

# 面向未来的通信： 量子安全技术的兴起

探索使用安全框架与验证工具，助力将量子算法及量子架构从理论模型和实验室环境推向安全可靠的现网部署

# 目录

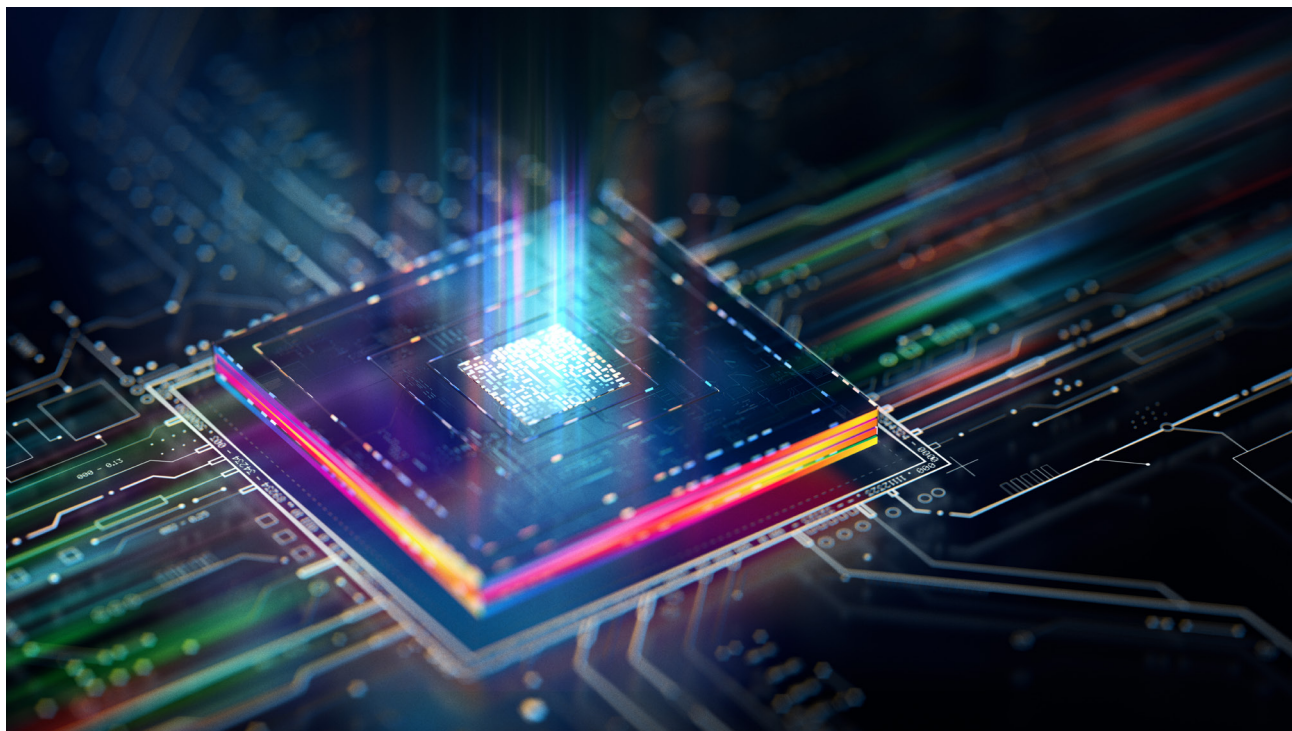
1	简介 .....	4
2	量子安全网络 .....	5
2.1	为什么需要 .....	5
2.2	标准 .....	5
2.3	QKD 和 PQC .....	7
2.4	对行业的影响 .....	8
3	量子安全测试领域 .....	9
3.1	测试 QKD 系统 .....	11
3.2	测试 PQC 系统 .....	16
3.3	测试混合系统 .....	22
3.4	KMS 互操作性测试 .....	24
4	其他测试注意事项 .....	25
5	总结 .....	28

量子安全通信不再是遥不可及的目标 - 它正在发生。多样化的技术生态系统正在推动这一进步，包括量子密钥分发 (QKD)、量子密码加密 (PQC)、端到端混合 QKD-PQC 模型、基于卫星的加密和密钥管理，以及将经典系统与量子安全系统相结合的过渡架构。鉴于量子计算的颠覆性潜力，这些创新正在改变我们对于安全通信的认知。

随着这些技术的不断发展，确保架构和系统部署具备最高的弹性、安全性、效率以及实际应用的可靠性变得至关重要。这在量子技术与物理基础设施交叉的光学层尤为重要。在许多情况下，挑战在于将量子科学（尤其是量子光学）从实验装置转化为可靠的现场解决方案。

标准和一致性对这一转变至关重要。但对基础设施的深刻理解也很重要，尤其是支撑安全量子传输的光学系统。光学不仅仅是一个组件，它是量子安全通信的基石。

拥有量子创新和深层光纤专业知识的值得信赖的合作伙伴是成功的关键。本文考察了大规模部署量子安全技术的关键因素。VIAVI 在这一点上有着独特的定位，将光纤领域数十年的领先地位与先进的量子研究相结合。VIAVI 在系统、物理和实验室验证方面拥有 30 多年的经验，为如何安全高效地将基于光子的通信从实验室过渡到实际部署提供了一个难得的视角。



# 1 简介

量子计算能力的预期爆炸式增长将重新定义数字安全的前景。随着量子处理器越来越接近实际实现，保护当今通信、金融系统和数字身份的加密基础面临着生存威胁。这个即将到来的里程碑 - 通常被称为 Q-Day - 标志着量子计算机将能够破解 RSA 和椭圆曲线密码 (ECC) 等广泛使用的公钥密码系统，使世界上许多加密数据容易被解密。

虽然 Q-Day 还没有到来，但现在就迫切需要采取行动。今天收集的数据明天就可以解密，这种威胁被称为“现在捕获，以后解密”。作为回应，政府、标准机构和企业正在加速采取能够承受量子机器计算能力的量子安全技术。

标准和一致性测试对这一发展至关重要。如果没有严格的验证，即使是最有前途的量子安全解决方案也有部署失败的风险。基础设施考虑事项，特别是涉及光纤、光子传输和信号完整性的考虑事项，必须得到精确解决。

然而，从理论到实践的转变是一项复杂的工作。量子安全技术不仅必须安全：它们还必须具有互操作性、弹性、可移植性，并且能够在现实环境中运行。这在传输和接收量子信号的光学层以及后量子密钥加密层尤其关键。在许多方面，挑战在于将量子技术 - 特别是量子光学 - 从实验室转移到现场，将它们从科学实验转化为可操作的系统。

这就是 VIAVI 的专业知识变得不可或缺的地方。VIAVI 在光纤、系统工程和实验室验证领域拥有 30 多年的领先地位，在支持量子转变方面具有独特的优势。我们的量子安全测试套件为评估量子防护技术的功能、合规性、性能和弹性提供了一个全面的平台。无论是集成到现有基础设施中还是部署在试验台中，VIAVI 解决方案都使利益相关者能够自信地评估和部署量子安全系统。

