量子城域网技术分析与工程实践

胡晓宇，李天泽
（中国电信股份有限公司上海分公司，上海 200040）

摘　要：量子保密通信利用量子QKD技术实现密钥的安全分发和传递，量子城域网是利用量子保密通信技术组网，为用户提供城域范围内的密钥服务，并与国家级的量子骨干网实现对接。对量子密钥分发中的量子层、密钥管理层、控制层和应用层的分层技术实现和具体功能进行分析。结合上海量子城域网的建设，对量子城域网的组网架构、实现方案和应用进行分析，提供量子城域网建设的参考。

关键词：量子密钥分发；BB84协议；量子城域网；密钥分发；密钥管理
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025075

0　引言

随着信息技术的飞速发展，网络安全问题日益严峻。传统加密技术依赖于计算复杂度，其安全性主要取决于加密算法和密钥长度的复杂程度。然而，随着量子计算技术的迅猛发展，传统加密方法，特别是非对称算法（如RSA、ECC）面临着前所未有的安全威胁。在这一背景下，量子密钥分发（quantum key distribution，QKD）作为一种基于量子力学原理的密钥分发技术，逐渐成为解决量子时代网络安全挑战的焦点。

QKD利用量子力学的基本特性，如不确定性和不可克隆性，能够实现理论上绝对安全的密钥分发。其中，BB84协议作为最早提出的量子密钥分发协议，以其简单且可行的原理，成为QKD研究和应用的基石。通过BB84协议，通信双方可以安全生成和分发密钥，确保通信的机密性与完整性。为应对量子计算带来的潜在威胁，全球多个国家和地区的政府与科研机构已积极开展QKD技术的研究与部署。例如，欧盟于2019年启动了Open European Quantum Key Distribution Testbed项目，旨在推动跨国QKD网络的建设和应用；中国则已建成了京沪干线、沪合干线等量子密钥分发骨干网项目，旨在利用量子通信技术提升国家网络安全与信息化能力。

在实际应用中，量子密钥分发骨干网络的延伸——量子城域网的建设是实现量子保密通信的重要环节。量子城域网不仅能够实现城域范围内客户之间的密钥安全分发，还可以与量子骨干网结合，覆盖全国范围的密钥分发服务。量子城域网是一个复杂的系统，涉及多层次、多节点的网络架构，各层之间需要协同工作，确保安全密钥的生成、分发和管理。网络建设过程中，需要重点关注网络的整体规划，包括设备ID命名规范、密钥预协商机制、密钥请求路由规则，以及加密路由器（网关）的实施细节，以确保网络的高效运行与密钥的安全性。

2024年，上海电信建成了上海量子城域网。

收稿日期：2024−12−11；**修回日期：**2025−02−17

本文将深入探讨量子城域网的技术实现与工作原理，并结合量子城域网的建设与实施，详细介绍上海量子城域网的组网方案。希望本文能为未来量子城域网的建设提供有价值的参考和借鉴。

1 量子密钥分发网络总体架构

QKD网络的核心功能是进行密钥的安全传递和分发。与传统的IP城域网不同，QKD网络传输的是加密密钥而非实际的数据内容。因此，为实现完整的数据加密和传输能力，QKD网络需要与传统的IP网络相结合，利用QKD生成的密钥来加密通过IP网络传输的数据。为此，国际电信联盟（ITU）发布了“Recommendation Y.3803: Quantum Key Distribution Networks – Key Management”，为量子网络构建及密钥管理提供了规范和指导，以确保其在实际应用中的安全性和可靠性。QKD网络自下往上的顺序依次包括量子层、密钥管理层、控制层和应用层等4个层次。此外，为保证网络的运行，需要配置网管系统对设备进行集中的监控和管理。量子密钥分发网络的整体架构如图1所示。量子密钥分发网络各层名称及作用见表1。

表1 量子密钥分发网络各层名称及作用

序号	名称	主要作用
1	量子层 Quantum layer	在量子设备之间负责点对点量子密钥交换 可类比IP之间的点到点二层链路（如以太或SDH）
2	密钥管理层 Key management layer	站点之间密钥管理 跨站点密钥传中继 可类比IP网络上的三层路由转发
3	控制层 controll layer	网络拓扑管理：建立量子层和密钥管理层的网络视图 网络寻址和路由管理：负责控制和建立端到端密钥分发路径 可类比SDN中的控制器（集中路由计算和路径下发）
4	应用层 Service layer	处理来自客户应用的密钥请求，发放会话密钥

2 量子层

在传统的加密通信中，会话密钥一般为通信双方通过IP信道带，使用非对称算法如RSA（国际标准）或SM2（国密标准）协商得到，其安全性基于大质数分解或离散对数等数学问题。量子计算概念出现后，SHOR算法可在多项式时间内

