doi: 10.3969/j.issn.1672-6073.2025.02.010

量子通信技术在城市轨道交通中的适用场景探索

蒋运平[1]，缪亚军[1]，李剑剑[2]，辛　华[1]，甘建文[2]
（1. 国科量子通信网络有限公司，上海 200120；2. 北京城建设计发展集团股份有限公司，北京 100037）

摘　要：我国城市轨道交通的信息化发展迅速，针对城市轨道交通信息系统的安全现状以及潜在的安全风险，研究量子通信技术在城市轨道交通建设过程中的应用场景。在现有城市轨道交通信息系统架构及建设方案的基础上，结合量子密钥分发网络在密码应用、数据安全保护等方面的优势，提出在安全计算环境、安全数据存储、安全数据流转等多个维度的融合创新思路，重点论述量子通信技术在数据的计算环境、安全传输、安全存储等环节发挥的数据安全流转保护作用，为后续量子通信技术在城市轨道交通信息化建设领域的深化应用提供参考。

关键词：城市轨道交通；清分及多线路中心系统；量子通信技术；量子密钥分发网络；数据安全
中图分类号：U231　　**文献标志码：**A　　**文章编号：**1672-6073(2025)02-0068-07

Exploration of the Application Scenarios of Quantum Communication Technology in Urban Rail Transit

JIANG Yunping[1], MIAO Yajun[1], LI Jianjian[2], XIN Hua[1], GAN Jianwen[2]
(1. CAS Quantum Network Co., Ltd., Shanghai 200120;
2. Beijing Urban Construction Design & Development Group Co., Ltd., Beijing 100037)

Abstract: This paper investigates potential applications of quantum communication technology in urban rail transit information systems, addressing current and emerging security challenges. Based on existing information system architectures in urban rail transit, we leverage the advantages of quantum key distribution networks for cryptographic applications and data security protection. The paper proposes integration strategies across multiple dimensions including secure computing environments, data storage, and data transmission. We specifically examine how quantum communication technology can enhance data security in computing environments, transmission processes, and storage systems. This research provides a framework for future applications of quantum communication technology in urban rail transit information systems.

Keywords: urban rail transit; AFC clearing center and multiple lines center; quantum communication technology; quantum key distribution network; data security

0　引言

当前城市轨道交通高速化、密集化、多样化、网络化和智能化的特征日益显现，全自动运行系统成为发展趋势，互联互通的网络化运营成为共识，当前城市轨道交通在信息化体系架构、数据交互、运营管理、基础资源使用、标准规范等方面还存在一定不足。在信息安全方面，虽然采用了传统的网络安全防护体系

收稿日期：2024-04-18　修回日期：2024-07-08
第一作者：蒋运平，男，本科，工程师，主要从事量子通信技术在轨交、电力、能源等领域的融合应用研究工作，jiangyunping@qtict.com
基金项目：国家自然科学基金青年基金项目(62302033)
引用格式：蒋运平，缪亚军，李剑剑，等. 量子通信技术在城市轨道交通中的适用场景探索[J]. 都市快轨交通，2025，38(2)：68-74.
JIANG Yunping, MIAO Yajun, LI Jianjian, et al. Exploration of the application scenarios of quantum communication technology in urban rail transit[J]. Urban rapid rail transit, 2025, 38(2): 68-74.

应对网络威胁，但量子计算日益迅猛发展，数据运行环境、数据存储和数据传输等环节存在未经授权的访问、数据泄露、系统/数据篡改等安全风险[1]。因此，城市轨道交通智能化建设向跨专业业务整合的方向迈进的同时，应结合创新、自主、可控的安全技术和产品，抵御数字时代轨交信息系统所面临的网络安全威胁和潜在安全风险，保障轨交业务系统安全、稳定、可靠的运行，强化数据安全能力。

量子通信技术是最先进入实用化阶段、发展最为成熟的量子信息技术，量子通信最典型的应用是量子密钥分发，即利用量子态来加载信息，通过一定的协议在通信双方之间共享密钥。量子力学基本原理保证了密钥的不可窃听，从而可从原理上实现无条件安全的量子保密通信。

量子通信技术能够与轨道交通领域所涉及的现有密码系统、密码协议及云平台、应用系统以模块化方式结合，实现即插即用。同时，配合使用一次一密(OTP)算法在量子通信网络的端到端之间实现信息论安全的加密，使其具备长期抗量子攻击的能力。

