认证的一致性也难以保障，在大规模异构可信数据空间中部署仍存在一定难度。

4.2　跨域群组密钥协商

可信数据空间内群组跨域通信需求持续增长，相较于两方跨域认证，跨域群组密钥协商面临更为复杂的应用场景。一方面，群组成员分属不同信任域，相互之间缺乏固有信任关系；另一方面，群组动态性强，群组权限调整易引发权限频繁变更。在此背景下，如何保障多平台、多组织在异构在线环境中的通信安全，成为亟待解决的难题。

跨域群组密钥协商广泛应用于工业互联网、车联网、卫星网络、物联网协同等场景，不同场景对密钥协商的功能需求存在明显差异。在动态物联网场景中，节点异构性强、可信程度低，且成员频繁上下线，密钥状态需要持续同步。Pérez 等[72]构建基于区块链的跨域群组密钥管理系统，该系统在区块链上记录群组成员状态与密钥更新信息，使不同信任域节点无需预先互信，即可同步获取统一的密钥状态，重点解决异构设备跨域密钥同步与去中心化

管理问题。Ali 等[73] 面向异构动态物联网设备，设计分布式区块链密钥管理协议，协议依托区块链完成域间密钥信息共享与同步，跨域群组成员可脱离中央协调节点，自主完成密钥更新与状态校验。

在车联网与智能合约协同场景中，系统对密钥协商的自动化、实时性要求更高。智能合约的引入，进一步提升了跨域群组密钥协商的自动化协作水平。Wei 等[74] 提出基于智能合约的分布式认证密钥协商协议，该协议将跨域认证与密钥协商逻辑以智能合约形式部署于区块链，各域节点无需依赖中央信任机构，即可完成群组密钥配置与更新。Naresh 等[75] 面向大规模无线传感器网络，聚焦动态成员管理与隐私保护，将智能合约作为核心控制模块，设计动态群组密钥协商方案，降低动态成员管理的人工干预成本，提升系统响应效率。在动态拓扑、高移动性网络场景（如飞行自组网、混合卫星网络）中，群组结构变化剧烈，对密钥更新效率与拓扑适配能力要求严苛。Zhou 等[76] 提出新型密钥协商协议，采用改进树形密钥封装机制，支持高动态环境下的密钥快速更新，即便面对大规模群组，也可有效降低计算开销。针对现有方案在混合卫星场景中存在的动态分层拓扑适配性弱、域间数据传输隐私保护不足等问题，Tan 等[77] 设计跨域异构数据聚合方案，该方案采用动态群组密钥协商机制，兼具高安全性与运行性能。此外，Braeken 等[78] 提出一种非对称群组密钥协商协议，利用椭圆曲线算法降低运算开销，提升群组密钥整体计算效率。

现有研究主要围绕区块链驱动的群组状态同步、智能合约支撑的自动化密钥管理、面向动态拓扑的高效群组密钥更新机制展开。但在高动态、大规模群组场景中，现有方案易受通信与同步开销制约；在成员频繁变更场景下，密钥一致性维护与实时更新能力仍有欠缺。同时，复杂跨域异构网络场景下的系统扩展性与稳定性仍有待提升。

表 3 给出跨域认证技术代表性方案对比情况。

5 未来展望

针对可信数据空间的数据流通场景，现有研究在密钥管理框架、密钥全生命周期管理以及密钥跨域认证协商方面已取得显著成果，但在工业互联网、车联网、智慧医疗等复杂应用场景中，现有研究仍存在诸多技术短板与挑战。结合本文综述内容，未来可从以下方向开展深入研究。

（1）动态开放环境中的自适应密钥管理机制

可信数据空间内的节点接入、退出与用户权限变更均具备高度动态性，如车联网场景下车辆节点动态上下线、工业互联网场景下设备权限实时调整、跨组织数据共享场景下用户角色动态切换等。现有密钥管理方案大多预设网络结构与运行环境处于稳定状态，难以适配节点成员与访问权限的频繁动态变更，易引发密钥更新延迟、同步开销过高等问题。未来可进一步探索基于上下文感知与动态风险评估的密钥管理框架，推动密钥策略由传统固定规则驱动模式向环境状态自适应驱动模式转变，提升复杂动态环境下的自主适配能力。该自适应能力不仅体现在对网络结构变动的适配性上，还可依据节点状

