

# 量子密钥分发和后量子密码融合研究

罗俊
（中电信量子信息科技集团有限公司，安徽 合肥 230088）

**摘　要：**针对量子计算对传统公钥基础设施的潜在威胁，通过分析量子密钥分发（quantum key distribution，QKD）与后量子密码（post-quantum cryptography，PQC）技术的互补性及两种技术融合的必要性，提出了一种融合QKD与PQC的密码基础设施功能模型，并具体描述了模型的基本组成网元及其功能模块，定义了各网元与模块间的接口参考点。通过QKD和PQC融合的混合密码系统，实现了属于不同密钥管理系统的语音终端之间的跨域加密通话场景。该模型的提出为电信运营商提升其基础网络与电信业务抗量子攻击能力提供了有力支撑。

**关键词：**密码基础设施；量子密钥分发；后量子密码
**中图分类号：**TN918
**文献标志码：**A
**doi:** 10.11959/j.issn.1000−0801.2025245

# Research on quantum key distribution and post-quantum cryptography fusion

LUO Jun
China Telecom Quantum Technology Co., Ltd., Hefei 230088, China

**Abstract:** In view of the threat of quantum computing to traditional public key infrastructure, by analyzing the technical complementarity of quantum key distribution (QKD) and post-quantum cryptography (PQC), as well as the necessity for integrating these two technologies, A functional model for cryptographic infrastructure that integrates QKD and PQC was proposed, basic network elements and functional modules of the model was described and interface reference points were defined, and an application scenario for cross-domain encrypted calls between voice terminals belonging to different key management systems through a hybrid cryptographic system that integrates QKD and PQC was realized, which provides a strong support for telecom operators to improve the anti-quantum attack capabilities of their basic networks and telecom services.

**Key words:** cryptographic infrastructure, quantum key distribution, post-quantum cryptography

## 0　引言

随着IP化的4G、5G网络等移动通信技术的快速发展，现代电信运营商面临着前所未有的信息安全挑战。传统的密码学方法，如基于公钥基础设施（public key infrastructure，PKI）的加密

收稿日期：2025−07−11；修回日期：2025−10−22

体系，虽然在过去的几十年间为数据传输提供了可靠的安全保障，但其安全性正受到量子计算技术快速进步的威胁。量子计算机的强大计算能力可能在未来破解现有的非对称加密算法，如RSA和ECC，这使得依赖这些算法的传统PKI体系面临失效的风险。因此，探索一种能够抵御量子攻击的新一代密码基础设施成为当务之急。

量子密钥分发（quantum key distribution，QKD）作为一种基于量子力学原理的新型密钥交换技术，以其“无条件安全性”[1]为核心优势，为解决上述问题提供了重要思路。QKD利用量子态的不可克隆性和测量扰动特性，确保了密钥分发过程的安全性，即使面对量子计算机的攻击也难以被破解[2]。这种技术不仅能够在理论上提供长期安全保证，还为构建下一代密码基础设施奠定了坚实基础。然而，单独依靠QKD并不能完全满足复杂网络环境下的多样化需求。因此，将QKD与后量子密码学（post-quantum cryptography，PQC）相结合，并与电信运营商网络深度融合，形成一套全新的运营商密码基础设施，成为当前研究的重要方向。

本文在分析QKD和PQC的技术特点及其互补性的基础上，提出了一种融合QKD与PQC的电信运营商密码基础设施功能模型。本文详细描述了组成该模型的基本网元和各网元内部的功能模块，定义了各网元和功能模块之间的接口参考点。基于QKD和PQC融合的混合密码系统，本文实现了属于不同密钥管理系统（key management service，KMS）的语音终端之间的跨域加密通话场景。和传统PKI体系相比，融合QKD与PQC的密码基础设施功能模型在安全性、灵活性和可扩展性方面都展现出显著的优势，能够为电信运营商提升其基础网络与电信业务抗量子攻击能力提供有力支撑。

## 1 方案研究

QKD和PQC作为两种面向量子计算时代的密码技术，各自具备独特的安全特性和应用场景。然而，单一使用QKD或PQC均无法全面满足电信运营商在复杂网络环境中的多样化需求。为此，将QKD与PQC进行深度融合，构建一套综合性密码基础设施，不仅能够充分发挥两者的优势，还能有效弥补各自的局限性，为电信运营商的基础网络和业务应用提供全方位的安全保障。

### 1.1 QKD与PQC技术的互补性

QKD的核心优势在于其“无条件安全性”，即基于量子力学原理的密钥分发过程不受计算能力的影响，即使面对量子计算机也无法被破解。然而，QKD的实际应用受限于量子信道的物理依赖性，其适用范围主要集中在特定场景下的密钥分发。相比之下，PQC通过设计抗量子攻击的数学算法，能够在传统网络架构中广泛部署，适用于各种通信需求。PQC的安全性依赖于数学难题的复杂性，尽管其设计目标是抵御量子计算攻击，但理论上仍可能存在未知漏洞。因此，QKD和PQC的结合能够形成一种多层次的安全保障机制：QKD负责提供底层密钥分发的绝对安全性，而PQC则在更高层次上为加密和认证提供抗量子攻击的能力。

