OTN专线量子安全防护技术的研究与部署

Research and Application of Quantum-Secure OTN Private Line Technology

刘俊通[1],张世华[2],张 斌[3],刘 扬[2],余 涛[1],刘文慧[1](1.中国联通江西分公司,江西 南昌 330096;2.中讯邮电咨询设计院有限公司郑州分公司,河南 郑州 450007;3.江西省公安厅,江西 南昌 330096)

Liu Juntong[1],Zhang Shihua[2],Zhang Bin[3],Liu Yang[2],Yu Tao[1],Liu Wenhui[1](1. China Unicom Jiangxi Branch,Nanchang 330096,China;2. China Information Technology Designing & Consulting Institute Co.,Ltd. Zhengzhou Branch,Zhengzhou 450007,China;3. Public Security Department of Jiangxi Province,Nanchang 330096,China)

摘 要:

基于后量子密码学理论体系,创造性提出将SM4算法应用于OPUk层载荷的逐包加密机制,构建融合量子密钥分发与国密算法的量子安全光传送网。依托100G QKD量子OTN环网实验平台,实现百万级量子密钥的实时调度,加解密时延稳定控制在1 μs以内,密钥更新速率提升300%。同时,系统性论证量子安全光层的技术原理、设备迭代路线、现网部署方案及未来演进方向,为量子安全网络提供了理论支撑与实践范式。

关键词:

量子安全;光传送网;OPUk加密;抗量子攻击;密钥即服务

doi:10.12045/j.issn.1007-3043.2026.10.014

文章编号:1007-3043(2026)10-0082-05

中图分类号:TN918

文献标识码:A

开放科学(资源服务)标识码(OSID):

Abstract:

Based on the post-quantum cryptography theoretical system, a creative packet-by-packet encryption mechanism applying the SM4 algorithm to the OPUk layer payload is proposed, and a quantum-secure optical transport network integrating quantum key distribution and national cryptographic algorithms is constructed. Relying on the 100G QKD quantum OTN ring network experimental platform, real-time scheduling of millions of quantum keys is realized. The encryption and decryption delay is stably controlled within 1 μs, and the key update rate is increased by 300%. Meanwhile, the technical principles, equipment iteration routes, current network deployment schemes, and future evolution directions of the quantum-secure optical layer are systematically demonstrated, providing theoretical support and practical paradigms for quantum-secure networks.

Keywords:

Quantum security; Optical transport network; OPUk encryption; Quantum attack resistance; Key as a service (KaaS)

引用格式:刘俊通,张世华,张斌,等. OTN专线量子安全防护技术的研究与部署[J]. 邮电设计技术,2026(10):82-86.

0 引言

全球网络安全形势日趋严峻,据Cybersecurity Ventures统计,2025年全球网络犯罪造成的经济损失达10.5万亿美元,到2031年将增至12.2万亿美元[1];美国官方数据进一步印证了这一趋势:FBI互联网犯罪投诉中心2025年度报告显示,当年针对美国关键基础设施的勒索软件事件超过2 100起,医疗行业以278起居首;网络犯罪投诉量首次突破100万件,同比增长26%[2]。传统加密技术面临双重挑战。

a)量子计算威胁。IBM量子处理器已突破433量子比特,凭借其并行计算和量子叠加态特征,在处理复杂密码破解、分子模拟等任务时展现出指数级的计算优势[3]。Google Quantum AI团队披露其表面代码纠错协议已实现逻辑量子比特错误率为10^{-3}的工程突破[4]。

b)架构脆弱性。Gartner报告指出75%的光传送网(OTN)专线存在密钥泄露风险,其中34%源于硬件

收稿日期:2026-09-10

安全模块的固件缺陷[5]。中国信通院《2024数字安全白皮书》披露，部分电力调度系统使用的国密SM2证书链中，38%的中继节点未启用CRL校验功能[6]。

对于OTN网络，需要突破三重技术瓶颈，具体如下。

a）融合难题。融合量子密钥分发（QKD）与传统OTN协议栈兼容性不足，单光子调谐机制与OTN波分架构存在频谱冲突，亟需优化毫秒级密钥同步与噪声环境下密钥池分配的稳定性。