表 3 跨域认证技术代表性方案对比

Table 3 Comparison of representative cross-domain authentication schemes

方案	核心方法	计算开销	动态扩展性	优点	局限性	适用场景
文献[65]	区块链匿名认证	高	中	可追溯、防篡改、隐私保护	共识开销较大	工业物联网跨域认证
文献[70]	多梅克尔哈希树、匿名认证	低	高	兼顾效率与隐私，与PKI系统集成	平衡性待验证	通用跨域认证
文献[72]	区块链记录群组状态	高	高	无需直接信任即可获得一致密钥状态	区块链存储与通信开销大	物联网群组通信
文献[74]	智能合约分布式认证密钥协商	高	高	自动化协作，减少人工干预	合约安全性需额外保障	车载自组网络
文献[76]	树状架构、拓扑感知	中	高	降低动态拓扑下密钥更新开销	维护成本较高	飞行自组网络
文献[77]	动态群组密钥协商	高	高	支持跨域高效协同与动态更新	混合网络场景复杂	混合卫星网络

态、权限变更与信任关系动态调整密钥生成、更新与撤销策略，进一步提升可信数据空间整体运行的稳定性。

（2）密钥管理中的轻量级与高安全性的平衡

现有轻量级密钥方案可有效降低设备资源消耗，但在智慧医疗、边缘数据共享等高敏感场景中，数据安全等级要求极高，而终端设备计算、存储资源受限，导致高强度安全加密需求与轻量化部署要求存在固有矛盾。同时，高性能加密算法在资源受限终端设备上的运行效率普遍偏低。未来可构建加密强度自适应调节机制，依据设备资源算力、数据敏感等级与实时安全态势动态匹配加密策略，实现安全性能与运行效率的动态平衡，适配不同应用场景的差异化部署需求。

（3）数据空间中的跨域协同安全机制

在跨组织数据共享、跨区域政务协同、多云平台数据流通等典型场景中，当前可信数据空间跨域认证方案大多依赖区块链、智能合约或其他可信第三方基础设施。对外部可信设施的过度依赖会导致通信开销居高不下，且随着交互频次增加，系统安全漏洞暴露风险显著提升。后续研究需重点突破跨域信任传递、多方协同认证与去中心化密钥协商机制等关键技术，以解决跨域交互中的身份映射、动态信任评估、群组成员一致性维护等难题，进而构建适配复杂数据流通场景、低成本、高可扩展的跨域安全协作模型。

（4）智能安全化的密钥管理策略

现有基于静态规则配置的安全策略与密钥管理方法，已难以适配复杂多变的业务需求与攻击范式。在工业互联网、智慧城市、大规模数据流通场景中，网络攻击呈现动态化、隐蔽化的发展趋势，传统静态密钥管理模式无法及时识别异常访问行为、快速响应突发安全威胁。未来可将机器学习、智能决策与用户行为分析技术与密钥管理深度融合，实现密钥更新时机预测、未授权访问检测、授权路径优化与攻击威胁主动预警等功能，推动可信数据空间安全体系持续迭代优化，促使密钥管理机制由“被动响应”向“主动预测、自主决策”演进。

6　结束语

可信数据空间已成为支撑全域数据安全流通的核心基础设施。本文系统梳理了可信数据空间的密钥管理基础机制、关键核心技术与跨域协同方案，现有研究在密钥生成、分发、更新、撤销等全流程技术上已取得长足进展，逐步形成适配跨域协同、动态数据流通场景的密钥安全管理体系。当前研究仍存在诸多短板：密钥管理机制对节点动态变动、权限频繁迭代的适配性不足；跨域协同存在通信开销高、信任维护复杂度大等问题；传统静态安全策略难以适配多变的攻击范式与业务场景。

