迈向量子互联网

（中国科学技术大学　陈　巍、张国威　编译自 Jon Cartwright. *Physics World*, 2023, (6): 35）

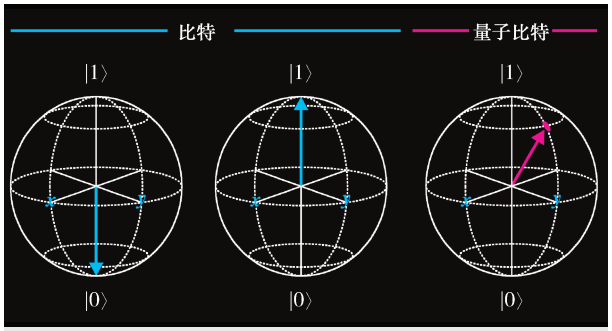
我们能否以完全安全和保密的方式在线发送数据？来自英国布里斯托的记者 Jon Cartwright探讨了“量子互联网”的最新进展。

目前，对电子邮件、医疗记录、银行交易或政府机密等信息进行加密，其安全性可以抵御最强大的超级计算机的破解。但可能只需要十年，量子计算机就将具备入侵这些私密数据的能力，使其突然间变得唾手可得。而近期的科学研究成果也正在传递一个信号：量子“炸弹”的引爆时间可能比我们想象的更早。

量子技术专家多年来一直在发出警告：量子计算机可能对信息安全产生威胁。2020年，英国国家网络安全中心发布了一份白皮书，建议大型公司和机构“应该在制定长期路线图时考虑量子计算机攻击的威胁”，并优选可以过渡到量子安全平台的系统。IBM公司在其2023年发布的《量子计算时代的安全》中指出，量子计算是对经典数据安全的“生存威胁”，并警告说，“毫无疑问，冲击即将到来——这不是存在与否的问题，而是多快到来和破坏性多大的问题。”

只有基于量子技术才能抵御量子攻击，并证明其安全性。幸运的是，物理学家们早已在研究量子密码学，特别是量子密钥分发(quantum key distribution，QKD)，为量子计算机无处不在的“后量子”世界做准备。QKD的优势在于利用了光子的量子特性对密钥进行加密，保证其传输时的安全性。安全的密钥则可以用于加密数据。

2004年，Id Quantique成为第一家利用QKD保障银行转账安全的公司。如今已有数十家企业正在提供QKD产品，基于QKD的网络也迅速扩大，并日趋复杂。日本东芝公司和英国电信公司(BT)建设的网络覆盖了约600平方公里，并且会计事务所安永已经在去年成为其首个客户。这是商业化QKD迈出的一大步，但只是正在迅速扩张的全球量子通信网络的缩影。未来，覆盖全国的商业化QKD网络，甚至是全球化、具备量子安全性的信息高速公路——“量子互联网”将会出现。



数字游戏。构建量子信息技术的基本单元是“量子比特”。经典比特以二进制值“0”或“1”编码信息，而量子比特可以处于两个值的叠加状态，并且可以相互纠缠。利用这些特征，量子计算机可以同时探索多变量问题的多种可能的解决方案。这使其在处理优化任务方面比经典计算机更有效率，例如预测分子结构和天气，或模拟金融市场。但量子计算机威胁数据安全的根本原因是其非常擅长进行大数分解，而这正是当前多数加密技术的基石

它可以将量子和经典计算机连接在一起，用户可以在其中传输敏感数据，而不用担心这些数据有朝一日会被窃取。问题是：我们离这个诱人的前景还有多远？它真的能实现吗？

安全性的关键

加密数据并不困难，在如今的互联网上，通常使用先进加密标准(AES)算法就可以做到。发送者使用一个密钥，通过算法加密信息后，将其通过互联网发送给接收者。后者需要用与加密相同的密钥解密数据，如果没有密钥，则几乎无法解密数据。这听起来很不错，但是应该如何在用户间共享密钥呢？直接通过网络发送密钥显然风险较大，因此需要使用“公钥密码学”加密该密钥。RSA算法是最常见的加密方式，它几乎被用于保障当今互联网的所有安全通信，URL开头的“https”就是一个例子。

