Exploration on the Application of Post-Quantum Cryptography in the Railway Field

Tian Zhao[1] Jun Dong[2] Yongnan Zhai[3] Jia Li[3]

1. China Railway Information Technology Group Co., Ltd., Beijing, 1000442, China
2. China Railway Express Co., Ltd., Beijing, 100003, China
3. China Railway Information Engineering Group Co., Ltd., Beijing, 100844, China

Abstract

With the rapid development of quantum computing technology, traditional public key cryptographic systems such as RSA and ECC, which rely on integer factorization or elliptic curve discrete logarithms, face significant security challenges from quantum algorithms like Shor's. As a critical information infrastructure, the railway information system covers various core operations including dispatch control and train-ground communication, imposing high domain-specific requirements and stringent real-time constraints on communication confidentiality, device authentication, and command integrity. A quantum attack would severely threaten train operation safety and system continuity. Addressing these security needs, this paper proposes a comprehensive railway quantum-resistant cryptography application solution featuring "local enhancement and overall compatibility," incorporating post-quantum cryptography (PQC) standards such as ML-KEM, ML-DSA, and SLH-DSA released by NIST.

Keywords

post-quantum cryptography; railway information system; secure communication; identity authentication; secure boot

抗量子密码在铁路领域应用探索

赵恬[1] 董军[2] 翟永南[3] 李佳[3]

1.中国铁路信息科技集团有限公司，中国·北京 100044
2.中铁快运股份有限公司，中国·北京 100000
3.中铁信息工程集团有限公司，中国·北京 100844

摘要

随着量子计算技术的快速发展，RSA、ECC等依赖大整数分解或者是椭圆曲线离散对数的传统公钥密码体系面临着被Shor等量子算法显著减弱的安全挑战。铁路信息系统作为关键信息基础设施，覆盖调度控制、车地通信等诸多核心业务，对通信保密、设备认证及控制命令完整性具有极高的领域特殊性与严苛的实时性约束。一旦遭受量子攻击，将严重威胁行车安全与系统的连续运行。针对上述安全需求，本文结合NIST已发布的ML-KEM、ML-DSA及SLH-DSA等抗量子密码（PQC）相关标准，提出了一种“局部增强、整体兼容”的铁路抗量子密码应用总体方案。

关键词

抗量子密码；铁路信息系统；安全通信；身份认证；安全启动

1 引言

量子计算的发展使传统公钥密码体系面临着全新的安全挑战。RSA、ECC等传统密码机制都是依赖大整数分解、离散对数或椭圆曲线离散对数等数学困难问题，诚然这些方法在经典计算条件下的确具有较高安全性，但当足够规模的量子计算机出现后，这些密码机制可能受到Shor算法等量子算法的显著削弱[1]。

【基金项目】铁路商用密码体系架构及应用研究，子课题1铁路信息系统密码应用架构及体系研究（项目编号：WJZG-CKY-2024041（2024P02））。

【作者简介】赵恬（1996-），女，中国北京人，硕士，工程师，从事网络安全、信创、商用密码研究。

铁路信息系统覆盖多类业务。对通信保密性、设备身份真实性、控制命令完整性和操作可追溯性均有较高要求。一旦攻击者通过伪造合法设备、篡改控制命令或替换软件镜像，将会严重影响行车安全和系统连续运行。

当前NIST已发布ML-KEM[2]、ML-DSA[3]和SLH-DSA[4]等多项抗量子密码标准，为工程应用提供了技术依据。也提出对关键基础设施，应尽可能更早开展密码资产盘点、风险分级和迁移路线规划。明确优先保护对象、机制选择和部署路径。

2 抗量子密码与铁路安全需求分析

2.1 抗量子密码概述

抗量子密码是在经典计算技术和未来量子计算技

术下均能够保持安全性的密码体制。是主要基于格或哈希的数学结构构建。从功能划分上看，主要包括密钥建立机制和数字签名机制。密钥建立机制主要用于在通信双方协商共享密钥；数字签名机制多用于保证身份真实性、消息完整性与行为不可否认性。对于铁路系统而言，安全通信链路通常需要密钥建立机制配合对称加密实现保密性与完整性保护；而在设备身份认证、控制命令保护、软件发布验证和日志固化等场景则更依赖数字签名机制来建立可信关系。