总体而言，未来可信数据空间密钥管理研究将聚焦动态自适应调控、高效跨域协同、智能安全管控三大核心方向，推动密钥管理机制由静态规则驱动逐步向环境感知、自主决策、协同演化模式演进，为复杂异构场景下的可信数据流通提供更安全、高效、可扩展的技术支撑。

参考文献：

[1] 白玉真，贾轩，王思源，等. 数据流通利用设施关键技术与建设路径研究 [J]. 信息通信技术与政策，2025，51（4）：34-39.
Bai Y Z，Jia X，Wang S Y，et al. Research on key technologies and construction paths of data circulation and utilization facilities[J]. Information and Communications Technology and Policy，2025，51（4）：34-39.

[2] 李恒，李凤华，史欣怡，等. 面向数据跨域安全流通的访问控制研究综述 [J]. 通信学报，2025，46（4）：238-254.
Li H，Li F H，Shi X Y，et al. Research on access control for secure cross-domain data circulation[J]. Journal on Communications，2025，46（4）：238-254.

[3] Singh A K，Sánchez M O，Caparros M G，et al. A security analysis of European data space architectures[J]. Data Science and Engineering，2025，10（3）：455-472.

[4] Costagliola A R，Mazzocca C，Bujari A，et al. VESPACE：a verifiable blockchain-based data space solution to empower the data economy[J]. Computer Communications，2025，239：108180.

[5] Liao Y Q，Kong X G，Yin L，et al. A trusted industrial data space for automotive supply chain （TIDS-ASC）：enabling secure and traceable data sharing[J]. Information Processing & Management，2026，63（5）：104710.

[6] Ghaffari F，Bertin E，Crespi N，et al. Distributed ledger technologies for authentication and access control in networking applications：a comprehensive survey[J]. Computer Science Review，2023，50：100590.

[7] Kharjana M，Pohrmen F H，Sahana S C，et al. Blockchain-based key management system in named data networking：a survey[J]. Journal of Network and Computer Applications，2023，220：103732.

[8] Badirova A, Dabbaghi S, Moghaddam F F, et al. A survey on identity and access management for cross-domain dynamic users: issues, solutions, and challenges[J]. IEEE Access, 2023, 11: 61660-61679.

[9] Alsheavi A N, Hawbani A, Othman W, et al. IoT authentication protocols: challenges, and comparative analysis[J]. ACM Computing Surveys, 2025, 57(5): 1-43.

[10] Yoon S, Han S, Hwang E. Joint heterogeneous PUF-based security-enhanced IoT authentication[J]. IEEE Internet of Things Journal, 2023, 10(20): 18082-18096.

[11] Wang C Y, Wang D, Duan Y H, et al. Secure and lightweight user authentication scheme for cloud-assisted Internet of Things[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2961-2976.

[12] Bhuva D R, Kumar S. A novel continuous authentication method using biometrics for IOT devices[J]. Internet of Things, 2023, 24: 100927.

[13] Sivaselvan N, Bhat K V, Rajarajan M, et al. A new scalable and secure access control scheme using blockchain technology for IoT[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 2957-2974.

[14] Saleem M A, Li X, Mahmood K, et al. Secure RFID-assisted authentication protocol for vehicular cloud computing environment[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(9): 12528-12537.

[15] Akram W, Mahmood K, Li X, et al. An energy-efficient and secure identity based RFID authentication scheme for vehicular cloud computing[J]. Computer Networks, 2022, 217: 109335.

[16] OASIS Standard. Key management interoperability protocol (KMIP) version 3.0[S/OL]. [2026-01-12]. https://docs.oasis-open.org/kmip/kmip-spec/v3.0/csd01/kmip-spec-v3.0-csd01.pdf

[17] Gandino F, Ferrero R, Montrucchio B, et al. Fast hierarchical key management scheme with transitory master key for wireless sensor networks[J]. IEEE Internet of Things Journal, 2016, 3(6): 1334-1345.

