面向工业互联网的密钥管理平台设计与实现

Design And Implementation of Key Management Platform for Industrial Internet

马长链[1]，杜忠岩[1]，韦 峥[2]，曲嘉旭[1]（1. 中国联通智能城市研究院，北京 100048；2. 苏州蓝鲸量子科技有限公司，江苏 苏州 215001）

Ma Changlian[1]，Du Zhongyan[1]，Wei Zheng[2]，Qu Jiaxu[1]（1. China Unicom Smart City Research Institute，Beijing 100048，China；2. Suzhou Blue Whale Quantum Technology Co.，Ltd.，Suzhou 215001，China）

摘 要：

为了提高工业互联网环境下密钥管理的安全性与效率，设计了一种基于多熵源协同的密钥管理平台。通过集成多种量子随机数发生器，增强了密钥池的多样性和随机性，从而提升整个系统的安全防护水平。采用动态调节机制，根据密钥池的存储量自动调整从各熵源读取密钥的速度。该平台通过有效管理密钥池，实现了密钥的高效存储与分发。

关键词：

量子随机数发生器；数据安全；工业互联网；密钥管理互操作协议

doi：10.12045/j.issn.1007-3043.2026.04.014

文章编号：1007-3043（2026）04-0082-05

中图分类号：TN918

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

In order to improve the security and efficiency of key management in the industrial Internet environment，it designs a key service management platform based on multi-entropy source collaboration. This platform integrates multiple quantum random number generators，enhancing the diversity and randomness of the key pool and thereby elevating the security protection level of the entire system. It employs a dynamic adjustment mechanism to automatically adjust the speed of reading keys from each entropy source in accordance with the storage volume of the key pool. Through effective management of the key pool，the platform achieves efficient storage and distribution of keys.

Keywords：

Quantum random number generator；Data security；Industrial Internet；Key management interoperability protocol

引用格式：马长链，杜忠岩，韦峥，等. 面向工业互联网的密钥管理平台设计与实现[J]. 邮电设计技术，2026（4）：82-86.

0 引言

随着第四次工业革命的到来，工业互联网作为新一代信息技术与制造业深度融合的产物，在全球范围内引发了一场深刻的产业变革。它不仅推动了制造业向数字化、网络化、智能化方向发展，还重构了工业生态体系，提升了产业链的整体效率。然而，随着工业互联网的广泛普及，其所面临的安全威胁也日益严峻。病毒、黑客攻击等网络安全问题不再局限于传统IT领域，而是迅速蔓延至工业控制系统中，严重威胁着工业生产的连续性和稳定性，甚至可能对国家安全和社会秩序造成冲击[1-3]。

密钥池是工业互联网密钥管理平台的核心组成部分之一，它存储了大量的加密密钥，用于保护数据的安全传输。在工业互联网环境中，密钥池需要快速响应大量的密钥请求，同时确保密钥的安全性和可靠性。随着工业互联网规模的不断扩大，密钥池的重要性日益凸显，只有确保密钥池的安全，才能保障整个工业互联网系统的安全。然而，目前大多数工业互联网密钥管理平台仍然依赖单一的量子随机数发生器（Quantum Random Number Generator，QRNG）作为熵源来生成密钥。这种单一熵源方案存在诸多不足：如果

收稿日期：2026-02-24

唯一的熵源发生故障或被攻击，整个系统的安全性将受到严重影响；在高负载情况下，单一熵源可能无法满足密钥池的需求，导致密钥生成速度下降，影响系统的响应时间和性能；在没有备用熵源的情况下，系统在面对突发故障时缺乏有效的应对措施，可能导致密钥池无法正常运作[4]。

为了解决上述问题，本文提出了一种基于多熵源协同工作的密钥池管理方案。该方案通过集成多个不同厂家的量子随机数发生器，显著提高了生成随机数的不可预测性和随机性，从而增强了系统的安全性。多熵源协同工作可以生成更多的随机数，确保密钥生成过程的连续性和可靠性；通过引入动态权重调整机制，平台可以根据实际情况优化各个熵源的贡献比例；统一的接口设计和协议适配层使系统可以轻松地接入新的熵源，无论是更换旧的设备还是引入新的技术，都能够快速适应[5-7]。

