arXiv:2305.01554v1 [quant-ph] 2 May 2023

通过量子密钥分发网络保障的精密授时设施之间的国际时间传递

Francesco Picciariello,[1] *Francesco Vedovato,*[1,2,*] *Davide Orsucci,*[3] *Pablo Nahuel Dominguez,*[3] *Thomas Zechel,*[3] *Marco Avesani,*[1] *Matteo Padovan,*[1,4] *Giulio Foletto,*[1] *Luca Calderaro,*[5] *Daniele Dequal,*[6] *Amita Shrestha,*[3] *Ludwig Bl¨umel,*[3] *Johann Furthner,*[3] *Giuseppe Vallone,*[1,2] *Paolo Villoresi,*[1,2] *Tobias D. Schmidt,*[3] 和 *Florian Moll*[3]

[1] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*

[2] *Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6A, IT-35131 Padova, Italy*

[3] *German Aerospace Center (DLR), Institute for Communications and Navigation,München er Straße 20, 82234 Weßling, Germany*[4] *Centro di Ateneo di Studi e Attività Spaziali "Giuseppe Colombo",Università di Padova, via Venezia 15, IT-35131 Padova, Italy*[5] *ThinkQuantum s.r.l., via della Tecnica 85, IT-36030 Sarcedo, Italy*

[6] *Telecommunication and Navigation Division, Agenzia Spaziale Italiana, Matera, Italy*

全球导航卫星系统（GNSS），例如全球定位系统和伽利略卫星导航系统，可在全球范围内提供精确的时间和空间坐标，是现代社会关键基础设施的一部分。为了确保全球导航卫星系统可靠运行，需要高度精确且稳定的系统时间，例如由分布在世界各地精密授时设施中的多台独立时钟提供的时间。人们会定期测量各精密授时设施之间的相对时钟偏差，以便在必要时备用同步全球导航卫星系统卫星时钟。精密授时设施之间通信的安全性和完整性至关重要：一旦通信遭到破坏，全球导航卫星系统服务就可能中断。因此，采用量子密钥分发进行保护是一个极具吸引力的应用场景，因为这项技术可提供信息论安全。我们已开展实地试验演示这一应用场景：在两处精密授时设施之间共享加密的时间同步信息，其中一处位于德国奥伯法芬霍芬，另一处位于意大利马泰拉，两地直线距离超过900公里。要跨越如此远的距离，需要卫星量子密钥分发系统，并通过一条"最后一公里"地面链路，将光学地面站连接到精密授时设施的实际所在地。在演示中，我们部署了两套完整的量子密钥分发系统，以保护两地的最后一公里连接；并通过仿真表明，即将投入使用的量子密钥分发卫星能够利用现有光地面站，在奥伯法芬霍芬和马泰拉之间分发密钥。

I. 引言

目前部署的公钥密码基础设施依赖计算假设。随着量子计算机的出现，这些安全假设正受到挑战：量子计算机通过实现 Shor 算法 [1], ，能够破解最常见的公钥加密方案，例如 RSA [2] 和椭圆曲线密码系统 [3]。因此，开始逐步淘汰目前使用的公钥密码系统至关重要。尽管已有新的密码算法被认为能够抵御量子计算攻击 [4], ，但更为彻底且长远的解决方案是采用量子密钥分发（QKD）。这项技术无需依赖计算假设，而是利用量子力学定律实现安全通信，从而达到信息论安全 [5–7]。量子密钥分发能够彻底规避即将到来的量子计算机以及其他所有潜在算法和硬件进展所带来的威胁。

支撑数字基础设施和通信基础设施的关键服务，由于其对现代社会至关重要，应当通过采用量子密钥分发，成为首批升级至后量子计算安全标准的系统。欧盟正通过在多个欧洲国家开展实验性量子通信网络的开发与测试，借助 OpenQKD 等倡议推动这一方向 [8]。

在本研究中，我们在 OpenQKD 项目框架内展示了安全传输时钟差数据的可行性，这些数据是同步两个相距遥远的精密授时设施（PTF）时钟所必需的。其中一个位于德国奥伯法芬霍芬（OP）的德国航空航天中心（Deutsches Zentrum f¨ur Luft- und Raumfahrt, DLR）；另一个位于意大利马泰拉（MA）的意大利航天局马泰拉激光测距天文台（MLRO）。这是一个影响重大的应用场景，因为针对 PTF 之间时钟同步数据的攻击可能导致大范围服务中断。事实上，能够操纵或伪造同步数据的攻击者，可能会使使用这些数据进行同步的时钟产生微小的时间偏移；这些偏移可能导致由某个正在运行的 PTF 生成的全球系统时间缓慢漂移。例如，全球导航卫星系统（GNSS）要正常运行，就需要极其精确的系统时间；若攻击其底层 PTF，可能会导致全球范围内

