# 量子通信技术在加密专线场景的应用研究

Research on Application of Quantum Communication Technology in Dedicated Encryption Line Scenarios

赵春旭，周彦韬，屈文秀，王泽林，王光全（中国联通研究院，北京 100048）
Zhao Chunxu，Zhou Yantao，Qu Wenxiu，Wang Zelin，Wang Guangquan（China Unicom Research Institute，Beijing 100048，China）

**摘　要：**
首先介绍了量子密钥分发（QKD）、后量子密码（PQC）以及量子随机数发生器（QRNG）等量子通信相关技术，并介绍了在网络不同层级的量子加密专线场景的融合创新方案。最后，介绍了中国联通基于上述几种量子通信相关技术所实现的面向不同量子加密专线场景的高安全、低成本、灵活组网的软硬管道多种解决方案，形成“通密一体化”服务能力，助力量子通信产业应用落地

**关键词：**
量子通信；后量子密码；量子加密专线
**doi：**10.12045/j.issn.1007-3043.2025.10.006
**文章编号：**1007-3043（2025）10-0030-06
**中图分类号：**TN914
**文献标识码：**A
**开放科学（资源服务）标识码（OSID）：**

**Abstract：**
It introduces some quantum safe technologies such as Quantum Key Distribution （QKD），Post-Quantum Cryptography （PQC），and Quantum Random Number Generators （QRNG）. It also presents integrated innovation solutions for quantum-encrypted private line scenarios across different network layers. Finally，it elaborates on China Unicom’s diverse solutions for various quantum-encrypted private line scenarios. These solutions offer high security，low cost，and flexible networking through both soft and hard pipelines，forming a comprehensive “encryption and communication integration” services capability that supports the practical application of quantum communication in the industry.

**Keywords：**
Quantum communication；Post quantum cryptography；Quantum encryption dedicated line

**引用格式：**赵春旭，周彦韬，屈文秀，等. 量子通信技术在加密专线场景的应用研究[J]. 邮电设计技术，2025（10）：30-35.

## 0 引言

上世纪90年代以来，量子调控技术的进步使人类可以对光子、原子等微观粒子进行主动的精确操纵，从而能够以一种全新的方式利用量子规律，使得量子技术与信息技术得以深度融合，促进了面向无条件安全的保密通信、超强的计算能力、突破经典极限的精密探测等量子信息技术的蓬勃发展。量子调控技术的进步和发展，使其可以对微观体系的量子态进行精确的观测与调控，以量子计算、量子通信、量子测量等技术为代表的第2次量子革命正在到来。

日前网络安全环境日益复杂，影响网络安全的因素也越来越多，应用系统正面临着加密算法种类繁杂和密码安全强度不足等问题，信息加密的重要性日益显著，加密技术被广泛应用于身份认证、数字签名、信息加密等业务环节。面对复杂的网络安全环境，密钥在传输、更新、使用和存储等环节面临安全风险，一旦密钥被窃取或破解，加密技术就失去了其应有的保障作用。为了应对安全威胁，国内外专家学者提出了量子通信和后量子密码等技术，并已大力开展了相关技术的标准化和产业化研究。

本文将从量子通信与后量子密码等技术入手，介

收稿日期：2025-09-16

绍其在量子加密专线场景的需求和应用场景，并对通密一体化解决方案进行探索。

## 1 量子密钥分发技术（QKD）

量子密钥分发（QKD）是最先实用化的量子信息技术，是量子通信发展的重要方向[1-3]。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。量子密钥分配以量子态为信息载体，基于量子力学的测不准关系和量子不可克隆定理，通过量子信道使通信收发双方共享密钥，是密码学与量子力学相结合的产物。QKD 技术在通信中并不传输密文，只是利用量子信道传输密钥，将密钥分配到通信双方，保证了密钥分发过程的安全性，以供应用两端业务通信时加密使用。

