ICS 33.180
CCS M 33

YD

中华人民共和国通信行业标准

YD/T XXXX—XXXX

量子保密通信网络架构

Quantum secure communication network architecture

（报批稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国工业和信息化部　　发布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：国科量子通信网络有限公司、中国信息通信研究院、科大国盾量子技术股份有限公司、中国移动通信集团有限公司、中国电信集团有限公司、中兴通讯股份有限公司、中国电子科技网络信息安全有限公司、北京邮电大学、安徽问天量子科技股份有限公司、华为技术有限公司、浙江九州量子信息技术股份有限公司、中国信息通信科技集团有限公司、北京科技大学。

本文件主要起草人：马彰超、李明翰、赖俊森、赵梅生、高有军、程明、古渊、徐兵杰、赵永利、刘婧婧、李政宇、封连重、钱懿、孙雷。

量子保密通信网络架构

1 范围

本文件规定了基于量子密钥分发（QKD）的量子保密通信网络功能架构，包括网络功能架构模型、网元及其功能模块、参考点、网络配置模型、基本业务流程等。

本文件适用于基于QKD的量子保密通信网络的设计、部署和运营。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

经典信道 classical channel

传输经典信号的信道。

3.2

密钥管理代理 key management agent；KMA

量子密钥分发（QKD）节点的密钥管理器中用于管理一个或多个QKD模组所生成密钥的功能单元。

注：密钥管理代理可从一个或多个QKD模组获取密钥，并对其进行密钥同步、长度调整、格式编排和存储，还负责通过密钥管理代理间的链路进行密钥中继。

3.3

密钥管理器 key manager；KM

量子密钥分发（QKD）节点中用于实现密钥管理层的密钥管理功能的网元。

3.4

密钥管理链路 key manager link

密钥管理器（KM）之间进行互联的通信链路。

3.5

密钥提供代理 key supply agent；KSA

量子密钥分发（QKD）节点的密钥管理器（KM）中用于负责向密码应用按需输出密钥的功能单元。

注：密钥提供代理（KSA）集成了面向密码应用的可编程应用接口（API）。在将密钥提供给密码应用之前，KSA会通过KSA间的交互链路进行密钥同步并验证其完整性。

3.6

量子密钥分发-密钥 QKD-key

由一对量子密钥分发（QKD）模块生成的对称随机比特序列，该序列可由QKD模组输出到密钥管理器中进行长度调整和格式编排。

3.7

保密增强 privacy amplification

通信双方根据 QKD 安全理论方案计算获得的安全成码率，将纠错后密钥进行压缩得到安全的最终密钥，从而将窃听者可能获得的信息量减少至安全阈值以下，也称隐私放大、密性增强。

3.8

量子信道 quantum channel

用于传输量子信号的通信信道。

3.9

量子密钥分发 quantum key distribution

通信双方通过传送量子态的方法实现信息理论安全的密钥分发过程，任何窃听行为都会因扰动量子态而被及时发现。

3.10

量子密钥分发链路 quantum key distribution link

两个量子密钥分发（QKD）模块之间的通信链路。

注：QKD链接包括用于传输量子信号的量子信道和用于传输QKD链路同步和密钥提取所需经典信号的经典信道。

3.11

量子密钥分发模组 quantum key distribution module

用于实现量子密钥分发（QKD）所需的量子光学过程（包括QKD协议、同步、密钥提取等）和密码学功能的软硬件系统。

注：QKD模组作为直接生成密钥的端点模块，可通过QKD链路进行互联。两种典型的QKD模组分别是QKD发送机（QKD-Tx）和QKD接收机（QKD-Rx）。

3.12

量子密钥分发网络 quantum key distribution network（QKDN）

由多个量子密钥分发（QKD）节点通过QKD链路连接组成的网络。

注：当QKDN中的两个QKD节点无法通过QKD链路直接相连时，可通过QKDN的密钥中继功能实现密钥分发。

3.13

量子密钥分发网络控制器 quantum key distribution network controller

量子密钥分发（QKD）网络控制层中用于实现QKD网络控制功能的网元。

3.14

量子密钥分发网络管理器 quantum key distribution network manager

量子密钥分发（QKD）网络管理层中用于实现QKD网络管理功能的网元。

3.15

量子密钥分发节点 quantum key distribution node

由一个或多个量子密钥分发（QKD）模组组成的节点，可防止未经授权的第三方侵入和攻击。

3.16

量子保密通信 quantum secure communication

结合量子密钥分发和对称密码技术的安全通信。。

3.17

量子保密通信网络 quantum secure communication network

利用量子密钥分发技术实现密钥分发，结合对称密码技术保护信息安全的通信网络。

3.18

用户网络 user network

用户利用量子密钥分发（QKD）网络提供的密钥来实现密码应用及其信息交互的网络。

4 缩略语

下列缩略语适用于本文件。

AES 高级加密标准（Advanced Encryption Standard）

API 可编程应用接口（Application Programming Interface）

FCAPS 故障、配置、计费、性能和安全性（Fault, Configuration, Accounting, Performance and Security）

HMAC 带密钥的杂凑算法（keyed-Hash Message Authentication Code）

ID 标识（Identifier）

IPsec 互联网安全协议（Internet Protocol Security）

IT-secure 信息理论安全（Information-Theoretically secure）

KM 密钥管理器（Key Manager）

KMA 密钥管理代理（Key Management Agent）

KSA 密钥提供代理（Key Supply Agent）

MDI 测量设备无关（Measurement Device Independent）

OTP 一次性密码本（One-Time Pad）

PQC 后量子密码学（Post-Quantum Cryptography）

QAN 量子密钥分发接入网（QKD Access Network）

QBN 量子密钥分发骨干网（QKD Backbone Network）

QKD 量子密钥分发（Quantum Key Distribution）

QKDN 量子密钥分发网络（QKD Network）

QKD-Rx 量子密钥分发接收机（QKD Receiver）

QKD-Tx 量子密钥分发发送机（QKD Transmitter）

QoS 服务质量（Quality of Service）

RNG 随机数发生器（Random Number Generation）

SPD 单光子探测器（Single Photon Detector）
TF 双场（Twin Field）
TLS 传输层安全协议（Transport Layer Security）

5 量子保密通信网络功能架构模型

量子保密通信网络由提供密钥分发能力的QKD网络和利用QKD网络分发的密钥实现密码应用的用户网络组成。QKD网络组网方案及其与用户网络的关系见附录A。

一种通用的量子保密通信网络功能架构模型如图 1所示。该模型主要包括：

——量子保密通信网络分层结构，包括：QKD网络部分的量子层、密钥管理层、QKDN控制层、QKDN网管层；用户网络部分的应用层、用户网络网管层。

——量子保密通信网络网元和链路，包括：QKD网络中的QKD模组、密钥管理器（KM）、QKDN 控制器和QKDN网管系统，以及QKD模块间的QKD链路、KM间的KM链路；用户网络中的密码应用、用户网络网管系统。