*通讯作者：francesco.vedovato@unipd.it

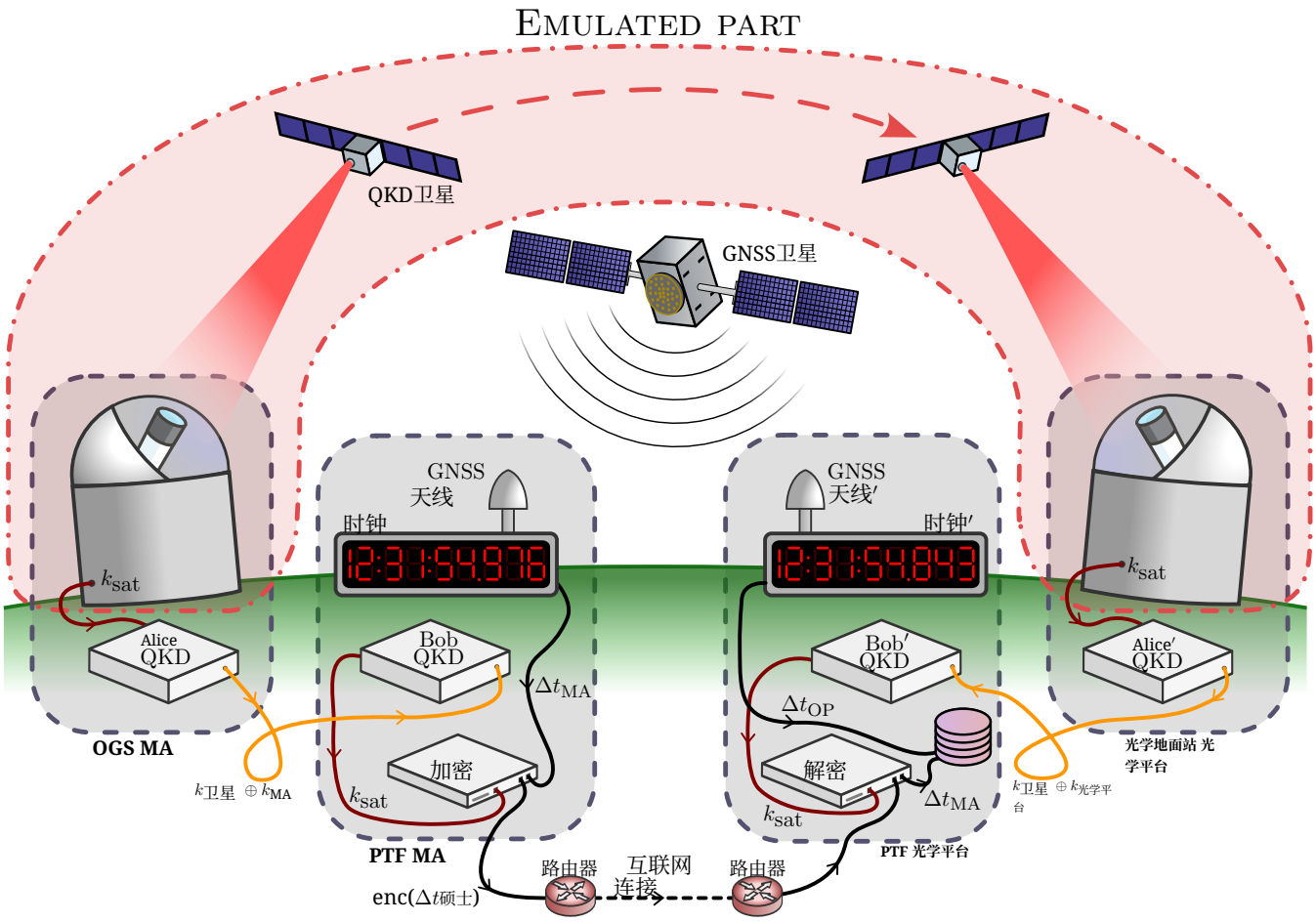


图1：量子加密时间传递用例演示示意图。左侧为马泰拉（MA）实验室，右侧为奥伯法芬霍芬（OP）实验室。灰色虚线框表示被视为处于安全边界内的设备（攻击者无法在物理上接触）。红色点划线框表示已进行模拟但尚未通过实验验证的设备，原因是目前尚无量子密钥分发卫星。说明：一颗量子密钥分发卫星将密钥 k_{sat} 分发给位于MA和OP的光学地面站；两条最后一公里量子密钥分发连接生成量子密钥 k_{MA} 和 k_{OP}，随后使用它们通过一次一密方式加密密钥 k_{sat}，并将其安全转发至位于MA和OP的PTF（分别传输密文$k_{\text{sat}} \oplus k_{\text{MA}}$ 和 $k_{\text{sat}} \oplus k_{\text{OP}}$）；在全可见卫星实验中，测量本地时钟与一颗全球导航卫星系统卫星之间的时间差 Δt_{OP} 和 Δt_{MA}；使用密钥 k_{sat} 对 Δt_{OP} 值进行AES加密，并通过互联网传输至MA，在那里使用同一密钥 k_{sat}进行AES解密；数值 Δt_{MA} 和 Δt_{OP} 保存在OP的本地，可用于监测时钟差$\Delta t_{\text{OP, MA}} = \Delta t_{\text{OP}} - \Delta t_{\text{MA}}$。

服务中断。

在我们的量子密钥分发展示中，我们保障了两个相距 900 多千米的 PTF 之间同步数据的传输（但这两个设施实际上并不属于伽利略地面段）。由于光功率会随距离呈指数级衰减，距离过长，无法通过直接光纤连接进行量子密钥分发交换 [7]。利用现有且已验证的技术实现如此远距离连接的一种方法，是使用卫星在两个设施之间建立量子密钥分发链路。具体而言，可以将卫星用作可信节点来中继量子生成密钥 [9]；或者采用更具雄心的方案，让卫星同时生成并分发纠缠光子对 [10] 给这两个

光子终端。在 MA 的光子终端和 OP 的光子终端附近都设有一个光学地面站（OGS），能够接收来自低地球轨道（LEO）卫星的光量子态，未来将用于卫星到地面量子密钥分发的实现。欧盟正在开发基于卫星的量子密钥分发技术，例如建造 Eagle-1 演示卫星 [11] 以及开展安全与密码任务（SAGA） [12]；关于量子密钥分发卫星项目的全面综述见参考文献 [11]。仍需完成的最后一步，是将量子生成密钥从各地的光学地面站安全转发至光子终端。这种“最后一公里”连接足够短，因此可以通过光纤上的量子密钥分发链路来确保安全，正如我们在实现中实验性地演示的那样；我们实验

性演示了这一点。如何利用量子密钥分发卫星和两条最后一公里连接来确保两个光子终端之间通信安全，其总体示意图如图1所示。

本文的结构如下。在第II节中，我们对用例演示和实验装置进行了初步描述。在第III 节中，我们介绍了两条最后一英里量子密钥分发连接的实现以及观测到的密钥生成率。在第IV 节中，我们介绍卫星量子通信链路的仿真，并展示该连接可借助现有的光地面站基础设施（例如位于马耳他和奥地利的两个光地面站）以及即将部署的量子密钥分发卫星实现。在第V 节中，我们进一步介绍时钟数据采集以及时间偏移的全景观测测量。在第VI 节中，我们给出结论并展望未来。

II. 用例演示描述与实验设置

本节对用例演示作总体介绍，如图1所示。该演示涉及四个实验部分的协调与同步运行：（1）通过全视野探测来自伽利略卫星星座的全球导航卫星系统信号，测量 OP 与 MA 中 PTF 时钟之间的时间偏移；（2）MA 中一条基于光纤的量子密钥分发链路；（3）OP 中的第二条量子密钥分发链路；（4）将时间差数据从 MA 实时加密并经认证地传输至 OP。

请注意，由于目前没有可进行量子态下行链路的欧洲卫星，因此，演示中需要使用卫星的部分尚未通过实验完成。在第 IV 节中，我们将说明，基于对卫星量子通信系统性能的合理假设，利用现有的光学地面站建立量子密钥分发链路是可行的。

A. 时间偏移测量

按照共视原理测量光学平台和 MA 处时钟之间的时间差：测量本地时钟与一颗同时处于两个光子终端 [13, 14]视线范围内的全球导航卫星系统卫星时钟之间的时间差。

GNSS卫星通过无线电信号传输其内部时钟 t_{sat}。在 OP 中的 PTF（以及 MA）处，利用大地测量型全球导航卫星系统接收机获取的本地时钟 t_{OP} （以及 t_{MA}）与 t_{sat}进行比较。由于光速有限，信号 t_{sat} 经过一定的传播时间 $\tau_{\mathrm{sat,\ PTF}}$后才到达 PTF，因此实际测得的时间差为

$$\Delta t_{\mathrm{PTF,sat}} = t_{\mathrm{PTF}} - \left(t_{\mathrm{sat}} - \tau_{\mathrm{sat,PTF}}\right) \tag{1}$$

其中， t_{PTF} 可指 t_{MA} 或 t_{OP}，$\tau_{\mathrm{sat、\ PTF}}$ 和$\Delta t_{\mathrm{PTF、\ sat}}$也同理。传播时间根据卫星星历数据（通过卫星测距测量 [13, 14]进行校准）以及 GNSS 接收天线的地理位置估算。要获得$\widetilde{\tau}_{\mathrm{sat、\ PTF}}$ $\tau_{\mathrm{sat、\ PTF}}$的准确估计，还需要电缆延迟和电离层效应等其他校准数据。随后计算校正后的时间差：

$$\Delta t^{\mathrm{corr}}_{\mathrm{PTF,sat}} = t_{\mathrm{PTF}} - \left(t_{\mathrm{sat}} - \tau_{\mathrm{sat,PTF}} + \widetilde{\tau}_{\mathrm{sat,PTF}}\right) \tag{2}$$

然后，通过将两个（经校正的）时间差相减，测得两个 PTF 时钟之间的时间偏移

$$\Delta t^{\mathrm{meas}}_{\mathrm{OP,MA}} = \Delta t^{\mathrm{corr}}_{\mathrm{OP,sat}} - \Delta t^{\mathrm{corr}}_{\mathrm{MA,sat}} \simeq t_{\mathrm{OP}} - t_{\mathrm{MA}} \tag{3}$$

请注意，相减后，卫星时钟的影响便被消除。

在全景观测测量中，可以同时使用一个或多个 GNSS 星座中的多颗卫星，以获得更精确的时间偏移估计；精度大致随所用卫星数量的平方根提高。此外，使用 GNSS 星座，即使两个光子终端之间从未有共同视野的卫星（例如，两个光子终端位于地球上的对跖点），也能测量它们之间的时间偏移。这是因为 GNSS 星座中的时钟彼此同步。在这种情况下，光子终端与 GNSS 系统时间之间的（经校正）时间差可表示为

$$\Delta t^{\mathrm{corr}}_{\mathrm{PTF,GNSS}} = t_{\mathrm{PTF}} - \bar{t}_{\mathrm{GNSS}} \tag{4}$$

其中中位数

$$\bar{t}_{\mathrm{GNSS}} = \underset{\mathrm{sat}\in\mathrm{GNSS}}{\mathrm{median}} \left(t_{\mathrm{sat}} - \tau_{\mathrm{sat,PTF}} + \widetilde{\tau}_{\mathrm{sat,PTF}}\right) \tag{5}$$

