连续变量量子密钥分发设备 CVQKD-101

产品白皮书

上海循态量子科技有限公司

2022 年 1 月

本文档的全部内容属于上海循态量子科技有限公司所有，未经明确书面许可，任何单位或个人不可擅自引用、复制、誊抄或转译本文档部分或全部内容，不得以任何形式或方式（电子、机械、影印、录制或其它可能的方式）进行商业传播或用于任何商业、盈利目的

目 录

1. 引言 2
2. 产品介绍 4
2.1. 产品简介 4
2.2. 产品参数 5
2.3. 产品外观及接口 6
2.4. 功能模块 8
3. 产品工作流程 9
4. 产品安全设计说明 9
5. 产品典型部署 9
6. 组网方式 10
6.1. 量子保密通信组网方式 10
6.2. 量子密钥传输方式 11
6.3. 点对点组网方式 12
6.4. 星形组网方式 12

循态量子

1. 引言

随着信息化系统的复杂程度越来越高，单凭一种安全技术已不能保障系统的安全性。近几年许多影响巨大的信息安全事故充分说明了这一点。例如中兴通讯的机密文件泄露引起美国制裁、CSDN 门户网站泄密超过 600 万用户信息被盗、华为电子邮件被曝一直被监控、联想电子邮件被国外黑客控制等等，都带来了巨大的经济和政治影响。B 站后台源码泄漏，代码包含了很多配置文件、密钥、密码等敏感信息。

数据窃取事件频发，这是因为现有技术和协议原因，传输和存储过程均是明文，极易被篡改或窃听。数据泄漏等严重安全事故越来越多，已成为黑客进行。APT 攻击的最主要途径。在美国前中情局雇员斯诺登曝光了美国监控行动“棱镜”项目，几乎所有数据信息每日通过不安全的链接，被国家安全局和其他情报机构使用数字收集装置来捕获、追踪。传统的网络安全技术已经不足以保证系统和系统内敏感数据的安全性，这就需要由密码技术来作为信息安全的最关键防线。密码技术可以从数据安全本身出发，实现数据机密性、完整性、不可否认性等安全保护，即使网络不安全、系统存在漏洞的情况下也可以保证数据安全。美国长期禁止出口重要密码算法，也充分说明密码算法对信息系统的安全性有着重大意义。但现有的经典密码体系同样面临严重的威胁，而量子保密通信技术可以实现无条件安全的通信。

量子，是构成物质的最基本单元，是能量、动量等物理量的最小单位，不可分割。像电子、光子等构成物质的基本粒子，统称为量子。

量子保密通信利用了量子力学测不准原理和不可克隆原理进行密钥的分发，从理论上保证了密钥在分发过程中的安全性，从而保证采用量子密钥加密数据的安全性。

经典保密通信利用数学的复杂度保证密钥安全，其安全性和高效性都无法和量子密钥相提并论。经典密码的安全性随着算力的提升，尤其是量子计算的出现，面临着日益严峻的挑战；而量子通信绝不会“泄密”，因为根据量子力学基本原理，任何窃听者通过任何手段对信道的窃听、测量，都会改变原有的量子态，而合法通信双方不仅可以发现这种窃听，而且能评估其信息泄露上限并加以剔除，因此在当前的技术体系架构里，量子保密通信具有无条件安全性。

正是因为具有传统通信所不具备的安全特性，量子保密通信在国家安全、政务、电信、金融、能源等具有信息安全需求的领域有着重大的应用价值和前景。

量子保密通信分为离散变量和连续变量两种主流密钥分发方式，离散变量密钥分发技术将信息调制编码在离散变量上，而连续变量分发技术则采用了量子态的连续变量进行编码，在成码率和融合性方面更具优势，近年来得到了广泛关注。

量子通信技术编码信息在光的量子状态传输它在宏观距离，并使特别变革性的应用在密码学。其中技术最成熟的是量子密钥分发(QKD)，它允许安全地共享私有加密密钥。QKD 利用量子物理学来证明任何窃听的尝试都发生在密钥交换和测量泄漏的信息，从而启用两个合法的合作伙伴知道它们打算用于加密的私钥是否为在传输过程中受损，到何种程度。因此 QKD 阻止了对手“先存储，后解密”的可能性。