QKD技术可以根据量子态光源是否存在纠缠，分为制备—测量类协议和基于量子纠缠的协议。当前实现商用化的设备一般使用制备—测量类协议。另外，为弥补实际系统中的安全漏洞，提升系统的安全性，近些年开展了测量设备无关的量子密钥分发协议的研究工作[4]。基于量子纠缠协议的QKD在实现多用户组网方面有其优势，但目前尚未实现产业化突破。另一方面，QKD协议也可以根据光源及编码方式的不同，分为离散变量量子密钥分发（DV-QKD）协议和连续变量量子密钥分发（CV-QKD）协议等[5-6]。前者将信息编码在单个光子上，并用单光子检测器进行检测；后者将信息编码在互不对易的正则分量上，采用相干检测器进行检测，2种QKD方案的无条件安全性均已得到充分证明。此外，近些年双场协议量子密钥分发（TF-QKD）得到了迅猛发展，可以实现长距离远程的密钥分发，是未来技术发展的重要方向[7-8]。

结合量子密钥分发技术和对称加密算法可以实现高安全的量子加密通信线路，以形成量子加密通信网络。国内外已开展了多项量子加密通信网络的实验及工程建设[9-11]。我国作为率先部署大规模量子加密通信网络的国家，已构建了总长超过1万km，覆盖京津冀、长三角、粤港澳大湾区、成渝、东北等区域的国家广域量子保密通信骨干网络以及多个重点城市的量子城域网。为了推动量子保密通信网络的进一步发展和产业链成熟，业界正在尝试建立完整的网络运营模式，由专业的量子加密通信网络运营商构建广域量子保密通信网络基础设施，为各行业的客户提供稳定、可靠、标准化的量子安全服务。

## 2 后量子密码技术（PQC）

密码学是动态发展的，随着现代计算机以及密码分析学的发展，密码算法的安全性会随时间而逐渐降低。当密码算法无法满足数据安全需求时，就需要向新的密码算法迁移。随着量子计算技术的迅速发展，传统密码学的安全性面临前所未有的挑战。量子计算凭借其强大的并行计算能力，能够在某些情况下显著减少密码算法的破解时间，威胁到现有的安全体系。因此，在密码学领域，探索后量子密码（PQC）的技术路线，旨在设计能够抵抗量子计算攻击的新型密码方案。

后量子密码算法的数学原理主要基于量子计算难以解决的数学问题，如基于格的密码学、多变量密码学、编码密码学和哈希密码学等。这些算法在设计时就考虑到了量子计算的威胁，因此能够在量子计算时代保持通信的机密性和完整性。基于格的密码算法因其多功能性和高效性，成为目前后量子密码学研究的主流方向之一。

目前国内外正在广泛开展PQC技术的研究和标准化工作。美国国家标准与技术研究所（NIST）自2015年起启动了后量子密码的算法筛选和标准化工作。经过多轮筛选评估，在2023年发布了4种后量子密码算法的标准草案，包括用于公钥加密的CRYSTALS-Kyber算法和用于数字签名的CRYSTALS-Dilithium、Sphincs+以及FALCON算法[12]。在2024年8月正式发布了首批3项PQC标准：FIPS 203、FIPS 204、FIPS 205，分别应用于密钥封装（KEM）以及数字签名，并在2025年3月加入备选方案HQC，为全球网络安全设定了新的标准。

在后量子密码领域，欧美等国家无论是迁移方案的准备还是后量子密码领域的研究成果，与我国相比均走在发展的前列。随着PQC标准初具雏形，各国先后提出后量子迁移规划及指南，同时也加快推进PQC产业化，抢占先机[13]。

## 3 量子随机数发生器（QRNG）

作为密码学的核心，密钥的质量主要依赖于随机数的不可预测性和不可重复性，对于随机数的不可预测性有极高的要求。传统的随机数发生器大多基于经典物理过程，无法建立严格的先验模型证明其随机性。量子随机数发生器是一种利用量子力学的不可

预测性来生成真随机数的装置，可以用来为信息安全领域提供高质量的随机数源[14]。

将量子随机数发生器作为硬件安全模块（Hardware Security Module，HSM）来提供密钥源，并构建具有高安全性、灵活、低成本的密钥管理平台，对外提供密码及数据加密服务，是量子随机数发生器的一种常见的用法。一般来说，量子密钥管理平台是一个统一的平台，能够管理和协调与密钥相关的操作，包括密钥生成、导入、查询、编辑、存储、备份、分发、吊销、启用、禁用、加解密、签名、验签等。平台可以集成各种量子设备和协议，实现对密钥生命周期的全面管理。平台可划分为量子密钥制备层、量子密钥管理层和量子密钥应用层。终端侧的量子密钥接入可通过结合国密等算法进行平台在线分发，或通过离线注入的手段以进一步保证安全性。特别是，采用在线分发的方式，可以与PQC算法进行深度的融合，提升其安全性。

