融合量子密钥分配的电信运营商密码应用体系

罗俊，刘驰，王丙磊
（中电信量子科技有限公司，安徽 合肥 230088）

摘　要：基于量子密钥分配（quantum key distribution，QKD）的通信网络具备实现 “perfect secrecy”（完美保密性）的能力，当前还不能满足大规模应用的需求，在实际应用中需要结合经典密码技术。提出了融合量子密钥分配的电信运营商密码应用体系的功能架构模型，介绍了模型的层次结构、核心的网元和功能模块以及接口关系，给出了应用体系的整体框架，介绍了框架的主要组成部分，描述了应用体系的典型应用场景及其工作流程。

关键词：量子密钥分配；密码；应用体系
中图分类号：TN918
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2023015

Telecom-operators cryptography application system with quantum key distribution

LUO Jun, LIU Chi, WANG Binglei
China Telecom Quantum Technology Co., Ltd., Hefei 230088, China

Abstract： The communication network based on quantum key distribution (QKD) has the ability to realize “perfect secrecy”. At present, it cannot meet the needs of large-scale applications and needs to combine classical cryptography in practical applications. Firstly, the functional architecture model of the telecom-operators cryptography application system integrating quantum key distribution was proposed, and then the hierarchy, the core network elements, the functional modules, and the interface relationships of the model were described. Furthermore, the framework of the application system was given, and the main components of the framework were introduced. Finally, the typical application scenarios and workflow were illustrated.

Key words： quantum key distribution, cryptography, application system

0　引言

量子通信是利用量子叠加态和纠缠效应进行信息传递的新型通信方式，基于量子力学中的不确定性、测量坍缩和不可克隆三大原理提供了无法被窃听和计算破解的绝对安全性保证。量子密钥分配（quantum key distribution，QKD）是量子通信的重要应用领域[1]，是利用量子力学特性保证通信安全性，借助量子叠加态的传输测量实现通信双方安全的量子密钥共享，从而为实现无条

收稿日期：2022–10–03；修回日期：2023–01–09

件绝对安全的保密通信创造条件。以量子密钥分配为基础的量子保密通信已成为未来保障网络信息安全的一种非常有潜力的技术手段，是量子通信领域理论和应用研究的热点。目前已有多个国家建立了基于 QKD 的通信网络，如美国国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）的 QKD 网络、欧洲基于量子密码的保密通信网络（secure communication based on quantum cryptography，SECOQC）、中国京沪干线等。近日，安徽合肥量子城域网正式开通，其量子密钥分配网络光纤全长 1 147 km，提供 150 节点左右用户站点覆盖能力，实现合肥市绝大部分政府单位的接入，成为目前国内规模最大、用户最多、应用最全的量子保密通信城域网。

香农在其代表性论文 *Communication theory of secrecy systems*（《保密系统通信原理》）中提出[2]，在一次一密且密钥与消息等长的条件下，可以做到通信的“perfect secrecy”，并给出了严格的数学证明。从理论上讲，基于 QKD 的通信网络具备实现“perfect secrecy”的能力，但当前 QKD 网络在传输速率、传输距离、部署范围等方面还不能满足大规模应用的需求，需要结合经典密码技术实现规模化应用。

1　功能架构模型

融合量子密钥分配的运营商密码应用体系功能架构模型如图 1 所示。该模型采用分层结构，包括提供量子密钥分配的量子通信层、提供密码基础服务的密码服务层、提供管理和编排服务的密码管理层以及使用密码服务的用户业务应用层 4 个层次。各层内部包括多个基本网元以及各网元内部的子功能模块，各层之间以及各层内部的各网元或子功能模块之间通过接口参考点进行命令和数据的交互。

1.1　基本网元及功能模块

（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配网络（quantum key distribution network，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）、QKD 模块和 QKD 链路。量子通信层中，通常由一对通过 QKD 链路连接的 QKD 模块执行 QKD 协议生成 QKD 密钥。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。

（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，其基本网元包括密钥管理系统（key management system，KMS）网元、硬件随机数发射器（random number generator，RNG）网元和硬件安全模块（hardware security module，HSM）网元。