2.2 典型抗量子算法及使用场景

ML-KEM 是当前抗量子密钥建立的主流方案之一，多用于在通信双方之间建立共享秘密。其基本思路是接收方生成密钥对，发送方利用公钥封装共享秘密，接收方再通过私钥恢复该秘密，双方据此派生会话密钥。ML-KEM 用途明确且性能较均衡，可适合用于铁路中心节点、车站系统、边缘网关和远程运维链路的安全通信。

ML-DSA 是当前抗量子数字签名标准化体系中的重要算法之一，适合用于铁路系统中的身份认证、控制命令签名、配置对象保护和日志留存等场景。在铁路业务中，签名机制不仅用于证明消息内容未被篡改，还需要进一步关联发送主体、权限状态、时间戳和业务序列等信息。这种绑定关联的方式可以有效避免签名数据脱离原有业务环境后的重复利用，极大程度上降低了伪造命令、篡改配置和重放历史消息的风险。

SLH-DSA 以及 LMS/XMSS/HSS 等哈希类签名机制更适合低频、高价值对象保护。由于其签名尺寸或状态管理要求较高，不宜用于高频控制业务，更适合根证书、离线发布对象、安全启动链和长期归档数据等场景。

2.3 铁路系统抗量子安全需求

铁路信息系统的安全防护具有极强的领域特殊性。由于行车调度与列车控制业务对实时性与连续性要求极高，密码机制的引入受到严格的性能约束，即关键控制链路的安全改造必须在不损耗系统原有实时响应能力的前提下进行[5]。

在安全目标的优先级上，铁路系统与常规IT网络存在显著差异。除基础的通信机密性外，系统的运行安全更依赖于实体的身份认证与指令的完整性校验。在典型业务场景中，未授权的设备接入或指令伪造往往比单一的数据泄露具备更大的破坏性。这要求现阶段的安全架构必须将设备身份鉴权、控制指令的细粒度授权、审计日志的不可否认性以及远程运维的安全接入作为核心防护对象[6]。

此外，铁路通信网络呈现典型的异构特征，其中既包含算力充沛的调度中心等骨干节点，也广泛分布着计算及存储资源受限的车载端与轨旁嵌入式设备，因此在铁路通信网络中安全方案难以依靠单一算法实现统一部署。针对调度记录、运行日志及固件镜像等具有长生命周期的核心资产，其密码防护机制还需具备前瞻性，以应对未来量子计算技术带来的长期保密与长期可信挑战。

3 抗量子密码在铁路领域的应用方案设计

3.1 总体方案设计

铁路领域引入抗量子密码不是简单地对现有密码组件的简单替换，而需要在现有安全体系、业务逻辑和设备条件约束下，对信任建立方式、关键对象保护方式以及密钥管理模式进行有针对性的重构。本文将铁路业务划分为“通信链路、控制命令、软件对象、信任与密钥”四类关键对象，并分别匹配密钥封装、数字签名、哈希校验和分级信任管理机制。

从总体上看，该方案设计主要围绕以下四个目标展开。

密码体制必须要满足未来量子威胁条件下的长期安全需求。铁路系统中大量设备服役周期较长，部分通信数据、日志记录、策略文件和发布对象还具有长期保存和长期验证需求。方案设计必须考虑未来密码环境变化带来的影响，使关键安全环节不再依赖容易受到量子攻击影响的传统公钥机制。换言之，方案设计的首要目标，是在铁路系统中逐步建立面向未来的量子安全基础。

保持既有系统总体稳定。铁路业务具有实时性强、连续运行要求高和改造窗口有限等特点，任何安全机制的引入都不能以明显增加系统复杂度和运行风险为代价。因此，本文不主张对铁路系统进行彻底的架构重构，而是强调在尽量保留现有业务协议、对称加密流程和控制逻辑的基础上，优先替换公钥协商、身份认证和对象签名等关键环节。也就是说，方案设计应遵循“局部增强、整体兼容”的思路。

实现异构业务对象的差异化防护。 前述分析表明，铁路系统内的通信链路、控制指令、系统固件（如升级包与配置文件）及信任启动链等安全客体，在时延敏感度、数据载荷、更新频次及安全定级上表现出显著的异质性。若采用单一抗量子密码套件进行全局覆盖，不仅易导致底层资源的错配与浪费，更可能突破高实时性场景的性能阈值。基于此，本研究引入细粒度的分类防护策略，将抗量子密码机制的选型与不同业务客体的多维属性相耦合，以确保安全防护粒度与实际工程需求的最优适配。