是在给定时刻对从 PTF 可见的全球导航卫星系统卫星集合计算得出的；采用中位数是因为它比平均值更稳健（例如，它不受单颗卫星时间读数毛刺的影响）。请注意，需要每颗可见卫星的星历数据。OP 与 MA 之间的时间偏移通过以下差值获得

$$\Delta t^{\mathrm{meas}}_{\mathrm{OP,MA}} = \Delta t^{\mathrm{corr}}_{\mathrm{OP,GNSS}} - \Delta t^{\mathrm{corr}}_{\mathrm{MA,GNSS}} \simeq t_{\mathrm{OP}} - t_{\mathrm{MA}} \tag{6}$$

其中已消除 GNSS 系统时间的影响。

在我们的演示中，我们采集了 16 颗伽利略卫星连续两天的时钟数据。GNSS 数据的采集以及传播时间的估计详情$\tau_{\mathrm{sat,\ PTF}}$ 详见第 V 节。

B. 使用量子密钥分发保障最后一公里连接

QKD能够在相距遥远的双方之间生成共享秘密比特串，双方通常称为Alice和Bob，

双方通过量子通信信道和经典认证信道相连。安全性由量子力学定律保障：未知量子态不可能被忠实复制，因此，试图获取量子态所编码信息的窃听者（通常称为Eve）必然会引入过量噪声。通过监测交换量子态的保真度，Alice和Bob可以对Eve可获取的信息量建立严格的上界。如果噪声过高，Eve可能获得过多的互信息，协议就必须中止；否则，就能生成安全的量子密钥。通过信息协调和隐私放大这两种经典后处理算法，可以使原始密钥达到近乎完美的隐私性和正确性 [6, 7]。

在我们的应用场景中，已建立两条量子密钥分发链路：一条使用 ThinkQuantum s.r.l. 提供的商用量子密钥分发系统 [15]（位于光学平台），另一条使用帕多瓦大学在 MA 开发的研究原型。建立这两条链路的目的是，在光学平台和 MA 的最后一公里连接中安全转发信息；Alice 模块（量子密钥分发发射机）位于光地面站，Bob 模块（量子密钥分发接收机）位于光子终端。这两条最后一公里连接采用可信节点配置：光地面站充当中间可信节点，生成 k_{sat} 并将其安全转发至光子终端这一最终目的地。MA（以及光学平台）的基于光纤的量子密钥分发链路用于在 Alice 和 Bob 模块之间分发本地生成的密钥 k_{MA} （k_{OP}）。随后，该密钥用于对卫星密钥进行一次一密加密，生成的密文 $k_{\mathrm{sat}} \oplus k_{\mathrm{MA}}$（$k_{\mathrm{sat}} \oplus k_{\mathrm{OP}}$）通过经认证的经典信道从 Alice 模块转发至 Bob 模块（该信道也用于支持量子密钥分发后处理）。Bob 模块使用 k_{MA} （k_{OP}）恢复数值k_{sat}，最后，密钥 k_{MA} （k_{OP}）完成其功能后即被删除。

如第 IV 节所分析的，将密钥k_{sat} 分发至马萨诸塞州（MA）和光学平台（OP）中的光学地面站（OGS），采用不久后即可投入使用的卫星量子密钥分发技术是可行的。为了进行本次演示，在分别运往 MA 和 OP 之前，已将一个随机比特串 k_{sat} 预先上传至两个 Alice 模块中。我们注意到，在采用实际的卫星量子密钥分发系统时，端到端量子密钥分发链路也是以类似的异步方式建立的。事实上，通过卫星分发量子密钥的时延可能长达数天甚至数周，具体取决于可用量子密钥分发卫星的数量以及当地天气条件。因此，必须提前充分创建密钥 k_{sat}，并在本地进行缓存，以便在必要的时间内保存。

C. 数据加密、认证与实时数据传输

用例演示的最后一部分是确保 MA 与 OP 之间时间偏移测量值通信的安全性。我们注意到，这些数据没有特别的隐私或机密性要求，因此无需加密。然而，为了避免潜在攻击者进行数据篡改，通信必须经过身份验证。

为保障时间偏移测量通信的安全性，我们采用了由 Rhode & Schwarz GmbH & Co [16], 制造的商用加密器原型 SITLine ETH4G/40G。两台 SITLine 设备和四套量子密钥分发系统均提供适配量子密钥分发的接口 ETSI GS QKD 004，使这两类设备之间的通信能够使用量子密钥。这类接口在量子密钥分发领域尚属较新，体现了这些系统已具备支持更先进量子密钥分发网络的能力。

如图 1所示，每两分钟，两个加密器都会向 Bob量子密钥分发设备请求一个密钥。密钥刷新时间是一项安全参数，可根据需求适当放宽。SITLine工作在数据链路层（ISO/OSI模型的L2层）。为了通过互联网将加密数据包从MA发送到OP，我们使用方案中所示的两个路由器，将数据封装到网络层（ISO/OSI模型的L3层）。密钥长度为256位，因此加密器能够对所有天线传输数据实施AES-256加密协议 [17]。由于加密器默认实施 AES，且我们对密钥生成没有特别限制，因此选择对实验期间传输的所有数据进行加密。请注意，使用 Wegman-Carter方案时，可以利用数量仅随消息长度对数增长的密钥比特，实现具备信息论安全性的身份验证 [18]。

两个路由器之间的经典信道启用后，MA 中天线获取的数据每 30 分钟自动发送至加密器，在 OP 中解密，并存储在计算机中进行分析。需要注意的是，我们的加密方案确保了从全球导航卫星系统天线到路由器另一端的数据安全。然而，对于许多卫星定位系统而言，全球导航卫星系统信号遭受欺骗攻击是当前面临的问题 [19], ，这类攻击可能从源头污染数据。如今，我们通过使用伽利略卫星网络来避免这一问题，该网络采用开放服务导航消息认证（OSNMA），其提供的认证方法比其他系统（如全球定位系统）更强 [20, 21]；此外，还会对全球导航卫星系统数据执行完整性和一致性检查，并使用多阵列天线来减少欺骗攻击和干扰。未来，可以将量子密钥分发卫星集成到该网络中，以便对这部分信号也进行认证 [22]。