- KMS 网元即密钥管理系统网元，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 manager，KIM）和密钥池（key pool，KP）组成。密码服务代理提供数据加/解密、实体鉴别、完整性校验等与密码运算功能的服务代理；密钥管理代理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；密钥充注管理器提供主密钥的充注功能；密钥池进行密钥缓存和三库（在用库、备用库、历史库）管理。
- RNG 网元提供真随机数，在本体系中表现为量子随机数发生器。
- HSM 网元以硬件的形式提供密码运算等密码服务功能，并采用虚拟化技术实现多个虚拟密码设备，以实现和云网应用的融合。

（3）密码管理层网元及其功能模块

密码管理层主要提供密码服务的管理编排，以实现密码相关业务的管理功能（故障管理、配置管理、计费管理、性能管理、安全管理）。其主

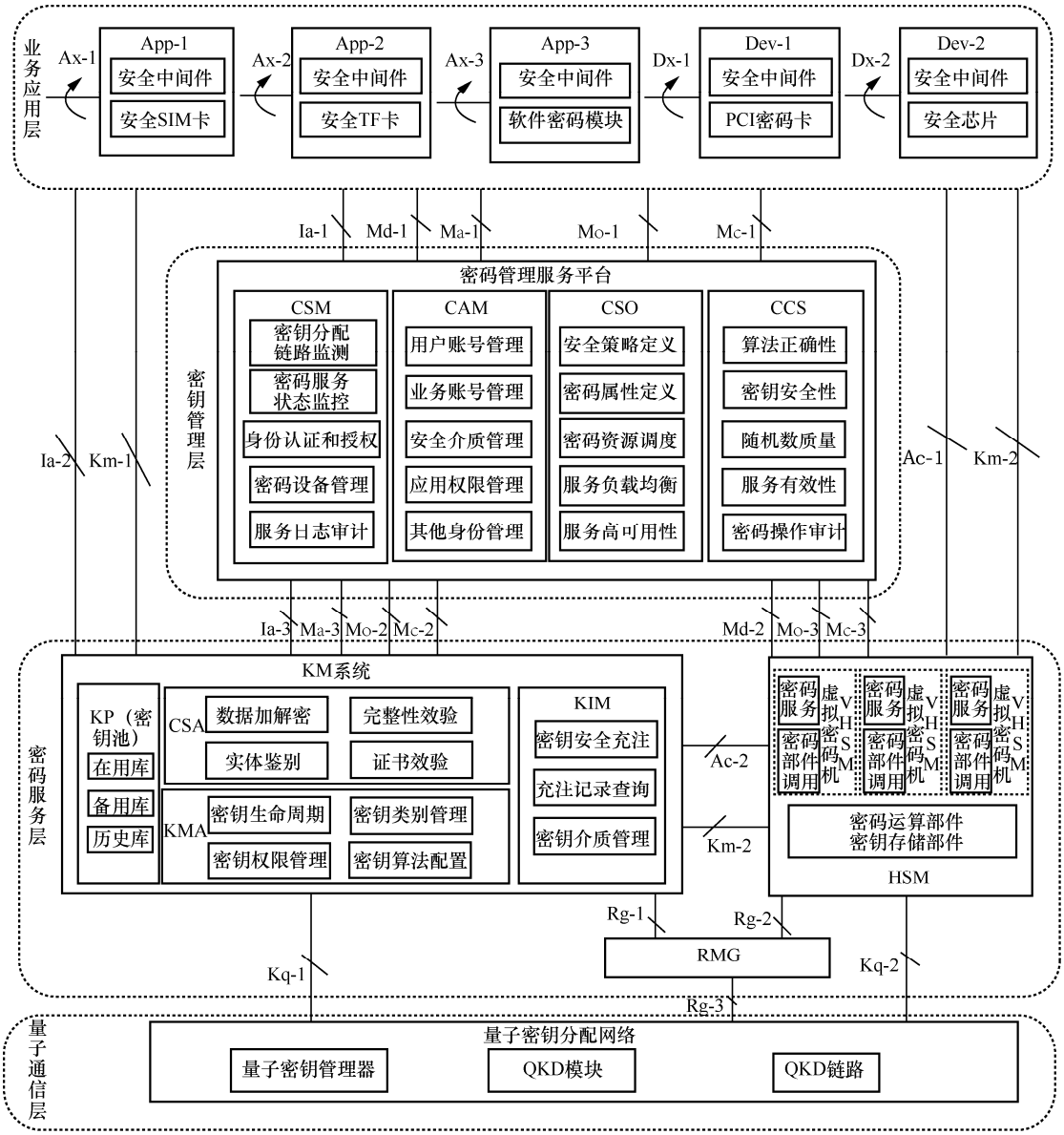

图 1　融合量子密钥分配的密码应用体系功能架构模型

要网元为密码管理服务平台（cryptgraphy management service platform，CMSP），该平台由密码服务管理（cryptgraphy service management，CSM）、密码应用管理（cryptgraphy application management，CAM）、密码服务编排（cryptgraphy service orchestration，CSO）和密码合规性监控（cryptgraphy compliance supervision，CCS）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。