构建支持平滑演进的工程落地范式。 鉴于铁路信

息系统具备超大规模、多级架构与广域分布的网络特征，全面、瞬时的密码体系重构在工程层面缺乏一定可行性。因此，本方案在设计之初即内化了分层演进的原则，支持以中心枢纽、骨干链路及高密级数据为先导节点率先构筑抗量子防线，进而呈辐射状向边缘终端及常规业务延伸。这种具备高可扩展性与平滑迁移能力的设计，是确保该安全架构具备现实部署价值的关键前提。

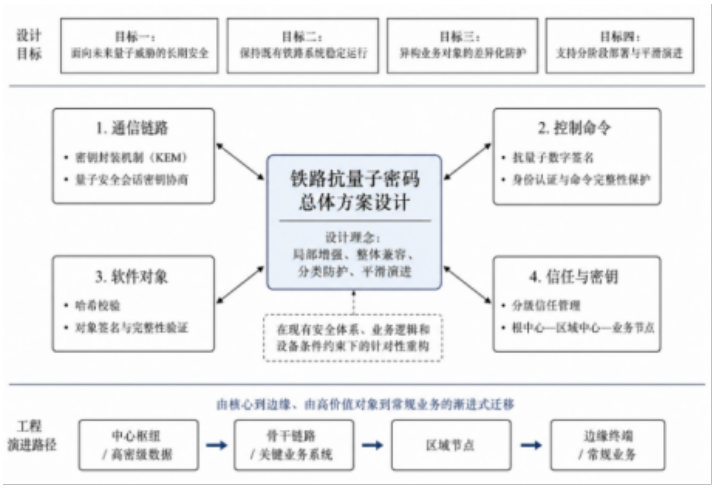


图1 铁路领域抗量子密码总体方案设计

3.2 面向安全通信的应用方案

现阶段，铁路系统的通信防护重心聚焦于调度控制链路及车地通信网络。由于控制指令的下发具有严格的毫秒级时延约束，且对节点真实性与传输防窃听的要求极高，亟需高效且安全的密钥交换协议作为底层支撑。针对上述高频通信链路，设计并部署时延开销可控的抗量子密钥建立机制，能够有效弥补现有公钥体系在未来算力环境下的脆弱性。

以“调度中心—车站网关”通信为例，调度中心通常需要与沿线车站网关、区域边缘节点或专业业务系统保持稳定连接，传输调度状态、运行计划、监测数据和运维指令。可在连接建立阶段引入ML-KEM完成抗量子密钥建立，在连接建立后继续使用既有对称加密机制保护业务数据。这一策略兼顾了底层密码升级与上层业务的可用性，是抗量子技术在铁路关键信息基础设施中落地最具工程可行性的优先方向。

车站网关预先持有由区域信任中心签发的设备证书和ML-KEM密钥封装公钥；调度中心在建立连接前获取网关证书、当前策略版本和证书状态信息。紧接着调度中心使用车站网关的ML-KEM公钥生成共享秘密和封装信息，并将封装信息放入握手消息。为防止握手消息被替换或降级，调度中心还应使用自身签名密钥对关键字段进行签名，关键字段包括双方身份、封装信息、随机数、时间戳、链路标识和策略版本。

车站网关收到握手消息后，首先验证调度中心证书是否由可信区域中心签发，再检查证书是否过期、是否被吊销以及是否具备访问该链路的权限。验证通过后，网关利用自身私钥对封装信息进行解封装，恢复共享秘密，并对确认消息进行签名返回。最终双方基于共享秘密、双方身份、随机数、链路标识和策略版本派生会话密钥。后续业务数据仍由对称密钥保护，抗量子算法的开销主要集中在会话入口，不会在每一条业务报文中重复出现。

这样的优势在于，抗量子机制能够在只改变会话入口而不改变大量既有业务数据。对于固定长连接链路，密钥封装和签名验证带来的开销会被长时间会话摊薄；对于资源受限链路，可通过会话复用、证书缓存和网关代理验证降低负担。当会话持续时间过长、累计报文数超限、链路异常重连或策略版本变化时，系统应触发重新握手，以降低长期使用同一会话密钥带来的风险。

