面向工业互联网的量子密钥服务管理系统方案研究

Research on Quantum Key Service Management System Scheme for Industrial Internet

马长链[1]，杜忠岩[1]，曲嘉旭[1]，黄晓宁[2]（1. 中国联通智能城市研究院，北京 100048；2. 江苏亨通问天量子信息研究院有限公司，江苏 苏州 215000）

Ma Changlian[1], Du Zhongyan[1], Qu Jiaxu[1], Huang Xiaoning[2]（1. China Unicom Smart City Research Institute, Beijing 100048, China; 2. Jiangsu Hengtong Qasky Quantum Information Research Institute Co., Ltd., Suzhou 215000, China）

摘 要：

随着互联网、大数据、物联网等信息技术迅猛发展，工业互联网应运而生，成为推动产业升级转型的关键力量。然而，工业互联网的发展进程也引发了数据安全方面的新挑战。针对工业互联网领域的数据安全问题，提出了一种基于量子密钥服务的方案，旨在通过量子加密技术构建端到端的安全流转机制，实现工业数据的实时加密保护。分析了工业互联网数据安全的需求，并概述了所提出的量子密钥服务管理系统方案的系统架构和应用价值，探讨了量子密钥的本地化存储、基于KMIP协议的密钥管理、三重证书机制的终端接入认证以及量子密钥的生命周期管控策略。

关键词：

工业互联网；量子密钥；工业数据安全；量子加密通信

doi：10.12045/j.issn.1007-3043.2026.02.014

文章编号：1007-3043（2026）02-0074-04

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the rapid development of information technology such as the Internet, big data, and the Internet of Things, the industrial Internet comes into being and has become a key force to promote industrial upgrading and transformation. However, this process has also brought new challenges to data security. To address the problem of data security in the field of industrial Internet, a scheme based on quantum key service is proposed, aiming at constructing end-to-end security flow mechanism through quantum encryption technology to realize real-time encryption protection of industrial data. It analyzes the data security requirements of industrial Internet, and summarizes the system architecture and application value of the proposed quantum key service management system scheme. The localization storage of quantum key, key management based on KMIP protocol, terminal access authentication based on triple certificate mechanism and the life cycle management strategy of quantum key are discussed.

Keywords：

Industrial Internet; Quantum key; Industrial data security; Quantum-encrypted communication

引用格式：马长链，杜忠岩，曲嘉旭，等. 面向工业互联网的量子密钥服务管理系统方案研究[J]. 邮电设计技术，2026(2)：74-77.

1 工业互联网数据安全需求分析

互联网、大数据、物联网等新一代信息技术快速发展，并迅速向传统工业生产领域渗透融合。世界各国积极抢抓工业体系数字化转型的机遇，纷纷发布国家战略推动新型工业化。在此背景下，工业互联网[1-2]应运而生，并成为新一轮产业升级转型的重要抓手。

工业互联网的发展打破了传统工业生产相对可信封闭的网络环境，使得涉及企业核心利益的生产数据、工艺数据、自动化控制数据、生产管理数据等工业数据暴露在互联网环境中，数据安全已经成为企业和社会关注的焦点，面向工业互联网领域的数据安全保护[3-8]也成为信息安全领域的重点研究方向。

针对工业互联网领域的数据安全问题，本文提出

收稿日期：2026-01-06

了面向工业互联网领域的量子密钥服务管理系统（下文简称“系统”）方案。该方案基于量子保密通信技术[9-12]，使用量子真随机密钥对工业数据进行实时加密保护，为工业互联网数据端到端安全流转构筑起坚实壁垒。

2 系统方案价值与设计

2.1 系统方案价值

该系统方案面向工业互联网领域，基于量子真随机密钥[13-16]的安全加密能力进行设计，具备对工业数据端到端加密的安全防护功能。系统可在不影响工业数据流实时性传输的前提下，实现大规模工业数据流的纵向加密管理，满足工业互联网场景下的低时延、高可靠加密传输需求。

2.2 系统方案设计

2.2.1 系统方案整体架构设计

系统负责对整个工业互联网体系中的各系统、各终端的加密密钥进行全生命周期安全管理。同时，系统方案的技术体系还需要考虑与工业互联网的强适配性，以及与业务体系的高融合性，以满足工业领域不同细分场景的数据加密需求。系统方案整体的技术架构如图1所示。

