ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 42829—2023

量子保密通信应用基本要求

Basic requirements of quantum secure communication applications

2023-08-06 发布　　2024-03-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：国科量子通信网络有限公司、中国移动通信集团有限公司、中国电信集团有限公司、中国信息通信研究院、科大国盾量子技术股份有限公司、中兴通讯股份有限公司、安徽问天量子科技股份有限公司、中国信息通信科技集团有限公司、神州数码信息服务股份有限公司、数据通信科学技术研究所、新华三技术有限公司、中国通信建设集团设计院有限公司、中国联合网络通信有限公司、瑞斯康达科技发展股份有限公司、江苏亨通问天量子信息研究院有限公司、安徽皖通邮电股份有限公司、北京邮电大学、北京中创为量子通信技术有限公司。

本文件主要起草人：马彰超、冯刚、马冰珂、徐文华、赵文玉、赵勇、古渊、刘婧婧、冯勇华、黄强、李申、万晓兰、韩鹏、王海军、张金旗、赵良圆、黎定军、赵永利、尹华磊。

量子保密通信应用基本要求

1 范围

本文件描述了量子保密通信的基本概念和应用场景，规定了量子保密通信在安全性、可扩展性、高效性、鲁棒性、应用灵活性、互操作能力、技术兼容性、可管理性、差异化策略控制等方面的基本要求。

本文件适用于基于量子密钥分发技术的量子保密通信系统设计、开发与应用。

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

量子密钥分发 quantum key distribution

通信双方通过传送量子态的方式实现信息论安全(3.11)的密钥生成和分发的方法和过程。

注：量子密钥分发也称量子密钥分配、量子密钥协商。

3.2

量子保密通信 quantum secure communication

以量子密钥分发(3.1)作为密钥分发功能组件，结合适当的密钥管理、密码算法和协议而形成的保密通信解决方案。

3.3

量子密钥分发模组 quantum key distribution module

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

注：量子密钥分发模组作为直接生成密钥的端点模块，可通过量子密钥分发链路互联。两种典型的量子密钥分发模组分别是量子密钥分发发送机和量子密钥分发接收机。

3.4

量子密钥分发网络 quantum key distribution network

由多个量子密钥分发节点通过量子密钥分发链路连接组成的网络。

注：当量子密钥分发网络中的两个量子密钥分发节点无法通过量子密钥分发链路直接相连时，通过量子密钥分发网络的密钥中继功能实现密钥分发。

3.5

可信中继 trusted relay

采用一个可信任的中继节点，该节点的设备和存储不会被非法方控制和侵入，与另外两个或多个合法通信节点连接并分别通过量子密钥分发(3.1)实现所连节点之间的密钥共享，从而拓展量子密钥分发(3.1)安全成码距离和范围的一种技术。

3.6

量子中继　quantum repeater

采用分段的量子纠缠分发、量子纠缠交换与量子纠缠纯化相结合的方式来实现远距离的量子纠缠分发，可用于拓展量子密钥分发(3.1)安全成码距离和范围。

注：相比可信中继(3.5)技术，量子中继技术不要求中继节点可信。

3.7

量子信号　quantum signal

量子通信中以量子态承载信息的物理信号，也即是量子信息的物理载体。

注：常用的量子信号如，对偏振、相位和轨道角动量等物理量编码/调制的单光子，对相位和振幅编码/调制的弱相干态光等。

3.8

经典信号　classical signal

现代通信技术中以经典物理量承载信息的物理信号。

注：常用的经典信号如，高电平、低电平、亮光脉冲、暗光脉冲、不同偏振状态的光脉冲和不同相位差的光脉冲等。

3.9

量子信道　quantum channel

传输量子信号(3.7)的信道。

3.10

经典信道　classical channel

传输经典信号(3.8)的信道。

3.11

信息论安全　information-theoretic security

一种以信息论为理论基础的密码系统安全性，要求即使窃密者拥有无限的计算能力，也无法破解该密码系统。

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)

ECP：加密控制协议(Encryption Control Protocol)

IC：集成电路(Integrated Circuit)

IKE：互联网密钥交换(Internet Key Exchange)

IPSec：互联网安全协议(Internet Protocol Security)

LAN：局域网(Local Area Network)

MACsec：媒体访问控制安全(Media Access Control Security)

MDI：测量设备无关(Measurement Device Independent)

OLT：光线路终端(Optical Line Terminal)

ONU：光网络单元(Optical Network Unit)

OTN：光传输网络(Optical Transport Network)

OTP：一次性密码本(One Time Pad)

PPP：点对点协议(Point to Point Protocol)

QKD：量子密钥分发(Quantum Key Distribution)

QKDN:量子密钥分发网络(Quantum Key Distribution Network)
SCADA:数据采集与监控系统(Supervisory Control And Data Acquisition)
SIM:用户身份识别模块(Subscribe Identity Module)
SSL:安全套接层(Secure Sockets Layer)
TF:双场(Twin Field)
TLS:传输层安全(Transport Layer Security)
VPN:虚拟专用网络(Virtual Private Network)
WDM:波分复用(Wavelength Division Multiplexing)