3.3 面向身份认证与控制命令的应用方案

在铁路抗量子密码体系中，实体的身份鉴权与指令级防护构成了整个安全架构的信任根基。铁路网络中广泛分布着各类计算主体，其面临的核心威胁往往源于主动的身份冒充与指令篡改。在缺乏强身份边界的场景下，即便底层通信链路已实现高强度加密，攻击者仍可通过伪造合法主体或重放历史报文轻易旁路信道防护，进而破坏系统的控制逻辑。为此，亟需依托区域信任中心构建抗量子公钥基础设施（PQC-PKI），通过签发融合设备标识、角色属性、生命周期及细粒度权限的后量子设备证书，实现全网计算节点的强可信接入。

列控中心或车站联锁系统需要向轨旁设备下发参

数更新、状态切换或控制确认类命令。发送端在生成命令时，不仅对命令正文进行签名，还应将命令编号、发送主体、接收对象、线路或区间标识、业务类型、权限等级、时间戳、序列号和策略版本一并纳入签名输入。

接收端在处理命令时应执行三类校验。第一类是密码校验，即检查发送端证书链和签名是否合法，确认命令内容未被篡改。第二类是权限校验，即确认发送端角色是否允许在当前业务域内下发该类命令，接收对象是否与证书和命令字段一致。第三类是时序与重放校验，即检查时间戳是否在允许窗口内，命令编号和序列号是否匹配，策略版本是否仍然处在有效期限内。只有三类校验均通过时，设备才进入执行流程；否则应拒绝命令并记录审计日志。

该机制构筑了三重安全闭环，有效抵御了铁路网络中的典型主动攻击。依托非对称签名的不可伪造性，阻断了未持有合法私钥的越权节点发起指令伪造的攻击路径；基于密码学散列与签名算法的强绑定特性，通信载荷内的任何比特级异动均将触发校验机制阻断，确保了传输过程中的严格数据完整性；通过将时间戳、递增序列号、目标节点标识及访问控制版本等上下文参量纳入签名运算，实现了控制报文的时空域隔离，从根本上消除了跨场景或跨时序的重放攻击隐患。

3.4 面向软件升级与安全启动的应用方案

铁路系统内的软件更新、配置下发及可信启动流程，构成了网络中典型的低频发、高价值核心业务流。针对升级包、参数库与底层固件等长效数据资产，任何形式的恶意篡改、非法替换或降级部署，均会瓦解系统的底层信任根基，进而引发全局性的级联失效。基于此，针对此类资产的防护策略必须超越单一的起源认证，建立多维度的准入校验模型。系统需在加载或执行前，对数字对象的版本时效性、适用域、目标实体标识及下发策略进行强校验，从而确保变更操作的绝对合规与合法。

当系统进行单元固件升级时，将由发布中心首先生成升级包，并同步生成元数据文件。元数据应包含版本号、适用设备类型、目标区域、最低允许版本、依赖版本、发布时间、发布批次、策略编号和回滚规则。紧接着发布中心计算升级包的摘要，并对摘要和元数据整体签名。区域中心在接收升级对象后可进行一次预验证，再按线路、区域或设备类型进行灰度下发。

设备端在接收到升级对象后先验证发布方证书和签名，再对升级包摘要进行重新计算并与元数据中的摘要比对。若签名合法但版本号低于最低允许版本，或目标区域、设备类型、依赖版本不匹配，设备依然会拒绝安装。对于行车安全相关设备，可采用双分区或A/B分区机制：新版本先写入备用分区，完成完整性校验和启动前校验后再切换；若启动失败，则回退到最近可信版本，并向区域中心上报告警。

系统的配置文件与安全策略同样需纳入防护范畴。鉴于此类数据载荷具有轻量化、高频更新的动态特征，它极易成为攻击者篡改控制逻辑、实施行为劫持的高危切入点。仅停留在基础签名验签层面的防护已显不足。系统需构建上下文的深度校验机制，将目标属性与密码学原语强制绑定。针对触及核心控制逻辑的高敏感度变更，确保策略演进全生命周期的绝对安全可控。

安全启动用于保证设备从上电开始处于可信状态。设备内置根信任公钥或证书，启动时依次验证引导程序、固件镜像、关键驱动、配置对象和业务应用。任一环节失败，设备应进入告警、隔离、备份启动或受限运行模式，避免加载未知代码。

根证书、引导程序和制造阶段固件等根层对象更新少、风险高，应由离线环境签发，并在检修或受控维护窗口写入设备。普通业务固件和配置对象可通过常规流程下发，但仍需受根信任链约束。这样可形成“发布—安装—启动—运行—审计”的安全闭环。