[18] Najafi Z, Babaie S. A lightweight hierarchical key management approach for internet of things[J]. Journal of Information Security and Applications, 2023, 75: 103485.

[19] Yu F R, Tang H, Mason P C, et al. A hierarchical identity based key management scheme in tactical mobile ad hoc networks[J]. IEEE Transactions on Network and Service Management, 2010, 7(4): 258-267.

[20] Lo J W, Hwang M S, Liu C H. An efficient key assignment scheme for access control in a large leaf class hierarchy[J]. Information Sciences, 2011, 181(4): 917-925.

[21] Odelu V, Das A K, Goswami A. A secure effective key management scheme for dynamic access control in a large leaf class hierarchy[J]. Information Sciences, 2014, 269: 270-285.

[22] Ragab H H, Bettahar H, Bouadbdallah A, et al. An efficient key management scheme for content access control for linear hierarchies[J]. Computer Networks, 2012, 56(8): 2107-2118.

[23] Xu C, Ren W, Yu L C, et al. A hierarchical encryption and key management scheme for layered access control on H. 264/SVC bitstream in the Internet of Things[J]. IEEE Internet of Things Journal, 2020, 7(9): 8932-8942.

[24] Abu A O, Qatawneh M, Almobaideen W, et al. A new hierarchical architecture and protocol for key distribution in the context of IoT-based smart cities[J]. Journal of Information Security and Applications, 2022, 67: 103173.

[25] Kokoris K E, Malkhi D, Spiegelman A. Asynchronous distributed key generation for computationally-secure randomness, consensus, and threshold signatures[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 1751-1767.

[26] Das S, Xiang Z, Kokoris K L, et al. Practical asynchronous high-threshold distributed key generation and distributed polynomial sampling[C]//32nd USENIX Security Symposium (USENIX Security 23). 2023: 5359-5376.

[27] Lu K J, Qian Y, Guizani M, et al. A framework for a distributed key management scheme in heterogeneous wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(2): 639-647.

[28] Xi W, Duan M C, Bai X X, et al. KEEP: secure and efficient communication for distributed IoT devices[J]. IEEE Internet of Things Journal, 2021, 8(16): 12758-12770.

[29] Panda S S, Jena D, Mohanta B K, et al. Authentication and key management in distributed IoT using blockchain technology[J]. IEEE Internet of Things Journal, 2021, 8(16): 12947-12954.

[30] De R M, Mantas G, Rodriguez J, et al. DECENT: decentralized and efficient key management to secure communication in dense and dynamic environments[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(7): 7586-7598.

[31] Hao Y, Cheng Y, Zhou C, et al. A distributed key management framework with cooperative message authentication in VANETs[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(3): 616-629.

[32] Al A M, Hashim F, Jahari Hashim S, et al. Hierarchical blockchain structure for node authentication in IoT networks[J].

Egyptian Informatics Journal，2022，23（2）：345-361.

[33] Raza S，Seitz L，Sitenkov D，et al. S3K：scalable security with symmetric keys：DTLS key establishment for the internet of things[J]. IEEE Transactions on Automation Science and Engineering，2016，13（3）：1270-1280.

[34] Dammak M，Senouci S M，Messous M A，et al. Decentralized lightweight group key management for dynamic access control in IoT environments[J]. IEEE Transactions on Network and Service Management，2020，17（3）：1742-1757.

[35] Gupta M，Kumar B S. Lightweight secure session key protection，mutual authentication，and access control （LSSMAC）for WBAN-assisted IoT network[J]. IEEE Sensors Journal，2023，23（17）：20283-20293.

[36] Yildiz H，Cenk M，Onur E. PLGAKD：a PUF-based lightweight group authentication and key distribution protocol[J]. IEEE Internet of Things Journal，2021，8（7）：5682-5696.

[37] Wazid M，Das A K，Odelu V，et al. Design of secure user authenticated key management protocol for generic IoT networks[J]. IEEE Internet of Things Journal，2018，5（1）：269-282.