目前量子通信主要有 2 条技术路径：

离散变量量子密钥分发（DVQKD）
特点:编码在**本征值为离散变量**物理量上,例如**单光子的偏正态**,代表协议:BB84 协议。
连续变量量子密钥分发（CVQKD）
特点:编码在**本征值为连续变量**物理量上,例如**相干态的正则分量**,代表协议:GG02 协议（高斯调制相干态协议）。

量子通信 2 条技术路径对比分析：

DV-QKD	CV-QKD
1：存在非对称测量算符 A1，A2，其中 A1 对应直线型偏振测量基，A2 对应对角线型偏振测量基； 2：接收数据 Y 与发送数据 X 存在一定的误码率 QBER； 3：对于每个脉冲，如果 Eve 进行截取发送，由于存在非对易编码方案，因此无法克隆，智能猜。那么他猜对的概率是 0.5+0.5*0.5=0.75，猜错的概率为 0.25，如果截取重发的脉冲多了，那么 Bob 侧测到的误码率就会显著提升，从而发现窃听存在。 4：DV 通过监测 QBER 发现窃听；	1：存在非对易测量符 X 与 P，其中 X 对应正则位置，P 对应正则栋梁； 2：Y=kX+ε；CV 是线性模型，Alice 和 Bob 数据相关，接收数据为发送数据衰减（k 为线性衰减系数）加噪声，ε 为噪声。 3：对于每个脉冲，如果 Eve 进行截取重发，由于存在非对易编码方案，因此无法克隆，只能猜，那么他猜对的概率是 0.5，猜错的概率也是 0.5，例如如果猜错测到 P，那么急于这个测量结果重发的态当 Bob 正确测量 X 的时候就会叠加一个噪声。截取重发的脉冲多了，那么 Bob 侧测到的噪声就会显著提升，从而发现窃听存在。 4：通过监测 ε 发现窃听；

2. 产品介绍

2.1. 产品简介

CVQKD-101产品是上海循态自主研发的新一代连续变量量子密钥分发终端设备。该系列产品基于量子力学原理，实现了密钥的安全分发，通过在通信双方

实时分发量子安全密钥，并使用安全密钥保护用户数据，实现了抗量子计算的数据安全加密解决方案，具有密钥生成速率高、抗攻击能力强、性价比高等特点，同时该系列产品相较市场上其他量子密钥分发设备，具有体积小，集成度高，鲁棒性好等优势，可广泛应用于政务、国防、金融、能源、5G、物联网、区块链等领域，。

产品特点

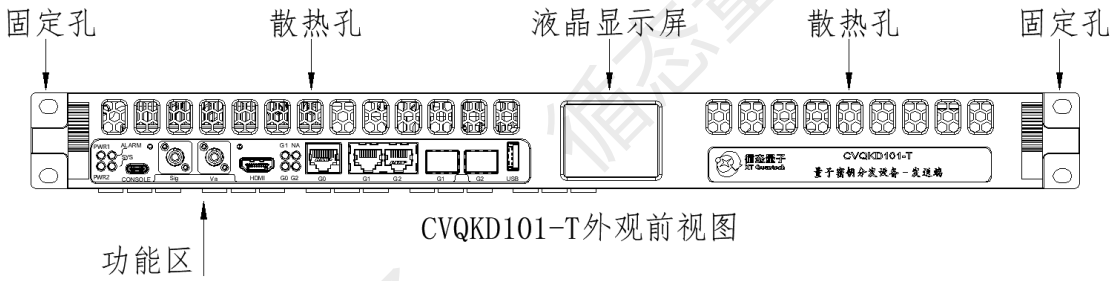
- 基于高斯调制相干态GG02协议；
- 抗本振攻击、波长攻击等各种攻击手段；
- 机箱为标准19英寸机架形式、1U高度，设计紧凑；
- 核心部件冗余备份；
- 采用FPGA优化，加速控制和协商过程；
- 基于FPGA的多层访问控制策略，有效隔离量子通信域和经典通信域；
- 采用单一波长传输量子信号和同步信号，最大程度地降低了用户TCO；
- 连续变量量子密钥分发采用多光子调制，抗干扰能力强，现网融合高；

