arXiv:2602.01426v1 [quant-ph] 1 Feb 2026

自由空间与卫星量子通信：原理、实现与挑战

Georgi Gary Rozenman[1] Alona Maslennikov[2] Sara P. Gandelman[3,4]Yuval Reches[3] Sahar Delfan[5] NeelKanthKundu[6,7] Leyi Zhang[8]Ruiqi Liu[81] 麻省理工学院数学系，美国马萨诸塞州剑桥市 02139[2] 波士顿大学化学系，美国马萨诸塞州波士顿市 02215[3] 特拉维夫大学雷蒙德与贝弗莉·萨克勒物理与天文学学院，以色列特拉维夫市 69978[4] 特拉维夫大学伊比与阿拉达尔·弗莱什曼工程学院电气工程学院，以色列特拉维夫市 69978[5] 德州农工大学量子科学与工程研究所物理与天文学系，美国德克萨斯州学院站 77843[6] 印度理工学院德里分校电子应用研究中心 (CARE) 与巴蒂电信技术与管理学院，印度新德里 110016[7] 墨尔本大学电气与电子工程系，澳大利亚维多利亚州墨尔本。[8] 中兴通讯股份有限公司无线与计算研究院，中国北京 100029

garyrozenman@protonmail.com

2026年2月3日

摘要

卫星量子通信是构建安全、全球规模量子网络这一目标中的一项关键进展。这类系统利用量子力学原理，通过量子密钥分发（QKD）及其他量子通信协议，提供无与伦比的安全性。本文全面综述卫星量子通信的现状，重点探讨从地面系统向空间系统的演进。我们探讨离散变量（DV）和连续变量（CV）量子通信技术在卫星部署背景下各自的优势与挑战。本文还讨论了通过墨子号卫星成功实现量子通信等重要里程碑，并概述了主要挑战，包括大气湍流以及

量子中继器的研发。要实现全球量子互联网，这些问题都亟待解决。本综述旨在总结该领域的最新进展，并就卫星量子通信未来的发展方向及推动其持续演进的潜在创新提供见解与展望。

在信息安全至关重要的时代，量子通信已成为一项革命性技术，为数据传输提供前所未有的保护。与易受拦截和网络攻击影响的经典通信方法不同，量子通信利用量子力学的基本定律，确保安全性在理论上牢不可破。卫星量子通信的发展是一项重大突破，它将安全链路延伸至地面基础设施的限制之外，并为构建全球量子网络奠定基础。本文考察卫星量子通信的现状，重点介绍离散变量和连续变量技术领域的重大进展，同时探讨仍然存在的挑战。随着全球对量子卫星的投资不断加速，实现安全互联的量子互联网已渐行渐近。这使卫星量子通信成为下一代安全技术的前沿。

1 量子通信概述

自文明诞生之初，人类的进步便与通信技术的发展密切相关。从烟雾信号和信鸽，到电报、无线电和互联网的发明，每一项技术创新都从根本上改变了社会互动和信息共享的方式。在当今高度互联的世界，通信网络是全球基础设施的基石，使人们能够跨越遥远距离无缝互动 [1]。然而，随着我们对数字通信的依赖日益加深，安全且防篡改的信息交换需求也变得日益迫切 [2, 3, 4]。尽管经典密码学方法已被证明行之有效，但它们仍容易受到日益强大的计算能力和不断演变的网络威胁的影响 [5, 6]。这一日益严峻的威胁推动了向量子通信的范式转变。这项革命性技术利用量子力学定律，确保信息传输在根本上安全。最有前景的发展之一是卫星量子通信，它拓展了地面量子网络的能力，并为构建全球量子安全基础设施奠定了基础 [7, 8, 9, 10, 11]。

随着社会持续受益于先进通信系统带来的无处不在的连接， [12], 安全性已成为所有类型网络中的关键问题 [13]。个人用户和垂直行业都要求高度安全性 [14], ，而量子通信可以为此提供支持 [15, 16]。

量子通信代表了实现安全信息传输方式的突破性转变 [17, 18], ，它利用量子力学原理提供前所未有的安全性水平 [19, 20]。从地面系统迈向卫星量子通信系统的历程，标志着在克服传统通信系统所面临的距离、信道损耗和窃听漏洞等限制方面取得了重大进展 [18, 17]。量子密钥分发（QKD）是量子通信最突出的应用，使双方能够以无条件安全性共享密码密钥，

由量子物理学定律保证 [16]。然而，由于光纤和自由空间信道中的衰减与退相干效应，在长距离上实现量子密钥分发一直颇具挑战 [21, 22]。通过卫星在太空部署量子通信系统为应对这些挑战提供了前景广阔的解决方案，为建立全球量子网络铺平了道路 [13]。

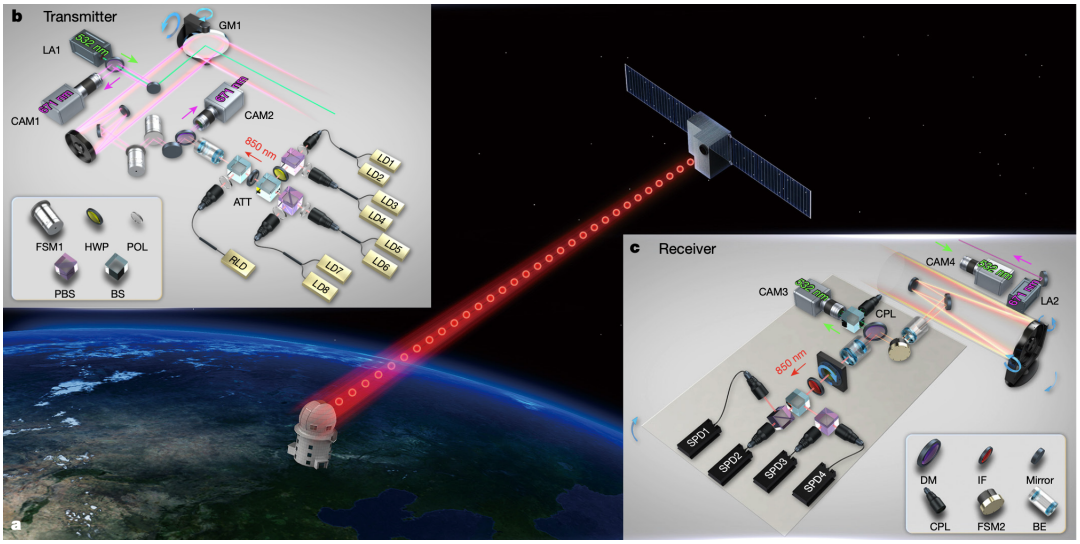

图1：利用墨子号卫星 [23]进行星地量子密钥分发（QKD）的实验装置。墨子号卫星重635千克，运行于距地球约500千米的太阳同步轨道，搭载三个有效载荷，用于开展包括量子密钥分发、贝尔测试和量子隐形传态在内的空间量子实验。卫星的QKD发射机采用八个激光二极管，发射波长约850纳米的衰减脉冲，这些脉冲经过由偏振分束器、半波片和分束器组成的BB84编码模块。编码后的量子信号与用于系统跟踪和时间同步的532纳米绿激光共轴对准，随后经由300毫米口径卡塞格林望远镜发射。光束控制通过用于粗跟踪的双轴万向节镜和用于精跟踪的快速转向镜实现，同时一束低功率671纳米激光用作偏振参考。在地面，兴隆站配备一台1000毫米口径望远镜，利用二向色镜分离入射的532纳米跟踪激光与850纳米量子信号。跟踪光束由相机监测以进行对准，量子信号则由包含分束器和四个单光子探测器的BB84解码器进行分析。地面站还将一束671纳米激光发回卫星，以实现互易跟踪。该双波长同步与混合跟踪系统能够实现精确对准和偏振补偿，从而在最远1200千米的距离上实现高速率量子密钥分发，展示了空间量子通信的重大进展。

发展卫星量子通信的动机，源于克服地面量子网络固有距离限制的需求 [24]。量子通信依赖纠缠和叠加等基本现象，可实现安全信息传输，这是经典系统无法比拟的能力。尽管

地面量子密钥分发系统在较短距离内表现良好，但在光纤和自由空间信道中会遭遇信号的指数级损耗，使其运行范围局限于数百公里。另一方面，基于卫星的系统可以在卫星与地面站之间传输量子信号，从而实现距离远得多的安全链路。通过绕开地球曲率的限制并减少大气衰减的影响，这些系统为构建全球规模的量子通信网络提供了可行方案。

2016年，中国墨子号卫星的发射标志着量子通信发展历程中的一个重要里程碑，证明了大规模开展卫星量子密钥分发的可行性。墨子号成功实现了数千公里距离的量子密钥分发，验证了量子通信协议在真实太空环境中的稳健性。通过在相距遥远的地面站之间建立安全链路，墨子号这样的卫星平台为未来全球量子互联网铺平了道路，使地球上任意两个地点之间都能实现安全信息交换。

2 自由空间量子密钥分发的关键协议

量子密钥分发（QKD）是一种安全通信技术，利用量子力学原理生成并分发密码密钥 [25]。与经典加密方法不同，QKD具有无条件安全性；即使面对计算资源无限的对手，其稳健性也不会受到损害。这使QKD成为金融、政府和国防等领域高安全性应用的理想解决方案 [26]。多年来，人们开发了多种量子密钥分发协议，各有特色和优势。应用最广泛的协议包括BB84、B92和Ekert协议。尽管它们对密钥信息的编码和传输方式各不相同，但都以量子力学的相同基本原理为基础，例如海森堡不确定性原理和不可克隆定理 [27, 25]

无论采用何种协议，所有量子密钥分发系统的目标都是相同的：使双方能够安全地生成一个共享密钥，用于对称加密。此过程可确保任何窃听尝试都会引入可检测的扰动，从而维护密钥交换的安全性 [28]。

2.1 BB84协议

BB84协议由 Charles Bennett 和 Gilles Brassard 于 1984 [29], 提出，是首个实用的量子密钥分发协议，并且至今仍是该领域的基础。如图 2所示，该协议的安全性基于两个关键假设：(1) 当使用非正交态时，只有以扰动量子态为代价才能获取信息，这一效应源于不可克隆定理；(2) 发送方与接收方之间存在经过认证的公共经典通信信道。

在 BB84协议中，Alice 希望将私密密钥安全地传输给 Bob。她首先生成两个 n 比特的随机字符串，$a = (a_1, \ldots, a_n)$ 和 $b = (b_1, \ldots, b_n)$。字符串 a 决定原始密钥比特，而 b 指定用于编码每个量子比特的基。对于每个索引 i，Alice 按如下方式将 a_i 编码为一个量子比特：如果 $b_i = 0$，她使用计算基 $\{|0\rangle, |1\rangle\}$，当 $a_i = 0$ 时制备 $|0\rangle$，当 $a_i = 1$时制备 $|1\rangle$；如果 $b_i = 1$，她使用哈达玛基 $\{|+\rangle, |-\rangle\}$，其中 $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$，当 $a_i = 0$ 时制备 $|+\rangle$，当 $a_i = 1$时制备 $|-\rangle$。 [29]。

以下四种量子比特态用于描述协议态 [30, 31],

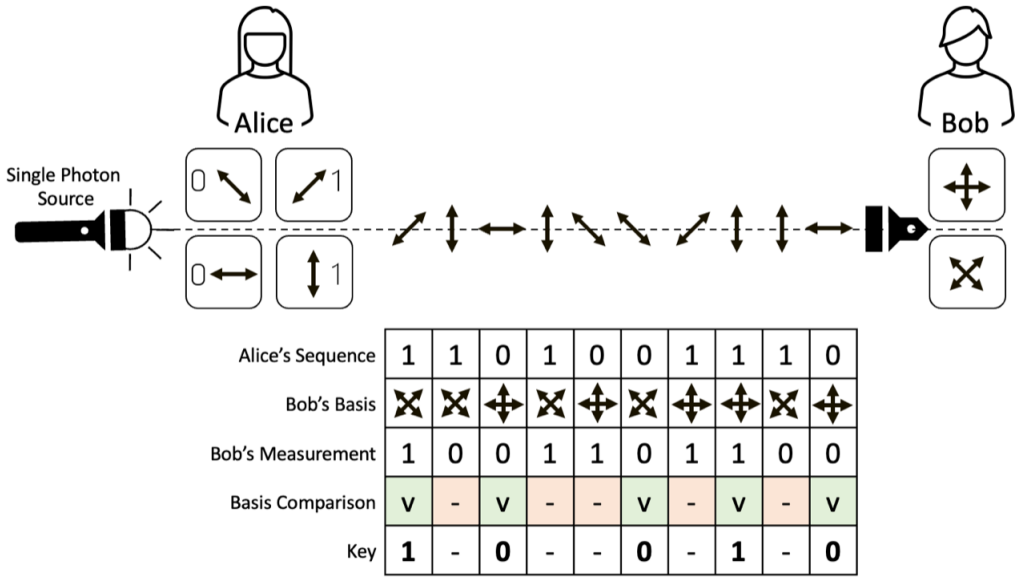

图 2：基于 BB84协议、通过自由空间通信信道实现的量子密钥分发系统示意图。两方（通常称为 Alice 和 Bob）希望通过公共信道进行安全通信。Alice 向 Bob 发送一系列单个光子，每个光子都具有随机偏振态（水平、垂直、对角或反对角）。随后，Bob 以随机选定的基（水平、垂直、对角或反对角）测量每个光子的偏振，并记录结果。之后，Alice 和 Bob 比较部分测量结果，以检测是否存在窃听行为。

$$
\begin{aligned}
|\psi_{00}\rangle &= |0\rangle \\
|\psi_{10}\rangle &= |1\rangle \\
|\psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \\
|\psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.
\end{aligned} \tag{1}
$$

比特 b_i 决定编码所采用的基 a_i （计算基或哈达玛基）。在不知道 b的情况下，无法确定地区分每个量子比特，因为这些量子比特当前处于彼此不正交的态。

通过公开且经验证的量子信道 ε，Alice向Bob发送态 ψ。Bob接收到的量子态由 ε（ρ）$= \varepsilon$（$|\psi\rangle\langle\psi|$）描述，其中 ε 表示信道噪声与潜在窃听的综合效应，我们将该窃听者称为Eve。Bob和Eve在接收到量子比特串 [31]之后，各自拥有自己的态。然而，由于只有Alice知道这一点，Bob或Eve基本上不可能区分这些量子比特的态。此外，不可克隆定理表明，除非Eve已经进行了测量，否则在Bob接收到发送给他的量子比特之后，Eve不可能持有这些量子比特的副本。但如果她为测量选择了错误的基，就会有1/2的概率扰动某个特定的量子比特。

总而言之，如图 2所示，

1. Alice 选择两个经典比特串 $a = (a_1, \ldots\ldots, a_{4n})$ 和 $b = (b_1, \ldots\ldots, b_{4n})$。字符串 a 编码原始密钥比特，而 b 指定编码基。2. 对于每个索引 i，Alice 将 a_i 编码为一个量子比特：若 $b_i = 0$，她使用计算基 $\{|0\rangle, |1\rangle\}$；若 $b_i = 1$，她使用哈达玛基 $\{|+\rangle, |-\rangle\}$。因此，她制备一组包含 $4n$ 个量子比特的序列，并通过量子信道将其发送给 Bob。3. Bob 接收这 $4n$ 个量子比特，并针对每个 i 随机选择一个测量基：计算基（0）或哈达玛基（1）。他的测量结果构成比特串 a' 和 b'，其中 b' 记录了他选择的基。4. Alice 公开她的基串 b。Bob 将其与自己的 b' 进行比较，他们只保留 $b_i = b'_i$ 的位置。这一步“筛选”平均会留下 $2n$ 个共享比特。5. 为了估算误码率（并判断是否可能存在窃听），Alice 和 Bob 公开比较这些比特中的随机子集 n。如果误码率过高，他们就中止；否则继续。6. 最后，Alice 和 Bob 对剩余的 $\sim n$ 个比特应用经典纠错和隐私放大协议，从中提取出长度为 m 比特的更短但安全的共享秘密密钥。

2.2 E91协议

纠缠可用于在双方之间有效地建立秘密密钥。尤其是，纠缠光子对具有固有的安全优势。例如，光子数分离（PNS）攻击 [32] 在基于纠缠的协议中成功的可能性要低得多，因为同时产生多个纠缠光子对的可能性极低 [33]。

在此类协议中，源会生成纠缠态并将其分发给 Alice 和 Bob。该源可以位于任何地方，并由任何实体运行，包括可能心怀恶意的实体。例如，Alice 可以在协议执行前于本地制备纠缠对，也可以由第三方（通常称为 Charlie）将纠缠对分发给 Alice 和 Bob [34]。

在最不利的对抗情形下，纠缠态的来源可能完全由 Eve 控制。因此，该来源被视为不可信，安全性分析通常会假设一种最坏情况：Eve 可以完全访问态制备过程。然而，Alice 和 Bob 共享一条经认证的经典通信信道，Eve 可以窃听该信道上的通信，但无法篡改消息。由于纠缠态在协议执行前就已分发，且 Alice 和 Bob 之间不需要直接的量子信道，基于纠缠的量子密钥分发协议通常能够简化整体安全性分析。

根据 [35], 中所述的协议，Alice 和 Bob 可以使用一个来源，该来源按以下状态分发最大纠缠的量子比特对：

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) \tag{2}$$

分发一系列 $|\Psi^-\rangle_{AB}$ 态，每对中的第一个量子比特分配给 Alice，第二个分配给 Bob。对于每一对纠缠态，Alice 和 Bob 分别从预先设定的集合 Ai 和 Bi中随机选择测量设置。随后，他们公开宣布各自的测量基。在所选方向相同的情况下，即 ($A1$, $B1$) 和 ($A3$, $B3$)，测量结果构成筛选密钥。相反，对于 Alice 和 Bob 测量基不匹配的情况，即 ($A1$, $B3$)、($A1$, $B2$)、($A2$, $B3$) 和 ($A2$, $B2$)，其测量结果用于评估 CHSH不等式，具体如下： [36]

$$S = |\langle A_1B_3\rangle + \langle A_1B_2\rangle + \langle A_2B_3\rangle + \langle A_2B_2\rangle| \tag{3}$$

在理想量子系统中，CHSH参数达到理论最大值 $S = 2\sqrt{2}$ 。然而，在实际实现中， $S > 2$ 便足以证明量子关联和分发密钥的安全性。

2.3 B92协议

Bennett 于 1992 [37], 提出的 B92协议是一种简化的量子密钥分发协议，仅使用两种非正交量子态。与采用四种量子态的 BB84协议不同，B92依靠不可克隆定理和测量引起的扰动这一基本原理，确保其能够抵御窃听。在该方案中，Alice 使用以下非正交偏振态对经典比特进行编码：

$$\begin{aligned} |\Psi_{00}\rangle &= |0^\circ\rangle = |H\rangle \\ |\Psi_{01}\rangle &= |45^\circ\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \end{aligned} \tag{4}$$

每次接收到量子态后，Bob都会随机选择一个测量基——直线基 $\{0^\circ, 90^\circ\}$ 或对角基 $\{45^\circ, -45^\circ\}$。只有当Bob所选的投影算符与Alice发送的量子态不 正交时，测量才会得到确定结果。这些发生概率为 $1 - |\langle\Psi_{00}|\Psi_{01}\rangle|^2$的确定结果构成原始密钥。

该协议的安全性根本上源于非正交量子态无法被完美区分这一事实。任何试图截获并测量量子态的窃听者，都不可避免地会引入可检测的扰动，因此，尽管设计极为简约，B92协议仍是一种可行且安全的量子密钥分发方法 [38]。

2.4 六态BB84协议

六态协议是BB84协议的自然扩展，它通过采用三个互为无偏基而非仅两个基来增强安全性 [39]。除BB84中使用的计算基（Z）和对角基（X）外，六态协议还纳入了泡利 Y 算符的本征态，它们对应右旋和左旋圆偏振态：

$$|\psi_{y^+}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}, \qquad |\psi_{y^-}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix}. \tag{5}$$

从物理上看，$|\psi_{y^+}\rangle$表示右旋（顺时针）圆偏振，此时电场矢量随时间旋转，垂直分量的相位领先水平分量 $\pi/2$。相反，$|\psi_{y^-}\rangle$ 对应左旋（逆时针）圆偏振，此时垂直分量的相位滞后 $\pi/2$。这些状态彼此正交且已归一化，可直接验证：

$$\langle\psi_{y^+}|\psi_{y^-}\rangle = \frac{1}{2}\left(1\times 1 + i\times(-i)\right) = \frac{1}{2}(1-1) = 0. \tag{6}$$

因此，两个圆偏振态构成了量子比特 Y本征态的完备标准正交基，正如水平/垂直偏振和对角/反对角偏振分别构成 Z 基和 X 基一样。 X、 Y和 Z 基的六个状态共同张成整个布洛赫球，从而对量子比特态空间进行完备采样；而四态BB84协议则局限于单个大圆。

该协议的运行方式与 BB84 类似：Alice 随机选择三个编码基（X、 Y 或 Z）之一来制备每个量子比特，而 Bob 则独立地在随机选择的基上进行测量。由于增加了第三个基，Alice 和 Bob 选中相同基的概率从 $1/2$ 降至 $1/3$，这意味着在筛选阶段大约有三分之二的原始比特会被丢弃 [40]。