RSA需要生成额外的两个密钥(公钥和私钥)来加密AES所用的密钥。公钥对所有人公开，但只有拥有私钥的人才能解密信息。希望获得AES密钥的人只需公开其公钥，待接收到用公钥加密的AES密钥后，使用其私钥解密即可。RSA通过大质数相乘产生密钥，然后将其结合简单的数学算法完成加密。传统的计算机很难逆向分解得到用于生成密钥的质因数，因此也就无法破译数据。据估计，即使用当前最先进的超级计算机，也需数十亿年才能破解使用2048位密钥的RSA标准。

相比之下，量子计算机则可以轻松快速地完成大数的质因数分解。因为这是当前大部分经典密码学的根基，因此会使整个互联网面临风险。虽然目前黑客还无法获得足够强大的量子计算机，但更大的危险在于，黑客可以实施“先截获、再破译”的攻击，即将加密后的数据储存下来，等到今后有更强大的量子设备时再进行解密。

设计可以更好抵御量子计算机攻击的新协议是解决该问题的一种方案。这些无需依赖质因数分解算法的协议被称为“后量子密码学”(post-quantum cryptography)。虽然这类算法正在被加紧研究，并且有望在接下来的几年内推出新的标准，但它们的完备性(integrity)依赖于对量子计算机实际限制的各种假设，而这些假设可能被大多数而非所有用户接受。鉴于QKD是唯一从理论上被证明安全的密钥分发方法，我们更希望从“AES+RSA”转向“AES+QKD”或AES与其他形式的后量子密码学方法结合。

工业影响

Andrew Shields是东芝剑桥研究院量子技术部门的负责人。他表示，非量子物理领域的大数据管理人员终于开始意识到了量子计算对数据安全的威胁。而在他从业的早期，主要的关注点还在1984年提出的BB84协议本身。在BB84协议中，量子比特以单光子偏振态的形式存在，例如：水平偏振光子代表“0”，垂直偏振光子代表“1”。基于量子力学原理，窃听者的测量会不可隐匿地改变被测量子比特的状态，从而使接收者可以推测信息是否被窃听。

BB84协议在理论上无懈可击，但实际生成和长距离传输单光子都非常困难。因此，东芝和英国电信组建的QKD使用了弱激光脉冲作为光源。但是，此类光源中存在一定的多光子脉冲，这些光子可能被编码到同一偏振状态。这里的安全性问题在于，如果一个密钥被编码在同一个脉冲的两个或更多的光子上，窃听者就可以截取其中的一个光子，而不改变其他光子的状态。这将使这些光子不再安全。2003年提出的“诱骗态”方法可以解决这一问题。它在承载真实密钥信息的信号光脉冲之间，掺杂一些光强更弱的“诱骗”光脉冲。当窃听者从总的信号中截取一些光子时，他们会从诱骗态光脉冲取出比信号光脉冲更少的光子，从而改变两者在总体混合脉冲中的比例，而这是接收端可以检测到的明显特征。“尽管在单光子和纠缠光子源方面已经有了很多进展，但使用弱激光源仍然是最有效的，”Shields表示，“使用诱

骗态协议，我们可以获得非常接近使用真正单光子源的理想密钥率。”事实上，基于诱骗态脉冲的协议已经成为长距离QKD的新标准。

在东芝的商用QKD系统中，还开发了一种“复用”技术，使量子光可以与不同波长的经典光一起被发送和接收。“量子通道将不得不依赖于现有的通信基础设施，因为从成本角度来看，更换它是不现实的，”Shields说。虽然在传输数据的光缆中，并非所有的光纤都被使用，因此量子和经典通信光纤传输并非绝对必要。但一种有说服力的观点认为，共享基础设施可以最大限度地发挥QKD在未来的潜力，并允许它在渐趋单芯的光纤网络的边缘接入使用。

搭建量子网络

东芝—英国电信量子城域网络连接了三个核心节点：伦敦西区、伦敦市和斯劳。英国电信光学研究高级经理Andrew Lord称，用户在任意三个节点之一的半径10—15 km范围内都可以注册并使用QKD传输数据。