（4）业务应用层网元及其功能模块

业务应用层包括的网元根据所配备密码部件的形态分为五大类：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上云应用 App-3、配

备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。

1.2　接口参考点

（1）管理类接口参考点

管理类接口参考点，包括以下 4 类。

- 管理编排接口参考点（Mo），是连接 CSO 模块和各类业务应用（Mo-1）、KMA 模块（Mo-2）以及 HSM 网元（Mo-3）的参考点，负责传输服务编排信息和数据。
- 设备管理接口参考点（Md），是连接 CSM 模块和各类业务应用的相关密码设备（Md-1）以及 HSM 网元（Md-2）的参考点，负责传输密码设备管控信息和数据。
- 应用管理接口参考点（Ma），是连接 CAM 模块和各类业务应用（Ma-1）以及 KMS 网元（Ma-2）的参考点，负责传输密码应用管控信息和数据。
- 密码合规性检查接口参考点（Mc），是连接 CCS 模块和各类业务应用（Mc-1）、KMS 网元（Mc-2）以及 HSM 网元（Mc-3）的参考点，负责传输合规管控信息和数据。

（2）服务类接口参考点

服务类接口参考点，包括以下 4 类。

- 密钥管理接口参考点（Km），是连接 KMA 模块和各类业务应用（Km-1）、HSM 网元和各类业务应用（Km-2），以及 HSM 网元和 KMA 模块（Km-3）的参考点，负责传输密钥管理信息和数据。
- 量子密钥分配接口参考点（Kq），是连接 QKM 和 KMA 模块（Kq-1）以及 HSM 网元（Kq-2）的参考点，负责传输量子密钥分配信息和数据。
- 密码算法调用接口参考点（Ac），是连接 HSM 网元和各类业务应用（Ac-1）以及 KMS 网元（Ac-2）的参考点，负责传输密码算法调用和密钥管理命令和数据。
- 随机数生成接口参考点（Rg），是连接 RNG 网元和 KMS 网元（Rg-1）、HSM 网元（Rg-2）以及 QKM（Rg-3）的参考点，负责传输随机数命令和数据。

（3）身份类接口参考点

身份类接口参考点包括身份管理和鉴权接口参考点（Ia），是连接 CAM 模块和各类业务应用（Ia-1）、KMS 网元和各类业务应用（Ia-2），以及 CAM 模块和 KMS 网元（Ia-3）的参考点，负责传输身份鉴权信息和数据。

（4）通信类接口参考点

通信类接口参考点，包括以下两类。

- 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。
- 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。

2　应用体系结构

一个完整的密码体系包括密码芯片、密码模块、密码设备、密码系统、密码应用等主要组成部分，而密钥是密码体系最为核心的关键要素。融合量子密钥分配的运营商密码应用体系，是把密钥作为整个密码应用体系的核心，并将其建立在 QKDN 之上，以量子随机数和量子可信信道实现密钥的生成和安全在线分发，以 QKDN 节点、密钥管理系统、密码管理服务平台、安全中间件、密码模块[3]（安全芯片/安全 SIM 卡/安全 TF 卡/PCI 密码卡/软件密码模块）等基本的密码网元构成安

全合规的量子密钥应用基础设施，以该基础设施为中心，在应用上覆盖物理与环境安全、设备与计算安全、应用与数据安全、网络与通信安全[4]，并结合电信领域软件定义网络（software defined network，SDN）和网络功能虚拟化的技术发展趋势，满足密码合规监管和安全可视化要求，形成以融合量子通信技术的集中密钥管理和“一次一密”的对称密码体制[5-6]为特色的密码应用体系。

2.1 整体框架

融合量子密钥分配的密码应用体系整体框架如图 2 所示，融合量子密钥分配的运营商密码应用体系由量子密钥应用和量子密钥应用基础设施两大部分构成，量子密钥应用基础设施贯穿功能架构模型的量子通信层、密码服务层、密码管理层以及业务应用层 4 个层次，通过安全中间件向用户各种类型的业务应用提供密码相关的