1 城市轨道交通信息安全面临的风险

近年来，国内城市轨道交通信息化系统的集成化、智能化程度越来越高，业务运行过程对信息系统的依赖性日益增强，信息安全面临巨大的挑战和威胁。城市轨道交通系统面临的信息安全风险包括但不限于以下 3 个方面。

1.1 云平台安全风险

云计算技术在轨道交通行业的应用发展遵循由易到难的原则，从起步较早的管理云、单专业云，发展到多专业云和线网城轨云，并开始应用到生产领域，城轨云无疑是目前赋能智慧城轨发展的必然选择[2]。

然而，国内传统的云平台在 OpenStack(开源的云计算管理平台)的基础上做了大量的优化和技术创新，主要框架还是 OpenStack。尽管传统的云平台提供了一些安全功能和机制，但其安全风险依然不容忽视。如云计算平台的虚拟化技术为用户提供了灵活的管理和使用策略，然而虚拟机共用主机资源，当其中一台被攻击时，其他虚拟机也存在被攻击的风险；云平台使用虚拟化技术提供计算和存储资源，虚拟化软件本身可能存在漏洞，攻击者可以通过虚拟机逃逸或者其他攻击手段获取宿主机的权限；云平台的数据安全风险包括数据在传输和共享过程中，未采取加密机制或加密机制存在缺陷，第三方调用采用明文方式进行传输等[3]，种类复杂多样的云上应用缺乏整体统一的安全规划和策略，快速应对云计算新技术演进面临的风险能力仍存不足。

1.2 数据安全风险

清分及多线路中心(AFC clearing and multi-line center，ACLC)作为负责城市轨道交通全线资金清算管理的重要系统，属于关键信息基础设施，在日常的运营过程中，自动售检票(automatic fare collection，AFC)系统产生了大量重要数据信息，例如设备运行指令信息、交易信息、乘客支付信息、乘客注册信息、人脸信息等，其中很多数据信息涉及系统安全、财务安全甚至人身安全，其数据的重要性不言而喻。AFC 系统采用传统的基于公钥基础设施(public key infrastructure，PKI)的方式部署加密模块(security access module，SAM)卡，对系统进行身份认证、文件签名、数据加密等，其安全机制的保障是基于密钥的安全性，通过复杂算法对数据进行加密。随着量子计算能力的日益提升，以及密钥破解算法的突破，基于计算复杂度和数学计算困难问题算法的破解难度和时间将大幅降低，攻击者通过窃听密钥协商过程并结合量子计算算力可瞬间破解出双方协商的密钥，窃取核心信息，传统密码体系的破解风险与日俱增。由于地铁密钥更新频率低，一旦被破解，将会对地铁业务造成不可估量的损失[4]。

近年来城市轨道交通建设保持高速增长，城市轨道交通数据从存储形式看，主要有系统配置文件、数据库文件、图形文件 3 种。数据库中关键字段以及重要的系统配置文件存在被窃取和泄露的风险。如 C3UK 公司在英国各地的火车站为乘客提供免费的 Wifi。2020 年 3 月该公司承认未能对包含用户信息的数据库提供保护，导致 1 万名英国铁路乘客的个人数据泄露。

1.3 传输安全风险

城市轨道交通的信号系统、通信系统、综合监控系统、清分中心系统和自动售检票系统等弱电系统通过轨道交通内部的专网实现平台系统与各节点终端的通信，内部存在多种通信链路，包括系统数据、设备实时状态、历史归档信息、事项记录、控制命令及结果反馈等，这些信息具有不同的数据流向，使用 TCP(传输控制协议)或 UDP(用户数据包协议)不同方式进行传输。在数据传输过程中，控制数据流尤为重要。一般数据流在操作员界面大多是进行数据的显示处理，而控制数据流赋予了操作员工作站对系统监控设备的控制功能，一旦篡改或伪造的控制命令下发，将

会对系统的正常运行造成损害，严重影响区域内人们的生活和工作，造成严重的经济损失。特别是在轨道交通无人驾驶线路中，不法分子通过使用网络抓包工具长期嗅探或相关行业人员获知信号系统的既有安全通信协议格式时，则可以通过伪装的方式给列车发送错误的运行控制信息和指令，从而产生难以预计的后果[5]。因此，城市轨道交通的传输安全风险需引起高度重视。