### 1.2 QKD与PQC融合的必要性

#### 1.2.1 覆盖不同安全需求

QKD的优势在于基于量子力学原理，提供理论上无条件安全的密钥分发，适用于高安全性需求的点对点通信场景，如金融、国防、政务等。PQC的优势在于基于抗量子攻击的数学难题，兼容现有网络基础设施，适用于大规模复杂网络环境，如互联网、物联网等。

QKD难以直接应用于复杂的多节点网络，而PQC无法提供QKD级别的物理层安全保障。融合QKD和PQC可以实现从物理层到应用层的全方位保护，满足不同场景下的安全需求。

#### 1.2.2　技术过渡期的需求

当前正处于从传统密码学到量子安全技术的过渡阶段，QKD 尚未普及，而 PQC 算法的长期安全性仍需验证，单一技术可能无法完全应对所有威胁。

在过渡期内，融合 QKD 和 PQC 可以形成多层次防护体系，降低迁移风险。使用 QKD 生成密钥，结合 PQC 算法加密数据，确保即使某一层被攻破，整体系统仍然安全。

#### 1.2.3　应对量子计算的不确定性

量子计算的实际发展速度尚不明确，未来可能出现突破性进展，导致现有技术失效。QKD 和 PQC 分别基于不同的安全假设（量子力学 vs 数学难题），融合使用可以分散风险。即使量子计算技术取得突破，融合方案仍能提供一定程度的安全保障。

#### 1.2.4　提升抗量子方案的性价比

QKD 的成本主要来自高昂的硬件成本（如单光子探测器、量子中继器）[3-4]及专用光纤或卫星通信链路[5]的建设费用，主要适用于高价值、高安全性需求的场景。PQC 的实施成本较低，主要涉及软件升级和算法优化，可基于现有网络基础设施，实现大规模部署和普及。

QKD 和 PQC 的融合能够充分发挥两者的互补优势，覆盖从物理层到应用层的安全需求。在技术过渡期和量子计算不确定性背景下，融合方案可以提供更全面的保护。在高价值场景中优先部署 QKD，在大规模场景中推广 PQC，实现成本与效益的最佳平衡。

### 1.3　QKD 与 PQC 融合方案的设计要点

QKD 和 PQC 在原理、应用场景和技术特点上存在显著差异，但它们并非相互排斥，而是可以互补的技术。为实现 QKD 与 PQC 的深度融合，充分发挥各自的技术优势，提出以下融合方案设计要点。

#### 1.3.1　分段部署

在关键链路中部署 QKD，用于高安全性需求的密钥分发；在其他链路中使用 PQC，降低整体成本。例如，在骨干网中使用 QKD，在终端设备之间使用 PQC。在过渡阶段，优先在高价值场景中部署 QKD，同时逐步推广 PQC，这种分段渐进式部署可以平衡短期投入与长期收益，最大化资源利用率。

#### 1.3.2　分层防护

在网络架构中，将 QKD 和 PQC 分配到不同的安全层次。QKD 提供物理层安全保障，使用 QKD 生成共享密钥，确保密钥分发的无条件安全性；PQC 提供应用层加密保护，使用 PQC 算法加密数据和签名，保护传输内容的安全性。

在骨干网中部署 QKD 设备，利用 QKD 保障核心节点之间的密钥分发。QKD 生成对称密钥，将这些密钥用于 PQC 算法的初始化或会话密钥交换。接入网使用 PQC 算法保护与终端设备之间的通信。

分层防护可以提供从物理层到应用层的全面保护，减少对单一技术的依赖，提高系统整体的鲁棒性，实现从点对点通信到复杂网络的无缝扩展，推动量子通信技术与经典网络的深度融合。

#### 1.3.3　混合密码系统

在实际部署中，同时使用传统密码算法、QKD 和 PQC，形成混合密码系统。引入 PQC 算法与传统算法混合使用，如 PQC+传统算法双重签名验签、PQC+传统算法双重密钥封装或并行封装，并在关键链路中部署 QKD，进一步提升安全性。可使用 QKD 生成主密钥，PQC 算法进行密钥派生和扩展，并在终端设备中嵌入轻量级 PQC 算法，确保兼容性和效率。

混合密码系统可实现平滑过渡，降低迁移风险，同时提供多层次的安全保障，适应不同场景需求。

1.3.4 动态切换机制

根据实时安全需求和网络环境，动态选择QKD或PQC，在高安全性需求场景中优先使用QKD，在资源受限或低安全性需求场景中使用PQC。通过开发智能调度系统，可根据流量类型、设备能力和安全等级实现技术间的动态切换。

