量子城域网在城市数字化底座中的创新实践

蔡敏，华静
（中国电信股份有限公司上海分公司，上海 200040）

摘　要：信息安全是国家发展重要的一环，量子通信技术是目前唯一原理上不可破解的保密技术。通过虚拟化技术针对量子密钥管理服务系统部署进行优化，提升了城市数字化系统数据在量子城域网承载过程中的运行效率和资源弹性，并通过平台部署验证测试，健全了政务服务量子保密通信配套机制，为项目实践提供了参考。

关键词：量子城域网；虚拟化；量子密钥管理服务系统
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000-0801.2025076

0　引言

随着云计算技术向构建新一代数据中心发展，以虚拟化为基础实现管理及业务的集中，对城市数字化底座服务资源进行动态调整和分配提出了新的要求。

量子保密通信利用单光子不可分割、量子态不可复制的特性实现通信双方间的安全密钥分配，结合“一次一密”技术实现传统通信方式所不具备的无条件安全特性，从理论上保证了利用量子保密系统加密的信息，在传输中不会被如今不断提高的计算能力和数学水平的破解，同时也能抵御潜在的量子计算机的威胁。

通过在城市数字化底座系统部署平台融合量子通信基础设施，将可实用化量子密钥分发并将量子安全加密能力纳入政务底座服务目录，可以为市区各级委办局平台用户提供高等级、高质量的基于抗量子计算的城市级密钥分发基础设施。

收稿日期：2024-11-20；**修回日期：**2025-02-10

1　场景分析

1.1　典型场景

依托量子城域网构建市域级量子保密通信网络的应用场景均是在数据中心和数据报送客户端新增实体的密钥分发和密钥应用物理设备，进行点对点的传输加密服务[1]。典型量子加密数据中心架构如图1所示。

- 量子城域网：基于量子密钥分发技术搭建的市域级保密通信网络，由众多分离的节点组成，各个节点间由光纤互联。量子城域网网络通过量子密钥分发设备实现相邻光纤连接节点间的量子密钥生成，通过中继密钥技术实现全网任意节点间的量子密钥共享，进而采用对称加密技术实现业务数据在网络中基于量子密钥的保密传输。
- 通信网络：用户所传输业务的通信网络，可以是互联网、政务外网、项目专