本文探讨了量子安全通信的发展前景，推动它的技术，以及测试和验证在确保安全无缝地过渡到后量子世界中的关键作用。

## 2 量子安全网络

### 2.1 为什么需要

数字加密是任何空间传输通信系统（如移动电话）的关键组件。窃听者可以监听电话并试图提取数据，但加密数据消除了这种威胁。随着量子计算机的兴起，现代加密方法面临被破解的风险。虽然量子计算机仍需 5-10 年才能问世，但恶意分子现在可以非法捕获数据，待量子计算机可用时再进行解密。这种威胁被称为“现在捕获，以后解密”（HNDL），它给政府、军队和金融机构带来了严重的担忧。这个问题的一个解决方案是采用 PQC 来保护敏感数据免受量子计算和窃取信息的潜在威胁。

移动标准机构 3GPP 正在发展其标准，以结合 PQC 算法来抵御未来的量子计算机攻击。3GPP 依赖其他标准组织（即美国国家标准与技术研究院 (NIST)）来制定标准化的 PQC 算法。对量子计算机可能造成的潜在攻击的担忧促使 GSMA（全球移动通信系统协会）建立了一个后量子电信网络任务组 (PQTN)，以建议移动运营商如何过渡到后量子就绪状态。

在确保互操作性、安全保障和量子安全通信系统的全球采用的需求的驱动下，QKD 的标准化工作已经进行了十多年。欧洲电信标准协会 (ETSI)、国际电信联盟 (ITU-T) 和 ISO/IEC 等组织已率先为 QKD 系统定义了框架、协议和安全要求。

### 2.2 标准

每个国家或地区都创建了量子技术的相关论坛，如 QuIC（欧盟）、QIC（加拿大）、Q-STAR（日本）、QED-C（美国）、UKQuantum（英国）、KQIA（韩国）、NQSIN（新加坡）和 QIIA（中国）。然而，这些论坛可能有不同的动机和目标。例如，美国通过《国家量子倡议法案》，旨在推动量子技术研究、人才培养和产业创新。中国的目标是通过“量子技术路线图”在特定应用领域（如密码学和材料科学）取得量子主导地位，并在研究、人力资源和基础设施方面采取多层次的方法。日本的目标是建立一个人人可以使用量子技术的社会，促进量子技术的全球化，并支持通过应用量子技术创造商业机会。

欧洲强调以量子通信、计算和传感为重点的基础研究，投资于量子硬件、软件和算法，以加强生态系统。这一努力培育了量子计算、传感和通信的研究中心。

ITU-T SG11、SG13 和 SG17 以及 ETSI ISG QKD 一直致力于 QKD 和 QKDN 标准化。ISO/IEC/JTC1 规定了 QKD 模块的一些评估方法。GSMA 为电信行业中的 PQC 和混合场景提供了指南。

NIST 在定义 PQC 算法方面处于领先地位，并已于 2024 年 8 月发布了首批三种算法。这些标准基于 CRYSTALS-Kyber、CRYSTALS-Dilithium 和 SPHINCS+ 算法，旨在确保针对未来量子计算能力的安全通信和数据保护。虽然 NIST 是建立 PQC 标准的美国机构，但许多国家/地区已选择采用 NIST 的建议，少数国家/地区决定创建自己的版本（即中国和韩国）。

ETSI、ITU-T 和 ISO/IEC 在定义 QKD 系统的框架、协议和安全要求方面处于领先地位。ETSI 的 QKD 工业规范组 (ISG-QKD) 尤其有影响力，它提出了针对 QKD 组件、网络架构以及与经典加密系统集成技术报告和规范。同时，ITU-T 致力于标准化 QKD 网络架构和关键管理接口，旨在协调全球部署战略。尽管取得了这一进展，但仍存在一些严峻挑战。

首先，不同供应商的 QKD 系统之间的互操作性仍然有限，阻碍了大规模、多供应商的部署。其次，可扩展性仍然是一个问题，特别是在将 QKD 从点对点链路扩展到复杂的网状网络时。第三，成本和基础设施要求（包括对专用光纤或可信节点的需求）阻碍了广泛采用。此外，QKD 系统的安全认证和一致性测试仍在发展中，没有在现实条件下普遍接受的性能和弹性基准。最后，将 QKD 与现有的安全基础设施相集成，并使其与新兴的后量子密码标准保持一致，这既是技术挑战，也是战略挑战。

## 2.3 QKD 和 PQC

当涉及到分发后量子密钥供系统使用时，有两种计划的方法：QKD 和 PQC。QKD 依靠量子力学的特性来交换密钥，这使得窃听几乎不可能，因为任何干扰的检测都将导致新的交换发生。这两种技术将会共存，因为在很多不同的情况下都需要量子抗性加密技术。

QKD 涉及使用量子位或量子信息单位通过光学手段（地面光纤、自由空间光学或卫星链路）交换加密密钥。这种方法保证了我们将知道窃听者是否截获了用于加密数据的密钥，使其本质上防篡改，因为它利用了量子力学的一个基本原理，即粒子纠缠（通常是光子）。任何干扰传输的企图都会产生干扰，通信协议会立即检测到这种干扰，导致通信立即停止。在这种情况下，可以在传输任何敏感数据之前发送新密钥。

QKD 的成本很高，因为它是基于硬件的，所以它最好的用途是在高度敏感的应用中，在任何情况下都必须保密。这些应用涉及固定位置的各方，并且成本不是主要考虑的问题。最能有效利用 QKD 的市场是政府、军队和某些金融服务领域，在这些领域，失败的代价可能是灾难性的。

另一方面，PQC 是一种基于软件的方法，它使用基于新的数学问题的算法来取代现有的密钥算法（RSA、ECC 等），这些算法容易受到 QC 攻击。我们不知道这些算法是否会被破解，所以不能 100% 保证。然而，与 QKD 相比，这是一种低成本的解决方案，有望成为主流选择。

总之，QKD 和 PQC 各有利弊。因此，对于真实网络和验证系统，必须考虑 QKD 和 PQC 的共存场景，以及经典的安全机制。

	QKD	PQC
设备	带有专用收发机的光纤	软件替换
安全方法	量子力学安全	计算安全
优点	无法嗅探	通过软件更轻松地进行升级
缺点	短距离（约 100 千米，基于卫星的 QKD 可以解决），成本高	不是 100% 安全，性能问题，需要时间进行迁移
标准化	ITU-T (Y.3800/X.1700 系列)，ETSI	IETF, NIST
用例示例	国家安全、专用线路	大规模通信、网上银行、企业网站

现实是，量子安全生态系统本质上是分散的，有专有的 QKD 协议、不同的 PQC 实现和不同的密钥管理系统。然而，从根本上和战略上来说，有必要加强这些技术的全球供应链，并提供不同的实施方法。