5 概述

量子保密通信是利用 QKD 与其他密码技术结合形成的保密通信技术。QKD 作为量子通信的一种典型应用,通过传送量子态的方式实现密钥的生成和分发。通信双方通过 QKD 分发密钥时,任何窃密行为都会因扰动量子态而被及时发现。

QKD 作为密码学中的密钥分发组件,可与多种加密、鉴别技术结合,以形成不同安全要求的量子保密通信方案,例如:

a) QKD 与同样具备可证明信息论安全性的加密方案(例如 OTP 算法)和鉴别方案(例如全域哈希算法)相结合,可实现具备信息论安全性的量子保密通信系统;
b) QKD 与能够抵抗量子计算攻击的加密方案和鉴别方案相结合,可实现能够抗量子计算攻击的量子保密通信系统。

量子保密通信通常由提供密钥分发能力的 QKD 系统和利用 QKD 生成的对称密钥实现密码应用的用户系统两部分组成。

基本的 QKD 系统通常由一对通过量子信道和经典信道连接的 QKD 模组组成,可在点对点链路上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。基于点对点 QKD 系统的量子保密通信典型应用见图 1。

通过 QKD 组网技术可将点对点 QKD 系统扩展为多用户的 QKDN,为连接网络的任意两个或多个用户提供量子密钥生成和分发功能。QKDN 的具体组网方案见附录 A。

基于 QKDN 的量子保密通信典型应用见图 2。用户网络中的应用发送端和接收端可利用 QKDN 中的 QKD 节点提供的对称密钥对实现加密通信等密码应用。QKD 节点可作为密钥提供方输出密钥给密码应用,也可作为可信中继节点实现基于 OTP 的密钥中继转发。QKDN 还可利用光路交换机、MDI-QKD 或 TF-QKD 的中间测量节点、量子中继站,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。