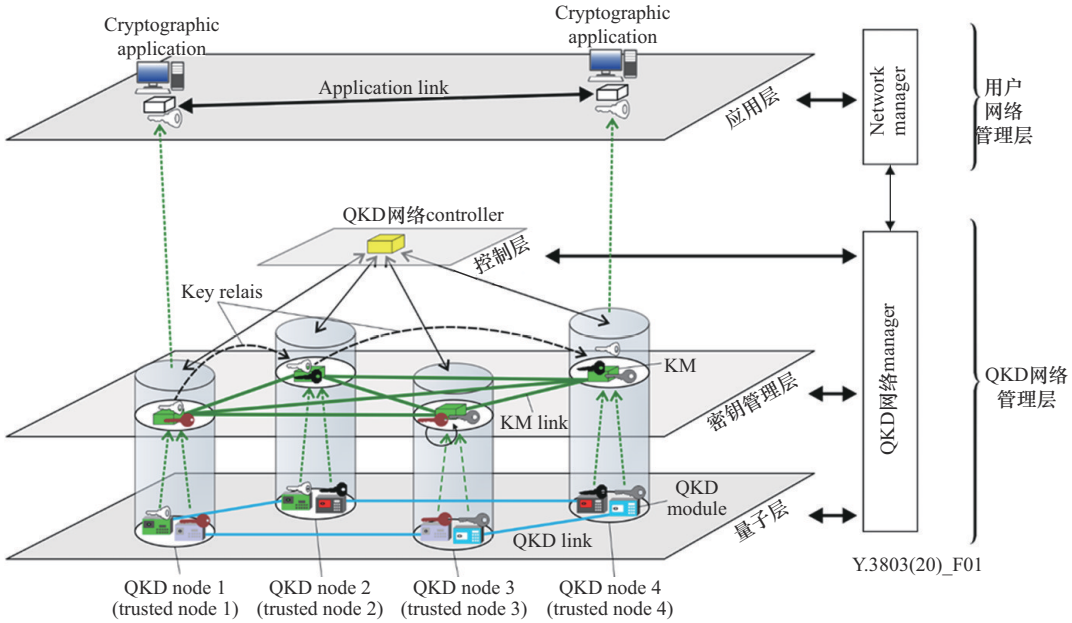

图1 量子密钥分发网络的整体结构

破解基于离散对数的非对称加密算法，因此密码学界产生了“量子危机”。

QKD 则是一种利用量子力学原理实现安全密钥协商的技术。QKD 的核心优势在于其依赖于量子力学中的不确定性原理和量子不可克隆定理，通信双方通过量子传递的信息无法被第三方窃听获取而不被发现，从而实现安全的密钥分发。QKD 技术被认为是抵御量子计算攻击的最有效手段之一，具有重要的应用前景。QKD 的通信协议主要包含基于单光子探测的 BB84 协议和基于连续变量的 GG02 协议，其中 BB84 协议的研究开始更早，应用更广泛。

2.1　基于单光子探测的 BB84 协议

BB84 协议于 1984 年被提出，是第一个实用的量子密钥分发协议。该协议通过在量子信道上传输量子信号，量子态（两种基矢上的 0 和 1）传输和接收光子，基于量子力学原理的测量和比对过程，从而生成一个安全的密钥。BB84 量子密钥协商过程如图 2 所示。BB84 的工作模式主要分为 5 个阶段。

（1）准备和发送阶段（QKD 发送端）

在发送端（QKD 发送端），量子密钥分发的过程从量子态的准备开始。

- 量子态生成：利用单光子源或纠缠光子源生成量子比特。
- 偏振调制：对量子比特进行偏振调制，使其处于 BB84 协议定义的 4 种量子态之一（水平、垂直、45°对角线和 135°对角线）。
- 量子态传输：通过光纤链路传输调制后的量子比特。

在这一步骤中，发送端 Alice 会随机选择一个基矢（如{0,1}或{+,×}），并将相应的量子态发送给接收端 Bob。

（2）传输阶段

量子态通过光纤链路传输，过程中可能会受到衰减和噪声的影响。

（3）接收和测量阶段（QKD 接收端）

在接收端（QKD 接收端），接收方 Bob 通过

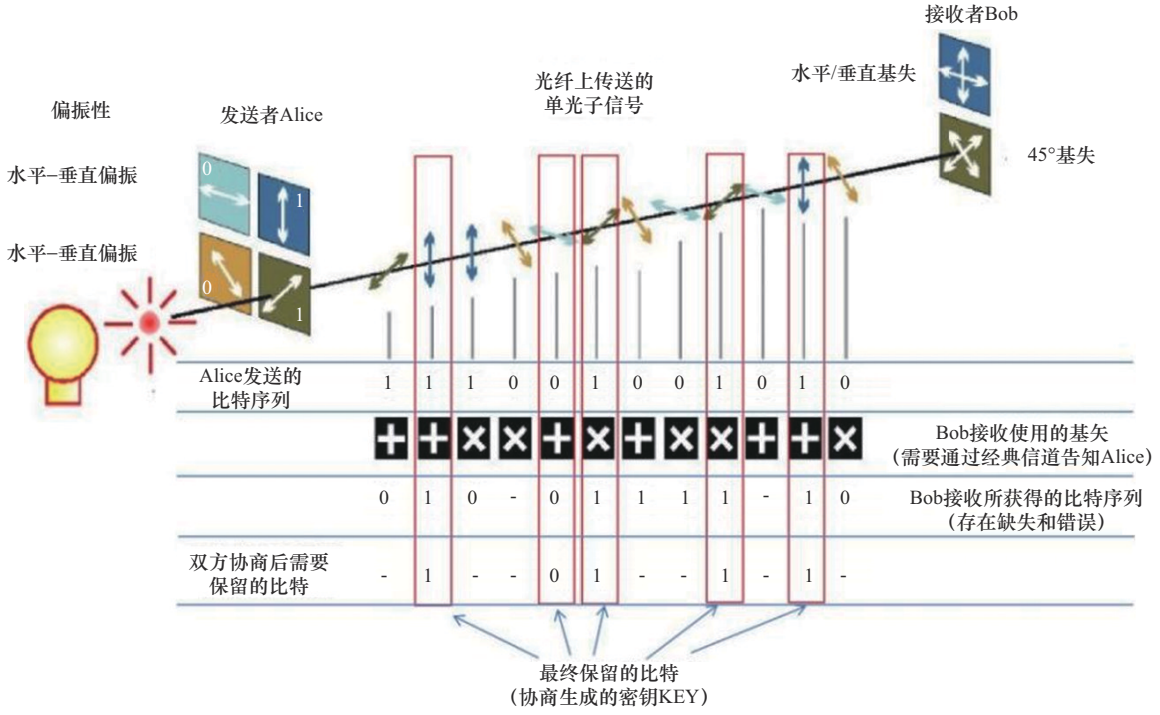

图 2　BB84 量子密钥协商过程

以下步骤进行测量和解码。

- 测量：Bob随机选择一个基矢进行测量（与Alice的选择独立），并记录测量结果。
- 偏振解调：将接收到的量子态进行解调。
- 数据处理：将测量结果转换为经典比特信息。