2022 年，高铁信号数据泄露事件。某科技人员通过相关电子设备，仅仅一个月采集的信号数据就已经达到 500 GB。不法分子如果利用这些数据故意干扰或恶意攻击高铁系统，严重时将会造成高铁通信中断，影响高铁运行秩序，对铁路的运营构成重大威胁；同时大量获取并分析相关数据，也存在高铁内部信息被非法泄露甚至被非法利用的可能。该案件是数据安全法实施以来，我国首例涉及高铁运行安全的危害国家安全类案件。

因此，在当前复杂的国际环境背景下，为应对以上潜在的风险和挑战，城市轨道交通信息系统迫切需要使用原创、自主、可控的安全技术和产品，抵御日益加剧的量子计算带来的威胁和挑战，为城市轨道交通信息系统的数字化转型升级和建设提供安全保障。量子通信技术基于物理原理，能够抗截获、抗窃听、抗破译地为通信双方分发具有信息理论安全性的对称密钥，从整体上提升密钥管理的安全性与独立性。当前，我国在量子通信技术领域处于世界领先地位，其体系设计、技术研发、产品化都具有自主可控的先发优势，在应对量子计算暴力冲击时，可有效保护现有数字化、信息化系统。

2 量子通信技术概述

量子通信是利用量子比特作为信息载体进行信息交互的通信技术。量子通信有两种典型的应用，分别是量子密钥分发和量子隐形传态。量子密钥分发是指利用量子态来加载信息，通过一定的协议在不同地点的通信双方共享密钥。量子力学基本原理保证了密钥的不可窃听，从而在原理上实现无条件安全的量子保密通信。量子隐形传态是指利用量子纠缠直接传输微观粒子的量子状态，即量子信息，而不用传输微观粒子本身。量子隐形传态可以连接量子信息处理单元构建量子网络，同时也是远距离密钥分发所需的量子中继的重要环节，因此国际学术界将量子密钥分发和量子隐形传态统称为量子通信。量子密钥分发是最先实现实用化和产业化的量子信息技术[6]。

本文以科技创新引领产业创新，积极培育和发展新质生产力为行动指引，深入分析，引入量子通信技术，通过量子密钥分发网络(quantum key distribution network，QKDN)和基于 QKDN 的密码应用系统(QKDN-harmonized security control system，Q-HSCS)与轨道交通信息系统融合形成融合量子通信技术的数据安全解决方案。该方案从安全计算环境、安全数据存储、安全数据流转等多个维度提升轨交系统的信息安全能力，打造轨交信息系统自主、可控、创新的安全管理机制。

2.1 量子密钥分发网络

量子密钥分发网络基于量子密钥分发技术(quantum key distribution，QKD)，收发两端利用随机的基矢制备或观测特定形态单光子(弱相干光)，实现量子密钥的跨域传递，具体原理如图 1 所示。量子密钥分发网络是由多个量子密钥分发节点通过量子密钥分发链路连接组成的网络。为连接网络的任意两个或多个用户提供量子密钥生成和更新功能，主要解决广域和城域范围内分布式节点之间密钥可达的问题[7]。

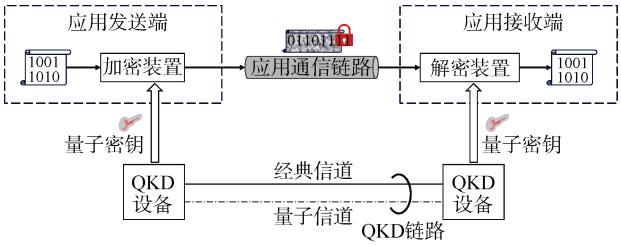

图 1 基于 QKD 的量子保密通信

Figure 1 Quantum-secure communication based on quantum key distribution

目前我国在量子通信领域已处于领先地位，在卫星量子通信方面，我国研制并成功发射了世界首颗量子科学实验卫星“墨子号”，在国际上率先实现了星地量子通信。随后，我国发射了世界首颗量子微纳卫星“济南一号”，为构建低成本、实用化的量子星座奠定基础。在城际量子通信方面，我国建成了国际上首条远距离光纤量子通信骨干网“京沪干线”。截至 2022 年底，我国建设完成的国家量子通信骨干网络地面干线总里程超过 10 000 km，覆盖京津冀、长三角、粤港澳、成渝等重要区域，已初步满足实用化要求[8]。