尽管筛选效率较低，六态协议对窃听的抵御能力却更强。由于 Eve 现在必须在三个互为无偏基中进行猜测，任何截获-转发尝试都会引入更高的量子比特误码率（QBER），使她更容易被发现。因此，这组扩展的非对易测量增强了协议对更广泛量子攻击（包括相干攻击）的安全性 [41]，同时凸显了圆偏振在实现完整布洛赫球覆盖和最大安全对称性方面的关键作用 [42]。

2.5 诱骗态协议

诱骗态协议是量子密钥分发中应用最广泛的方法之一，能够增强对光子数分裂攻击的防护能力 [43, 44]。与理想的 BB84 协议不同，实际的量子密钥分发系统通常依赖弱相干脉冲，而这类脉冲偶尔会发射多个光子。因此，它们容易受到光子数分裂攻击：窃听者可以从多光子脉冲中分出一个

光子，而不扰乱量子态，从而危及安全性，并严重限制安全传输距离和最大信道长度。

为了解决这一问题，诱骗态协议在发送端引入了额外的强度等级：一个信号态和若干个诱骗态 [45]。通过随机改变光子数分布，并仅在传输完成后公布强度等级，Alice 可以防止窃听者有选择地攻击多光子源 [46]。

成功的光子数分裂攻击要求所有强度等级下的比特误码率（BER）保持一致，但由于诱骗态的光子统计特性不同，这是不可能实现的。因此，合法用户可以通过分析每个强度等级下的比特误码率来检测企图实施的光子数分裂攻击，同时还能获得显著更高的安全密钥率和更长的信道距离 [47]。

诱骗态协议通常分三个阶段进行 [48]。1. Alice 向 Bob 发送一系列光子脉冲，并在信号态、诱骗态和真空态之间随机选择。信号态承载实际的量子密钥信息，诱骗态用于监测信道，而真空态则有助于估计探测器处的背景噪声和暗计数。

2. Bob 为每个入射光子随机选择一个测量基（通常为直线基或对角基），并记录测量结果及所用的基。

3. Alice 公开宣布每个脉冲所使用的强度级别（信号、诱骗态或真空态）。双方剔除无法确定的事件，并利用剩余数据估算误码率。只有基匹配的信号态测量结果才用于最终密钥生成。如果诱骗态和真空态呈现出异常的误码统计特征，则表明可能存在窃听。

诱骗态协议的实施显著提升了采用不完美光子源的量子密钥分发系统的安全性，使其能够应用于实际场景。

2.6 使用振幅调制的纯偏振量子比特诱骗态BB84

采用弱相干脉冲（WCP）的偏振编码BB84系统必须抵御光子数分裂（PNS）攻击。引入平均光子数各异的诱骗脉冲，可通过单光子产额 Y_1 和误码率 e_1的不一致性揭示窃听者。全偏振实现方案适用于自由空间、光纤和空间链路，因为它们无需保持干涉稳定性。集成式幅度调制器的最新进展使得如今能够以数百兆赫兹的速率产生三强度（“真空 + 弱 +信号”）脉冲组，同时保持光谱不可分辨性并封闭侧信道 [25]。

逻辑比特编码在偏振态中

$$\{|H\rangle, |V\rangle\}\ (Z\ \text{basis}), \qquad \{|D\rangle, |A\rangle\}\ (X\ \text{basis}),$$

由单个增益开关激光器产生。偏振调制器设置基和比特，超快幅度调制器控制平均光子数 $\mu \in \{\mu_{\text{sig}}, \mu_{\text{dec}}, 0\}$。由于强度是光脉冲的属性，而不是偏振态中编码的量子信息的一部分，因此只要调制器与偏振无关，强度调制就不会扰动量子比特 [49]。

嵌入萨尼亚克干涉仪中的 $LiNbO_3$ 相位调制器可将相位调制转换为强度调制，从而实现速率超过 600 MHz、消光比大于 30 dB 的逐脉冲衰减。采用单一激光源可确保所有发射脉冲具有相同的光谱

和时间特性，从而消除“使用哪台激光器”侧信道，并抑制可能危及安全性的图案效应。

在三强度诱骗态实现中，Alice 随机制备具有不同平均光子数的光脉冲。平均光子数为 μ_{sig}的信号态用于密钥生成，而平均光子数为 μ_{dec}的诱骗态则专门用于信道参数估计。第三类脉冲对应平均光子数为 $\mu_{\mathrm{vac}} = 0$的真空态，可用于直接估计背景和探测器暗计数贡献。典型工作参数为

$$\mu_{\mathrm{sig}} \simeq 0.5, \qquad \mu_{\mathrm{dec}} \simeq 0.1, \qquad \mu_{\mathrm{vac}} = 0,$$

相应的制备概率为

$$p_{\mathrm{sig}} \approx 0.8, \qquad p_{\mathrm{dec}} \approx 0.1, \qquad p_{\mathrm{vac}} \approx 0.1.$$

这种强度与概率的选择在安全密钥率效率和多光子发射概率之间取得平衡，从而能够对单光子产额和误码率给出严格界限，同时在实际的自由空间和卫星量子密钥分发系统中保持高吞吐量 [48]。

对于相位随机化弱相干脉冲，光子数服从泊松分布。因此，总增益 Q_μ 和误码增益 $Q_\mu E_\mu$ 为：

$$Q_\mu = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} Y_n, \qquad Q_\mu E_\mu = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} Y_n e_n.$$

对于两种非零强度，线性规划界 Y_1 和 e_1 可对 $\mu_{\mathrm{dec}} \ll \mu_{\mathrm{sig}}$给出严格界限。有限尺寸修正通常按 $O\left(\sqrt{\ln(1/\varepsilon)/N}\right)$的量级变化。

2.7 相干单向协议

相干单向（COW）协议利用分布在时间仓对中的弱相干光脉冲来编码密钥比特。在此方案中，Alice 发送一个脉冲作为第一个时间仓，并在第二个时间仓发送真空态，以编码比特“0”；而比特“1”则编码为先发送真空态，随后发送一个脉冲。为检测窃听并监控信道完整性，Alice 会随机穿插诱骗序列，通常是两个连续脉冲（脉冲–脉冲）或两个连续真空态（真空–真空） [50, 51, 52]。这种方法将时间仓编码与相干性监测相结合，确保长距离安全通信。

Alice 的装置以连续波（CW）激光器为起点，该激光器提供稳定的相位参考，这对于监测脉冲间的相干性至关重要。光束经强度调制器调制，根据所需的比特模式或诱骗序列切分为离散的时间仓脉冲。随后，光学衰减器将脉冲衰减为弱相干态（WCP），其典型光子数为 $\mu \sim 0.1$–0.2。这确保大多数脉冲中包含零个或一个光子，从而在使用现成激光源的同时实现量子行为 [53]。

Bob 的装置使用无源分束器（例如 90/10）将入射信号分成两条独立路径。大部分信号（数据线路）用于密钥生成，其余信号（监测线路）用于相干性验证。在数据线路上，时间分辨单光子探测器（SPD）记录光子的到达时间。在早期时间仓中探测到光子对应比特“0”，而在晚期时间仓中探测到光子对应比特“1”。在监测线路上，不平衡马赫–曾德尔干涉仪（MZI）

引入等于一个时间分箱的延迟，使相邻脉冲之间能够发生干涉。该干涉仪具有两个输出端口，每个端口均连接到探测器 D_c （相长干涉）以及 D_d （相消干涉）。这些探测器的相对计数使 Bob 能够计算干涉可见度 [54]:

$$V = \frac{P(D_c) - P(D_d)}{P(D_c) + P(D_d)}, \tag{7}$$

其中， $P(D_c)$ 和 $P(D_d)$ 分别是每个输出端观测到的探测概率。较高的可见度表明相干性得以保持，而偏差则意味着存在信道噪声或窃听。

Bob 使用精确的时间戳记录所有探测事件。量子传输完成后，他公布发生探测事件的时间仓。随后，Alice 公开指出哪些时隙对应诱骗态，哪些对应数据，从而使 Bob 能够筛选原始密钥、估算量子比特误码率（QBER），并评估信道相干性 [55]。

令 $|\alpha\rangle$ 表示相干态， $|0\rangle$ 表示真空态。Alice 在每对时间分箱中制备的量子态为 [56]:

$$|\phi_0\rangle = |\alpha\rangle \otimes |0\rangle, \tag{8}$$
$$|\phi_1\rangle = |0\rangle \otimes |\alpha\rangle, \tag{9}$$
$$|\phi_D\rangle = |\alpha\rangle \otimes |\alpha\rangle. \tag{10}$$

在监测干涉仪中，相邻的相干脉冲会发生干涉。

COW协议对光子数分裂攻击具有内在的鲁棒性。窃听者无法在不破坏相位相干性的情况下，无侵入地测量各个脉冲的时间分箱占据情况；因此，任何窃听尝试都会导致干涉可见度出现可测量的下降。这使得可见度监测成为对抗窃听的有效对策 [57]。

2.8 使用类量子比特态（傅里叶量子比特）的高维量子密钥分发协议

高维量子密钥分发（HD-QKD）通过在比传统 BB84 [58] 等协议所用的二维系统更大的希尔伯特空间中编码信息，推动了量子通信的重大进展。这种方法利用轨道角动量（OAM）[59], 时间仓编码和空间模式等自由度，可提高每个光子的信息容量、增强噪声容忍度，并提升安全性。

传统量子密钥分发协议使用二能级量子系统（量子比特），每个光子编码一个比特。相比之下，高维量子密钥分发使用量子多能级比特——d能级量子系统——每个光子可编码多个比特，从而提高密钥率，并有望增强抵御窃听的能力。

高维量子密钥分发（HD-QKD）领域的一项最新进展，是提出了一种兼具大希尔伯特空间优势与基于量子比特方案实验简便性的协议。在这种方法中，Scarfe 等人[58] 提出了一种类似 BB84 的高维协议，采用所谓的傅里叶量子比特（F-qubits）；它们是嵌入在 d维计算基中的类量子比特叠加态 [58]。

与依赖由所有 d基态的平衡叠加构造而成的互为无偏基（MUBs）的传统高维量子密钥分发协议不同，F-qubit 协议用仅由两个 计算基元素叠加而成的状态取代傅里叶基。一个

F-qubit 的形式为

$$|\phi_{jk}^{(m)}\rangle = \frac{1}{\sqrt{2}}\left(|j\rangle + \omega_d^m\,|k\rangle\right), \tag{11}$$

其中 $\omega_d = e^{2\pi i/d}$，$j < k$，以及 $m \in \{0,\ldots,d-1\}$。尽管这些状态相对于计算基并非相互无偏，但它们仍具有足够的相位灵敏度，可通过有效的相位误差估计来界定 Eve 所能获取的信息[60]。

该协议的执行方式与 BB84 类似。Alice 和 Bob 通过在计算基中制备和测量状态 $\{|n\rangle\}$来生成原始密钥材料，而 F-qubit 状态仅用于参数估计。通过测量 F-qubit基中的误差统计数据，Alice 和 Bob 可以间接推断与计算基相关的相位错误率，从而在集体攻击（进而也包括相干攻击）下界定 Eve 可获取的信息。重要的是，尽管用于检测的状态所支持的维数较低，该方案仍能实现无条件安全性。

A 该方案的关键结果是保留了高维量子密钥分发的主要优势。Th e 秘密 每个筛选后的光子的密钥率按以下方式变化

$$R = \log_2 d - h_d(E_d) - h_d(E_d^{\mathrm{ph}}), \tag{12}$$

其中，E_d 和 E_d^{ph} 分别是 dit 误码率和相位误码率，而 h_d 是 d维香农熵。因此，该协议实现的信息密度超过每个探测到的光子 1 比特，同时保持了高维系统所特有的、随维数增加而提高的可容忍误码率。

在实验方面，Scarfe等人 在 $d = 4$中使用光的轨道角动量（OAM）模式，在有噪声的实验室自由空间信道中演示了该协议。通过利用 F-qubit 状态相较于传统傅里叶模式更大的空间延展范围和更好的模式重叠，他们在真实噪声条件下测得的筛选密钥率为每个光子 $R \approx 1.28$ 比特。图 1–3 展示了典型的 F-qubit 模态结构、实验性 OAM 实现，以及用于相位误差估计的相关概率结果矩阵。

从系统角度看，F-qubit 协议显著降低了状态制备和探测的复杂度。由于每个检验态无论 d 如何都只涉及两个模式，实验开销不会随维数增加，因此该方法特别适用于空间模式、时间分箱和集成光子实现。这种类量子比特的高维量子密钥分发架构，因而为在带宽受限的自由空间和卫星信道中实现高密钥率、耐噪声的量子密钥分发提供了一条切实可行的途径。

在高维量子密钥分发中，发送方（Alice）和接收方（Bob）使用一组 d 正交态（模式），并结合互为无偏基（互 unbiased 基） $\{|\psi_i\rangle\}_{i=1}^{d}$，满足

$$\langle\psi_i|\psi_j\rangle = \delta_{ij}, \tag{13}$$

$$|\langle\phi_i|\psi_j\rangle|^2 = \frac{1}{d}, \quad \forall i,j \in \{1,\ldots,d\} \tag{14}$$

其中 $\{|\psi_i\rangle\}$和 $\{|\phi_i\rangle\}$是两个互 unbiased 基 [62]。

对于保真度F （无差错概率）的 d维协议，Alice与Bob之间的互信息由 [63]中的式(9)给出：

$$I_{AB} = \log_2 d + F\log_2 F + (1-F)\log_2\left(\frac{1-F}{d-1}\right) \tag{15}$$

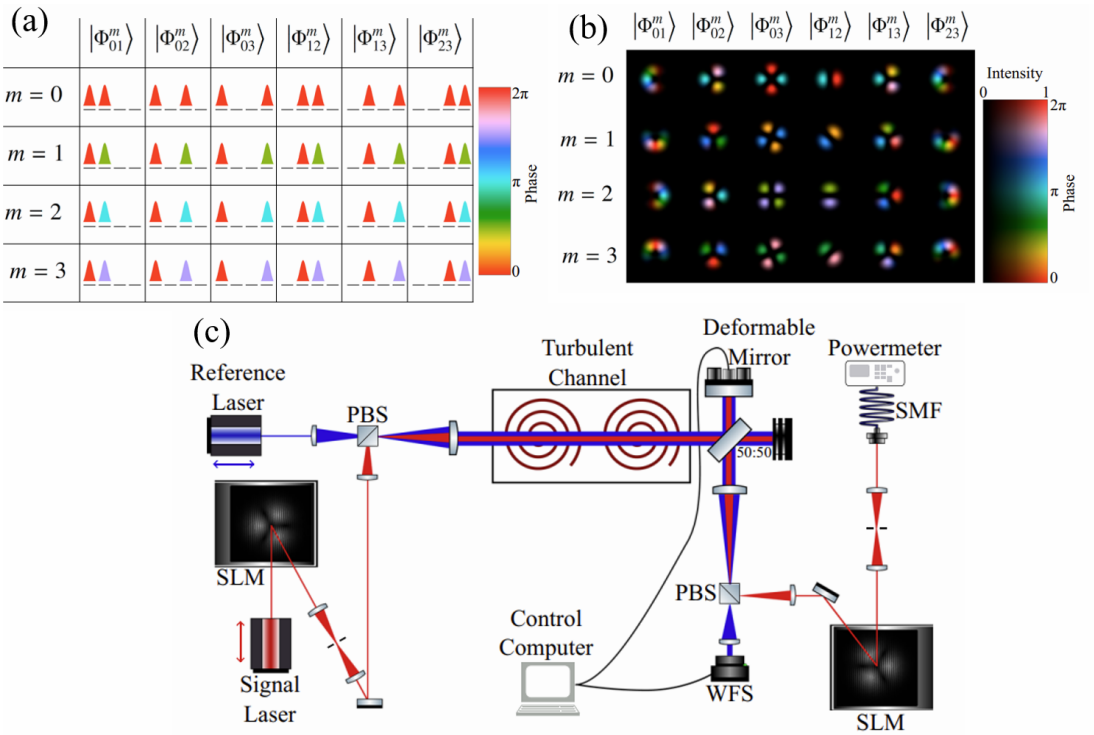

图 3：使用类量子比特态（傅里叶量子比特）的高维量子密钥分发（高维量子密钥分发）。（a） $d = 4$时间仓编码中傅里叶量子比特（F-qubit）态的概念示意图。逻辑基态占据不同的时间仓，而傅里叶量子比特由仅包含两个逻辑态的等权叠加态构成，并具有离散相对相位 $\omega_d^m = e^{2\pi im/d}$，因此无需使用完整的互为无偏基即可估计相位误差。（b）在含噪自由空间信道中，利用光的轨道角动量（OAM）模式实现 F-qubit 协议的实验装置。空间光调制器（SLM）生成并投影拉盖尔–高斯模式的类量子比特叠加态，自适应光学则在探测前补偿湍流引起的畸变。（c）四维空间中 F-qubit 基的测量概率结果矩阵，展示理想理论分布（左）以及经湍流信道传输后实验观测到的分布（右）。这些统计数据可用于间接重建相位错误率，并表明每个筛选后的光子可实现超过一个比特的安全密钥生成[58]

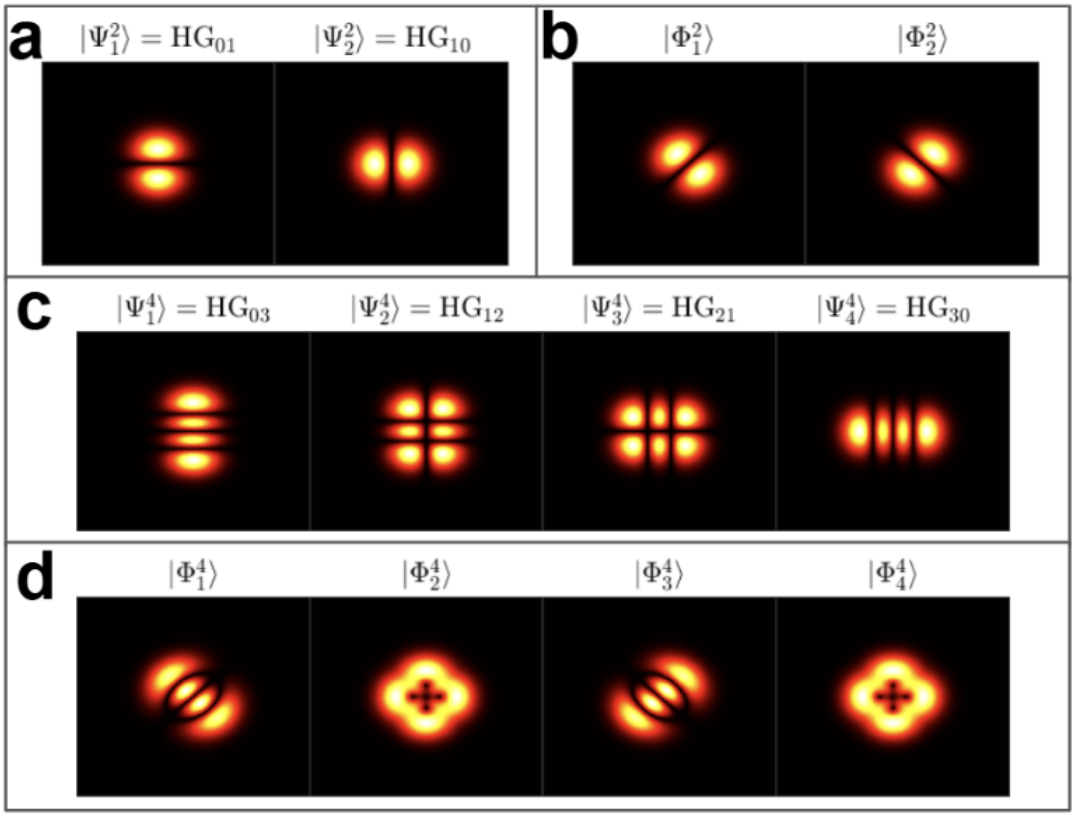

图4：维度为 $d = 2$ 的厄米特-高斯基模拟振幅（a），以及维度为 $d = 4$ 的厄米特-高斯基模拟振幅（c）及其互 unbiased 基（b、d） [61]。

其中， $F = 1 - Q$ 和 Q 是量子比特误码率（QBER）。

Th该公式将标准二元互信息推广到了更高维度，并 d 明确 地同时纳入了维度 d和保真度。

高维量子密钥分发（HD-QKD）的一种特别强大的实现方式是使用光的空间模式，尤其是携带轨道角动量（OAM）的空间模式 [64]。空间模式在光子的横向空间分布中构成正交基，从而能够在高维希尔伯特空间中进行编码 [65]。

空间模式，如厄米-高斯（HG）或拉盖尔-高斯（LG）模式，提供了可扩展的正交态 [66]:

$$\mathrm{HG}_{mn}(x,y) = H_m\left(\sqrt{2}\frac{x}{w(z)}\right) H_n\left(\sqrt{2}\frac{y}{w(z)}\right) \exp\left(-\frac{x^2+y^2}{w^2(z)}\right) \tag{16}$$

其中， H_m 是厄米多项式， $w(z)$是束腰。

空间模式的互 unbiased 基可以利用傅里叶关系构造:

$$|\Phi_n^d\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp\left(\frac{2\pi i n k}{d}\right) |\Psi_k^d\rangle \tag{17}$$