——量子保密通信网络功能模块，即包含在网元及链路内部的各功能模块。

各网元及功能模块之间交互信息的接口参考点。

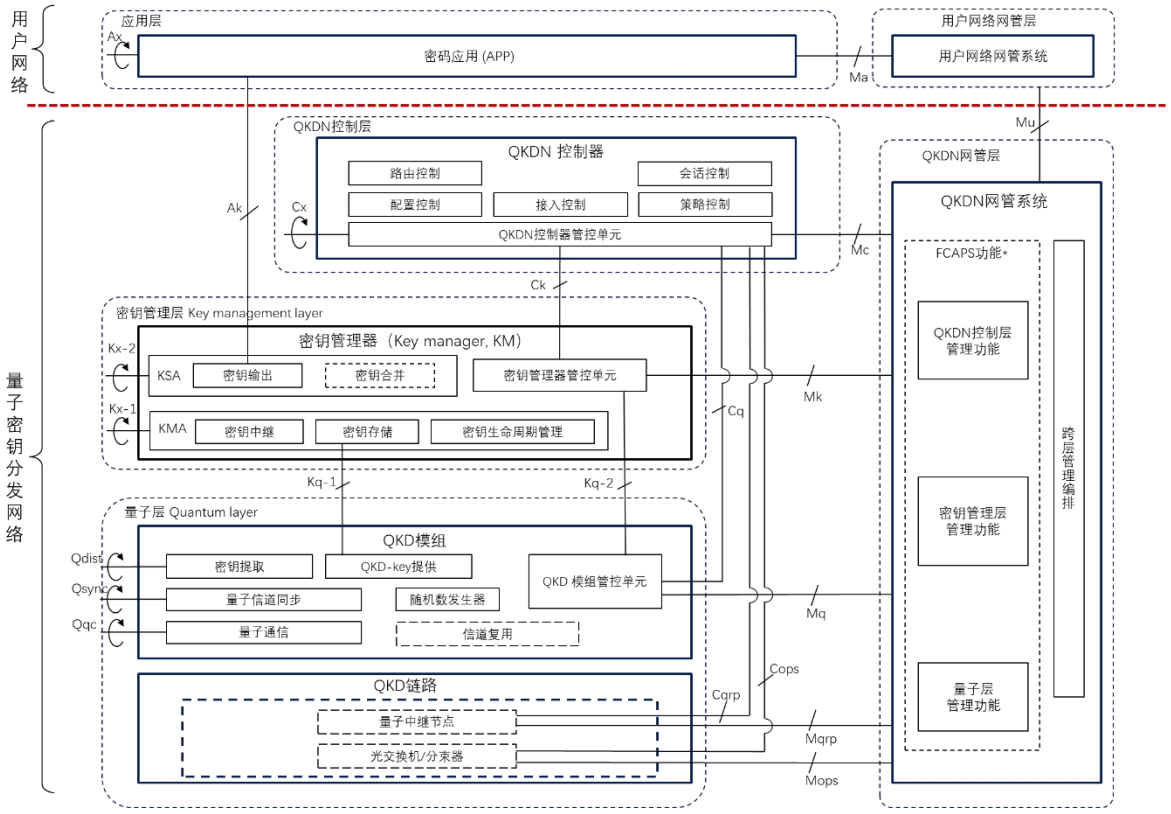

图 1 量子保密通信网络功能架构模型

6 量子保密通信网络网元

6.1 量子层网元及其功能模块

在量子层中，通常由一对 QKD 模组通过 QKD 链接连接，执行 QKD 协议来生成 QKD 密钥（QKD-key）。

根据 QKD 协议的不同，QKD 模组的角色有所区别。例如，对于基于“制备-测量”方案的 QKD 协议，QKD 模组包括发送端和接收端。对于基于测量辅助方案的 QKD 协议（例如 MDI-QKD 和 TF-QKD），QKD 模组则仅扮演发送器角色，接收器由 QKD 链路中的中间节点负责。在基于纠缠的 QKD 协议中，QKD 模组则仅用作接收器，而产生纠缠量子信号的发送器由 QKD 链路中的中间节点负责。

QKD 模组通常由以下功能模块组成：

a) 量子通信功能：负责制备、发送、传输和探测量子信号。

b) 量子信道同步功能：负责为量子信道提供高精度（皮秒级）的时间同步功能，以支持量子信号的发送和检测。

c) 密钥提取功能：通常执行以下经典数据处理过程，包括：

1) 进行基矢比对以匹配 QKD 模组调制和/或检测量子信号时所使用的基矢；

2) 进行参数估计以判断 QKD 信道是否安全，并为纠错和保密增强设置参数；

3) 进行纠错和保密增强，以在 QKD 模组之间生成对称且安全的密钥。

d) QKD-key 输出功能：根据 KM 请求生成 QKD-key 并安全地提供给 KM。

e) 随机数生成（RNG）功能：负责生成随机数并提供给量子通信功能和密钥提取功能模块使用。

f) QKD 模组管控单元功能：负责 QKD 模组与 QKDN 中的 KM、QKDN 控制器和 QKDN 管理器的 I/O 通信。

g) 多路信道复用功能（可选）：用于实现 QKD 模组之间的多路量子信道、经典通道的波分复用。

QKD 链路除了提供用于量子信号和经典信号传输的信道之外，还可包括如下可选功能模块：

a) 光交换机/分束器功能：负责针对多对 QKD 模组间的通信信道进行光路切换或分路操作，为 QKDN 中的不同用户间的 QKD 链路提供光层路由。

b) 量子中继点功能：在 QKD 链路中部署的用于特定 QKD 协议处理的中间节点或量子中继器。

注：这里将MDI-QKD、TF-QKD协议的中间测量节点和量子中继器统称为量子中继点。

6.2 密钥管理层网元及其功能模块

在密钥管理层中，由 KM 负责接收和管理 QKD 模组生成的密钥，对密钥进行中继并将密钥提供给密码应用。 KM 由密钥管理代理（Key Management Agent，KMA）、密钥提供代理（Key Supply Agent，KSA）和 KM 管控单元等功能模块组成，具体介绍如下。

KMA 包括如下子功能模块：

a) 密钥存储功能：从 QKD 模组接收密钥、同步、鉴权、调整长度（组合或拆分）以及格式编排等，并存储经过处理的密钥和元数据（例如密钥 ID、密钥长度、密钥类型和生成时间）；

b) 密钥中继功能：利用 KMA 间的通信链路进行密钥的中继，以实现 QKDN 中端到端的密钥分发。对密钥进行中继时应采用具有信息理论安全性（ITS）的加密方式，建议使用一次性密码本（OTP）方案；

c) 密钥生命周期管理功能：负责 KM 中的密钥生命周期管理，包括从 KM 接收密钥到交付给应用程序使用的全过程，还可根据特定密钥管理策略，例如在密钥使用后或有效期终止情况下，对密钥执行销毁或归档操作。