量子密钥管理平台的用途广泛，具有灵活便捷、支持海量终端的特点，更适合在边缘接入和低成本加密等场景使用。

## 4 量子加密专线场景

QKD和PQC等技术实现了抗量子计算的密钥安全交换，可以为通信双方之间建立高度安全的对称密钥，并结合对称加密算法实现数据加密通信，现阶段数据加密传输依然是量子密码的应用聚焦点。在数据加密传输中，出于对系统安全性的考虑，通常是在原有加密专线的基础上进行量子安全的升级改造，以形成高度安全的量子加密专线。

开放式系统互联通信参考模型（Open System Interconnection，OSI），定义于ISO/IEC 7498-1，是国际标准化组织（International Organization for Standardization，ISO）制定的一个用于计算机或通信系统间互联的标准体系，使各种计算机在世界范围内互连为网络，一般称为OSI参考模型或七层模型。它是一个七层的、抽象的模型体，不仅包括一系列抽象的术语或概念，也包括具体的协议。在OSI网络不同层级结合QKD及PQC等量子技术，可以实现多种量子加密专线使用场景。如物理层的OTN协议，数据链路层的以太网协议，网络层的IP以及更上层的SSL/TLS协议等，均可进行量子加密的改造，提升加密专线安全性。

### 4.1 OTN量子加密专线

在运营商主营业务的OTN专线中，可以将量子加密与OTNSec协议进行融合，采用量子密钥实现源宿节点之间的双向OTN业务量子加密传输与解密接收，这是当前较为主流的研究方向。当前国内CCSA ST7量子通信与信息技术特设任务组正在进行OTNSec相关行业标准的制定，主要包括对基于OTNSec协议的量子保密通信应用设备的技术协议、功能要求和性能要求以及相应测试方法进行了规范。OTNSec是对现有OTN负载帧中包含的OPUk数据进行加密，在ITU国际标准中已有相关的定义。可以将OTN设备进行量子密钥的对接适配，使其能够获取外部输入的量子密钥以用于对线路侧OPUk载荷的加密。此外，OTN设备的量子密钥也可以在客户侧使用，在进行OTN成帧封装之前进行以太网等信号的加密，再送入线路侧进行传送。

### 4.2 IPSec量子加密专线

在传统VPN方案中，IPSec是加密专线广泛使用的加密协议。IPSec作为现代网络的基础加密框架，用于在网络层提供机密性、完整性和认证。在量子威胁背景下，IPSec协议也需要通过协议扩展、混合模式和产业化落地，来抵抗量子计算的攻击。IKE是一种用于两方在互联网层建立安全通信通道的协议，它是IPSec套件中用来进行密钥交换的部分。

在IPSec量子加密专线场景中，可以将IKE密钥交换过程生成的密钥替换为QKD或PQC技术产生的密钥。比如以量子密钥替换现有基于公钥算法分配的密钥，对传输数据进行加密，提升远程访问及应用数据传输的安全性。传统网关与量子密钥加解密方案的有机结合，既能够通过QKD技术解决现有经典保密通信系统中对称密钥安全分配及密钥窃听检测等难题，也能够满足经典通信协议，支持各类组网模式，在实际部署中对用户原有应用系统基本无影响。在PQC应用方面，IPSec协议所涉及的StrongSwan、Libreswan等开源实现已在主干分支中加入了Kyber/Dilithium算法的密钥封装和签名支持。国外部分企业已经在企业远程接入VPN中开展混合KEM测试，验证NIST算法的性能和互操作性。

### 4.3 SSL/TLS量子加密专线

TLS是一种客户端与服务器之间建立应用层安全通信通道的协议，从SSL协议演变而来。该协议一般采用密钥协商、预共享密钥等方案来分发主密钥，然后再由主密钥进一步计算出会话密钥，会话密钥则采用AES、DES等加密算法确保通信的机密性和完整性。