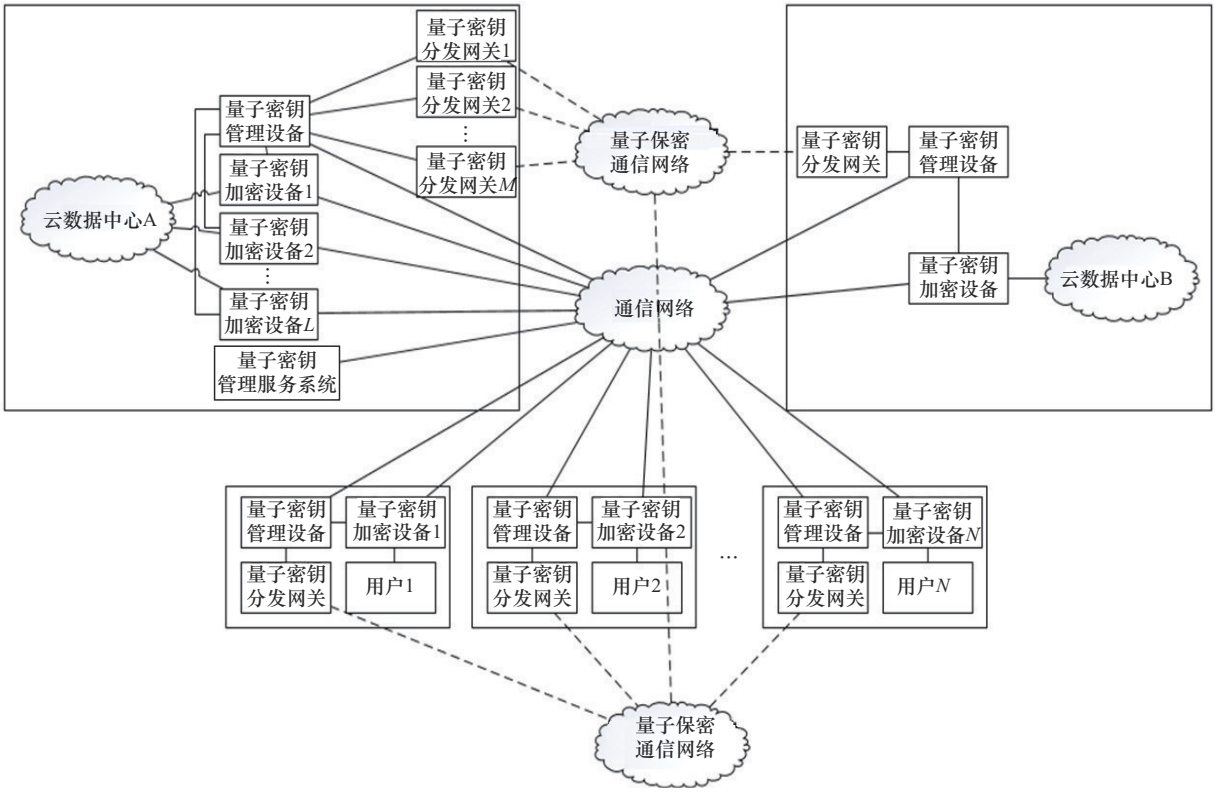

图1　典型量子加密数据中心架构

网或机构内网。在政务云场景下通常是政务外网。

- 云数据中心：多功能的建筑物，能容纳多个服务器以及通信设备。可包括任意多个，案例中为简化模型选用两个。部分省级政务云数据中心会依托两家以上运营商，基于双数据中心同时构建双活政务云平台。
- 量子密钥分发网关：集成量子信号发射或接收模块，满足量子通信网络中的量子密钥分发需求，提供安全的量子密钥。
- 量子密钥管理设备：提供量子密钥分发控制、量子密钥管理、量子密钥中继/交换、量子密钥输出、光量子交换控制等功能。
- 量子密钥加密设备：以量子密钥为会话密钥的应用加密设备，包括IPsec-VPN、SSL-VPN等多种加密设备。

通过针对现有场景分析，目前量子城域网用户和业务数量扩张过程中，会造成数据中心需额外管理设备和线路连接的堆积，既无法适应数据网络中多样化和复杂化的传输安全需求，也和数据中心硬件设备集中化精简化灵活化管理的发展方向相悖，缺乏资源部署的可扩展性；另外，不同用户不同业务间无法共享利用和管理量子密钥，这造成了量子密钥资源和量子密钥存储资源的浪费，不能体现城市数字化底座多租户场景下虚拟化部署的优点；再一方面，不同用户间无法共享利用量子密钥加密资源，也造成了加密资源的浪费。此外，实施/运维人员目前只能通过现场手动增加和安装物理密钥管理和密钥加密设备的方式，来安装、实施、配置和上线新增用户和项目以及运维已有设备，耗费大量人力。

1.2　核心场景需求

- 量子密钥生成与管理：通过量子密钥分

发设备生成量子密钥，并进行管理。

- 量子密钥分发流程控制：控制网络内各节点间的量子密钥分发流程和中继流程。
- 量子密钥加密应用：以量子密钥为会话密钥的应用加密设备，包括IPsec-VPN、SSL-VPN
- 资源动态调节：根据使用情况动态调节计算资源、内存资源、存储资源等资源的使用。

1.3　具体指标和参数

- 量子密钥分发速率：量子密钥分发设备应支持至少 1 Mbit/s 的密钥生成速率，以满足高速数据传输的需求。
- 量子密钥长度：量子密钥长度应至少为256位，以保证足够的安全性。
- 系统吞吐量：量子城域网应支持至少 1 Gbit/s 的数据传输速率，以满足大规模数据传输的需求。
- 资源动态调节能力：系统应能够在1 min内完成资源的动态调节，以快速响应用户需求的变化。
- 系统可用性：量子城域网的系统可用性应达到99.99%，以保证服务的连续性和稳定性。

2　关键技术

2.1　量子密钥分发协议

量子密钥分发（QKD）是最先实用化的量子通信技术，是量子通信的重要方向。量子密钥分发可以在空间分离的用户之间以信息理论安全的方式共享密钥，这是经典密码学无法完成的任务。

量子密钥分发的安全性是以物理原理为基础的，其基本方法是使用量子态来编码信息，通过对量子态的制备、传输和检测来达到安全分发随机数，即密钥的目的；对于量子态的编码、传输和测量方法的规定，称之为量子密钥分发协议。