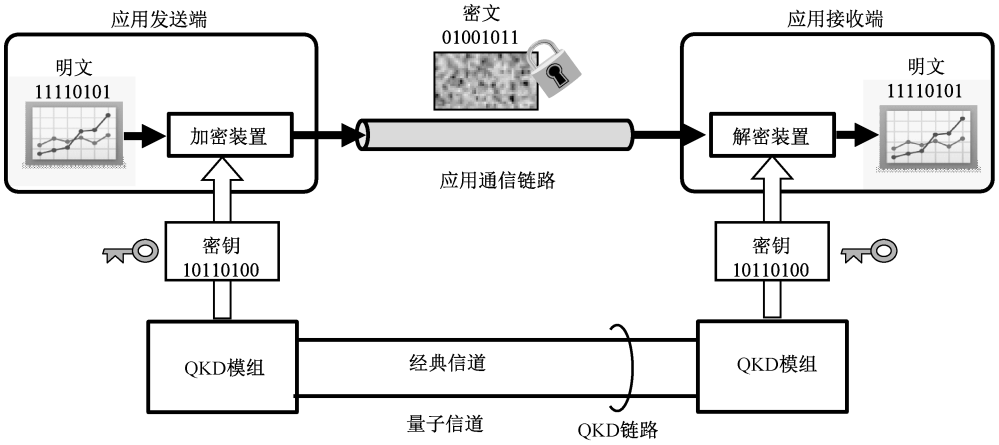

图 1　基于点对点 QKD 系统的量子保密通信

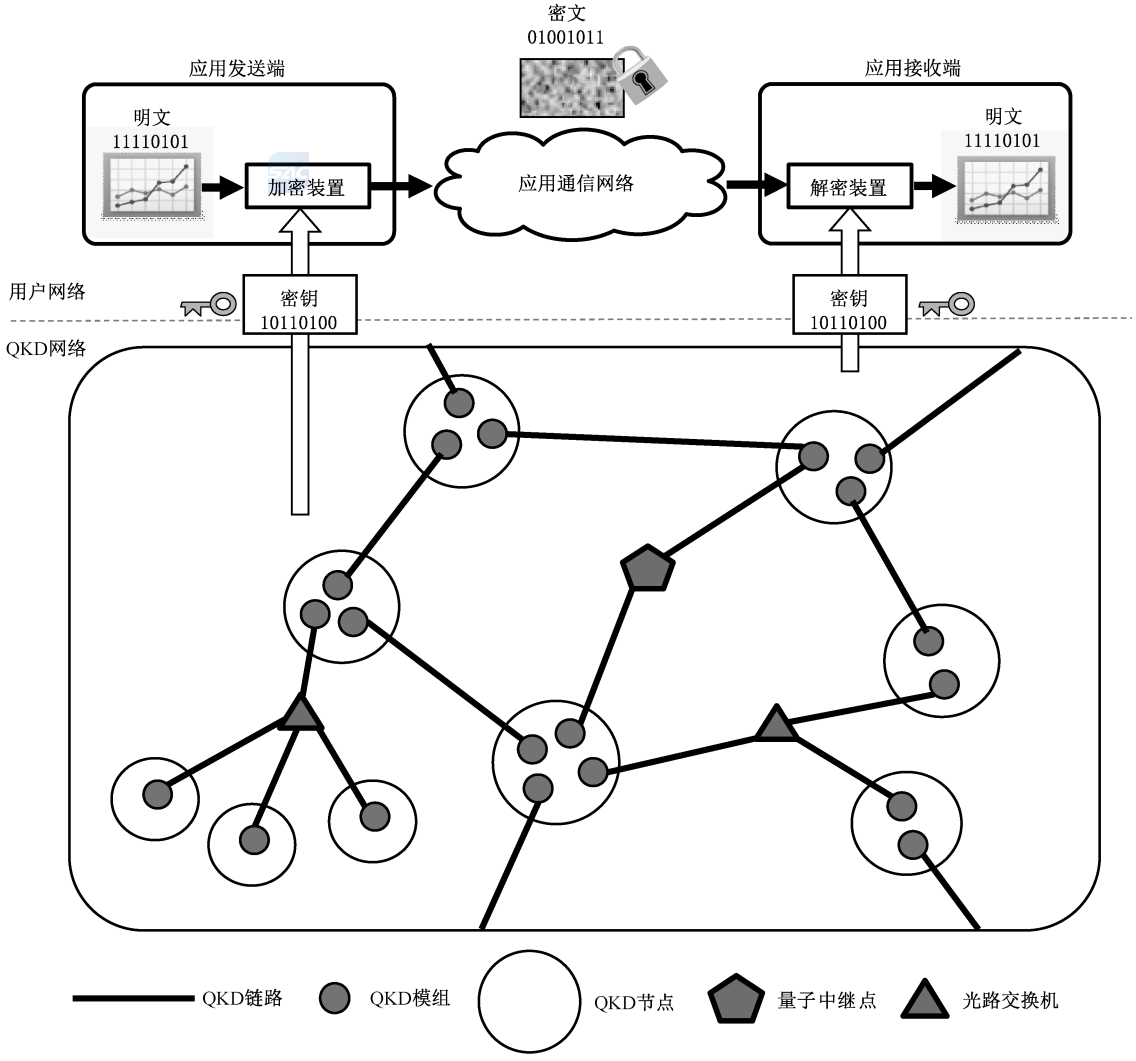

图 2　基于 QKDN 的量子保密通信

6 应用基本要求

量子保密通信基于QKD实现密钥分发功能。QKD作为基于量子通信技术的新型密码学功能组件，同时具有通信技术和密码技术二方面特征。

量子保密通信系统应在安全性、可扩展性、高效性、鲁棒性、应用灵活性、互操作能力、技术兼容性、可管理性、差异化策略控制方面满足如下要求。

a) 安全性要求：
   1) 应为量子保密通信用户提供信息论安全的密钥分发功能；
   2) 应采用经理论安全性证明的QKD协议；
   3) 应提供针对QKD系统的安全性测评；
   4) 应具备针对已知的量子层安全威胁的防御能力；
   5) 如采用可信中继技术，应提供有效的可信节点安全防护手段。

b) 可扩展性要求：
   1) 应灵活支持广域网所需的骨干、城域、接入等多种组网拓扑结构；
   2) 应可依据业务需求变化支持灵活、经济地扩容、升级和重配置；
   3) 应支持适用于接入网的一对多QKD。

c) 高效性要求：
   1) 应支持高效的密钥提供和密钥中继功能；
   2) 应支持依据用户需求和网络负载的变化，灵活选择密钥的传输路径，调度网络物理资源；
   3) 应具备高可靠、低时延、大容量的密钥分发提供能力。

d) 鲁棒性要求：
   1) 应支持稳定可靠的量子保密通信网络设计、部署和运营；
   2) 在某些链路或节点出现故障时，应支持快速故障定位和恢复。

e) 应用灵活性要求：
   1) 应灵活支持多样性的终端、用户和应用；
   2) 应支持灵活易用的可编程应用接口；
   3) 应支持与多种信息通信系统协议和应用的灵活集成。

