GPS Solutions (2024) 28:48
https://doi.org/10.1007/s10291-023-01580-9

ORIGINAL ARTICLE

Quantum-secured time transfer between precise timing facilities: a field trial with simulated satellite links

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 Blümel[3] · Johann Furthner[3] · Giuseppe Vallone[1,2] · Paolo Villoresi[1,2] · Tobias D. Schmidt[3] · Florian Moll[3]

Received: 26 April 2023 / Accepted: 10 November 2023

Abstract

Global Navigation Satellite Systems (GNSSs), such as GPS and Galileo, provide precise time and space coordinates globally and constitute part of the critical infrastructure of modern society. To reliably operate GNSS, a highly accurate and stable system time is required, such as the one provided by several independent clocks hosted in Precise Timing Facilities (PTFs) around the world. The relative clock offset between PTFs is periodically measured to have a fallback system to synchronize the GNSS satellite clocks. The security and integrity of the communication between PTFs is of paramount importance: if compromised, it could lead to disruptions to the GNSS service. Therefore, securing the communication between PTFs is a compelling use-case for protection via Quantum Key Distribution (QKD), since this technology provides information-theoretic security. We have performed a field trial demonstration of such a use-case by sharing encrypted time synchronization information between two PTFs, one located in Oberpfaffenhofen (Germany) and one in Matera (Italy)—more than 900 km apart. To bridge this large distance, a satellite-QKD system is required, plus a "last-mile" terrestrial link to connect the optical ground station (OGS) to the actual location of the PTF. In our demonstration, we have deployed two full QKD systems to protect the last-mile connection at both locations and have shown via simulation that upcoming QKD satellites will be able to distribute keys between Oberpfaffenhofen and Matera, exploiting already existing OGSs.

Keywords Quantum key distribution · Time transfer · Optical communication · Quantum network

Introduction

The currently deployed public-key cryptography infrastructure hinges on computational assumptions. These security assumptions are being challenged by the advent of quantum computers, which by implementing Shor's algorithm (Shor 1994), can break the most common public-key encryption schemes, such as RSA (Rivest et al. 1978) and elliptic curve cryptosystems (Miller 1986). Therefore, it is paramount to start transitioning away from the currently employed public-key cryptosystems. Although new cryptographic algorithms are believed to be resilient to quantum computation attacks (Bernstein and Lange 2017), a more radical and long-term solution is to rely on Quantum Key Distribution (QKD). This technology allows secure communication without using computational assumptions but rather harnesses the laws of quantum mechanics to achieve information-theoretic security (Bennett and Brassard 1984; Xu et al. 2020; Pirandola et al. 2020). QKD can fully evade the threat posed by the

✉ Francesco Vedovato
francesco.vedovato@unipd.it

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

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

[3] German Aerospace Center (DLR), Institute for Communications and Navigation, Münchener Straße 20, 82234 Weßling, Germany

[4] Centro di Ateneo di Studi e Attività Spaziali "Giuseppe Colombo", Università degli Studi di Padova, via Venezia 15, 35131 Padua, Italy

[5] ThinkQuantum s.r.l., via Della Tecnica 85, 36030 Sarcedo, Italy

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

Published online: 20 December 2023

upcoming quantum computers and by all other potential algorithmic and hardware advancements.

Because of their crucial importance for modern societies, the critical services that underpin the digital and communication infrastructures shall be among the first systems to be upgraded to post-quantum-computation security standards through QKD. The European Union is pushing in this direction by developing and testing experimental quantum communication networks in several European countries through initiatives such as OpenQKD (https://openqkd.eu/) and Petrus (https://petrus-euroqci.eu/), which is coordinating the deployment of the European Quantum Communication Infrastructure (EuroQCI).

In this work, realized within the OpenQKD project, we demonstrate the possibility of securely transmitting clock difference data needed for synchronization of clocks of two distant Precise Timing Facilities (PTFs). One is located at the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt, DLR) in Oberpfaffenhofen (OP), Germany; the second is located at the Matera Laser Ranging Observatory (MLRO) of the Italian Space Agency in Matera (MA), Italy. This is a highly impactful use-case since attacks performed on the clock synchronization data between PTFs could lead to large-scale service disruptions. In fact, an attacker who can manipulate or forge synchronization data has the possibility to introduce small temporal shifts in the clocks that employ such data for synchronization; these shifts may result in a slow drift of the global system time, which is generated by one of the PTF in duty. Global Navigation Satellite Systems (GNSSs), for instance, require a very precise system time to operate correctly, and an attack to the underlying PTF could result in a worldwide disruption of the service.