[38] Benmalek M. SEKM-IoT：secure and efficient key management for dynamic access control in smart IoT systems[C]//Proceedings of the 2024 IEEE 21st International Conference on Smart Communities：Improving Quality of Life using AI，Robotics and IoT （HONET）. Piscataway：IEEE Press，2024：97-102.

[39] Guo D K，Cao K，Xiong J，et al. A lightweight key generation scheme for the Internet of Things[J]. IEEE Internet of Things Journal，2021，8（15）：12137-12149.

[40] 蒋京玮，汪定，张国印，等. 面向移动边缘计算的密钥管理协议 [J]. 计算机学报，2022，45（6）：1348-1372.
Jiang J W，Wang D，Zhang G Y，et al. Private key management scheme for mobile edge computing[J]. Chinese Journal of Computers，2022，45（6）：1348-1372.

[41] Wang J S. A single-root，multi-curve，context-isolated，pqc-pluggable cryptographic identity primitive with stateless secret rotation[PP]. arXiv preprint arXiv：2511.20505，2025.

[42] Tan Z W，Bao Y T，Tan Y，et al. Attribute-based weight exchange with direct revocation mechanism for fine-grained data sharing[J]. IEEE Transactions on Dependable and Secure Computing，2026，23（3）：6602-6619.

[43] Li Y F，Xu Y J，Zhang G Q，et al. HIPCAM：data stream-driven group key management for in-vehicle network with seamless key updates[J/OL]. IEEE Transactions on Vehicular Technology，2026. DOI：10.1109/TVT.2026.3660852.

[44] Kajita K，Emura K，Ogawa K，et al. CGKA-FA：secure and flexible group key agreement with authentication update[J]. Journal of Information Processing，2026，34：294-308.

[45] Huan X T，Miao K T，Chen W，et al. Kerra：an Internet of Things wireless key generation resistant to replay attacks[J]. IEEE Internet of Things Journal，2024，11（17）：29035-29048.

[46] Yuan X W，Jiang Y，Li G Y，et al. Wireless channel key generation based on multisubcarrier phase difference[J]. IEEE Internet of Things Journal，2024，11（20）：32939-32955.

[47] Yang H Q，Xu W T. LLMKey：LLM-powered wireless key generation scheme for next-gen IoV systems[C]//Proceedings of the IEEE INFOCOM 2025 - IEEE Conference on Computer Communications Workshops （INFOCOM WKSHPS）. Piscataway：IEEE Press，2025：1-6.

[48] Ghosal A，Conti M. Key management systems for smart grid advanced metering infrastructure：a survey[J]. IEEE Communications Surveys & Tutorials，2019，21（3）：2831-2848.

[49] Jung J，Kim B，Cho J，et al. A secure platform model based on ARM platform security architecture for IoT devices[J]. IEEE Internet of Things Journal，2022，9（7）：5548-5560.

[50] Yang J R，Chen S，Cao Y. A PUF-based key storage scheme using fuzzy vault[J]. Sensors，2023，23（7）：3476.

[51] Prabhu K B，Ganapathy S. A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications[J]. Computer Networks，2019，151：181-190.

[52] Li J X，Wu J G，Chen L，et al. Blockchain-based secure key management for mobile edge computing[J]. IEEE Transactions on Mobile Computing，2023，22（1）：100-114.

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

[54] Jiang J W，Wang D，Zhang G Y. QPause：quantum-resistant password-protected data outsourcing for cloud storage[J]. IEEE Transactions on Services Computing，2024，17（3）：1140-1153.

[55] Qin Z G，Xiong H，Wu S K，et al. A survey of proxy re-encryption for secure data sharing in cloud computing[J]. IEEE Transactions on Services Computing，2016，（99）：1.

[56] Nuñez D，Agudo I，Lopez J. Proxy re-encryption：analysis of constructions and its application to secure access delegation[J]. Journal of Network and Computer Applications，2017，87：193-209.

[57] Guo H，Zhang Z F，Xu J，et al. Accountable proxy re-encryption for secure data sharing[J]. IEEE Transactions on De-

pendable and Secure Computing，2021，18（1）：145-159.