互操作性测试和验证框架对于降低集成中的风险、加快生态系统的发展和遵守标准至关重要。它们服务于公共利益，而这是单个供应商实验室无法提供或没有动机提供的。

## 2.4 对行业的影响

后量子就绪会影响所有行业 - 政府、金融、医疗保健、军事、电信等。在数字传输过程中，所有个人、财务和政府数据都必须加密。一旦量子计算机可用，坏人可以随时随地在任何系统上使用它们，因此保护数据的竞赛现在就开始了。即使在量子计算机问世之前，就存在 HNDL 的风险，即数据可能现在被截获并存储，待量子解密成为可能后，便可获取敏感信息。

每个垂直行业单独管理其向 PQC 的迁移路径，但共享许多共同元素，例如迁移路线图。例如，电信管理机构 GSMA 发布了一份题为 [“后量子密码电信使用案例指南”](#) 的报告。印度储备银行发布了一份题为 [“在量子计算时代保护印度银行业”](#) 的白皮书。

然而，所有行业对可信验证平台的需求都在不断增长，这对于监管认证、投资者信心和跨领域技术部署至关重要。该平台应支持全面的混合环境，并执行不同的验证方案，包括（但不限于）：

- 结合 PQC 可扩展性和 QKD 信息论安全性的混合仿真
- 从物理光子传输到应用层握手协议的分层测试
- 同步、回退逻辑、优先级和密钥刷新行为的 HKMS 测试
- 混合弹性的混沌测试：当 QKD 链路出现故障或 PQC 降级时评估连续性
- 数字孪生环境模拟跨越边缘城域网、云和卫星（包括非地面网络，即 NTN）、自由空间光学和基于卫星的 QKD 的混合经典量子网络
- 跨部署模型的性能基准测试：公共与私有，核心与边缘

### 3 量子安全测试领域

量子安全网络目前处于迁移状态，需要考虑生命周期管理和大规模商业化。VIAVI 支持所有测试领域：



1990.900.0725

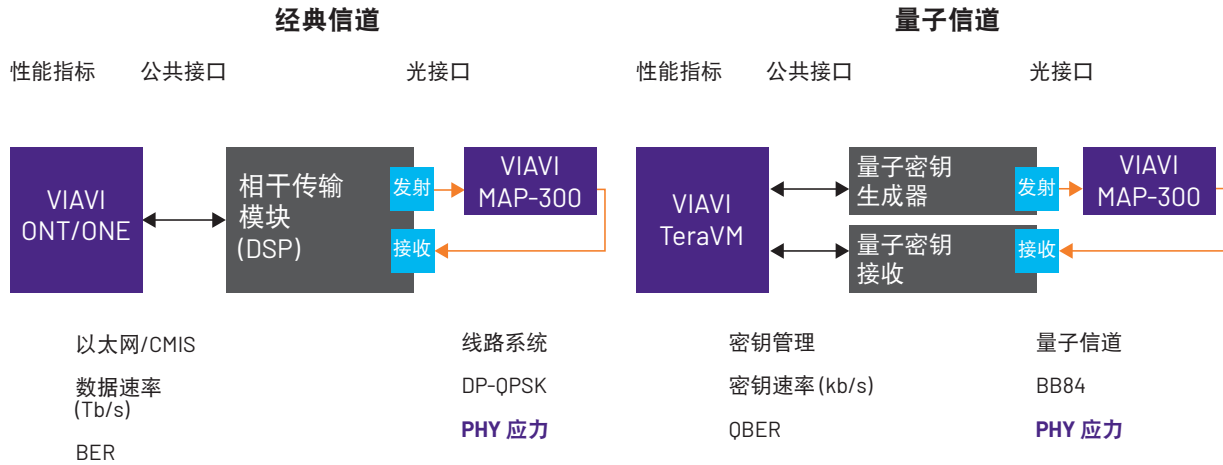
- 基础研究：QKD 优化、QKD 光子学、PQC 算法、PQC 优化、量子安全、量子模拟
- 应用研究和验证：QKD 密钥管理自动化、QKD/PQC 基于 AI 的线程检测、基于 AI 的 PQC 抗扰性（包括与非 PQC 协议的混合）、用于混合系统的基于 AI 的测试自动化
- 民用测试：认证、能效、可扩展性、成本效益、互操作性、云功能
- 大规模商业化方面/要求：电信、金融、汽车、政府、医疗保健、航空航天

本文回顾了支持量子安全测试的 VIAVI 产品套件各个组件：

量子安全网络功能	VIAVI 产品
密钥管理系统测试	TeraVM Security 
PQC 性能测试	TeraVM Security、VAMOS、CyberFlood、TestCenter   
QKD 量子信道评估	MAP-300 
光纤监控	ONMSi 远程光纤测试 
光纤传感	FTH-DTSS 
网络可观测性	NITRO <sup>®</sup> AIOps、ONMSi   NITRO AIOps
光纤基础设施/现场验证	OneAdvisor 800  INX 760 
运营效率	NITRO AIOps  NITRO AIOps
高端光学器件	光谱传感滤波器、光传感器滤波器 

下图显示了整体环境以及 VIAVI 套件的位置。

### 量子信道与经典信道



测试量子信道和测试经典信道在许多方面是相同的  
光子界面的性质非常不同  
**然而，它们都是通过一种光纤进行传输的，而这种结构必须被模拟出来。**  
光应力的水平和类型肯定会发生变化

1991.900.0725

## 3.1 测试和监控 QKD 系统

QKD 系统有多项基本测试要求。其中包括：

- 通过创建一个灵活、可重新配置的光子系统来模拟代表实际生产网络的各种功率和频谱负载场景，从而对 QKD 造成干扰。这可用于验证新的 QKD 系统或其子组件的性能或适用性。
- 根据光纤类型、DWDM 信号（如果有）的幅度和位置、波长增加或删除时的瞬态条件以及 P2P 链路中新光学设备（例如光开关）的鉴定来评估 QKD 系统的弹性
- 对 P2P 链路进行压力测试，以产生一系列受控的光学压力，如放大器的带内/带外噪声、移动线缆带来的偏振干扰、有源光学元件（开关、衰减器、波长选择开关）的抖动或稳定性、光学连接器引起的单次或多次反射事件。
- 面向服务层的 ETSI GS QKD 014 符合性测试。测试 QKD 密钥管理系统层的弹性，即关于它可以如何有效地服务 L3 VPN 应用层以检索用于建立 IKEv2 (RFC8784) IPSec VPN 隧道的后量子预共享密钥 (PPK)。当为高级后量子安全配置 VPN 链路的频繁密钥轮换时，这更有意义。TeraVM IKEv2 客户端仿真具有 ETSI GS QKD 014 API 支持，以从 KMS/QKD 层获取 PPK，并且当密钥在具有 PPK 认证的后量子安全 IKEv2 VPN 隧道中连续轮换时，可以在负载下测试 QoE。
- 针对光缆的物理攻击测试，如温度和应变以及未经授权的开挖工程。