动态切换机制可灵活适配不同场景，提高资源利用率，实现动态可调的安全保障，从而增强系统的整体适应能力。

1.3.5 互操作性

通过标准化接口实现密钥的共享和转换，确保QKD和PQC之间的无缝协作，避免技术差异导致的兼容性问题。

1.3.6 冗余设计

在关键节点和链路中同时部署QKD和PQC，形成双重保护机制，以应对单一技术失效的风险。

## 2 功能模型

基于QKD和PQC的电信运营商密码基础设施功能模型如图1所示。该模型采用分层架构，包括提供量子密钥分发的量子通信层、提供密码基础服务和密钥管理的密码服务层，以及使用密码服务的用户业务应用层3个层次。各层内部包含多个基本网元及其子功能模块，层间、网元间及子功能模块间通过定义的接口参考点实现命令和数据的交互。该模型实现了QKD和PQC的深度融合，基于PQC算法并结合经典商用密码和公钥基础设施，对整个基础设施实施了全面身份化的安全策略。用户与基础设施各网元之间，以及基础设施内部各层、各网元之间均基于后量子数字证书和后量子签名算法进行双向身份鉴别[6]，并在两两之间建立基于双向身份鉴别的双向传输层安全通道[7-8]。

### 2.1 基本网元及功能模块

2.1.1 量子通信层网元及其功能模块

量子通信层主要由量子密钥分发器网络（QKDN）构成。QKDN中与密码系统相关的模块包括量子密钥管理器（quantum key manager，QKM）、量子密钥分发器（quantum key distributor，QKD）和量子网络控制器（quantum key distribution network controller，QKDNC）。量子通信层中，通常由一对通过QKD链路连接的量子密钥分发器执行QKD协议来生成QKD密钥（QKD-key）。QKM负责接收和管理由QKD模块生成的密钥，对密钥进行中继并将密钥提供给应用或用户的密钥管理系统。QKDNC负责密钥路由，在集中式密钥中继模式下作为中心平台计算中继密钥。

2.1.2 密码服务层网元及其功能模块

密码服务层从量子通信层获取密钥，并面向业务应用层提供密钥管理和密码运算等密码服务，其基本网元包括KMS、密码管理服务平台（cryptgraphy management service platform，CMSP）、证书认证系统（certificate authority system，CAS）、身份与访问管理（identity and access management，IAM）、协同密码运算系统（co-crypto system，CCS）。

KMS网元由密码服务代理（cryptography service agent，CSA）、密钥管理代理（key management agent，KMA）、密钥充注管理器（key injection management，KIM）、QKD密钥池和PQC公钥池（key pool，KP）组成。CSA提供数据加解密、实体鉴别、完整性校验等密码运算功能的服务代理；KMA提供密钥全生命周期和密钥权限等与密钥相关的管理和配置功能；KIM提供主密钥的充注功能；KP进行密钥缓存和三库（在用库、备用库、历史库）管理，QKD密钥池存储QKD分发的量子密钥，PQC公钥池存储从KMS获取量子密钥的用户的PQC公钥。

CMSP网元由密码服务管理（cryptgraphy service management，CSM）、密码应用管理（cryptgraphy application management，CAM）、密码服务编排（cryptgraphy service orchestration，CSO）、