量子安全SSL/TLS VPN采用量子密钥替代原有的基于算法复杂度确保安全性的预共享密钥，可极大提升通信系统安全性。

量子安全SSL/TLS VPN常应用于安全接入等场景，可以通过量子密钥管理平台来支撑互联网或移动专线网络访问云的部分业务和公共区业务，量子密钥管理平台是此类访问的唯一接入通道。量子密钥管理平台可通过量子安全SSL/TLS VPN+量子安全U盾的方式，实现接入认证、授权管理、VPN接入、移动设备管理和移动应用管理等功能，为各类智能移动终端和远程办公用户提供可信的安全接入和实时的业务访问。在与PQC结合方面，IETF草案提出了在混合模式下使用TLS的密钥交换组件，如使用传统的ECDHE算法和后量子安全的算法如ML-KEM分别生成部分密钥，并通过连接的方式组合成一个整体，然后提供给会话密钥的密钥派生函数使用。

### 4.4 MACSec量子加密专线

MACSec是一种以太网链路层的安全协议，可以通过身份认证、数据加密、完整性校验、重播保护等功能保证以太网数据帧的安全性。与IPSec类似，它也具有自身的密钥交换协议并可与量子加密技术进行融合实现MACSec量子加密。

## 5 中国联通量子加密专线实践

量子加密专线可以采用通密分离、通密耦合以及通密一体3种模式（按照密钥的来源以及与加密应用设备的结合方式来划分）。通密分离是加密应用设备与密钥来源处于不同的安全域内，通过网络接口实现密钥到加密应用设备的传输。通密耦合是两者处于同一安全域内，密钥通过设备间的接口进行传输。通密一体是两者进行深度融合，处于同一设备域内，密钥通过设备内部的接口进行传输。

当前，量子加密专线通常需要2种信道：用于传输QKD信号的量子信道和传输加密数据的经典信道。其中量子信道传输的是经过衰减的光脉冲，是弱光信道，而经典信道传输的是经典光通信的强光信号。为了避免经典光信号对量子信号的串扰，量子通信通常使用独立的光纤来进行传输，从而导致对光纤资源的大量消耗。

为了避免对光纤资源的过度消耗，减少量子加密专线的建网成本，需要研究量子信号和经典光通信进行共光纤传输技术，这也是本文重点关注研究通密一体化方案的原因[15]。以QKD、PQC和QRNG技术为基础，结合网络不同层级的通信设备打造通密一体化产品，以实现面向不同安全需求及组网架构的高安全、低成本、灵活组网的软/硬管道量子加密专线解决方案。

如图1所示，通密一体化量子加密专线系统产品目前主要有4种方案，分布在通信网络不同层级，以满足不同区域、不同带宽和不同成本的各类场景需求。在主控中心通过中国联通OTN-CPE管控系统，IP专业管控系统以及量子密钥管理平台，即量子密钥云平