f) 互操作能力要求：
   应支持量子保密通信网络中的不同厂商产品的互通能力。

g) 技术兼容性要求：
   1) 应支持多种类型QKD技术混合组网；
   2) 应提供QKD技术的升级迁移支持；
   3) 应支持多种密码算法。

h) 可管理性要求：
   应支持针对量子保密通信网络设备、网络配置、运维操作、监控、变更、升级、计费等方面的有效管理。

i) 差异化策略控制：
   应支持依据不同用户的特定安全等级及业务需求，提供差异化的密钥服务质量控制和灵活的计费方式。

7 应用场景

7.1 概述

量子保密通信可与信息通信系统中的各层协议结合应用，见图 3。

量子保密通信可服务于不同的行业应用，典型的行业应用场景示例见附录 B。

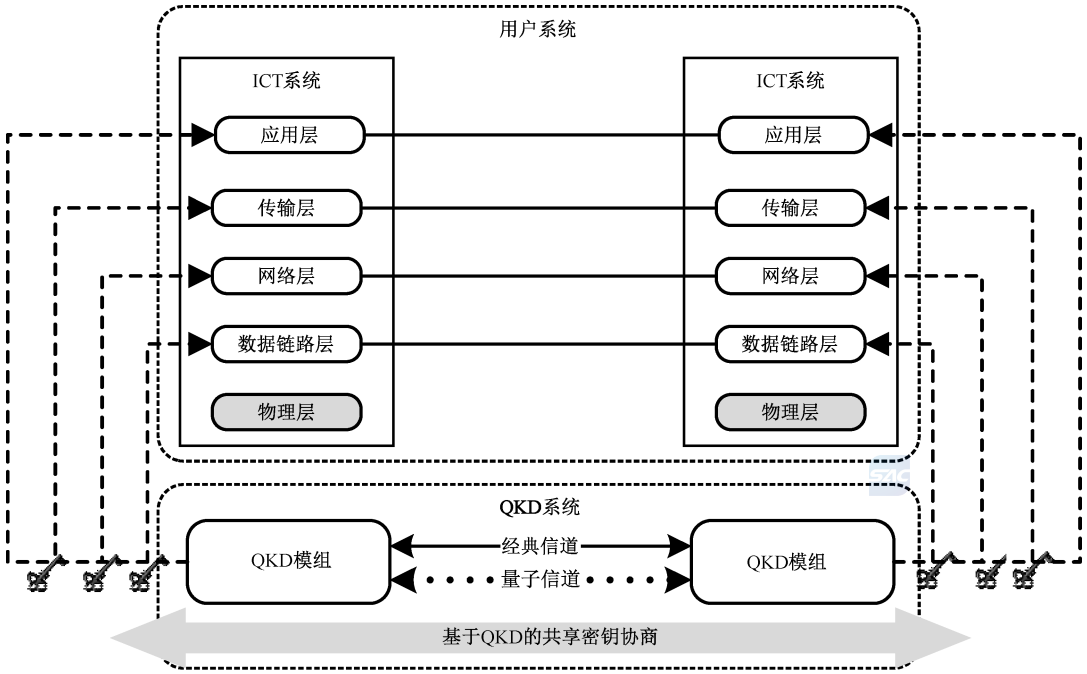

图 3 QKD 在信息通信系统中的分层结合应用示意

7.2 QKD 在数据链路层协议中的应用

QKD 可与数据链路层协议结合应用，例如 PPP、MACsec 协议。

PPP 工作在数据链路层，用于网络中两组节点之间的连接。PPP 中的加密功能通过 ECP 来实现，用于在 PPP 数据帧中实现加密算法。QKD 可用于实现 PPP 中的密钥协商过程。

MACsec 协议用于支持连接到 LAN 或互连 LAN 的授权系统的数据机密性、完整性和真实性。QKD 可作为一种密钥交换技术在 MACsec 协议中集成应用。

点对点链路上的 QKD 设备可与传统的链路加密机集成，构成基于 QKD 的链路加密机。该链路加密机可利用 QKD 生成的对称随机数作为会话密钥，实现分组密码算法（例如 AES）或序列密码算法（例如可实现最高安全性的 OTP）。

7.3 QKD 在网络层协议中的应用

QKD 可与网络层协议结合应用，例如 IPSec 协议。

IPSec 是用于保障 IP 通信安全的一组协议套件。IPSec 可实现数据流中 IP 数据包的鉴权和加密。IPSec 中的 IKE 协议负责建立安全的网络连接。IKE 协议使用公钥协商的方式来建立的共享的会话密钥，用于数据加密。

QKD 作为新型密钥交换技术，可与 IKE 协议融合。基于 QKD 增强的 IKE 协议，能够利用 QKD

生成的共享密钥实现 IPSec 载荷加解密功能，可根据安全等级需求使用分组加密算法或 OTP 算法。

7.4 QKD 在传输层协议中的应用

QKD 可与传输层协议结合应用，例如 TLS 协议或 SSL 协议。

TLS 协议或 SSL 协议用于在传输层中为网络通信提供端到端的安全服务。其通常使用公钥密码算法来建立会话密钥，用于保护敏感信息传输，例如电子商务交易中的信用卡信息。

在 QKD 与 TLS 协议结合使用的场景中，QKD 生成的密钥可用于替换 TLS 协议中的会话密钥，也可用于基于 OTP 方式的加密传输。

QKD 生成的密钥还可替代 TLS 协议中消息鉴别码算法所需的密钥，用于实现消息鉴别功能。

7.5 QKD 在应用层协议中的应用

QKD 可与应用层协议结合应用，例如加密语音/视频通话或会议、即时通信等业务。

应用层协议可利用 QKD 为通信收发两端提供的对称共享密钥，用于用户身份鉴别、鉴权或消息鉴别，也可用于实现业务载荷的加密传输。

附 录 A
（资料性）
QKDN 组网方案

QKDN 可将点对点 QKD 系统扩展为多用户网络，为连接网络的任意两个或多个用户提供量子密钥生成和分发功能。目前已知的 QKDN 组网方案包括以下几种。

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。该方案受到量子信号衰减带来的传输距离限制，仅适用于小规模网络。