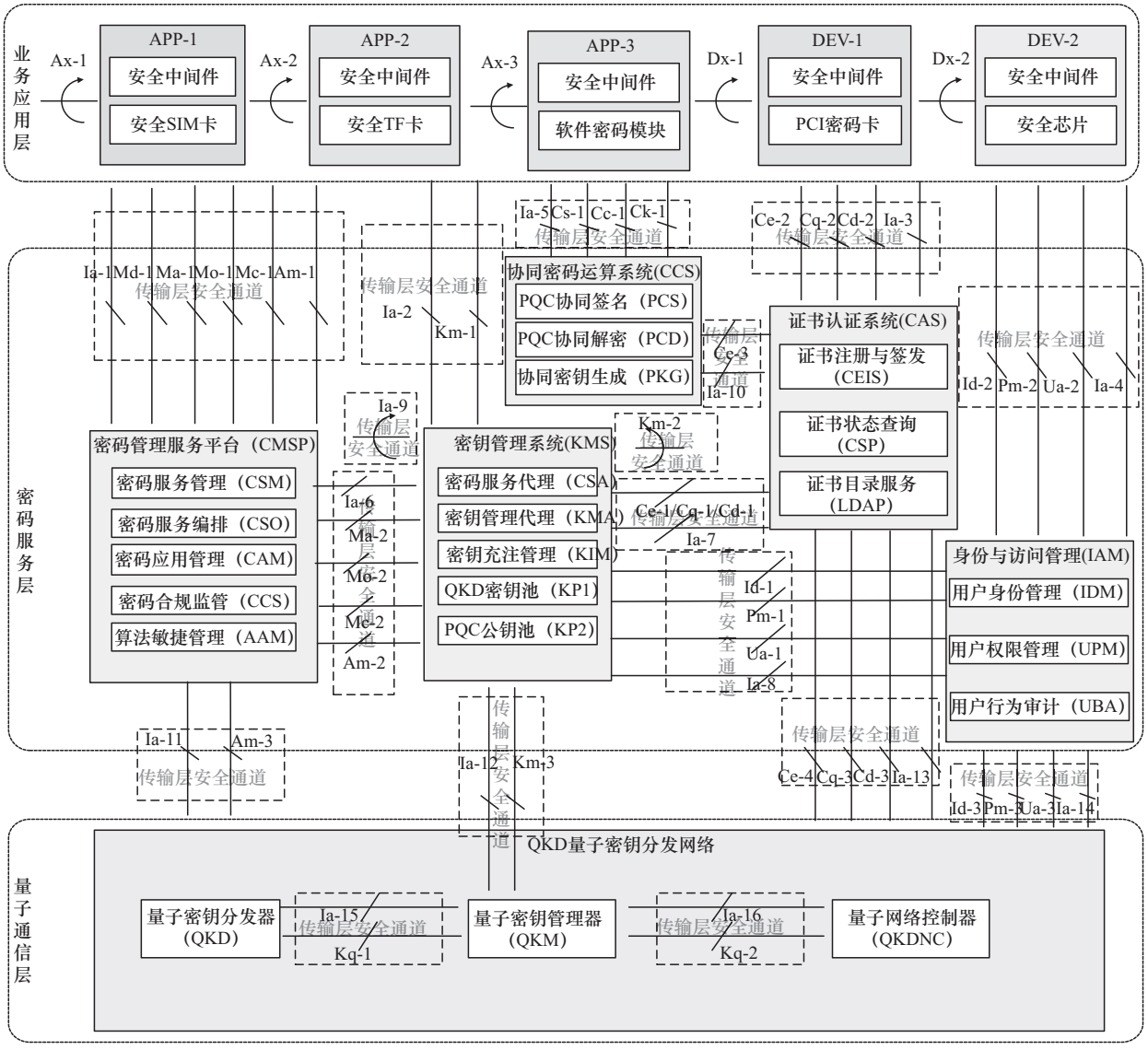


图 1　基于 QKD 和 PQC 的电信运营商密码基础设施功能模型

密码合规监管（cryptgraphy compliance supervision，CCS）和算法敏捷管理（algorithm agility management，AAM）模块组成。CSM 模块负责密钥分发链路监测、密码服务状态监控、身份认证和授权、密码设备管理以及服务日志审计；CAM 模块负责用户账号管理、业务账号管理、安全介质管理、应用权限管理和身份管理；CSO 模块负责安全策略和密码属性管理、密码资源调度等服务编排功能；CCS 模块负责算法正确性、密钥安全性、密码服务有效性、随机数质量等合规管理和密码操作审计；AAM 模块负责对基础设施各网元和用户终端使用的 PQC 算法配置和算法库根据 PQC 算法的演进情况进行在线更新，包括算法的替换、安全补丁、算法策略配置等，以实现应用 PQC 算法的密码敏捷性。

CAS 网元提供 PQC 和商用密码算法的混合证书服务，包括用户数字证书注册与签发（certificate enrollment and issuance，CEIS）、证书状态查询（certificate status protocol，CSP）、证书目录服务（lightweight directory access protocol，LDAP，提

供证书撤销列表和证书文件的下载）。

IAM网元提供用户身份管理（identity management，IDM）、用户权限管理（user privilege management，UPM）和用户行为审计（user behavior audition，UBA）功能。

CCS网元提供PQC协同签名（PQC co-signature，PCS）、PQC协同解密（PQC co-crypt，PCC）和PQC公共密钥生成（PQC key generation，PKG）的服务端运算。由于PQC算法处于一个长期演进的过程，因此采用软件可以保障算法的敏捷性，但软件实现密码运算的安全性，特别是数字签名和密钥的解封装需要采用协同密码运算的手段，并结合服务端的硬件密码设备来实现。

2.1.3　业务应用层网元及其功能模块

业务应用层的网元根据所配备密码部件的形态分为5大类：配备安全SIM卡的智能手机类应用（APP-1）、配备安全TF卡的专用终端类应用（APP-2）、配备软件密码模块的SaaS类上云应用（APP-3）、配备PCI密码卡的网关类设备（DEV-1）、配备密码安全芯片的终端类设备（DEV-2）。这些不同的网元通过安全中间件和其他网元交互。