量子密钥分发协议有多种，总体而言其安全性都基于以下量子物理原理。

（1）单量子不可再分。量子是物理量变化的最小单元，单个量子不可分割。量子密钥分发若采用单个量子（通常为单光子）作为信息载体，则攻击者无法通过窃取单量子的一部分并测量其状态的方法来获得密钥信息。

（2）未知单量子态无法精确测量。根据不确定性原理，量子的一对非对易物理量不能被同时测准。在量子密钥分发双方随机选择非对易物理量的其一进行编解码时，攻击者即使截取了量子信号，也无法有效测准单量子的状态。如果攻击者根据测量结果重新制备一个量子发送给接收方，将不可避免地改变单量子状态，导致解码结果与编码不一致。量子密钥分发双方可通过检测误码率来判断攻击行为及其强度，并在后处理中进行消除。

（3）未知单量子无法精确复制。量子相干叠加（同时处于多种状态）的特性使得不存在通用的方法获得任意未知单量子的多个精确一致拷贝。在量子密钥分发双方随机调制单量子态时，如果攻击者试图在截获量子信号后复制多个拷贝，将不可避免地导致复制态与初始态存在偏差，进而导致解码结果与编码不一致，量子密钥分发双方同样可进行检测发现和后处理消除。

以上述物理原理为基础，目前对于一部分量子密钥分发协议，如BB84、E91、MDI-QKD协议等，已经给出了严格的数学推导，可证明其信息理论安全性。量子密钥分发协议相对传统密钥分发协议在安全性方面有以下优势：量子密钥分发的安全性基于如上所述的量子力学基本原理，不依赖于对计算复杂性的要求和假设，其安全性和理论完备性能够得到充分保证；即使在量子计算技术成熟的条件下，其密钥分发过程也具有可

靠的安全性。量子密钥分发可以有效应对计算技术以及量子计算飞速发展给传统密码体系带来的严重威胁。

2.2 密钥中继技术

通过量子密钥生成，形成点对点量子密钥分发，受量子密钥生成的距离和配对数量限制，采用密钥中继技术，将点对点量子密钥再次分发形成多点对多点的密钥。密钥中继原理如图2所示。

中继原理：（1）节点A首先将Kr和Kab进行异或，得到（Kr⊕Kab）并将其传输给节点B；（2）节点B将收到的（Kr⊕Kab）与（Kab⊕Kbc）异或得到（Kr⊕Kbc）后传输给节点C（此处无生成Kr的过程）；（3）节点C、D重复节点B的操作，最后将Kr传输到节点E；（4）节点E将收到的（Kr⊕Kde）与Kde异或得到Kr。

中继安全性说明：（1）量子密钥分发网络中采用的是一次一密异或的密钥中继方式；（2）中继节点不存储明文密钥；（3）中继节点存储与两侧相邻节点之间的量子密钥的异或密钥，如节点B存储的为（Kab⊕Kbc），即节点B不知道Kr。

密钥中继技术使得任意两点均具有共享的密钥对，摆脱了量子密钥生成时对距离的限制，使得组建远距离量子密钥分发网络成为可能。

2.3 量子组网方式

量子密钥分发网络支持星形拓扑、环形拓扑、网状拓扑、链形拓扑等多种组网方式，本文根据用户节点分布情况，综合网络的健壮性和接入方便性，选择骨干环形+接入星形的混合组网方式。

城域范围内，通过在集控站/接入站/中继站部署若干设备，使该站点可与多个用户节点进行星形拓扑结构组网，灵活实现该集控站/接入站/中继站覆盖范围内用户节点的接入。星形拓扑结构由一个中心节点（即集控站节点或接入站节点）和若干分布在一定范围内的用户节点构成，主要用于城域网范围内，未超过量子密钥分发终端成码极限。

环形拓扑结构中，全部节点设备线路构成环形，集控站节点、接入站、中继站节点和用户节点组成环状网络，每个节点量子密钥分发终端均可同两个邻接节点进行量子密钥分发，并通过密钥管理系统的动态密钥中继路由功能，用户节点可通过两条中继路由实现量子密钥共享。