In our QKD demonstration, we have secured the transmission of synchronization data between two PTFs that are located more than 900 km apart (but which are not actually part of the Galileo ground segment). This distance is too large to perform a QKD exchange via a direct optical fiber connection, due to the exponential loss of optical power (Pirandola et al. 2020). A method that could allow bridging such a long distance with currently existing and demonstrated technology would be to employ a satellite to create a QKD link between the two facilities. This may be done either by using a satellite as a trusted node to relay a quantum-generated key (Liao et al. 2018) or, more ambitiously, by employing a satellite that can generate and distribute entangled photon pairs simultaneously (Yin et al. 2020) to the two PTFs. Both the PTF in MA and the one in OP have an Optical Ground Station (OGS) located nearby that can receive optical quantum states from a satellite in Low Earth Orbit (LEO) and will be employed, in the future, for satellite-to-ground QKD implementations. The European Union is developing technologies for satellite-based QKD, for example, through the construction of the Eagle-1 demonstrator satellite (Sidhu et al. 2021) and the activities of the Security And cryptoGrAphic Mission (SAGA) (Lewis and Travagnin 2022); a comprehensive review on QKD satellite projects can be found in the work by Sidhu et al. (2021). The last required step is the secure forwarding of the quantum-generated key from the OGS to the PTF at each location. This "last-mile" connection is short enough that it can be secured with a QKD link over an optical fiber, as we experimentally demonstrated in our implementation. The general overview of how to secure communication between the two PTFs with a QKD satellite and two last-mile connections is presented schematically in Fig. 1.

Use-case demonstration description and experiment setup

In this section, we give a high-level description of the use-case demonstration, as schematically presented in Fig. 1. The demonstration involved the coordinated and simultaneous operation of three experimental parts: (i) a time offset measurement between the PTF clocks in OP and in MA, made possible by all-in-view detection of GNSS signals from the Galileo constellation; (ii) a fiber-based QKD link in MA and a second QKD link in OP; (iii) the real-time, encrypted, and authenticated transmission of time difference data from MA to OP.

Since no European satellite capable of quantum state downlink is currently available, part of the demonstration that would require the use of a satellite has not been performed experimentally. In the following we show, however, that it is feasible to establish a QKD link with the currently existing OGS, making reasonable assumptions on the performance of the satellite quantum communication system.

Time offset measurement

The time difference $\Delta t_{OP,MA}$ between the clock in OP and the clock in MA is measured according to the common-view technique, performed by measuring the time difference between the local clocks and the clock of a GNSS satellite which is in line of sight from both PTFs, as described in the works by Allan and Weiss (1980) and Defraigne and Petit (2003) and detailed in the Supplementary Information. In our demonstration, clock data from 16 Galileo satellites has been collected over two days.

Securing the last-mile connections with QKD

QKD allows generating a common secure key between distant parties, usually denoted as Alice and Bob, and requires a quantum channel and a classical authenticated channel.