纯相位空间光调制器（SLM）通常用于制备和测量这些态。

在完美保真度（$F = 1$）下，Alice 与 Bob 之间的互信息达到$I_{AB} = \log_2 d$ 比特/筛选后的光子，体现了高维量子密钥分发在信息容量方面的根本优势。此外，最大可容忍的量子比特误码率（QBER）会随维数增加而提高：对于 $d = 2$ ，阈值为 $Q_c \approx 14.64\%$；对于 $d = 3$ ，阈值升至$Q_c \approx 21.13\%$，并且在更高维数下 [63]仍会继续增加。这种增强的误差容限使高维量子密钥分发系统即使在噪声更大或湍流更强的信道条件 [67]下，也能维持安全密钥生成。

然而，这些优势也伴随着实际的权衡。随着维数 d 增加，模式串扰和对准误差变得更加显著，而高阶空间模式表现出更大的光束发散以及对光学像差的更高敏感性。这些影响可能降低可实现的密钥率，并限制最大传输距离。因此，最优的高维量子密钥分发实现 [68] 必须在编码基的维数、系统稳定性、信道保真度和可用探测资源之间进行平衡，以最大化安全性和性能。

3 纠错协议的进展

量子密钥分发（QKD）系统必须协调光子损耗、探测器缺陷和环境噪声所导致的错误，以便合法用户 Alice 和 Bob 获得相同的共享秘密密钥。由于经典纠错不可避免地会向窃听者泄露部分信息，现代量子密钥分发协议将错误协调和隐私放大整合为统一的后处理 流程，用以确定最终密钥长度和安全性证明 [69]。

3.1 经典协调协议

最早的协调方法 *Cascade* 会在多轮中进行交互式奇偶校验，以识别并纠正不匹配的比特。尽管其比特错误效率 β 可接近

0.99，但多轮通信开销会限制长距离和基于卫星的链路的吞吐量，而这类链路的延迟不可忽略。

为克服这一问题，采用低密度奇偶校验（LDPC）码或极化码的一次性前向纠错（FEC）方案已成为标准。LDPC码可通过置信传播算法实现近乎实时的译码，并在典型量子比特误码率（1–5%）下达到 $\beta \approx 0.95$–0.98 的效率。如今，基于现场可编程门阵列和专用集成电路的LDPC译码器实现可达到每秒数十兆比特的处理速度，即使在仅持续数百秒的短暂卫星过境期间，也能实现实时密钥蒸馏。极化码利用信道极化，同样已被证明在降低存储需求的同时能够逼近香农极限，因此适用于嵌入式量子密钥分发载荷。

3.2 连续变量纠错

在连续变量（CV）量子密钥分发中，Alice和Bob交换的是相关的高斯变量，而非离散比特。在此，协调（亦称信息协调）需要将连续样本映射为离散码字。多维协调与多边低密度奇偶校验码相结合，即使在低信噪条件下也能实现较高效率（$\beta > 0.9$）。实时实现采用迭代置信传播译码器，利用信道提供的软信息，使连续变量量子密钥分发即使在过量噪声和衰落存在的情况下，也能通过城域和卫星链路运行。

3.3 隐私放大与有限密钥分析

协调后，隐私放大会消除可能泄露给窃听者的任何残余信息。具体做法是对协调后的密钥应用通用哈希函数（例如托普利兹或里德–所罗门矩阵），以压缩密钥。对于卫星过境期间这类有限数据块，最终密钥长度 l 满足

$$l = s_{\mathrm{raw}}[1 - h(Q)] - \mathrm{leak}_{\mathrm{EC}} - \Delta_{\mathrm{sec}},$$

其中， s_{raw} 是筛选比特数， Q 是测得的量子比特误码率，$\mathrm{leak}_{\mathrm{EC}}$ 量化了纠错过程中泄露的信息，而 Δ_{sec} 则考虑了有限样本统计偏差。有限密钥分析可确保短时量子链路（例如持续数分钟的单次卫星过境所建立的链路）也具有可组合安全性。

3.4 新兴趋势

近期进展聚焦于自适应和硬件加速的纠错框架。机器学习辅助译码器会根据不断变化的信道条件动态调整低密度奇偶校验参数，从而降低湍流或衰落信道中的协调失败率。将基于图形处理器的低密度奇偶校验译码器与现场可编程门阵列隐私放大引擎相结合的混合前向纠错架构已在实验室量子密钥分发系统中得到验证，其后处理吞吐量超过 100 Mb/s。在空间搭载实现中，执行星载低密度奇偶校验译码的抗辐射现场可编程门阵列可最大限度地降低经典下行带宽需求，并支持完全自主的卫星量子密钥分发运行 [70]。

总之，这些在纠错编码、有限密钥安全性和自适应后处理方面的进展，为下一代自由空间和卫星量子通信提供了关键支撑，弥合了实验室演示与可全球扩展的量子网络之间的差距。

4 基于光纤的量子密钥分发最新进展 n

量子密钥分发（QKD）的发展伴随着光子源和探测器技术的进步而迅速推进。首个突破100 km距离门槛的基于纠缠的量子密钥分发实验采用了BBM92协议，并使用时间-bin纠缠光子对。该系统集成了基于NbN纳米线的超导单光子探测器（SSPDs），针对电信波长（1.5 μ m）下的高速探测进行了优化；同时采用周期性极化铌酸锂（PPLN）波导作为高亮度纠缠光子源。为确保相位相干性，实验使用了稳定的平面光波电路马赫–曾德尔干涉仪（PLC-MZIs）。与早期的基于纠缠的量子密钥分发系统相比，这项工作取得了显著进步，凭借更高的光源亮度和探测效率，将可行传输距离从数十公里拓展至一百多公里 [71]。

此后不久，连续变量量子密钥分发（CVQKD）在24.2 km光纤上得到实验演示，安全密钥率达到3.45 kbps。该系统采用偏振复用和频率转换技术传输连续波本振（CW-LO），同时将导波声波布里渊散射（GAWBS）抑制了27 dB以上。尽管在低信噪条件下性能受到协调效率的限制，该结果仍展示了连续变量量子密钥分发在城域规模距离上实现高速安全通信的潜力 [72]。

随后的进展实现了量子密钥分发在90 km距离上与双向1.25 Gb/s经典数据业务并行传输的演示。该演示采用诱骗态 BB84，结合亚纳秒门控InGaAs雪崩光电二极管（APDs）和时间滤波以抑制拉曼噪声。系统在50 km处达到507 kbps，在90 km处达到7.6 kbps，并在65 km上成功与10 GbE共存，为量子密钥分发与实际光纤基础设施的集成迈出了重要一步 [73]。

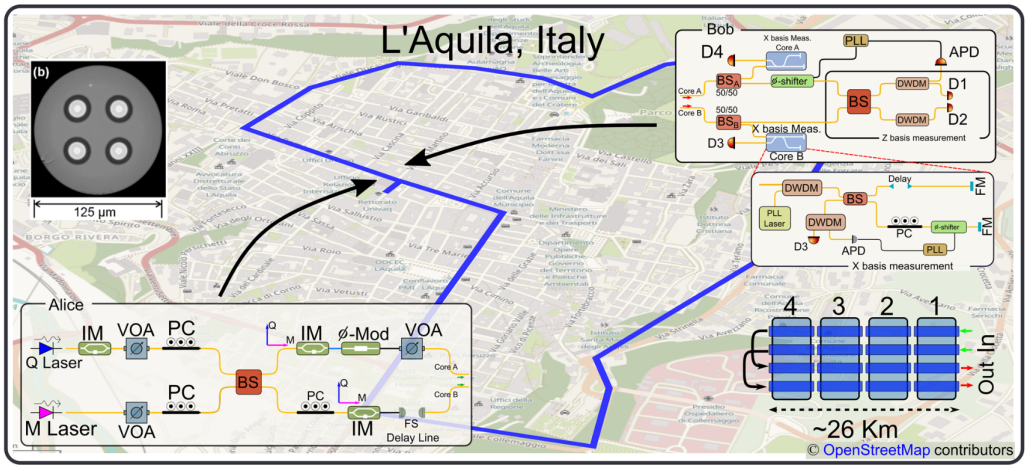

图 5：通过多芯光纤现场部署的高维量子密钥分发。混合时间-路径编码态通过一条 52 km 环路传输，该环路由已部署的四芯光纤中的两个空间纤芯构成。该系统采用诱骗态调制，并使用双频带锁相环实现主动相位稳定。改编自：*Nature Communications*，2024年。

为进一步延长安全通信距离，一项创纪录的测量设备无关量子密钥分发（MDIQKD）实现利用超低损耗光纤达到了 404 km。这

套系统采用经过优化的四强度诱骗态协议和高效率超导纳米线单光子探测器（SNSPDs），同时考虑了有限尺寸统计效应。通过消除对测量设备的信任，MDIQKD 增强了抵御基于探测器的侧信道攻击的安全性，并证实了未来卫星兼容链路的可行性 [74]。其他研究则着眼于降低系统成本。一项演示采用了发光

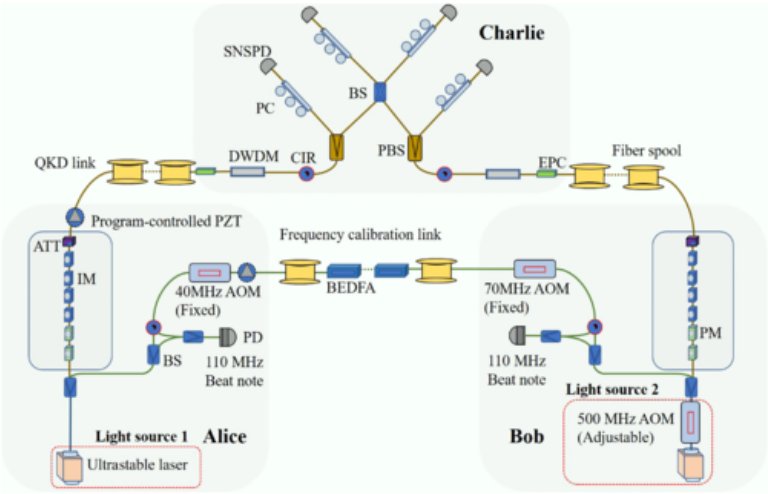

图 6：404 km MDI-QKD 的示意图。Alice 和 Bob 的独立光源生成相位随机化的弱相干态，并在中心节点（Charlie）处发生干涉。诱骗态技术和先进的超导纳米线单光子探测器可实现安全的长距离通信。改编自：Yin 等人 [75]

采用 1310 nm 发光二极管（LED）而非激光器，结合无源光学元件和诱骗态协议，在 1 km 距离上实现了 10.9 kbps 的安全密钥率。这种低成本架构展现了量子密钥分发在本地及城域应用中的可行性 [76]。迄今最先进的系统结合了高相干激光源、外差频率校准和超导探测器，以实现发送或不发送双场量子密钥分发（SNS-TFQKD）协议。该系统通过 658 km 的超低损耗光纤运行，实现了每脉冲 9.22×10^{-10} 比特的安全密钥率（0.092 bps），并经有限尺寸分析验证。值得注意的是，该系统还同时充当分布式振动传感器，可在 500 km 的校准链路上以 1 km 的精度定位环境扰动。这些成果拓展了量子密钥分发的距离极限，并展示了其在通信感知融合网络中的多功能潜力 [77]。

5 量子通信进展：重要实验里程碑

5.1 1 km 自由空间量子密钥分发的实践

Buttler 等人（1998）展示了一套实用的自由空间量子密钥分发系统，该系统采用 B92协议和非正交偏振态，在夜间通过 1 km 的大气路径运行。该装置使用一台波长为 772 nm、衰减至每脉冲 0.1 个光子的二极管激光器，通过普克尔斯盒对偏振进行编码，并使用单光子探测器和空间滤波

来抑制背景噪声。系统实现了可靠的比特生成，误码率低于 1.5%，验证了在真实户外环境下进行安全密钥交换的可行性。该研究还评估了地面到卫星量子密钥分发的可行性，估算采用标准光学设备时可实现的夜间密钥率为 35–450 Hz，并预测使用自适应光学可带来显著提升。这些结果彰显了量子密钥分发在长距离视距应用中的实用潜力，包括卫星重新密钥协商。该系统在长达 950 m 的自由空间路径上成功实现了量子密钥分发，且比特误码率较低。在 950 m、每脉冲 0.1 个光子的条件下，Bob 检测到 50 比特/秒，与理论预测相符。240 m 处的量子比特误码率为 0.7%，500 m 和 950 m 处均为 1.5%。通过二维奇偶校验，可从原始序列中生成无误码密钥。研究依据两种窃听模型——截获重发攻击和分束器攻击——分析了系统的安全性，结果表明系统具有较强的鲁棒性，隐私放大能够抵御极少量的信息泄漏。这些结果支持了安全自由空间量子密钥分发的可行性，并表明通过自适应光学等改进，此类系统有望以切实可行的密钥率扩展至卫星通信。

5.2 日光与夜间条件下的10公里自由空间量子密钥分发实践

Hughes 等人（2002年）利用BB84协议，证明了在日光与夜间条件下经10千米大气链路实现自由空间量子密钥分发的可行性。尽管存在背景噪声，该系统仍实现了密码学级密钥生成，并建立了广义性能模型，用以在不同大气与仪器条件下外推其表现——表明量子密钥分发在夜间可延伸至45千米。这些结果为可扩展的视距量子安全通信系统奠定了基础。

发射机（Alice）采用四台772纳米二极管激光器，各自编码一种BB84偏振态。1兆赫兹时钟先触发1550纳米定时脉冲，随后触发1纳秒数据脉冲，并平均衰减至 < 1 光子。在发射前，通过光谱滤波与空间滤波抑制背景光。

接收方（Bob）使用一台18厘米卡塞格林望远镜、0.1纳米干涉滤光片，并利用单光子探测器（SPDs）进行被动偏振分析。如图19示意所示，光子经分束器路由至对应于直线基和对角基的偏振分析器；探测在窄 $\sim$ 1纳秒时间窗口内记录，并与所发射脉冲同步。

链路跨越新墨西哥州两处高海拔地点，距离为 9.81 千米，并配备视觉对准摄像机和支持系统运行的无线公共信道链路。系统在不断变化的条件下始终可靠运行：

- **日光($\langle\mu\rangle \approx 0.49$)**：筛选密钥率为每秒 100–2000 比特/，比特误码率（BER）为 $\sim 5\%$。
- **夜间($\langle\mu\rangle \approx 0.14$)**：筛选速率相当，误码率降低至 $\sim 2\%$。

白天，背景光主导了噪声预算；而夜间，探测器暗计数则成为限制因素。经过密钥筛选、纠错和隐私放大后，最终生成的秘密密钥保密效率最高可达每个传输比特 8×10^{-4} 个秘密比特。在昼夜联合试验中，总共提取出超过 1.68×10^{5} 个秘密比特，且所有密钥均通过了标准密码学随机性测试。

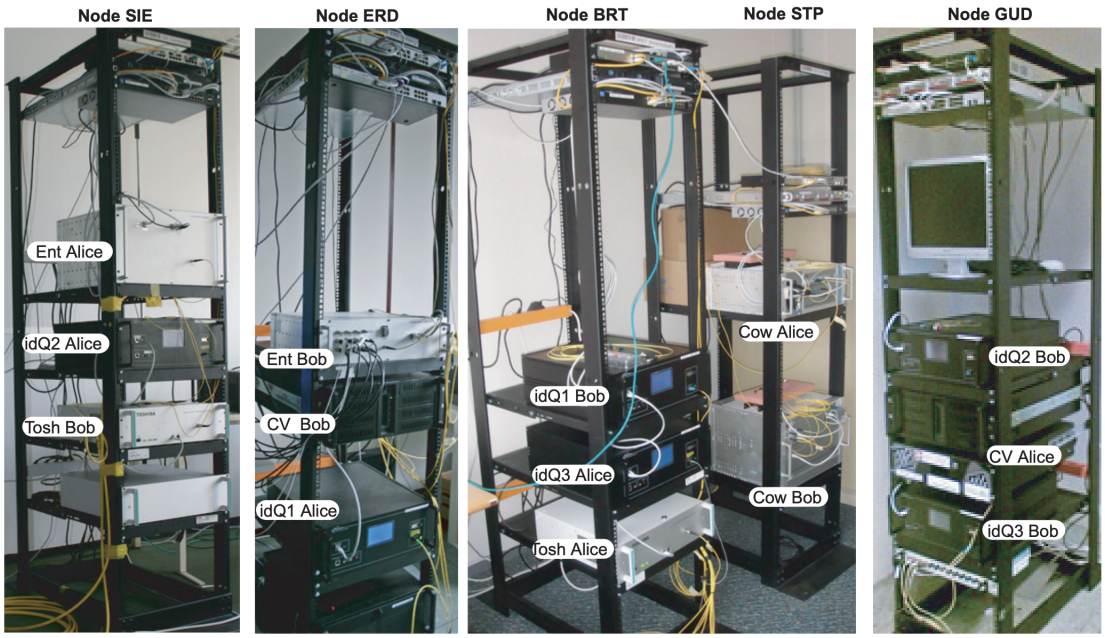

图7：维也纳城域现场试验中部署的SECOQC量子密钥分发（QKD）网络节点机架照片。每个19英寸机架集成了来自多家供应商的偏振编码和相位编码QKD模块、密钥管理单元、经典认证硬件、光配线架和冗余电源，从而支持在全城范围的SECOQC试验床内对异构量子链路进行即插即用互连。转载自 [78]。

该系统经证明能够抵御现实条件下的截获-转发攻击和光子数分离攻击，凸显了自由空间量子密钥分发在真实环境中的实用可行性 [79]。

5.3 DARPA量子网络的工作

DARPA量子网络由 BBN Technologies、哈佛大学和波士顿大学于2005年合作开发，是首个投入运行的量子密钥分发网络。与早期独立运行的量子密钥分发系统不同，该网络通过光纤和自由空间光链路，在城域规模距离上实现了持续的真实环境密钥分发。其目标是证明量子安全通信能够以联网规模实现，并支持多种量子密钥分发技术，在实际条件下可靠运行。该网络覆盖马萨诸塞州剑桥，跨度最长达29千米，使用标准 SMF-28光纤，并包含六个节点，其中包括 Alice、Bob、Anna 和 Boris，节点之间可进行可编程光交换。网络集成了多个量子密钥分发平台：BBN 的 Mark 2 弱相干相位调制光纤系统、与波士顿大学合作开发的偏振纠缠光子系统，以及由美国国家标准与技术研究院和 QinetiQ 提供的高速自由空间系统。所实现的量子密钥分发协议包括 BB84、通过 Cascade 和 Niagara 实现的纠错、熵估计、隐私放大，以及基于 IPsec 的身份验证。软件栈支持多种熵模型，包括 Bennett、Slutsky、Myers-Pearson 和 Shor-Preskill，也支持不同的筛选模式，例如经典 BB84 和 SARG。性能因链路配置而异。例如，Anna 向 Bob 发送平均光子数为0.5的脉冲时，密钥生成速率约为每秒1,000个秘密比特，量子比特误码率（QBER）为3%。相比之下，Boris 链路衰减较高（11.5 dB），且探测器效率低，因此需要暂时在$\mu = 1.0$的条件下运行，最终密钥生成量为零。Mark 2系统展现出稳定的运行性能，脉冲速率达每秒330万次，并可调节光子速率和衰减设置，以匹配光纤跨度损耗。系统设计如图7所示。光纤长度和衰减带来了实际挑战，例如连接器引起的损耗，以及有效路径长度超过50千米的链路跨度，因此需要仔细校准光子速率和衰减设置。网络拓扑同时采用光纤和自由空间链路，并包含部分投入运行的纠缠光子节点（Alex 和 Barb）；此外，还计划使用更多 QinetiQ硬件进行扩展。截至2005年初，DARPA量子网络已投入运行，并展示了量子密钥分发在多节点、城域规模环境中的实用可行性，为未来可扩展的量子安全通信奠定了重要基础[80]。软件改进（例如 Niagara 前向纠错（FEC）协议）显著降低了通信开销和 CPU使用率，相较于 Cascade，编码效率仅略有降低。持续推进的工作重点是启用纠缠和自由空间链路、部署超导探测器等改进硬件，并完善通信协议。最终，该项目展示了如何在复杂的真实网络中持续提供稳健的密码服务，即使面对硬件差异、衰减和环境挑战也不例外 [81]。

5.4 维也纳的 SECOQC 量子密钥分发网络 a

作为SECOQC项目的一部分，慕尼黑大学于2009年开发了一套自由空间量子密钥分发系统，以评估安全的最后一公里量子通信的可行性，其路径为一条

视距城市链路。该系统设计用于与城域量子密钥分发网络中的光纤节点集成，利用偏振编码弱相干脉冲（WCP）展示了稳健的高速率密钥交换。它基于带诱骗态的BB84协议，采用经衰减的850纳米激光脉冲，将信息编码为四种偏振态。发送方（Alice）位于西门子论坛（节点FRM），使用激光二极管产生偏振和光子数可变的弱脉冲。接收方（Bob）位于相邻建筑（节点ERD），使用硅雪崩光电二极管（Si-APD）探测入射光子。望远镜收集自由空间光束，光束随后穿过一系列旨在抑制背景噪声的光学滤光片和光谱滤波器。窄带通滤波器、空间滤波以及借助实时反馈严格保持对准，使系统能够在各种光照条件下可靠运行。密钥生成率超过10 kbit/s，高于典型的短距离光纤量子密钥分发系统，并在昼夜周期中保持稳定。