2.2. 产品参数

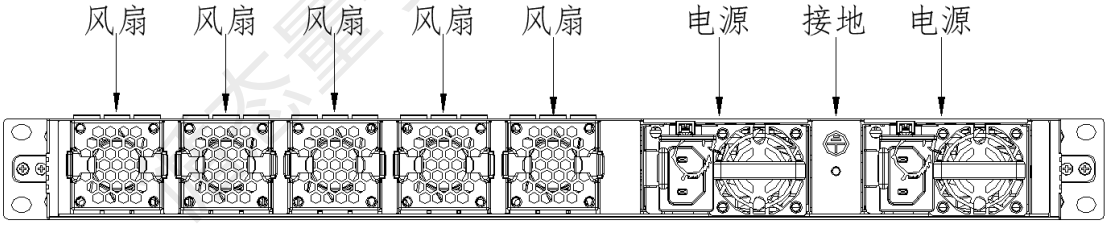
	参数
工作频率	10MHz
密钥成码率@5dB	150Kbps
密钥成码率@10dB	25Kbps
密钥成码率@20dB	1Kbps
工作波长	全C波段可调；符合ITU标准，频率范围193.3-196.05THz
电源功耗	<200W
尺寸	481mm*550*44mm(1U)

2.3. 产品外观及接口

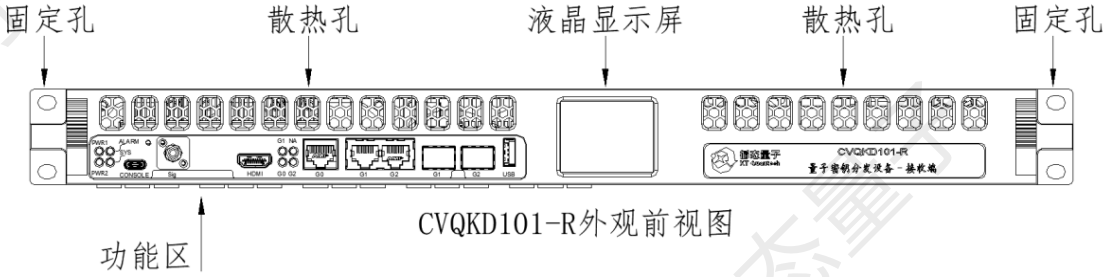
2.3.1. 产品外观



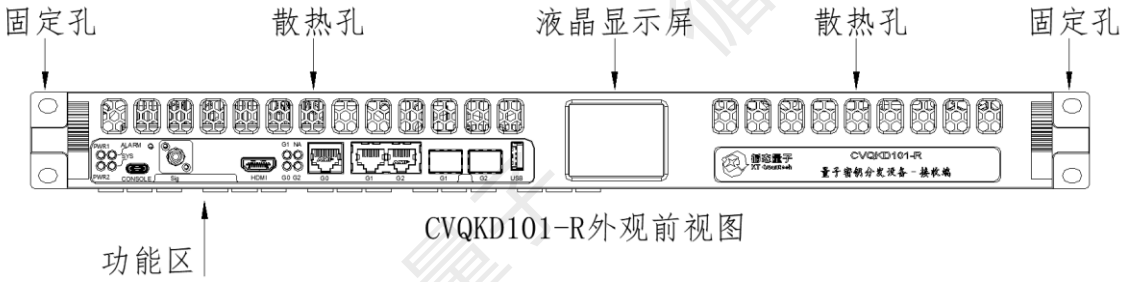
CVQKD101-T外观前视图



CVQKD101-T外观后视图



CVQKD101-R外观前视图



CVQKD101-R外观前视图

2.3.2. 接口说明

1. 指示灯

- PWR1

绿色—常亮标示电源 1 工作正常、长灭标示电源 1 未正常供电或工作异常；

- PWR2
- 绿色—常亮标示电源 2 工作正常、长灭标示电源 2 未正常供电或工作异常；
- ALARM

  红色—系统告警时该指示灯常亮；
- SYS

  绿色--常亮标示系统正在初始化、闪烁标示系统已启动完成并且运行正常、常灭标示系统启动异常；
- G0~G2

  以太网端口指示灯、常亮标示对应端口 LINK、闪烁标示对应端口数据收发、常灭标示对应端口不 LINK；

2. 接口

- CONSOLE

  系统控制台接口，接口类型为 USB-C，波特率为 115200；
- Sig

  CVQKD101-T 的量子信号光输出光口（默认 FC/APC），或者 CVQKD101-R 的量子信号光输入光口；
- Va

  CVQKD101-T 的量子信号光的监控测试光口（默认 FC/APC）；
- HDMI

  该接口可支持外接显示器，显示密钥分发设备在初始化以及正常工作过程中的流程及状态信息。
- G0（E）