KSA 包括如下子功能模块：

a) 密钥提供功能：通信两端的 KSA 利用 KSA 间的通信链路对双方共享的密钥对进行同步和认证，并按需将密钥提供给密码应用程序；

b) 密钥组合功能：用于将 QKD 生成的密钥和通过其他密钥交换方法（例如 PQC）生成的密钥进行组合，以获得多重安全保障。

KM 管控单元功能负责实现 KM 与 QKD 模组、QKDN 控制器以及 QKDN 管理器等网元的连接。

6.3 QKDN 控制层网元及其功能模块

在 QKDN 控制层，QKDN 控制器负责控制 QKD 网络的各种资源，以确保 QKD 网络安全、稳定、高效、鲁棒地运行。QKDN 控制器包含以下功能模块：

a) 会话控制功能：支持 KMA 实现密钥中继的会话过程控制，同时还支持 KSA 实现面向多种密码应用提供密钥的会话过程控制；
b) 路由控制功能：为 KM 之间提供合适的密钥中继路由，并根据量子层和/或密钥管理层的故障、性能和/或可用性状态，对密钥中继进行重路由选择，以确保密钥中继和密钥提供的连续性；
c) 配置控制功能：负责获取 QKD 模组和 QKD 链路、KM 和 KM 链路的配置以及状态信息，并对接收到的故障预警、诊断结果等进行响应和处理，对 QKD 链路和 KM 链路进行适应性的重配置；
d) 策略控制功能：负责基于特定的服务质量（QoS）管理和计费策略来控制 QKDN 网络资源；
e) 接入控制功能：负责实现针对 QKD 网络用户的身份鉴别、权限管理和访问控制。

6.4 QKDN 管理层网元及其功能模块

在 QKDN 管理层中，QKDN 网管系统负责整个 QKDN 的故障管理、配置管理、计费管理、性能管理和安全性管理（FCAPS），并支持与用户网络网管系统的对接。它包含以下功能模块：

a) 故障管理功能：负责监视、检测、诊断及修复 QKDN 发生的故障问题。在发生故障时，还可向 QKDN 控制器提供支持，以根据需要对密钥中继路径进行路由选择和重路由控制；
b) 配置管理功能：负责管理 QKDN 资源的提供、配置和发现，以及 QKDN 拓扑结构的获取和管理。当 QKDN 支持密钥中继功能时，它也可协助 QKDN 控制器来提供密钥中继路由；
c) 计费管理功能：负责统计密钥提供服务的使用情况以及对计费系统提供支持；
d) 性能管理功能：负责监视和分析 QKDN 管理资源的性能状态。它还支持 QoS 保障、QoS 策略管理和 QKDN 性能信息的可视化展示；
e) 安全管理功能：负责从 QKDN 采集或接收与安全相关的管理信息，支持密钥生命周期管理，并管理 QKDN 中的身份鉴别、权限管理、访问控制等安全功能。

QKDN 网管系统将分别针对量子层、密钥管理层和 QKDN 控制层的需求执行基于 FCAPS 的管理功能，具体包括如下要求：

a) QKDN 控制层管理功能：QKDN 网管系统应为 QKDN 控制层中的网元及功能模块提供 FCAPS 管理功能。该功能还负责辅助 QKDN 控制器在发生故障和/或性能出现问题时控制密钥中继路由的提供和重选；
b) 密钥管理层管理功能：QKDN 网管系统应为密钥管理层中的网元及功能模块提供 FCAPS 管理功能，该功能还负责辅助 QKDN 控制器进行密钥生命周期管理；
c) 量子层管理功能：QKDN 网管系统应为量子层中的网元及功能模块提供 FCAPS 管理功能；
d) 跨层管理编排功能：QKDN 网管系统应支持对 QKDN 控制层、密钥管理层和量子层的网元及功能模块的管理决策和执行进行统一的协调编排。该功能还负责与其他 QKDN 外部的网管功能（特别是用户网络网管系统）进行管理信息交互。

6.5 应用层网元及其功能模块

应用层主要包括密码应用功能，利用 QKDN 提供的共享密钥对，在通信两端进行基于 QKD 的各类安全通信应用。

6.6 用户网络网管系统及其功能模块

用户网络网管层主要包括用户网络网管系统，负责执行针对用户网络的 FCAPS 相关管理功能。

7 量子保密通信网络参考点

7.1 QKD 模组相关参考点

Qqc：通过 QKD 链路连接相邻两个量子通信功能模块的参考点，负责传输量子密钥分发协议中的量子信号；

Qsync：通过经典通信链路连接相邻两个量子信道同步功能模块的参考点，负责为量子信道提供高精度的时间同步功能，以支持量子信号的发送和检测；

Qdist：通过经典通信链路连接相邻两个密钥提取功能模块的参考点，负责执行密钥提取功能涉及的基矢匹配、参数估计、纠错和保密增强等操作所需要的参数和数据的传输。

7.2 KM 相关参考点

Kq-1：连接密钥管理层的KMA与量子层的QKD-key输出功能模块的参考点，负责传输QKD-key输出功能模块生成的密钥；

Kq-2：连接密钥管理层的KM管控单元与量子层的QKD模组管控单元的参考点，负责传输KM对QKD模组的各类管理与控制操作指令，同时接收由QKD模组返回的QKD链路、QKD模组参数及状态等信息；

Kx-1：连接两个KMA的参考点，负责传输KMA之间密钥中继、密钥同步、密钥认证、KMA相互身份认证等所需的操作指令、参数和数据；

Kx-2：连接两个KSA的参考点，负责传输KSA之间共享密钥认证、KSA相互身份认证等所需的操作指令、参数和数据；

Kx’：通过KM链路连接本地KM模块与集中式KM模块的参考点，负责传输集中式控制QKDN中集中式密钥中继所需的操作指令、参数和数据。

7.3 QKDN 控制器相关参考点

Ck：连接QKDN控制层的QKDN控制器管控单元模块与密钥管理层的KM管控单元模块的参考点，负责传输QKDN控制器与密钥管理层KMA、KSA之间交互的各类管控信息与数据；

Cq：连接QKDN控制层的QKDN控制器管控单元模块与量子层的QKD模组管控单元的参考点，负责传输QKDN控制器与QKD模组间交互的各类管控信息与数据；

Cops：连接QKDN控制层的QKDN控制器管控单元模块与量子层QKD链路中的光交换机/分束器功能模块的参考点，负责传输QKDN控制器与光交换机/分束器功能模块间交互的各类管控信息与数据；

Cqrp：连接QKDN控制层的QKDN控制器管控单元模块与量子层QKD链路中的量子中继点功能模块的参考点，负责传输QKDN控制器与中继节点功能模块间交互的各类管控信息与数据；

Cx：连接不同的QKDN控制器管控单元模块的参考点，负责QKDN控制器间控制信息和指令等数据的交互。

7.4 QKDN 网管系统相关参考点

Mk：连接QKDN网管系统与KM管控单元模块的参考点，负责传输QKDN网管系统与密钥管理层的KMA、KSA间交互的各类网管信息与数据；

Mq：连接QKDN网管系统与QKD模组管控单元的参考点，负责传输QKDN网管系统与QKD模组间交互的各类网管信息与数据；

Mops：连接QKDN网管系统与QKD链路中的光交换机/分束器功能模块的参考点，负责传输QKDN网管系统与光交换机/分束器功能模块间交互的各类网管信息与数据；

Mqrp：连接QKDN网管系统与QKD链路中的量子中继点功能模块的参考点，负责传输QKDN网管系统与量子中继点功能模块间交互的各类网管信息与数据；

Mc：连接QKDN网管系统与QKDN控制器管控单元模块的参考点，负责传输QKDN网管系统与QKDN控制器间交互的各类网管信息与数据；

Mu：连接QKDN网管系统与用户网络网管系统的参考点，负责传输QKDN网管系统与用户网络网管系统间交互的各类网管信息与数据；

7.5 密码应用相关参考点

Ak：连接密码应用与密钥管理层KSA的参考点，负责密码应用与KSA间的相互认证，以及KSA向密码应用提供密钥；

Ax：连接应用层通信双方的密码应用的参考点，负责基于特定的传输协议在密码应用间进行信息交互。

7.6 用户网络网管系统相关参考点

Ma：连接用户网络中的用户网管系统与密码应用层各类密码应用的参考点，负责传输用户网络网管系统与密码应用间交互的各类网管信息与数据。

8 量子密钥分发网络配置模型

8.1 概述

基于量子保密通信网络功能架构模型， QKDN 可根据应用场景需求灵活选择不同的网络配置模型，包括：分布式控制、集中式控制、多级节点集中式控制、集中式的控制和密钥中继等。