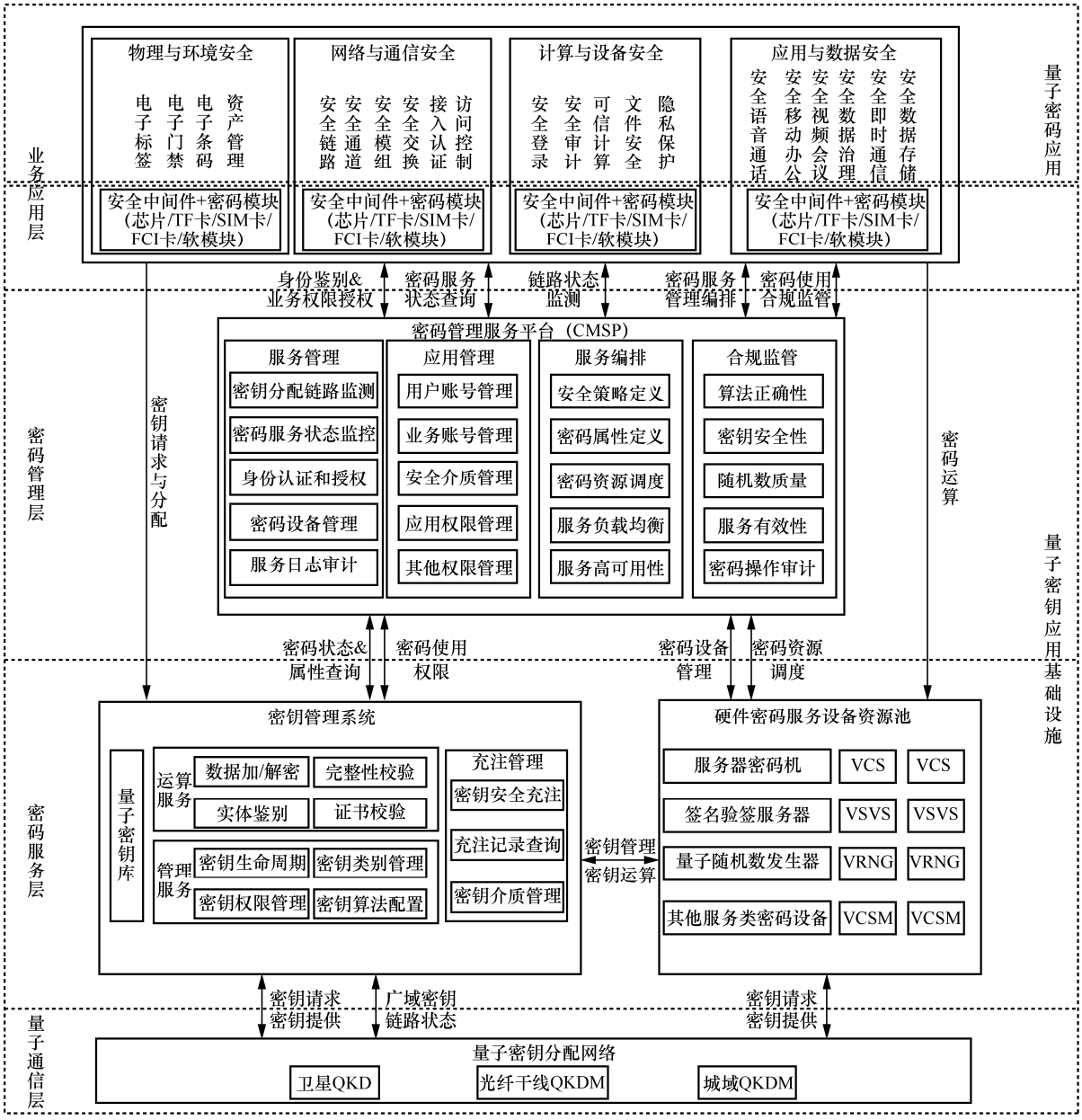

图 2 融合量子密钥分配的密码应用体系整体框架

各类安全服务，包括量子密钥的请求与分配、密码运算的服务端调用、身份鉴别和授权、通过调用各类密码模块实现本地的密钥管理和密码运算等。

2.2　业务应用层

业务应用层中各种设备、终端和应用所广泛部署的安全中间件在整个密码应用体系中具有关键作用，是连接量子密钥应用基础设施和用户业务应用的桥梁，向上屏蔽各类密码模块的差异性和各种密码服务的细节，提供抽象、稳定和统一的密码服务接口和安全入口，向下则结合密码管理服务平台提供服务路由、负载均衡、身份鉴别、故障容错等高可用性能力和安全支撑，并通过适配器模式集成不同密码资源的密码能力。在某种程度上，安全中间件可以看作一种分布式的、服务前移的密码服务类“应用程序接口（application program interface，API）网关”。