2.2 基于 QKDN 的密码应用系统 Q-HSCS

基于 QKDN 的密码应用系统是基于 QKDN 网络优势研发的量子密码应用体系，它构造了一种新型的建立在安全可靠密钥分发基础上、针对分布式业务或分布式业务承载平台间数据流转策略的安全管控系统，

是信息和通信技术(information and communications technology，ICT)与量子密钥分发网络融合的桥梁。

基于QKDN的密码应用系统Q-HSCS由融合安全管理平台(harmonized security control management，HSCM)和安全执行模块(security executive module，SEM)两部分组成，采用星型控制体系。HSCM是SEM的中心管理平台，对SEM进行集中管理和控制，具备用户、业务管理，设备、网络管理，互联互通以及密钥管控能力。SEM通过软件开发工具包(software development kit，SDK)与QKDN进行对接，实现节点间密钥共享和多点之间量子密钥协同管理，通过应用程序编程接口(application programming interface，API)与云、业务侧、数据管理侧进行对接，结合QKDN优势实现对云、业务、用户的统一认证、操作集管理(策略)、数据/参数保护、关键进程保护，使得业务、数据的流转，承载平台的安全策略及虚拟化保护都在安全应用模块及关联设备中运行，结合QKDN的跨域一体化的密钥管控作为数据可控安全执行环境的管理策略触发要素。具体的Q-HSCS的应用流程如图2所示。

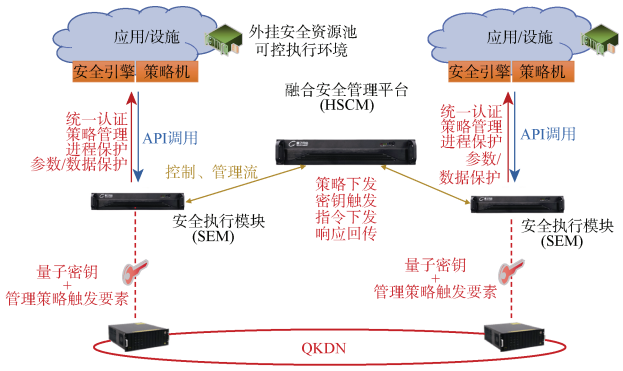

图2　Q-HSCS融合应用流程

Figure 2　Integration process of quantum-enhanced hybrid secure computing system

Q-HSCS体系通过在API中增加与被保护系统间在认证、执行动作、执行结果方面的控制机制，可以实现类似于安全增强型Linux(Security-Enhanced Linux)的安全控制策略功能，并在此基础上增加了执行动作比对。在专网、广域和城域范围内，Q-HSCS体系借助QKDN实现安全的密钥共享，结合经典密码应用，在面向广域场景时有效避免传统密钥迁移过程中“中间人攻击”的问题，同时基于可靠的密钥共享机制，保护HSCM对多个节点、多用户的协同策略分发或更新、策略库保护密钥更新。

3　融合应用场景建设思路

城市轨道交通作为我国重要的基础设施，其关键系统、关键设备的运行情况直接关系到城市轨道交通行业的信息安全程度。因此，基于我国量子技术目前的发展状况和产业现状，并结合城市轨道交通现有的架构，在线网中心可部署自主可控的量子通信设备、量子密码应用系统，打造轨交领域的量子安全层，依据业务系统的安全要求，通过融合适配实现量子安全能力赋能轨道交通信息系统，使其具备抗量子计算攻击能力，为城市轨道交通系统的安全、高效率运行奠定基础。本文基于现有的技术和产品，结合轨道交通信息系统的建设，提出以下3个典型应用场景的建设思路。

3.1　安全的计算环境

城轨云作为智慧城轨的数字底座，由生产中心、灾备中心、站段云平台组成。设置安全生产网、内部管理网、外部服务网3个域，由统一云平台进行管理，为轨交领域的“八大专业、十八个业务系统”提供资源服务，实现资源集约化、智能化。城市轨道交通的信号系统、通信系统、综合监控系统、清分中心系统和自动售检票系统等弱电系统是支撑城市轨道交通安全、稳定运行的关键控制系统和信息系统。因此，为这些系统提供自主、可控、安全、可靠的运行环境和存储环境显得非常重要[9-10]。