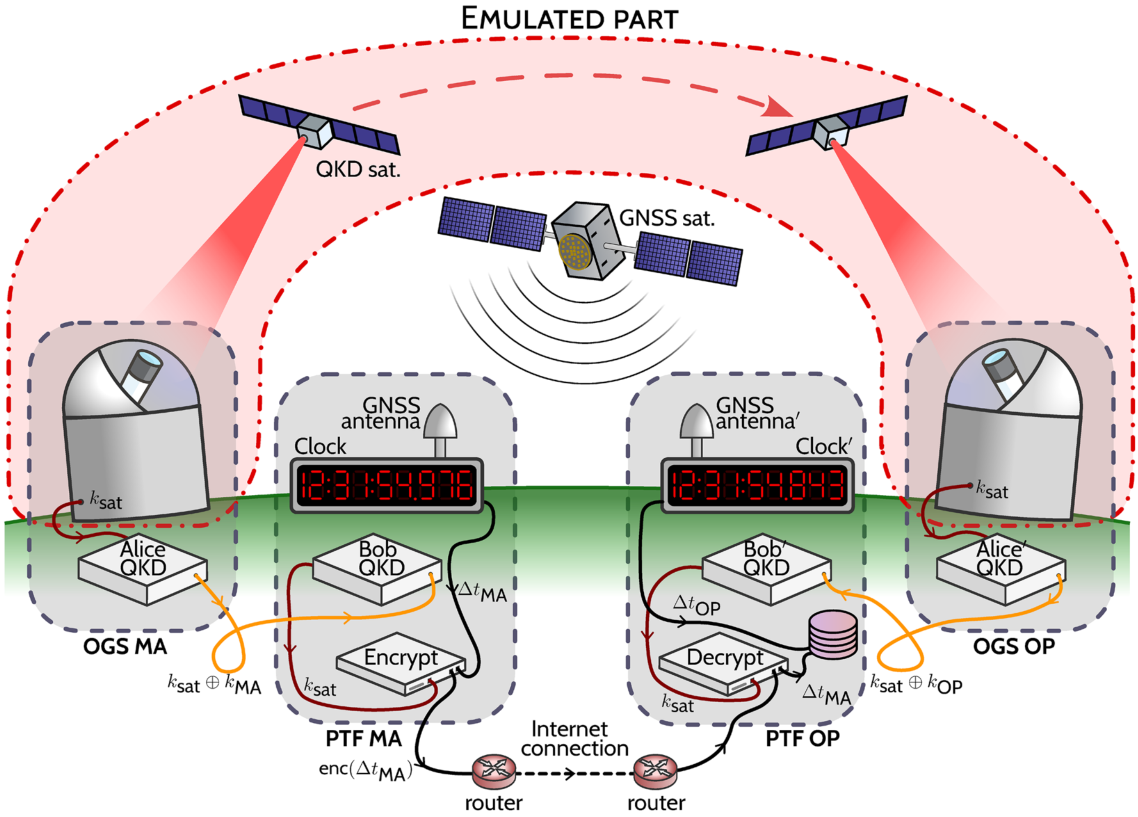


Fig. 1 Representation of the quantum encrypted time-transfer use-case demonstration. Matera (MA) laboratories are on the left and Oberpfaffenhofen (OP) laboratories are on the right. The gray dashed lines enclose the equipment considered to be within secure perimeters (physically inaccessible to attackers). The red dashed-dotted line encloses the equipment that has been emulated and not yet experimentally demonstrated due to the unavailability of QKD satellites. Description: a QKD satellite distributes the key k_{sat} to both the OGSs in MA and OP; the two last-mile QKD connections generate quantum keys k_{MA} and k_{OP} which are then used to one-time pad the key k_{sat} and securely forward it to the PTF in MA and OP (transmitting the encryptions $k_{sat} \oplus k_{MA}$ and $k_{sat} \oplus k_{OP}$, respectively); the time differences Δt_{OP} and Δt_{MA} between the local clocks and a GNSS satellite are measured in an all-in-view experiment; the Δt_{MA} value is AES-encrypted with key k_{sat} and is transmitted to OP over the internet, where it is AES-decrypted using the same key k_{sat}; the values Δt_{OP} and Δt_{MA} are saved and stored locally in OP, where are used to monitor the clock difference $\Delta t_{OP,MA}$= Δt_{OP}—Δt_{MA}

The QKD protocol can be divided in two subsequent phases: (i) the quantum transmission phase, in which photons are exchanged between Alice and Bob through the quantum channel, and (ii) the classical post-processing involving information reconciliation and privacy amplification (Xu et al. 2020; Pirandola et al. 2020).

In our demonstration, we implemented a fiber-based last-mile QKD connection in both MA and OP to securely forward the satellite key k_{sat} shared by the two OGSs (which are trusted nodes) to the two PTFs. The QKD system used in OP to locally generate the key k_{OP} was a commercial product provided by ThinkQuantum s.r.l. (https://www.thinkquantum.com/), while the one used in MA to generate k_{MA} was a research prototype developed by the University of Padova.

As analyzed in the following, the distribution of a key k_{sat} to the OGS in MA and OP is feasible with satellite QKD technology that will be available in the near future. For the current demonstration, a random bit string k_{sat} had been uploaded into both Alice modules just prior to their shipment to MA and OP, respectively. We note that when a real satellite QKD system is employed, the end-to-end QKD link is established in a similarly asynchronous manner. In fact, the latency in the distribution of quantum keys via satellite can be several days depending on the number of QKD satellites available and the local weather conditions. Therefore, the key k_{sat} must be created well in advance of its intended use and buffered locally for the necessary time.

Data encryption, authentication and real-time data transfer

The final part of the use-case demonstration is to secure the communication of the time offset measurements between MA and OP. To secure the communication of the time offset measurements, we exploited at each PTF one SITLine ETH4G/40G commercial encryptor made by

Rhode & Schwarz GmbH & Co (https://www.rohde-schwarz.com/). Both the SITLines and the QKD systems provide a standard interface, the ETSI GS QKD 004, which enables the communication between the two types of devices to use the quantum secret key. This type of interfaces is fairly new in the QKD field and shows the systems' readiness for more advanced QKD networks.

As sketched in Fig. 1, every two minutes, the two encryptors ask the Bob QKD devices for a secret key. The SITLine works at the data-link layer (L2 of the ISO/OSI model), and to send the encrypted packets from MA to OP through the Internet we had to implement an encapsulation of the data into the network layer (L3 of the ISO/OSI model) with the two routers depicted in the scheme. The key is 256 bits long, thus allowing the encryptors to implement the AES-256 encryption protocol (Daemen and Rijmen 2000). Since the encryptors implement AES by default and we did not have restrictions on the key production, we chose to encrypt all the data transferred during the experiment. Note that by using a Wegman-Carter scheme, it could be possible to authenticate the data with information-theoretic security using a number of secret bits that scale only logarithmically in the message length (Wegman and Carter 1981).