（4）经典通信和协商

Alice和Bob通过经典通信信道交换基矢信息，并丢弃基矢不匹配的测量结果。这样，他们保留的比特序列将具有高度的相似性和随机性。

（5）纠错和隐私放大

为了确保最终密钥的安全性和可靠性，Alice和Bob进行纠错和隐私放大。

- 纠错：通过信息交换和纠错算法，修正测量误差，确保双方比特序列的一致性。
- 隐私放大：通过算法减少任何可能被窃听者掌握的信息量，提高密钥的安全性。

在上述量子密钥分发的过程中可能存在窃听者，窃听采用的手段可能是通过分光方式进行窃听，也可能是通过中间人的方式窃听后重放。

- 对于分光攻击，由于单光子的不可分性和不可克隆性，窃听者不可能收到与接收者同样的比特信息，因此窃听无效。
- 对于中间人攻击，窃听者即使接收到了量子信道的数据，由于发送者采用随机的偏振基矢发送0/1信号，而中间人并不知道其发送的基矢序列。因此无法正确地接收密钥，而错误基矢的测量会破坏量子态，无法重放给接收者。
- 还有一种中间人攻击方式是窃听者同时截获量子信道和经典信道的数据，再进行重放，对此类攻击的防范措施是发端和收端利用预置密钥对双方经典信道进行认证和加密保护。

BB84协议的实现也面临着一些技术挑战，例如，单光子源的实现、探测器的效率和误码率等因素都会影响协议的实际性能。为了提高BB84协议的实用性和安全性，引入诱骗态等技术对BB84实行改进，以达到实用的目的。

- 诱骗态技术（decoy state method）通过在真实信号中引入不同强度的虚假信号（诱骗态），可以有效检测和防御窃听者的攻击，特别是针对光子数分离攻击。这种技术能够在不显著增加系统复杂性的情况下，提高密钥生成的安全性和效率。
- 设备和技术改进：在设备和技术方面，通过优化单光子源和探测器，以提高BB84协议的实际应用性能。例如，采用量子点作为单光子源可以显著提高光子源的稳定性和效率。另外，误码校正和隐私放大技术也被应用于BB84协议，以提高其抗干扰能力和安全性。

2.2 连续变量QKD（CV-QKD）

连续变量QKD（continuous-variable QKD，CV-QKD）使用连续变量（如光的强度和相位）来编码信息，相较于离散变量QKD，CV-QKD具有更高的密钥生成率和更好地与现有光通信基础设施兼容的优势。CV-QKD使用高斯调制的相干态，其安全性已在渐近条件下得到证明，并进一步扩展到有限大小的情况下。此外，CV-QKD的实现还受益于电信行业的标准设备，如连续波激光器和相干接收器。

3 密钥管理层和控制层架构

QKD网络的量子层主要完成点对点的密钥交换，由于传输距离的限制，点对点量子密钥的传输距离不大于80 km（实际在40 km左右）。因此

QKD网络引入了可信中继的概念，通过一级一级的QKD中继级联，实现远距离的密钥传输。量子城域网要满足城域内任意接入点的密钥传递，就需要多个中继站点将多个点对点的链路连接起来，形成一张密钥分发网络，完成跨区域的密钥分发功能，这就需要通过密钥管理层和控制层实现。密钥管理层功能架构模型如图3所示。

ITU-T Y.3803中将密钥管理（KM）的功能细分为密钥供应代理（KSA）和密钥管理代理（KMA），中国的行业标准统称为KM。

3.1　密钥管理层

密钥管理层负责密钥的生成、分发、存储和管理。其主要功能如下。

- 密钥的生成与中继：量子密钥的产生使用量子随机数发生器。管理系统通过密钥交换操作，解决量子密钥的中继问题。以此确保量子密钥的完整性和安全性，提供逻辑上的点对点密钥分发服务，满足实际应用中的安全需求。
- 密钥存储与管理：密钥生成后，需要通过安全的机制进行存储和管理。密钥管理系统包含密钥存储、更新和撤销机制，以确保密钥在整个生命周期内的安全性和有效性。通过这些机制，密钥管理层可以维护密钥的机密性和完整性，保障QKD网络的整体安全。

密钥端到端分发工作流程如图4所示，流程如下。

（1）量子设备间的密钥协商：不同站点（如终端站和中继站）之间的量子QKD设备通过BB84或GG02协议进行密钥协商，持续生成点对点的加密密钥k-*nm*（*n*、*m*为相邻的节点编号）。这些密钥用于加密客户的会话密钥，确保数据传输的安全性。