基于QKDN的量子密码应用系统与传统云平台的密钥管理组件融合适配，将量子安全能力赋能传统云平台，对传统云平台的计算、存储等虚拟化资源和云上应用进行全方位安全增强，提升云平台组件自身的安全以及所提供云服务的安全，增强云内和云间的数据安全流转能力，实现云平台的可控认证启动、可控运行监控、关键数据加密、一体化的密钥和密码应用管控，构建可控执行环境。因此，可在轨交的线网主用中心和灾备中心部署融合量子通信技术的云平台作为轨交信息化系统的安全基座，为业务系统的运行提供自主、可控、安全的计算环境和存储环境。具体的应用场景如图3所示。

3.2　安全的数据存储

ACLC系统是整个网络的资金清算管理中心，负责地铁系统内部各条线路及与其他商业实体之间的财务清算和运营管理，由数据处理服务器、前置通信服务器、历史数据服务器、文档管理服务器、网络管理服务器、运营管理服务器及附属设备共同构成，实现

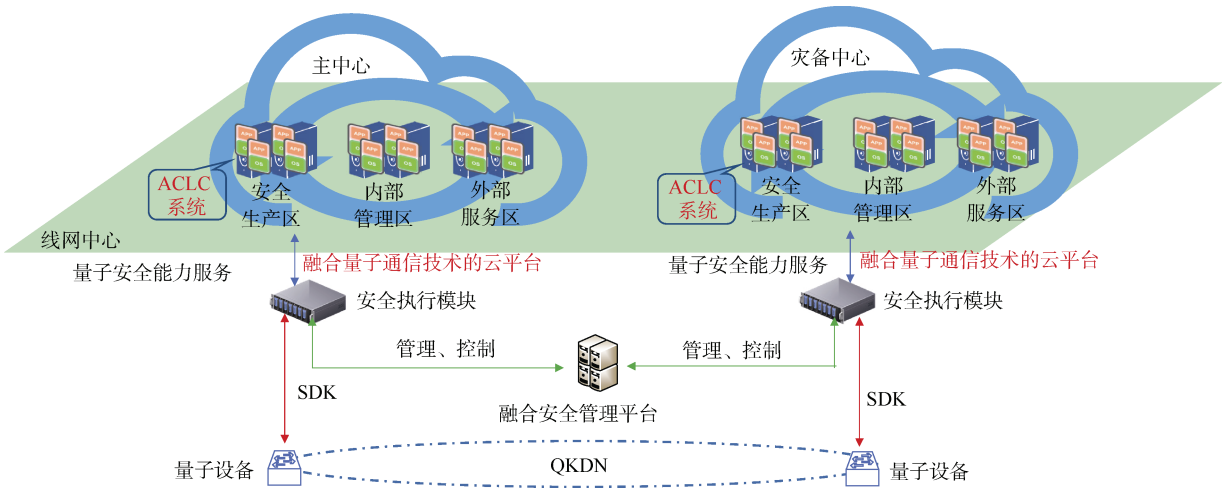

图 3　融合量子通信技术的云平台应用场景

Figure 3　Application scenarios of quantum communication technology in cloud platform

对各线路系统中所有设备进行监视，对全部数据进行收集和处理，对运营、票务、财务、维修进行集中管理。因此，ACLC 系统数据在轨道交通系统的安全管理、运行调度优化、客流管理与预测、故障处理与应急响应、决策支持与规划优化以及信息发布与乘客服务等方面发挥着至关重要的作用，对于保障城市轨道交通系统的安全、高效运行具有重要意义[11]。

加密是一种非常重要的数据保护方式，可以实现对数据的加密存储保护，防止敏感数据被非法获取、非法解密。在该场景中，可采用 Q-HSCS 体系的安全执行模块，通过授权的 SDK 接入量子通信网络获取高熵值的量子密钥，安全执行模块将量子密钥结合国密算法提升量子安全服务能力，通过 API 接口与 ACLC 业务系统融合适配，实现对系统的敏感/核心数据进行机密性、完整性保护，对系统的参数、策略及关键进程进行保护，保证数据的完整性和安全性的同时，降低数据泄露和黑客攻击的风险，帮助用户更好地利用数据实现商业和社会价值，具体实现场景如图 4 所示。