1 多熵源接入

本章主要介绍量子随机数发生器的概念和具体实现策略，包括标准化接口设计、协议适配层、动态权重调整、冗余与容错机制以及实时监控与自适应调整策略等。

1.1 量子随机数发生器

量子随机数发生器是一种利用量子力学的不可预测性来生成真随机数的装置，其主要作用在于为信息安全领域提供高质量的随机数源，尤其是在加密算法中，可用于生成密钥或其他需要高度随机性的数据[8]。在密码学中，密钥的质量直接影响到加密算法的安全，使用量子随机数生成的密钥具有极高的随机性，能够有效防止基于模式识别的攻击[9]。

1.2 多熵源接入策略

多熵源指的是同时接入多个量子随机数发生器。这些量子随机数发生器可能来自不同的制造商，但通过统一的接口和协议整合到系统中。多熵源接入平台旨在通过集成多种类型的熵源，提高密钥生成的随机性和可靠性。在本系统中，将来自不同厂家的量子随机数发生器有效地接入到同一平台中是研究的重点，其中关键的接入策略如下。

1.2.1 标准化接口设计

平台对接量子熵源的接口做了标准化设计。平台可通过标准化的接口 RESTful API、SDK 获取随机数，无论 QRNG 的内部如何实现，只要能够按照这个标准接口提供随机数，就能够被系统识别和使用，确保不同厂家的 QRNG 能够通过统一的接口与密钥管理平台进行交互。

1.2.2 协议适配层

各个厂家的量子熵源在接入路由器之前的原始协议可能不同，协议适配层可处理不同熵源设备的专有协议，将专有协议转换为标准化的 TCP/IP 协议，将设备输出的数据格式转换为统一的格式。

1.2.3 动态权重调整

通过实时监控主密钥池的状态，自动调整从熵源读取密钥的速度，以确保系统在不同负载情况下的稳定性和性能。本文采用基于反馈控制的比例-积分-微分（PID）控制算法来实现这一目标，使用内置的监测模块收集数据，并通过接口传递给控制算法。此外，系统可调整数据采集频率，以平衡实时性和系统负载。

1.2.4 冗余与容错机制

为每个熵源配备至少一个冗余备份，当主熵源出现问题时，系统能够自动切换到备用熵源，增强系统的鲁棒性，减少单点故障的风险。

1.2.5 实时监控与自适应调整

通过部署一套监控系统，持续监测熵源的健康状况和性能指标，并根据这些数据动态调整接入策略，及时发现并应对熵源的变化或异常情况，确保系统始终处于最佳工作状态。

2 密钥管理平台系统设计

本章将详细介绍系统的整体架构以及各个关键组件的设计思路，包括熵源控制中心、主控单元、主密钥池和用户密钥池，以展示如何通过多层次的安全措施来增强系统的可靠性和安全性。

2.1 系统架构

密钥管理平台系统架构如图 1 所示。

2.2 组件设计

2.2.1 熵源控制中心

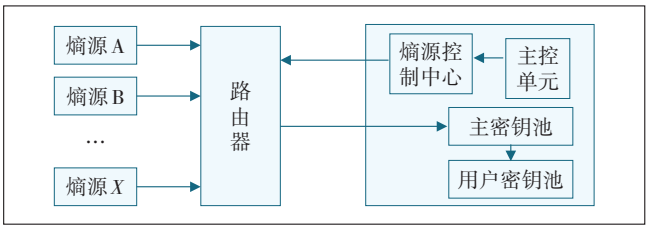

图 1　工业互联网防护平台系统架构

熵源控制中心是平台的核心部分，负责管理不同厂商提供的熵源设备。这些熵源设备的实现方式和输出端口型号可能有所不同，但它们最终通过统一的网口接口接入到路由器中。熵源控制中心统一协调从熵源读取随机数的过程，并将生成的密钥放入主密钥池中。

2.2.2 主控单元

主控单元负责监测主密钥池的容量，并根据预设的策略调整从熵源读密钥的速度。当主密钥池的容量低于80%时，主控单元会指示熵源控制中心加快从熵读取密钥的速度；当主密钥池的容量接近上限时，主控单元会减慢读取速度，并舍弃最早存入主密钥池的密钥，以保持池中密钥更新和管理的合理性。

2.2.3 主密钥池

主密钥池用于存储由熵源生成的密钥，是平台分发密钥的主要来源。主密钥池的容量是动态管理的，当密钥池容量低于设定阈值时，系统会自动加快密钥的生成速度；当容量接近上限时，则减慢生成速度并清理老旧密钥，以保证密钥池内的密钥始终处于最佳状态。