b）性能损耗。外置加密机引入5 μs以上的时延与光信号衰减，量子随机数生成诱发时钟抖动，无法满足金融级交易等高性能业务。

c）标准缺失。IETF缺少QKD over OTN互联规范，现有G.709标准未明确规定量子信道开销字节，运营商采用私有封装方案存在厂商锁区问题。

针对当前网络安全风险及OTN网络与量子加密融合的技术瓶颈，本文聚焦量子安全OTN专线的核心技术问题，从网络架构设计、关键技术研究、实验数据验证3个维度开展研究。

1 量子安全OTN架构设计

量子安全OTN专线是基于量子密码技术的光传输安全产品，面向客户提供超大带宽DC互联、政企OTN量子安全专线等场景解决方案，在OTN专线领域打造差异化能力，提升市场核心竞争力。本文采用管控—转发—密码三级架构实现量子安全OTN专线的搭建（见图1），其中，管控层依托SDN控制器实现全网资源智能调度，采用区块链技术构建可信认证机制；转发层基于OTN硬管道承载量子密钥分发信号，通过光业务单元（OSU）弹性管道实现业务流量的灵活适配；密码资源层部署量子密钥生成与分发设备，采用后量子密码算法实现传输数据加密。

a）管控层。该层由O/B域管理系统与多厂商网管平台构成，主要承担量子OTN业务的客户受理、服务开通及业务策略下发等管理职能。量子安全OTN运营平台通过北向接口实现开放互通，具备量子OTN网元全生命周期管理及网络资源可视化查询等关键运维能力。私有部署模式下无须集成电信运营支撑系统。

b）量子加密转发层。该层由端到端量子光传送网络节点构成，OTN设备通过集成定制化板卡的方式实现量子安全功能，实现协议透明的端到端加密传输，业务层无感知。

c）密码资源层。该层实现分布式密钥管理系统（KMS）的协同控制与统一管理，有效支撑OTN专线在本地业务、跨区域业务及跨省际业务场景下的量子密码服务能力。通过北向接口与量子安全OTN运营平台实现协议对接，提供密码资源状态监控与配置查询功能。