然而，这种能力来之不易。“我们的主要业务是在客户之间传输数据，无论其是否被加密，”Lord说。“问题是，如何将量子用于其中？”网络需要管理量子信号，保证其到达正确的终端，同时还要修改标准的波分复用(WDM)数据信道。最大的难题是当高功率激光在光纤中传输时，会干扰精密的量子状态。“一不小心，经典数据就会淹没量子通道。”因此，QKD系统设计者必须与WDM厂商合作进行优化，通过缜密的设计才能达到量子网络的要求。

根据Lord所述，该网络自2022年6月以来一直在无故障地运行。除了会计事务所巨头安永，还引起了其他金融部门、医疗保健公司，以及政府的兴趣。这有助于Lord、Shields及其同事确定市场对量子网络的需求，以及如何创建全国范围的广域量子服务。英国电信正在开展一项由英国政府支持的可行性研究，预估使用现有技术实现这样的网络所需的代价。

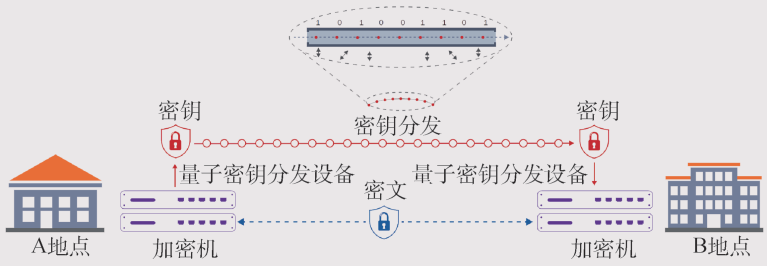
但是，使用现有技术搭建可以跨大西洋的洲际光纤量子网络仍然力有不逮：微弱的量子信号每传输50公里，密钥生成的速率就会降低约10倍。有两种方案可以解决该问题，其一是使用卫星通信。2020年，中国研究者利用“墨子号”卫星在距离1100多公里的青海德令哈站和乌鲁木齐南山站之间实现了QKD。但“墨子号”每晚在地面站上空仅停留5分钟，密钥无法持续更新。更高的轨道可以提供更长的覆盖时间，但同时信号也会更微弱。另一种方法是使用“量子中继器”。该装置放置于长距离信道的中间，将具有纠缠特性的光子对分发到信道两端。输入光子通过与其中的一个光子相互作用，可以将其状态传送到远端的另一个纠缠光子上。因此，量子中继器可以成为拓展量子信号传输距离的桥梁。虽然量子中继器的部分技术已经得到了验证，但全功能的量子中继器尚未实现。

无形的成功？

虽然通往量子互联网的道路仍然布满荆棘，但相关技术正在得到迅速发展，大量资金也在近些年开始涌入这一领域。2018年，欧盟宣布将在未来10年内至少投入10亿欧元，用于开展量子旗舰计划。美国政府仅在今年就拨款近8.5亿美元，更多的资金则通过谷歌、IBM和微软等计算机巨头私下地投入。英国政府承诺在下一个十年期的量子战略规划中拨款25亿英镑用于量子技术开发，并希望能再带动10亿英镑的私人投资。

也许十年内，量子互联网就可能以某种形式出现在我们的身边。但颇具讽刺意味的是，对致力于此的人来说，只有失败才会获得关注。如果他们成功了，我们的敏感数据将不会被窃取，大多数人甚至不会意识到量子计算机曾造成过威胁。

使用单光子流的量子密钥分发



量子密钥分发(QKD)保障数据在互联网中传输而不被量子计算机窃取。它使用由单光子流组成的密钥对数据进行加密，其中“0”是水平偏振的光子，“1”是垂直偏振的光子。当接收者得到密钥时，他们可以使用QKD解密数据，并计算出是否有人窃听。由量子力学保证了这种窃听或测量必将改变密钥的状态。(译者注：QKD仅用于保证密钥分发过程的安全性，加解密仍需使用其他算法来完成。且“0”或“1”代表的是非正交基下的一组光子，如“0”代表水平偏振或另一组编码基下45°偏振的光子)