（2）密钥管理与存储：各站点的KMA将通过QKD生成的密钥安全存储起来，并在相邻的QKD站点之间形成多个密钥对，以便在后续密钥传输中使用。

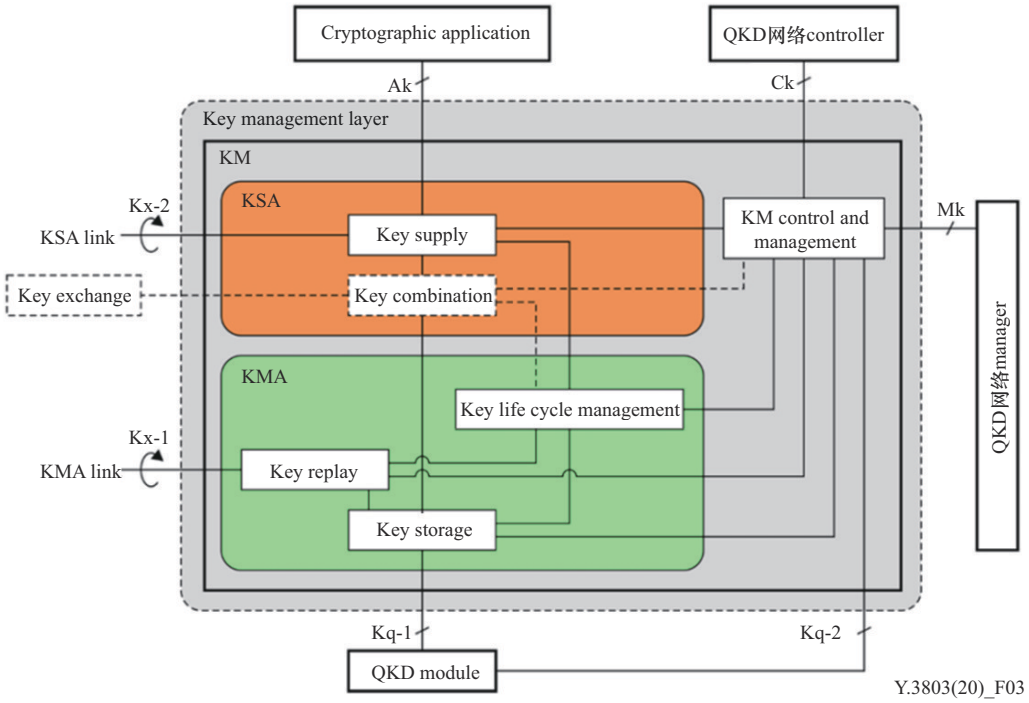

图3　密钥管理层功能架构模型

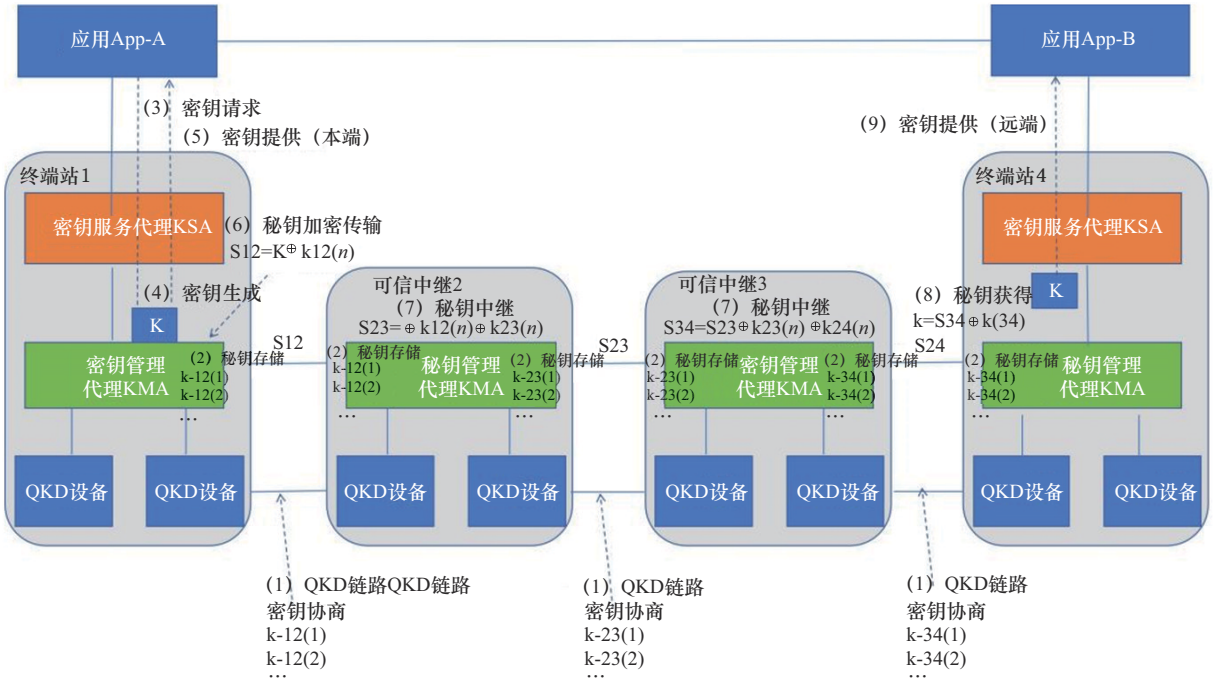

图4 密钥端到端分发工作流程

（3）密钥申请与分发：当应用需要密钥时，它会向密钥管理服务（KMS）请求会话密钥。KMS随即向KMA申请对应的量子密钥，确保密钥生成的安全性。

（4）随机会话密钥生成：KMA通过量子随机数发生器生成随机会话密钥K，并将该密钥传送给KMS，以便后续的密钥分发流程。

（5）会话密钥传递给应用：KMS将生成的会话密钥K发送至本地应用端，确保应用能够安全使用该密钥进行通信加密。

（6）会话密钥的远端传输：当会话密钥K需要传输到远端应用时，KMA会首先判断下一中继站的身份。假设站点1需将密钥传输至站点2，它会取出预存的QKD密钥k12(n)，将会话密钥K与k12(n)进行异或操作生成加密密文S12。随后，S12通过站点之间的IP链路传输至站点2。值得注意的是，k12(n)使用一次一密的方式，用后立即丢弃。