2.4 量子加密技术

（1）传统加密实现方式

传统加密包含对称和非对称加密体系，对称加密一般有两种实现方法，一种是由多名机要员送密码本，这种方式的密码本更新频率不会很高；另外一种方式是采用非对称加密体系传输对称密钥，而非对称密码本身是基于计算复杂度构造的加密算法，从理论上存在被破译的可能。

（2）量子加密实现方式

量子加密目前有两种实现方式，一种是基于量子密钥分发网，一种是基于量子密码服务平台。

量子密钥分发网产生对称的真随机量子密钥，量子密钥存储在量子密钥管理终端中，量子加解密设备从量子密钥管理终端获取量子密钥，结合密码卡中采用的加密算法（国密或传统加密

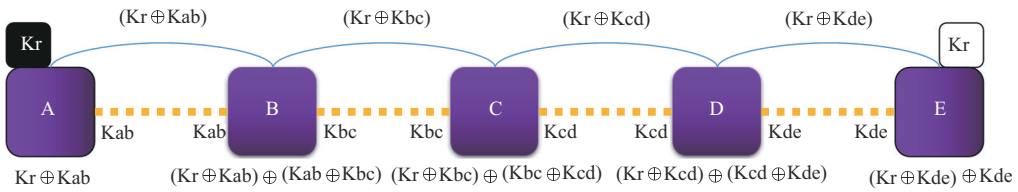

图2 密钥中继原理

算法），对数据进行加密。

量子密码服务平台可基于量子密钥分发技术，将量子密钥扩展至各类前端设备，保证设备在身份认证、数据传输等全流程的数据安全性。

（3）量子加密和传统加密的区别

量子加密与传统加密均可采用国密或传统加密算法，本质区别在于密钥，量子密钥具有真随机特性，加密方式采用量子密钥+国密（传统）加密算法；传统加密采用伪随机密钥+国密（传统）加密算法。

3　架构设计

针对现有场景下技术不足的问题，本文通过设计一种基于量子城域网架构承载的城市数字化底座服务的虚拟化云架构部署面向多租户的量子密钥管理服务系统，实现量子密钥管理应用方法和平台的优化，提供量子云密钥管理与安全服务系统的按需服务并纳入政务云服务目录。在日常运营方面，系统初次配置安装后，可根据使用情况动态调节包括计算资源、内存资源、存储资源等资源的使用，在用户量增加后，可在无须增添物理资源的情况下，方便快捷地提高量子云密钥管理与安全服务系统的性能。

3.1　量子密钥管理服务系统

基于城市数字化底座服务的虚拟化的量子云密钥管理与安全服务系统包括量子云密钥管理服务和量子云资源管理服务两个模块。

量子云密钥管理服务是对量子密钥管理系统的虚拟化。其运行状态上报给量子云资源管理服务进行资源的动态调节。量子密钥管理服务系统模块设计如图3所示。

量子云资源管理服务向量子云密钥管理与安全服务系统、网络内所有数据中心的量子密钥虚拟管理资源池以及池内虚拟设备和量子密钥加密资源池以及池内设备的信息上报接口收集包括CPU、内存、存储等运行状态信息，根据所配置的规则进行判断和决策。

执行模块对一定时间内资源占用超过阈值的虚拟设备的资源进行调整，资源操控的方式包括以下两种。

（1）在资源池尚有充足空闲资源的情况下，直接对资源进行调节。

（2）在量子云密钥管理与安全服务系统或资源池空闲资源不足的情况下，向政务云云管平台申请资源弹性伸缩进行调节。

3.2　量子云密钥资源分配流程

多租户环境下，新增用户初始量子云密钥资源分配流程，如图4所示。

<table>
<tr><td colspan="5">量子云资源管理服务</td></tr>
<tr><td></td><td>状态信息收集和监控模块</td><td>规则配置模块</td><td>判断和决策模块</td><td>执行模块</td></tr>
<tr><td rowspan="3">量子云密钥管理与安全服务系统资源管理</td><td>CPU状态信息收集</td><td rowspan="3">规则配置模块</td><td rowspan="3">判断和决策模块</td><td rowspan="3">执行模块</td></tr>
<tr><td>内存状态信息收集</td></tr>
<tr><td>存储状态信息收集</td></tr>
<tr><td rowspan="3">量子密钥虚拟管理资源池资源管理</td><td>CPU状态信息收集</td><td rowspan="3">规则配置模块</td><td rowspan="3">判断和决策模块</td><td rowspan="3">执行模块</td></tr>
<tr><td>内存状态信息收集</td></tr>
<tr><td>存储状态信息收集</td></tr>
<tr><td rowspan="3">量子密钥加密资源池资源管理</td><td>CPU状态信息收集</td><td rowspan="3">规则配置判断</td><td rowspan="3">判断和决策模块</td><td rowspan="3">执行模块</td></tr>
<tr><td>内存状态信息收集</td></tr>
<tr><td>存储状态信息收集</td></tr>
</table>