Once the classical channel between the two routers is enabled, the data acquired from the antenna in MA is automatically sent to the encryptor every 30 min, decrypted in OP and stored in a computer for analysis. Our encryption scheme ensures the security of the data from the GNSS antennas to the other end of the routers. However, spoofing of the GNSS signals is a current issue for many satellite positioning systems (Ceccato et al. 2018), and these types of attack could poison the data at the source. As of now, this is avoided by using the Galileo satellite network, which uses Open Service Navigation Message Authentication (OSNMA), which provides stronger authentication methods than other systems, such as GPS (Götzelmann et al. 2023); furthermore, integrity and consistency checks are performed in the GNSS data, alongside the use of multi-array antennas to reduce spoofing and jamming. In the future, QKD satellites could be integrated into the network to also authenticate this part of the signal (Dai et al. 2020).

Last-mile QKD links

In this section, we show in detail how the two last-mile QKD links have been implemented at the two locations, and the performance—in terms of quantum bit error rate (QBER), which is the mismatch of the signals sent by Alice and received by Bob, and secret key rate (SKR)—achieved in our demonstration.

Matera infrastructure

The QKD system based in MA was similar to the one described in Avesani et al. (2022), which implements the 3-state efficient BB84 protocol (Fung and Lo 2006) with polarization modulation and 1-decoy technique (Rusca et al. 2018). Alice is mainly composed of a laser at 1310 nm, emitting pulses with a repetition rate of 50 MHz, an intensity modulator, which allows setting the mean photon number needed for the decoys, and a polarization modulator based on the iPOGNAC scheme (Avesani et al. 2020). Denoting the horizontal and vertical polarization states with $|H\rangle$ and $|V\rangle$, respectively, this scheme allows for the preparation of the left and right circular polarization states denoted by $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$, which form the key basis $Z = \{|L\rangle, |R\rangle\}$, and of the diagonal state $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, which is part of the check basis $X = \{|D\rangle, |A\rangle\}$ with $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$. It is worth noting that this is the first time the iPOGNAC scheme is used with a QKD signal in the O-band. Finally, the pulses are attenuated below the single-photon level with a variable optical attenuator before entering the fiber channel. The two intensities used for the 1-decoy technique are $\mu_1 = 0.6$ and $\mu_2 = 0.17$. The electronics are mainly composed of a System-on-a-Chip (SOC) with an FPGA and a CPU (Stanco et al. 2022).

After generation, the attenuated laser pulses enter the quantum channel traveling toward Bob. The quantum channel is a 10-km long single-mode telecom fiber with 8.5 dB of total losses. Bob decodes the states through a time-multiplexing scheme: although this scheme introduces an extra 3 dB of losses, it allows to improve compactness and significantly reduces the cost of the system. Indeed, the implemented system only requires one InGaAs/InP single-photon avalanche diode (SPAD), which in this case is a PDM-IR from Micro Photon Devices s.r.l., which provides 15% quantum efficiency. The time tags corresponding to the photons arrivals are recorded by a quTAU, from qutools GmbH, time-to-digital converter and transmitted to a computer for data processing. To further reduce architecture requirements, the QKD system exploits the Qubit4Sync algorithm (Calderaro et al. 2020) for the time synchronization between Alice and Bob, avoiding the need for a dedicated system that distributes the clock reference.

In MA, the authenticated classical channel between the OGS and the PTF was established using a standard internet connection, the total key generation time during the demonstration lasted 18 h and the system generated 119 Mb of secure key in that period. The performance of the QKD system used in MA is shown in the left panels of Fig. 2.