## 量子信道评估

测试环境中的量子信道评估测量量子通信链路在真实或模拟条件下保持量子位完整性的程度。这确保了信道在部署之前支持安全量子协议。测试环境中的量子信道评估还涉及表征量子通信链路的行为，通常用于评估其对 QKD 或其他量子协议的适用性。

QKD 的两种主要类型是离散变量 QKD (DV-QKD) 和连续变量 QKD (CV-QKD):

- DV-QKD: 使用离散量子状态（如光子的偏振或离散相位）对信息进行编码，并需要精确的时钟同步来检测光子到达时间。BB84 和 E91 等协议就属于这一类。使用单光子探测器（例如，APD、SNSPD）。
- CV-QKD: 使用相干激光正交（振幅和相位）的连续调制。信息通过零差或外差检测提取，通常基于高斯调制协议，如 GG02。对时间不太敏感，但需要相位参考对准（本地振荡器校准）。零差或外差探测器（经典光电二极管）用于探测器。

DV-QKD 在长距离上提供更高的安全保证，但是涉及复杂的硬件和较低的密钥速率。CV-QKD 更适用于使用标准电信组件的短距离、高速率应用。测试方法必须考虑其独特的物理和协议特征，特别关注噪声、同步和组件校准。

在测试环境中，量子信道评估的工具和方法包括单光子探测器、量子光源、OTDR 和其他经典光纤工具、层析成像工具以及噪声注入等模拟器。关键测量包括量子比特误码率 (QBER)，它测量传输的量子比特（量子位）的误码率。高 QBER 可能表示噪音或窃听。其他测量包括损耗/衰减 (dB/千米)、相干时间/偏振稳定性、信道保真度以及定时抖动和同步。

测试包括：使用光学平台和精密元件进行短距离测试的实验室台架测试；模拟“真实世界”距离（10 千米、50 千米等）的仿真测试；已安装光纤的现场试验，以及卫星或机载测试（自由空间光学）。

对于量子安全案例，信道评估可能侧重于特定方面，包括：

- 抗侧信道攻击：测试确保量子安全密码实现不易受到侧信道攻击，侧信道攻击利用了诸如功耗或电磁辐射之类的意外信息泄漏
- 量子安全加密验证：组织评估量子安全加密方法，以保护关键基础设施免受新出现的威胁
- 性能和兼容性测试：量子安全加密解决方案的效率和与现有 IT 系统的集成经过测试，以确保无缝过渡

这些评估有助于为量子时代做好准备，确保他们的通信渠道在未来基于量子的网络威胁面前保持安全。

一般来说，测试设置还会经历迭代优化，以减少误差源，如失调、温度漂移和探测器暗计数，目标是最大化键控速率，同时将 QBER 保持在安全阈值以下（BB84 QKD 通常小于 11%）。

### **VIAVI 解决方案：MAP-300**

量子测试需要配备有开关、波长管理工具、掺铒光纤放大器（EDFA）以及衰减器等设备的实验室来控制各种量子实验条件。QST 将构建用于量子技术试验/评估的网络。VIAVI MAP-300 是一款模块化、紧凑型且易于重新配置的光测试平台，具备远程和自动化的功能。它有效地探索了量子技术在计算、网络、加密和密码学领域的极限。

MAP-300 能够支持 QKD 损伤，它通过构建灵活且可重新配置的光子系统来实现这一功能，该系统能够模拟出代表实际网络的个中功率和光谱负载情况。这可用于验证新的 QKD 系统或其子组件的性能或适用性。还可以进行相关研究，以明确（甚至标准化）以下条件矩阵，从而确定在何种条件下 QKD 系统能够正常运行：

- 光纤的类型
- DWDM 信号的幅度和位置（如有）
- 当波长被添加或移除时的瞬态情况
- P2P 链路中的新光学设备（例如光开关）的鉴定

在 QKD P2P 链路中，通过创建并插入全光元件来产生一系列可控的光应力。

- 放大器的带内和带外噪声
- 移动光纤引起的偏振干扰
- 有源光学元件（开关、衰减器、波长选择开关）的抖动或稳定性
- 光学连接器引起的单个或多个反射事件。
- 针对不同噪声和干扰水平下 QKD 的纠错机制开发的研究。研究现有技术并开发更好的方法。

## 光纤监控

通过检测潜在的物理层攻击，光纤监控可以在量子安全通信中发挥重要作用。例如，光纤窃听可能会危及 QKD 或其他量子安全协议的安全。QKD 依赖于量子力学的基本性质 - 具体来说，测量一个量子系统会干扰它。然而，如果攻击者实际窃听光纤，他们可能会试图在不被发现的情况下拦截信号。

在光纤窃听场景中，光纤监控有助于检测异常情况，如信号损失增加、反向散射或时间延迟，警告中心局未经授权的接入尝试，并通常保持物理传输介质的完整性。

光纤监控也增强了整体量子安全保障。即使不使用 QKD，PQC 算法也依赖于安全的物理基础设施。如果有人可以被动地窃听光纤，他们可能会在今天收集加密数据，并在以后用量子计算机破解 (HNDL)。因此，光纤监控充当了第一道防线，通过以下方式确保光通信网络的完整性和安全性，从而阻止被动窃听，并用物理层安全性补充量子安全加密：

- 量子安全加密：光纤监控通过将 QKD 和 PQC 集成到光网络中，帮助维护安全的数据传输。这可以确保敏感信息免受量子时代的网络威胁。
- 超安全量子通信：研究人员已经成功地使用光网络远距离发送量子信息，证明了量子安全消息传递的可行性，而不需要昂贵的低温冷却。<sup>1</sup>这一进步增强了金融交易、医疗保健数据和政府通信的安全性。
- 用于量子密码术的低延迟光纤：一些组织正在测试新的光纤技术，如空芯光纤，以提高量子密码术的效率<sup>2</sup>。这些创新有助于扩大量子安全加密的应用范围，使其在现网部署中更加实用。

与光纤传感一样，在量子安全环境中，光纤监控可以确保安全和弹性通信网络。

<sup>1</sup>[https://techblog.comsoc.org/2025/05/03/ultra-secure-quantum-messages-sent-a-record-distance-over-a-fiber-optic-network/?copilot\\_analytics\\_](https://techblog.comsoc.org/2025/05/03/ultra-secure-quantum-messages-sent-a-record-distance-over-a-fiber-optic-network/?copilot_analytics_)

<sup>2</sup>[https://www.luxquanta.com/luxquanta-collaborates-in-test-of-low-latency-fibre-in-data-centers-led-by-lyntia-n-71-en?copilot\\_analytics\\_](https://www.luxquanta.com/luxquanta-collaborates-in-test-of-low-latency-fibre-in-data-centers-led-by-lyntia-n-71-en?copilot_analytics_)