图3　量子密钥管理服务系统模块设计

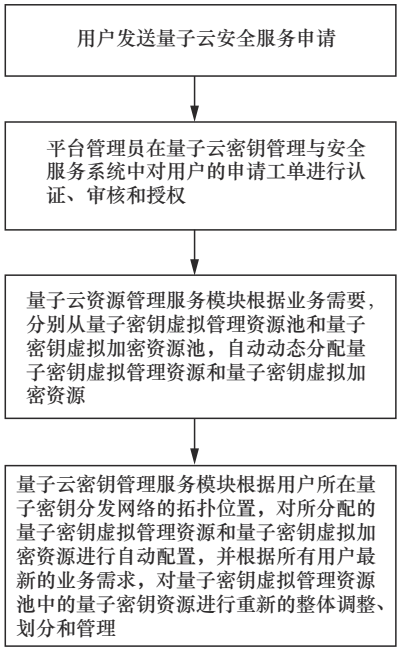

图4　量子云密钥资源分配流程

量子密钥管理资源池可根据政务统一管理平台的服务请求，配置一台或多台虚拟量子密钥管理设备，每个虚拟量子密钥管理设备向上可根据需要连接一台或多台量子密钥分发设备获取、管理和存储量子密钥，向下根据需要连接一台或多台虚拟量子密钥加密设备提供量子密钥进行加密。

量子密钥管理资源池的虚拟量子密钥管理设备，由量子云密钥管理与安全服务系统的量子密钥管理服务进行量子密钥分发流程、中继流程和应用管理。量子密钥管理资源池本身和所有虚拟量子密钥管理设备的运行状态上报给量子云密钥管理与安全服务系统，由量子云资源管理服务进行资源的动态调节。

4　验证部署

4.1　平台网络现状

以某省城市数字化底座服务平台为例，依托两家运营商，基于双数据中心同时构建双活云平台，共包含4个云数据中心，每个机房均包括互联网区和政务外网区，两个区互相隔离，只能通过网闸摆渡数据。其中政务外网网络为单独建设的一张专网，规则上不能与外网直接连接。平台网络现状如图5所示。

数据路由规则如下。

- 不同机房但同运营商，政务外网区和互联网区间可通过光纤直接通信。
- 不同运营商，政务外网和互联网之间通过各自网络区进行通信。
- 政务外网区通过专网与委办局进行数据通信。
- 互联网区通过互联网与公众进行数据通信。