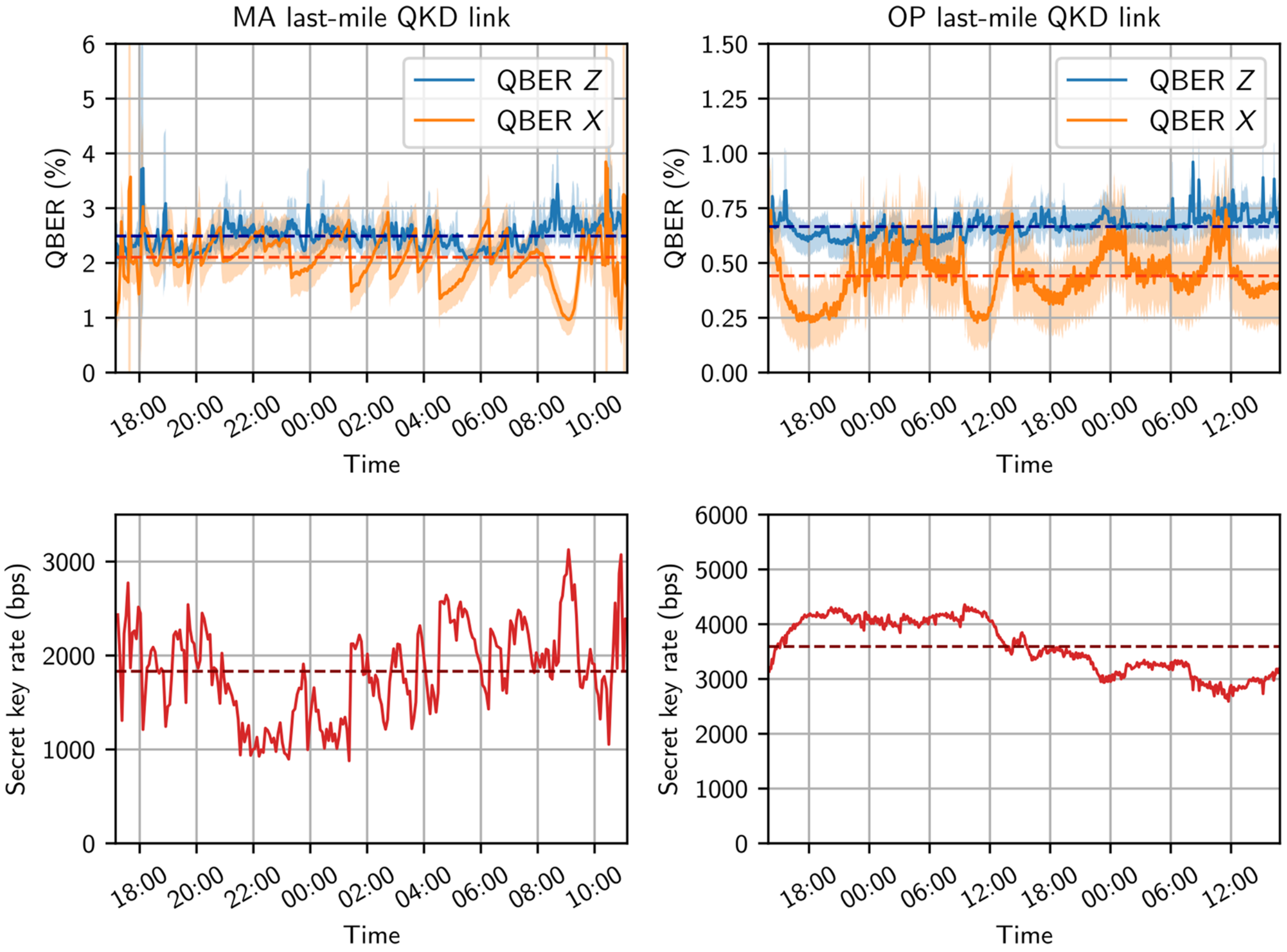


Fig. 2 Summary of the performances of the two QKD systems in terms of QBER and SKR. The QBER is plotted with a rolling window of 5 min and the color bands represent ± 1 standard deviations. Dashed lines are the average values. For Matera, they are 2.5%, 2.1% and 1.9 kbps for the QBER in Z basis, QBER in X basis, and SKR, respectively. For Oberpfaffenhofen, they are 0.7%, 0.4% and 3.6 kbps for the QBER in Z basis, QBER in X basis, and SKR, respectively

Oberpfaffenhofen infrastructure

For the specifications of the QKD system placed in OP, please refer to the QUKY platform developed by ThinkQuantum s.r.l. As the system used in MA, the QUKY platform implements the 3-state 1-decoy efficient BB84 protocol via polarization encoding and the synchronization technique named Qubit4Sync.

In the OP implementation, the quantum channel was a 500-m long single-mode fiber to which extra losses were added for a total amount of 12 dB and the authenticated classical channel was established via another fiber channel by exploiting two Small Form-factor Pluggable (SFP) bidirectional transceivers. The total working time was 51 h and the system generated 660 Mb of secure key. The performance of the QKD system used in OP is shown in the right panels of Fig. 2. A picture part of the setup OP is shown in Fig. 3.

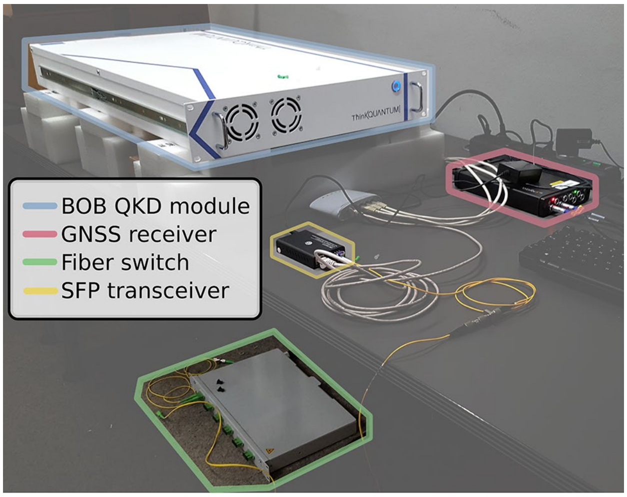


Fig. 3 Photo of the experimental setup in OP

Satellite channel simulation

To evaluate the pre-sharing of keys between the OGSs in MA and OP, we simulated a QKD protocol between a satellite transmitter and two receivers placed in our two ground stations. The purpose of the simulation is to estimate the average available SKR that can be one-time-padded with the last-mile QKD key to propagate the pre-shared key to the end-nodes PTF-MA and PTF-OP. The two locations are already equipped with two telescopes with apertures 1.5 m (MA) and 0.8 m (OP). We assume that there are two QKD receivers for a 1550-nm source that require a fiber-injection system to collect the signal from the telescopes up to the detectors. The simulation goes as follows: first we propagate a satellite on a given orbit that allows it to pass over both the ground stations, then we compute for each pass the channel statistics to estimate the losses and the raw key accumulation on the ground stations, and finally we compute the SKR generation following standard finite-key security proofs (Rusca et al. 2018).