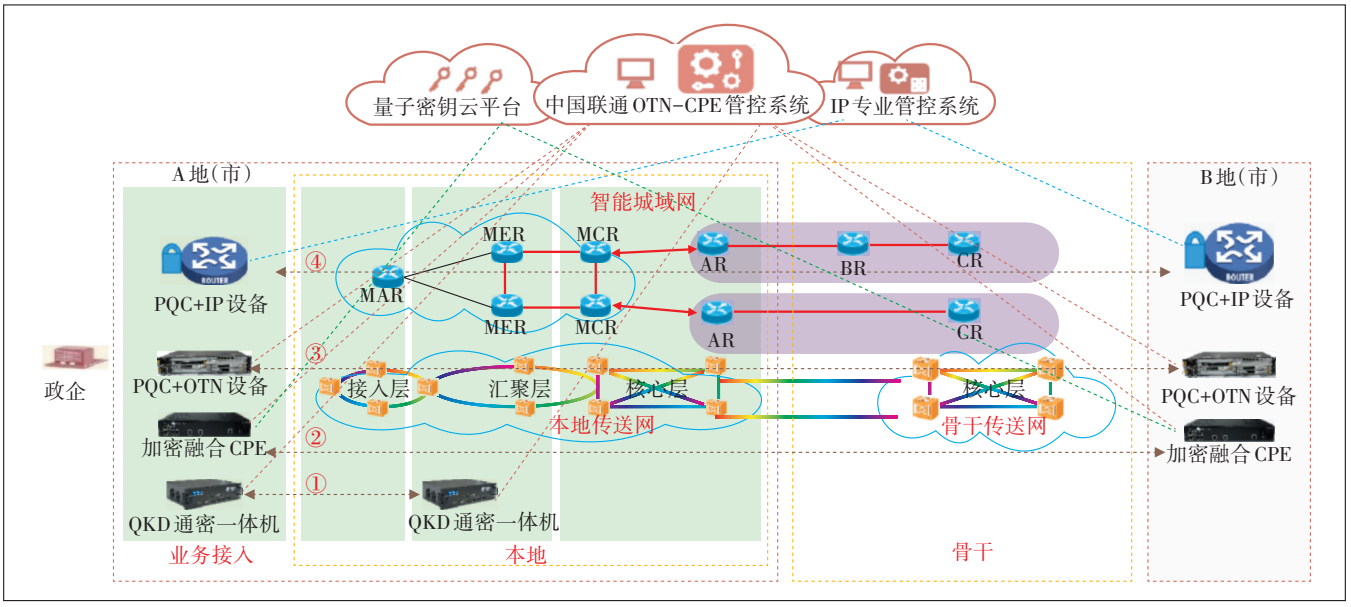


图1 量子加密专线系列产品组网示意

台对设备及量子加密专线业务进行管控。除了设备上的通密一体化融合，管控平台的融合也是未来业务发展的趋势。

在经典光通信设备与量子加密技术结合方面，首先基于QKD技术进行了融合创新，打造了国内首款深度融合的通密一体量子加密设备，采用的是中国联通拥有自主知识产权的G.698.4光通信设备。此设备是一种单纤双向波长自适应城域接入型波分复用（WDM）系统，主要面向超宽带城域综合接入应用场景。采用DWDM技术，提供波长级的全光接入。为了更好地实现共纤传输，选用了连续变量量子密钥分发技术（CV-QKD）。与离散变量量子密钥分发技术（DV-QKD）相比，其发射端和接收端不需要使用专用的激光源及单光子探测器，仅使用光通信常用光器件，可大幅降低成本。另外，CV-QKD的信号功率更高，更适合与经典光通信进行DWDM共纤传输。

图2所示为此款QKD融合光传输通密一体化设备的架构示意，主要包括连续变量量子密钥分发模块、业务加密及验签模块、光转换模块以及统一网管模块，实现了10G高速率业务的量子安全传输功能。此设备首次实现量子通信与经典通信的共网管功能，可接入中国联通自研管控平台，采用“一张网”管理界面，便于集中化运维。

当前，此产品实现了10G以太网业务加密功能。未来，将持续开发QKD与光通信设备的融合产品，打造OTN业务的线路侧加密能力，提升业务加密速率并进一步降低业务加密所引入的额外时延，不断丰富完善QKD技术在光通信产品的商用化能力。