[58] Zhou Y Y，Zhao L，Li F G，et al. Exfiltration-resistant proxy re-encryption for IoT data sharing in unreliable clouds[J]. IEEE Transactions on Dependable and Secure Computing，2025，22（4）：4070-4085.

[59] Pan G L，Tan H W，Zheng W Y，et al. Three-factor authentication and key agreement protocol with collusion resistance in VANETs[J]. Journal of Information Security and Applications，2025，90：104029.

[60] Agyekum K O，Xia Q，Sifah E B，et al. A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain[J]. IEEE Systems Journal，2022，16（1）：1685-1696.

[61] Ahsan M，An B，Kanhere S S，et al. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain[J]. Journal of Network and Computer Applications，2020，176（prepublish）：102917.

[62] Liu T, Zhang L, Kan H B, Zhang J H. Publicly verifiable threshold proxy re-encryption and its application in data rights confirmation[EB/OL]. Cryptology ePrint Archive, 2025. https://eprint.kobi.one/2025/345.pdf.

[63] Feng J Y，Li Y，Wang T，et al. A certificateless threshold proxy re-encrypted data-sharing scheme with cloud-chain collaboration in industrial internet environments[J]. IEEE Internet of Things Journal，2024，11（20）：33247-33268.

[64] Luo C Y. Distributed cross-domain anonymous authentication scheme in internet of things[J]. IEEE Internet of Things Journal，2025，12（13）：24710-24721.

[65] Cui J，Liu N，Zhang Q Y，et al. Efficient and anonymous cross-domain authentication for IIoT based on blockchain[J]. IEEE Transactions on Network Science and Engineering，2023，10（2）：899-910.

[66] Tong F，Chen X，Wang K M，et al. CCAP：a complete cross-domain authentication based on blockchain for Internet of Things[J]. IEEE Transactions on Information Forensics and Security，2022，17：3789-3800.

[67] Shen M，Liu H S，Zhu L H，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.

[68] Zhang Y，Li B，Wu J X，et al. Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT[J]. IEEE Internet of Things Journal，2022，9（22）：22501-22515.

[69] Hou D K，Zhang J. Blockchain assisted cross-domain key management for seaminglessly secure metaverse[J]. Blockchain：Research and Applications，2026：100460.

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

[71] 王菲菲，汪定. 基于雾计算的智能医疗三方认证与密钥协商协议 [J]. 软件学报，2023，34（7）：3272-3291.
Wang F F，Wang D. Fog computing-based three-party authentication and key agreement protocol for smart healthcare[J]. Journal of Software，2023，34（7）：3272-3291.

[72] Pérez G J C，Braeken A，Benslimane A. Blockchain-based group key management scheme for IoT with anonymity of group members[J]. IEEE Transactions on Information Forensics and Security，2024，19：6709-6721.

[73] Ali K M，Kouicem D E，Doudou M，et al. A decentralized blockchain-based key management protocol for heterogeneous and dynamic IoT devices[J]. Computer Communications，2022，191：11-25.

[74] Wei L，Cui J，Zhong H，et al. A decentralized authenticated key agreement scheme based on smart contract for securing vehicular ad-hoc networks[J]. IEEE Transactions on Mobile Computing，2024，23（5）：4318-4333.

[75] Naresh V S，Allavarpu V V，Reddi S. Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN[J]. The Journal of Supercomputing，2022，78（6）：8708-8732.

[76] Zhou T，Hong S，Shen J，et al. An efficient iTreeKEM-based group key agreement protocol for flying ad-hoc networks[J]. IEEE Transactions on Mobile Computing，2025.

[77] Tan H，Fang C，Shen J，et al. Cross-domain heterogeneous data aggregation with dynamic group key agreement for hybrid satellite networks[J]. IEEE Transactions on Dependable and Secure Computing，2026，23（3）：4830-4844.

[78] Braeken A. Pairing free asymmetric group key agreement protocol[J]. Computer Communications，2022，181：267-273.