（7）中继站2的密钥解密与传递：中继站2的KMA接收密文S12后，使用已存储的k12(n)对其进行解密（通过异或操作），从而获得会话密钥K。然后，它判断下一个中继站是站点3，并将会话密钥K与已存储的QKD密钥k23(n)再次异或，生成新的密文S23，并通过IP链路传输至站点3。为了降低中途泄密风险，可以连续完成多次异或操作，不在中间生成明文K。

（8）多级中继站的操作：如果从源到终点之间存在多个中继站，则每个中继站都重复上述解密和再次加密的操作，确保密钥安全地逐步传递到最终的目的地。

（9）终端站点获取会话密钥：最终的终端站点通过类似的流程解密密文，成功获取会话密钥K，并将其传递给应用B，实现端到端的安全加密通信。

整个QKD密钥的分发过程体现了预存密钥和对称加密的基本特点。由于QKD所生成密钥的高安全性，它能够有效保护应用层的会话密钥，确保整个通信过程的安全性。这种结合了量子密钥分发与传统对称加密的方式，显著提高了加密系统的安全防护能力，确保了密钥传输和使用过程中不会被窃听或篡改。

3.2　控制层

根据ITU-T Y.3800，控制层由用户网络管理、QKD网络管理和QKD网络控制器3个主要部分组成。

- 用户网络管理：负责处理用户业务请求，确保用户能够高效、安全地使用QKD服务。
- QKD网络管理：负责监控和管理整个QKD网络网络的运行状况，包括设备状态、网络性能和安全事件等。
- QKD网络控制：负责控制密钥服务的实现，管理密钥生成、分发和存储等过程，确保密钥在网络中的安全流转。

控制层的核心功能通常由一台或多台核心控制器KMS承担，这些控制器部署在QKD网络的核心节点中。它们通过传统IP专网与终端用户站，中继站连接，负责控制有量子密钥的分发过程。具体来说，控制层的功能和作用包括以下几个方面。

- 设备登记与状态报告：网络内的QKD和KM设备在正常运行时需要在核心控制器上注册登记，并定期上报其运行状态。这确保了核心控制器能够实时监控整个网络的健康状况，及时发现并解决潜在问题。
- 密钥服务请求处理：当应用层请求的密钥服务涉及跨多个站点的路径选择时，核心控制器会依据当前的网络拓扑和运行状态，计算出最优的密钥分发交换路径。然后，控制器会控制路径上的各个网络节点按照既定的密钥中继方向执行密钥转发操作，最终为加密应用提供服务。
- 拓扑优化与路径计算：控制器根据实时的网络拓扑信息，计算密钥分发/交换的最优路径，确保在网络负载和状态变化时仍能高效地进行密钥分发。这不仅提高了网络的整体效率，还增强了网络的可靠性和安全性。

因此控制层在QKD网络中发挥着至关重要的作用，不仅确保了网络的高效运行和安全管理，还为用户提供了可靠的密钥服务，满足了实际应用中的多种需求。

3.3　应用层

应用层负责密钥的提供服务，确保QKD网络能够为各种实际应用提供支持。密钥可以用于各种应用场景，如加密通信、数据保护、身份验证等。通过将QKD生成的密钥应用于这些场景，提供高等级的安全保障。

应用层需要设计和实现标准化的应用协议和接口，以便于用户和应用程序能够方便地接入QKD网络并使用密钥服务。下面以行业标准YD/T 4303-2023《基于IPSec协议的量子保密通信应用设备技术规范》为例介绍。

行业标准YD/T 4303-2023规定了基于IPSec协议的量子保密通信应用网关设备和终端设备的技术协议、功能性能要求及相关测试方法。该标准加入了量子密钥支持，在以下方面对IPSec协议进行了改进。

- 第一阶段协商与QKD服务信息交换：在IPSec协议的第一阶段协商过程中，通信双方交换QKD服务信息，如图5所示。具体来说，通信双方在协商过程中会交换QKD服务的相关信息，如协议中的N(USE_QKDi)和N(USE_QKDs)消息。通过这些信息的交换，双方能够确定使用QKD服务的具体参数和方式，从而确保量子密钥的安全性和可靠性。
- 量子密钥获取与融合：IPSec协商完成后，双方将从QKD网络中获取量子密钥QK，如图6所示。随后通过融合生成手段，将传统IPSec协商生成的工作密钥组SKEYID与量子密钥QK结合，生成新的融合量子工作密钥组QSKEYID。

通过融合量子QKD技术，IPSec可提供更高安全级别加密服务，满足应用中的高标准安全需

图5 IPSec融量子第一阶段交互示意图

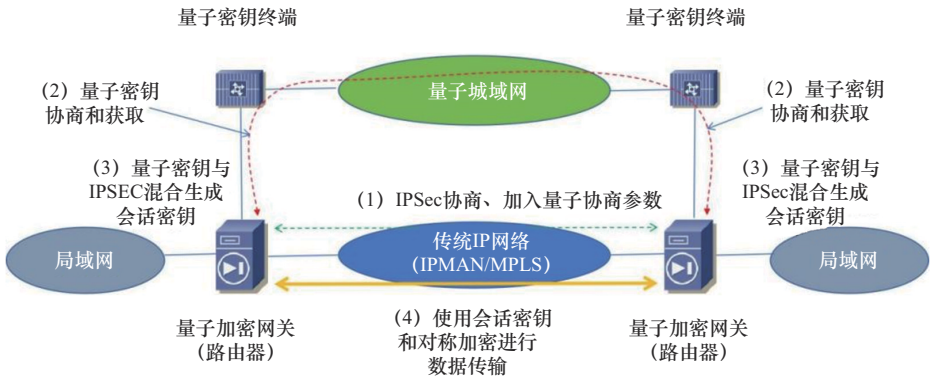

图6 基于IPSec的量子保密通信系统示意图

求，可有效地应对量子计算对加密算法的威胁，实现抗量子计算安全。

4 量子城域网工程实践

4.1 网络整体架构

量子城域分为核心层，汇聚层和接入层。量子城域网架构如图7所示。

- 核心层：核心层承担城域范围的密钥传递工作，一般采用环形结构，具有很高的可用性。核心层还负责与骨干网互联。核心层部署集控站和中继站，其中集控站负责整网运行控制，中继站实现