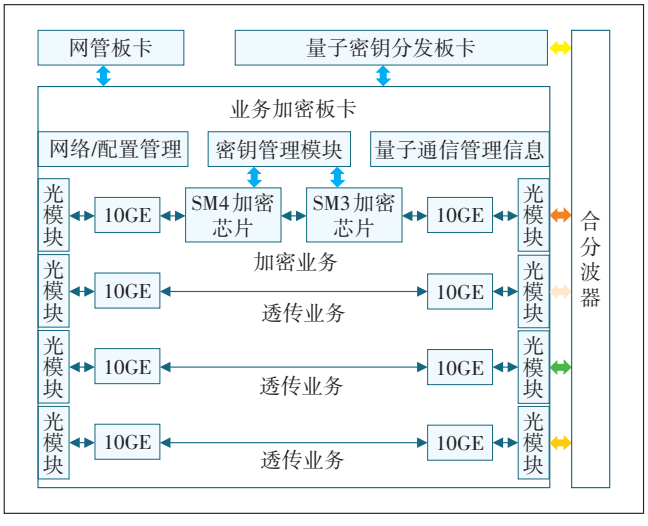


图2　QKD融合光传输通密一体化设备架构示意

如图3所示，我们还打造了通密一体后量子（PQC）光传输设备。该产品具备安全合规、轻量级、低成本、纳秒级延时等特性。此设备同时集成了量子随机数发生器以保障密钥生成以及协议安全性。同时，该设备还集成了国密安全芯片，实现板上密钥管理及关键信息存储的安全性。设备首次集成了后量子密码算法软硬协同加速器。在此基础上构造了一种适用于标准以太网的后量子安全协议，能够高效完成点对点的安全认证以及密钥交换。该协议可有效兼容现有的以太网数据包结构，易于快速集成以完成现网的安全改造。同时，设备还集成了国密SM4算法全流水硬件加速器，支持双向10G同步业务加解密功能，实现了真正的纳秒级加解密延时，能够应用于工控、金融、国防等对时延敏感的应用场景。

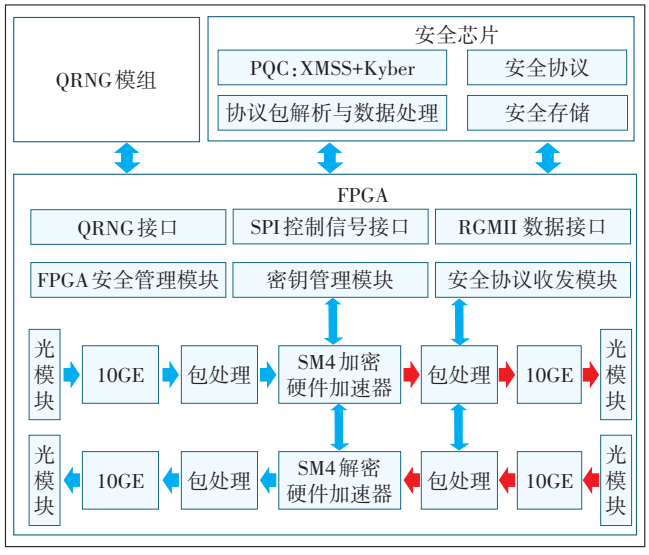


图3　PQC融合光传输通密一体化设备架构示意

如图4所示，为了应对低成本、灵活部署的量子加密专线需求，我们基于OTN-CPE设备打造了量子安全加密CPE终端设备。此设备结合基于量子随机数的量子密钥云平台，可实现百兆以下小颗粒量子安全加密专线业务快速开通。量子安全加密终端预置了量子随机数密钥与身份凭证，以实现平台侧对硬件设备的身份认证，保证终端的可信接入，并结合国密算法实现量子安全加密能力。此CPE加密终端应用于用户侧，可灵活接入中国联通政企精品网实现加密业务快速部署。