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的 QKD 节点中，并利用逐跳 QKD 链路生成的密钥建立基于 OTP 方案的信息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 QKDN 的传输距离。该方案实施时需确保 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间测量节点。这些中间测量节点无需是可信节点。

d） 量子中继方案：该方案利用量子中继站实现量子态在网络中的端到端传输。量子中继站是将信息以量子态形式存储并转发的网络中间节点。该方案通常需要在通信链路沿线部署多个基于量子纠缠分发的量子中继站，以实现远距离的 QKD。这些量子中继站无需是可信节点。

附 录 B
（资料性）
量子保密通信在典型行业中的应用场景

B.1 数据中心备份及业务连续性应用场景

在不同数据中心之间执行数据备份及业务连续性等业务时，量子保密通信可用于保障数据中心之间数据传输的安全性。

随着大数据和云计算的发展，数据容灾备份越来越重要。特别对于数据安全性和可靠性要求高的行业，例如金融、电力、航空、互联网等，数据中心灾备的可靠性和安全性尤为重要。

这类场景通常将企业主要的数据处理集中在数据中心主站点，同时额外部署备份站点，用于对主站点数据实现远程备份或双活。在发生灾难或故障时，主站点数据出现丢失的情况下，备份站点可辅助主站点恢复数据。主站点与备份站点之间的通信要求严格的数据保密性。

见图 B.1，在主站点和备份站点之间可使用基于 QKD 的链路加密机，通过 QKD 按需更换密钥，建立加密通信链路。

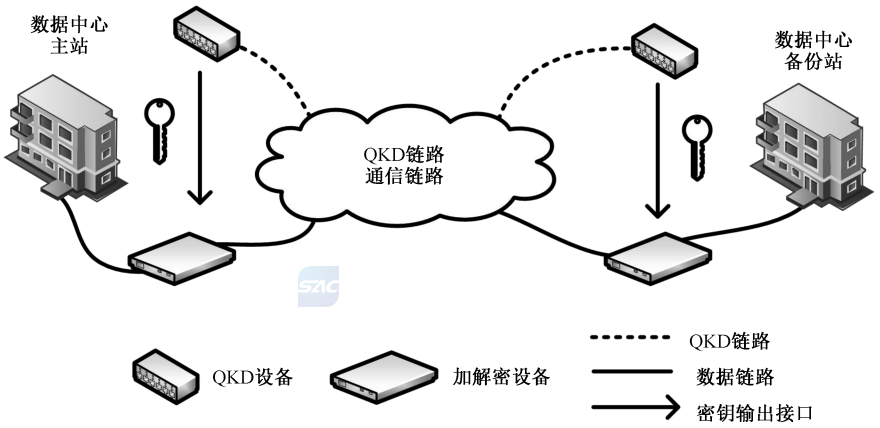

图 B.1 量子保密通信在数据中心灾备的应用场景

B.2 政企专网应用场景

量子保密通信可用于保护政企专网及其服务的安全性。

政企专用网络，即企业或政府机构通过自有网络或从运营商租用的光纤通信链路网络，将其总部及所属一个或多个分支机构、数据中心连接组成的专有网络。通过企业专网可为各分支机构提供各种应用服务，例如电子邮件、电话、音视频、数据存储和计算等信息服务。

企业或政府机构通常要求通信服务提供高度的机密性、完整性和真实性，可采用专用的安全系统。通常采用基于 IPSec 或 TLS 的 VPN 技术实现数据中心与分支机构之间的数据业务加密。