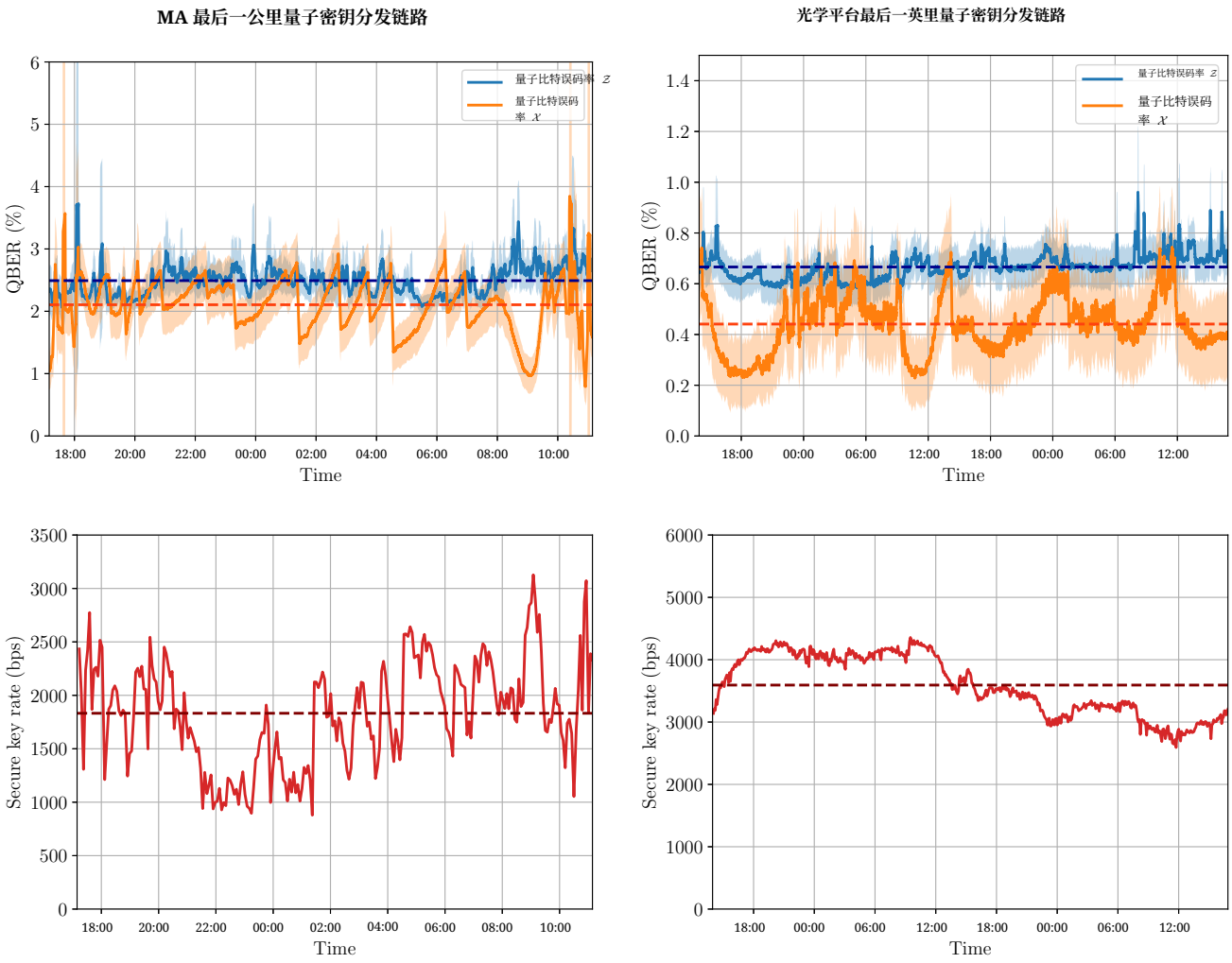


图 2：两个量子密钥分发系统在量子比特误码率和密钥生成率方面的性能概要。量子比特误码率采用 5 分钟滚动窗口绘制，色带表示 ± 1 个标准差。虚线表示平均值。对于马泰拉， Z 基中的量子比特误码率、 X 基中的量子比特误码率和密钥生成率的平均值分别为 2.5%、2.1% 和 1.9 kbps。对于奥伯法芬霍芬， Z 基中的量子比特误码率、 X 基中的量子比特误码率和密钥生成率的平均值分别为 0.7%、0.4% 和 3.6 kbps。

III. 最后一公里量子密钥分发链路

MA 中光学地面站与 PTF 之间，以及 OP 中光学地面站与 PTF 之间的共享密钥 k_{sat} 分发工作，交由两个基于光纤的量子密钥分发系统完成。这两个系统实现了必要的“末端”连接，以生成本地密钥 k_{MA} 和 k_{OP}。本节将详细介绍这两条末端量子密钥分发链路在两个地点的实施方式，以及我们在演示中取得的性能——即量子比特误码率（QBER），也就是 Alice 发送的信号与 Bob 接收的信号之间的不匹配率，以及安全密钥率（SKR）。

A. 马泰拉基础设施

位于 MA 的量子密钥分发系统与参考文献 [23]，中所述的系统类似，该系统实现了三态高效 BB84协议 [24]，采用偏振调制和单诱骗态技术 [25]。发射机主要由一个波长为 1310 nm 的激光器组成，该激光器以 50 MHz 的重复频率发射脉冲；一个强度调制器，用于设定诱骗态所需的平均光子数；以及一个基于 iPOGNAC方案的偏振调制器 [26]。值得注意的是，这是首次将 iPOGNAC方案用于 O波段的量子密钥分发信号。最后，脉冲经可变光衰减器衰减至单光子水平以下，然后进入光纤信道。电子设备主要由一款配有现场可编程门阵列和中央处理器的片上系统（SoC）组成。完整的片上系统架构说明请参阅参考文献 [27]。

生成后，衰减激光脉冲进入量子信道并向接收机传输。量子信道是一段长 10 km 的标准单模电信光纤：包括发射机和接收机接口处额外损耗在内，总损耗为 8.5 dB。

接收机通过时间复用方案解码这些状态：尽管该方案会额外引入 3 dB 的损耗，但能够提升系统的紧凑性，并显著降低系统成本。事实上，所实现的系统仅需一个 InGaAs/InP 单光子雪崩二极管（SPAD），本例中采用的是 Micro Photon Devices S.r.l. 的 PDM-IR，其量子效率为 15%。光子到达时对应的时间标签由 qutools GmbH 的 quTAU 时间数字转换器记录，并传送至计算机进行数据处理。

为进一步降低架构要求，量子密钥分发系统利用 Qubit4Sync算法 [28] 实现发射机与接收机之间的时间同步，从而无需专用系统来分发时钟基准。

在 MA 中，演示期间的密钥生成总时间为 18 小时，系统在此期间生成了 119 Mb 安全密钥。MA 中所用量子密钥分发系统的性能显示在图2。

B. 奥伯法芬霍芬基础设施

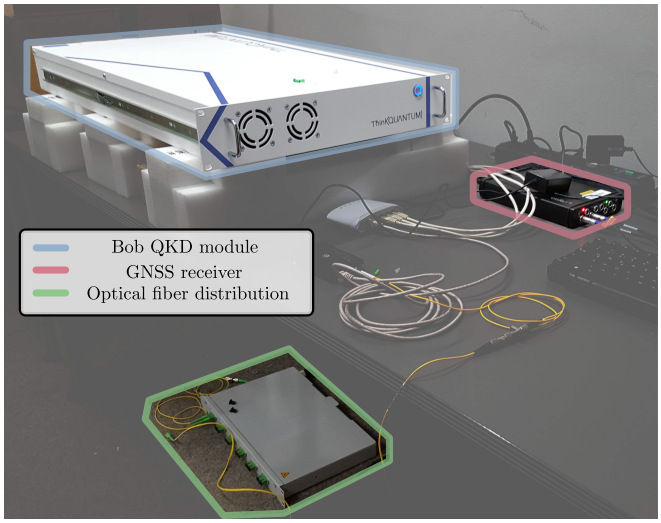


图 3：光学平台（OP）中实验装置的照片。Bob量子密钥分发模块（ThinkQuantum）基于 QUKY 平台。全球导航卫星系统接收机为商用 PolaRx5接收机（Septentrio）。

有关部署在光学平台中的量子密钥分发系统的规格，请参阅 ThinkQuantum s.r.l. 开发的 QUKY平台 [15]。作为 MA 中使用的系统，QUKY平台通过偏振编码和名为 Qubit4Sync 的同步技术，实现了三态单诱骗高效 BB84协议，并配备所需的协议栈，包括经过身份验证的辅助数据传输和原始密钥后处理（信息协调与隐私放大），以生成安全密钥

在光学平台（OP）的实现中，量子信道采用了一段长500米的标准单模光纤，并额外增加了损耗，使总损耗达到12 dB。系统总工作时间为51小时，生成了660 Mb的安全密钥。光学平台（OP）中所使用的量子密钥分发系统的性能如图2右侧各面板所示。光学平台（OP）实验装置的部分照片如图3所示。

IV. 卫星信道仿真

为了评估 MA 和 OP 中光学地面站（OGSs）之间的密钥预共享（理想情况下，该密钥源自卫星到地面的量子密钥分发（QKD）信道），我们模拟了卫星发送端与分别部署在两个地面站中的两个接收机之间的量子密钥分发协议。该模拟旨在估算可用密钥生成率（SKR）的平均值，该密钥生成率可通过最后一公里量子密钥分发密钥进行一次一密加密，从而将预共享密钥传递至终端节点 PTF-MA 和 PTF-OP。

这两个地点已配备两台望远镜，孔径分别为 1.5 m（MA）和 0.8 m（OP）。我们假设有两台用于 1550 nm 光源的量子密钥分发接收机，需要通过光纤注入系统将望远镜收集到的信号传送至探测器。

仿真过程如下：首先，我们将卫星沿给定轨道传播，使其能够经过两个地面站；然后，我们针对每次经过计算信道统计数据，以估算地面站的损耗和原始密钥累积；最后，我们根据标准的有限密钥安全性证明计算密钥生成率生成情况 [25]。