2.3　密码管理层

密码管理层中的密码管理服务平台是整个运营商密码应用体系的枢纽，类似于业务中台，体现的是运营商安全可视化以及业务集中受理和业务全程可管可控的核心需求。CMSP 承担的功能主要是密码服务及相关业务的管理编排和合规监管，为分布式泛在化部署的安全中间件提供管理和服务能力支撑，并集成身份管理模块进行全网统一的身份管理、认证和鉴权。从 SDN 的视角来看，CMSP 作为整个运营商密码应用体系的控制器和部分管理器的角色存在。

由于运营商业务的复杂性和用户类别的广泛性，在密码应用体系中会存在多个密码系统，以实现一定程度的安全隔离和业务封闭性，但这些彼此分割的用户和业务之间又会存在一定的互联互通需求。CMSP 具备密钥分发链路监测能力，可实现连接不同量子密钥分配网络节点的不同密码系统间的用户、业务、介质、权限、密钥分发链路的关联关系管理，是从属于不同密码系统的用户业务之间互联互通的桥梁。

2.4　密码服务层

密码服务层主要提供密钥管理和密码运算资源。本体系中的密钥管理系统，是将量子通信技术融入传统密码体系的关键环节。量子随机数发生器或量子密钥分配网络面向密钥管理系统提供具备量子属性的密钥，通过密钥管理系统的全网分发实现具备量子属性的密钥在运营商网络的全面应用。密钥管理系统对具备量子属性的密钥的生成、充注、存储、分发、使用、备份和销毁进行全生命周期管理。

密码服务层中的密码运算资源，则面向运营商网络功能虚拟化的核心业务需求，实现各类硬件密码设备的虚拟化和资源池化，包括服务器密码机、签名验签服务器、量子随机数发生器以及其他服务类的密码设备，通过基础设施即服务（infrastructure as a service，IaaS）的方式构成 HSM 资源池，提供可伸缩、高可用的弹性密码运算服务。

2.5　量子通信层

量子通信层的 QKDN 构成了整个密码应用体系的基石。量子密钥分配网络基于诱骗态 BB84 量子密钥分配协议[7-10]，采用偏振编码进行量子密钥分配，通过量子态信号传输（通过光纤或自由空间等量子信道发送加载了密钥信息的量子态的光脉冲）和协议后处理（通过经典信道完成量子态密钥的筛选、纠错和安全增强），并向密钥管理层和应用层提供密钥输出，为本体系提供了传输过程不可窃听、不可破译的具有量子属性的密钥。当前投入实用化的 QKDN 已经具有卫星、光纤干线、城域网等多种形式。量子密钥分配网络框架模型如图 3 所示，QKDN 包括量子层、密钥管理层、QKDN 控制层等核心层[1]，每一个具备密钥分发能力的 QKD 节点（可信节点）均由 QKDN 控制器、KMS、QKD 模块构成，不同 QKD 节点之间通过 QKD 链路（QKD link）建立密钥管理链路（KM link），从而为连接 QKD 节点的应用（本体系中统一由 KMS