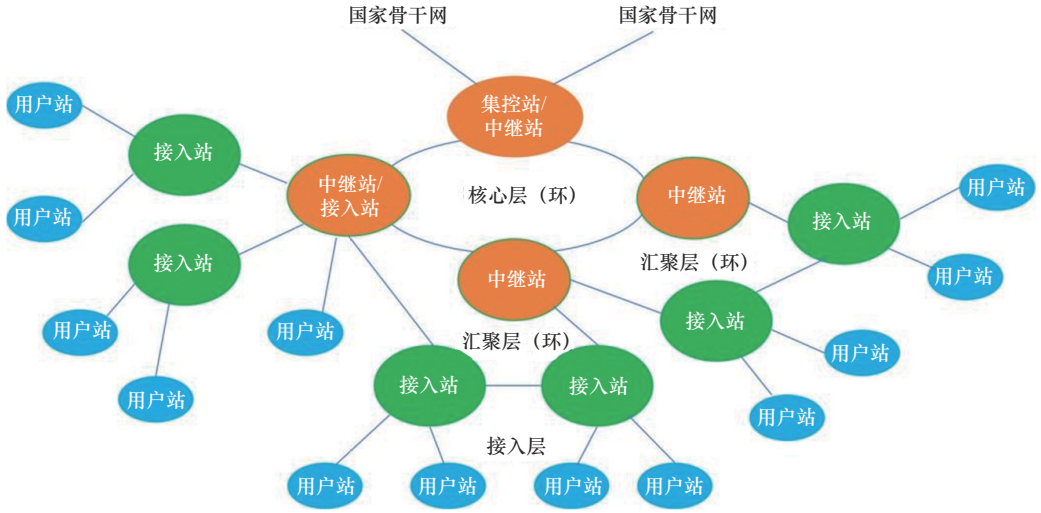

图7 量子城域网架构

具体的密钥转发。

- 汇聚层/接入层：该层负责本区域的密钥分发工作，并与核心层相连，实现跨区域的密钥交换。汇聚和接入层主要由于接入站和对应的中继站组成，结构可以是环形、总线型或树状。
- 用户层：部署于用户站点（机房）的量子密钥设备组成，用于向用户的应用提供密钥服务。

城域网的节点在功能层面分为集控站、中继站、接入站和用户站 4 类站点。当城域网规模较小时，出于成本考虑可以合并多个站点功能组成复合站点。量子城域网接入站的典型结构如图 8 所示。站点类型及对应设备配置见表 2。

在城域网的具体实践中，QKD 设备采用光纤直连方式，实现站点之间的光量子信号传输和同步协商信号（协商信号基于 IP），距离一般不超过 40 km（链路衰减不超过 18 dB）。为保证各站点之间除量子 QKD 外的业务连通性（KM-KM，KMS-KM，设备与网管等），各站点还需要通过 IP 网络连通。在具体的工程实践中，上海电信城域网采用了 MPLS VPN 网络实现量子城域网站点