2 关键技术研究

2.1 量子密码服务模型

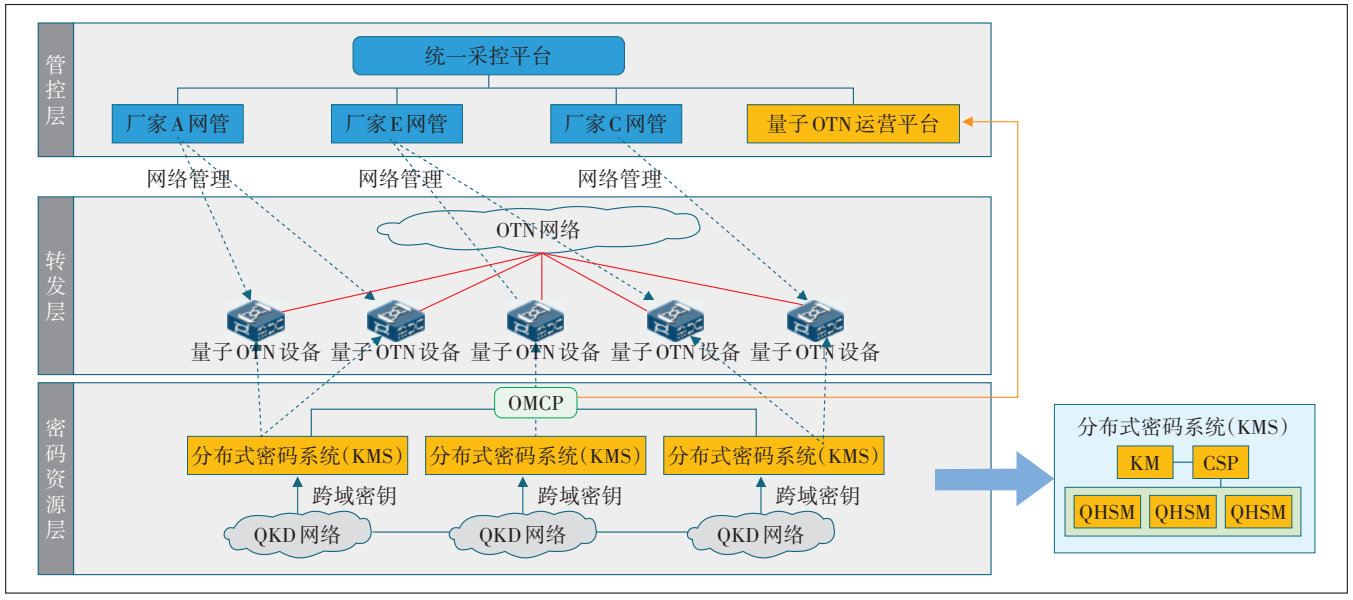


图1　量子OTN的网络设计架构

量子OTN密码服务模型如图2所示。基于量子OTN设备所属服务域的特性,结合网络架构与业务特征,通过智能分析引擎动态解析其适配的服务模式,主要包含以下3类。

a)域内服务。针对同一服务域内的量子OTN设备(如图2中A区域内的设备),量子密码服务系统启动域内服务机制。该模式依托服务域量子密钥资源池,通过双活架构的量子随机数发生器(QRNG)集群实现每秒TB量级的随机数生成能力,并结合三级缓存体系(内存缓存—固态缓存—磁盘阵列)完成密钥资源的智能预置与动态调配。

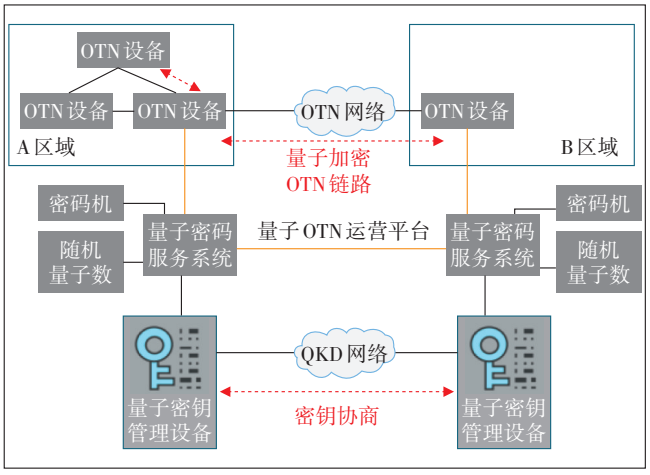


图2 量子OTN密码服务模型

b)跨域服务。对于分属不同服务域的量子OTN设备(如图2中的A区域与B区域的设备),由核心节点部署的分布式量子密码服务系统执行跨域服务机制。系统通过量子密钥中继网关与底层QKD网络互联,采用分段式密钥协商协议生成跨域对称密钥池,每日密钥更新容量可维持超过10^{15} bit,并基于区块链技术实现多域密钥资源的可信计量与审计追踪。

c)QKD服务。为满足特定用户群体的差异化需求,系统保留传统QKD直连组网方式的密钥获取通道。该模式支持BB84、E91等典型量子密钥分发协议,兼容光纤信道(单模/多模)与自由空间传输介质,提供从接入层(10 km)到干线层(1 000 km)的全场景QKD服务,最高可实现10 Mbit/s@25 dB信道损耗的密钥成码率。