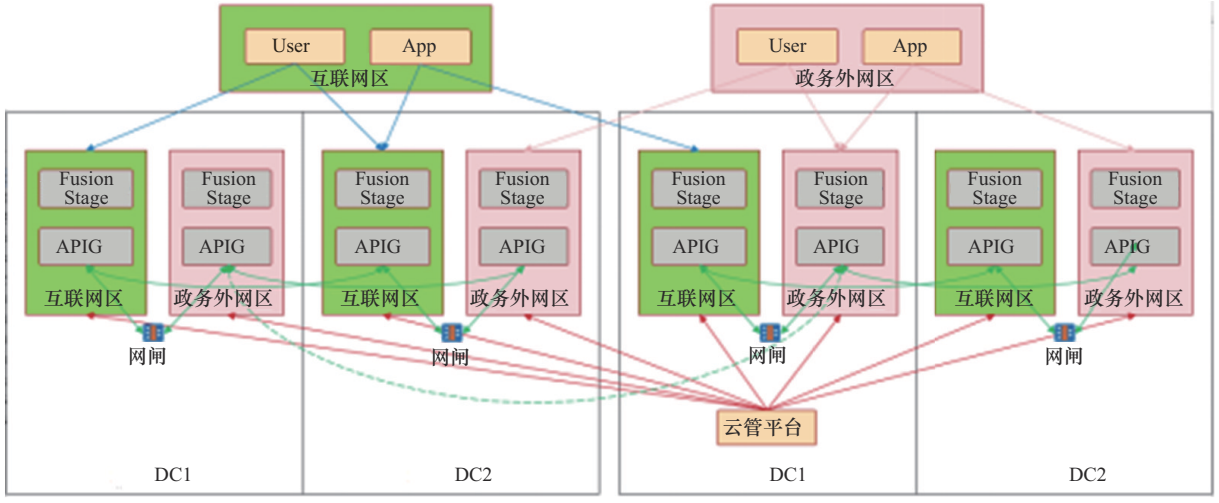

图5　平台网络现状

4.2　平台部署设计

为了简化管理，方便实施，以及实现量子城域网资源的高效利用，使用了虚拟化平台统一归集的思路对城市数字化底座平台量子保密服务进行了优化改造测试。在 4 个数据中心 DC 机房间的信息交换及备份使用量子密钥分发产生的量子密钥进行加密。整体采用网络分层架构，分为经典的数据传输网和量子通信网络，在云平台数据中心 4 个 DC 的出口网关、各业务单位的出口网关上分别接入并旁挂一台量子安全加密路由器设备，量子城域网服务部署设计如图 6 所示。

量子密钥管理服务系统作为量子安全通信网络的中枢控制，综合考虑网络内的节点在线、量子密钥分布应用层需求路径限制等因素，在城市数字化底座平台上部署量子云密钥管理与安全服务系统，并对接云管平台实现资源池的动态调控。按照一定规则控制网络内各节点间的量子密钥分发流程和量子密钥中继流程，进而实现全网量子密钥的最优分布。

城市数字化底座平台作为一个多租户的数据共享服务平台，涉及多个方面的数据汇总，在数据汇聚过程中，结合量子密钥分发的高安全性，面向委办局租户等应用单位在数据源端与目的端之间构造安全通道来进行数据传输。在云计算数据中心的出口网关、各业务单位的出口网关上分别接入并旁挂一台量子安全加密路由器设备，如图 7 所示。

数据中心 DC 之间通过资源池内的虚拟量子密钥管理和加密设备进行云间量子加密安全传输，数据中心通过虚拟量子密钥管理和加密设备，与 N 个委办局租户的物理量子密钥管理和加密设备进行量子加密的接入安全传输。所有云上系统与虚拟设备，均可进行 CPU、内存和存储资源的自动动态调控。

5　结束语

本文通过在城市数字化底座服务中融合量子城域网，实现了量子保密服务面向多租户服务的量子云密钥管理的优化改造测试，为政务服务数据的传输与存储提供具有真随机特性的量子密钥，通过对密钥权限进行管理，控制信息的访问权限，提高了数据传输的安全性，加强了量子城域网与城市数字化底座云服务的深度融合，为城市数字化底座云平台提供具备基于信息论理论基础的无条件安全特性和长期安全性数据通信支撑，进一步完善了城市数字化底座云整体信息化