### **VIAVI 解决方案：带光纤测试头(FTH)的 ONMSi 远程光纤测试系统(RFTS)**

ONMSi 是一种光网络监控系统，它可对从 PON 核心直至驻地的网络进行监控 - 从而改善任何类型的网络的运作支持和服务质量 (QoS)。ONMSi 是一种远程光纤测试系统，它可全天候扫描光纤网络并自动检测和定位故障，而不必派遣现场技术人员。基于行业领先的 VIAVI 光学技术，集成了光时域反射仪 (OTDR) 和光开关的光纤测试头 (FTH) 不断将数据与基准进行比较，如果出现任何光纤退化，就会发出警报。

## **光纤传感**

光纤传感可以通过充当量子或后量子安全网络物理层的实时入侵检测系统来增强量子安全通信。简而言之，光纤传感通过分析光线如何沿光纤反射或散射，将光纤变成分布式传感器。这可以通过瑞利散射（用于振动或声学传感）、布里渊散射（用于应变和温度）和拉曼散射（用于温度分布）来实现，所有这些散射都可以检测长距离上甚至微小的变化。

光纤传感通过提供以下功能支持量子安全：

- **QKD 链路的篡改检测：**QKD 假设物理入侵会扰乱量子态。光纤传感技术通过探测任何重大入侵前对光纤的窃听、弯曲或切断企图，又增添了一层防护。例如，如果有人试图弯曲光纤来虹吸光子，光纤传感可以检测应变或振动并触发警报。
- **监控延迟窃听：**在 PQC 中，攻击者可能现在就窃听光纤，存储加密数据，以后用量子计算机解密。光纤传感检测这种被动窃听，使攻击者更难保持不被发现。
- **增强的态势感知：**光纤传感可以检测振动、环境干扰和未经授权的施工，这些都可能威胁到关键的量子安全基础设施。它提供了一个安全边界，特别是对于地下或暴露的光纤布线。

光纤传感通过提供物理攻击的早期预警来加强量子安全系统，并通过实时分布式监控来补充量子密码学，保护 QKD 和 PQC 免受物理层漏洞的影响。它可以通过实现安全和精确的测量，同时保持数据完整性以应对潜在威胁，在量子安全环境中发挥至关重要的作用。例如，通过提供无需依赖量子纠缠的远距离（即 50 千米光纤）安全量子遥感 (SQRS)，或基于光纤的量子传感用于环境监测、灾害响应和军事监视，确保传输的数据保持机密性并能够抵抗窃听。

这些进步凸显了光纤传感在量子安全应用中不断增长的潜力，为更具弹性和可扩展性的量子技术铺平了道路。

## VIAMI 解决方案：FTH-DTSS

VIAMI 光纤测试头分布式温度和应变传感 (FTH-DTSS) 利用市场上最通用的光纤传感解决方案来监控电力电缆、管道和电信电缆的温度和应变。作为 NITRO 光纤传感解决方案的一部分，FTH-DTSS 提供对光缆和光纤资产的连续监控。这种技术利用光缆提供关于资产内部和周围环境所产生的温度和应变的连续实时信息，并可立即进行检测和定位。FTH-DTSS 的一些功能包括：

- 我们的创新技术专为要求高精度和可靠性的行业而设计，可提供分布式温度和应变传感 (DTSS)，用于对超长光缆的温度和应变进行绝对测量，是众多应用中不可或缺的工具。
- 能够检测各种应用中的异常，如关键基础设施（电力设施）、管道（石油、天然气、水等）、电信网络（数据中心互连 - DCI）等。
- 主动监控跟踪温度和应变的变化，这些信息可用于提高运营效率和响应能力，并允许采取预防性/主动行动来减轻潜在的损害或中断。

## 3.2 测试 PQC 性能

当谈到将现有的加密算法迁移到后量子算法时，一个突出的问题是更长的加密密钥的影响。此外，跨移动系统的各种组件采用 PQC 可能会引入性能和架构影响，尤其是在无线带宽有限的用户终端上。在启用 PQC 的配置下，彻底测试地面网络 (TN) 和 NTN 是至关重要的。以下是电信行业提出的一些担忧：

公司	PQC 迁移问题
<a href="#">SKT</a>	开发 Q-SDN、QKDN Federation 等量子密码术网络集成技术，实现不同厂商设备之间、运营商之间、国家/地区之间的量子密码术网络集成运行和控制。
<a href="#">Vodafone</a>	Vodafone 和 IBM 宣布合作，将 IBM Quantum Safe 技术集成到 Vodafone 安全网 (Vodafone Secure Net) 中，这是该公司的一体化数字安全服务。概念验证旨在通过实施 PQC 标准来保护智能手机用户免受未来量子计算的威胁。
<a href="#">Softbank</a>	当在数据传输基础设施中部署加密协议时，它们会给通信带来巨大的负载，并导致延迟问题，从而导致质量差和吞吐量低。

公司	PQC 迁移问题
<a href="#">5G Americas</a>	预计会出现潜在的性能和互操作性问题，这将需要彻底的测试。
<a href="#">印度电信部</a>	由于新的 PQC 算法操作繁重，它们可能会影响组织的关键运营。持续测试新产品或更新产品并监控其性能至关重要。
<a href="#">电信 GSMA 指南</a>	部署必须进入测试阶段，以评估某些后量子密码算法的可行性，从而将性能影响降至最低。
<a href="#">印度储备银行</a>	一些值得关注的因素包括性能开销和复杂的实现，这需要大量的测试。
<a href="#">BIS</a>	新的加密实现必须经过全面测试，以确保它们在现有基础设施中正常运行，保持性能水平，并且不损害系统完整性。

## PQC 测试

PQC 协议的实施会造成额外的网络性能开销，从而影响最终用户体验。测试对于开发和部署加密系统而言至关重要，包括基于 PQC 的系统。PQC 旨在创建针对量子计算机威胁的安全算法。测试有助于 PQC 的几个关键领域：

- **安全保障**
  - 算法抗性测试验证了 PQC 算法对加密攻击的抵抗力。这包括在不同场景下测试算法，包括使用经典和量子算法的场景，以评估其弹性。
- **性能评估**
  - 计算效率测试评估 PQC 算法的计算效率。这包括测量加密/解密速度、密钥生成速度和整体系统性能。确保 PQC 算法的效率对于在实际应用中的广泛采用至关重要。
- **互操作性测试**
  - 与现有系统集成：加密系统通常需要与已建立的基础设施和协议进行交互。测试对于保证 PQC 算法无缝集成到不同系统中至关重要，可避免兼容性问题。
- **标准化合规性**
  - 遵守标准：该测试证实了 PQC 算法符合既定的加密标准，促进了跨平台的互操作性和一致实施。