与 SECOQC 节点模块集成后，自由空间链路得以无缝接入更广泛的光纤量子密钥分发基础设施。该系统通过向 SECOQC 可信中继架构提供安全密钥材料，证明自由空间链路能够作为有效的最后一公里接入信道，尤其适用于光纤部署不切实际或成本过高的场景。该装置支持全天候、全自动连续运行，保持较低的量子比特误码率（QBER），并展现出对环境波动的强大抵御能力。SECOQC 自由空间量子密钥分发实现证实，基于偏振的 BB84 量子密钥分发能够在现实环境下，通过短距离视距城市链路可靠运行。其较高的密钥率、稳定的性能以及与现有网络的顺畅集成，凸显了它作为灵活接入方案的实用性，适用于大都市范围内的量子安全通信，也彰显了异构量子密钥分发技术的互操作性。

5.5 面向移动接收端的自由空间量子密钥分发 r

Bourgoin等人（2015年）报告了首次成功演示：从固定发射机向移动接收端进行自由空间量子密钥分发，以模拟低地球轨道（LEO）卫星的角速度。该实验针对卫星量子密钥分发面临的关键工程挑战，包括实时光束跟踪、偏振漂移补偿和飞行时间校正。他们验证了在模拟卫星过境的动态条件下进行安全密钥交换的可行性。发送方（Alice）位于实验室，通过将一台810 nm脉冲激光器与一台1550 nm连续波激光器进行和频产生，生成532 nm弱相干脉冲。这些脉冲经过偏振和强度调制，以利用诱骗态实现BB84协议。光束经望远镜发射，并通过信标激光器和基于摄像机的跟踪系统进行稳定。为校正光纤诱导双折射造成的实时偏振漂移，发射机配备了偏振补偿模块，其中的电动波片由层析斩波器系统引导。接收方（Bob）安装在一辆以33 km/h行驶的皮卡上，与600 km低地球轨道卫星的表观角速度相匹配。Bob使用分束器、波片和单光子探测器对光子偏振进行被动分析。通过850 nm信标和实时反馈系统维持捕获与跟踪。图1展示了实验布局和卡车行驶路线，图2详述了Alice和Bob使用的光学元件。尽管接收端处于移动状态，量子链路仍以0.75°/s的角速度保持稳定，超过了典型的低地球轨道卫星速度。

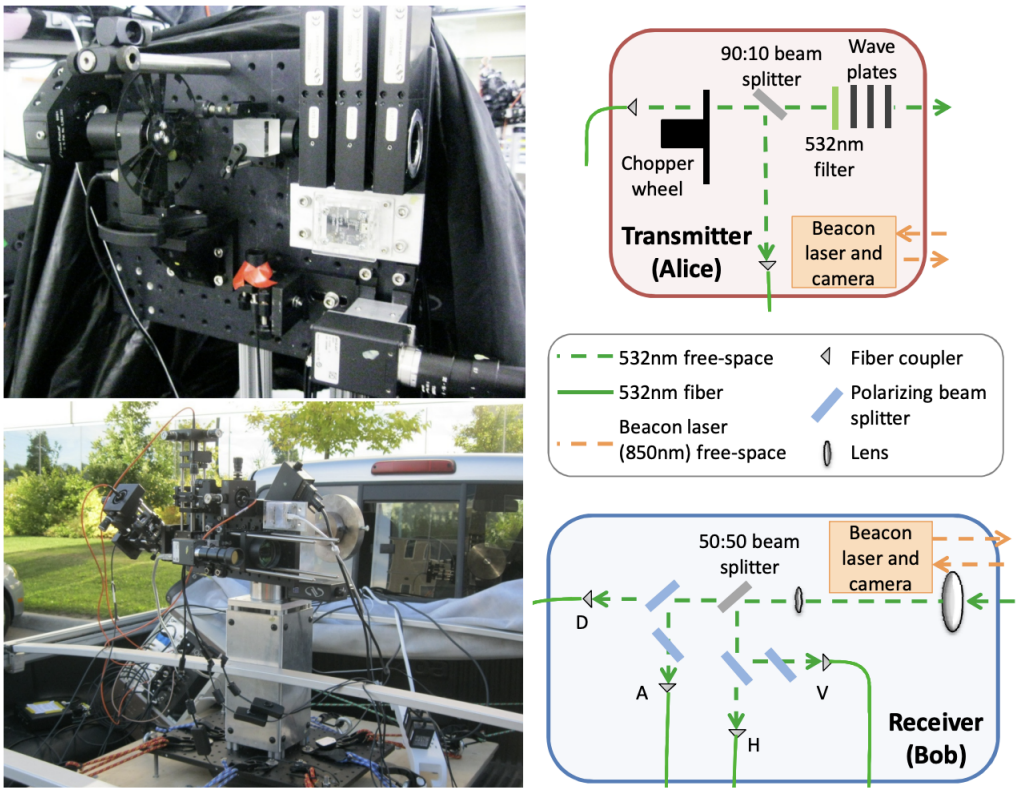

图 8：用于移动接收端自由空间量子密钥分发的发射机（Alice，顶部）和接收方（Bob，底部）装置。Alice 产生一束 ~10毫米准直光束，并利用内嵌偏振膜的斩波轮对 BB84 态进行编码。一个 10% 反射式分束器将部分光分流至光纤耦合偏振计，以实时进行偏振态层析。测量数据驱动一组电动波片，以补偿发射端光纤引起的偏振漂移。只有通过斩波轮开放槽的脉冲才用于密钥生成。Bob 安装在移动平台上，利用一个分束器和两个偏振分析器实施被动基选择测量。改编自 Bourgoin 等人 [82]。

系统总链路损耗为 30.6 dB，主要归因于光束发散和指向抖动，尤其是移动接收机处的影响。捕获后，Alice 处的角偏差降至 0.005°，Bob 处则降至 0.06°。系统利用基于 GPS 的模型校正飞行时间（TOF）变化，并在整个传输过程中持续监测量子比特误码率和光子计数率。在一个持续 4 秒的高信噪比窗口内，系统实现了约 11.5 kb 的原始密钥率，并在渐近假设下获得了 160 比特的安全密钥长度。主要误差来源是 6% 的量子比特误码率，主要由源保真度和偏振态纯度不理想造成。系统对这些误差进行了实时主动补偿；建模分析发现，剩余误差源于光束不对称性和调制器限制。

他们的工作证明了地面站与移动平台之间进行量子密钥分发在实践中的可行性，并为未来基于卫星的实现提供了重要见解。通过整合实时偏振控制、精密跟踪和精确的时间校正，该实验成功模拟了一次真实的卫星过境，并生成了安全密钥。尽管安全比特产出量有限，但结果证实，通过进一步改进（例如降低固有量子比特误码率、提高接收机稳定性），实用的卫星量子密钥分发已指日可待。本文提出的系统布局和补偿策略，为未来天地量子通信任务奠定了稳固基础。

5.6 日光条件下面向星间通信的长距离自由空间量子密钥分发

Liao等（2017）开展了一项使用1,550 nm光子的53 km自由空间量子密钥分发实验，证明了在高损耗和高背景条件下实现安全自由空间量子通信的可行性。这一高度可行性是通过采用电信波段光子、上转换探测和单模光纤空间滤波实现的。该研究以日光条件下星间量子通信的需求为动机，为基于卫星星座的全球量子网络奠定了关键基础。

该实验在中国青海湖上进行，发送方（Alice）与接收方（Bob）相距53 km。Alice采用了四台工作波长为1,550.14 nm的分布式反馈（DFB）激光器（见图11），并实施了带诱骗态的BB84协议。

信号光子经254 mm口径望远镜准直，实现了约 12 μrad的接近衍射极限发散角。在Bob端，一面420 mm抛物面镜收集入射光子，随后将其耦合进入单模光纤（SMF）。工作于室温的上转换单光子探测器（SPDs）将入射的电信波段光子转换为可见光波长，从而可用硅雪崩光电二极管（Si-APDs）进行探测。基于GPS的计时系统与高频光学跟踪系统共同确保了整个传输过程中的同步和光束稳定性。

尽管处于日光条件下，系统仍稳定运行，总信道损耗为 48 dB，其中光纤耦合造成 14 dB，几何扩散、大气吸收和探测器效率损失造成 34 dB。实验采用低密度奇偶校验（LDPC）码进行纠错，实现了每秒 20–400 比特的安全密钥率。在 1,756 秒的有效传输时段内，共生成 157,179 个安全比特。平均量子比特误码率（ QBER ）保持在 3.5% 以下。上转换单光子探测器显著提升了系统性能，其暗计数率较低（20 Hz），且能有效滤除背景光。该 53 km 链路的运行条件与低地球轨道（LEO）星间场景中预期的条件相当或更为严苛，

验证了日间运行对于卫星量子密钥分发的可行性。研究结果还凸显了自由空间量子密钥分发系统与光纤量子密钥分发系统之间的兼容性，为未来全球量子通信网络提供了可扩展的架构。探测器性能和光束指向精度的持续提升，预计将进一步提高系统可靠性并扩大运行范围。

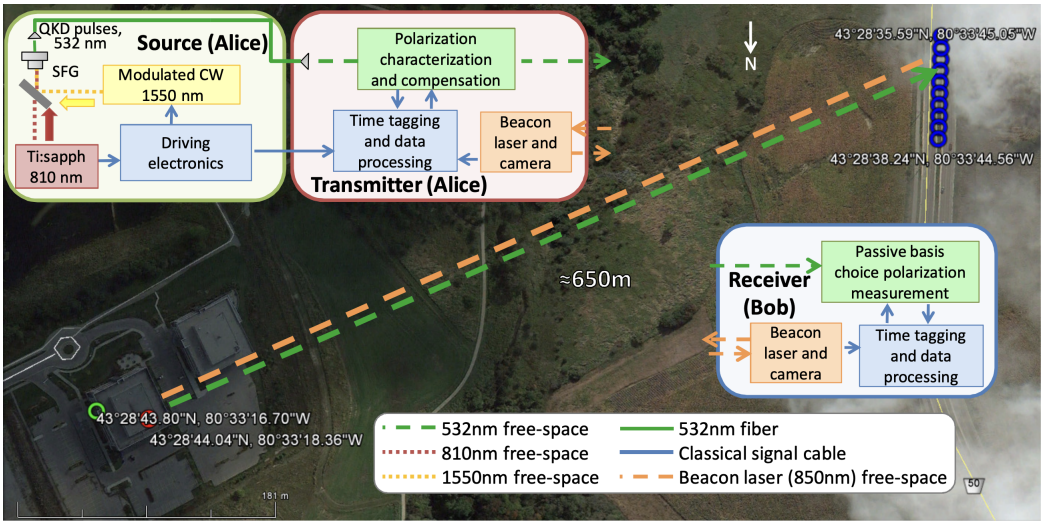

图 9：移动接收机自由空间量子密钥分发现场测试示意图及对应地图。Alice 包括一个位于建筑物底层实验室内的光源（绿色圆圈），以及一个通过光纤连接的屋顶发射机（红色圆圈）。安装在卡车上的 Bob 沿一段 80 m 长的道路行驶；蓝色圆圈标出测试期间卡车每秒一次的位置。卡车移动时，主动激光信标跟踪与指向系统会保持链路对准，无线局域网则提供认证经典信道。发射机与卡车之间的视线距离为 $\approx 650\text{m}$。地图数据：Google、DigitalGlobe。转载自 Bourgoin 等 [82]。

5.7 星地量子密钥分发

在此前工作的基础上，Liao等（2017）利用墨子号卫星实现了首次成功的星地量子密钥分发，在长达 1,200 km 的距离上完成了安全密钥交换。这项里程碑式的实验克服了地面量子密钥分发系统的根本限制，为构建全球规模的量子通信网络奠定了基础。

运行于500公里太阳同步轨道的墨子号卫星搭载了一台850纳米诱骗态BB84量子密钥分发发射机，其中包含八个用于编码偏振态的激光二极管。星载的300毫米口径望远镜实现了约 10 μrad的窄光束发散角。

地面接收操作在兴隆站进行，使用一台配备 BB84 解码光学系统和四个单光子探测器的 1 米望远镜。在轨道过境期间，卫星以 $\sim 7.6\text{km/s}$ 的速度运行，要保持精确对准，需要在卫星和地面终端上安装复杂的捕获、瞄准与跟踪（APT）系统。

卫星与地面站之间通过 532纳米脉冲信标激光器实现同步，定时抖动达到 ~ 0.5ns。为在卫星过境期间保持偏振保真度，电动半波片可根据轨道运动进行动态偏振补偿。

2016年12月19日，墨子号成功与地面站建立了量子密钥分发链路，距离范围为645 km至1,200 km。在273秒的传输期间，系统记录到167万个筛选密钥比特；在最近接近点附近，密钥率峰值达到12 kbit/s，在最远距离处则降至1 kbit/s。平均量子比特误码率（QBER）为1.1 %，与背景噪声和偏振可见度的预期影响相符。图3展示了单次卫星过境的关键性能指标，包括轨道距离、实时筛选密钥率和量子比特误码率（QBER）；这些指标会随角速度变化，尤其是在卫星经过头顶时，跟踪变得更具挑战性。经过纠错和隐私放大后，本次会话最终生成了300,939个安全比特。在23个夜间的测试中，系统始终实现了1–3%的量子比特误码率，峰值安全密钥率最高达40.2 kbit/s。这些结果在相近距离下，链路效率比基于光纤的量子密钥分发系统高出20个数量级以上，清楚地展示了卫星量子通信的独特优势。通过避开光纤和地面信道中不可避免的严重光子损耗，卫星方案实现了洲际尺度上的安全量子密钥交换。墨子号作为天基中继，为互联城域量子密钥分发网络提供了一种可扩展的架构。

5.8 一体化的4600千米星地量子通信网络

Chen等人（2021年）报告了首次成功实现大规模量子通信网络，该网络集成了卫星量子密钥分发系统和地面量子密钥分发系统。该网络覆盖4600千米，将700多条基于光纤的量子密钥分发链路与两条星地信道相结合，从而实现了跨越多个城市和偏远地区的实用安全量子密钥分发。这一成就标志着向全球量子互联网发展迈出了关键一步。该架构由四个城域光纤量子密钥分发网络（城域量子密钥分发网络）、一条长达2000千米的国家级光纤骨干网以及两条高速星地链路组成。地面光纤量子密钥分发链路采用带诱骗态的BB84协议，并分别使用工作频率为40 MHz和625 MHz的商用InGaAs/InP探测器和上转换单光子探测器。

在卫星量子密钥分发方面，墨子号卫星以200 MHz的重复频率发射经BB84编码的850纳米光子。对地面站光学系统和光谱滤波器进行升级后，光子耦合得到增强，背景噪声受到抑制，从而改善了链路性能。星地信道连接了相距2600千米的兴隆站和南山站，使混合网络能够实现端到端安全密钥交换。在一次持续364秒的卫星过境期间，该系统实现了最高462 kbps的筛选密钥率和平均47.8 kbps的最终安全密钥率，约为此前卫星量子密钥分发演示实验的40倍。

共收集到 58.1 Mbit 的筛选密钥材料，平均量子比特误码率仅为 0.5%。高性能跟踪和自适应曝光控制使系统能够在低仰角（5°）下可靠运行，将可行的链路距离扩展至 2,000 km 以上。图 3 展示了筛选密钥率和量子比特误码率随距离的变化（上）、扩大的卫星覆盖角示意图（中），以及最远达 2,043 km 的成功密钥生成（下）。

他们的结果与地球同步卫星链路预期的光学损耗相符，证实了远距离卫星量子密钥分发的可行性。通过成功连接地面光纤

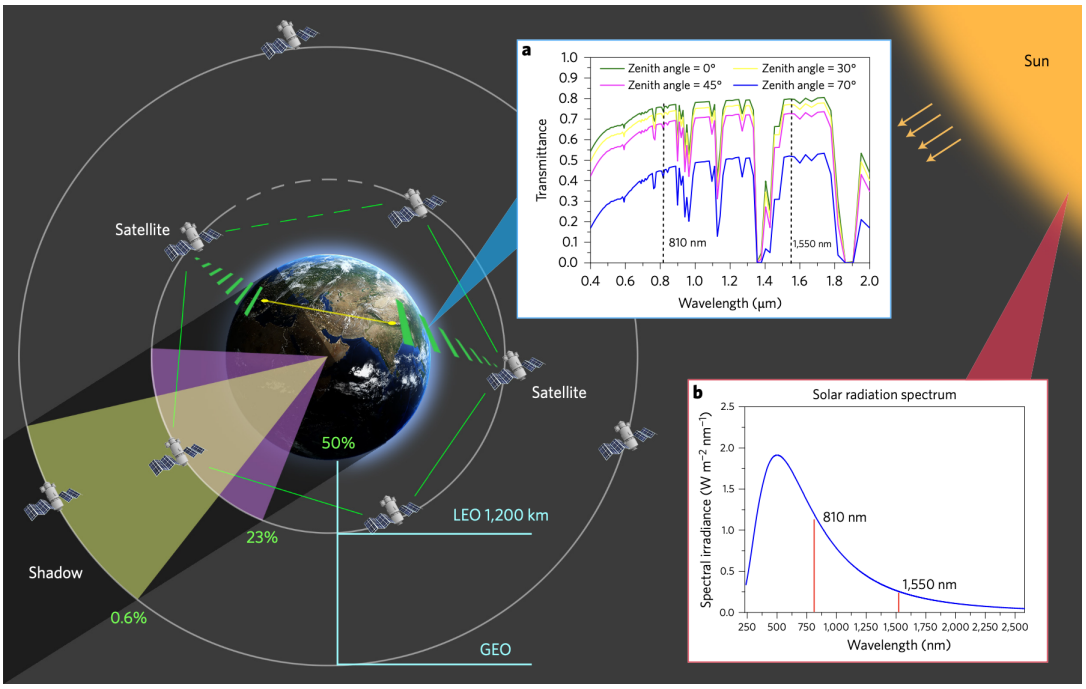

图 10：基于卫星星座的全球量子网络。全球量子网络需要由许多低地球轨道（LEO）卫星或若干地球同步（GEO）卫星组成卫星星座。卫星处于地球阴影（“夜间”）中的时间与其轨道高度成反比。(a) 特定天顶角下从可见光到近红外波段的大气透过率。(b) 从可见光到近红外波段的太阳光谱辐照度。改编自 S.-K. Liao等人 [83]。



图11：青海湖周边53千米日间自由空间量子密钥分发实验的鸟瞰图。Alice和Bob位于相对的湖岸。（a）1，550纳米激光二极管（LD）被编码为四种BB84偏振态（$|H\rangle$，$|V\rangle$，$|+\rangle$，$|-\rangle$），使用两个偏振分束器（PBS）和一个分束器（BS）实现。810纳米信标激光器和1，548纳米参考激光器经波分复用器（WDM）合束后，通过三片式准直器（TC）发射，用于光学对准和跟踪；光谱分析仪（OSA）用于校准信号光谱。（b）发送终端由安装在双轴旋转台上的望远镜和光学跟踪系统组成（电荷耦合器件（CCD）、快速转向镜（FSM）、干涉滤光片（IF））。（c）接收终端采用离轴抛物面镜，并与单模光纤（SMF）耦合。（d）接收到的光子经20米光纤传输至测量模块，该模块包含两个偏振分束器、一个分束器和四个探测器。（e）基于周期性极化铌酸锂（PPLN）的上转换单光子探测器模块采用窄带体布拉格光栅（VBG）来抑制背景。有关对准和跟踪的详细信息，请参见方法。地图数据：Google、CNES/Airbus、DigitalGlobe、Landsat/Copernicus。改编自S.-K. Liao 等人[83]。

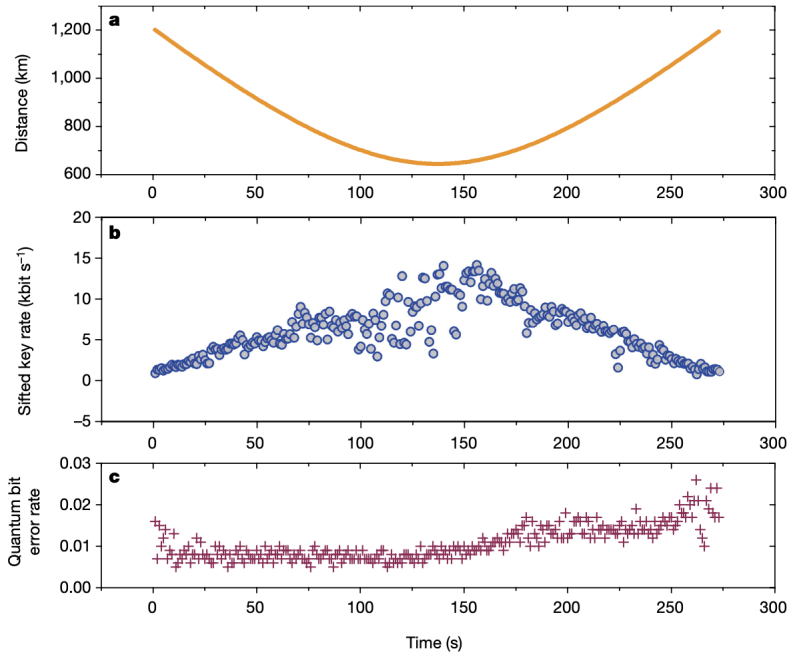

图 12：单次轨道运行期间星地量子密钥分发的性能。(a) 从兴隆地面站观测到的墨子号卫星轨迹。(b) 筛选密钥率随时间和斜距（卫星—地面站距离）的变化。(c) 观测到的量子比特误码率（QBER）。讨论见正文；其他日期的数据见扩展数据表2和扩展数据图1。改编自 S.-K. Liao 等人 [23]