  G0 系统管理接口，为千兆以太网电口，用户可以通过本接口访问、管理和配置本设备；
- G1（E/O）

  G1 为系统密钥输出口，为千兆以太网光电复用接口，用户可以通过本接口按照约定的流程和格式输出安全密钥。
- G2（E/O）

  G2 为系统协商接口，为千兆以太网光电复用接口，该接口用于密钥分发过程中，收发端之间必要的经典信息交互。

- USB

  密钥分发主控板提供的 USB3.0 接口，支持外接存储或者其它专用设备；

3. 显示屏

2.0 寸 LCD 显示屏将显示设备在上电初始化以及正常工作时的关键状态信息，如电源工作状态、FPGA 初始化是否正常、密钥分发过程中的关键参数等。

2.4. 功能模块

CVQKD101 型量子密钥分发设备主要可以分为 5 个模块：机箱模块（包括机箱结构、电源和风扇）、量子随机数模块、光路模块、数据收发模块和数据处理模块。各模块的具体功能如下：

2.4.1. 机箱模块

机箱结构是整个设备的结构基础，为其他功能模块提供安装、固定和连接的支撑；系统电源为整个系统提供电源供给。风扇将设备内部热量交换至设备外部，保证设备内各模块、部件工作温度符合要求。

2.4.2. 量子随机数模块

量子随机数模块为整个密钥分发过程（包括如量子态的制备、测量基选择以及数据后处理等过程）提供最原始的真随机数，进而保证量子密钥分发过程以及最终密钥的安全。

2.4.3. 光路模块

光路模块是整个量子密钥分发系统的核心部件。CVQKD101-T 的光路模块包括激光源、脉冲生成、高斯调制、衰减控制以及反馈监控等，主要实现量子态的制备和发射功能；CVQKD101-R 的光路模块包括测量基选择、量子态相干探测和反馈监控等，主要实现量子态的探测功能。

2.4.4. 数据收发模块

数据收发模块主要是配合和驱动光路模块，如将从量子随机数源获取的随机编码信息发送给发射端光源模块并将其编码在光场的正则位置和动量上；以及对接收端光源模块量子态相干探测恢复出的信号进行采集和接收，并传输给数据处理模块进行数据的后处理以获取安全密钥。