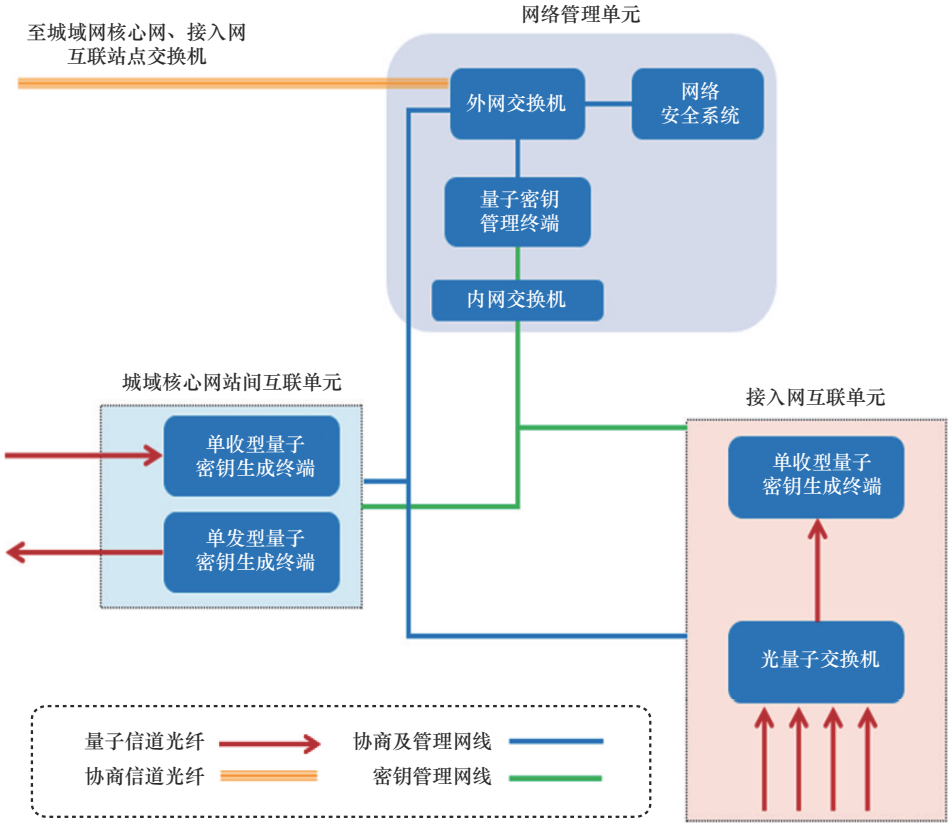

图 8　量子城域网接入站的典型结构

表 2　站点类型及对应设备配置

站点类型	量子设备配置	IP 设备
集控站	QKD 设备、KM 密钥管理器、KMS 控制平台	交换机、路由器、防火墙等传统网络设备，用于各节点量子设备之间的通信和互联
中继站	QKD 设备、KM 密钥管理器	
接入站	QKD 设备、KM 密钥管理器、光量子交换机 KM	
用户站	KMT 密钥管理终端（QKD 与 KM 合一设备）、加密路由器（用于业务加密）	

之间的互联。根据量子密钥分发控制流/业务流，管理流等不同的需求，划分为多个VPN，各种业务之间实现隔离和独立承载，同时在各站点的出口均配置了防火墙、IPS等设备，提升量子城域网的安全性。

4.2 量子城域网设备标识规范

量子城域网中的设备采用统一的编码规则进行管理，用ID作为号标识设备，ID为9位十进制数字，量子网络设备ID规范如图9所示。

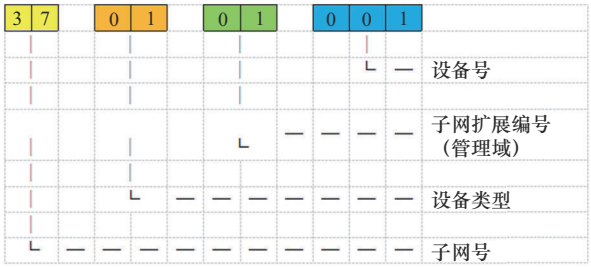

图9 量子网络设备ID规范

- 子网号（第1、2位）：用于标识设备所属的量子密钥分发网络，如上海城域网。该编号在全国范围内唯一，因此可实现不同网络之间的对接。
- 设备类型号（第3、4位）：用于标识设备的类型，例如，QKD设备的编码为01、光交换机的编码为02、KM设备的编码为04、量子密钥应用终端设备的编码为09。
- 子网扩展号（第5、6位）：用于进一步细分当前密钥分发网络内的不同管理域，每个管理域由独立的网络控制核心服务器进行管理，而各管理域的控制核心则由更上级的QKD网络控制核心服务器统一管理。
- 设备编号（第7～9位）：在上述所有信息相同的情况下，用于区分具体的设备。

编号规范通过层次化的编码结构，不仅确保了网络设备的唯一性和管理的有序性，还能够有效支持复杂的网络拓扑结构和多层次的管理需求。通过明确区分不同子网和设备类型，该规范能够促进量子密钥分发网络的扩展性和灵活性。此外，子网扩展号的设计为未来网络的进一步细化管理提供了可能，使得网络能够适应不同规模和复杂度的应用场景。这种规范化的设备ID管理方式，有助于提高网络的可维护性和可扩展性，确保量子通信网络的高效运行和安全管理。

4.3 密钥分发的路由组织

量子密钥分发路由是QKD网络的关键，设备ID既作为设备标识，又作为QKD网络地址。QKD密钥分发采用的是集中控制模式，QKD设备入网后，KM设备以及QKD设备都会向KMS注册自身的信息，KMS通过计算后可得到整网的拓扑信息，并将密钥转发路径信息告知KM，KM可向目标ID进行密钥发送或中继传递。这与传统IP网络基于目标地址和下一跳的路由机制类似，路由设计直接影响了网络的稳定性、扩展性和整体安全性。

在密钥分发中，存在如下3类路由。

- 一级路由：一级路由存在于两个具有量子QKD链路直连的站点之间。一级路由实现的是逐跳转发，如A-B-C-D，传递的密钥在通过逐跳转发方式从源到达目的，中间经过的中继站不断完成密钥的加解密中继，可类比于IP网络的逐跳转发。
- 二级路由：QKD密钥传输过程中的中间节点数量较多时，如果采用逐跳转发的中继方式，需要经过的节点数量较多。特别是在长途干线中，密钥中继需要通过大量可信中继节点，开销大，时延长。为了降低密钥传输时延，可启动密钥预存机制，KM可与其他非直连KM预协商并存储一部分密钥。这种密钥预

存策略能够实现非QKD直连的站点之间直接进行密钥传递，显著减少逐跳密钥传递的延迟。远距离密钥分发请求时，源KM可以直接利用已经预协商存储的密钥与目标KM进行密钥传递（需要保证源KM与目标KM IP可达），也可类比于IP网络中的隧道或虚拟连接virtual link。量子城域网L1和L2路由如图10所示。

- 三级路由：跨网络密钥分发的扩展。针对跨QKD网络（如城域网与骨干网对接）的密钥分发请求，三级路由机制提供了更为复杂和灵活的解决方案。三级路由在支持跨网络、跨区域的密钥分发中起到了关键作用，进一步扩展了QKD网络的应用范围，可类比于IP网络中BGP外部网关协议。

4.4　量子城域网的业务应用

QKD技术的不断发展，为各行业带来了新的安全保障方式。量子城域网作为QKD技术的大规模落地应用基础设施，其发展前景十分广阔。以下是针对不同行业和应用场景的7个方向展望。