## 2.2　接口参考点

2.2.1　管理类接口参考点

管理类接口参考点，包括以下4类。

（1）管理编排接口参考点Mo，是连接CSO和各类业务应用（Mo-1）、KMA（Mo-2）的参考点，负责传输服务编排信息和数据；

（2）设备管理接口参考点Md，是连接CSM和各类业务应用相关密码设备（Md-1）的参考点，负责传输密码设备管控信息和数据；

（3）应用管理接口参考点Ma，是连接CAM和各类业务应用（Ma-1）、KMS（Ma-2）的参考点，负责传输密码应用管控信息和数据；

（4）密码合规性检查接口参考点Mc，是连接CCS和各类业务应用（Mc-1）、KMS（Mc-2）的参考点，负责传输合规管控信息和数据。

2.2.2　服务类接口参考点

服务类接口参考点，包括以下4类。

（1）密钥管理接口参考点Km，是连接KMA和各类业务应用（Km-1）、KMS之间互联（Km-2），以及KMA和QKM（Km-3）的参考点，负责传输与密钥管理相关的信息和数据。

（2）量子密钥分发接口参考点Kq，是连接QKM和QKD（Kq-1）、QKM和QKDNC（Kq-2）的参考点，负责传输与量子密钥分发相关的信息和数据。

（3）协同密码运算调用接口参考点，是连接CCS的协同密码运算各模块和各类业务应用的参考点，包括PCS（Cs-1）、PCC（Cc-1）和PKG（Ck-1），负责传输相应协同密码算法调用和与密钥管理相关的命令和数据。

（4）证书服务接口参考点，是连接CAS各类服务模块与各网元及用户终端的参考点，包括连接KMS与CEIS（Ce-1）、用户终端与CEIS（Ce-2）、CCS与CEIS（Ce-3）以及连接量子密钥分发网络各网元（QKD、QKDM、QKDNC）与CEIS（Ce-4）的参考点；连接KMS与CSP（Cq-1）、用户终端与CSP（Cq-2）以及连接量子密钥分发网络各网元与CSP（Cq-3）的参考点；连接KMS与LDAP（Cd-1）、用户终端与LDAP（Cd-2）以及连接量子密钥分发网络各网元与LDAP（Cd-3）的参考点，负责传输相关证书服务的命令和数据。

2.2.3　身份类接口参考点

身份类接口参考点，包括以下4类。

（1）身份鉴别接口参考点Ia。本模型采用全面身份管理的安全策略，用户与基础设施各网元之间、基础设施内部各网元之间的数据和命令交互均通过双向身份鉴别并建立双向传输层安全通道。Ia是连接CMSP与各类业务应用（Ia-1）、KMS与各类业务应用（Ia-2）、CAS与各类业务

应用（Ia-3）、IAM与各类业务应用（Ia-4）、CCS与各类业务应用（Ia-5）、CMSP与KMS（Ia-6）、KMS与CAS（Ia-7）、KMS与IAM（Ia-8）、KMS之间（Ia-9）、CCS与CAS（Ia-10）、CMSP与量子密钥分发网络各网元（Ia-11）、KMA与QKM（Ia-12）、CAS与量子密钥分发网络各网元（Ia-13）、IAM与量子密钥分发网络各网元（Ia-14）、QKD与QKM（Ia-15）、QKM与QKDNC（Ia-16）的参考点，负责传输身份鉴别信息和数据。

（2）身份管理接口参考点Id，是连接KMS和IDM（Id-1）、各类业务应用与IDM（Id-2）以及连接量子密钥分发网络各网元与IDM（Id-3）的参考点，负责传输用户身份标识和属性等相关信息及数据。

（3）权限管理接口参考点Pm，是连接KMS和UPM（Pm-1）、各类业务应用与UPM（Pm-2）以及连接量子密钥分发网络各网元与UPM（Pm-3）的参考点，负责传输用户访问权限相关信息及数据。

（4）行为审计接口参考点，是连接KMS和UBA（Ua-1）、各类业务应用与UBA（Ua-2）以及连接量子密钥分发网络各网元与UBA（Ua-3）的参考点，负责传输用户行为审计相关信息及数据。

#### 2.2.4　通信类接口参考点

通信类接口参考点，包括以下两类。

（1）用户应用间的通信协议接口参考点Ax，是智能手机类（Ax-1）、专用终端类（Ax-2）以及SaaS上云类（Ax-3）密码应用之间进行同类应用互操作的参考点，负责基于特定的传输协议在同类密码应用间进行信息和数据交互。

（2）用户设备间的通信协议接口参考点Dx，是网关类（Dx-1）和终端类（Dx-2）密码设备之间进行同类设备互操作的参考点，负责基于特定的传输协议在同类密码设备间进行信息和数据交互。