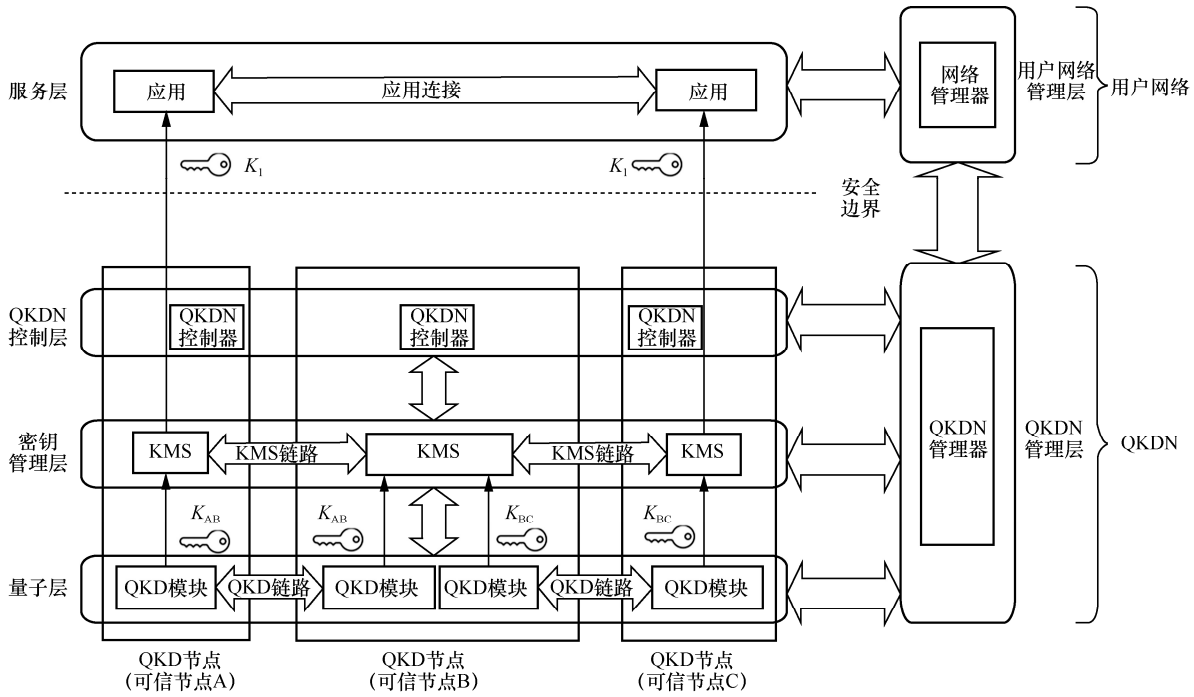

图 3　量子密钥分配网络框架模型

直接连接 QKD 节点，由 KMS 面向应用提供密钥）提供具有量子属性的密钥，并实现连接不同 QKD 节点的应用之间的密钥同步。

3　典型应用场景

语音类应用是电信运营商最为核心的业务之一。当前基于 4G 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 新空口语音承载（voice over new radio，VoNR）高清通话正在移动端得到越来越广泛的使用。VoNR 和 VoLTE 作为面向手机和数据终端的高速无线通信标准，基于 IP 多媒体子系统（IP multimedia subsystem，IMS）网络和会话初始化协议（session initialization 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，而不再需要维护和依赖传统的电路交换语音网络。正是由于语音的 IP 化传输，其安全性显得至关重要。目前 VoNR 和 VoLTE 采用 3GPP 提出的认证与密钥协商（authentication key agreement，AKA）协议完成用户和网络间的身份认证[11-12]，该方法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实现用户的身份认证安全性。由于长期共享密钥长期频繁的使用，其安全性必然会下降。在 VoNR 和 VoLTE 之外，移动互联网上也存在大量互联网电话（voice over IP，VoIP）类应用，这类应用的标准化程度不高，而且普遍存在对服务器的依赖度高、缺乏端到端的密码方案等问题。

在本密码应用体系中，采用预充注大容量用户主密钥以及实时在线分发加密通信会话的工作密钥的方式实现语音加密通信和密钥分发过程的双重“一次一密”，具有较高的密码安全性。除了实现属于同一密钥管理系统内的语音终端之间的域内加密通话，本体系还通过 QKDN 实现了属于不同密钥管理系统（连接不同的 QKD 节点）的语音终端之间进行跨域加密通话，加密通话过程示意图如图 4 所示，具体流程如下。