该网络依托具备高吞吐量卫星信道的基础设施，在洲际尺度上实现了安全、高速率的量子密钥分发。针对可扩展性、硬件性能和远距离运行等关键挑战，该实验推动了全球量子互联网的实际落地。其所展示的能力也支持未来通过地球同步轨道实现卫星星座和洲际量子密钥分发的可行性

5.9 日光与夜间的自由空间量子密钥分发

Cai 等人（2024年）全面实验演示了在20公里地面链路上于日光和夜间持续运行的自由空间量子密钥分发。通过将高速稳定光源与接近理论极限的噪声抑制技术相结合，他们解决了此前将量子密钥分发限制在夜间并导致后处理延迟的关键挑战。这项工作为持续全天的卫星量子通信奠定了关键基础。

实验在位于丝绸之路度假村（海拔2266米）的卫星载荷原型（Alice）与南山地面站（海拔2070米）之间进行。该系统采用基于萨尼亚克干涉仪的调制方案实现偏振与强度控制，实施了625 MHz的BB84诱骗态协议。1550 nm的量子光子经法布里–珀罗腔（半高全宽28 pm）滤波，时间门控至800 ps，并通过单模光纤耦合进行空间滤波。光谱、空间与时间滤波相结合，将背景噪声降至最低。借助集成的双向激光通信实现了实时密钥提取，并使用低密度奇偶校验码编码完成同步与纠错。发射光束的发散角为 $\sim$20 μrad，所形成的光斑与1.2米接收望远镜相匹配。图1展示了完整的系统配置，包括发射机与接收端光学系统、跟踪系统、滤波组件以及实时处理模块。

2020年5月31日至6月13日期间，该系统在各种严峻条件下保持了持续的量子密钥分发运行。尽管天气时有变化，该系统仍生成了超过42.7 Mbits的安全密钥，平均最终密钥率为495 bps。每小时链路效率介于–43.3至–34.7 dB之间，量子比特误码率（QBER）始终保持较低水平（0.87%–2.16%），即使在直射阳光下也是如此。这些结果归功于有效的噪声抑制和精确的滤光，这使暗计数保持在250 cps以下。光束质量评估显示，远场发散角为 $\sim$60 μrad，并使用 R_0 相干长度对大气湍流进行了表征。其性能与星地量子密钥分发系统的性能非常接近，证实了在现实自由空间条件下进行实时密钥生成的可行性。图2总结了24小时内的性能指标，展示了链路效率、大气相干长度、量子比特误码率和最终安全密钥率的每小时变化趋势。

高速调制、稳健滤波与实时经典通信的结合，解决了与日间运行和密钥处理延迟相关的长期限制。实验条件与未来低地球轨道（低地球轨道）卫星场景中预期的条件高度吻合，证实了系统的可行性。展望未来，自适应光学、更精细的时间滤波以及在可见光波长下运行等改进，有望进一步提升系统的稳健性与可扩展性，为通过高轨卫星星座实现全球量子通信铺平道路。

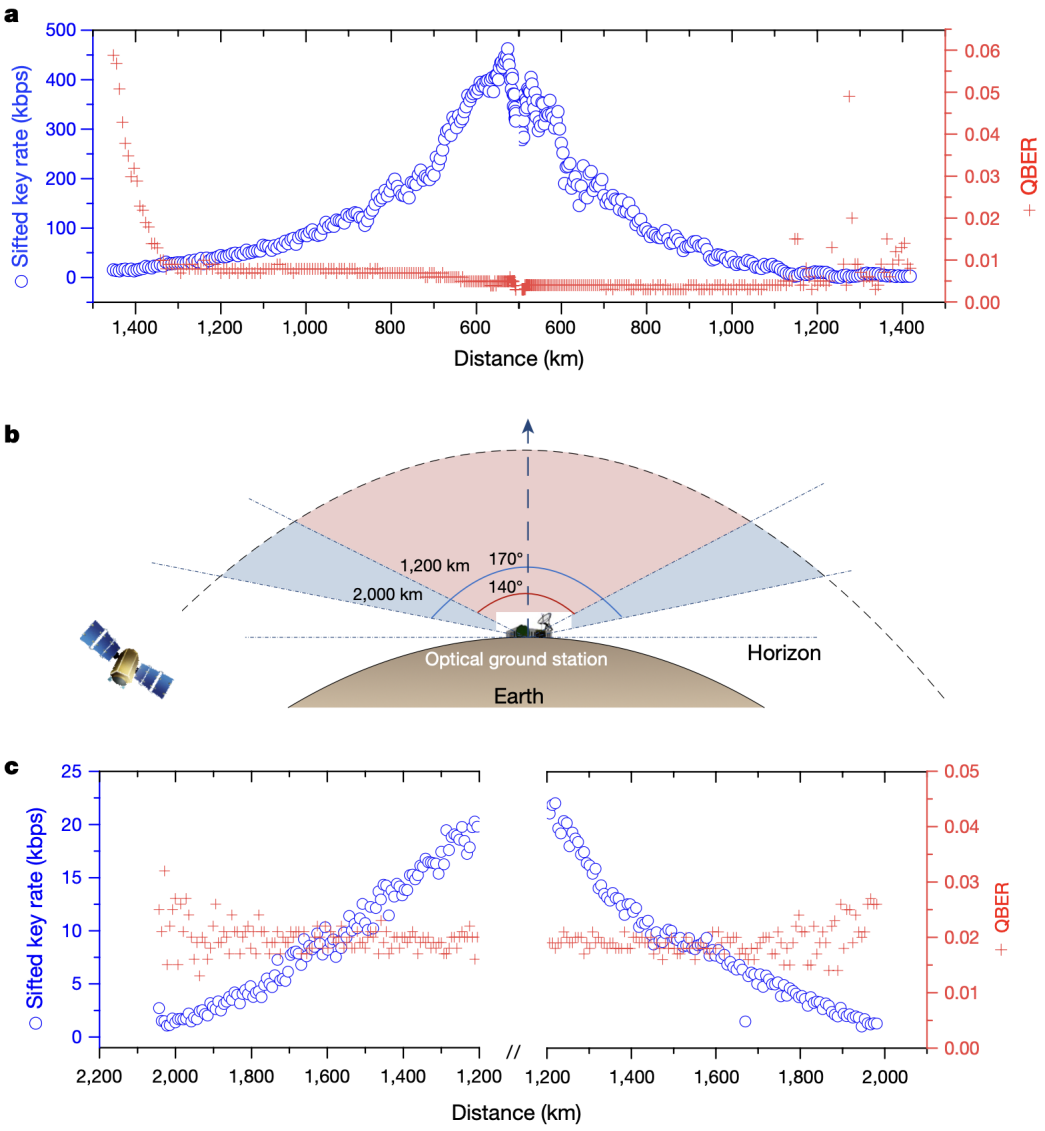

图13：高速星地量子密钥分发的性能。(a) 筛选密钥率（蓝色圆圈；左轴）和观测到的量子比特误码率（QBER；红色加号；右轴）随卫星至南山地面站斜距的变化。(b) 高速星地量子密钥分发覆盖角示意图：覆盖角（通信距离）从约 140°（∼1,200 km；红色）扩展至约 170°（∼2,000 km；蓝色）。(c) 远距离星地量子密钥分发测试，显示距离超过1,200 km[84]时的筛选密钥率（蓝色圆圈；左轴）和观测到的QBER（红色加号；右轴）

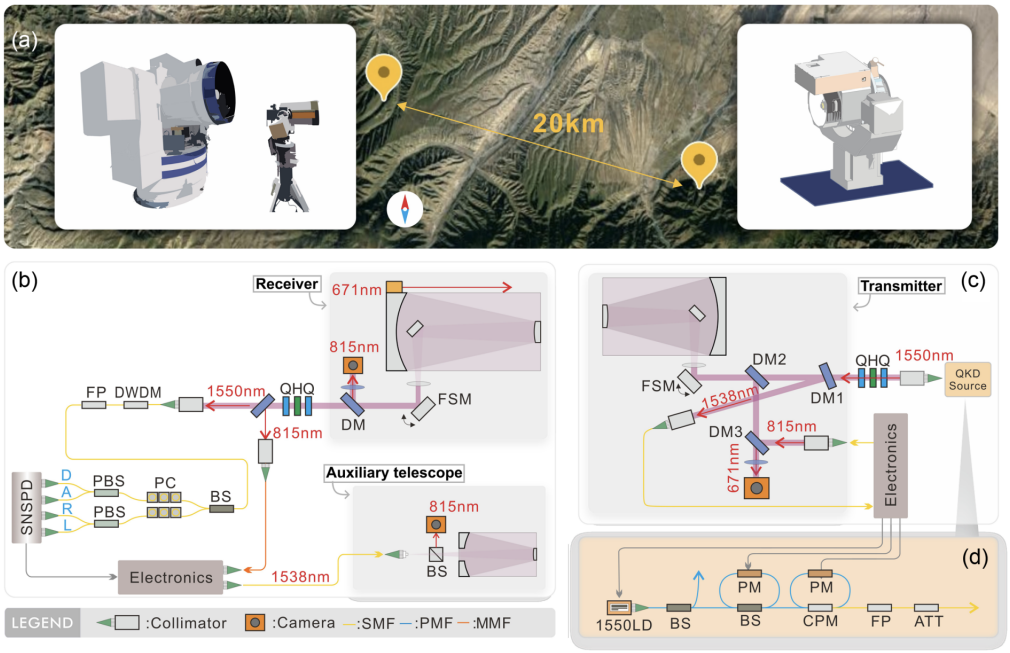

图14：在20公里地面链路上全天实时进行自由空间量子密钥分发。(a) 全天连续运行的20公里信道现场布局。(b) QKD接收机。(c) QKD发射机。(d) 高速稳健型量子密钥分发光源。发射机和接收机首先通过捕获-瞄准-跟踪（APT）系统（见补充材料1），使用815 nm下行信标和671 nm上行信标，捕获并维持地面光链路。高速稳健型光源制备1550 nm量子信号，由发送方发射，并由接收方收集和探测。实时密钥蒸馏使用815 nm下行通信激光和1538 nm上行通信激光。在发射机中，DM1反射1538 nm并透射1550 nm；DM2反射650–850 nm并透射1538–1550 nm；DM3反射671 nm并透射815 nm。在接收机中，辅助望远镜（面板b，右下方）用于发射1538 nm。缩写：LD，激光二极管；BS，（光纤）分束器；PM，相位调制器；CPM，定制偏振模块；FP，法布里-珀罗滤波器；ATT，衰减器；SMF，单模光纤；PMF，保偏光纤；MMF，多模光纤；M，反射镜；CAM，相机；FSM，快速转向镜；DM，二向色镜；Q，四分之一波片；H，半波片；DWDM，100 GHz密集波分复用器（粗滤波）；PC，光纤偏振补偿器；PBS，光纤偏振分束器；SNSPD，超导纳米线单光子探测器。改编自W.-Q. Cai等[85]。

5.10 基于微卫星的实时量子密钥分发 on

Li 等人（2025年）利用轻型微卫星和便携式光学地面站（光学地面站）实现了首次实时星地量子密钥分发。这项工作标志着向可扩展量子卫星星座迈出了重要一步，通过具有成本效益且可快速部署的基础设施实现安全的全球通信。在一次卫星过境期间，他们获得了高达107万安全比特，并演示了中国与南非之间的加密洲际通信。

微卫星济南一号被发射至500千米的太阳同步轨道，搭载了22.7千克的量子密钥分发载荷和一台200毫米口径望远镜。其量子光源由单个850纳米激光二极管组成，并通过基于萨尼亚克干涉仪的方案进行调制，以实现625 MHz的BB84协议和诱骗态，从而支持高重复频率并抵御侧信道攻击。星上和地面站均采用电动波片进行偏振补偿。

图1概述了系统布局。在城市和偏远地区均部署了紧凑型光学地面站（每台100 kg）。这些地面站配备了280 mm卡塞格林望远镜、偏振分析模块、窄带通滤光片和低噪声硅雪崩光电二极管探测器（暗计数¡800 cps）。两级捕获、瞄准与跟踪（APT）系统实现了微弧度级精度。图3展示了卫星和光学地面站的设计。实时双向激光通信确保了精确的时间同步（100 ps）和数据交换（104 Mbps），从而能够在每次卫星过境期间立即进行密钥蒸馏。

该系统成功在20个轨道周期内执行实时量子密钥分发，连接了中国和南非的地面站。2022年9月25日，卫星飞越济南期间，安全密钥交换持续了约6分钟。卫星实现稳定的捕获、瞄准与跟踪且仰角超过10–15°后，量子密钥分发便开始进行。斜距从2,000 km变化至500 km。图4展示了密钥性能指标：随着距离缩短，光子探测率上升（4b）；量子比特误码率保持在0.76%至1.79%之间（4c），实时蒸馏得到406,784个安全比特（4a）。所有站点的性能均保持一致，平均量子比特误码率低于2.5%。最佳结果是在南非斯泰伦博斯单次过境期间获得的107万个安全比特。表1总结了各站点的系统性能，证实系统在不同光照和地理条件下均能有效运行。精确的偏振补偿以及对环境光的抵御能力，进一步验证了系统的稳健性。低密度奇偶校验（LDPC）码的使用以极低的开销实现了高效纠错。包含光子探测、同步、基矢协调、纠错和隐私放大等步骤的六步实时蒸馏协议，使最终安全密钥能够在每次过境期间即时提取。此外，还在中国和南非之间（相距12,900 km）进行了洲际量子密钥分发展示，以卫星充当“太空邮差”传递安全密钥。生成的密钥用于对图像文件进行一次一密加密，实现了实用的近实时安全通信，总延迟为1.5小时。

这项工作展示了一种利用微卫星和便携式地面站实现天基量子密钥分发的可扩展、高效架构。与早期工作（如墨子号）相比，该设计将有效载荷和地面系统的质量减少了一个数量级以上，可实现快速部署、降低成本并保持高性能。集成实时经典通信与快速密钥蒸馏，消除了早期卫星量子密钥分发实验中的相关延迟。该系统始终实现了较高的密钥率（每次过境最高可达 1.07 Mbits）、较低的量子比特误码率（¡2.5%）和亚微弧度跟踪精度——即使在真实环境条

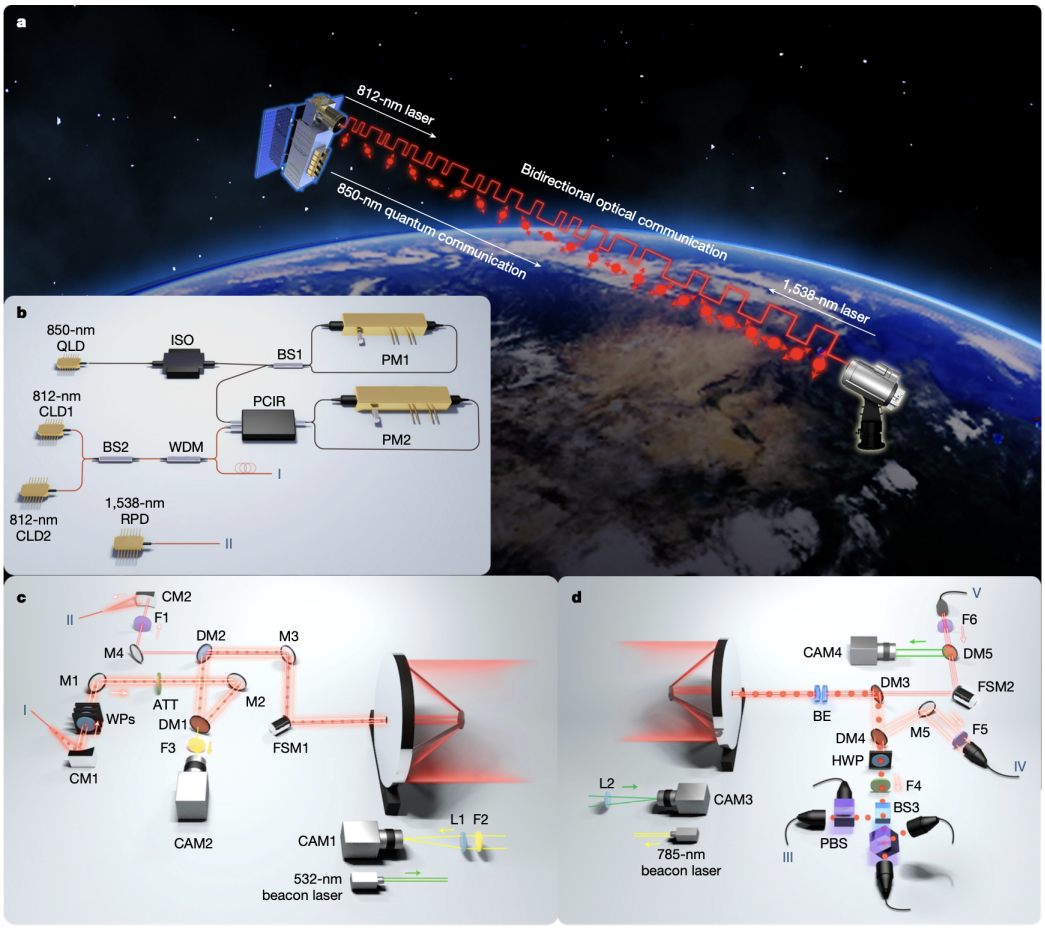

图 15：星地量子密钥分发实验装置。（a）星地实验概览。除下行链路的 850纳米量子光子外，卫星和光学地面站（OGS）还提供双向光通信——812纳米下行激光和 1，538 纳米上行激光——以实现实时密钥蒸馏和安全通信。地图数据：Google Earth、Data SIO、NOAA、美国海军、美国国家地理空间情报局、全球海底地形图、Landsat/Copernicus、国际北冰洋水深图。（b）基于单激光二极管和外调制的量子密钥分发光源。缩写：QLD，量子激光二极管；CLD，通信激光二极管；ISO，隔离器；BS，分束器；PM，相位调制器；PCIR，偏振模块；RPD，接收雪崩光电二极管；WDM，波分复用器。（c）卫星光学设计。标记 I 表示承载 812纳米通信光束和 850纳米量子信号的输出单模光纤（SMF）；标记 II 表示接收 1，538 纳米上行链路的多模光纤（MMF）。CAM1 为捕获相机；CAM2 为精跟踪相机。其他光学元件：CM，凹面镜；WP，波片；M，反射镜；ATT，衰减器；DM，二向色镜；F，滤光片；L，透镜；FSM，快速转向镜。（d）便携式光学地面站。标记 III、IV 和 V 分别表示接收 850纳米量子光子和 812纳米下行链路的多模光纤，以及传输 1，538 纳米上行链路的单模光纤。BE，扩束器；PBS，偏振分束器。改编自 Y. Li 等 [86]。

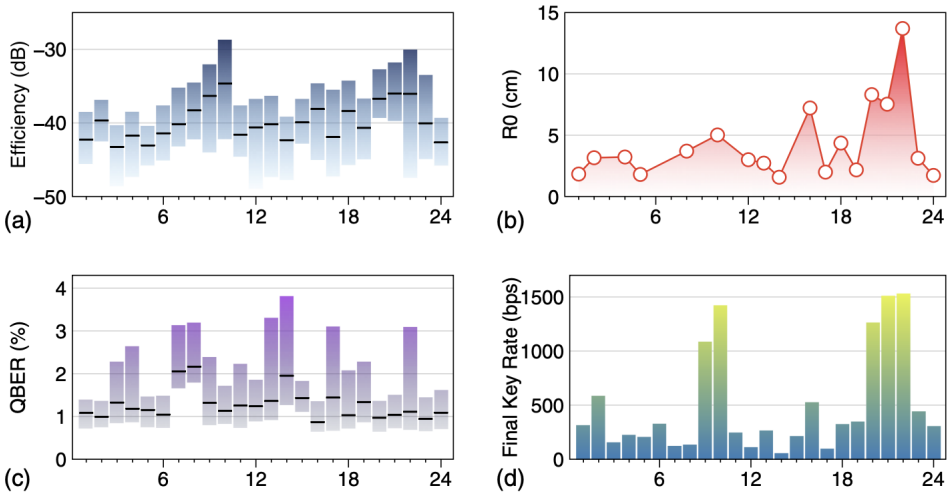

图16：自由空间量子密钥分发的实验结果。(a) 链路效率。(b) R_0。(c) 量子比特误码率（QBER）。(d) 最终密钥率。数据采集于5月31日至6月13日期间的不同日期。 R_0 测试在量子密钥分发运行前的几分钟内未进行精跟踪，而效率、QBER 和最终密钥率数据点则为约1小时运行结果的平均值。改编自 W.-Q. Cai 等 [85]。

大气条件。其灵活性和便携性为可扩展卫星星座奠定了基础。展望未来，改进方向可能包括芯片级光源、日间运行，以及在多种轨道上部署以扩大覆盖范围。这些进展有望推动全球量子互联网的发展，实现超安全通信、远距离量子纠缠分发，并为全球用户提供安全接入。