在不同的 QKDN 配置模型下，QKDN 由多种类型的网络节点构成。

这里的网络节点是由包含多种 QKDN 功能模块组合而成的逻辑实体，并不一定映射于特定的物理设备。

8.2 QKDN 配置模型 1：分布式控制

QKDN 配置模型 1 采用分布式的 QKDN 控制方案，如图 2 所示。在 QKDN 配置模型 1 中，QKDN 由 I 型 QKD 节点组成。I 型 QKD 节点包含完整的 QKD 模组、KM 和 QKDN 控制器功能。该类 QKDN 无需依赖于集中式的 QKDN 控制器，可通过分布式路由控制等功能实现分布式组网。

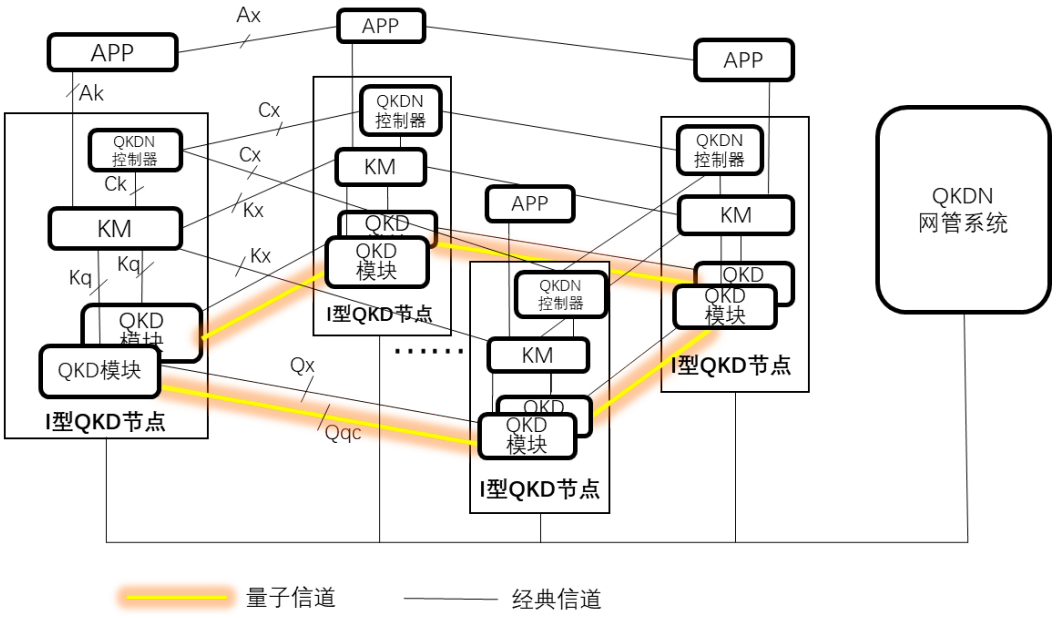

图 2 QKDN 配置 1：分布式控制

8.3 QKDN 配置模型 2：集中式控制

QKDN 配置模型 2 采用集中式的 QKDN 控制器方案，如图 3 所示。

在 QKDN 配置模型 2 中，QKDN 由 II 型 QKD 节点以及一个或多个集中式 QKDN 控制器节点组成。II 型 QKD 节点仅包含 QKD 模组和 KM 功能。QKD 网络中各 QKD 节点及 QKD 链路的路由控制、资源调度等功能由集中式部署的 QKDN 控制器进行统一优化控制。

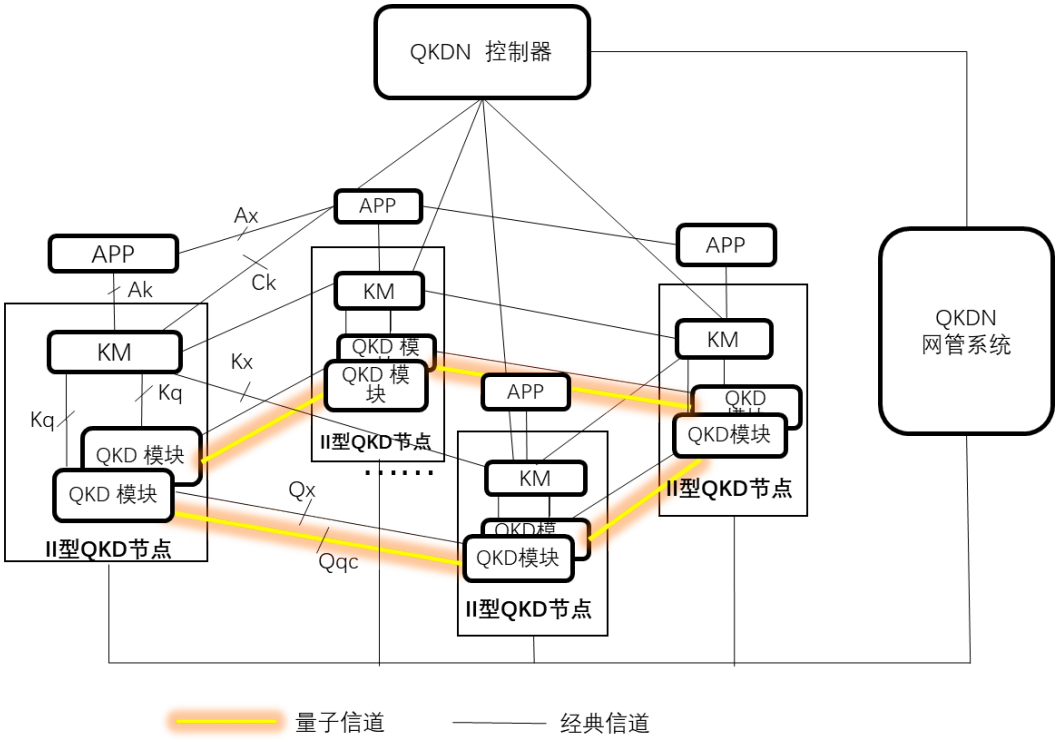

图 3 QKDN 配置 2：集中式控制

8.4 QKDN 配置模型 3：多级节点集中式控制

QKDN 配置模型 3 采用由多级 QKD 节点组成的集中式控制方案，如图 4 所示。在 QKDN 配置模型 3 中，II 型 QKD 节点根据角色的不同，可进一步分为 3 种类型：QKDN 用户节点、QKDN 接入节点和 QKDN 中继节点。