A. 轨道传播

我们模拟了一颗高度为 500 km 的低地球轨道（LEO）卫星。该轨道的倾角为 75.6 度，升交点赤经（RAAN）为 300.6 度，每天经过两个地面站上空两次。卫星配备了一台直径为 15 cm 的发射望远镜，以及一个光源波长为 1550 nm 的量子密钥分发系统。卫星在一段时间内沿轨道运行，轨道按 1 秒的步长进行离散化。对于每个步长，如果有地面站可用以建立光学量子信道，则按照以下章节所述进行信道模型分析，以计算探测统计量。我们仅考虑仰角高于 20 度的过境，因为仰角较低时，大气吸收和湍流会显著降低链路质量



图 4：实验时长为一天的卫星轨道传播。两个点分别表示位于意大利 MA 和德国 OP 的两个地面站。蓝线表示卫星传播所经过的轨道。白色线段表示卫星与地面站之间可进行光通信。

。图 4展示了模拟轨道的一个示例。

两个站点每天的平均有效过境时间分别为：MA 为 9.04 分钟，光学平台为 10.20 分钟，通常每天过境两次。值得注意的是，得益于波长的选择（该波长下大气造成的损耗较少、背景噪声较低），即使利用白天过境期间累积的探测结果，也能够生成安全密钥。

B. 信道模型

对于轨道上的每一个点，我们根据发射机、接收机和信道的物理参数，计算从卫星到地面站的信道效率。计算信道效率时，我们仅考虑离散化轨道上每个点的平均值。

信道效率 η 计算为

$$\eta = \eta_a \eta_g \eta_f \eta_0 \tag{7}$$

其中 η_a 表示大气透射率，由大气散射和吸收造成，取自 LOWTRAN [29]（见图 5），η_g 表示几何透射率，由接收机望远镜尺寸有限、截断入射光束所造成，η_f 表示角度透射率，由接收系统的角度接收范围有限以及指向误差造成，而 η_0

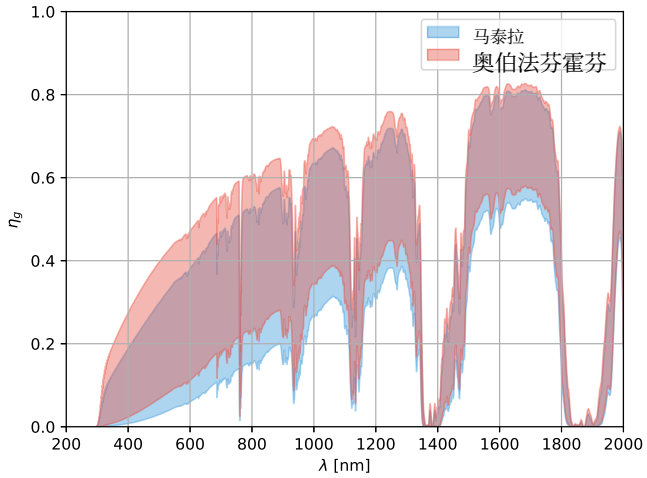


图 5：MA 和光学平台两个站点的卫星至地面大气透射率，范围从天顶方向（透射率较高）到仰角 20 度（透射率较低）。数据使用 LOWTRAN [29] 计算，计算时考虑了中纬度冬季大气。

计入系统的所有固定附加损耗。

为计算 η_g，我们首先将光束从发射机孔径传播至地面。接收机处的光束半径 w_g 取决于高斯光束 θ_d 的衍射极限发散，以及大气湍流 θ_t 引起的发散；大气湍流会扰动光束波前。我们假设发射机的角指向误差可以忽略。

因此，总散度 θ 计算为

$$\theta = \sqrt{\theta_d^2 + \theta_t^2} = \sqrt{\left(\frac{\lambda}{\pi w_0}\right)^2 + \left(\frac{\lambda}{\pi \rho_0}\right)^2} \tag{8}$$

其中 λ 是量子密钥分发信号的波长，w_0 是发射机处的高斯光束半径，ρ_0 是球面波 [30]的大气相干长度。根据折射率结构常数 C_n^2，可以计算星地路径的 ρ_0，即

$$\rho_0 = \left[1.46 k^2 R \int_0^1 (1-\xi)^{\frac{5}{3}} C_n^2(\xi R) d\xi\right]^{-\frac{3}{5}} \tag{9}$$

其中，$k = 2\pi/\lambda$ 为光子的波数，R 为到地面站的斜距，关于 ξ的积分考虑了光束沿路径的传播，而 $C_n^2(\xi R)$用于获取与点 ξR高度相关的 C_n^2。我们采用 Hufnagel-Valley 模型描述C_n^2，该模型有两个自由参数：地面高度处的 C_n^2 值和平均风速 [31]。

利用傍轴近似，地面处的光束半径表示为 [32]

$$w_g = \sqrt{w_0^2 + (\theta R)^2} \tag{10}$$

接下来， η_g 计算为高斯光束在带有内圆形遮挡的圆形孔径上的积分（这是卡塞格伦结构的典型情况，此时次镜会部分遮挡主镜）。由此得到 [33]

$$\eta_g = \exp\left(-\frac{D_{\mathrm{Rx,occ}}^2}{2w_g^2}\right) - \exp\left(-\frac{D_{\mathrm{Rx}}^2}{2w_g^2}\right) \tag{11}$$

其中， D_{Rx} 为接收望远镜主镜的直径，$D_{\mathrm{Rx,\ occ}}$ 为（部分遮挡的）次镜直径。请注意，在 $D_{\mathrm{Rx}} \ll w_g$的极限情况下，几何透射率近似正比于望远镜面积，因此

$$\eta_g \approx (D_{\mathrm{Rx}}^2 - D_{\mathrm{Rx,occ}}^2)/2w_g^2 \tag{12}$$

角透射率 η_f 由接收望远镜的视场与系统的角指向误差叠加计算得出：

$$\eta_f = 1 - \exp\left(-\frac{\theta_{\mathrm{Rx}}^2}{2\alpha_{\mathrm{Rx}}^2}\right) \tag{13}$$

其中， θ_{Rx} 为接收机固有的半视场角，α_{Rx} 为望远镜的指向误差。

在 η_0 中，我们考虑了附加损耗，例如接收端光学器件造成的损耗（估计约为 3–5 dB），以及信号光纤耦合造成的损耗（采用高端自适应光学系统时估计约为 8–10 dB） [33, 34]。由于无法获得不同设备的测量数据，我们决定将 η_0 固定为 13 dB。

C. 密钥分析

我们模拟采用一种诱骗态的高效 BB84协议，并遵循文献 [25] 中提出的安全性证明。该安全性证明考虑了有限密钥效应，因此必须先完成预先选定数量的测量，才能将安全密钥作为协议的输出。

计算出信道效率，也就知道了从卫星接收光子的概率，随后我们便开始在接收机侧累积光子计数，即进行量子态测量。对于轨道上的每个位置，我们都可以计算出在相应时间内探测器接收到的光子数。所谓的原始密钥由 Alice 和 Bob 测量基匹配的所有测量结果构成；达到有限密钥分析所需的密钥长度后，我们便计算安全密钥率。我们累积不同次过境产生的原始密钥：这是出于设计上的考虑，其优点是能够提高安全密钥生成率，因为密钥越长，有限密钥开销的影响越小；另一方面，这需要卫星侧配备更大的存储器，并出于安全原因进行额外的存储器管理。由于

我们选择使用波长为 1550 nm 的系统，并且必须将信号耦合到单模光纤中以降低背景噪声，因此可以利用高端探测器进行测量。超导纳米线单光子探测器（SNSPD）效率可超过 90% η_{det} ，且噪声极低，每秒计数少于 100 次，因此是此类应用的最佳选择。我们还必须考虑协议运行期间出现的错误，这些错误最终会导致双方共享的密钥不匹配。错误的主要来源是探测器记录到的随机事件，这些事件来自信道的背景光和探测器本身（以暗计数的形式），以及量子器件非理想性导致的量子态编码和解码错误。仿真的其他参数均作为输入，而背景光则可通过 LOWTRAN [29] 将其定义为漫射大气辐亮度。其他影响探测的因素，例如来自太阳照射卫星后反射的直射光，则未予考虑。