（1）密钥充注

语音终端初始化时进行用户主密钥的预充注，通过离线充注的方式向安全 SIM 卡内充注大

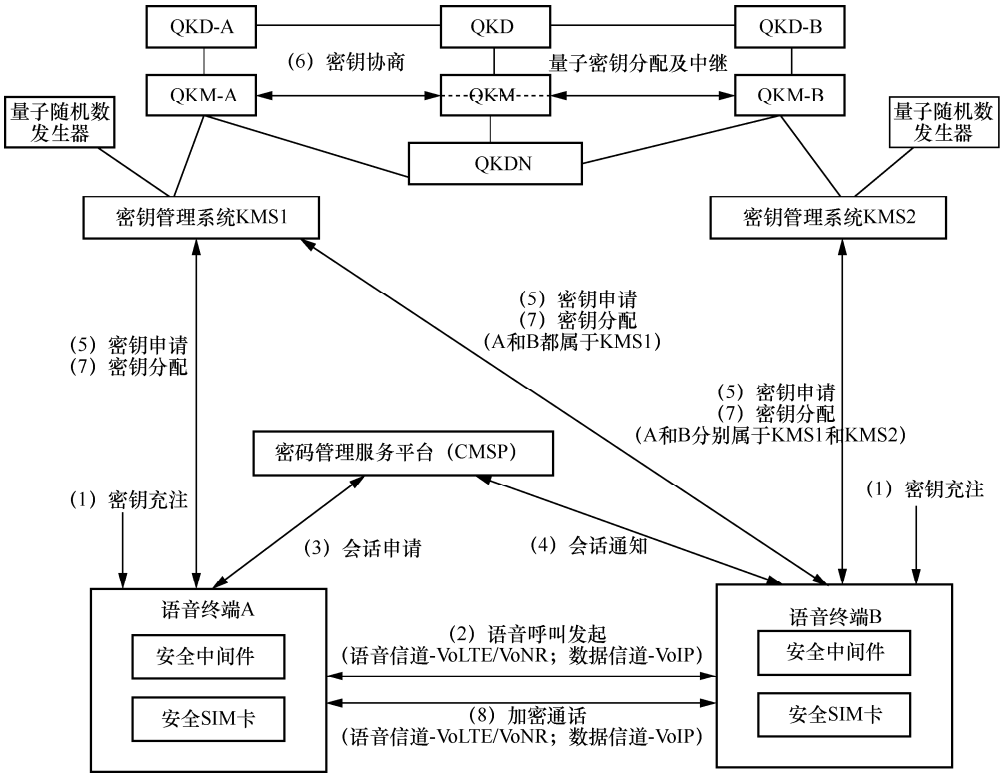

图 4　加密通话过程示意图

容量的对称密钥（以 128 bit 的 SM4 对称密码算法为例，2 MB 的存储空间可充注 10 万条以上的密钥），并在该 VoLTE 终端所属的 KMS 建立密钥池加密存储所充注的密钥。

（2）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。

（3）会话申请

当主叫方语音终端 A 发起加密呼叫，其安全中间件通过数据信道访问至 CMSP 进行业务查询和身份鉴别，确认被叫方语音终端 B 的平台所属关系，建立会话相关信息并返回给主叫方 A。

（4）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，唤醒被叫方的安全中间件，同时将加密通话的主叫方 A 相关信息发送给被叫方。

（5）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，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 管理时，KMS 直接向量子随机数发生器申请并获取实时随机数作为工作密钥（working key，WK）；当主被叫用户属于不同 KMS 管理时，其各自从属的 KMS 分别携带主叫方或被叫方终端的相关信息向主叫方或被叫方各自关联的量子密钥分配网络的 QKM（图 4 中主叫方关联 QKM-A，被叫方关联 QKM-B）请求用于该次加密通话的 WK。密钥申请报文由随机选择语音终端安全 SIM 卡内的一条用户主密钥（user master key，UMK）进行完整性保护，报文结构如下。

SM3_HMAC (LABEL||SID_WK||SID_CALL||UID||KeyID||NUMBER_CALL||NUMBER_CALLED,UMK)

其中，SM3_HMAC 表示采用国密算法 SM3 和

UMK 对报文进行带密钥的杂凑运算，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，KeyID 表示主密钥 ID，NUMBER_CALL 和 NUMBER_CALLED 分别表示主叫和被叫号码。

（6）密钥协商

当主被叫用户属于不同 KMS 管理时，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 获得一致的密钥并通过私有信道传送给各自关联的 KMS。

（7）密钥分配

KMS 获取工作密钥后，KMS 和语音终端间采用基于对称密码体制的安全分发机制[6]，通过随机选择语音终端安全 SIM 卡内的一条 UMK，将要下发的 WK 进行加密保护，并和密钥 ID 一起发给终端（发送的消息整体以该 UMK 为密钥，使用带密钥的密码杂凑算法进行完整性保护）。语音终端的安全中间件获取工作密钥密文信息后，通过安全 SIM 卡内的同一条用户主密钥进行完整性验证和解密，获取本次会话的工作密钥。主叫方与被叫方语音终端均采用此方法获得会话的工作密钥。用户主密钥在密钥管理系统的密钥池和终端的安全 SIM 卡内部均采用用户标识+密钥 ID 的方式进行存储和检索，已经使用过的用户主密钥标注为作废。密钥分发报文结构如下。