我们也将后量子密码技术应用于数据通信设备中进行融合创新，形成后量子安全网关产品。图5所示为PQC安全网关构建安全加密业务，实现用户端到

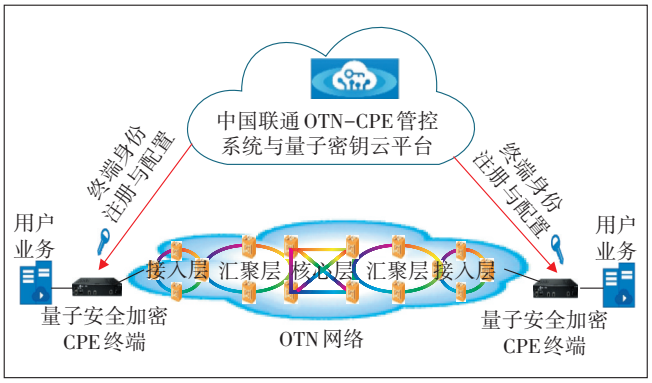


图4　量子安全加密CPE终端及组网示意

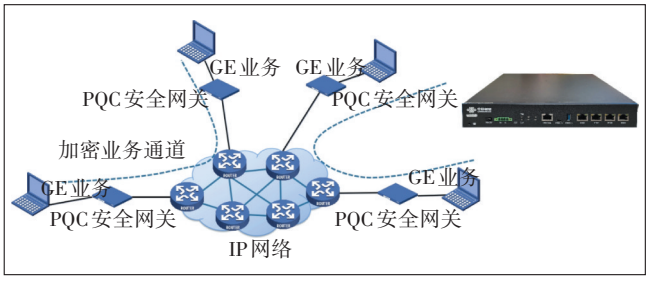


图5　PQC安全网关及组网示意

端加密的组网示意。此产品在构建安全VPN隧道的IPSec协议流程中，引入后量子算法与国密算法，提升了密钥交换安全性。产品同样集成了硬件加速器，实现了2.5G带宽的低时延业务加解密。同时，与光通信组网方案相比，此产品保留了三层交换功能的灵活性，可以满足大规模复杂组网的需求，适用于更加灵活的低成本量子安全互联场景。

## 6 结束语

本文介绍了量子加密通信中QKD、PQC和QRNG 3种关键技术及目前的研究现状，并进一步将其引入到量子加密技术应用最为重要的量子加密专线场景。在量子加密专线场景中，针对网络不同层级的不同安全协议均可进行量子加密的安全能力提升改造，以满足不同客户的实际需求。最后，介绍了中国联通在量子加密专线方向的探索与实践，中国联通打造了4款量子加密安全融合产品，实现安全通信的全面升级，以更高的速度、更强的安全性和更低的成本为各行各业的信息安全提供有力保障。

**参考文献：**

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore: IEEE, 1984: 175-179.

[2] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[3] 裴昌幸，朱畅华，聂敏，等. 量子通信[M]. 西安：西安电子科技大学出版社，2013.

[4] LO H K, CURTY M, QI B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[5] LEVERRIER A, GARCÍA-PATRÓN R, RENNER R, et al. Security of continuous-variable quantum key distribution against general attacks[J]. Physical Review Letters, 2013, 110(3): 030502.

[6] LEVERRIER A. Composable security proof for continuous-variable quantum key distribution with coherent states[J]. Physical Review Letters, 2015, 114(7): 070501.

[7] WANG S, YIN Z Q, HE D Y, et al. Twin-field quantum key distribution over 830-km fibre[J]. Nature Photonics, 2022, 16(2): 154-161.

[8] LUCAMARINI M, YUAN Z L, DYNES J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400-403.

[9] KIM T, SEAN K. Development of quantum technologies at SK telecom[J]. AAPPS Bulletin, 2016, 26(6): P2.

[10] PEEV M, PACHER C, ALLÉAUME R, et al. The SECOQC quantum key distribution network in Vienna[J]. New Journal of Physics, 2009, 11(7): 075001.

[11] RARITY J G, THOMPSON M G, ERVEN C, et al. UK quantum technology hub for quantum communication technologies (via York)[EB/OL]. [2025-02-17]. https://research-information.bris.ac.uk/en/projects/uk-quantum-technology-hub-for-quantum-communication-technologies.

[12] NIST. Migration to post-quantum cryptography quantum readiness: testing draft standards[Z]. U.S. Department of Commerce, 2023.

[13] 西电广研院. 后量子密码迁移白皮书(2024)[R/OL]. [2025-02-17]. https://www.cipheroncloud.com/upload/files/2024/6/fb59b3aab1faa61c.pdf.

[14] 周泓伊，曾培. 量子随机数发生器[J]. 信息安全研究，2017，3(1)：23-35.

[15] MAO Y Q, WANG B X, ZHAO C X, et al. Integrating quantum key distribution with classical communications in backbone fiber network[J]. Optics Express, 2018, 26(5): 6010-6020.

**作者简介：**
赵春旭，毕业于北京大学，高级工程师，博士，主要从事量子通信与高速光通信技术的应用研究工作；周彦韬，毕业于北京邮电大学，工程师，硕士，主要研究方向为光通信网络与量子通信新技术应用；屈文秀，毕业于北京邮电大学，高级工程师，博士，主要从事量子信息领域现网融合技术及产业化应用研究工作；王泽林，毕业于西北工业大学，教授级高级工程师，硕士，主要研究方向为IP、云网融合、算力网络、白盒开源等；王光全，教授级高级工程师，主要研究方向为光网络与量子通信。