在表I 中列出了仿真中使用的最相关参数。

数量	值
λ	1550 纳米
η_{det}	0.9
w_0	0.15 米
η_0	13 dB
$D_{\mathrm{Rx}}^{\mathrm{MA}}$	1.5 米
$D_{\mathrm{Rx,occ}}^{\mathrm{MA}}$	0.1 米
$D_{\mathrm{Rx}}^{\mathrm{OP}}$	0.8 米
$D_{\mathrm{Rx,occ}}^{\mathrm{OP}}$	0.3 米
θ_{Rx}	6。25 µrad
α_{Rx}	100 微弧度
C_n^2 在地面高度	10^{-14} $\mathrm{m}^{-2/3}$
风速	21 米/秒
卫星高度	500 千米
卫星倾角	75.6°
卫星升交点赤经	300。6°
卫星近地点幅角 84.38°	
卫星平近点角	38。29°
光源重复频率	500 MHz
编码误差	0.5 %
暗计数率	100 Hz
探测器死时间	10 ns
时间抖动	10 ps
有限密钥长度	100 Mb
保密参数	10^{-10}
正确性参数	10^{-15}

表 I：卫星量子密钥分发仿真的相关输入参数。

D. 仿真结果

两座光学地面站（OGS）在全年内生成的密钥总量分别为：MA 为 5.42 Gb，OP 为 1.71 Gb，相当于平均密钥生成率（SKR）分别为 171.7 bps 和 54.1 bps。由于这两套加密系统所采用的加密协议需要 256 bpm，因此满足这一要求。卫星每次过境平均生成 1.55 Mpbs 的原始密钥，具体数值取决于天顶角。

如果考虑到阴天的概率，在最坏情况下，阴天会导致无法进行光学通信，但结果仍高于阈值。根据参考文献 [35]，MA 和光学平台的阴天概率分别为 34.2 % 和 55.3 %。相应地，平均密钥生成率分别为 113.01 bps 和 24.17 bps。

V. 全球导航卫星系统及时钟数据采集与数据分析

光学平台中的时钟与 MA 中的时钟之间的时间偏移采用全视法测量，如第IIA [14]节所述。为实现卫星时钟与 PTF 之间的一致比较，必须估算传播时间 $\tau_{\text{sat, PTF}}$并将其扣除。真实传播时间的估算值 $\widetilde{\tau}_{\text{sat, PTF}}$ 通过将所有已知的相关影响相加得到，这些影响分为动态效应和静态效应：

$$\widetilde{\tau}_{\text{sat,PTF}} = \widetilde{\tau}_{\text{dynamic}} + \widetilde{\tau}_{\text{static}} \tag{14}$$

动态变化的传播时间可表示为

$$\widetilde{\tau}_{\text{dynamic}} = \frac{\chi}{c} + \Delta t_{\text{rel}} - \Delta t_{\text{tropo}} - GD \tag{15}$$

with

$$\chi = \left[P_{\text{IF}} - \left\|\vec{x}_{\text{sat}} - \vec{x}_{\text{rec,IF}}\right\| - S\right] \tag{16}$$

其中， P_{IF} 为卫星与接收机之间的无电离层伪距， $\vec{x}_{\text{sat}}$ 为卫星在发射时刻于国际地球参考框架（ITRF）中的位置，$\vec{x}_{\text{rec, IF}}$ 为接收机天线在 ITRF 中的无电离层相位中心， S 为与地球自转相关的萨格纳克改正， Δt_{rel} 为相对论改正， Δt_{tropo} 为对流层引起的延迟， GD 为卫星发射信号的群时延。更多详情请参见参考文献 [14]。通常会针对测量期间可用的每颗卫星计算这一量，并将其显示在《通用 GPS GLONASS 时间传递标准》（CGGTTS） [36]中。分析需要连续 13 分钟的数据采集，且期间不能与卫星失去联系。

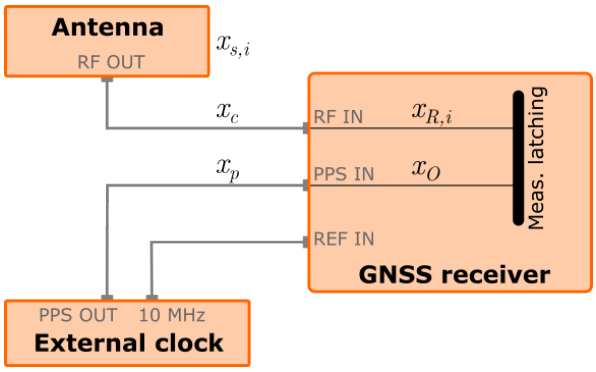


图 6：系统测量时延示意图。$x_{s,\,i}$：信号 i 在天线中的延迟；$x_{R,\,i}$：信号 i 在接收机射频部分的延迟； x_C：射频电缆中的延迟（包括放大器和分路器）； x_p：PPS电缆中的延迟； x_O：PPS输入端与接收机内部时间基准之间的延迟。更多信息请参见参考文献 [37, 第 4 节。1]

静态校正项源于 PTF测量系统中的传播延迟。这些延迟包括天线、射频电缆以及全球导航卫星系统接收机内部的延迟：

$$\widetilde{\tau}_{\text{static}} = \frac{1}{c}(x_s + x_c + x_R - x_O - x_p) \tag{17}$$

其中，各延迟项的说明见图 6。

A. 全球导航卫星系统数据采集

我们测量了光学平台 PTF 与 MA PTF 之间的时间偏移。两个光子终端均使用商用 PolaRx5接收机（Septentrio），并连接至扼流圈多频段GNSS天线（NovAtel GNSS-750、Leica AR25）。接收机与本地 PTF 提供的外部 10 MHz 和 1 PPS信号同步，并可通过应用标准的电离层和对流层修正自动计算差值$\Delta t_{\text{clock, sat}}$。为简便起见，我们没有校准接收机系统的内部延迟（天线电缆、射频电缆等），但在测量两个 PTF 之间的真实偏移时应进行校准。Septentrio 接收机使用其自带的软件记录GNSS数据（Septentrio Rx-control），其中包括每颗观测卫星的导航电文、在两个频段测得的伪距、信号功率和信噪比，以及多普勒频移 [37]。

每个PTF的PolaRx5接收机持续记录全球导航卫星系统数据，并将其以一种称为Septentrio二进制文件（SBF）的无损格式保存。每天00:00都会创建一个新的SBF文件，数据则持续追加到当前SBF文件中，直至当天结束。为了进行时间传递和同步，使用Septentrio Rx-control软件提供的脚本sbf2cggtts.exe将SBF文件转换为CGGTTS格式。