3.3　安全的数据流转

在城市轨道交通的信息系统中，可以利用量子通信技术对城市轨道交通中节点间的核心/敏感交互数据进行加密传输，从而提高节点间数据流转的安全性，数据安全流转的典型场景如下。

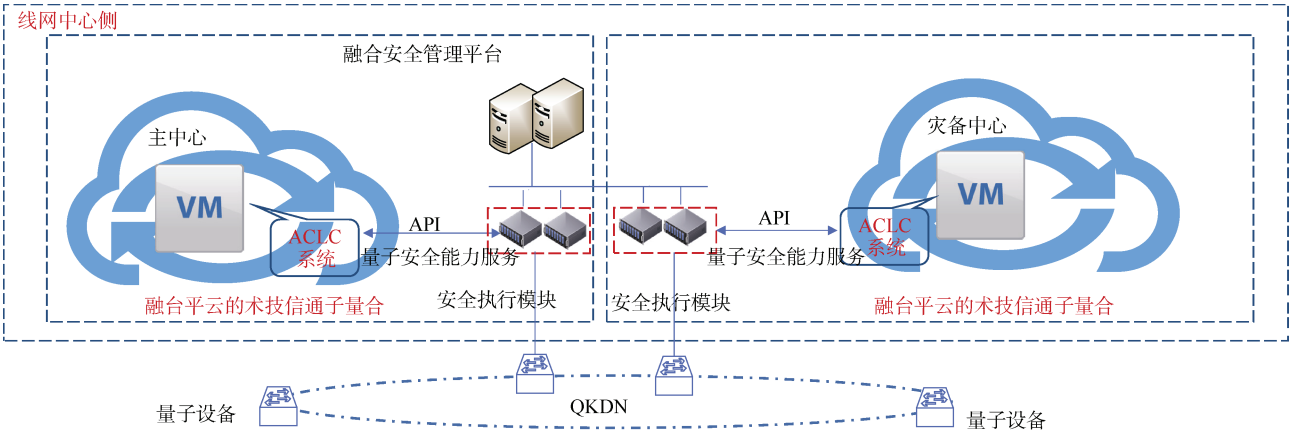

图 4　ACLC 系统与量子通信技术的融合应用场景

Figure 4　Application scenarios of quantum communication technology in AFC clearing center and multi-line center systems

3.3.1　线网主中心与灾备中心间数据流转

城市轨道交通作为城市公共交通的重要组成部分，在承担大规模客运服务的同时，需要保障行车安全以及良好的乘客体验。因此，要求城轨业务系统及其配套系统具备一定的可靠性保障，同时要求承载系统运行平台具备容灾能力。对于城轨业务而言，同城

主备数据中心架构可满足大多数业务灾备需求，主备中心间的光纤链路用于主备中心间数据的同步，保障业务的连续性[12]。

量子安全传输是基于量子密钥分发技术产生量子密钥，通过安全执行模块结合国密算法，对轨道交通信息系统的数据流量进行机密性和完整性保护，提供链路级安全传输服务，提升数据流转的安全水平。对于城市轨道交通中的主备中心之间数据的跨域流转，可在两端部署量子安全传输设备，基于 QKDN 以在线、实时产生的量子密钥作为密钥源，构建量子安全传输通道，保障主备中心之间的数据流转安全。量子安全传输设备可依据现场环境，旁路或串行部署，不介入应用系统，不改变原有安全策略，不影响现有网络架构，最大限度降低对原有架构的影响。具体实现如图 5 所示。