2.2 OPUk层量子加密

本文创新设计光层—电层联合加密方案来实现OTN传输过程中在OPUk(Optical Channel Payload Unit)层的量子加密(见图3)。

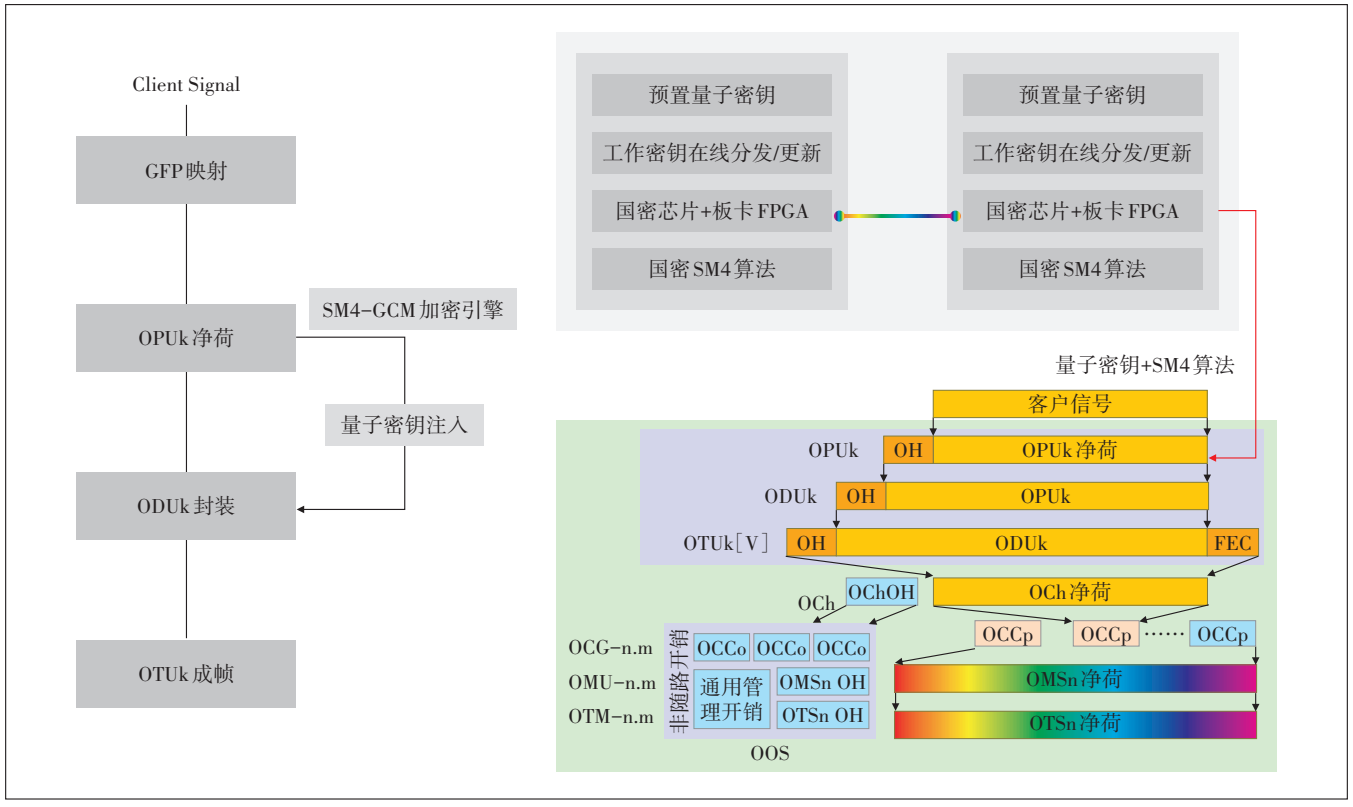


图3 量子OTN基于OPUk层的量子加密

2.2.1 净荷预处理（GFP映射）

采用ITU-T G.7041通用成帧规程作为封装标准，该国际标准定义了面向字节的同步映射机制，支持多种业务信号的灵活封装。

如图4所示，量子OTN净荷预处理的帧结构由4个核心字段构成。其中，PLI（Payload Length Indicator，2 B）用于明确指示后续Payload数据域的长度，确保接收端能精准划分数据边界；cHEC（Header Error Check，2 B）采用CRC-16算法对帧头部进行校验，实时检测传输过程中的比特翻转或头部篡改；Payload为可变长数据域（1~1 500 B），支持灵活适配不同业务的数据承载需求；tHEC（Tail Error Check，4 B）使用CRC-32强化校验，对完整数据帧进行二次验证。

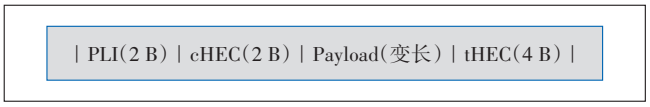


图4　量子OTN净荷预处理的帧结构示意

2.2.2 量子加密引擎

加密算法采用国密SM4-GCM模式，分组长度为128 bit，硬件加速字节置换算法，性能提升30%，支持动态随机化IV生成机制。密钥管理通过量子密钥分发（QKD BB84协议）获取长度为256 bit的密钥，采用后量子格密码（NTRU）加密体系。每帧独立密钥经QRNG强化，支持GHASH算法生成256 bit MAC认证标签。密钥生命周期含12 h自动轮换策略，废弃密钥量子被擦除销毁。