VIAVI 还可以利用长期的 VPN 测试经验，我们将采用这些经验来测试 PQC 算法，旨在防止不良行为者“现在存储，以后解密”的风险。

这包括：

- 后量子 (PQ) VPN 混合测试：使用混合密钥测试 IKEv2 对等连接
  - 测试发起方而非响应方的 PQ VPN 混合：如果双方都不支持 PQ VPN 密钥，请确保建立经典 IKEv2 隧道
  - 测试不匹配的 PQC KEM 选择：如果协商无法在发起方和响应方之间找到匹配的密码，测试将失败
  - 压力测试 PQ VPN 隧道：在两个 PQC 支持站点之间长时间传输大型数据文件，以确保双方的文件传输完整
- IPSec VPN PQC 算法支持：
  - 支持 NIST 标准化 KEM 算法以及几种后量子算法

### **VIAVI 解决方案：TeraVM Security**

从性能角度来看，确保系统为 PQC 做好准备并且不受影响的最佳方法是测试。这就是 VIAVI TeraVM 的用武之地。

TeraVM 是一款软件测试工具，它通过模拟用户和流量，并将 VPN 头端压测至极限，来测量 VPN 处理流量、过滤恶意软件时的用户性能表现，其 VPN 性能测试已持续开展 20 余年。通过使用 PQC 标准化算法加密 VPN 隧道，将 VPN 测试扩展到 PQC 测试是对现有软件工具的简单扩展。这意味着需要衡量额外的 KPI，例如：密钥大小变化、密钥更新轮次、混合密钥等。

许多企业的 IT 部门在公司范围内推广一项新功能之前都会对其进行测试。这可能涉及一小组测试人员，他们从世界各地登录以测试新功能。虽然这种方法适用于大多数升级和错误修复，但对于涉及额外计算开销的更改来说就不够了。仅在美国，就有超过 10000 家员工超过 1000 人的企业，因此有必要进行规模测试，以确保顺利过渡到 PQC。

TeraVM 可以模拟数万名员工及其位置（远程、VPN、现场、托管设备等），然后模拟他们的办公室流量，如协作工具、视频会议、专用应用程序访问等。TeraVM 可以在员工数量不断增加的情况下运行流量，同时监控延迟、吞吐量和 MoS 分数等 KPI，确保有信心上线运行。

## VIAMI 解决方案: CyberFlood 安全与性能解决方案

CyberFlood 是一款全面自动化的安全与性能测试平台，旨在验证网络、应用程序及设备在真实环境中的运行表现。它使团队能够轻松生成数百 Gbps 的真实流量，模拟复杂的网络攻击，并大规模评估系统弹性和安全效率，帮助组织确保其基础设施、服务和安全控制能够在当今快速变化的威胁环境中提供可靠的性能和强大的保护。

当组织为 PQC 准备安全基础设施时，他们不仅要验证新密码实施的正确性，还要验证这些算法对安全检测、互操作性和整体网络性能的影响。这正是 CyberFlood 发挥关键作用之处。

CyberFlood 为支持 PQC 的环境提供先进的规模与性能测试，帮助安全团队在部署前评估量子安全加密对防火墙、代理及其他基于检测的安全控制措施的影响。由于 PQC 算法通常会引入更大的密钥大小和更多计算密集型处理，因此安全基础设施可能会经历延迟增加、吞吐量降低和硬件压力增加。CyberFlood 帮助组织在实际部署之前量化这些影响。

CyberFlood 支持符合当前 NIST 标准的 PQC 密码套件测试，包括 FIPS 203 密钥封装机制和 FIPS 204 数字签名。它还支持混合 KEM 测试，包括在支持 PQC 的系统与不完全支持量子安全握手的系统交互时验证回退行为。这对于识别互操作性问题，并确保在迁移过程中安全通信能够以最小的中断持续进行至关重要。

通过将 PQC 密码套件集成到现实的 HTTP 协议流量、应用和威胁模拟中，CyberFlood 允许安全团队在类似生产的条件下验证量子安全部署。这有助于确认在加密流量、应用会话和混合密码环境扩展时，检测策略仍然有效。CyberFlood 对于测试中间人检测场景尤其有价值，在这种情况下，解密和分析受 PQC 保护的流量的负担可能会显著影响防火墙和网关的性能。

借助 CyberFlood，组织可以：

- 验证加密 PQC 流量之间的安全控制、性能和互操作性
- 评估防火墙和检测系统在量子安全加密额外负载下的运行表现
- 验证与传统或未启用 PQC 的系统通信的混合回退机制
- 尽早发现基础设施差距，以降低迁移风险，避免不必要的成本，并改进升级规划
- 获得应对量子时代威胁的未来安全运营所需的信心

## VIAMI 解决方案: TestCenter

TestCenter 是一个全面的端到端网络和云验证平台，旨在帮助服务提供商、数据中心和设备供应商验证演进架构的性能、可靠性和可扩展性。它设计为统一的第 2-3 层测试环境，能够提供大容量流量生成、广泛的协议仿真以及实时分析功能，可支持从传统以太网验证到下一代 AI 数据中心交换网络的各类测试需求。TestCenter 的灵活产品组合涵盖硬件设备、高速以太网测试模块、虚拟化测试环境和 AI 规模工作负载仿真，使客户能够加快开发周期、优化配置，并确保为要求苛刻的多供应商高速网络部署做好准备。

随着网络向量子弹性架构发展，TestCenter 为验证下一代 PQC 网络架构提供了一个强大且可扩展的基础。TestCenter 的统一第 2-3 层设计提供了大容量流量生成、确定性测量和广泛的协议仿真，这些功能已经得到了服务提供商、超大规模企业和云运营商的信任，可以大规模验证高速以太网环境。通过支持快速发展的网络设计中的多速率操作，包括从 10G 扩展到 1.6T 的高速接口，TestCenter 能够对准备承载更重的净荷、加密元数据和 PQC 增强协议引入的延迟敏感交换模式的交换网络进行全面的压力和性能验证。

随着组织对交换结构和云骨干网进行现代化改造，以适应 AI 工作负载并保护它们免受未来量子威胁的影响，TestCenter 的成熟优势，如大规模流量可扩展性、全面的协议覆盖和实时分析，对于验证这些升级后的基础设施的弹性至关重要。该平台能够模拟高密度流量模式，验证跨多供应商环境的互操作性，并在极端负载条件下评估网络就绪性，这为确保在不影响吞吐量或可靠性的情况下部署 PQC 算法提供了重要基础。支持下一代 AI 数据中心验证的相同功能，如多速率测试、拥塞分析和工作负载仿真，可直接转化为评估高速以太网交换网络上 PQC 增强传输、握手和密钥交换机制所需的性能基线。

通过将确定性高性能流量建模与灵活的硬件和虚拟测试环境相结合，TestCenter 使工程团队能够加快向量子安全网络设计的迁移。TestCenter 提供了一个面向未来的验证框架，有助于确保高速、云规模和以 AI 为中心的基础设施在量子时代保持可靠、可互操作和安全。

### **VIAVI 自动化管理和编排系统 (VAMOS)**

VAMOS 是一个基于云的统一平台，可自动执行 VIAVI 无线测试产品（包括 TeraVM Security）的测试活动、案例和执行。凭借可定制的工作空间和配置，VAMOS 简化了整个测试工作流程，提高了团队和实验室的资源利用率。