见图 B.2，在企业网内部各节点之间可使用基于 QKD 的链路加密机，建立加密通信链路。

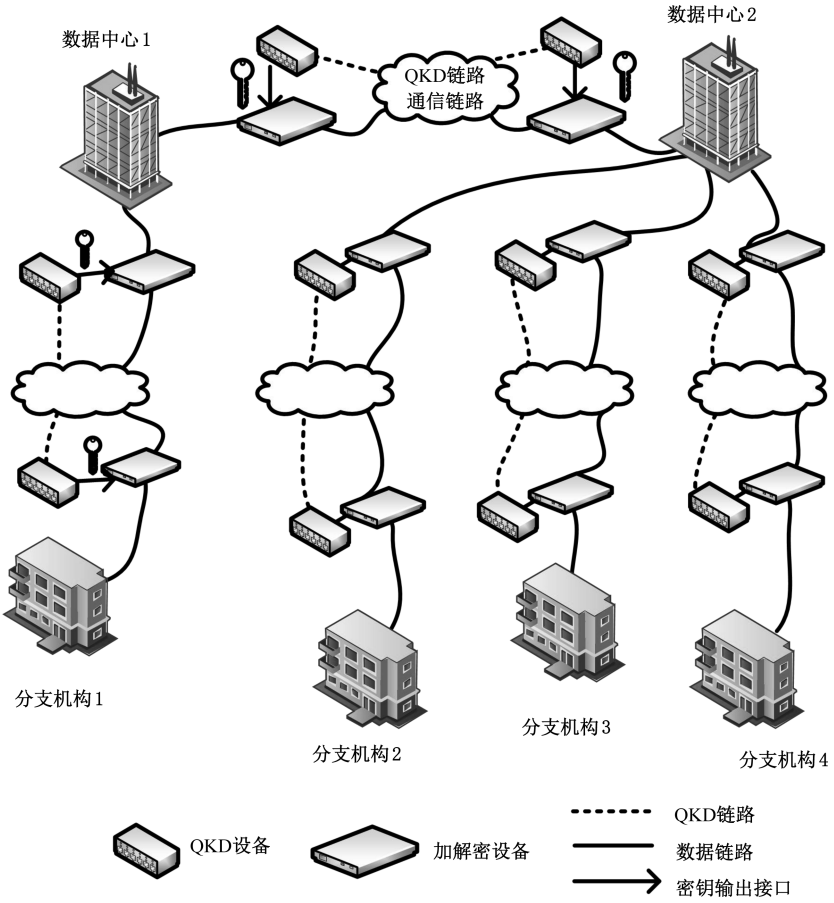

图 B.2　量子保密通信在企业专网的应用场景

B.3　关键基础设施监控和数据采集应用场景

量子保密通信可用于保护关键基础设施中的 SCADA 数据通信安全性。

关键基础设施，通常包括通信服务、供水服务、电力生产和分配服务、天然气、石油、金融服务、卫生服务、运输系统、粮食生产和分配系统等，对于社会经济的正常运行发挥着重要作用。这些系统的安全性和可靠性依赖于其通信基础设施子系统，其信息真实性、完整性、机密性均十分重要。

以铁路网为例，铁路控制中心一方面需要读取并处理轨道沿线各区段边界、交叉口、站点等处的传感器输入的信息；另外，控制中心还需要向信号开关、交叉关口、显示器等下发控制指令。该系统要求所有信息均可鉴别来源，同时某些信息需加密并提供完整性保护。

利用 QKDN 为各通信节点以信息论安全方式分发的密钥，可实现高安全性的鉴权、加密和完整性保护功能。

见图 B.3，该场景通常可构建专用的 QKD 广域网络来支持，由 QKDN 提供多节点的密钥分发管理、密钥中继转发等功能。业务使用方通常需通过专用接口访问 QKDN，为通信双方分发密钥并执行数据加解密等操作。

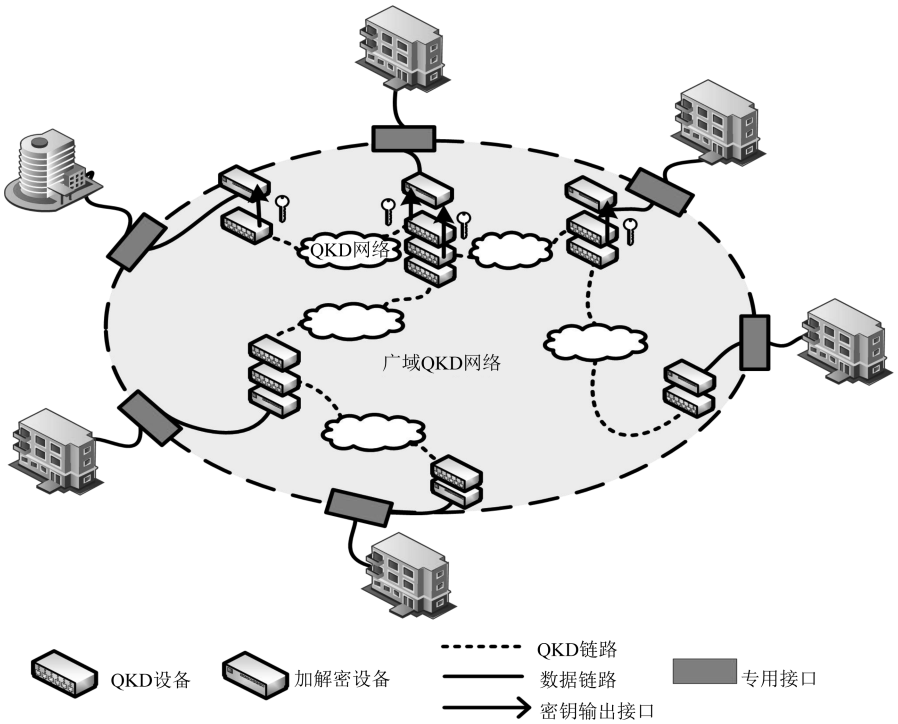

图 B.3　量子保密通信在关键基础设施监控与数据采集的应用场景

B.4　电信骨干网应用场景

QKD 可用于为电信网络的骨干网节点之间通信提供安全服务。

目前电信骨干网多采用 WDM 技术。利用电信骨干网中独立的光纤或富余的波道建立 QKD 链路，通过 QKD 链路分发的密钥，可对 WDM 业务通道实现高安全等级加密。

见图 B.4，以 OTN 技术为例，QKD 设备生成的对称密钥可用于 OTN 设备间业务数据加解密。QKD 系统所需的量子信道、经典信道以及承载 OTN 业务的数据信道，可通过波分复用方式在同一条光纤中传输。