2.2.3 密钥分发系统

QRNG基于单光子偏振态测量，熵值≥0.999。QKD网络采用相位编码BB84协议，误码率<0.5%，通过SM4/SM9国密算法实现抗量子攻击的端到端加密。

3 实验网数据验证

3.1 实验网架构概述

在某省联通搭建量子OTN实验网（见图5），其拓扑如下。

a）3个核心节点，采用核心光传送网设备，分别部署在不同的数据中心，形成三角形骨干架构。

b）6个接入节点，部署光终端设备，通过多模光纤与核心层建立双路由保护连接，覆盖不同的区域业务。

c）部署量子密钥分发网络设备，构建连接核心节点的闭环系统，采用波分复用技术实现量子信道与业务信道同纤传输。

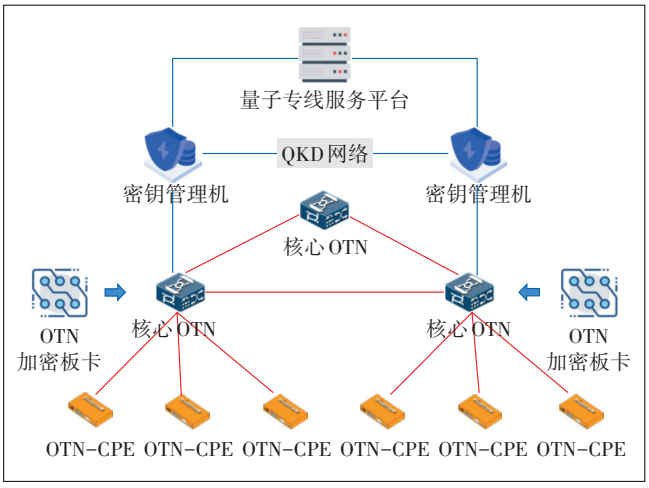


图5　量子OTN实验网

d）采用分布式服务器集群部署量子专线服务平台，包含密钥协商模块、网络拓扑管理单元和实时监控系统，支持与现有网管平台接口对接。

本实验网采用通密协同方案，该方案可平衡安全与灵活性。OTN设备与独立的QKD设备协同工作，密钥通过独立的量子网络进行分发，安全性高，兼容性强。当然，在OTN业务板卡与CPE之间存在着业务未被加密的隐患，数据在进入运营商核心网络之前（用户侧到CPE段）仍存在暴露风险，这类暴露风险仅存在单个的分支网点，产生的危害及影响范围极小。

实验网采用分层架构设计，核心层实现10 Gbit/s业务承载，接入层支持GE光接口，量子密钥生成单元与业务加密网关采用硬件级联动机制；网络管理系统集成自动化配置功能，支持量子密钥池的动态分配策略，可根据业务等级实现差异化密钥更新周期，最小粒度达到分钟级；传输层采用开放式光层架构，预留扩展接口支持未来量子中继设备的接入，光纤链路部署偏振稳定控制装置以保障量子态传输的稳定性；安全体系实现量子密钥全生命周期管理，涵盖生成、分发、存储、更新及销毁环节，密钥注入过程采用物理隔离通道，核心密码机通过三级等保认证。

基于以上实验网络完成多维度验证测试，包括72 h连续密钥生成测试（平均成码率为7.8 kbit/s±5%）、核心节点倒换测试（业务中断时间<50 ms）以及跨厂商设备互通性测试。

3.2 实验效果及指标

传统OTN专线加密方案是在两端部署VPN加密机,基于国密算法实现专线的端到端加密。量子安全OTN技术作为创新性光通信安全解决方案,通过量子密钥分发与光传送网协议栈的深度耦合,实现了传输安全性与网络性能的帕累托优化。基于实验网的实测数据与传统VPN加密机方案的对比分析如表1所示,本方案的技术优势如下。