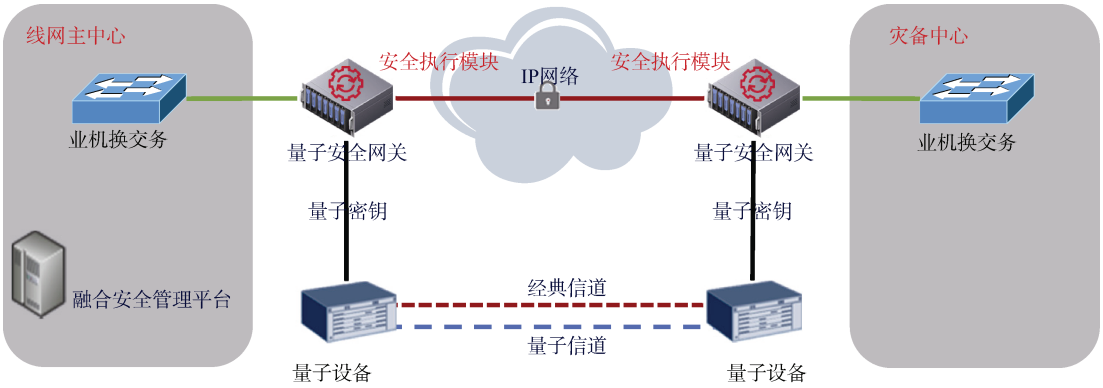

图 5　主备中心基于量子通信技术的安全传输应用场景

Figure 5　The application scenarios of quantum communication technology for secure transmission between primary and backup centers

3.3.2　线网中心与车站间数据流转

车站的半自动售票机、智慧客服等终端设备不仅包含交易信息，还可以进行人脸注册、移动支付票务处理等，涉及许多个人信息，并且车站分布广、现场环境复杂，车站与线网中心之间的数据流在交互过程中存在被有目的的拦截和窃取的可能，同时控制指令和数据也面临伪造和篡改的风险，车站到线网中心的信息安全难以保障[11]。

在该场景中，融合安全管理平台通过充注设备，将量子安全服务密钥通过安全介质转移到车站的安全执行模块中，从而与线网中心侧的安全执行模块构建量子安全传输通道，对关键业务信息进行加密传输。车站侧的业务系统可依据业务安全需求，通过 API 接口调用安全执行模块的量子安全服务能力实现对业务数据的机密性、完整性保护，保障数据的密文出局，实现城市轨道交通数据的安全流转。具体实现如图 6 所示。

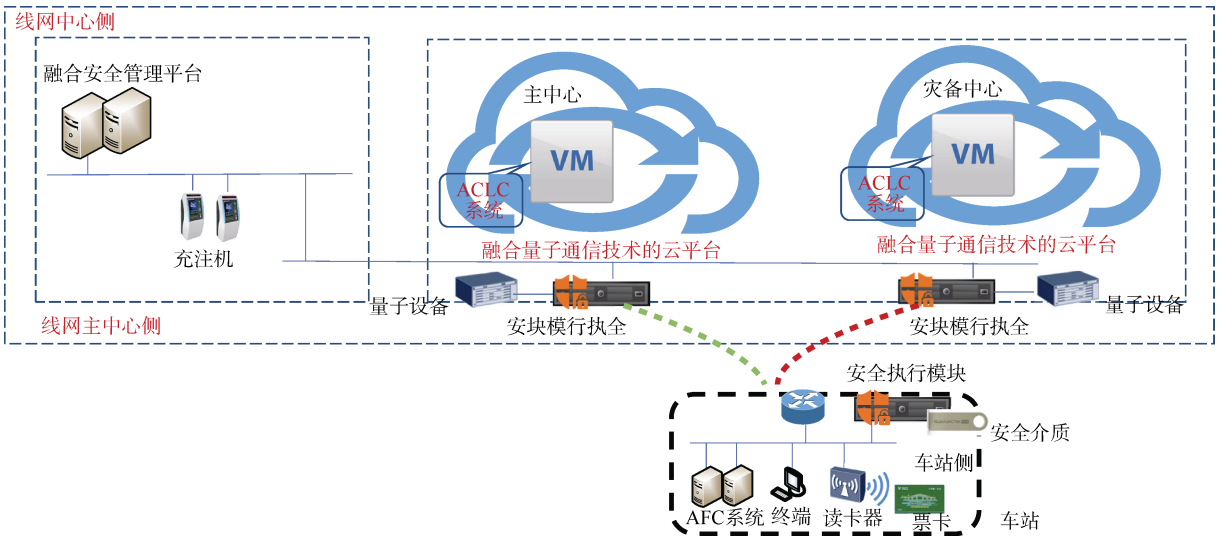

图 6　中心与车站基于量子通信技术的应用场景

Figure 6　Application scenarios of quantum communication technology in center-station connections