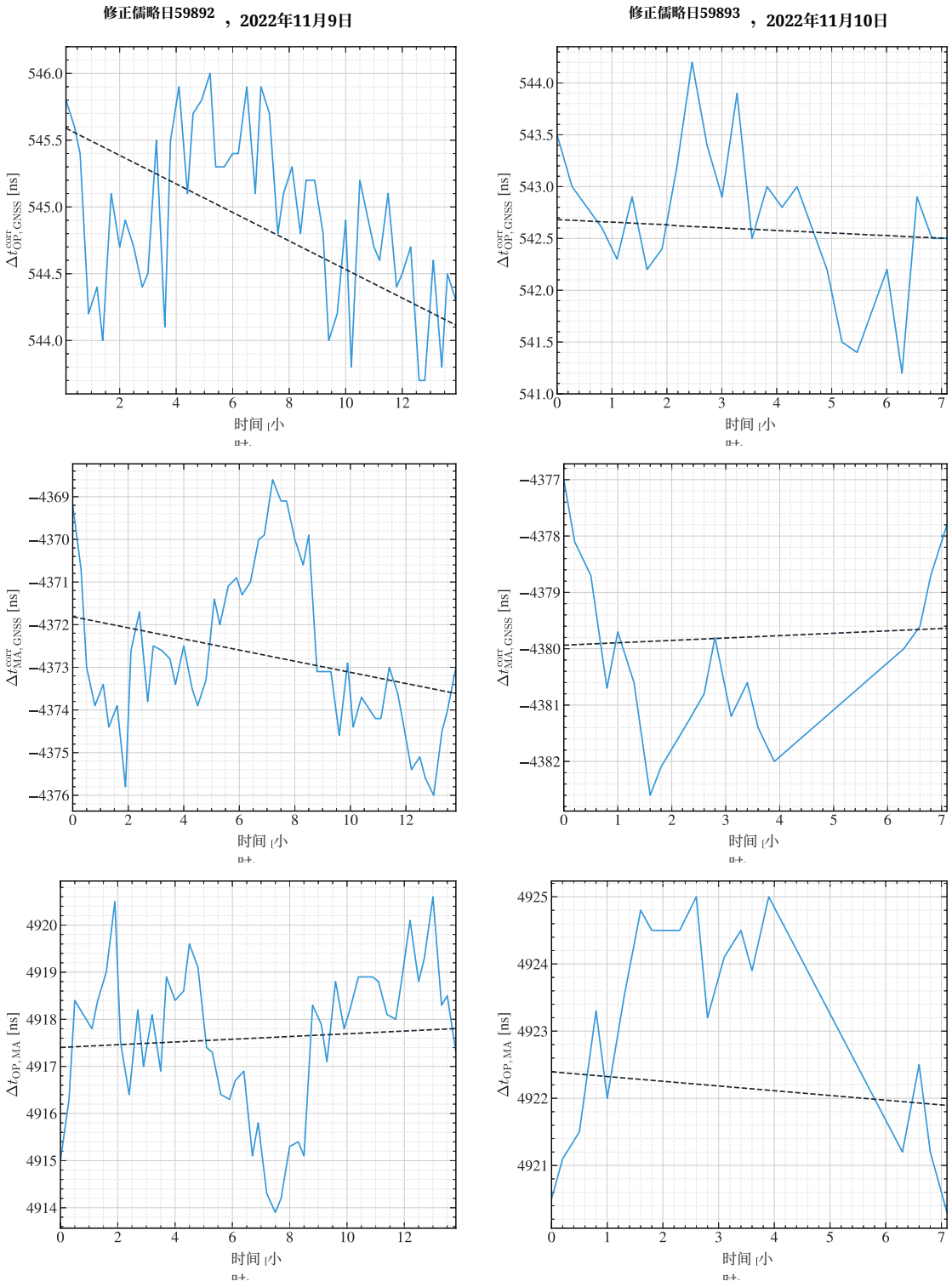


图7：实验实施期间在马耳他和光学平台测得的时间偏差及其差值$\Delta t_{\mathrm{OP,\ MA}}$。测量活动的第一天（修正儒略日59892，2022年11月9日）显示在左列，时间偏差的每日趋势（虚线）为 $t_{\mathrm{OP}} = -2.6$ 纳秒/天、 $t_{\mathrm{MA}} = -3.1$ 纳秒/天和$\Delta t_{\mathrm{OP,\ MA}} = 0.7$ 纳秒/天。测量活动的第二天（修正儒略日59893，2022年11月10日）显示在右列，时间偏差的每日趋势（虚线）为 $t_{\mathrm{OP}} = -0.6$ 纳秒/天、$t_{\mathrm{MA}} = 1.0$ 纳秒/天和$\Delta t_{\mathrm{OP,\ MA}} = -1.7$ 纳秒/天。

B. 通过量子密钥分发（QKD）安全通信传输时钟差数据

在我们的演示中，数据从 MA 单向发送至 OP 并存储在本地，因此可在 OP PTF 计算两个时钟之间的时间偏移；未来的实验也可以实现双向数据传输。由于计算 CG-GTTS 数据至少需要 13 分钟不间断的观测时间，我们决定每隔 30 分钟发送一次数据更新。

自定义数据传输软件打开最新的 SBF文件，并通过调用外部`sbf2cggtts.exe` 例程将其转换为 CGGTTS格式。随后对数据进行初步分析，其中绘制了当前观测日每颗$\Delta t_{\mathrm{clock,\ sat}}$ 卫星的时钟偏差。此外，还计算并绘制了测得的时钟偏差的中位数，如公式（5）所示。

从 MA 实验室收集的数据通过由量子密钥分发保护的 TCP/IP连接发送至光学平台实验室，参见第 IIB 节。文件末尾附有一条尾部消息，其中显示文件发送的时间和日期、通过将所有可见卫星的时钟值相加计算出的校验和，以及文件名。

在 OP 接收端，MA 实验室发送的数据保存在本地，并按照上述方法执行相同的数据分析。随后进行初步的校验和分析，以确保数据传输一致。

接下来，确定一个时间窗口来计算时钟偏差。在该时间窗口内，两个 PTF 都必须有可用的 CGGTTS 数据。情况并非总是如此，例如，某个系统的日志记录可能会停止数小时，或者系统可能需要重启。

最后，通过相减先前计算出的中位数值，计算得出$\Delta t^{\mathrm{meas}}_{\mathrm{OP,\ MA}} \simeq t_{\mathrm{OP}} - t_{\mathrm{MA}}$ 如公式（6）所示。

C. 后处理中时间偏差的差异与时钟同步

在此次测量活动中，我们仅考虑来自欧洲伽利略卫星导航系统星座的全球导航卫星系统卫星，这些卫星由地面站保持与伽利略系统时间（GST）同步。通过将SBF文件转换为CGGTTS格式，可以显示本地PTF与给定伽利略卫星之间的相对时钟偏差。通常，两个实验室同时观测到的伽利略卫星至少有5颗。对于全可见卫星实验而言，一些时钟信号比其他信号能够提供更准确的数据，这取决于特定卫星及其相对于PTF的位置。实际上，不同的卫星时钟可能具有不均匀的性能，而多路径效应等本地失真效应在仰角较低时可能会变得非常显著，从而使得 an

地平线以上的卫星。因此，按照式（5），在每个观测时间对所有可见卫星的数值取中位数，即可获得 PTF 与 GST 之间时钟偏差的稳健估计量。

如图7左栏所示，OP PTF 与 GST 之间的相对漂移约为 -2.6 纳秒/天，而 MA PTF 与 GST 之间的漂移为 -3.1 纳秒/天（在可用测量数量最多的修正儒略日 MJD-59892 测得）。通过计算 PTF 时钟与 GST 之间的相对偏差之差，得到其在 MJD-59892 时约为 4917 纳秒，相对漂移为 0.7 纳秒/天，这与预期一致，是一个很小的值。

测得时钟偏移数据后，可以执行重新校准程序，使本地和远程时钟同步。或者，也可以在本地保存测得的时钟差，并用其追踪时钟随时间的相对漂移。

VI. 结论与展望

在本实验中，我们展示了集成网络的部署，该网络能够传输经量子密钥分发保护的时间差数据。实验需要配置并协调多个子系统的运行，而这些子系统对实验的成功都至关重要。其中包括分别位于 MA 和 OP 端的原子钟，以及用于执行全视野时间偏差测量的全球导航卫星系统接收机；分别部署在 MA 和 OP 的光纤量子密钥分发系统，两者均可实现量子生成密钥的末端安全中继；最后，还包括通过加密且经身份验证的互联网连接实时安全传输时间差数据。在实验活动期间，这些子系统均同时正常运行，最终成功展示了这一应用场景。

我们指出，增加量子密钥分发安全层不会影响光子终端时间同步的质量或及时性：同步程序通常每天或每周执行一次，因为测量本地时钟之间显著的时间偏移需要数小时的积分时间 [14]。要了解这是如何实现的，请注意，时钟偏差测量中对时间要求最严格的部分是通过全球导航卫星系统信号获取完成的，见式（4）。随后，可以通过比较两个远端光子终端的本地时间差数据来确定它们之间的时钟偏差，如式（6）所示。此操作对时间要求并不严格：之后进行数据处理，即可还原任意过去时刻的时钟偏差。

这一应用场景还可以进一步拓展。最重要的是，应当展示真实卫星量子密钥分发系统接入网络，以实现量子生成密钥的长距离中继。这或许很快就能实现，因为未来几年已有多个卫星实验平台计划发射