a) QKDN 用户节点。QKDN 用户节点是位于 QKD 用户侧的可信节点。它负责从 QKDN 获取密钥，并为特定的密码应用提供相应的密钥以进行保密通信。用户节点由 QKD 模组和 KM 组成。通常用户节点仅包含一个 QKD 发送机模块（QKD-Tx），以降低用户设备成本。用户节点的 KM 需实现密钥存储、密钥提供和密钥中继功能。

b) QKDN 接入节点。QKDN 接入节点是负责汇聚其连接的多个用户节点的密钥业务流，并基于可信中继方案将密钥业务流通过 OTP 通道转发到远端的 QKD 节点。用户节点可以直接与接入节点连接，或通过光交换机（Optical switch）来接入。通常接入节点包含功能强大的 QKD 接收机模块（QKD-Rx），可以同时处理来自多个用户的 QKD 信号，还可集成多用户调度功能，将信道资源在多个关联用户间进行动态分配。接入节点的 KM 需具备密钥存储和密钥中继功能。

c) QKDN 中继节点。QKDN 中继节点负责建立密钥中继路由，以实现远距离的密钥分发，突破点对点量子信道的距离限制。中继节点通常包含至少一对 QKD-Tx 和 QKD-Rx，以连接前后两跳 QKD 链路。中继节点的 KM 需具备密钥的存储和中继功能。

通过 QKD 用户节点、接入节点和中继节点的组合，可支持多种灵活的 QKDN 拓扑结构。例如，多个用户节点和接入节点可组成 QKD 接入网络（QAN），适用于城域网络覆盖；多个中继节点可组成 QKD 骨干网（QBN），通过连接多个 QAN 实现广域网络覆盖。

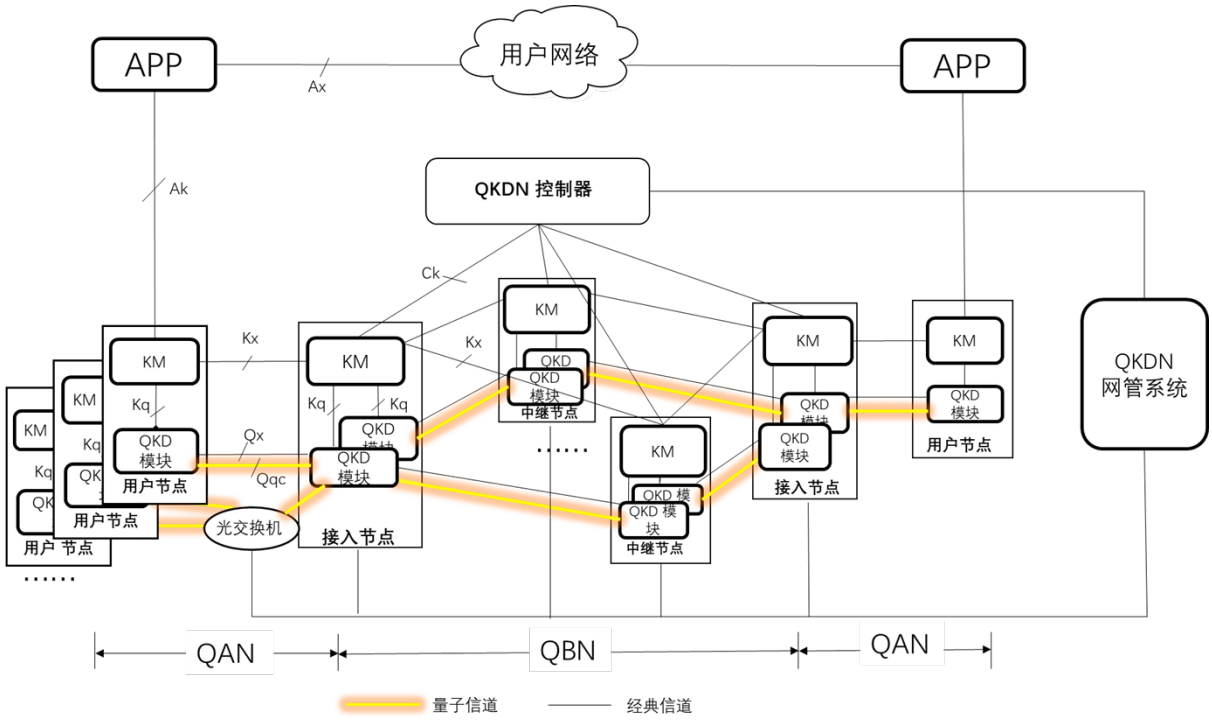

图 4 QKDN 配置 3：多级节点的集中式控制

8.5 QKDN 配置模型 4：集中式的控制和密钥中继

QKDN 配置模型 4 采用集中式的网络控制和集中式的密钥中继功能，如图 5 所示。该配置方案可降低 QKDN 中多个中继节点进行密钥中继时两两直接交互所需的连接管理及鉴权信令开销，简化 QKD 节点

功能并提高密钥中继效率。

在 QKDN 配置方案 4 中，QKDN 不仅将网络路由控制等控制器功能集中化，还将 KM 中的密钥中继功能进行集中化。KM 模块分为本地 KM 和集中式 KM 两部分，集中式 KM 可与 QKDN 控制器合设。QKD 节点之间无需进行密钥加密传输，而是将前后两跳 QKD 链路生成的密钥做异或处理后，发送至集中式 KM 进行集中运算，再交给目的用户端处理生成端到端密钥。