Orbit propagation

We simulate a Low Earth Orbit (LEO) satellite at an altitude of 500 km. The orbit has an inclination of 75.6 degrees and a Right Ascension of the Ascending Node (RAAN) of 300.6 degrees, passing over the two ground stations twice a day, and is equipped with a transmitter telescope having a diameter of 15 cm, and a QKD system with a source at 1550 nm. The satellite is propagated over a period of time, where the orbit is granularized over steps of 1 s each. For each step, if a ground station is available to enable the optical quantum channel, a channel model analysis, see below, is made to compute the detection statistic. In Fig. 4, an example of the simulated orbit is shown.

The average useful pass time per day for the two stations is 9.04 min for MA and 10.20 min for OP, with usually two passes per day. Note that, thanks to the wavelength choice, for which the atmosphere presents fewer losses and lower background noise, it is possible to generate a secure key even with the detections accumulated during daylight passes.

Channel model for the satellite links

We compute the channel efficiency from the satellite to the ground station for each point of the orbit, starting from the physical parameters of the transmitter, the receiver, and the channel. We consider only the average values at each point of the granularized orbit to calculate the channel efficiency.

The channel efficiency η is calculated as

$$\eta = \eta_A \eta_g \eta_f \eta_0 \tag{1}$$

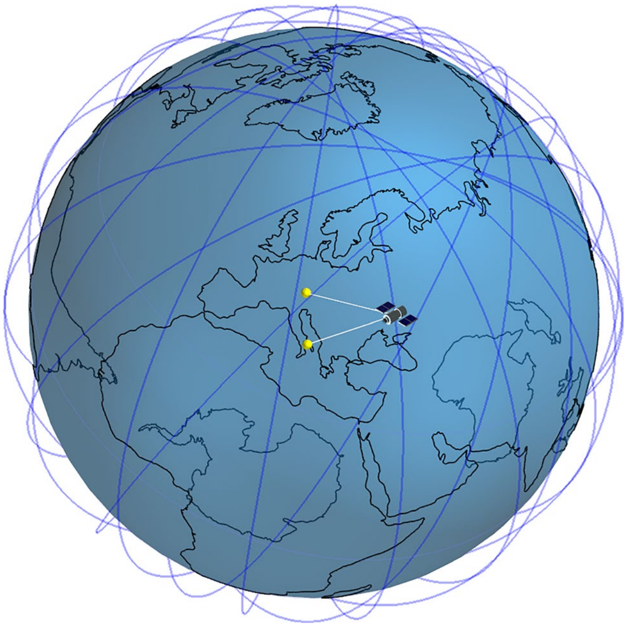


Fig. 4 Propagation of the satellite orbit for one day of the experiment duration. The two dots represent the two ground stations placed in MA, Italy, and OP, Germany. The blue line is the orbit through which the satellite has been propagated. The white segments indicate that optical communication between the satellite and ground stations is available

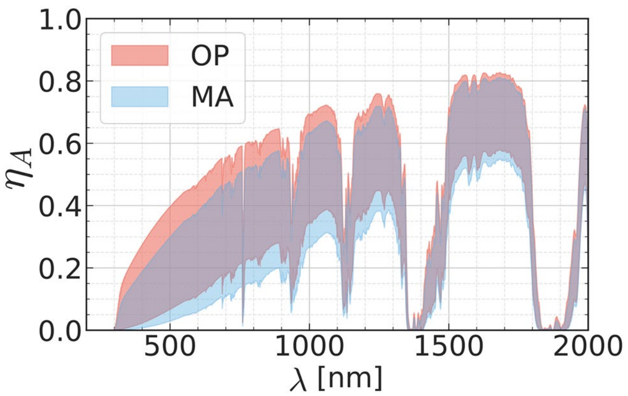


Fig. 5 Atmospheric transmission from satellite to ground for the two sites in MA and OP, from zenith (higher transmission) to 20 degrees of elevation (lower transmission). The data was computed with Lowtran considering a mid-latitude winter atmosphere

where η_A is the atmospheric transmittance, caused by atmospheric scattering and absorption, retrieved from Lowtran (Kneizys et al. 1988) (see Fig. 5), η_g is the geometric transmittance, caused by the finite size of the receiver telescope that clips the incoming beam, η_f is the angular transmittance, caused by the finite angular acceptance of the receiving system and the pointing error, and η_0 takes into account all the fixed additional losses of the systems.