3.5 根信任与密钥管理方案

根信任与密钥管理是各类抗量子方案长期运行的基础。若缺少统一信任体系，单点算法安全也难以形成整体防护。本文建议采用“根中心—区域中心—业务节点”三级模型。根中心负责根密钥、系统策略和区域授权；区域中心负责证书签发、密钥状态同步和吊销信息发布；业务节点持有通信密钥、签名密钥或设备证书，完成具体业务处理。

铁路局管范围内同时存在高速铁路车站、普速线路车站、动车段、通信机房和沿线轨旁设备。根中心不直接参与每一次业务认证，而是通过离线或高安全级别环境为区域中心签发授权证书；区域中心根据设备注册信息为车站网关、车载终端和轨旁设备签发业务证书，并维护吊销列表或增量状态列表。业务节点在建立会话、处理命令或安装升级对象前，优先检查本地缓存的证书状态；若缓存过期或长期无法同步，则进入降级或受限模式，不再执行高风险操作。

密钥体系应按功能分类，避免一把密钥承担多种用途。通信密钥用于会话建立；身份签名密钥用于设备认证、命令签名和日志签名；对象发布密钥用于升级包、参数库和策略文件签发；根层签发密钥用于根证书、引导对象和高价值信任对象。分类管理虽会增加运维成本，但可降低单点泄露影响，避免某类密钥

失效后波及全部业务。

密钥生命周期应覆盖生成、分发、启用、更新、吊销和销毁。根层密钥、区域中心密钥和发布密钥宜在受控环境或硬件安全设备中生成；业务节点密钥可在安全芯片、可信执行环境或受控初始化流程中生成。密钥分发应与设备注册、证书装载和策略绑定同步进行，避免密钥启用与权限状态不一致。

吊销机制应兼顾实时性和可用性。铁路系统可采用“中心维护、区域缓存、节点检查”的方式管理证书状态。中心保存全量吊销记录，区域中心下发增量状态列表，业务节点在会话建立、命令处理或升级验证前检查本地缓存。若节点长期无法同步状态，应进入降级或受限模式，避免继续执行高风险操作。

密钥轮换应结合铁路运维节奏。中心平台和区域网关可采用较短轮换周期，现场设备和车载终端则应结合检修窗口、固件升级和证书到期时间更新。根层密钥不宜频繁变更，应采用离线保存、多方审批和严格审计；普通业务密钥则应支持到期提醒、异常吊销和应急替换。这样才能使抗量子密码方案具备长期工程可运行性。

4 结论与展望

铁路领域引入抗量子密码并不是简单替换 RSA 或 ECC，而是要根据业务对象和设备能力进行分类部署：通信链路重点采用 ML-KEM 建立会话密钥，身份认证和控制命令重点采用 ML-DSA 保障真实性与完整性，软件升级和安全启动重点采用摘要签名、链式验证和哈希类签名增强长期可信。抗量子密码在铁路系统中具有明确应用价值，但其工程落地仍需进一步验证。后续研究可围绕真实铁路网关、车载终端和嵌入式设备开展原型测试，量化不同算法在签名尺寸、验证耗时、证书链长度和带宽占用方面的影响；同时，还应结合行业标准和设备更新周期，研究传统密码与抗量子密码混合部署、灰度迁移和统一运维管理机制。随着抗量子标准和产业生态逐步成熟，铁路信息系统有必要提前完成密码资产梳理和迁移路线设计，为未来长期安全运行奠定基础。

参考文献

[1] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring [C]// Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe: IEEE, 1994: 124-134.

[2] National Institute of Standards and Technology (NIST). FIPS PUB 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard [S]. Gaithersburg: NIST, 2024.

[3] National Institute of Standards and Technology (NIST). FIPS PUB 204: Module-Lattice-Based Digital Signature Standard [S]. Gaithersburg: NIST, 2024.

[4] National Institute of Standards and Technology (NIST). FIPS PUB 205: Stateless Hash-Based Digital Signature Standard [S]. Gaithersburg: NIST, 2024.

[5] 国务院. 关键信息基础设施安全保护条例[Z/OL]. 2021.

[6] 中国国家标准化管理委员会. GB/T 39786-2021信息安全技术信息系统密码应用基本要求.