系统在业务逻辑实现上分为存储层、管理层和分发层。

存储层主要负责量子密钥本地化安全存储，上接量子密钥制备终端，获取真随机量子密钥，下接管理层，实现对量子密钥的负载均衡分配。

管理层主要负责量子密钥的全生命周期管控，管控内容包含量子密钥的存储安全、分发安全、更新安全、销毁安全等。同时，该层基于密钥管理互通协议（Key Management Interoperability Protocol，KMIP），实现不同密钥源的接入与互通。

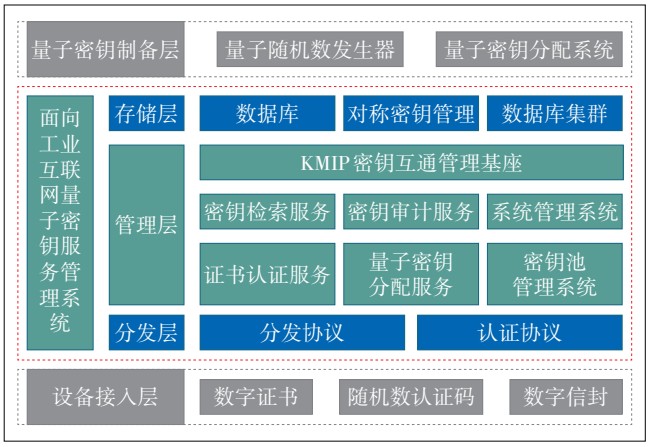

图1 系统方案的技术架构

分发层主要负责量子密钥分发，终端的安全接入认证、鉴权等相关功能。

在实际部署中，系统部署于工业互联网体系的PaaS层，为感知层、PaaS层、SaaS层赋能，实现对工业数据端到端的纵向安全加密。

2.2.2 功能模块规划

基于整体架构，系统方案包含6个功能模块。

a）密钥管控模块。负责量子密钥在体系中流转的全生命周期管控，包括密钥源的接入、基于KMIP协议的密钥互通管理、密钥池管理、密钥记录与统计等。

b）证书管理认证模块。负责对感知层设备的安全认证、平台与终端之间的密钥协商、证书的存储及管理、证书认证等。

c）密钥分发模块。负责分发两方的双向认证、线程处理、事件监听与心跳等。

d）加解密服务模块。负责密钥的请求与接收、对数据的加解密等。

e）接口服务模块。负责面向感知层端侧的南向接口服务、面向服务端侧的北向接口服务。

f）系统管理模块。负责整个系统平台的基础管理，如菜单管理、日志管理、资源管理等。

3 系统方案核心技术难点分析与实现

3.1 系统方案核心技术难点分析

系统方案设计的核心技术难点如下。

a）量子密钥本地化安全存储机制。

b）基于量子密钥的数字签名和身份认证机制。

c）基于量子密钥的工业数据处理与低时延加解密技术。

d）量子密钥的全生命周期管控机制。

3.2 系统方案核心技术实现

3.2.1 量子密钥本地化存储和密钥池管控技术

密钥的存储关乎业务系统的实际安全性。系统通过物理接口从量子密钥终端中获取量子真随机密钥源，然后采用SM1、SM2等对称、非对称国密算法，对量子密钥文件进行本地化存储。使用SM3国密签名算法来实现快速高效的密钥完整性和真实性验证，保证量子密钥在储存过程中不被破坏。在大规模连接场景下，可采用数据库集群实现密钥存储的负载均

衡，利用时序数据库做索引。这样既能保证量子密钥安全，又不影响密钥使用，还不提高系统负荷。

终端密钥池存储采用主备密钥池模式，保证量子密钥的持续可用性。密钥池管控系统提供量子密钥安全存储服务，支持以密文等方式保存量子密钥。

3.2.2 采用KMIP协议管控量子密钥建立统一管理基座

KMIP协议是一种用于密钥管理的互通协议，旨在提高信息的安全互通性。KMIP协议为密钥管理领域提供了统一的规范。

系统方案主要采用KMIP协议中的密钥检索、密钥更新等机制，旨在为其他密钥源或者密钥系统提供统一的标准体系通信架构。该方案将本地化的工业互联网量子密钥服务管理系统作为服务端，其他密钥源或者密钥系统作为客户端，通过双向认证机制，使用访问控制列表和安全关联来限制对特定密钥或操作进行访问。

3.2.3 基于三重证书机制提供工业互联网终端接入认证安全及密钥分发通道安全

证书是一种验证用户身份的电子文件，它将公钥的值与持有对应私钥的人、设备、服务等进行绑定。证书体系是指证书的逻辑层次结构，其中证书的信任关系呈现为树状结构。自签名是从根证书开始，由它签发二级根证书，二级根证书再签发其下级证书，依此类推，直至最后一级证书签发为最终用户证书。