2.2.4 用户密钥池

用户密钥池用于备份分发出去的密钥，确保在用户再次申请使用同一密钥时能够快速响应。用户密钥池中的密钥会被持续维护，直到用户申请销毁这些密钥为止。用户密钥池可以提高密钥的重用效率，并且在密钥需要销毁时确保其被彻底清除。例如，即时会话密钥可以使用一次性密钥或短期有效的密钥，保证其生命周期极短，即使泄露也不会带来长期影响。

3 多熵源密钥池动态管理方法

为了确保密钥管理平台在不同负载情况下的性能，本章将详细介绍多熵源密钥池动态管理方法、密钥管理互操作协议（Key Management Interoperability Protocol，KMIP）的实现以及密钥池的设计与管理策略。

3.1 密钥生成速度动态调整

为了优化密钥生成和管理，系统通过实时监测主密钥池的容量，自动调整从熵源读取密钥的速度，以确保系统在不同负载情况下的性能。本文采用了基于反馈控制的PID控制算法，这种动态调整机制可以有效平衡密钥生成速度与密钥池容量，避免密钥池的过度膨胀或不足[10]，具体实现步骤如下。

3.1.1 状态监测

a）数据采集。定期采集密钥池的状态，包括当前密钥数量、密钥请求量、密钥池剩余容量等。

b）监测工具。系统使用内置的监测模块收集数据，并通过接口传递给控制算法。同时，系统可调整数据采集频率，以平衡实时性和系统负载。

3.1.2 PID调节机制

首先，设定目标密钥池的容量范围（例如密钥占密钥池的80%~90%）。如果密钥池容量低于80%，则需要增加密钥读取速率；如果超过90%，则需要减少读取速率。

然后，计算误差。系统根据误差调整密钥读取速率。定义误差$e(t)$为当前密钥池中的剩余密钥数量X与目标剩余密钥数量X_{target}之间的差值，即：

$$e(t) = X_{\text{target}} - X \tag{1}$$

PID控制器的输出$u(t)$可以表示为：

$$u(t) = K_p e(t) + K_i \int_0^t e(\tau)\mathrm{d}\tau + K_d \frac{\mathrm{d}e(t)}{\mathrm{d}t} \tag{2}$$

其中，K_p是比例系数，K_i是积分时间常数，K_d是微分时间常数。

3.1.3 权重计算

根据PID控制器的输出$u(t)$，调整各熵源的权重，确保密钥池中剩余密钥数量接近目标值。假设设置了n个熵源设备，每个设备的权重$W(s)$可以表示为：

$$W(s) = \frac{u(t)}{\sum_{1}^{n} u(t)} \tag{3}$$

3.1.4 动态调整

在分发速率方面，系统根据计算出的权重动态调整各熵源的随机数分发速率，确保高需求时增加随机数生成速率。在工作数量方面，系统根据计算出的权重调整各熵源的工作数量，即激活更多熵源来满足高需求。

3.1.5 反馈和修正

系统实时监控调整效果，通过实际密钥池状态数据验证调整的有效性。同时，系统可根据反馈结果调整PID参数（K_p、K_i、K_d），优化系统性能。动态调整算法流程如图2所示。