## 3　应用场景

语音类应用是电信运营商最为核心的业务之一。当前主流的长期演进语音承载（voice over long-term evolution，VoLTE）和在VoLTE基础上发展而来的5G新空口承载语音（voice over new radio，VoNR）高清通话，基于IP多媒体子系统（IP multimedia subsystem，IMS）网络和会话初始化协议（session initiation protocol，SIP），其语音服务（控制和媒体层面）作为数据流在数据承载网络中传输。作为架构在4G和5G网络上全IP条件下的端到端语音方案，其安全性显得至关重要。目前，VoNR和VoLTE采用3GPP提出的认证密钥协商协议AKA（authenticated key agreement）完成用户和网络间的身份认证[9-10]。AKA协议基于一个长期共享密钥和一个序列号，通过保证长期共享密钥的机密性来实现用户的身份认证安全性。由于长期共享密钥的长期频繁使用，其安全性必然会下降。至于互联网上更为常见的VoIP类应用，在IP固有的安全性问题之外，还普遍存在标准化程度不高，对服务器的依赖度高，缺乏端到端的密码方案等问题。

在本基础设施中，通过QKD和PQC融合的混合密码系统实现了属于不同KMS（连接不同的QKD节点）的语音终端之间的跨域加密通话。QKD和PQC分段部署、分层防护：不同KMS之间的骨干关键链路部署QKD，即通信干线采用QKD提供的物理层安全保障进行干线会话密钥分发；KMS和终端用户之间的用户接入链路使用PQC提供的应用层加密保护，使用PQC加密和签名算法保护“最后一公里”的会话密钥分发。语音终端加密通话过程如图2所示。