To compute η_g, we first propagate the optical beam from the transmitter aperture to the ground. The beam radius at the receiver w_g depends on the diffraction-limited divergence of the Gaussian beam θ_d, and on the divergence caused by the atmospheric turbulence θ_t, which perturbs the beam wavefront. We assume that the angular pointing error of the transmitter is negligible. Therefore, the total divergence θ is calculated as

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

where λ is the QKD signal wavelength, w_0 is the Gaussian beam radius at the transmitter, and ρ_0 is the atmospheric coherence length of the spherical wave (Fante 1975). From the refractive-index structure constant C_n^2 one can compute ρ_0 for a satellite-to-ground path as

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

where $k = 2\pi/\lambda$ is the wavenumber of the photons, R is the slant range to the ground station, the integral over ξ considers the propagation of the beam through the path and $C_n^2(\xi R)$ retrieves the C_n^2 associated to the height of the point ξR. We employ the Hufnagel-Valley model for C_n^2, which has two free parameters: the value of C_n^2 at ground level and the average wind speed (Andrews and Phillips 2005).

The beam radius at the ground, exploiting paraxial approximation, is given by (Ricklin and Davidson 2002)

$$w_g = \sqrt{w_0^2 + (\theta R)^2} \tag{4}$$

Next, η_g is calculated as the integral of a Gaussian beam over a circular aperture with an inner circular obscuration (as typical for Cassegrain configuration, where the secondary mirror partially occludes the primary mirror). This results in Scriminich et al. (2022)

$$\eta_g = \exp\left(-\frac{D_{Rx,occ}^2}{2w_g^2}\right) - \exp\left(-\frac{D_{Rx}^2}{2w_g^2}\right) \tag{5}$$

where D_{Rx} is the diameter of the primary mirror of the receiver telescope and $D_{Rx,occ}$ is the diameter of the (partially occluding) secondary mirror. Note that, in the limit $D_{Rx} \ll w_g$, the geometric transmittance is approximately proportional to the telescope area, such that

$$\eta_g \approx (D_{Rx}^2 - D_{Rx,occ}^2)/2w_g^2 \tag{6}$$

The angular transmittance η_f is computed as the superposition of the field of view of the receiver telescope and the angular pointing error of the system:

$$\eta_f = 1 - \exp\left(-\frac{\theta_{Rx}^2}{2\alpha_{Rx}^2}\right) \tag{7}$$

where θ_{Rx} is the intrinsic receiver half-field of view, and α_{Rx} is the pointing error of the telescope.

In η_0, we consider additional losses such as the losses due to the optical components at the receiver after the telescope (e.g., lenses, mirrors, dichroic mirrors, filters and isolators), estimated to be around 3–5 dB, and the losses due to the fiber injection of the signal, estimated to be around 8–10 dB for high-end adaptive optics systems (Scriminich et al. 2022; Lim et al. 2019). Without the availability of measurements from different devices, we have decided to fix η_0 to 13 dB.

Secret key analysis for the satellite links

We simulate the efficient BB84 protocol with one decoy state, following the security proof presented by Rusca et al. (2018). The security proof takes into account finite key effects, requiring to realize a previously chosen number of measurements before being able to get a secure key as an output of the protocol.

After the computation of the channel efficiency, thus knowing the probability of receiving a photon from the satellite, we start the accumulation of photon counts on the receiver side. For each point of the orbit, we can calculate the number of photons received at the detector during its associated time. The so-called raw key is obtained by all the measurements in which Alice and Bob bases match, and after reaching the required key length for the finite-key analysis, we compute the secret key rate. We accumulate the raw key produced in different passes: this is a design choice that has the advantage of having a higher secure key generation rate since, for longer keys, the finite key overheads are less prominent; on the other hand, it requires larger memory at the satellite's side and additional memory management for security reasons. Due to our choice of using systems at a wavelength of 1550 nm, and because we must couple the signal into a SMF to reduce the background noise, we can exploit high-end detectors to perform the measurement. The superconducting nanowire single-photon detectors (SNSPDs) can reach an efficiency η_{det} higher than 90% with an ultra-low noise of fewer than 100 counts per second, and thus are the best choice for this type of application.

We have to consider the presence of errors during the protocol that will eventually lead to a mismatch between the secret keys shared by the two parties. The main sources of errors are random events that get registered by the detectors, coming from the background light of the channel and the detector itself (in the form of dark counts) and the incorrect encoding and decoding of the quantum state due to nonidealities of the quantum devices. While the other parameters are inputs of the simulation, the background light can be defined as the diffuse atmospheric radiance exploiting LOWTRAN. Other effects that impact the detection, for example, the direct light coming from the sun's reflection on the satellite, are not considered. In Table 1, the most relevant parameters used in the simulations are shown.

Simulation results for the satellite links

The total secret key generated over a full year in the two OGS is 5.42 Gb for MA and 1.71 Gb for OP, that is equal to an average SKR of 171.7 bps and 54.1 bps, respectively. Since the encryption protocol implemented by the two encryption systems needs 256 bpm, the requirement is satisfied. The satellites generated an average of 1.55 Mbps of raw key per pass, depending on the zenith angle.