3.2 密钥管理互操作协议（KMIP）

3.2.1 密钥存储与管理

KMIP用于存储从不同熵源设备获取的随机数生成的密钥，同时，KMIP支持密钥的生命周期管理。

3.2.2 密钥分发

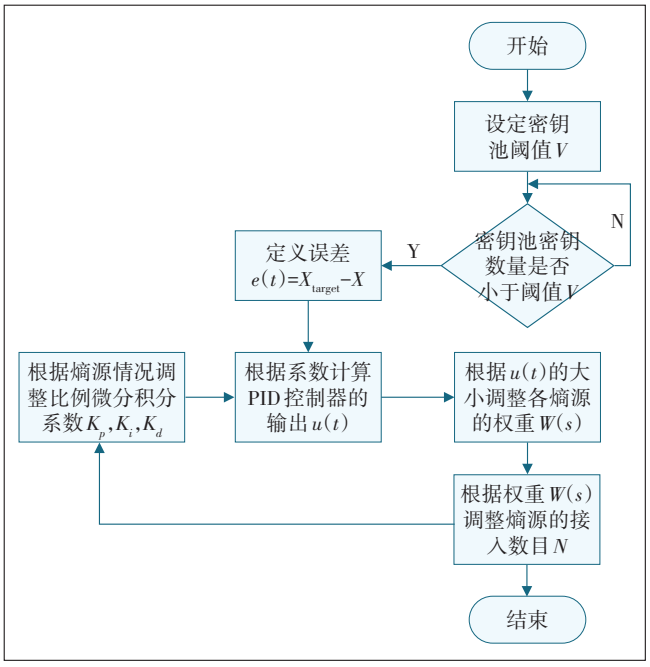

图2　动态调整算法流程

当用户或系统需要密钥时，KMIP可以确保密钥的安全分发：KMIP客户端向KMIP服务器请求密钥，KMIP服务器通过加密通道将密钥发送给客户端。

3.2.3　安全传输

KMIP支持加密的通信，以确保密钥在传输过程中的安全。KMIP使用加密协议来保护密钥数据的传输，防止在传输过程中被截获或篡改。

3.2.4　密钥生命周期管理

KMIP支持密钥的整个生命周期管理，包括密钥的生成、存储、使用、更新、撤销和销毁等操作，有助于确保密钥的安全性和有效性[11]。

3.3　密钥池管理

3.3.1　密钥池设计

密钥池使用链表来存储密钥，每个密钥项包含密钥本身、生成时间戳及其状态。密钥池可设置最大容量密钥数，当达到容量限制时，系统将使用先进先出（FIFO）策略删除最早存入的密钥。

3.3.2　密钥的生成与存储

系统从量子随机数[12]发生器获取原始随机数，经处理后生成密钥，密钥长度为256位。密钥使用高级加密标准（AES）算法，并通过加密链表对密钥数据进行存储，确保其在密钥池中的安全。

3.3.3　密钥池管理策略

a）密钥的添加与删除。在从熵源获取新密钥后，首先验证密钥的唯一性和有效性。通过加密存储后，将密钥插入到链表尾部。一旦密钥池达到最大容量，系统会自动删除链表头部的最旧密钥，以释放空间。删除操作包括从链表中移除密钥并更新池的状态。

b）密钥池的动态调整。实时监控密钥池中的密钥数量，若池中密钥接近容量上限，则降低从熵源读取新密钥的速率；若池中密钥量低且请求量大，则增加读取速率，可从多个熵源并行获取密钥。系统使用PID控制算法动态调整密钥的生成速率，确保在不同负载下密钥池的稳定性和响应时间。

3.3.4　密钥池安全性

a）密钥的保护。密钥池仅允许经过认证的系统组件访问密钥数据，并采用基于角色的访问控制来限制访问权限。此外，密钥池采用了加密保护，密钥池内所有的密钥在存储和传输过程中都使用AES-256加密，防止数据泄露。

b）审计与日志。系统记录每次密钥的生成、使用、更新及删除事件，日志包括时间戳、操作类型、操作结果等信息。系统具备审计功能，可定期审计日志，检查是否存在异常操作。此外，还可利用日志进行系统监控，发现潜在的安全问题并采取相应措施。

4　实验与分析

4.1　测试目的

验证设计的密钥管理平台管理与控制2个异厂家量子熵源的能力，确保密钥管理平台能有效地管理多个异厂家量子熵源设备。

4.2　测试环境

测试环境搭建示意如图3所示，具体配置如下。

a）量子熵源设备。熵源设备A最大输出速率为100 Mbit/s，熵源设备B最大输出速率为100 Mbit/s。

b）服务器配置。本测试的操作系统为Ubuntu 22.04 LTS，网络接口为千兆网卡（1 Gbit/s），处理器为Intel Xeon E5-2670，内存为32 GB RAM，硬盘为1 TB

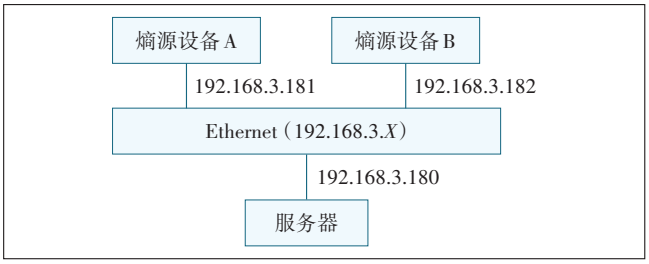

图3　测试环境搭建示意

SSD。

c）网络配置。熵源设备通过交换机连接至服务器，并通过iperf3、syslog、netstat、ping等方式进行测试。

4.3 测试方法

4.3.1 带宽测试

使用iperf3测试工具同时测试2个熵源设备的网络带宽。每个设备的输出速率为100 Mbit/s，测试期间通过网络监控确保数据流量不超过服务器网络接口的最大带宽（1 Gbit/s）。