2.4.5. 数据处理模块

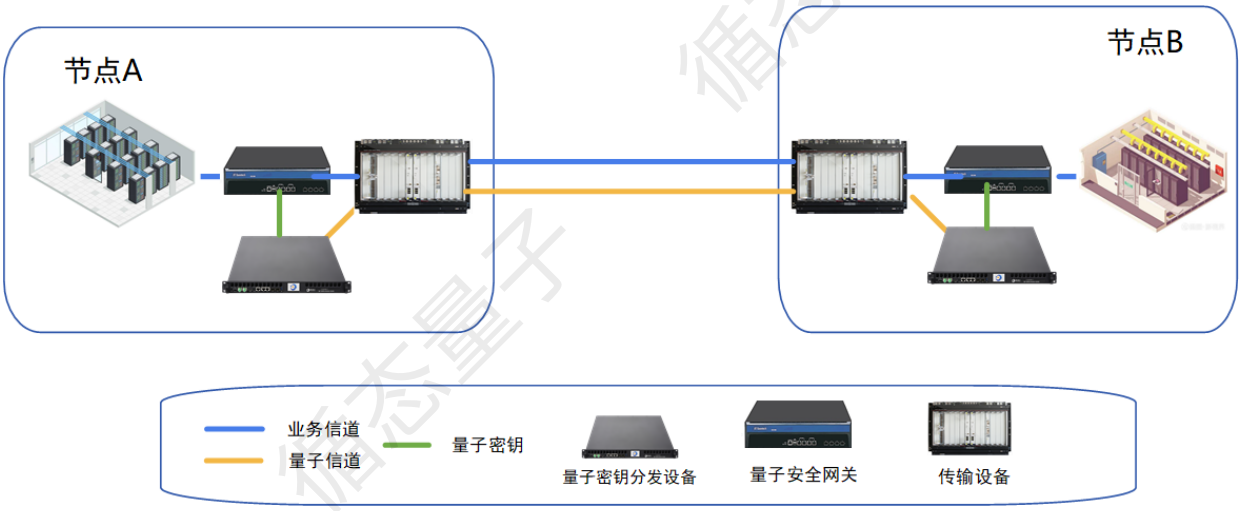
数据处理模块主要完成对原始密钥数据的处理，如基矢比对、数据协商和保密增强等，并最终输出安全的量子密钥。

3. 产品工作流程

4. 产品安全设计说明

5. 产品典型部署

CVQKD-101 的典型部署方式如下：



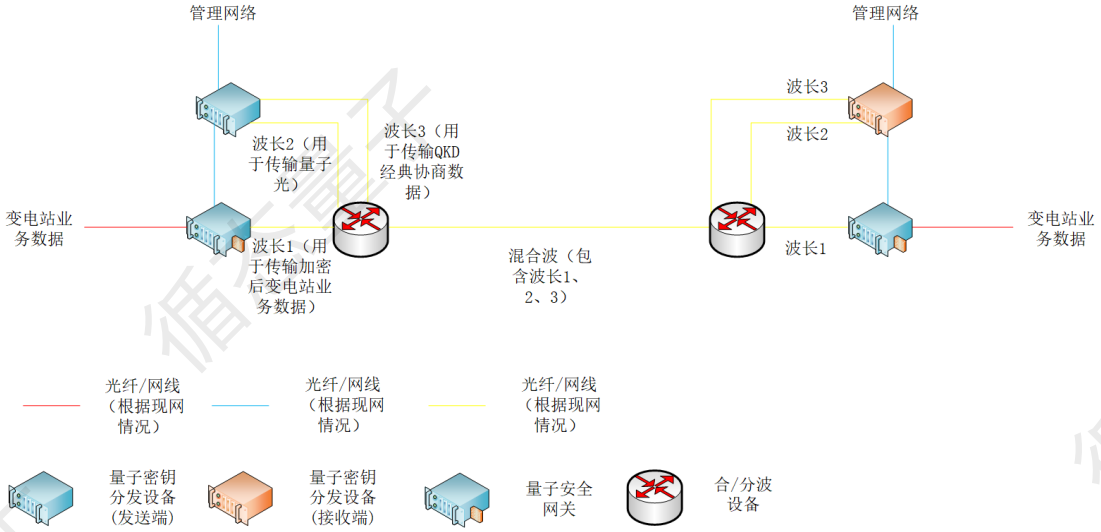
用户之间通过部署连续变量量子密钥分发设备（CVQKD）实现量子密钥分发，

随后加/解密设备从 CVQKD 获取量子密钥，用户业务系统发送的数据通过加密/解密网关加密后传输，实现数据安全传输。

加/解密设备：

可以使用原有设备或更换新设备。如果使用原有设备，需要原有设备能支持外接密钥并提供密钥接口协议。如果更换为量子安全网关，目前我司设备可支持基于 IP 地址加密，及针对数据流的源地址和目的地址。