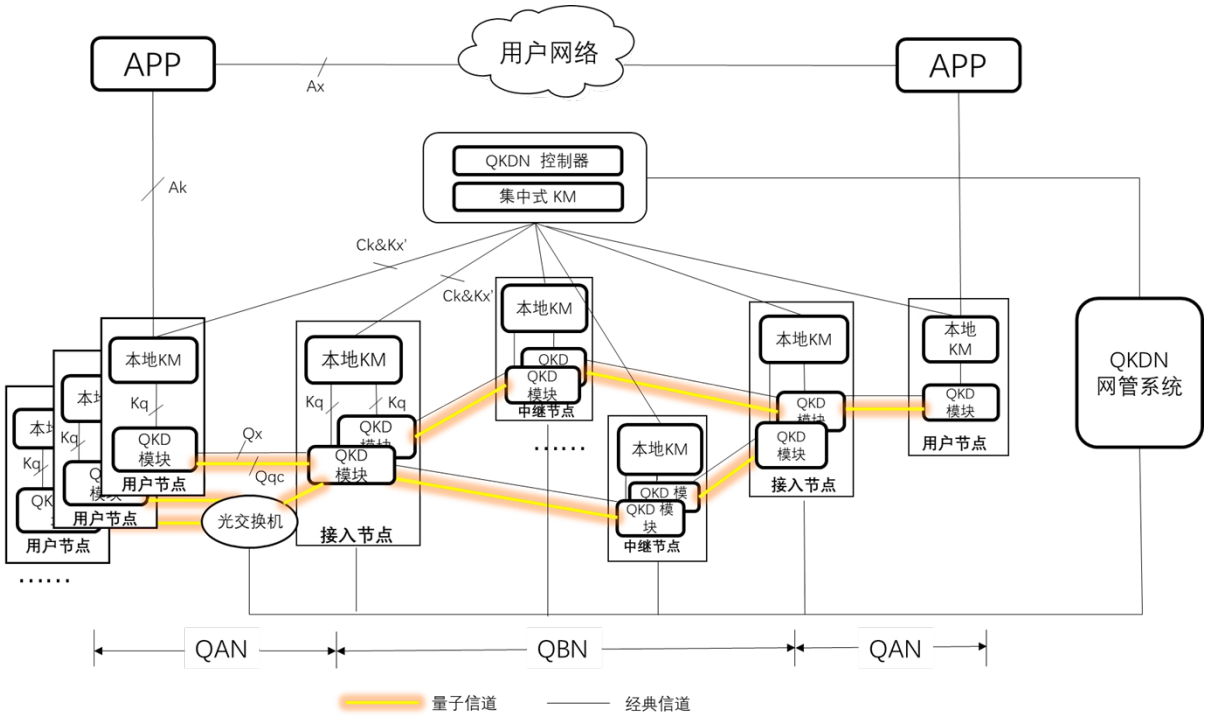

图 5 QKDN 配置模型 4：集中式的控制和密钥中继

9 量子保密通信网络基本业务流程

9.1 概述

基于所述量子保密通信网络功能架构模型，量子保密通信网络应支持的基本业务流程包括：系统初始化、密钥生成、密钥请求与提供、密钥中继、密钥中继重路由。

9.2 初始化功能流程

量子保密通信网络初始化的基本流程如图 6 所示，包含如下步骤：

a) 用户网络网管系统下发服务启动指令，并将密码应用的策略与配置信息等提供给 QKDN 网管系统；

b) QKDN 网管系统分别向 QKDN 控制器、密钥管理器 KM、QKD 模组下发初始化指令，并提供相应模块的初始配置。

注：上述步骤 a)为可选步骤，仅当用户网络负责 QKDN 网络功能启动时执行；当 QKDN 网管系统采取独立部署并负责 QKDN 网络功能启动时，仅需执行步骤 b)。

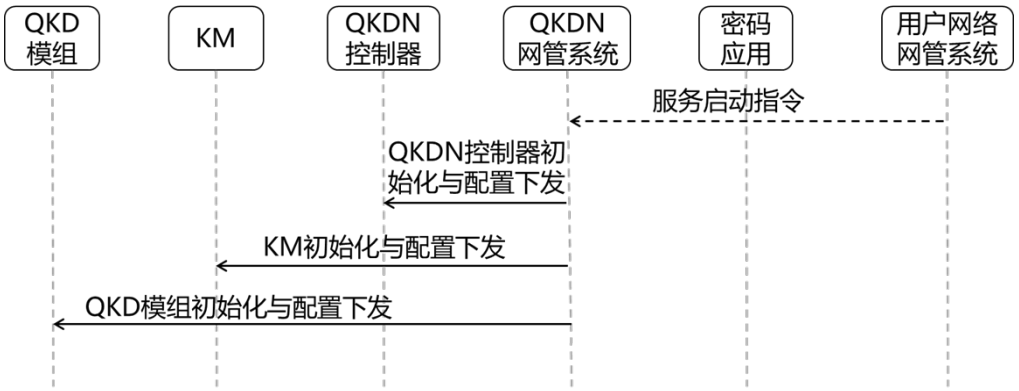

图 6 QKDN 系统初始化流程示意

9.3 密钥生成功能流程

密钥生成的基本流程如图 7 所示，包含如下步骤：

a) QKDN 控制器通知 QKD 链路启动光路连接，并通知对应的 QKD 模组准备启动密钥生成流程；

b) QKDN 控制器控制 QKD 模组，启动密钥生成流程；

c) QKD 模组执行 QKD 协议，制备、发送与接收量子信号，并完成量子信号的同步以及密钥提取等必要操作，生成密钥；

d) QKD 模组将生成的密钥与元数据推送到同一节点的 KM 模块；

e) KM 模块对接收到的量子密钥与元数据进行密钥同步、正确性检查、格式编排与存储；

f) KM 模块将密钥生成过程的状态信息反馈给 QKDN 控制器与 QKDN 网管系统；

g) 重复步骤 c)～f)，直到生成足量的密钥；

h) QKDN 网管系统向 QKDN 控制器发送必要的辅助信息；

i) QKDN 控制器向 KM 模块发送停止密钥生成的指令，停止生成密钥。

注 1：上述步骤 a)为可选步骤，当 QKD 链接以及 QKD 模组处于就位状态，且无需进行光路切换等操作时，可跳过步骤 1。

注 2：上述步骤 e)为可选步骤，当 KM 模块直接使用和存储 QKD 模组提供的密钥和元数据时，可跳过步骤 e)。

注 3：上述步骤 h)为可选步骤，例如 QKDN 网管系统可将正在执行密钥生成操作的两个节点的网管状态等信息提供给 QKDN 控制器，协助 QKDN 做出正确决策。