4.3.2 稳定性测试

熵源设备A与熵源设备B在服务器端稳定运行24 h，并监控其连接状态、数据包丢失、延迟等指标。

4.3.3 多设备管理控制测试

在服务器上运行设备管理工具，通过该工具同时管理2个熵源设备的连接状态。测试操作包括同时启动、暂停、重启、调整设备参数等，以测试平台是否能正常管理多个设备。

4.4 测试结果

4.4.1 带宽利用

熵源设备A最大速率为98.5 Mbit/s，熵源设备B最大速率为97.8 Mbit/s，当2个设备同时工作时，2个设备的总数据吞吐为196.3 Mbit/s。在千兆网卡环境下，带宽利用率为19.6%，网络接口未达到饱和状态，可提供足够的带宽来支持更多设备的接入。

4.4.2 稳定性

在24 h测试过程中，熵源设备A与熵源设备B未出现任何掉线或重启情况。数据包丢失率平均为0.02%，其中，熵源设备A为0.03%，熵源设备B为0.01%。丢包发生在高峰时段，未对整体性能造成明显影响。平均延迟波动为1.2 ms，最大延迟波动为2.3 ms，在容忍范围内。

4.4.3 设备管理

在同时管理2个熵源设备时，管理工具响应时间为2 s，操作界面无明显延迟或卡顿。在执行设备重启操作时，2个熵源设备均能够成功重启，无交互冲突或错误。

4.5 结论

本次测试表明，2个量子熵源设备在千兆网卡环境下能够稳定工作，带宽利用率较低，未出现明显的性能瓶颈。本文设计的密钥管理平台对多量子熵源设备管理功能运行稳定，管理界面响应迅速，整体系统表现良好，适合在生产环境中部署和使用。

5 结束语

基于多熵源协同的工业互联网密钥管理平台通过集成多种量子随机数发生器，显著提升了密钥池的多样性和随机性，增强了系统的安全性。其采用的动态调节机制能够根据密钥池的存储量自动调整从各熵源读取密钥的速度，从而实现了密钥的高效存储与分发。实验结果表明，该平台不仅能够有效地平衡密钥池的存储容量与密钥生成速度，确保在高负载情况下快速响应用户的密钥请求，而且还提高了密钥管理的安全性，增强了系统的灵活性和可扩展性。

参考文献：

[1] 蔡岳平，李栋，许驰，等. 面向工业互联网的5G-U与时间敏感网络融合架构与技术[J]. 通信学报，2021，42(10)：43-54.
[2] 黄韬，汪硕，黄玉栋，等. 确定性网络研究综述[J]. 通信学报，2019，40(6)：160-176.
[3] 赖英旭，刘增辉，蔡晓田，等. 工业控制系统入侵检测研究综述[J]. 通信学报，2017，38(2)：143-156.
[4] 周泓伊，曾培. 量子随机数发生器[J]. 信息安全研究，2017，3(1)：23-35.
[5] 罗文俊，闻胜莲，程雨. 基于区块链的电子医疗病历共享方案[J]. 计算机应用，2020，40(1)：157-161.
[6] 高建，陈文彬，庞建民，等. 基于组合密钥的智能电网多源数据安全保护[J]. 电信科学，2020，36(1)：134-138.
[7] 王彤，朱敏玲. 序列检测和近似熵检测的快速实现研究[J]. 计算机工程与应用，2020，56(15)：113-117.
[8] 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.
[9] 陈婉婉，李荭. 最快实时量子随机数发生器问世[J]. 科教文汇，2021(20)：1.
[10] 陈发堂，郑金贵，陈峰，等. 基于PID控制的自适应密钥生成[J]. 南京邮电大学学报(自然科学版)，2023，43(3)：11-18.
[11] MSAHLI M，SERHROUCHNI A，BADRA M. Extending TLS with KMIP protocol for cloud computing[C]//2016 8th IFIP International Conference on New Technologies，Mobility and Security (NTMS). Larnaca：IEEE，2016：1-6.
[12] 聂友奇，张军. 实用化量子随机数发生器研究进展[J]. 信息安全研究，2017，3(1)：86-90.

作者简介：
马长链，毕业于北京邮电大学，高级工程师，硕士，主要从事量子信息安全、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；韦峥，毕业于北京邮电大学，高级工程师，硕士，主要从事无线通信、水下无线光通信、量子信息安全、工业互联网等技术研究工作；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。