6 自由空间量子密钥分发中的大气湍流及其校正 6.1 物理起源与度量指标

大气湍流源于温度、压力和湿度的随机涨落，这些涨落会沿光路产生随机的折射率非均匀性。经典结构函数参数 $C_n^2(z)$ 和无量纲的 *Rytov*方差 σ_{Ry}^2 仍是量化湍流强度的主要工具。对于平面波，方差定义为 $\sigma_{\mathrm{Ry}}^2 = 1.23\, C_n^2 k^{7/6} z^{11/6}$，其中 $k = 2\pi/\lambda$，路径长度为 z [87]。需要注意的是，对于球面波（用于近似卫星下行链路），由于光束发散 [87]，Rytov方差按平面波值的 $0.4\times$ 缩放。

弱、中、强湍流区通常分别以 $\sigma_{\mathrm{Ry}}^2 \lesssim 0.3$、$\sim 1$ 和 $\gtrsim 1$ 为界。卫星下行链路经常进入后两种状态，尤其是在地平线附近，折射会使湍流层变长 [88]。关键在于，尽管用于描述强度涨落的Rytov近似在强聚焦区会失效，但近期的波动光学仿真已证实，弗里德参数的经典解析公式（R_0）在强散射区内仍然准确（最高可达 $\sigma_{\mathrm{Ry}}^2 \approx 26.7$）[89]。这证明，仍可将 R_0 用作卫星链路的基本设计参数，无需针对强散射进行复杂修正。

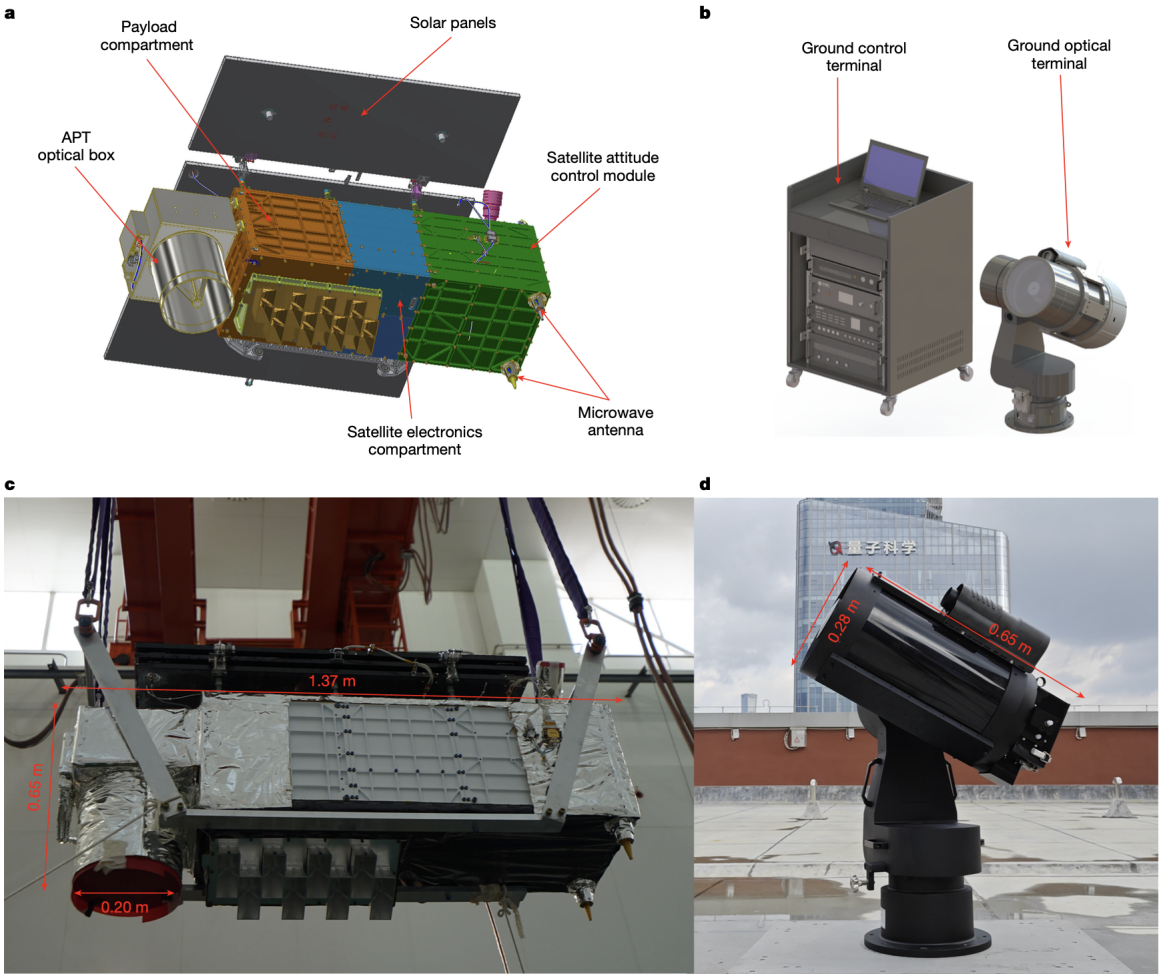

图 17：微卫星与便携式光学地面站（OGS）。(a) 微卫星由捕获-瞄准-跟踪（APT）光学箱、有效载荷舱、卫星电子设备舱、姿态控制模块、微波天线和太阳能电池板组成。(b) 光学地面站由控制终端和光学终端组成。(c) 火箭集成前的微卫星照片；其发射状态包络约为 1.37 m $\times 0.49\,\mathrm{m} \times 0.65\mathrm{m}$，望远镜口径为 0.2 m。(d) 部署在济南市区的便携式光学地面站照片；其主望远镜包络约为 $0.65\mathrm{m} \times 0.28\mathrm{m} \times 0.28\mathrm{m}$。改编自 Y. Li 等 [86]

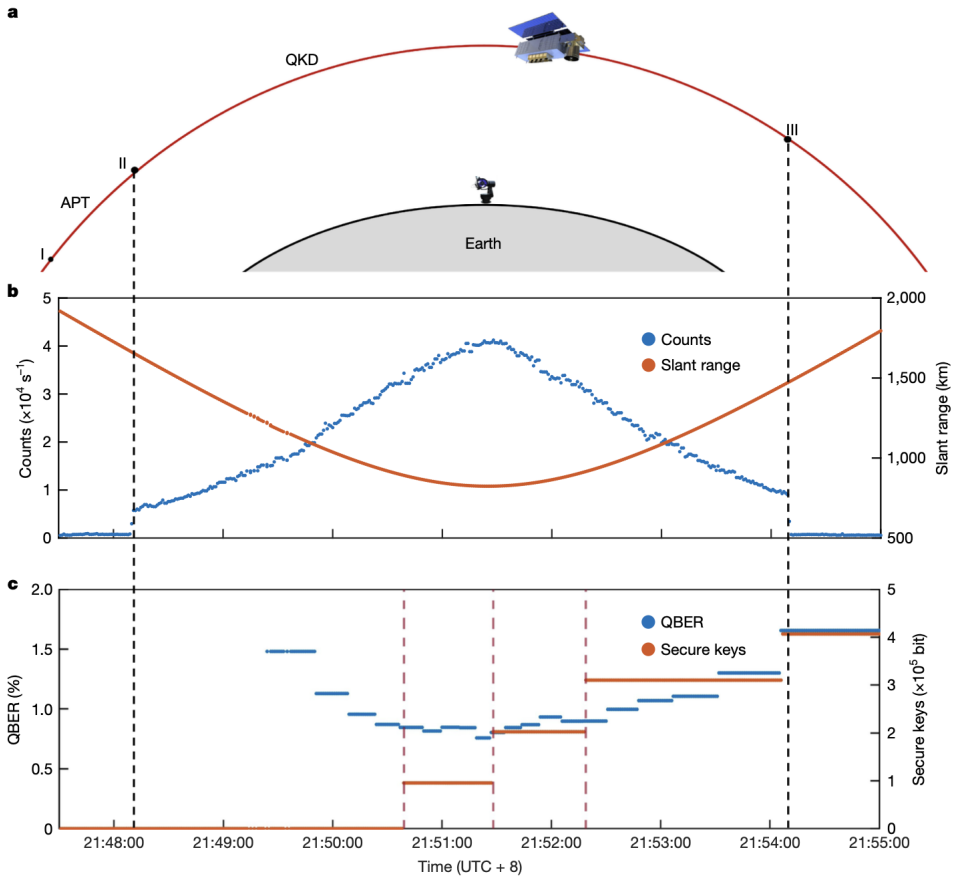

图18：星地量子密钥分发实验装置。（a）星地实验概览。除850纳米下行链路量子光子外，卫星和光学地面站（OGS）还支持双向光通信——采用812纳米下行激光和1，538纳米上行激光，实现实时密钥蒸馏和安全通信。地图数据：Google Earth、Data SIO、NOAA、美国海军、美国国家地理空间情报局、全球海底地形图、Landsat/Copernicus、国际北冰洋水深图。（b）基于单激光二极管和外部调制的量子密钥分发光源。缩写：QLD，量子激光二极管；CLD，通信激光二极管；ISO，隔离器；BS，分束器；PM，相位调制器；PCIR，偏振模块；RPD，接收雪崩光电二极管；WDM，波分复用器。（c）卫星光学设计。标记I和II分别表示承载812纳米通信光束和850纳米量子信号的输出单模光纤（SMF），以及接收1，538纳米上行链路的多模光纤（MMF）。CAM1为捕获相机；CAM2为精跟踪相机。其他光学元件：CM，凹面镜；WP，波片；M，反射镜；ATT，衰减器；DM，二向色镜；F，滤光片；L，透镜；FSM，快速转向镜。（d）便携式光学地面站。标记III、IV和V分别表示用于接收850纳米量子光子的多模光纤、用于接收812纳米下行激光的多模光纤，以及用于发射1，538纳米上行链路的单模光纤。BE，扩束器；PBS，偏振分束器。改编自 Y. Li等 [86]。

折射率结构参数 C_n^2 定义为 [90]:

$$C_n^2 = \frac{\langle [n(\vec{x}) - n(\vec{x}+\vec{r})]^2 \rangle}{r^{2/3}}, \tag{18}$$

其中， n 为折射率， $\vec{x}$ 表示沿传播路径的位置， $\vec{r}$ 为间隔矢量。参数 C_n^2 通常从弱湍流条件下的 10^{-17} $\mathrm{m}^{-2/3}$ 变化到强湍流条件下的 10^{-13} $\mathrm{m}^{-2/3}$ 。

6.2 湍流统计与信道建模

湍流中的量子信道会发生衰落：瞬时透射率 η 服从概率密度 $P(\eta)$。对于弱湍流（$\sigma_{\mathrm{Ry}}^2 \lesssim 1$），对数正态模型已足够[91]:

$$\mathcal{P}(\eta_{\mathrm{atm}}) = \frac{1}{\sqrt{2\pi}\sigma\eta_{\mathrm{atm}}} \exp\left[-\frac{1}{2}\left(\frac{\ln \eta_{\mathrm{atm}} + \overline{\theta}}{\sigma}\right)^2\right]. \tag{19}$$

除此之外，混合对数正态分布或椭圆光束分布更为优越，同时仍可用于安全性证明，且在解析上易于处理 [87]。这些模型预测，一旦 $\sigma_{\mathrm{Ry}}^2 \gtrsim 1$ [87]，光束扩展（短期展宽）而非光束漂移将成为密钥率劣化的主要原因。

湍流对光束的影响可通过相位屏建模，其中像差由泽尼克多项式描述:

$$\xi(\rho,\phi) = \sum_{n,m} c_{n,m} Z_{n,m}(\rho,\phi), \tag{20}$$

其中$Z_{n,m}$ 为泽尼克模态，$c_{n,m}$ 为表示各像差瞬时振幅的随机系数。这些系数的统计方差定义为$\sigma_{n,m}^2 = \langle |c_{n,m}|^2 \rangle$，并通过弗里德参数 R_0随湍流强度而变化。根据标准湍流理论 [92]:

$$\sigma_{n,m}^2 = \gamma_{n,m}\left(\frac{D}{R_0}\right)^{5/3}, \quad \text{with} \quad R_0 \approx 1.68(C_n^2 L k^2)^{-3/5}. \tag{21}$$

弗里德参数的这一表达式采用了平面波近似。

6.3 对量子密钥分发性能的影响

波动损耗与静态损耗近似。 利用真实的诱骗态 BB84 仿真器， **（作者？）** 表明，对数正态衰落造成的安全密钥惩罚在湍流变得 极其 强烈之前可忽略不计，从而验证了大多数城域链路常用的静态损耗近似 [91]。然而，同一研究也揭示了改进机会：丢弃信噪比较差的数据块（信噪比筛选）可将最终秘密密钥提高 $\sim$ 25%，方法是在深度衰落期间剔除高量子比特误码率帧 [91]。

空间模态敏感性。 模态结构至关重要。一项受控的实验室对比表明，在白天视宁度条件下，传播距离超过 1–2 km 时，平面波（PW）编码比轨道角动量（OAM）模式更能耐受闪烁；在相同湍流条件下，PW 模式的串扰低三倍 [93]。这一优势源于

OAM 的定义取决于光轴；沿传播轴的倾斜像差会导致 OAM 中的模式混合，而一维 PW 模式不受正交方向波前倾斜的影响 [93]。

在量子通信中，湍流引起的畸变会在高维编码方案中引入误差。对于 d维双互无偏基协议（2-MUB protocol，BB84 的推广）中使用的轨道角动量模式，湍流条件下的渐近安全密钥率 $R(d, e_q)$ 由公式 12 定义。当误码率超过特定阈值（例如，$\approx 11\%$（$d = 2$），且阈值会随更高的 d而升高）时，安全性便会受到损害（$R < 0$）；对于公里级轨道角动量链路，当湍流强度超过 $C_n^2 \gtrsim 10^{-15}\ \mathrm{m}^{-2/3}$时，通常会出现这种性能失效。经典类比系统也对密切相关的波传播现象进行了研究。具体而言，研究表明，表面重力水波可提供一个可控平台，用于研究色散、波包展宽、干涉以及有效势景观；这些现象所处的条件在数学上类似于傍轴光传播。此类流体动力学类比系统有助于直观理解复杂介质中的波演化、退相干和模式耦合，并可补充用于自由空间量子信道的数值相位屏模型和波动光学模型 [94, 95, 96, 97]。

6.4 被动缓解策略

孔径平均与接收分集。 对于长期光束腰$w_{\mathrm{lt}} \gg a_R$ （接收方半径）的高斯光束，通过对多个子孔径进行平均可抑制闪烁。采用光学合束的三支路相干探测接收机，在无需主动光学的情况下使 Q因子提升了4–6 dB，为卫星地面站提供了切实可行的方案 [98]。

相干噪声抑制。 在连续变量（CV）量子密钥分发（QKD）中，本振（LO）可充当强大的空间和光谱滤波器。通过使信号与本振发生干涉，只有与本振模式匹配的模式才会被探测到。这实际上将光谱滤波带宽缩窄至脉冲带宽（例如，$\Delta\lambda \approx 0.1$ pm），与直接探测滤波器（~ 1 nm）相比，可将背景噪声降低数个数量级。这一机制使日间运行即使在太阳背景光很强的情况下也成为可能 [99]。

6.5 高级接收机架构

为进一步缓解离散变量（DV）系统中的衰落和热噪声，人们提出了条件动力学肯尼迪（CD-Kennedy）接收机 [98]。与静态接收机不同，CD-Kennedy接收机利用导频比特估计瞬时湍流衰落 η_{eq}。它会动态调节本振振幅，使其与“0”比特状态的信号发生相消干涉，从而有效抵消信号并减少错误。这种自适应方法使接收机在弱湍流或低热噪声条件下能够超越标准量子极限（SQL）；而在这些条件下，静态肯尼迪接收机和II型接收机通常无法做到这一点 [98]。

光子集成电路（PICs）为这些先进架构的小型化提供了途径，同时增强了其抵御振动和热漂移的能力，而这些问题一直困扰着体光学。近期的演示采用了包含可调谐马赫-曾德尔干涉仪（MZIs）网格的硅光子芯片，将其用作相干合束器 [101]。虽然这些器件主要通过经典信号进行表征，以验证模式混合效率，但其线性特性使其可直接应用于量子信号；在这类应用中，最大限度地提高耦合到单模光纤中的效率是关键挑战。在这些器件中，二维光学天线阵列

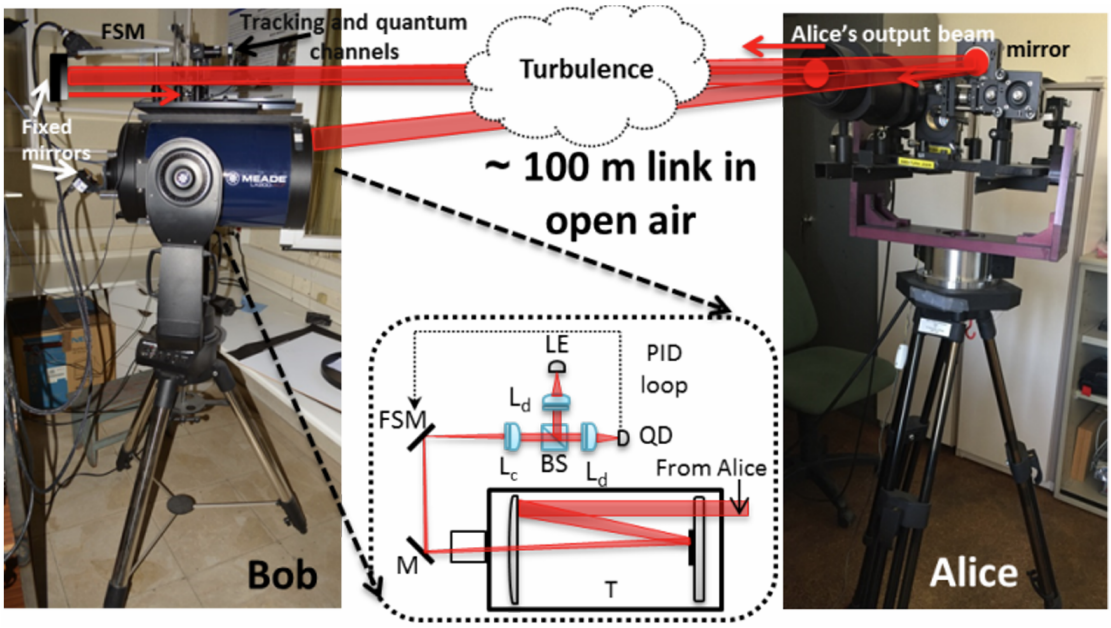

图19：100 m处闭环校正系统的接收方与发送方照片。T为施密特-卡塞格林式直径25 cm的望远镜，M为固定反射镜；FSM为快速转向镜；Lc和Ld为消色差双合透镜；BS为50/50分束器；LE和QD分别为横向和四象限位置灵敏探测器；PID为比例-积分-微分回路 [100]。

将畸变的自由空间光束耦合进波导，由局部反馈回路控制的 MZI网格对信号进行相干求和。这实际上复现了大孔径平均接收机的功能，但具有显著更高的空间分辨率和混合效率 [101]。

对于闪烁严重的卫星下行链路，已开发出可扩展的光子集成电路架构，例如 32 路输入相干合束器 [102]。这些合束器可以与多平面光转换（MPLC）器件配合使用，在芯片上进行相干合束之前，将畸变波前空间解复用为正交模式（例如厄米-高斯模式）[103]。这种“空间解复用”方法能够回收原本会因单模光纤耦合中的模式耦合误差而损失的功率 [104]。作为光子集成电路的补充，介电超表面也正成为用于自由空间到光纤耦合的超紧凑接口；与传统自适应光学反射镜相比，它们能够以可忽略不计的占用空间实现动态波前整形 [105]。

6.6 主动波前校正

倾斜补偿是第一阶段校正。Fernandez等人展示了利用象限探测器（QDs）和快速转向镜（FSMs）校正城域量子密钥分发链路中由光束漂移引起的波前倾斜 [100]。在量子接收机中，象限探测器优于横向效应（LE）探测器，因为其在焦平面处的响应最大且与信噪比（SNR）无关，而横向效应探测器难以应对量子信号通常具有的低信噪比 [100]。

由象限探测器控制的闭环快速转向镜，在一条 100 米试验场上将焦平面漂移降低了 9 倍（图 19），相当于实现了 $\approx 10\times$ 日光量子密钥分发的太阳背景抑制 [100]。缩放规则表明，当发射机/接收机直径（$D_T,\ D_R$） $=(4,\ 8)$ 厘米时，仅接收端校正足以应对最长 $\sim$ 1–2.5 千米的距离，具体取决于 C_n^2；超过这一距离后，发射机端预补偿便至关重要 [100]。

6.7 用于信道估计与校正的机器学习 $\mathbf{n}$

最新进展表明，机器学习（ML）和深度学习（DL）在湍流抑制方面可以显著优于经典控制回路，尤其是在预测时间波动和校正严重相位畸变方面。传统的自适应光学依赖波前传感器（如 Shack-Hartmann），而这类传感器在强闪烁条件下表现不佳。研究已证明，深度学习方法，尤其是卷积神经网络（CNN），能够直接根据强度图像预测湍流相位屏，从而免去复杂的波前重建过程 [106]。