4 结束语

我国量子科技领域整体上已经实现了从跟踪、并跑到部分领跑的飞跃，在量子通信方面的研究和应用处于国际领先地位。量子通信技术作为抗量子计算攻击的重要手段，是保护现有数字化、信息化系统及关键基础设施等的有效措施。本文通过分析城市轨道交通信息系统在数据安全方面可能存在的风险和不足，提出了融合量子通信技术的数据安全建设思路，对于解决数据流转场景下的数据安全和安全管控问题具有一定的参考价值，在一定意义上提供了一种抗量子计算和抗经典介入攻击的手段，是探索量子信息技术在城市轨道交通领域形成新质生产力的尝试。

城市轨道交通系统是一个涉及多种技术领域，由多种设备、多种硬软件、多种设施组成的复杂系统。在当前国家科技自立自强、产业链供应链安全和信息安全自主可控的大背景下，城市轨道交通系统建设应结合先进的、自主可控的新兴技术，不断地研究和提高整体系统的安全性与可靠性。本文介绍的融合量子通信技术的数据安全建设思路在轨交行业的典型应用场景，旨在给出一种系统思想，为进一步探索量子通信技术在城市轨道交通领域的深化应用提供参考，加速量子信息等新兴技术在轨道交通领域形成新质生产力，推动城市轨道交通信息系统建设高质量发展。

参考文献

[1] 杨耀. 城市轨道交通数字化转型若干问题思考[J]. 城市轨道交通研究, 2024, 27(9): 301-304.
YANG Yao. Reflections on several digital transformation issues of urban rail transit[J]. Urban mass transit, 2024, 27(9): 301-304.

[2] 轨道世界. 我国城轨云发展概况. (2022-07-05)[2024-03-22]. https://t.cj.sina.com.cn/articles/view/1002429827/3bbfdd830190162wg?finpagefr=p_104.

[3] 中国网信网. 云计算服务主要安全风险及应对措施初探. (2022-07-22)[2024-03-22]. https://www.cac.gov.cn/2022-07/22/c_1660132930876799.htm?eqid=e04e92aa000b66f50000000564651e86.

[4] 王健, 李郁, 张亦然, 等. 量子保密通信在 AFC 系统的应用[J]. 铁路通信信号工程技术, 2023, 20(12): 78-82.
WANG Jian, LI Yu, ZHANG Yiran, et al. Application of quantum secure communication in AFC systems[J]. Railway signalling & communication engineering, 2023, 20(12): 78-82.

[5] 钱蔚, 徐烨. 国产加密技术在轨道交通信号系统中的应用[J]. 城市轨道交通研究, 2019, 22(10): 132-135.
QIAN Wei, XU Ye. Application of Chinese encryption technology in urban rail transit signal system[J]. Urban mass transit, 2019, 22(10): 132-135.

[6] 中国信息协会量子信息分会. 量子安全技术白皮书(2020)[M]. 北京: 中国信息协会量子信息分会, 2020.

[7] 国家市场监督管理总局, 国家标准化管理委员会. 量子保密通信应用基本要求: GB/T 42829—2023[S]. 北京: 中国标准出版社, 2023.

[8] 潘建伟. 量子信息科技的发展现状与展望[J]. 物理学报, 2024, 73(1): 7-14.
PAN Jianwei. Quantum information technology: Current status and prospects[J]. Acta physica sinica, 2024, 73(1): 7-14.

[9] 城市轨道交通云平台构建技术规范: T/CAMET 11002—2020[S]. 北京: 中国城市轨道交通协会, 2020.
Technical specification for cloud platform establishment of urban rail transit: T/CAMET 11002—2020[S].

[10] 城市轨道交通云平台网络安全技术规范: T/CAMET 11005—2020[S]. 北京: 中国城市轨道交通协会, 2020.
Technical specification for cloud platform cyber security of urban rail transit: T/CAMET 11005—2020[S].

[11] 周品荣. 城市轨道交通 ACLC 系统信息安全研究[J]. 信息技术与网络安全, 2020, 39(8): 72-75.
ZHOU Pinrong. Research on information security of urban rail transit ACLC system[J]. Information technology and network security, 2020, 39(8): 72-75.

[12] 城市轨道交通大数据平台技术规范: T/CAMET 11003—2020[S]. 北京: 中国城市轨道交通协会, 2020.
Technical specification for big data platform of urban rail transit: T/CAMET 11003—2020[S].

（编辑：王艳菊）