共享的工具试验台和单独的沙箱支持广泛的测试需求，而强大的分析和报告功能可提高测试精度和可靠性。

通过集成 AI、ML 和实验室即服务 (LaaS)，VAMOS 显著降低了运营成本，从而最大限度地减少了人工工作量并加快了故障分析。结果是：更快的上市时间、更高的质量和更严格的预算控制。主要优势如下所示。

#### **减少运营开支**

- 通过智能自动化减少工时
- 通过优化的工作流加快上市时间
- 通过精确和一致的测试提高服务质量

#### **最大限度地提高实验室效率和有效性**

- 端到端测试执行的零接触自动化
- AI/ML 驱动的洞察力可缩短响应时间并增强工程专业知识

#### **实现随处测试执行**

- 全局调度层跨实验室位置平衡资源
- 通过独立于位置的执行实现成本优化的测试
- 开放的、与工具无关的自动化框架，具有随时可用的调度功能

#### **确保同类最佳的工具利用率**

- 高级工具选择和漏失分析可检测现场级问题
- 优先选择能在周期早期识别实际问题的工具和流程

#### **利用 COTS 平台上的硬件/软件分解**

- 面向不同测试场景的共享计算资源
- 一次性按需沙箱中的动态软件工具预置
- 首选带有灵活硬件插件的纯软件工具，取代僵硬的设备

### 3.3 测试混合系统

量子网络中的混合系统将经典网络组件与量子技术（如 QKD、量子中继器和 PQC）集成在一起。测试这些系统需要涉及功能、性能、安全和环境因素的多维方法：

#### 试验台上的迁移测试

目标：模拟运营商所需的迁移场景。

- QKD、PQC 和经典安全方法的共存场景
- QKD、PQC 和经典安全方法之间的回退场景

#### 功能测试

目标：确保经典组件和量子组件按预期协同工作。

- 量子-经典接口测试：验证量子信号和经典系统之间的时钟同步；测试 QKD 控制协议
- 协议栈验证：确保 QKD 与 IPsec、TLS 或 PQC 的集成

#### 性能测试

目标：测量并优化吞吐量、延迟、错误率、会话数量和会话建立时间。

- 关键指标：量子比特误码率 (QBER)；安全密钥速率 (bps)；延迟和抖动、会话数量、会话建立时间
- 使用案例：测量混合加密场景中的安全密钥生成和消耗

#### 安全测试

目标：验证量子安全和混合加密弹性。

- 模拟 PNS、中间人和侧信道等攻击
- 验证向 PQC 的安全回退
- 测试量子随机数发生器 (QRNG) 的熵质量

#### 环境和物理层测试

目标：确保在真实条件下的稳健性能。

- 损耗、色散、偏振效应的光纤测试
- DWDM 中量子流量与经典流量的共存
- 自由空间光学（如卫星链路）的大气测试

#### 试验台上的集成测试

目标：模拟类似生产的环境。

- 将实时光纤链路和仿真量子节点相结合
- 部署在国家或私人量子试验台中

### AIOps 和监控集成

目标：使用 AI/ML 监控和调整混合网络

- 实时分析经典和量子指标
- 对篡改或降级使用异常检测
- 混合链路运行状况的实时可视化和警报

测试区	经典组件	量子组件	工具/方法
迁移	以下组件的组合	以下组件的组合	以下组件的组合
功能	网络堆栈、路由	QKD、QRNG	协议分析器、QKD 控制台
性能	带宽、抖动	QBER、密钥生成速率	光纤测试仪、NetSquid、QuISP
安全性	防火墙、VPN、PQC	量子攻击模拟	渗透测试、侧信道工具
物理层	DWDM、光纤、射频	光子传输	OTDR、光纤传感、偏振工具
集成和监控	编排、AIOps	密钥使用、故障检测	NMS、AIOps 仪表板、VIAVI NITRO

通过利用前面章节中提供的 VIAVI 测试解决方案，可以测试包括迁移在内的几种混合场景。

### 3.4 KMS 互操作性测试

一个至关重要的新焦点领域是密钥管理系统 (KMS) 互操作性，它在 QKD、PQC 和混合环境之间架起了加密控制平面的桥梁。

密钥管理系统必须在不同的密码学领域（如光密码、格基密码或混合密码）之间交换密钥，与多种标准（如 ETSI GS QKD 014、ITU-T Y.3805 和 IETF 的 KEMTLS 草案）进行交互，并在多个厂商和协议之间运行，确保密钥生命周期、轮换周期和分发路径的一致性。

这些因素意味着 KMS 互操作性需要以下评估、测试和验证：

- 跨供应商合规性验证：验证是否符合标准，并确保混合供应商实施下的一致行为。
- 弹性测试：模拟密钥交付延迟、损坏或丢失，并验证应用程序是否能够自动请求新密钥或回退到 PQC。
- 可扩展性评估：确保 KMS 能够以确定性延迟和零密钥冲突的方式处理大规模密钥分发（例如，数百万个安全会话）。
- 安全测试：验证 QKD 节点、KMS 服务器和客户端应用程序之间的安全握手和身份验证机制，确保防止回放或中间人攻击。

## 4 其他注意事项

### AIOps

面向 IT 运营的人工智能(AIOps)已经应用于量子安全环境中，以增强安全性、自动化威胁检测和优化数据传输。它可以通过主动管理和保护支持量子和后量子加密系统的基础设施来增强量子安全。AIOps 在不断发展，但在基础层面上，它提供了多种优势：

1. 威胁检测和异常响应：量子安全系统不仅依赖于密码学，还依赖于安全稳定的操作。AIOps 可以检测数据流中可能指示窃听、光纤窃听或中间人攻击的异常行为。它还可以分析来自 QKD 系统的日志，检测包括量子比特误码率(QBER)峰值、意外信号衰减和可疑设备重新认证在内的异常。AIOps 通过使用根据正常操作行为训练的机器学习模型来实现这一点，帮助快速标记异常值。
2. 自动化基础设施监控：量子安全系统通常需要低延迟、稳定的环境。AIOps 通过监控量子或混合网络上的延迟、抖动和丢包来帮助维护这一点；基于实时 AI 见解优化路由或交换；以及自动响应可能影响量子密钥交换或后量子加密协议的退化。
3. 适应性安全态势：量子安全实现可能涉及混合系统（经典 + 量子/后量子加密）。AIOps 可以根据感知的威胁级别动态调整加密强度或协议使用，然后根据观察到的系统性能和风险级别推荐量子安全算法部署。
4. 加密漂移和合规管理：AIOps 可以跟踪传统或不兼容的加密库的使用，从而检测和标记非量子安全算法（如 RSA 或 ECC）的使用，然后建议使用 PQC 库（如 CRYSTALS-Kyber、Falcon）进行自动替换。