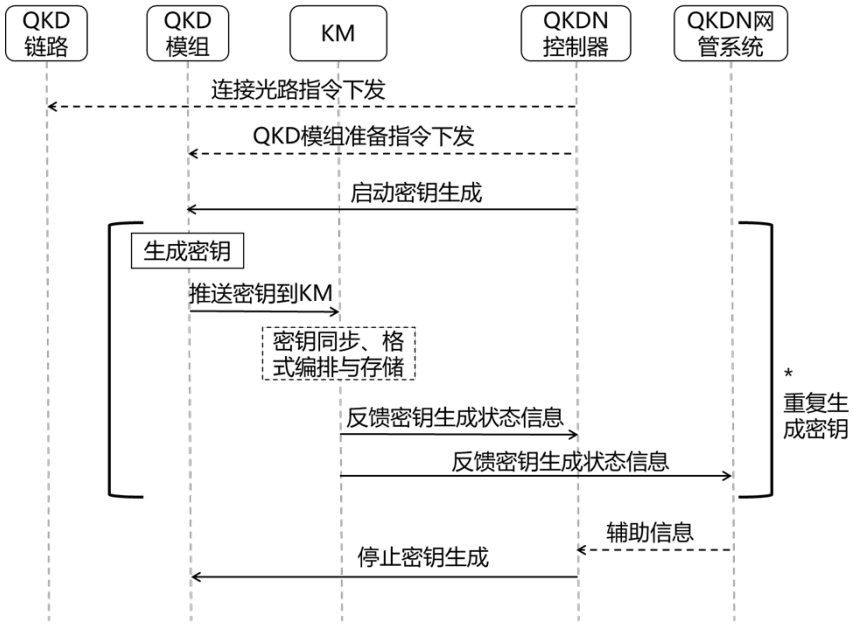

图 7 QKDN 密钥生成流程示意

9.4 密钥请求与提供功能流程

密钥请求与提供的基本流程如图 8 所示，包含如下步骤：

a) 密码应用向所属 KM 发起密钥请求。

b) KM 检查与密码应用请求所对应的对端 KM 之间当前共享的密钥量是否充足：

1) 如果当前密钥量充足，执行步骤 c)；

2) 如果当前密钥量不足，KM 向 QKDN 控制申请发起与对端 KM 的密钥生成流程，并按需进行密钥中继流程（例如，当两个 KM 不直接相邻时）；

c) KM 模块向密码应用提供所需的密钥。

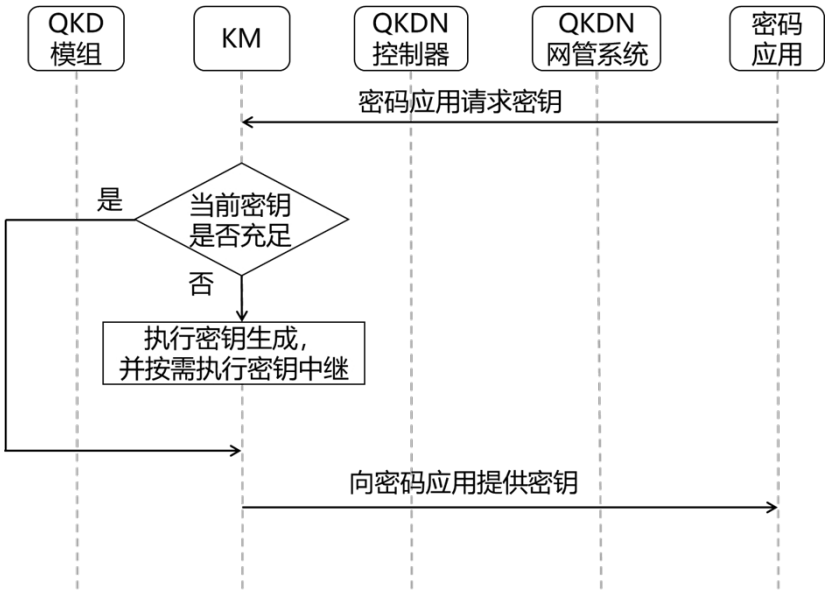

图 8 QKDN 密钥请求与提供流程示意

9.5 密钥中继功能流程

密钥中继的基本流程如图 9 所示，包含如下步骤：

a) KM 模块判断当前是否有可用的密钥中继路由：
   1) 存在可用路由，执行步骤 c)；
   2) 不存在可用路由，KM 向 QKDN 控制器申请密钥中继路由，执行步骤 b)；
b) QKDN 控制器接到申请，决定可用的密钥中继路由，并下发到对应的 KM 模块；
c) KM 根据密钥中继路由执行密钥中继功能。

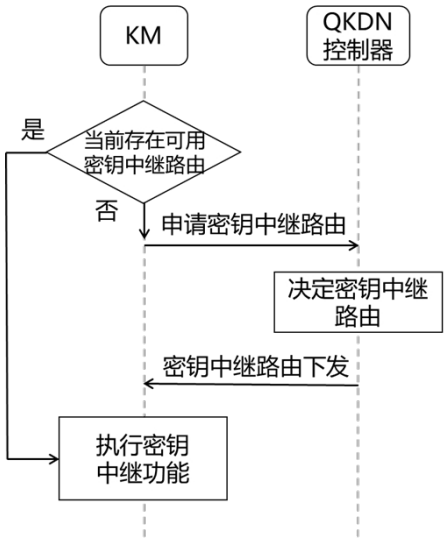

图 9 QKDN 密钥中继流程示意

9.6 密钥中继重路由功能流程

通过 QKDN 控制器进行密钥中继重路由控制的基本流程如图 10 所示，包含如下步骤：

a) QKD 模组将自身及其关联 QKD 链路的状态信息向 QKDN 控制器上报；
b) QKDN 控制器分析接收到的 QKD 链路与 QKD 模组的状态信息；
c) KM 向 QKDN 控制器上报管理密钥的相关信息；
d) QKDN 控制器分析接收到的 KM 管理密钥的相关信息；
e) QKDN 控制器向 QKDN 网管系统请求网络拓扑与相关辅助信息；
f) QKDN 网管系统向 QKDN 控制器返回网络拓扑与相关辅助信息；
g) QKDN 控制器根据步骤 a)～e)接收到的信息和分析结果，决定是否需要进行密钥中继重路由；
h) QKDN 控制器将路由更新信息下发到 KM 模块，并同步给 QKDN 网管系统
i) KM 根据新获得的密钥中继路由信息执行密钥中继功能。