认证体系理论上可以无限延伸，但从技术实现与系统管理角度来看，认证层次并非越多越好。层次越多，技术实现就越复杂，管理难度也会相应增大。一般国际上最大型的认证体系结构不超过4层，本系统方案采用3层认证体系，具体如图2所示。

第一层是自签名的用户根证书，它处于离线状态，是认证体系的安全根基。

第二层是由根证书签发的中间层证书，处于在线状态，它是签发系统用户的证书。

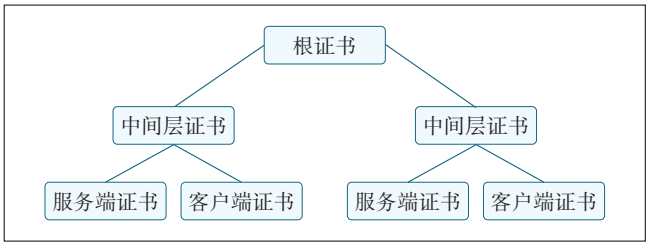

图2 用户证书认证体系

第三层是用户证书，由中间层证书签发。从用户证书的证书信任链可以看出整个用户的证书认证体系结构，用户证书在其应用范围内是受到信任的。

3.2.4 量子密钥生命周期管控策略及分级加密策略

量子密钥的生命周期涵盖量子密钥的采集、存储、分发、使用和销毁等过程。工业互联网量子密钥服务管理系统对量子密钥的整个生命周期进行安全监控，同时具备异常预警和报警处理功能。该系统对从量子密钥源采集的量子密钥进行特征值提取并设定有效期，然后将量子密钥存储于密钥池中并定期进行有效期检查和基于特征值的完整性检查。当量子密钥分发到移动通信终端后，系统会通过和终端的交互持续进行跟踪。对于检验异常（包括密钥异常和终端异常）的密钥，系统会对其进行处理、记录，并触发报警。

每次处理业务请求时，工业互联网量子密钥服务管理系统首先结合数据敏感程度列表及用户使用场景，对数据划定安全级别。对于安全级别不同的数据，分别采用对称加密、非对称加密、一次一密等算法进行加密。对称、非对称算法采用基于量子密钥的SM1、SM3、SM4、SM9算法，通过将量子密钥作为种子来提高算法的安全性。用户根据自己的需要对用户数据、业务操作数据提供不同级别预置加密策略，当无用户设定时，系统也会采用默认的国密算法进行加密，保障用户数据安全。

3.2.5 面向移动保密通信的量子密钥无线分发技术

经典的量子保密通信技术通常分为三层体系：最下层为量子密钥的制备，中间层为量子密钥的分发，最上层为量子密钥的应用。在制备层，常见的量子密钥制备方式有QKD网络以及量子随机数发生器。中间层可分为物理信道分发和业务信道分发，其中物理信道通常为有线信道，业务信道为4G、5G等无线信道。在工业互联网场景下，有线信道阻碍较多，无线业务信道分发成为首选，同时设计了基于内生安全的跨域密钥无线分发技术。

系统在网络运行状态下，通过策略的组合，在不影响网络运行和性能的前提下，实现网络动态安全防护。使不可信网络的安全性达到不低于专网（物理隔离）的安全程度。系统方案基于零信任接入鉴权和动态传输加密机制，实现动态安全防护。零信任接入鉴权保证了终端接入的可信性，动态传输加密机制实现了密钥的安全分发，以此构建整个密码分发体系的免

疫基础，从而实现整体密码分发的内生安全机制。

感知层终端首次接入时，需要采用基于量子密钥的数字证书认证方式对其进行身份认证。身份认证结束之后，在敏感业务传输之前或者高危行动之前，需进行动态的重复鉴权，以保证接入的可靠性。首先，感知层终端随机从量子密钥池中选取密钥，利用SM3算法对该部分量子密钥及终端身份信息生成哈希值，结合SM2算法形成签名，再基于签名制作证书，在初始化过程中将证书存储至终端安全域中，利用该证书进行身份认证，并设计了证书更新机制，以保证在业务鉴权时终端的安全。数字签名证书设计遵循《信息技术安全技术实体鉴别》(GB/T 15843.3-2016)和《信息安全技术术语》(GB/T 25069-2010)等国家标准，证书认证方式采用双向认证机制，以此保证可靠性。