表1　量子OTN实验效果

指标	本方案	传统VPN加密机方案	提升幅度
加密时延	0.7 μs	5.2 μs	86.54%
密钥更新效率	1 600 次/s	400 次/s	300%
故障恢复时间	<50 ms	>200 ms	75%
功耗(100G端口)	18 W	25 W	28%

a)超低时延传输特性。基于OPUk净荷层加密架构,结合国产ASIC量子安全芯片的硬件加速机制,加密时延从传统VPN方案的5.2 μs显著降低至0.7 μs(降幅为86.54%),满足金融高频交易(HFT,<1 μs)和工业时间敏感网络(TSN,<5 μs)等场景的严格时序约束。通过通用成帧规程(GFP)与SM4-GCM(Galois/Counter Mode)算法的联合优化,实现400 Gbit/s线速加密性能,时延抖动被控制在±0.3 μs范围内(置信区间为3σ)。

b)动态安全增强机制。依托QKD网络拓扑与QRNG构建的分布式密钥池系统,实现1 600 次/s的密钥更新速率,较传统VPN加密机方案提升300%。采用帧同步动态密钥(DFK)策略实现"一帧一密"的安全防护。在某省联通试验网连续72 h压力测试中,量子密钥误码率(Quantum Bit Error Rate,QBER)维持在0.48%±0.05%(均值±标准差),可有效防御光子数分离(PNS)攻击、时移攻击等量子窃听手段,密钥供给系统可用性达到99.999%(年中断时间≤5.26 min)。

c)高可靠组网架构。通过ODUk(Optical Channel Data Unit)子网连接保护(SNCP)与量子密钥双源热备机制的协同控制,故障恢复时间≤50 ms,光层保护倒换成功率经G.8031标准验证达到100%。

d)能效优化设计。实现单100G端口功耗从25 W降至18 W(能效提升28%)。经某省联通实验网300个加密端口全年运行数据测算,年度节能达5.04万kW·h,折合二氧化碳减排42.3 t(按中国区域电网基准线0.581 0 kgCO_2/kW·h计算),符合国家"双碳"战略目标的技术演进路径。

4 结论与展望

量子安全OTN技术与"量子密钥注入+光层内生安全"的融合创新,经实验网验证了其可行性,具备商业价值。实测数据表明,该系统在加密时延(0.7 μs)、密钥更新效率(1 600 次/s)等核心指标上实现数量级突破,打造加密即服务的新型光网络底座。OTN网络全生命周期投资回报率达233%,年均可节约运营成本1 100万元,可保障政务、金融等关键领域的信息主权,助力"东数西算"安全落地。

未来,将从4个维度进行深化研究。在技术层面,研发硅基光子集成芯片,突破400 km无中继传输瓶颈;在标准层面,推动ITU-T G.qt.sec国际标准的制定,建立评估认证体系;在应用层面,探索与星地量子通信网的协同组网,结合IDN实现加密策略与业务需求的智能匹配;在产业生态方面,搭建多方联合创新实验室,重点攻克医疗、工业互联网等场景,构建自主进化的量子安全光网络生态共同体。

参考文献:

[1] Cybersecurity Ventures. Cybercrime to cost the world $12.2 trillion annually by 2031[EB/OL]. [2026-08-26]. https://cybersecurityventures.com/official-cybercrime-report-2025/.

[2] GovTech. FBI: Ransomware still a top threat to critical infrastructure [EB/OL]. [2026-08-26]. https://www.govtech.com/security/fbi-ransomware-still-a-top-threat-to-critical-infrastructure.

[3] IBM. IBM unveils 400 qubit-plus quantum processor and next-generation IBM quantum system two [EB/OL]. [2026-08-26]. https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two.

[4] Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit[J]. Nature, 2023, 614(7947): 676-681.

[5] Gartner. 2024 OTN network security risk assessment [EB/OL]. [2026-08-26]. https://www.gartner.com/en/documents/5578628.

[6] 中国信息通信研究院. 2024数字安全白皮书[R/OL]. [2026-08-26]. http://www.caict.ac.cn/kxyj/qwfb/bps.

作者简介:

刘俊通,毕业于电子科技大学,主要从事通信网络的规划与建设工作;张世华,工程师,硕士,主要从事云计算、安全方面的咨询、规划和设计工作;张斌,毕业于南昌大学,江西省公安厅督察审计总队副总队长,三级警务技术主任,副高职称,硕士,主要从事公安大数据建模分析工作;刘扬,教授级高级工程师,长期从事云核心网、数据网咨询、规划、标准化研究和工程设计工作;余涛,毕业于南昌大学,主要从事通信网络的规划与建设工作;刘文慧,毕业于江西师范大学,主要从事通信网络的规划与建设工作。