AIOps 的几个关键应用存在于量子安全环境中，其中最重要的是通过监控网络流量的恶意活动来进行威胁检测和响应，在可能危害敏感数据之前检测潜在的量子时代网络威胁。它还可用于评估密码基础设施，并自动过渡到后量子密码标准（从而确保长期安全）。

总之，AIOps 通过检测整个堆栈的威胁和异常来增强量子安全系统，确保 QKD 或 PQC 部署的操作完整性，实现动态防御（包括自动加密调整），并监控是否符合量子安全标准。

### **VIAVI 解决方案：NITRO® AIOps**

VIAVI 提供 NITRO AIOps，这是一种先进的端到端、自上而下的智能引擎，可作为一种伞式解决方案，无缝集成到多供应商、多技术和多领域环境中。NITRO AIOps 的 AI 驱动能力提供了一个独特的机会来简化 NOC 复杂性和精简操作。NITRO AIOps 提供了许多好处，包括：

- 降低 TCO：利用 AI 和预测性维护，NITRO AIOps 有效地减少了代价高昂的停机时间。先进的 AIOps 在资源分配、容量规划和优化方面的能力进一步增强了成本控制，即使在最复杂的情况下也能促进可持续的网络运营。
- 运营支出减少：NITRO AIOps 通过自动化提升了网络管理、故障排查和服务保障，释放了零接触操作的全部潜力，提高了运营效率。
- 数字化转型 - 5G 货币化：NITRO AIOps 通过实时分析和预测性维护实现网络数字化转型，在问题影响用户之前发现问题。它的自我修复功能优化了性能，即使在高峰负载期间也能确保无缝的用户体验。

### **量子网络中的现场测试光纤**

光纤现场测试在量子网络中至关重要，因为这些网络依赖于极其脆弱的量子态进行通信。即使是光纤基础设施中的微小缺陷或不一致，也可能扰乱或完全破坏量子信号。

光纤量子安全网络对物理层条件高度敏感，并依赖于高质量的光纤。现场测试确保光纤支持安全的量子密钥交换。

在混合网络中，许多量子安全部署将使用现有的电信光纤和传统数据。现场测试验证了光纤可以处理量子 and 经典流量，可以安全运行，没有噪声或干扰，并且光纤符合量子安全部署要求。

因此，光纤现场测试对于量子安全网络（尤其是 QKD）至关重要，因为它可以确保量子密钥传输的信号完整性，有助于保持对安全性至关重要的低错误率，并检测可能危及量子验证加密的漏洞。

### **VIAVI 解决方案: OneAdvisor 800**

VIAVI OneAdvisor 800 旨在简化不断发展的网络测试需求，以维护各种有线和无线网络。

OneAdvisor 800 的模块化设计使网络技术人员能够在众多测试场景之间轻松切换，这些场景大致分为三类：无线、传输和光纤。

OneAdvisor 800 提供直观的触控手势操作界面，并配有辅助应用程序，可引导技术人员完成仪器使用；其拥有丰富的模块和性能，可匹配任何网络应用，实现快速、无差错的测试；此外，它还能轻松开通并验证任何新型 WDM 服务（包括 CWDM、DWDM、MWDM、LWDM），并满足未来高速业务激活、OSA 以及以太网/BERT 测试的需求。整合报告将需要管理的测试工作量减少了 50%。

光纤测试能力包括：光连接器检查、OTDR 和 PON-OTDR、FiberComplete PRO™ 双向 IL/ORL 和 OTDR (TruBIDIR)、DWDM OTDR、光谱测试，以及用于海底电缆验收和故障排查、高速 DWDM 陆上传输网络、4G/5G 无线接入网络（回传、中传和前传）、数据中心、数据中心园区和互连 (DCI) 测试、FTTH/PON 网络测试（任何标准、非平衡/分接或索引拓扑）、用于 DAA、R-PHY 和 C-RAN 的 DWDM 接入网络，以及企业/LAN 测试的高级色散测试。

对于传输测试，OneAdvisor 800 具有以下几个优点：

- 方便携带。最小的 400G/800G 测试设备之一
- 无与伦比的冷却性能。同类最佳的 400G/800G 便携式设备-易于冷却的 ZR 可插拔设备
- 卓越的电池续航时间。可扩展到多个电池，支持数小时不连接电源使用
- 广泛的测试覆盖范围。模块化提供跨线速率和协议的一体化解决方案
- 灵活。测试光纤（OTDR、OSA）和所有以太网速率（800、400、200、100、50、40、25、10 和 1）
- 多光学器件支持。支持 QSFP-DD800/QSFP-DD/QSFPx、OSFP800/OSFP、SFP-DD/SFPx，并完全支持相干光学器件

### **VIAVI 解决方案: INX™ 760**

INX 760 是现场技术人员的终极工具，在确保洁净光纤连接方面提供了无与伦比的效率。作为超过 25 年的开拓性创新和专业知识的结晶，它是下一代光纤端面检测和分析的巅峰之作。虽然光纤端面检测已经成为许多现场技术人员的标准做法，但污染仍然是光网络问题的头号原因。随着新型连接器的出现、现场使用的连接器数量的增加以及新光纤技术人员的增加，该行业已经到了一个转折点。

## 光学安全与性能

虽然本文概述了量子网络的挑战和相关的 VIAVI 测试解决方案，但 VIAVI 还为量子网络提供了行业领先的独特光学涂层，包括[光谱传感滤波器](#)和[光传感器滤波器](#)。VIAVI 光学安全和性能 (OSP) 业务部门成立于 1948 年，前身为光学涂层实验室 (OCLI)，75 年来一直是定制光学领域的创新领导者。作为高性能光学领域值得信赖的顾问和长期合作伙伴，我们提供优质的解决方案和无与伦比的客户服务体验。凭借在工程、研究和应用知识方面的深厚根基，没有任何其他供应商能够在应对您的简单或复杂的光学挑战方面与 VIAVI 匹敌。从原型到生产，我们的专业知识、技术和流程为客户提供了竞争优势。

OSP 滤波技术可以帮助客户以最少的干扰和最高的保真度提取光学信号，以最高的精度在任何要求的规模下设计表面。

## 5 总结

随着量子计算的发展，传统的加密方法面临着越来越大的脆弱性。为了解决这一问题，VIAVI 开发了 TeraVM Security Test，这是一款开创性的云化赋能测试平台，专门用于评估后量子密码 (PQC) 的部署实施方案。该解决方案支持 NIST 规定的算法，并协助组织向抗量子安全框架过渡。此外，VIAVI 还提供用于量子信道评估的 MAP-300、用于光纤监控和传感的 ONMSi 和 FTH-DTSS，以及用于光纤网络安装、故障排查和维护的全套现场测试仪。



北京            电话: +8610 8233 0055  
上海            电话: +8621 6859 5260  
上海            电话: +8621 2028 3588  
                  (仅限 TeraVM 及 TM-500 产品查询)  
深圳            电话: +86 755 8869 6800  
网站:            www.viavisolutions.cn