。 [11]此外，替换由 AES 保护的连接，采用信息论安全加密和认证，以增强经典通信链路的安全性，也可能很有意义。从长远来看，利用量子密钥分发保护时间同步的所有环节（包括全球导航卫星系统部分），将具有重要的科学（及实际）价值。具体而言，采用参考文献 [22] 中展示的方法，可以利用量子密钥分发信号以及精确、真实的卫星测距数据，认证未来 GNSS 星座的时钟信号是否有效。

致谢

我们感谢 e- Geos spa 的 Michele Paradiso 和意大利航天局的 Vincenzo Buompane 在马泰拉激光测距天文台提供的合作与支持。本研究获得以下项目资助：欧盟地平线2020研究与创新计划 OpenQKD 项目（资助协议编号 857156）；意大利航天局 Q-SecGroundSpace 项目（协议编号 2018年-14-HH.0，CUP：E16J16001490001）；欧盟 PON Ricerca e Innovazione 2014-2020年 FESR/FSC——ARS01-00734 QUANCOM 项目。

作者贡献

所有作者均参与了研究构思与设计。研究活动的管理与协调责任由 Davide Orsucci、Francesco Picciariello、Francesco Vedovato、Giuseppe Vallone、Paolo Villoresi、Amita Shrestha 和 Florian Moll 承担。实验实施与数据收集由 Francesco Picciariello、Francesco Vedovato、Davide Orsucci、Marco Avesani、Matteo Padovan、Luca Calderaro、Pablo Nahuel Dominguez 和 Thomas Zechel 完成。数据分析由 Francesco Picciariello、Francesco Vedovato、Matteo Padovan、Giulio Foletto、Pablo Nahuel Dominguez 和 Thomas Zechel 完成。所用软件由 Francesco Picciariello、Francesco Vedovato、Matteo Padovan、Giulio Foletto、Marco Avesani、Luca Calderaro、Pablo Nahuel Dominguez 和 Thomas Zechel 开发。以下作者为实验实施提供了技术设备：Daniele Dequal、Ludwig Bl¨umel、Tobias Schmidt、Luca Calderaro、Marco Avesani、Francesco Vedovato、Giuseppe Vallone 和 Paolo Villoresi。手稿初稿由 Francesco Picciariello、Francesco Vedovato、Davide Orsucci、Matteo Padovan、Pablo Nahuel Dominguez 和 Thomas Zechel 撰写。为促成本出版物所涉项目提供资金支持的工作由 Florian Moll、Johann Furthner、Tobias Schmidt、Giuseppe Vallone 和 Paolo Villoresi 完成。所有作者均阅读并批准了最终手稿。

[1]P. W. Shor，载于 *Proceedings 35th annual symposium on foundations of computer science* 1994 124 （IEEE，），第–134页。[2] R. L. Rivest、A. Shamir和L. Adleman，《美国计算机协会通讯》**21**，120（1978年）。[3] V. S. Miller，载于 *Conference on the theory and application of cryptographic techniques* 1986 417 （施普林格，），第–426页。[4] D. J. Bernstein和T. Lange，《自然》**549**，188（2017年）。[5] C. H. Bennett和G. Brassard，载于 *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing* 1984 （）。[6] F. Xu、X. Ma、Q. Zhang、H.-K. Lo和J.-W. Pan，《现代物理评论》**92**，025002（2020年）。[7] S. Pirandola、U. L. Andersen、L. Banchi、M. Berta、D. Bunandar、R. Colbeck、D. Englund、T. Gehring、C. Lupo、C. Ottaviani等，《先进光学与光子学》**12**，1012 2020（）。[8] *OpenQKD website*，https://openqkd.eu/。[9] S.-K. Liao、W.-Q. Cai、J. Handsteiner、B. Liu、J. Yin、L. Zhang、D. Rauch、M. Fink、J.-G. Ren、W.-Y. Liu等，《物理评论快报》**120**，030501（2018年）。[10] J. Yin、Y.-H. Li、S.-K. Liao、M. Yang、Y. Cao、L. Zhang、J.-G. Ren、W.-Q. Cai、W.-Y. Liu、S.-L. Li等，《自然》582，501（2020）。[11] J. S. Sidhu、S. K. Joshi、M. G¨undo˘gan、T. Brougham、D. Lowndes、L. Mazzarella、M. Krutzik、S. Mohapatra、D. Dequal、G. Vallone等，《IET量子通信》2，182（2021）。[12] L. A 和 T. M（2022），国际标准连续出版物号 1831-9424（在线），URL https://publications.jrc.ec.europa.eu/repository/handle/JRC129425。[13] D. W. Allan 和 M. A. Weiss，载于 *34th Annual Symposium on Frequency Control* 1980 334 346 （IEEE，），第 – 页。[14] P. Defraigne 和 G. Petit，《计量学》40，184（2003）。[15] *Thinkquantum s.r.l*，https://www.thinkquantum.com。[16] *Rhode & Schwarz GmbH & Co*，https://www.rohde-schwarz.com/。[17] J. Daemen 和 V. Rijmen（1998），第1820卷。[18] M. N. Wegman 和 J. L. Carter，《计算机与系统科学杂志》22，265（1981）。[19] S. Ceccato、F. Formaggio、G. Caparra、N. Laurenti 和 S. Tomasin，载于 *2018 IEEE/ION Position Location and Navigation Symposium (PLANS)* 2018 1515 1524 （），第 – 页。[20] *Galileo Open Service Navigation Message Authentication (OSNMA)*，https://www.gsc-

europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma。[21]M. G¨otzelmann, E. K¨oller, I. V. Semper, D. Oskam, E. Gkougkas, J. Simon 和 A. de Latour，载于 *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)* 2021 385 401 （），第 – 页。[22] H. Dai、Q. Shen、C.-Z. Wang、S.-L. Li、W.-Y. Liu、W.-Q. Cai、S.-K. Liao、J.-G. Ren、J. Yin、Y.-A. Chen 等，《自然·物理》16, 848（2020）。[23] M. Avesani、G. Foletto、M. Padovan、L. Calderaro、C. Agnesi、E. Bazzani、F. Berra、T. Bertapelle、F. Piccia-riello、F. B. L. Santagiustina 等，《光波技术学报》40, 1658（2022）。[24] C.-H. F. Fung 和 H.-K. Lo，《物理评论A》74, 042342（2006）。[25] D. Rusca、A. Boaron、F. Gr¨unenfelder、A. Martin 和 H. Zbinden，《应用物理学快报》112, 171104（2018）。[26] M. Avesani、C. Agnesi、A. Stanco、G. Vallone 和 P. Vil-loresi，《光学快报》45, 4706（2020）。[27] A. Stanco、F. B. L. Santagiustina、L. Calderaro、M. Avesani、T. Bertapelle、D. Dequal、G. Vallone 和 P. Villoresi，IEEE量子工程汇刊3, 1（2022）。[28] L. Calderaro、A. Stanco、C. Agnesi、M. Avesani、D. De-qual、P. Villoresi 和 G. Vallone，《物理评论应用》13, 054041（2020）。[29] F. Kneizys、E. Shettle、L. Abreu、J. Chetwynd 和 G. Anderson，*User guide to lowtran 7*（1988）。[30] R. Fante，《IEEE会刊》63（1975）。[31] L. C. Andrews 和 R. L. Phillips，*Laser Beam Propagation through Random Media* 2005 （SPIE，）。[32] J. C. Ricklin 和 F. M. Davidson，《美国光学学会会刊A辑》19（2002）。[33] A. Scriminich、G. Foletto、F. Picciariello、A. Stanco、G. Vallone、P. Villoresi 和 F. Vedovato，《量子科学与技术》7, 045029（2022）。[34] C. B. Lim、A. Montmerle-Bonnefois、C. Petit、J.-F. Sauvage、S. Meimon、P. Perrault、F. Mendez、B. Fleury、J. Montri、J.-M. Conan 等，载于 *2019 IEEE International Conference on Space Optical Systems and Applications (ICSOS)* 2019 （）。[35] *Climate report website*, https://weatherspark.com/。[36] P. Defraigne 和 G. Petit，《计量学》52, G1（2015）。[37] *PolaRx5TR User Manual*, Septentrio NV/SA, URL https://www.septentrio.com/en/products/gnss-receivers/reference-receivers/polarx-5tr。