- 政务行业的量子安全应用传输网络：面向政务行业用户，量子城域网可以构建覆盖整个区域的量子安全应用传输网络，提升政务系统的安全等级。通过量子密钥加密的应用，确保政务数据在传输过程中的高度安全，防止信息泄露和篡改，为政务数据安全提供坚实的保障。
- 高校和科研网络的量子安全传输：针对高校专网及科研平台的数据加密需求，量子城域网能够覆盖整个科研网络，提供量子安全传输保障。量子密钥分发技术为科研信息系统中的数据传输提供了高安全性，确保科研数据在传输过程中的机密性和完整性，尤其适用于涉及国家安全的科研项目。
- 信息系统加密保护：对于信息系统和平台数据的加密保护，量子密钥支撑体系的建立可以显著提升其安全性。将量子密钥引入现有的信息系统加密机制中，能够有效防止传统加密手段易受量子计算攻击的威胁，为信息系统的长期安全

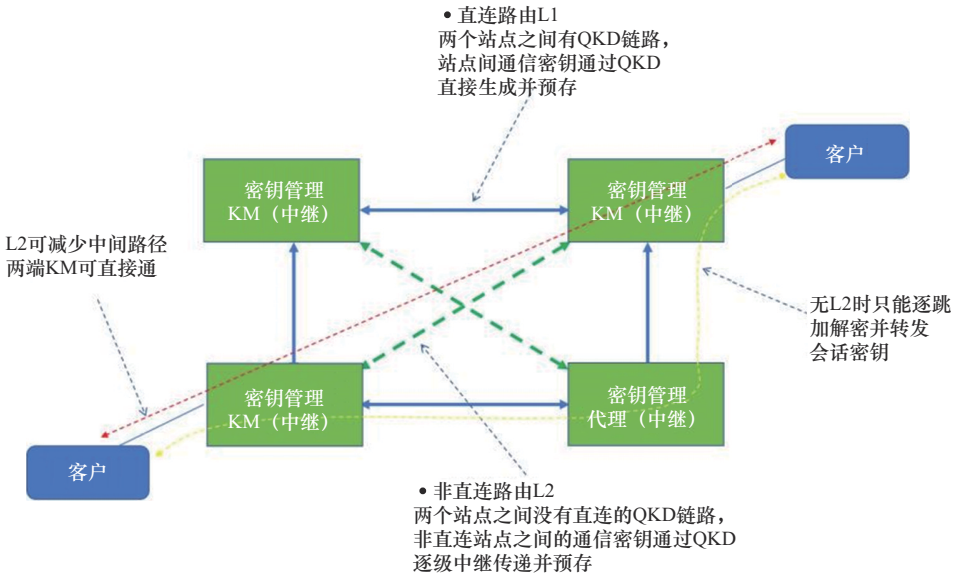

图10　量子城域网L1和L2路由

运行提供保障。

- 5G物联网安全解决方案：针对5G定向物联网卡用户，量子城域网能够提供更加安全的物联网解决方案。量子加密技术的引入能够确保物联网设备之间的数据传输安全，尤其适用于那些具有高安全性需求的物联网场景，如智能交通、智能电网和医疗设备等领域。
- 视频监控数据的安全传输：在视频监控数据传输方面，量子加密技术能够有效增强数据传输的安全性。量子城域网可以结合视频监控系统，通过量子密钥对视频数据进行加密，防止监控数据在传输过程中的泄露和篡改，提升视频监控系统的整体安全水平。
- SD-WAN加密传输需求：将量子加密技术应用于软件定义广域网（SD-WAN）场景，可以满足SD-WAN用户对于加密隧道传输的高安全性需求。量子城域网能够为SD-WAN用户提供基于量子密钥的加密解决方案，确保数据在不同网络节点之间传输时的安全性和可靠性。
- 高安全专线的量子+国密加解密能力：针对政务、公检法、企业等行业用户的高安全专线需求，量子城域网可以提供基于量子技术与国密算法结合的光传送网（OTN）端到端加/解密能力。该解决方案将量子加密与国家标准的加密算法结合，为高安全专线传输提供了双重保障，满足行业用户对数据传输安全性的极高要求。

量子城域网将在多行业和多场景中展现出巨大的应用潜力，进一步提升网络安全和数据传输的保密性，为未来信息化社会的安全保障体系提供重要支撑。

5 结束语

量子密钥分发网络因其无条件安全的特性正逐步被各行各业认可。上海量子城域网作为全球首个运营商建设的城市级量子密钥分发网络，可为政府、金融、医疗、教育等行业提供高质量的密钥分发服务，还可以结合电信IP城域网/广域网、OTN等传统通信基础设施提供安全通信服务，将在保护国家信息安全和企业信息安全方面发挥更大的作用。

参考文献：

[1] ITU-T. Recommendation Y.3804 quantum key distribution networks – control and management[EB]. 2020.

[2] ITU-T. Recommendation Y.3803 quantum key distribution networks – key management[EB]. 2020.

[3] 中华人民共和国工业和信息化部. 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.

[4] HU L Y, AL-AMRI M, LIAO Z Y, et al. Continuous-variable quantum key distribution with non-Gaussian operations[J]. Physical Review A, 2020, 102(1): 012608.

[5] 中华人民共和国工业和信息化部. 基于IPSec协议的量子保密通信应用设备技术规范: YD/T 4303-2023[S]. 2023.

[作者简介]

胡晓宇（1975– ），男，中国电信上海公司政企客户支撑响应中心高级工程师，主要研究方向为开源云计算、IP网络、量子保密通信等。

李天泽（2001– ），男，中国电信上海公司政企客户支撑响应中心工程师，主要研究方向为量子保密通信、IP网络、SD-WAN等。