除了波前校正，机器学习也越来越多地用于实时信道估计。在连续变量（CV）量子密钥分发中，神经网络已被用于利用导频音预测信道透射率和过量噪声 [107]。与静态统计模型相比，这种“机器学习辅助”方法能够更准确地设定后选择阈值，并通过适应瞬时大气条件有效提高安全密钥率 [107]。此外，基于时间序列分析的预测模型可以提前数毫秒预测信道透射率，从而有望降低自适应速率协议中的时延惩罚 [108]。

6.8 强湍流下的安全性

中强湍流要求有限密钥分析纳入完整的 $P(\eta)$ 及过量噪声项。Ghalaii 和 Pirandola（2022）推导了中强湍流下量子通信的极限，并修订了 PLOB界，将湍流引起的光束展宽纳入其中。总透射率被建模为四种不同损耗机制的乘积[87]:

$$\eta = \eta_{\mathrm{lt}}\eta_{\mathrm{eff}}\eta_{\mathrm{cd}}\eta_{\mathrm{atm}}, \tag{22}$$

其中:

- η_{lt} 表示长期湍流透射率，它考虑了超出衍射极限的折射率涨落所导致的光束展宽和破碎;
- η_{atm} 表示大气消光，根据比尔-朗伯定律建模，描述气溶胶和分子吸收及散射造成的损耗;
- η_{eff} 表示静态接收方效率，概括望远镜配置中的光学损耗以及探测器有限的量子效率;
- η_{cd} 表示相干探测效率，具体指模式匹配损耗，这与本地本地振荡器（LLO）方案相关;在这类方案中，本地产生的参考脉冲与受畸变的信号光束在空间上无法完美重合。

对于 $\sigma_{Ry}^2 > 1$，与光束展宽相比，光束漂移可以忽略不计，因此可将安全性分析简化为对具有高损耗[87]的稳定信道进行分析。

一项可组合连续变量量子密钥分发证明表明，只要零差探测器的 $\eta_{\mathrm{det}} \gtrsim 60\%$ 和电子噪声 $v_{\mathrm{el}} \lesssim 0.01$ 散粒噪声单位满足条件，在 $\sigma_{\mathrm{Ry}}^2 \sim 10$ 仍可实现正密钥率 [87]。主要发现包括:

- 即使在强湍流条件下（夜间 $\sigma_{Ry}^2 \approx 38$ ），使用现实的接收方设备，在 10千米距离仍可实现正密钥率。
- 增大接收孔径（$a_R > 30$ 厘米）可以补偿较高的背景噪声，但代价是热光子数增加。
- 对于天顶角较大的卫星链路（例如，遮蔽角 $\theta_m = 80°$），即使在 500 千米轨道高度下，连续变量量子密钥分发仍然可行，块大小为 $\sim 10^{10}$–10^{12}。

6.9 开放问题与展望

未来研究仍面临若干尚待解决的挑战，尤其是自由空间量子通信从实验室演示迈向实际部署之际。在深强湍流区域 ($\sigma_{\mathrm{Ry}}^2 \gg 10$)，经验数据十分稀缺，需要开展系统的测量活动，以准确表征性能并验证椭圆光束分布等理论模型 [87]。除了这些基础表征需求之外，若干有前景的研究方向也已显现:

混合主被动缓解架构。 虽然自适应光学 (AO) [100]和信噪比 (SNR) 筛选 [91]等单项技术已展现出潜力，但对它们进行协同整合仍缺乏充分研究。将实时波前校正与智能帧选择相结合的统一架构，有望带来叠加的性能提升。例如，AO 可稳定光束质心以最大限度提高耦合效率，而信噪比筛选则可剔除因闪烁未得到校正而导致量子比特误码率升高的残余帧。

标准化湍流表征。 该领域缺乏针对量子信道的标准化指标。诸如 C_n^2 和 R_0 之类的经典参数无法全面刻画量子态退化。开发量子专用工具——例如直接测量纠缠退化程度——将有助于更准确地预测性能 [91]。

全集成光子接收机。 对于面临严格尺寸、重量和功耗（SWaP）约束的卫星载荷而言，从体光学向芯片级接收机转变是一个关键前沿。未来研究必须利用超表面和MPLC器件，解决强湍流条件下自由空间到芯片耦合的效率问题。此外，开发能够在单一平台上集成湍流传感与校正功能的“自适应”光子集成电路，有望消除对复杂外部自适应光学环路的需求 [101, 102]。

AI驱动的自主量子链路。 机器学习有望超越简单的参数估计，实现完整的链路自主。未来的“认知型”地面站可以利用深度强化学习预测湍流模式，并主动调整自适应光学设置，从而最大限度地减少时延误差。此外，端到端学习架构可以在实时条件下联合优化发射机调制和接收机后处理策略，并调整协议（例如在DV和CV之间切换），以匹配瞬时大气“天气”状况 [107]。

系统设计人员实用检查清单

1. 在本地表征 $C_n^2(z)$，并将其转换为 σ_{Ry}^2；针对卫星链路 [89]，区分平面波与球面波模型。2. 对于短链路（< 2 km），优先采用倾斜校正；对于闪烁占主导的较长链路，孔径平均通常效果更佳 [100, 98]。3. 在有限密钥分析中，将过量噪声和衰落方差纳入预算；仅当 $w_{\mathrm{lt}} \gg w_{\mathrm{st}}$（通常为 $\sigma_{\mathrm{Ry}}^2 > 1$）时才忽略光束漂移 [87]。4. 如果背景计数超过信号的 1–2%，则考虑进行信噪比筛选，以便从噪声数据中恢复密钥 [91]。5. 使用高能脉冲实现导频引导损耗跟踪，实时估算瞬时透射率 η，从而准确地对信号分箱以进行后选择 [99]。6. 对于低仰角的卫星链路，应特别考虑路径延长以及有效湍流强度的增加 [87]。

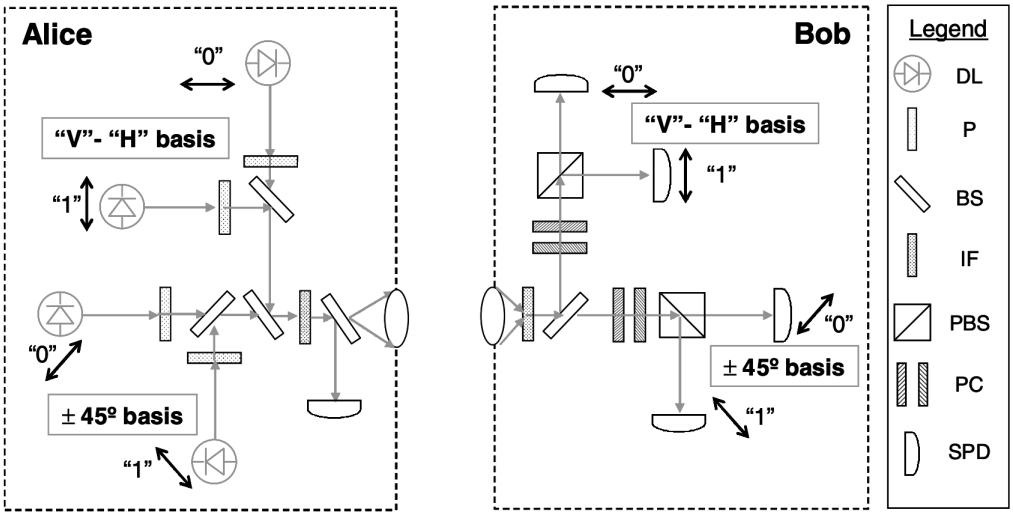

图20：BB84量子密钥分发发射机（Alice）和接收方（Bob）的偏振光学布局。转载自 Richard J. Hughes 等人发表于 New Journal of Physics 4, 43 (2002) 的图2[109]。Alice 的四个数据激光器（DL）的输出首先经过大幅衰减（平均光子数 μ¡ 1），然后由偏振片（P）线性偏振为 BB84态（双向箭头）。脉冲经非偏振分束器（BS）合束后，穿过空间滤波器（图中未示出）以消除空间模式信息，再经过干涉滤光片（IF）以抑制频谱侧信道，最后到达一个 50:50 分束器。透过该分束器的光子传向 Bob，反射的光子则由一个在 20 ns 门控时间内工作的单光子探测器（SPD）采样，以监测发射的 μ值；各数据激光器的相对时序经过匹配，误差在 SPD 的定时抖动范围内。在 Bob 端，入射脉冲先经过一个干涉滤光片，再由第一个分束器随机导入两个分析臂之一。在反射臂中，通过偏振控制器（PC）和偏振分束器（PBS）选择直线（H/V）基；若 PBS 两个输出端的 SPD 恰有一个在定时窗口内触发，则记录一个有效比特。透射臂则在共轭的对角（±45°）基上进行类似测量。多重探测事件（触发的 SPD 多于一个）会被记录，但不纳入密钥生成。

7 自由空间量子密钥分发的标准化

标准化对于自由空间量子密钥分发至关重要，因为它能确保不同系统和实现之间的兼容性与可靠性。通过制定通用协议、硬件要求、性能基准和测试方法，标准化使量子密钥分发能够无缝集成到现有通信网络中。它还能增强不同供应商之间的互操作性，促进广泛采用和规模化发展，从而有利于开拓更大的市场。此外，标准化的安全框架有助于验证自由空间量子密钥分发系统抵御潜在威胁的稳健性，确保全球网络安全应用中的基于量子密钥分发的加密值得信赖。

表1：标准制定组织中量子密钥分发工作项目概要

标准组	Work item code	标题	卫星量子密钥分发相关内容
国际电信联盟电信标准化部门 FG-QIT4N	D2.2	量子信息技术for网络use case：量子密钥分发网络	讨论量子密钥分发网络的用例，包括将量子密钥分发网络作为自由空间卫星— 将量子密钥分发网络作为自由空间卫星在线计划的... 地面或星间网络，识别架构影响和技术要求。
	D2.5	标准化展望和技术成熟度：Quantum key分发network	介绍前沿领域的进展量子密钥分发研究，重点关注卫星量子密钥分发，并强调其是标准化 量子密钥分发网络关键问题的重要方面。
ITU-T SG13	Y.3800	支持量子密钥分发的网络概述支持量子密钥分发的网络概述献	提供概念层结构QKDN 的特征及其定义能力。
	Y.3802	量子密钥分发网络——功能架架构	定义功能架构模型并指定参考点，以支持基于卫星的量子密钥分发网络 量子密钥分发网络。
	TR.SQKDN	标准化考量事项of基于卫星的QKDN	分析架构和功能基于卫星的QKDN
ITU-T SG17	TR.SQKDN-SC	安全性考量for基于卫星的量子密钥分发网络	提供关于潜在安全风险、安全要求，安全措施，针对基于卫星的 量子密钥分发网络。
ETSI 卫星地球站和系统技术委员会	DTS/SES-00469	卫星量子密钥分-发（S-QKD）卫星系统及相关光学-地面站（OES）	用例和参考架-构架、量子密钥分发协议和技术措施／运行措施型量子密钥分发系统。

许多国际标准制定组织（标准制定组织）都投入大量精力制定自由空间量子密钥分发标准，其中最主要的两个是国际电信联盟（ITU）和欧洲电信标准协会（ETSI）

其中的主要部分。

自2018年起，国际电信联盟电信标准化部门一直在制定量子网络标准。最初，该部门成立了网络量子信息技术焦点组（FG-QIT4N），以探讨量子信息技术在网络中的演进与应用，其中量子密钥分发是一项关键技术。FG-QIT4N 的成果文件将量子密钥分发网络（QKDN）讨论为自由空间卫星—地面网络或星间网络，并概述了预期的架构影响、技术要求，以及将指导未来标准化工作的协议、性能和安全要求。基于 FG-QIT4N 提供的基础性见解，国际电信联盟电信标准化部门第13研究组（SG13）一直在制定一系列量子密钥分发网络标准，包括要求、功能架构和业务流程，其中，将支持量子信道组网的自由空间光信道确定为量子密钥分发网络的一项能力。除这些技术规范外，第13研究组和第17研究组（SG17）还编制技术报告，分析基于卫星的量子密钥分发网络的功能要求和安全方面。

在 ETSI 中，量子密钥分发的标准化工作由专门的行业规范组（量子密钥分发行业规范组）开展。不同于国际电信联盟电信标准化部门在网络层面对量子密钥分发进行标准化，量子密钥分发行业规范组关注组件和接口等设备级规范。然而，量子密钥分发行业规范组的大部分工作聚焦于光纤网络，自由空间量子密钥分发的规范则属于 ETSI 卫星地球站和系统技术委员会（卫星地球站和系统技术委员会）的职责范围。卫星地球站和系统技术委员会已启动“卫星量子密钥分发（S-QKD）卫星系统及相关光学地球站（OES）”技术规范的制定工作，以规定卫星量子密钥分发系统的参考架构、量子密钥分发协议以及技术/运行措施。上述国际电信联盟电信标准化部门和 ETSI 工作项目的详细信息汇总于表1。

8 挑战与未来展望

尽管卫星量子通信取得了显著进展，但仍面临诸多挑战。首要技术挑战是大气湍流，它可能导致传输量子信号发生退相干和损耗。在卫星与地面站之间通信路径的最后一段，这种湍流尤为显著。目前正在开发各种自适应光学技术和纠错协议，以减轻这些影响并提高所接收量子态的保真度。

另一项关键挑战是量子中继器的开发，它对于突破直接传输所带来的限制、扩大量子通信的范围至关重要。量子中继器依赖纠缠交换和量子存储器，目前仍处于实验阶段，但它们是实现远距离、高保真度量子通信的关键。与此同时，研究人员正致力于缩小量子通信组件的尺寸，并将其集成到更小、更具成本效益的卫星平台中，例如立方体卫星，这有望显著降低部署全球量子网络的成本和复杂性。

卫星量子通信的未来前景广阔，新的协议和技术有望不断涌现，进一步提升量子通信系统的安全性和效率。量子通信卫星的持续发展，加上地面站技术和量子中继器网络的进步，很可能会在未来十年内促成全球量子互联网的实现。

表格 2：展示通信距离不断增加的关键量子密钥分发实验总结 ce

协议	**距离 实现 (km)**	**主要重要实验方法**
基于发光二极管的 BB84	1.0	采用发光二极管、无源光学元件实现低成本方案，面向最后一公里安全通信，配备单光子探测器 通信
连续变量量子密钥分发 (判离散变量信号)	24.2	后选择技术、偏振复用和量 子态层析成像，以提升采用 连续变量测量
诱骗态 BB84	90.0	先进的时间滤波和粗波分复用，可实现 在同一条链路上与双向 1 Gbps 经典数据共存。 光纤
基于纠缠的 量子密钥分发	100.0	使用超导 纳米线单光子 探测器 （超导纳米线单光子探测器）和超稳定马赫-曾德尔干涉仪，以 在长距离传输中保持纠缠保真度
测量- 设备- 独立 QKD	404.0	通过四强度诱骗态协议增强安全性， 高效率超导纳米线单光子探测器和优化的参数估计 通过超低损耗光纤
双场 QKD （SNS协议）	658.0	由相位锁定的超长距离通信 稳定激光器、外差频率校准和实时 相位补偿

致谢

G.G.R. 感谢 C. L. E. Moore 教职奖和麻省理工学院理学院研究创新种子基金的支持，该基金由 Alfred P. Sloan 基金会资助。N. K. Kundu 感谢印度国家量子任务、INSPIRE 教师奖学金（注册号：IFA22-ENG 344）、ANRF 总理早期职业研究资助（ANRF/ECRG/2024/000324/ENS）以及德里印度理工学院新教师种子基金提供的资金支持。

参考文献

[1] Anton A Huurdeman. 全球电信史. John Wiley & Sons，2003年。[2] Ralph C Merkle. 在不安全信道上的安全通信。《*ACM* 通讯》，21(4)：294–299，1978年。[3] Ruba Abu-Salma，M Angela Sasse，Joseph Bonneau，Anastasia Danilova，Alena Naiak- shina 和 Matthew Smith。采用安全通信工具的障碍。载于*2017* 年 *IEEE* 安全与隐私研讨会（*SP*），第 137–153 页。IEEE，2017年。[4] Thanh Tri Vo，Duong Anh Nguyen 和 TT Nhan Do。贸易与投资自由化的经济后果：以越南为例。全球化及其经济后果，第 214 页，2021年。[5]Betrand Ayuk Tambe，Ngoako Solomon Mabapa，Hlekani Vanessa Mbhatsani，Tshifhiwa Cynthia Mandiwana，Lindelani Fhumudzani Mushaphi，Merriam Mohlala 和 Xikombiso Gertrude Mbhenyane。南非林波波省家庭社会经济决定因素与粮食安全：一项横断面调查。《农业与粮食安全》，12(1)：19，2023年。[6] Samer Muthana Sarsam。自动驾驶车辆的网络安全挑战：威胁、漏洞与缓解策略。*SHIFRA*，2023：34–42，2023年。[7] Hui Dai，Qi Shen，Chao-Ze Wang，Shuang-Lin Li，Wei-Yue Liu，Wen-Qi Cai，Sheng-Kai Liao，Ji-Gang Ren，Juan Yin，Yu-Ao Chen 等。迈向基于卫星的量子安全时间传递。《自然·物理》，16(8)：848–852，2020年。[8] Attila A Yavuz，Saif E Nouma，Thang Hoang，Duncan Earl 和 Scott Packard。混合后量子时代的分布式网络基础设施与人工智能。载于*2022 IEEE* 第四届智能系统、隐私与安全国际会议（*TPS-ISA*），第 29–38 页。IEEE，2022。[9] Adam M Lewis，Martino Travagnin 等。欧洲安全量子通信基础设施：政策愿景的技术背景。欧盟出版局：卢森堡，2022。[10] Javier Oliva del Moral，Antonio deMarti iOlius，Gerard Vidal，Pedro M Crespo 和 Josu Etxezarreta Martinez。关键基础设施的网络安全：后量子密码学视角。*IEEE*物联网期刊，11(18)：30217–30244，2024年。[11] Alessia Zornetta。量子安全全球加密政策。《国际法律与信息技术杂志》，32：eaae020，2024年。[12] Abel Uzoka，Emmanuel Cadet 和 Pascal Ugochukwu Ojukwu。电信在促进物联网（IoT）连接与应用方面的作用。《科学技术综合研究与评论》，2(02)：055–073，2024年。[13] Mario Frustaci，Pasquale Pace，Gianluca Aloi 和 Giancarlo Fortino。评估物联网领域的关键安全问题：当前与未来挑战。*IEEE*物联网期刊，5(4)：2483–2495，2017年。

[14] Mehrnoosh Monshizadeh、Vikramajeet Khatri 和 Iris Adam。垂直行业的安全性。*Wiley 5G参考：安全*，2021年。[15] Chonggang Wang 和 Akbar Rahman。量子赋能的6G无线网络：机遇与挑战。*IEEE无线通信*，29(1):58–69，2022。[16] Togu Novriansyah Turnip、Birger Andersen 和 Cesar Vargas-Rosales。迈向6G身份验证与密钥协商协议：后量子混合密码学综述。*IEEE通信综述与教程*，2025年。[17] Gianfranco Cariolaro。量子通信，第2卷。施普林格，2015年。[18] Jasminder S Sidhu、Siddarth K Joshi、Mustafa G¨undo˘gan、Thomas Brougham、David Lowndes、Luca Mazzarella、Markus Krutzik、Sonali Mohapatra、Daniele Dequal、Giuseppe Vallone 等。空间量子通信进展。*IET QuantumCommunication*，2(4):182–217，2021年。[19] Arslan Shafique、Syed Ali Atif Naqvi、Ali Raza、Masoud Ghalaii、Panagiotis Papanastasiou、Julie McCann、Qammer H Abbasi 和 Muhammad Ali Imran。利用量子与经典密码学实现医疗图像安全传输的混合加密框架：适用于基于物联网的远程医疗网络。《科学报告》，14(1):31054，2024年。[20] Karuna S Bhosale、Siddhi Ambre、Zlatka Valkova-Jarvis、Anamika Singh 和 Maria Nenova。量子技术：释放其力量，塑造网络安全的未来。载于*2023*年第八届照明青年会议（照明），第1–4页。IEEE，2023年。[21] Mritunjay Shall Peelam、Anjaney Asreet Rout 和 Vinay Chamola。物联网的量子计算应用。*IET Quantum Communication*，5(2):103–112，2024年。[22] Georgi Gary Rozenman、Neel Kanth Kundu、Ruiqi Liu、Leyi Zhang、Alona Maslennikov、Yuval Reches 和 Heung Youl Youm。量子互联网：量子信息技术与6G网络的协同融合。*IET Quantum Communication*，4(4):147–166，2023年。[23] Sheng-Kai Liao、Wen-Qi Cai、Wei-Yue Liu、Liang Zhang、Yang Li、Ji-Gang Ren、Juan Yin、Qi Shen、Yuan Cao、Zheng-Ping Li 等。星地量子密钥分发。《自然》，549(7670):43–47，2017年。[24] Awais Khan、Tinh Thanh Bui、Junaid ur Rehman、Symeon Chatzinotas、Simon L Cotton、Octavia A Dobre、Trung Q Duong 和 Hyundong Shin。融合非地面与地面量子匿名网络。*IEEE网络*，2025年。[25] Ramona Wolf。量子密钥分发。施普林格，2021年。[26] Victor Lovic。量子密钥分发：优势、挑战与政策。剑桥大学科学与政策交流中心，2020年。[27] Michael M Wolf、David P´erez-Garc´ıa 和 Geza Giedke。玻色信道的量子容量。*Physical Review Letters*，98(13):130501，2007年。[28] Maithili S Jha、Samrit Kumar Maity、Manish Kumar Nirmal 和 Jaya Krishna。量子密码学与量子密钥分发协议综述。*Int. J. Adv.Res. Ideas Innov. Technol*，5:144–147，2019年。