物理连接示意图如下：



6. 组网方式

6.1. 量子保密通信组网方式

目前比较成熟的量子保密通信技术主要是通过量子信道进行量子密钥分发，使用传统的加密设备使用量子密钥进行数据加密。量子密钥分发保障密钥分发的安全性，并提供相对充足的密钥，通过提升传统加密设备的加密密钥更新速率和通信加密强度提升通信的安全性。对于传统加密设备，不需要进行物理方面的改造，只需要将涉及到密钥交换部分中的经典密钥替换为量子密钥进而得到量子安全网关，一般情况下只需要通过简单的软件改动即可实现。例如，使用 IPSec 或 TLS/SSL 协议的传统加密设备，只需要在加密设备中提供一个从量子密钥分发设备接收量子密钥的软件接口，就可以在加密设备中使用量子密钥替换经典密

钥。

按照网络复杂程度和覆盖范围的不同，量子保密通信网络按网络拓扑结构来划分包括点对点、星形、链形及网状几种。通常，简单组网为点对点或星形，城域组网多为星形或网状，广域组网多为链形加星形或网状。

6.2. 量子密钥传输方式

按照传输原理和方式的不同，目前传输量子密钥主要分为两大类，即采用独立光纤信道传输和经典-量子波分复用共纤传输。

基于独立光纤的量子网络如下图所示，其中按照功能不同需要三类信道，一是用于传输光量子信号的量子信道，目前主要采用光纤方式；二是用于传输量子密钥分发及管理过程中交互信息的交互信道，目前可以采用网线、光纤或者无线等传输方式；三是用于传输用户加密数据的业务信道，目前可以采用网线、光纤或者无线等传输方式。

图 6-1 量子密钥单纤传输

如图所示，在用户业务场景光纤资源紧张的情况下，可以采用经典-量子波分复用终端将业务信道、交互信道、量子信道通过波分的方式整合在一根光纤中，实现光纤资源的复用，降低投入成本，提高光纤的利用率。

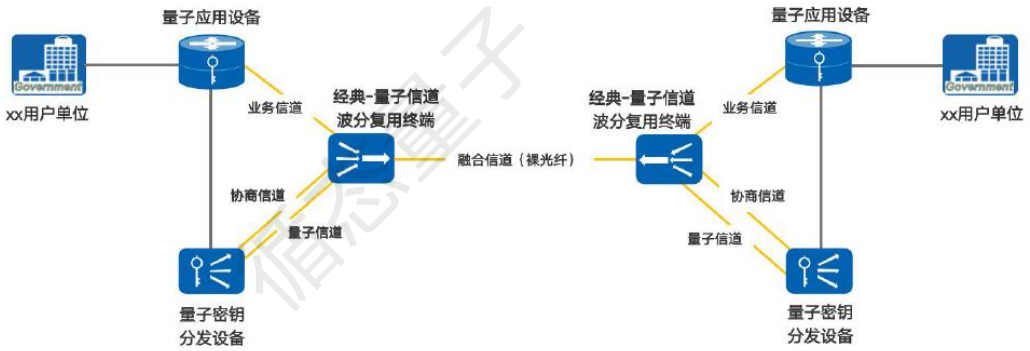


图 6-2 业务数据与量子密钥共纤传输

6.3. 点对点组网方式

点对点量子保密通信是最基本的量子保密通信实现方式，下图给出了点对点量子保密通信组网方式，需要使用一条单独的光纤线路实现量子密钥的传输，而原有的业务通道光纤线路保持不变。