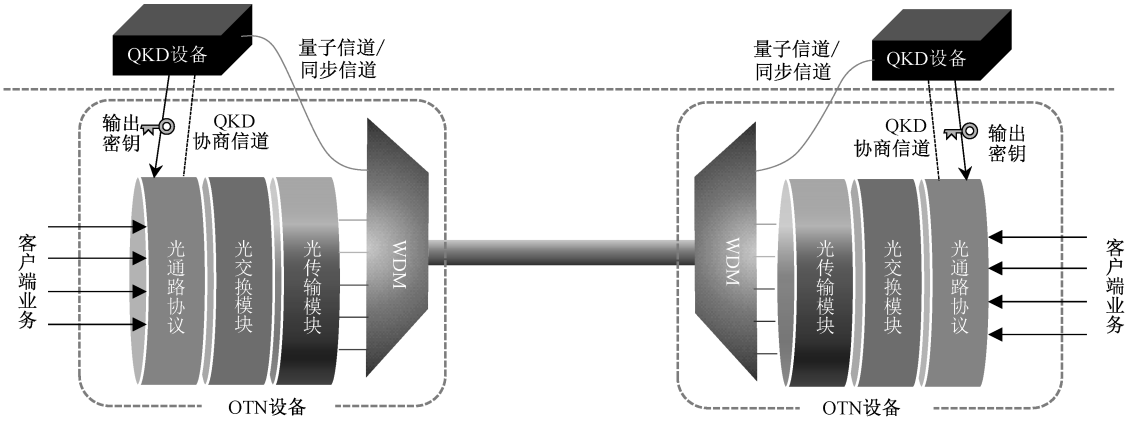

图 B.4　量子保密通信在电信骨干网保护的应用场景

B.5 电信接入网应用场景

QKD 可用于保护电信接入网中的数据通信安全。

以基于 PON 技术的电信接入网为例，其通常由一个 OLT 与多个 ONU 连接组成。OLT 通常安装在电信网接入机房中，ONU 安装在终端用户附近。下行业务信息从 OLT 向下游广播到所有 ONU，而上行业务则采用时分或波分复用方案实现。PON 网络中每个 ONU 都可接收到 OLT 的所有下行链路信号，可使用加密措施防止 ONU 窃密。

见图 B.5，可在每个 ONU 处部署 QKD 发射机，在 OLT 处部署 QKD 接收机。通过 QKD 系统可在 PON 网络中的 OLT 和 ONU 之间安全地分发密钥，支持 ONU 用户数据的加密传输。

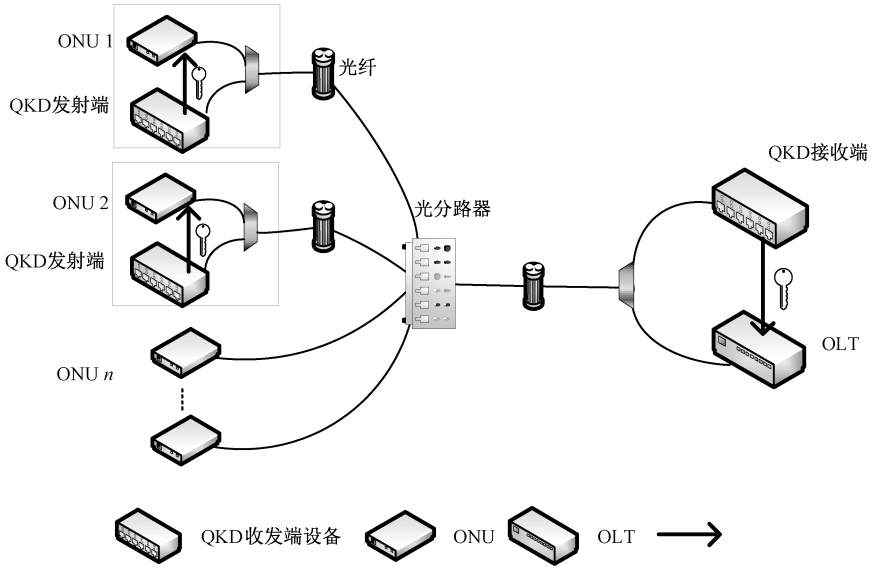

图 B.5 量子保密通信在电信接入网保护的应用场景

B.6 自由空间远距离保密通信应用场景

通过基于自由空间的 QKD 可保护远距离站点之间的数据传输安全性。

QKD 可与基于卫星、飞机等飞行器的无线通信系统相结合，实现远距离站点之间高安全的密钥分发。

见图 B.6，以卫星通信场景为例，地面站 A 和 B 是远距离地理分隔的两个网络节点，例如由海底通信光缆相连的海洋两岸。当卫星经过地面站 A 和 B 时，可与它们之间分发对称的共享密钥。该密钥可用于对称加密方案中，以确保地面站 A 与地面站 B 之间远距离通信的数据传输安全性。

该用例还可扩展到多颗卫星的场景，它们之间通过自由空间链路相互连接，可构成覆盖全球的卫星 QKDN。由于空间信道相比地面大气衰减显著降低，卫星之间可以较高的密钥分发速率远距离分发密钥。