语音终端加密通话过程的步骤如下。

**步骤1**　密钥充注和证书签发。

用户语音终端的安全SIM卡等安全介质和安全中间件启动初始化，进行签名证书和加密公钥

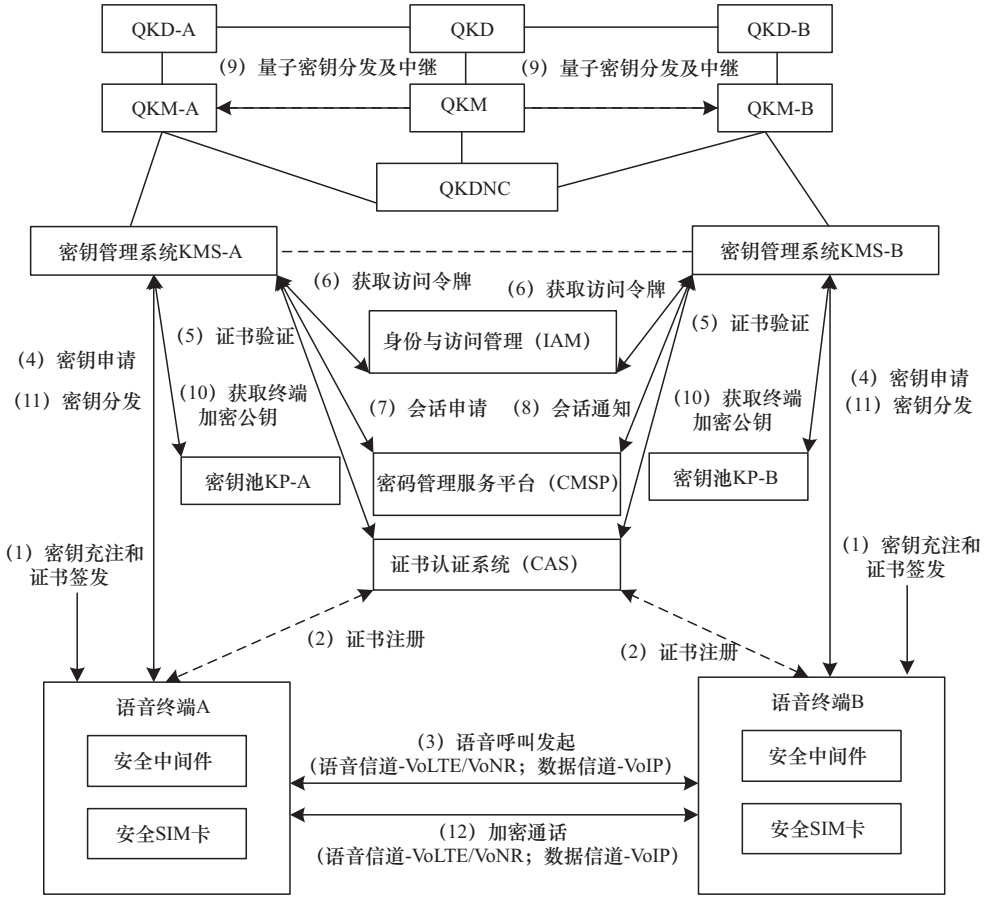


图 2　语音终端加密通话过程

的生成和充注。终端调用安全SIM卡等安全介质生成SM2和PQC签名密钥对，并导出签名公钥为PKSC#10等格式的证书签发请求（certificate signing request，CSR）文件，通过该终端所属的KMS作为代理向CAS进行在线证书注册并获得SM2和PQC签名证书。KMS同时为该用户终端生成SM2和PQC加密密钥对（PQC加密算法可采用FIPS203：*Module-Lattice-based Key-Encapsulation Mechanism Standard*生成密钥对并用于后续密钥封装[11]），并和签名证书一起注入安全SIM卡等安全介质，加密公钥存入KMS的公钥池。

**步骤2**　证书注册。

步骤1中KMS作为终端代理，使用终端生成的CSR并采用SCEP（simple certificate enrollment protocol）或ACME（automatic certificate management environment）和EST（enrollment over secure transport）等自动化证书管理协议向CAS进行在线证书注册，获得CAS作为根CA为终端签发的SM2和PQC签名证书。

**步骤3**　语音呼叫发起。

主叫方语音终端A发起呼叫，触发加密会话建立和密钥申请流程。

**步骤4**　密钥申请。

主被叫语音终端的安全中间件携带会话的相关信息向各自归属的KMS申请工作密钥，使用商密和PQC混合签名进行身份鉴别：

SM2_Sign(LABEL||SID_WK||SID_CALL||UID||NUMBER_CALL||NUMBER_CALLED, PRIV_SM2)||PQC_Sign(LABEL||SID_WK||SID_CALL||UID||NUMBER_CALL||NUMBER_CALLE

D, PRIV_PQC) || Cert_SM2 || Cert_PQC || Token

其中，SM2_Sign 表示采用国密算法 SM2 和用户 SM2 私钥 PRIV_SM2 对报文进行 SM2 数字签名，PQC_Sign 表示采用 PQC 算法和用户 PQC 私钥 PRIV_PQC 对报文进行 PQC 数字签名（PQC 签名算法可采用 FIPS204：*Module-Lattice-Based Digital Signature Standard*[12]），LABEL 以固定字符串表示密钥申请标签，SID_WK 表示本次申请密钥的会话标识，SID_CALL 表示本次所申请密钥用来保护的通信会话标识，UID 表示用户标识，NUMBER_CALL 和 NUMBER_CALLED 分别表示主叫和被叫号码。Cert_SM2 表示 SM2 签名证书，Cert_PQC 表示 PQC 签名证书。Token 表示授予语音终端的访问令牌，首次密钥申请时 Token 为空。

**步骤 5**　证书验证。

KMS 向 CAS 验证 Cert_SM2 和 Cert_PQC 的有效性，可通过 OCSP（online certificate status protocol）协议实时查询证书状态或 LDAP 协议查询证书信息，也可以下载 CRL 进行证书验证。

**步骤 6**　获取访问令牌。

KMS 验证终端用户身份后，通过 Token 确定用户的访问权限。如果 Token 为空或者 Token 过期，则向 IAM 获取用户的访问令牌。IAM 根据用户注册信息发放用户的访问令牌。

**步骤 7**　会话申请。

KMS 判断主叫或被叫用户是否属于自己的管理范围。当主被叫用户属于同一个 KMS 管理，KMS 直接调用密码机产生实时随机数作为工作密钥（WK）；当主被叫用户属于不同 KMS 管理，主叫方 KMS（图 2 中为 KMS-A）访问 CMSP 进行业务和身份查询，确认被叫方语音终端 B 所属 KMS（图 2 中为 KMS-B），建立并返回会话和被叫方 KMS 相关信息。

**步骤 8**　会话通知。

CMSP 按照主叫方 A 上传信息中的主被叫号码进行业务开通状态判定，并推送通知和会话相关信息到被叫方 B 所属 KMS，同时将加密通话的主叫方 A 的相关信息（包括其所属 KMS）发送给被叫方所属 KMS。

**步骤 9**　量子密钥分发与中继。

当主被叫用户属于不同 KMS 管理，QKM-A 和 QKM-B 之间进行主叫方和被叫方所请求的 WK 的密钥协商，其实质上是通过量子通信网络进行具有量子属性密钥的生成、可信中继和安全分发，最终 QKM-A 和 QKM-B 获得一致的 WK 并通过传输层安全通道传送给各自关联的 KMS。