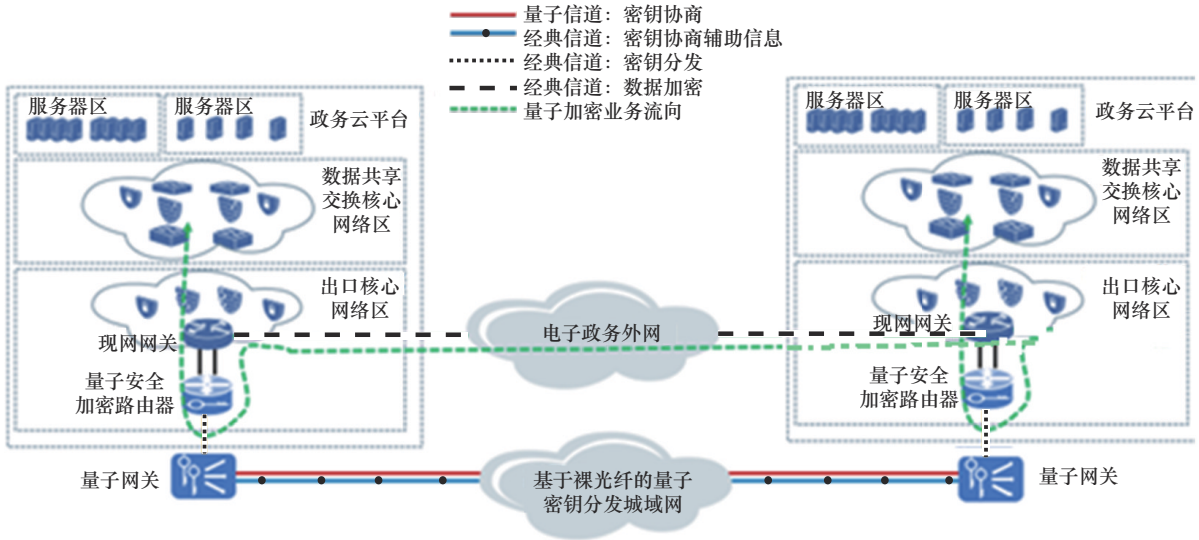

图 6　量子城域网服务部署设计

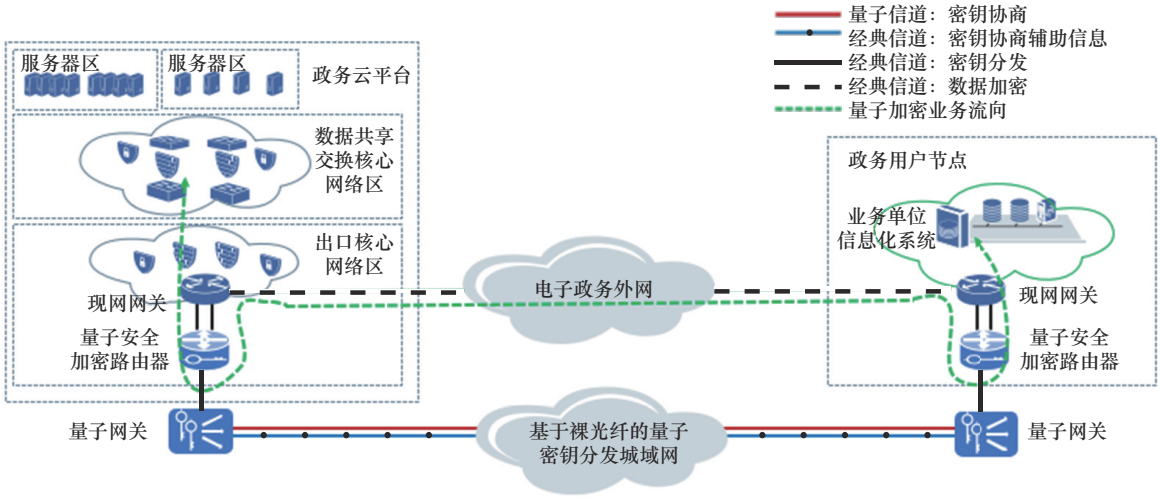

图7　用户节点量子城域网数据传输

建设体系和信息安全保障体系。

此外，量子城域网可以为城市各行各业数字化转型提供安全密钥服务，满足各领域用户对信息安全的高等级需求。满足前端设备使用过程中的数据安全需求，基于广域网量子密钥分发技术，将量子密钥或量子随机数通过离线方式充注给终端的安全模块，扩展至各类前端设备，通过独特的架构设计和算法体系，保证移动电话、笔记本等移动终端、网关产品及各种物联网终端全流程的数据安全性，确保数据和信息在传输过程中实现“密钥分发不可窃听，信息加密不可破译”。

未来随着QKD组网技术成熟，终端设备趋于小型化、移动化，QKD还将扩展到电信网、企业网、个人与家庭、云存储等更广阔的应用领域[2]；长远来看，随着量子卫星、量子中继、量子计算、量子传感等技术取得突破，通过量子通信网络将分布式的量子计算机和量子传感器连接，还将产生量子云计算、量子传感网等一系列全新的应用。

参考文献：

[1] 中国电信股份有限公司上海分公司, 上海中创产业创新研究院. 上海量子科技产业发展白皮书（2024）[R]. 2024.

[2] 中国通信标准化协会. 量子保密通信技术白皮书[R]. 2019.

[作者简介]

蔡敏（1978–），女，中国电信股份有限公司上海分公司政企支撑中心二级专家、高级工程师，主要研究方向为IP网络技术、5G2B、物联网和移动分组域等。

华静（1978–），男，中国电信股份有限公司上海分公司政企事业群一级专家、高级工程师，主要研究方向为网络安全、IP网络设计、云计算、数据中心相关技术。