通信双方经过证书认证互相确认身份后。首先，系统利用SM2算法生成公私钥对，结合量子密钥和SM4算法对公钥进行加密，然后将其发送至感知层终端，终端使用对应的预存量子密钥(证书)解密，从而获得公钥；其次，量子密钥服务管理系统利用私钥对待发送的密钥文件进行加密，用上述方法进行二次加密后发送至终端。终端依次使用预存量子密钥、公钥解密，获得最终密钥文件，并将其进行存储。如果量子密钥文件的量不足，系统就会利用量子加密通信终端剩余的量子密钥重复上述过程获取新的量子密钥。也可以通过密钥扩展算法，扩大密钥容量，以满足终端的量子密钥需求。

4 总结

工业互联网是新一代信息通信技术与工业经济深度融合的产物。它以网络为基础、平台为中枢、数据为要素、安全为保障，是实现工业数字化、网络化、智能化转型的基础设施，也是制造强国和网络强国建设的重要支撑。但与此同时，工业互联网的发展使工业系统逐步从“封闭隔离式”演进为“开放交互式”，这引入了极大的信息安全隐患。

目前，国内工业制造体系仍停留在工业3.0自动化改造阶段，工业互联网的发展受阻，其原因之一便是在纵向数据安全方面，缺少相应的安全解决方案。工业互联网的核心思想是智造化，在网络侧实现公网“专用”，以实现低成本的任意场景的海量物联。本文提出的工业量子密钥服务管理系统以量子真随机密钥为核心，基于纵向的密钥流管理，该系统可实现无所不在的密钥和随时随地加密。同时，本系统方案可以在几乎不影响工业网络性能的前提下，实现IoT融合，保障海量接入终端数据的端到端高安全。该系统既契合工业互联网网络架构，又符合工业互联网的核心思想，可助力工业互联网的进一步发展。

参考文献：

[1] 余晓晖，刘默，蒋昕昊，等. 工业互联网体系架构2.0[J]. 计算机集成制造系统，2019，25(12)：2983-2996.
[2] 熊姝涵. 工业互联网标识解析的市场应用模式探索[J]. 通信与信息技术，2022(4)：85-87.
[3] 朱立锋. 关于工业互联网数据安全解决思路的探讨[J]. 电子技术应用，2022，48(2)：1-3.
[4] 李瑞，荣雅雯. 工业互联网数据安全的防控方法[J]. 数字技术与应用，2022，40(9)：225-227.
[5] 刘廉如，张尼，张忠平. 工业互联网安全框架研究[J]. 邮电设计技术，2019(4)：53-57.
[6] 杨超，郭刚，叶林佶，等. 工业互联网数据安全治理实践[J]. 信息安全与通信保密，2022(9)：18-27.
[7] 王晨宇，鹿瑞超，陶小峰. 工业互联网数据安全流通关键技术[J]. 信息通信技术，2022，16(6)：15-19，26.
[8] 黄晏瑜，胡瑞敏，孙建国. 工业互联网数据安全隐私保护技术概述[J]. 工业信息安全，2022(10)：29-38.
[9] C.E. Shannon. Communication Theory of Secrecy Systems[J]. Bell System Technical Journal，1949，28(4)：656-715.
[10] 冷超，杜忠岩，王题，等. 量子保密通信技术及其在智慧城市中的应用研究[J]. 邮电设计技术，2023(4)：33-37.
[11] 郭光灿. 量子信息技术研究现状及未来[J]. 中国科学(信息科学)，2020，50(9)：1395-1406.
[12] 杜忠岩，冷超，王题，等. 面向5G网络的量子加密在智慧城市中的应用[J]. 邮电设计技术，2022(5)：16-21.
[13] 谢小兵. 量子密码技术原理及应用前景初探[J]. 金融电子化，2021(7)：64-66.
[14] 李子臣. 商用密码算法原理与C语言实现[M]. 北京：电子工业出版社，2020：28-82.
[15] 胡倩倩，冯宝，李冬. 基于量子随机数发生器的量子密钥分发系统[J]. 计算机应用与软件，2023，40(4)：324-328.
[16] 陈杰. 应用量子加密，保障信息安全[J]. 信息化建设，2023(9)：63-64.

作者简介：
马长链，毕业于北京邮电大学，高级工程师，硕士，主要从事量子加密通信、北斗定位、工业互联网等技术研究工作；杜忠岩，毕业于华中科技大学，教授级高级工程师，硕士，主要从事移动通信、北斗定位、智慧城市等技术研究工作；曲嘉旭，毕业于美国俄亥俄州立大学，工程师，硕士，主要从事以“5G+北斗”为技术核心的通导遥一体化时空服务技术研究工作；黄晓宁，毕业于西南民族大学，主要从事量子加密通信、密码信息技术、工业互联网等技术研究工作。