[29] Charles H Bennett、Gilles Brassard 等。IEEE国际计算机、系统与信号处理会议论文集，1984年。[30] Yuval Bloom、Ilai Fields、Alona Maslennikov 和 Georgi Gary Rozenman。量子密码学——一项简化的本科实验与模拟。*Physics*，4(1):104–123，2022。[31]Dagmar Bruß 和 Norbert L¨utkenhaus。量子密钥分发：从原理到实践。*Applicable Algebra in Engineering, Communication and Computing*，10:383–399，2000年。[32] Ohad Lib、Kfir Sulimany 和 Yaron Bromberg。利用可编程光转换器处理高维纠缠光子。*Physical Review Applied*，18(1):014063，2022。[33] Artur K Ekert。基于贝尔定理的量子密码学。***Physical Review Letters***，67(6):661，1991年。[34] Goren Gordon 和 Gustavo Rigolin。利用部分纠缠态实现量子密码学。***Optics Communications***，283(1):184–188，2010年。[35] Yoshihisa Yamamoto 和 Kouichi Semba。量子信息技术的原理与方法，第624卷。施普林格，2016年。[36]Eden Arbel、Noa Israel、Michal Belgorodsky、Yonathan Shafrir、Alona Maslennikov、Sara P Gandelman 和 Georgi Gary Rozenman。量子态层析与贝尔测试的光学模拟——一项新颖的本科实验。*Results in Optics*，第100847页，2025年。[37] Charles H Bennett。利用任意两种非正交态实现量子密码学。***Physical Review Letters***，68(21):3121，1992年。[38] Sara P Gandelman、Alona Maslennikov 和 Georgi Gary Rozenman。量子密码学实践：使用脉冲激光进行B92协议实验。载于*Photonics*，第12卷，第220页。MDPI，2025年。[39] Dagmar Bruß。六态量子密码学中的最优窃听。*PhysicalReview Letters*，81(14):3018，1998年。[40] Helle Bechmann-Pasquinucci 和 Nicolas Gisin。量子密码学六态协议中的非相干与相干窃听。*Physical Review A*，59(6):4238，1999年。[41] Matthew McKague 和 Michele Mosca。广义自测试与六态协议的安全性。载于量子计算、通信与密码学会议，第113–130页。施普林格，2010年。[42] RS Amal 和 J Solomon Ivan。用于布洛赫球上优化问题的量子遗传算法。*Quantum Information Processing*，21(2):43，2022年。[43] Tobias Schmitt-Manderbach、Henning Weier、Martin F¨urst、Rupert Ursin、Felix Tiefenbacher、Thomas Scheidl、Josep Perdigues、Zoran Sodnik、Christian Kurtsiefer、John G Rarity 等。144公里自由空间诱骗态量子密钥分发的实验演示。*Physical Review Letters*，98(1):010504，2007年。

[44] Danna Rosenberg、Jim W Harrington、Patrick R Rice、Philip A Hiskett、Charles G Peterson、Richard J Hughes、Adriana E Lita、Sae Woo Nam和Jane E Nordholt。光纤中的长距离诱骗态量子密钥分发。*Physical Review Letters*，98(1):010503，2007年。[45] Qin Wang、Xiang-Bin Wang和Guang-Can Guo。采用预报单光子源的量子密钥分发实用诱骗态方法。*Physical Review A—Atomic,Molecular, and Optical Physics*，75(1):012312，2007年。[46] Jeffrey H Shapiro。利用量子照明抵御被动窃听。*PhysicalReview A—Atomic, Molecular, and Optical Physics*，80(2):022320，2009年。[47] Vidhya Prakash Rajendran和P Deepalakshmi。缓解量子密钥分发中的光子数分束攻击：对安全性漏洞的综合分析。载于*2024*年第五届电子与可持续通信系统国际会议（*ICESC*），第47–53页。IEEE，2024年。[48] Xiongfeng Ma、Bing Qi、Yi Zhao和Hoi-Kwong Lo。面向量子密钥分发的实用诱骗态。*Physical Review A*，72(1):012326，2005年。[49] Nikhil Dhingra、Hamid Mehrvar和Pierre Berini。硅波导上的高速偏振无关等离激元调制器。*Optics Express*，31(14):22481–22496，2023年。[50] George L Roberts、Marco Lucamarini、James F Dynes、Seb J Savory、ZL Yuan和Andrew J Shields。无调制器相干单向量子密钥分发。*Laser &Photonics Reviews*，11(4):1700067，2017年。[51] HF Chau。采用三种以上光子强度脉冲的诱骗态量子密钥分发。*Physical Review A*，97(4):040301，2018年。[52] Damien Stucki、Nicolas Brunner、Nicolas Gisin、Valerio Scarani和Hugo Zbinden。快速简便的单向量子密钥分发。*Applied Physics Letters*，87(19)，2005年。[53] Adarsh Jain、Parthkumar V Sakhiya和RK Bahl。量子密钥分发系统用弱相干脉冲源的设计与研制。载于*2020*年*IEEE*电子、计算与通信技术国际会议（*CONECCT*），第1–5页。IEEE，2020年。[54] Amirhosein Dadahkhani、Soheil Hajibaba、Hamid Asgari、Majid Khodabandeh、Fatemeh Rezazadeh、Azam Mani和Seyed Ahmad Madani。增强安全性相干单向量子密钥分发的实验实现。《*IEEE*开放获取》，2025年。[55] Siddharth Das、Riccardo Bassoli和Frank HP Fitzek。采用符合5G标准的纠错方案评估量子信道。载于*2024*年*IEEE*未来网络世界论坛（*FNWF*），第417–422页。IEEE，2024年。[56] Martin Sandfuchs、Marcus Haberland、Venkatesh Vilasini和Ramona Wolf。基于相对论原理的差分相移量子密钥分发安全性。*Quantum*，9:1611，2025年。[57] Emilien Lavie和Charles C-W Lim。面向高损耗信道的改进型相干单向量子密钥分发。*Physical Review Applied*，18(6):064053，2022.

[58] Lukas Scarfe、Felix Hufnagel、Manuel F Ferrer-Garcia、Alessio D'Errico、Khabat Heshami和Ebrahim Karimi。湍流信道中高维量子通信的快速自适应光学。*Communications Physics*，8(1):79，2025年。[59] Alan E Willner、Hao Huang、Yan Yan、Yongxiong Ren、Nisar Ahmed、Goudong Xie、Changjing Bao、Long Li、Yinwen Cao、ZJAIO Zhao等。利用轨道角动量光束的光通信。***Advances in Optics and Photonics***，7(1):66–106，2015年。[60] Mujtaba Zahidy、Domenico Ribezzo、Claudia De Lazzari、Ilaria Vagniluca、Nicola Biagi、Ronny M¨uller、Tommaso Occhipinti、Leif K Oxenløwe、Michael Galili、Tetsuya Hayashi等。已部署多芯光纤上的实用高维量子密钥分发协议。*Nature Communications*，15(1):1651，2024年。[61] Joseph Meyer、Yuval Reches、Georgi Gary Rozenman、Yaron Oz、Haim Suchowski和Ady Arie。利用光的空间模式进行自由空间量子密钥分发的类比：扩展距离与维数。*Optics Letters*，50(10):3297–3300，2025年。[62] Mhlambululi Mafu、Angela Dudley、Sandeep Goyal、Daniel Giovannini、Melanie McLaren、Miles J Padgett、Thomas Konrad、Francesco Petruccione、Norbert L¨utkenhaus和Andrew Forbes。基于轨道角动量并采用互为无偏基的更高维量子密钥分发。*Physical Review A—Atomic, Molecular, andOptical Physics*，88(3):032305，2013年。[63] Nicolas J Cerf、Mohamed Bourennane、Anders Karlsson和Nicolas Gisin。使用d能级系统的量子密钥分发安全性。***Physical Review Letters***，88(12):127902，2002年。[64] Alison M Yao和Miles J Padgett。轨道角动量：起源、行为与应用。***Advances in Optics and Photonics***，3(2):161–204，2011年。[65] Ilaria Vagniluca、Beatrice Da Lio、Davide Rusca、Daniele Cozzolino、Yunhong Ding、Hugo Zbinden、Alessandro Zavatta、Leif K Oxenløwe和Davide Bacco。面向实用高维量子密钥分发的高效时间箱编码。*Physical ReviewApplied*，14(1):014051，2020年。[66] Bahaa EA Saleh和Malvin Carl Teich。***Fundamentals of Photonics***，两卷集。John Wiley & Sons，2019年。[67] Muhammad Kamran、Muhammad Mubashir Khan和Tahir Malik。利用结构光在高维量子密钥分发系统的量子信道中诱导湍流。*AppliedPhysics B*，130(4):56，2024年。[68] Fr´ed´eric Bouchard、Khabat Heshami、Duncan England、Robert Fickler、Robert W Boyd、Berthold-Georg Englert、Luis L S´anchez-Soto和Ebrahim Karimi。采用扭曲光子的高维量子密钥分发协议实验研究。*Quantum*，2:111，2018年。[69] Barbara M Terhal。面向量子存储器的量子纠错。*Reviews of ModernPhysics*，87(2):307–346，2015年。

[70] Aristeidis Stathis、Argiris Ntanos、Nikolaos K Lyras、Giannis Giannoulis、Athanasios D Panagopoulos 和 Hercules Avramopoulos。《迈向卫星/光纤融合的 1550 nm 诱骗态BB84量子密钥分发网络：可行性分析与系统要求》。载于*Photonics*，第 11 卷，609 页。MDPI，2024年。[71] T. Honjo、S. W. Nam、H. Takesue、Q. Zhang、H. Kamada、Y. Nishida、O. Tadanaga、M. Asobe、B. Baek、R. Hadfield、S. Miki、M. Fujiwara、M. Sasaki、Z. Wang、K. Inoue 和 Y. Yamamoto。通过光纤实现长距离基于纠缠的量子密钥分发。*Opt. Express*，16(23):19118–19126，2008年11月。[72] Quyen Dinh Xuan、Zheshen Zhang 和 Paul L. Voss。基于光纤、采用离散信号的 24 km 连续变量量子密钥分发系统。*Opt. Express*，17(26):24244–24249，2009年12月。[73] K. A. Patel、J. F. Dynes、I. Choi、A. W. Sharpe、A. R. Dixon、Z. L. Yuan、R. V. Penty 和 A. J. Shields。高码率量子密钥分发与数据在光纤中的共存。*Phys. Rev. X*，2:041010，2012年11月。[74] Hua-Lei Yin、Teng-Yun Chen、Zong-Wen Yu、Hui Liu、Li-Xing You、Yi-Heng Zhou、Si-Jing Chen、Yingqiu Mao、Ming-Qi Huang、Wei-Jun Zhang、Hao Chen、Ming J un Li、Daniel Nolan、Fei Zhou、Xiao Jiang、Zhen Wang、Qiang Zhang、Xiang-Bin Wang 和 Jian-Wei Pan。通过 404 km 光纤实现测量设备无关量子密钥分发。*Physical Review Letters*，117:190501，2016年11月。[75] Yin Jiang 和 Jinfeng Liao。旋转条件下物质的配对相变。*PhysicalReview Letters*，117(19):192302，2016年。[76] Xiu-Xiu Xia、Zhen Zhang、Hong-Bo Xie、Xiao Yuan、Jin Lin、Sheng-Kai Liao、Yang Liu、Cheng-Zhi Peng、Qiang Zhang 和 Jian-Wei Pan。基于LED的光纤量子密钥分发：迈向低成本应用。*Photon. Res.*，7(10):1169–1174，2019年10月。[77] Jiu-Peng Chen、Chi Zhang、Yang Liu、Cong Jiang、Dong-Feng Zhao、Wei-Jun Zhang、Fa-Xi Chen、Hao Li、Li-Xing You、Zhen Wang、Yang Chen、Xiang-Bin Wang、Qiang Zhang 和 Jian-Wei Pan。通过 658 km 光纤进行量子密钥分发并实现分布式振动传感。*Physical Review Letters*，128:180502，2022年5月。[78]Momtchil Peev、Christoph Pacher、Romain All´eaume、Claudio Barreiro、Jan Bouda、Winfried Boxleitner、Thierry Debuisschert、Eleni Diamanti、Mehrdad Dianati、James F Dynes 等。维也纳的 SECOQC 量子密钥分发网络。*New journal ofphysics*，11(7):075001，2009年。[79] Cecilia Clivati、Alice Meda、Simone Donadello、Salvatore Virz`ı、Marco Genovese、Filippo Levi、Alberto Mura、Mirko Pittaluga、Zhiliang Yuan、Andrew J Shields 等。面向实际双场量子密钥分发的相干相位传递。*Nature communica-tions*，13(1):157，2022年。[80] Dong Pan、Gui-Lu Long、Liuguo Yin、Yu-Bo Sheng、Dong Ruan、Soon Xin Ng、Jianhua Lu 和 Lajos Hanzo。量子安全直接通信的演进：迈向量子互联网之路。*IEEE Communications Surveys & Tutorials*，26(3):1898–1949，2024年。

[81] Amir Javadpour、Forough Ja'fari、Tarik Taleb、Yue Zhao、Bin Yang 和 Chafika Benza¨ıd。面向物联网的加密即服务：机遇、挑战与解决方案。*IEEE Internetof Things Journal*，11(5):7525–7558，2023年。[82] Jean-Philippe Bourgoin、Brendon L Higgins、Nikolay Gigov、Catherine Holloway、Christo- pher J Pugh、Sarah Kaiser、Miles Cranmer 和 Thomas Jennewein。面向移动接收端的自由空间量子密钥分发。*Optics express*，23(26):33437–33447，2015年。[83] Sheng-Kai Liao、Hai-Lin Yong、Chang Liu、Guo-Liang Shentu、Dong-Dong Li、Jin Lin、Hui Dai、Shuang-Qiang Zhao、Bo Li、Jian-Yu Guan 等。日光条件下的长距离自由空间量子密钥分发，迈向星间通信。*Nature Photonics*，11(8):509–513，2017年。[84] Yu-Ao Chen、Qiang Zhang、Teng-Yun Chen、Wen-Qi Cai、Sheng-Kai Liao、Jun Zhang、Kai Chen、Juan Yin、Ji-Gang Ren、Zhu Chen 等。覆盖 4,600 公里的天地一体化量子通信网络。*Nature*，589(7841):214–219，2021年。[85] Wen-Qi Cai、Yang Li、Bo Li、Ji-Gang Ren、Sheng-Kai Liao、Yuan Cao、Liang Zhang、Meng Yang、Jin-Cai Wu、Yu-Huai Li 等。日光和夜间条件下的自由空间量子密钥分发。*Optica*，11(5):647–652，2024年。[86] Yang Li、Wen-Qi Cai、Ji-Gang Ren、Chao-Ze Wang、Meng Yang、Liang Zhang、Hui-Ying Wu、Liang Chang、Jin-Cai Wu、Biao Jin 等。基于微卫星的实时量子密钥分发。*Nature*，第 1–8 页，2025年。[87] Masoud Ghalaii 和 Stefano Pirandola。中等至强湍流空间中的量子通信。*Communications Physics 2022 5:1*，5:1–12，2022年2月。[88] Jasminder S. Sidhu、Siddarth K. Joshi、Mustafa G¨undo˘gan、Thomas Brougham、David Lowndes、Luca Mazzarella、Markus Krutzik、Sonali Mohapatra、Daniele Dequal、Giuseppe Vallone、Paolo Villoresi、Alexander Ling、Thomas Jennewein、Makan Mohageg、John G. Rarity、Ivette Fuentes、Stefano Pirandola 和 Daniel K.L. Oi。空间量子通信进展。*IET Quantum Communication*，2:182–217，2021年12月。[89] David Voelz、Erandi Wijerathna 和 Hanyu Zhan。强湍流散射区中 Fried 参数的公式是否准确？*OSA Continuum, Vol. 3,Issue 9, pp. 2653-2659*，3:2653–2659，2020年9月。[90] Valerian Ilich Tatarski。《湍流介质中的波传播》。Courier Dover Publications，2016年。[91] C Erven、B Heim、E Meyer-Scott、J P Bourgoin、R Laflamme、G Weihs 和 T Jen- newein。研究自由空间传输统计并改善湍流大气中的自由空间量子密钥分发。*New Journal of Physics*，14:123018，2012年。[92] Robert J Noll。泽尼克多项式与大气湍流。*JOSA, Vol. 66, Issue3, pp. 207-211*，66:207–211，1976年3月。[93] Mohammad Mirhosseini、Brandon Rodenburg、Mehul Malik 和 Robert W Boyd。湍流环境中的自由空间通信：平面波与轨道角动量编码的比较。*Journal of Modern Optics*，61:43–48，2014年。

[94] Georgi Gary Rozenman、Freyja Ullinger、Matthias Zimmermann、Maxim A Efremov、Lev Shemer、Wolfgang P Schleich与Ady Arie。利用表面重力水波观测相空间视界。*Communications Physics*，7(1):165，2024年。[95] Georgi Gary Rozenman、Shenhe Fu、Ady Arie与Lev Shemer。表面重力水波中的量子力学与光学类比。《流体》，4(2):96，2019年。[96] Georgi Gary Rozenman、Denys I Bondar、Wolfgang P Schleich、Lev Shemer与Ady Arie。经典波的玻姆轨迹与量子势观测。《物理学文稿》，98(4):044004，2023年。[97] Georgi Gary Rozenman、Denys I Bondar、Wolfgang P Schleich、Lev Shemer与Ady Arie。线性势中三缝实验的玻姆力学。《欧洲物理期刊专题》，232(20):3295–3301，2023年。[98] Renzhi Yuan与Julian Cheng。湍流信道中采用接收分集的自由空间光量子通信。《*IEEE*通信汇刊》，68:5706–5717，2020年9月。[99] Stefano Pirandola。自由空间量子通信的极限与安全性。《物理评论研究》，3，2021年。[100] Veronica Fernandez、Jorge G´omez-Garc´ıa、Alejandro Ocampos-Guill´en与Alberto Carrasco-Casado。利用象限探测器校正大气湍流引起的波前倾斜，以实现日光条件下的快速自由空间量子通信。《*IEEE*开放获取》，06:3336–3345，2018年。[101] Andres Ivan Martinez、Gabriele Cavicchioli、Seyedmohammad Seyedinnavadeh、Francesco Zanetto、Marco Sampietro、Alessandro D'Acierno、Francesco Morichetti与Andrea Melloni。用于自由空间光链路湍流补偿的自适应集成光子接收机。《科学报告》*2024*年*14:1*，14:20178–，2024年8月。[102] Lorenzo de Marinis、Peter Seigo Kincaid、Yann Lucas、Lea Krafft、Vincent Michau、Matteo Cherchi、Mikko Karppinen与Giampiero Contestabile。用于自由空间光链路湍流抑制的硅光子32输入相干合束器。《*IEEE*开放获取》，13:31718–31728，2025年。[103] Vincent Billault、Anaelle Maho、Jean Paul Mazellier、Patrick Feneyrou、Michel Sotom、Herve Lonjaret、Luc Leviandier、Arnaud Brignon、Jerome Bourderionnet与Xavier Normandin。基于空间解复用器与光子集成相干合束电路的自由空间光通信接收机。*Optics Express*，第*29*卷，第*21*期，第*33134-33143*页，29:33134–33143，2021年10月。[104] Yanli Ran、Zepeng Wei、Juncheng Fang、Ting Lei与Xiaocong Yuan。通过误差分析提升多平面光转换轨道角动量复用器性能。*Optics Express*，第*32*卷，第*14*期，第*25317-25326*页，32:25317–25326，2024年7月。[105] Mario Bad´as Aldecocea、Johannes Algera、Jasper Bouwmeester、Pierre Piron与J´erˆome Loicq。用于星间自由空间光通信的金属透镜。见Fr´ed´eric Bernard、Nikos Karafolas、Philippe Kubik与Kyriaki Minoglou编，国际空间光学会议——*ICSO 2024*，第13699卷，第1369913页。SPIE，2025年。

[106] Xingyu Wang、Tianyi Wu、Chen Dong、Haonan Zhu、Zhuodan Zhu与Shanghong Zhao。融合深度学习，以实现大气湍流下自由空间轨道角动量编码量子密钥分发的相位补偿。*Photonics Research*，第*9*卷，第*2*期，第*B9-B17*页，9:B9–B17，2021年2月。[107] Kexin Liang、Geng Chai、Zhengwen Cao、Qing Wang、Lei Wang与Jinye Peng。机器学习辅助的连续变量量子密钥分发过量噪声抑制。*arXiv*预印本 *arXiv:2207.10444*，2022。[108] Jianmin Yi、Hao Wu与Ying Guo。海洋湍流中可借助机器学习预测的被动连续变量测量设备无关量子密钥分发。*Entropy 2024*年，第*26*卷，第*207*页，26:207，2024年2月。[109] Richard J Hughes、Jane E Nordholt、Derek Derkacs与Charles G Peterson。日光与夜间条件下10千米的实用自由空间量子密钥分发。*New Journal of Physics*，4(1):43，2002年。