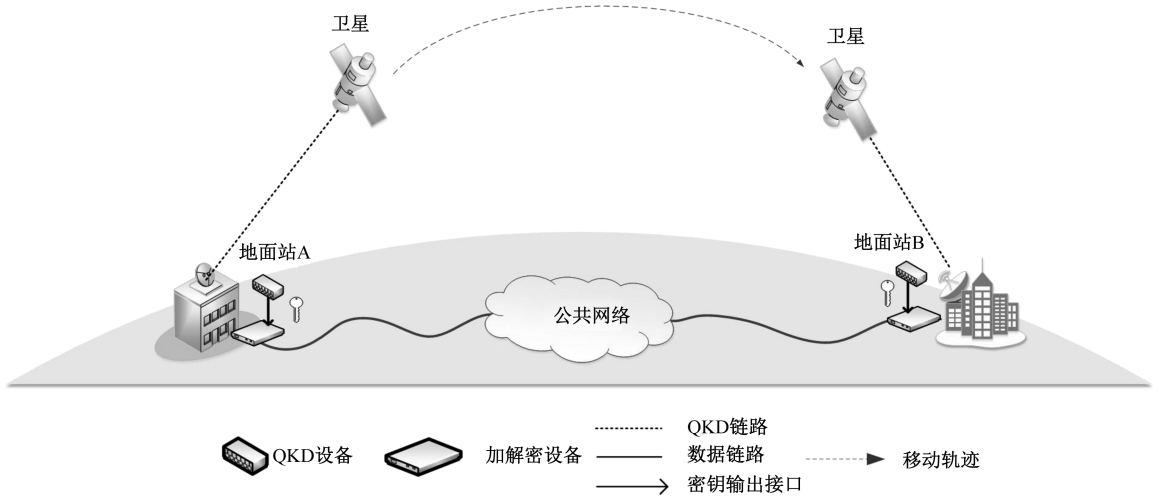

图 B.6　量子保密通信在卫星远距离保密通信的应用场景

B.7　移动终端安全服务应用场景

将通过 QKD 生成的对称密钥对，提前预置在移动终端中，可在移动办公、移动作业、移动支付、物联网等多种场景保护其通信安全性。

见图 B.7，将 QKDN 产生的对称量子密钥对，分别预置在量子安全服务密钥分发中心和靠近用户的量子密钥充注设备中。

当移动终端用户首次接入或密钥耗尽时，可通过量子密钥更新设备充注一定量的密钥，预置在终端的安全存储媒体（例如智能 IC 卡、智能密码钥匙、SIM 卡、安全芯片等）中，用于其后续通信过程中的鉴权和会话加密。

在移动终端与服务器通信时，可首先通过移动终端预置的部分量子密钥，通过量子安全服务密钥分发中心完成身份鉴别。然后，利用量子安全服务密钥分发中心在移动终端和服务器之间协商会话密钥，产生一次性使用的会话密钥，结合 OTP 或其他对称密钥加密算法对会话信息加解密。

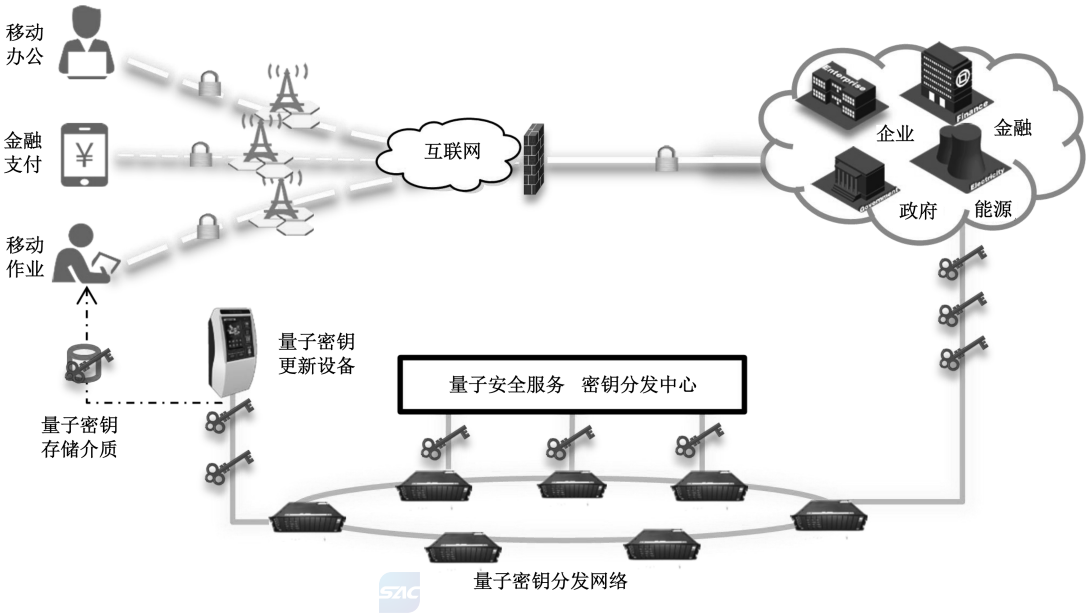

图 B.7　量子保密通信在移动终端安全服务的应用场景

参 考 文 献

[1] GB/T 17901.1—2020 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] ETSI GS QKD 002 V1.1.1 (2010-06) Quantum Key Distribution;Use Cases