**步骤 10**　获取终端加密公钥。

主被叫终端所属 KMS 从各自密钥池中分别取出主被叫终端的加密公钥，包括 SM2 加密公钥和 PQC 加密公钥。

**步骤 11**　密钥分发。

主被叫终端所属 KMS 分别向主被叫终端分发 WK，使用商密和 PQC 混合密钥封装进行工作密钥的安全传递：

SM4_ENC(WK, K1 ⊕ K2) || SM2_Encap(K1, PUB_SM2) || PQC_Encap (K2, PUB_PQC) || SM2_Sign （LABEL||SID_WK||SID_CALL||UID，PRIV_SM2_KMS） || PQC_Sign （LABEL||SID_WK||SID_CALL||UID， PRIV_PQC_KMS） || Token

其中，LABEL 以固定字符串表示密钥分发标签，SID_WK 表示本次申请密钥的会话标识，SID_CALL 表示本次所申请密钥用来保护的通信会话标识，UID 表示用户标识，SM4_ENC (WK， K1⊕K2)表示采用国密算法 SM4 和 K1⊕K2 得到的密钥对 WK 进行对称加密运算。SM2_Encap 表示采用国密算法 SM2 和用户 SM2 公钥 PUB_SM2 对随机密钥 K1 进行 SM2 密钥封装，PQC_Encap 表示采用 PQC 算法和用户 PQC 公钥 PUB_PQC 对随机密钥 K2 进行 PQC 密钥封装，Token 表示首次密钥申请或失效后重新申请

的用户访问令牌。

**步骤12** 加密通话。

以上的密钥请求和分发过程与语音终端的通信会话建立过程是彼此独立的。安全中间件获得WK后，若语音终端的通信连接已建立完成，则使用该次会话的WK对语音数据进行加密，建立主被叫方之间的加密通话。

## 4 结束语

QKD的密钥分发过程基于量子力学原理，可以面对量子计算机的威胁，但其适用范围主要集中在特定场景下的密钥分发；PQC基于数学算法，能够适用于各种通信需求，但其安全性依赖于数学难题的复杂性，理论上仍存在未知漏洞。本文提出的融合QKD和PQC的电信运营商密码基础设施功能模型，通过分段部署、分层防护，形成QKD和PQC结合的混和密码系统，能够提供多层次的安全保障机制，更好地应对量子计算的攻击，为电信运营商提供高安全性的密码支撑能力。

下一步，结合QKD设备小型化、芯片化、长距化的技术发展趋势，以及在密钥、签名大小和性能方面具有优势的轻量化PQC算法的研究进展，可以实现更为密集化、低成本的QKD密钥分发节点部署，并将终端侧的QKD应用延伸到物联网和可穿戴设备等资源受限环境中，在后量子密码的助力下大幅度提升量子密钥分发的使用范围。

## 参考文献：


[1] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[2] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[3] 密码行业标准化技术委员会. 诱骗态BB84量子密钥分配产品技术规范: GM/T 0108—2021[S]. 2021.
Technical Committee for Standardization of Cryptography Industry. Decoy-state BB84 quantum key distribution product technology specification: GM/T 0108—2021[S]. 2021.

[4] 中国通信标准化协会. 量子密钥分发(QKD)系统技术要求 第1部分：基于诱骗态BB84协议的QKD系统: YD/T 3834.1—2021[S]. 2021.
CCSA. Quantum key distribution (QKD) system technical requirements part 1: QKD system based on decoy state BB84 protocol: YD/T 3834.1—2021[S]. 2021.

[5] LIAO S K, CAI W Q, LIU W Y, et al. Satellite-to-ground quantum key distribution[J]. Nature, 2017, 549(7670): 43-47.

[6] 全国网络安全标准化技术委员会. 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制: GB/T 15843.3—2016[S].2016.
National Technical Committee for Network Security Standardization. Information technology - security techniques - entity authentication - part 3: mechanisms using digital signature techniques: GB/T 15843.3—2016[S]. 2016.

[7] 中国国家标准化管理委员会. 信息安全技术 传输层密码协议（TLCP）：GB/T 38636—2020[S].2020.
China National Standardization Administration Committee. Information security technology—transport layer cryptography protocol(TLCP): GB/T 38636—2020[S].2020.

[8] 国家密码管理局. SSL VPN技术规范: GM/T 0024—2023[S]. 2023.
State Password Administration. SSL VPN specification: GM/T 0024—2023[S]. Beijing, 2023.

[9] 3GPP. 3G security; security architecture: TS 33.102 V19.1.0[S]. 2025.

[10] 3GPP. Security architecture and procedures for 5G system: TS 33.501 V19.3.0[S]. 2025.

[11] NIST. Module-lattice-based key-encapsulation mechanism standard: FIPS 203[S]. 2024.

[12] NIST. Module-lattice-based digital signature standard: FIPS 204[S]. 2024.



[作者简介]

**罗俊**（1975– ），男，博士，中电信量子信息科技集团有限公司研究员级高级工程师，主要研究方向为网络安全、密码技术和量子密钥分发在电信运营商网络中的应用。