注: QKDN 控制器可以周期性执行上述步骤 a)～e)，以更好地获知和更新 QKDN 网络、拓扑以及密钥管理等动态信息。

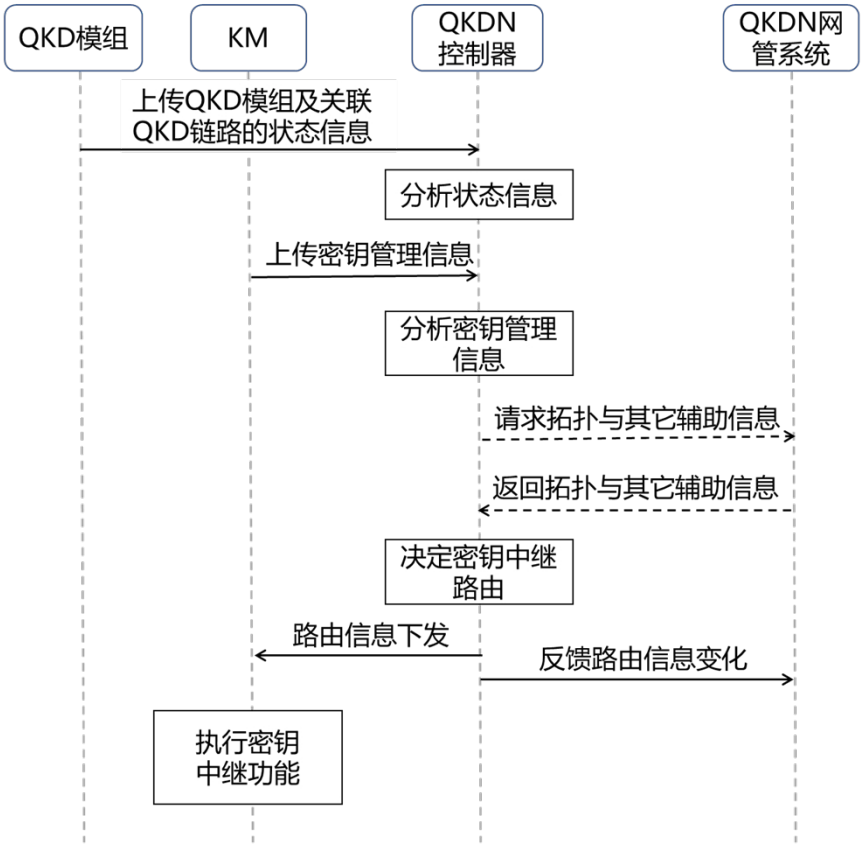

图 10 QKDN 密钥中继重路由控制流程示意

附 录 A
（资料性）
QKD 网络与用户网络的关系概述

QKD是一种点对点（P2P）密钥协商技术。通过点对点QKD链路相连的一对QKD模组可为应用发送端和接收端提供共享密钥对，用于加密通信等密码应用，如图A.1所示。

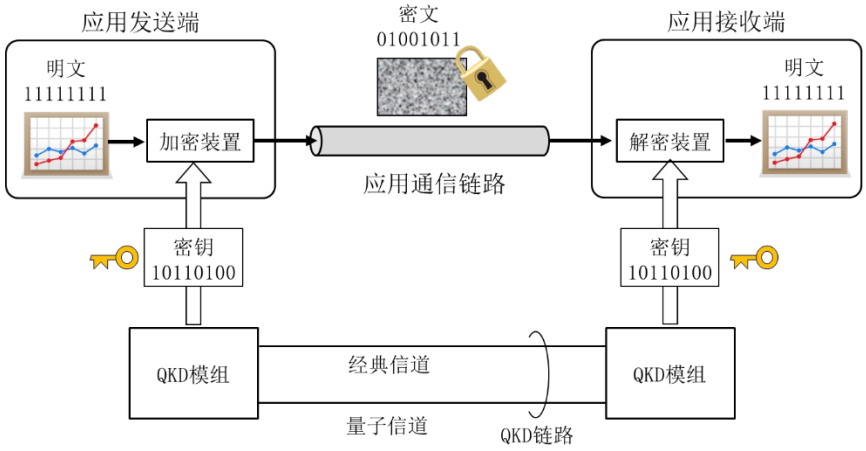

图 A.1 基于点对点 QKD 的量子保密通信示意图

通过QKD网络则可为连接网络的的任意两个或多个用户提供量子密钥生成和分发。将点对点QKD系统扩展为多用户的QKD网络，目前主要有如下方式：

a) **光交换/分束器方案：**该方案利用光路交换机或光分束器，在多对QKD模组之间实现QKD链路的（光层路由）切换或拆分，从而为不同用户采用一对多或多对多的方式按需生成QKD密钥。但由于量子信号衰减带来的传输距离限制，该方案只能用于小型网络，无法扩展QKD距离；

b) **可信中继方案：**该方案将点对点QKD链路生成的密钥存储在可信QKD节点中，并利用逐跳QKD链路生成的密钥建立基于一次性密码本（One-Time Pad，OTP）方案的信息理论安全加密传输通道（简称OTP通道）。进一步，将用户所需的端到端密钥，通过OTP通道加密传输至通信两端用户侧，以实现端到端的量子保密通信。该方案可有效扩展QKD网络的传输距离，是目前远距离QKD网络中广泛采用的解决方案。但其需假定QKD可信中继节点是受信任的安全节点，可防止任何未经授权方的入侵和攻击。

c) **测量辅助中继方案：**该方案需利用MDI-QKD、TF-QKD等需要中间节点测量的新型QKD协议，来扩展点对点QKD链路传输距离，从而允许在更长的距离或更高损耗的信道上生成密钥。该方案需在QKD链路中增加部署用于执行量子态测量操作的中继站，这些中继站无需是可信节点。

d) **量子中继方案：**该方案将QKD协议所需传递的量子态在网络中直接进行端到端的传输，以确保安全性。这需要实现将信息以量子态形式存储并转发的网络中间节点，即量子中继器。通常需要在通信链路沿线部署多个可进行量子纠缠分发的量子中继站，这些中继站同样无需是可信节点。该方案是实现远距离QKD的理想解决方案，但量子中继通常所需的量子存储器或量子纠错技术目前仍不成熟。

这里给出基于上述多种组网方案的QKD网络概念模型，以及QKD网络与用户网络之间的逻辑关系，如图A.2所示。

QKD网络通过可信或非可信的中继节点，可以在连接同一QKD网络的任意QKD节点之间进行密钥分发。QKD节点可作为密钥提供方输出密钥给密码应用，也可作为密钥的可信中继节点实现QKD距离的扩展。

QKD网络还可利用光路交换机、MDI-QKD或TF-QKD的中间测量节点、量子中继器，实现量子信号的中继传输。这里将MDI-QKD、TF-QKD的中间测量节点和量子中继器统称为量子中继点。

光路交换机和量子中继点仅作为量子信号的中继点，不涉及密钥的生成或分发，无需依赖于可信节点。这里可将光路交换机和量子中继点看作QKD链路的一部分，用于支持QKD网络实现更长的传输距离和灵活的拓扑结构。

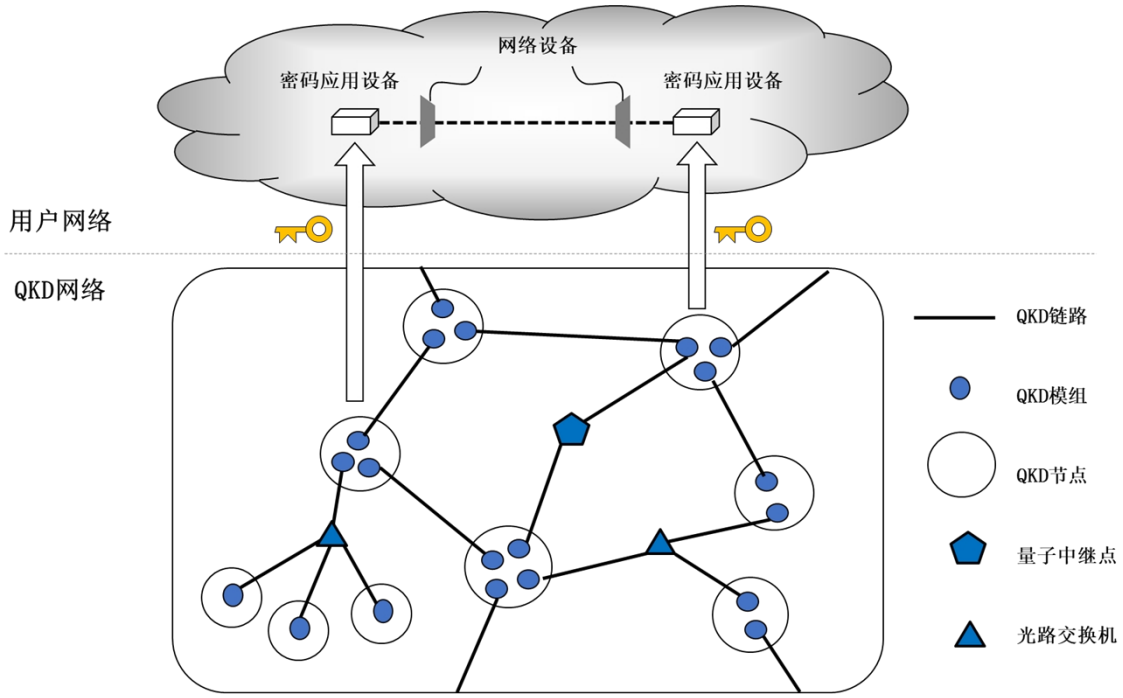

图 A.2 QKD 网络及其与用户网络的关系示意图

参 考 文 献

[1] GB/T 17901.1-1999 信息技术 安全技术 密钥管理 第1部分：框架

[2] GM/T 0051-2016 密码设备管理 对称密钥管理技术规范

[3] ISO/IEC 18031, Information technology — Security techniques — Random bit generation.

[4] ITU-T Y.3800 (2019), Overview on Networks Supporting Quantum Key Distribution.

[5] ITU-T Y.3802 (2020), Quantum key distribution networks – Functional architecture.

[6] ETSI/ISG QKD GS 002（2010）. Quantum Key Distribution; Use Cases.

[7] ETSI/ISG QKD GS 007 (2018) . Quantum Key Distribution (QKD); Vocabulary.