SM3_HMAC (LABEL||SID_WK||SID_CALL ||UID||KeyID||SM4_ENC(WK,UMK)，UMK)

其中，LABEL 以固定字符串表示密钥分发标签，SM4_ENC(WK,UMK)表示采用国密算法 SM4 和用户主密钥 UMK 对 WK 进行对称加密运算。

（8）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。安全中间件获得工作密钥后，若语音终端的通信连接已建立完成，则使用该次会话的工作密钥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

“一次一密”在信息论上具有“perfect secrecy”，可以抵抗任何算法的破解，包括量子计算。采用量子通信技术进行的密钥分发，即 QKD，由量子力学中的量子不可分割原理和不可克隆定理保证了密钥在分配过程中不会被任何第三方无感知地截获，成为实现“一次一密”密钥分发的理想方式。但是当前的 QKD 技术依赖于光纤网络，并且单光子的探测设备成本较高，应用范围有限，目前只能进行核心网络的部署，无法应用在终端和接入级设备上。

本文对量子通信技术和传统的密码技术进行融合，将具备无条件物理安全特性的 QKDN 和具备计算安全特性的传统密码应用体系相结合，提出了融合 QKD 的运营商密码应用体系。该体系满足电信运营商业务集中管控和安全可视化的业务需求，以密码合规为前提，以融合量子通信技术的集中密钥管理和“一次一密”的对称密码体制为特色，适应电信领域软件定义网络和网络功能虚拟化的技术发展趋势，能够为电信运营商提供具备高安全性的密码支撑能力。

参考文献：

[1] ITU. Overview on networks supporting quantum key distribution: ITU-T Y.3800-2019[S]. 2019.

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

[3] 全国信息安全标准化技术委员会. 信息安全技术 密码模块安全要求: GB/T 37092-2018[S]. 2018.
National Information Security Standardization Technical Committee. Information security technology-security requirements for cryptographic modules: GB/T 37092-2018[S]. 2018.

[4] 全国信息安全标准化技术委员会. 信息安全技术 信息系统密码应用基本要求: GB/T 39786-2021[S]. Beijing, 2021.
National Information Security Standardization Technical

Committee. Information security technology - baseline for information system cryptographic applications: GB/T 39786-2021[S].2021.

[5] International Organization for Standardization. Information technology-security techniques - key management - part 1: framework: ISO 11770-1-2010[S]. 2010.

[6] International Organization for Standardization. Information technology - security techniques - key management - part 2: mechanisms using symmetric techniques: ISO 11770-2-2018[S]. 2018.

[7] BENNETT C H，BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. [S.l.:s.n.] , 1984: 175-179.

[8] 濮荣强. BB84 协议与量子密钥分发的应用[J]. 淮北师范大学学报(自然科学版), 2022, 43(1): 68-73.
PU R Q. BB84 protocol and application of quantum key distribution[J]. Journal of Huaibei Normal University (Natural Sciences), 2022, 43(1): 68-73.

[9] 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.
Cryptography Standardization Technical Committee. Decoy-state BB84 quantum key distribution product technology specification: GM/T 0108-2021[S]. 2021.

[10] 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: YDT 3834.1-2021[S]. 2021.
China Communications Standards Association. Technical requirements for quantum key distribution (QKD) system - part1: decoy state BB84 protocol QKD system: YDT 3834.1-2021[S]. 2021.

[11] 3GPP. 3G security: security architecture: TS 33.102 V17.0.0[S]. 2022.

[12] 3GPP. Security architecture and procedures for 5G system: TS 33.501 V17.7.0[S]. 2022.

[作者简介]

罗俊（1975– ），男，博士，中电信量子科技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配在电信运营商网络中的应用。

刘驰（1990– ），男，中电信量子科技有限公司工程师，主要研究方向为数据安全、量子通信技术和量子密钥分配在电信运营商网络中的应用。

王丙磊（1986– ），男，中电信量子科技有限公司工程师，主要研究方向为移动安全、量子通信技术和量子密钥分配在电信运营商网络中的应用。