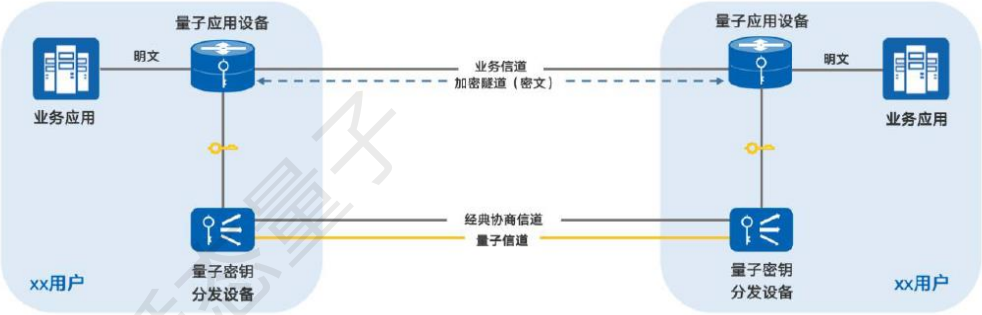


图 6-3 点对点组网

点对点组网方式适用于某企业或机构两节点间的专用应用场景，此方式优点是结构清晰、部署简单，在两点间有直连光纤资源的情况下，只需要在两节点部署量子密钥分配设备及相应的交换机和软件服务器即可实现；缺点是两节点间需要有直连光纤资源，即之间不能存在光电转化、光放大等设备，在光纤资源上有一定的限制。

此外，在当前技术条件下，基于光纤的点对点量子保密通信受密钥分发最大距离限制，可以通过在两节点之间接入可信中继的方法，实现远距离的端对端量子保密通信。

6.4. 星形组网方式

量子保密通信还支持星形组网方式，通过光开关设备实现一对多的量子保密通信网络建设。用户部署量子密钥分发设备和量子网络管理设备，用户节点部署量子密钥分发设备，即可实现中心对多个用户节点的量子密钥分发，节约设备成本。

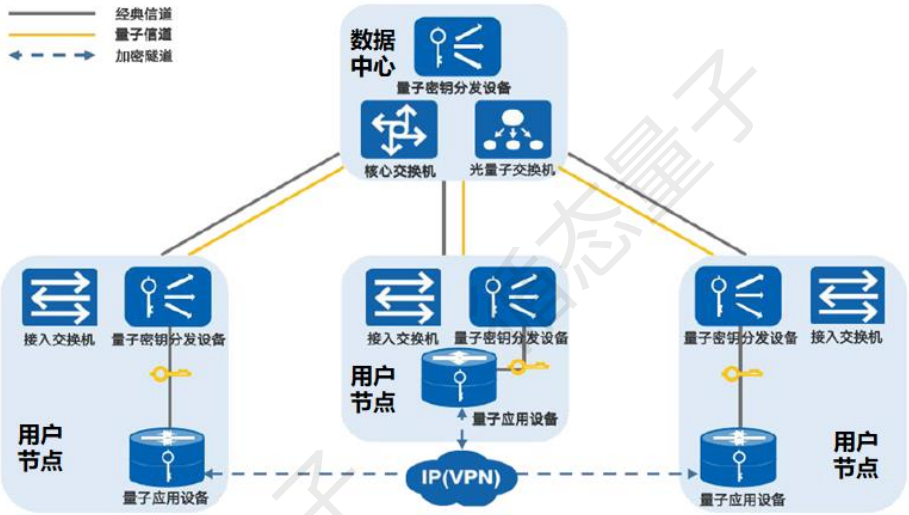


图 6-4 星形组网

星形组网方式主要应用于同一机构内部组建专网，及不同机构间组建量子保密通信网络。

星形组网方式优点在于：①管理集中，中心站点能方便地提供服务和对网络进行重新配置；②节点管控便易，添加或删除节点容易；③网络结构简单，容易检测和隔离故障；④数据传输率高，业务适应性强，用户节点仅与中心节点，无需支持多用户节点访问权争用。

星形组网方式的缺点：①路线利用率低，每条链路仅供中心站点与对应节点使用；②对中心站点的可靠性和冗余度要求高，资源共享能力差；③安装和维护费用高，需要大量光纤资源。