If we consider the probability of having overcast days that, in the worst condition, do not allow optical communication, we are still above the threshold. From the climate report website available at https://weatherspark.com/ we see that the overcast probability is 34.2% for MA and 55.3% for OP. The average SKRs become 113.01 bps and 24.17 bps instead.

Table 1 Relevant input parameters for the satellite QKD simulations

Quantity	Value
λ	1550 nm
η_{det}	0.9 ($\approx$ 0.5 dB)
w_0	0.15 m
η_0	13 dB
D_{Rx}^{MA}	1.5 m
$D_{Rx,occ}^{MA}$	0.1 m
D_{Rx}^{OP}	0.8 m
$D_{Rx,occ}^{OP}$	0.3 m
θ_{Rx}	6.25 µrad
α_{Rx}	100 µrad
C_n^2 at ground level	$10^{-14}\ m^{-2/3}$
Wind speed	21 m/s
Satellite altitude	500 km
Satellite inclination	75.6°
Satellite RAAN	300.6°
Satellite argument perigee	84.38°
Satellite mean anomaly	38.29°
Source repetition rate	500 MHz
Coding error	0.5%
Dark count rate	100 Hz
Detector dead time	10 ns
Temporal jitter	10 ps
Finite key length	100 Mb
Secrecy parameter	10^{-10}
Correctness parameter	10^{-15}

GNSS and clock data acquisition and analysis

The time offset between the clock in OP and the clock in MA is measured using the all-in-view method, as presented in the Supplementary Information. The propagation time of the satellite signal to the PTF, $\tau_{\text{sat,PTF}}$, must be estimated and then subtracted to perform a consistent comparison between the satellite clock and the PTF. Its estimation $\widetilde{\tau}_{\text{sat,PTF}}$ is obtained by adding together all the known contributions, including dynamic and static effects:

$$\widetilde{\tau}_{\text{sat,PTF}} = \widetilde{\tau}_{\text{dynamic}} + \widetilde{\tau}_{\text{static}} \tag{8}$$

The dynamically changing propagation time can be obtained as

$$\tilde{\tau}_{\text{dynamic}} = \frac{\chi}{c} + \Delta t_{\text{rel}} - \Delta t_{\text{tropo}} - GD \tag{9}$$

with

$$\chi = P_{IF} - \left|\left|\overrightarrow{x_{sat}} - \overrightarrow{x_{rec,IF}}\right|\right| - S \tag{10}$$

where P_{IF} is the ionosphere-free pseudorange between satellite and receiver, $\overrightarrow{x}_{\text{sat}}$ is the position of the satellite in the International Terrestrial Reference Frame (ITRF) at the emission time, $\overrightarrow{x}_{\text{rec,IF}}$ the ionosphere-free phase center of the receiver antenna in ITRF, S is the Sagnac correction associated with earth's rotation, Δt_{rel} are relativistic corrections, Δt_{tropo} the delay originated from the troposphere and GD the group delay of the emitted signal by the satellite. More details can be found in the work by Defraigne and Petit (2003). This quantity is usually computed for every satellite available during the measurement time and is displayed in the Common GPS GLONASS Time Transfer Standard (CGGTTS) (Defraigne and Petit 2015). The analysis requires a 13-min data collection without losing contact with the satellite.

The static correction term is due to propagation delay in the PTF measurement system. These include the delays from the antenna, RF-cables, and within the GNSS receiver,

$$\widetilde{\tau}_{\text{static}} = \frac{1}{c}(x_s + x_c + x_R - x_O - x_p) \tag{11}$$

where the delay terms are explained in Fig. 6.

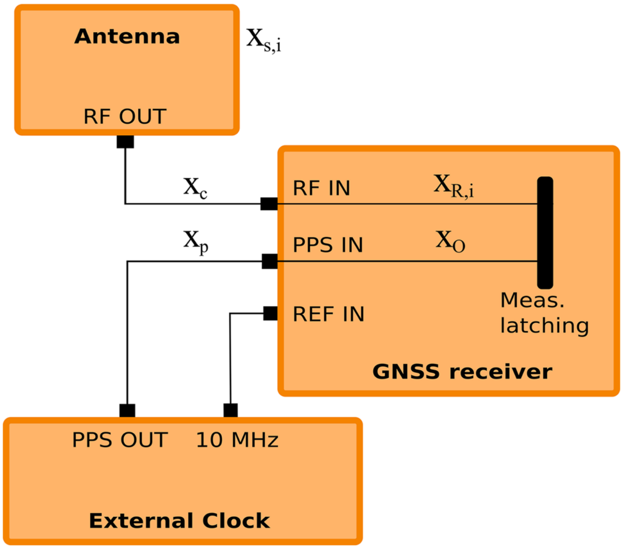


Fig. 6 Schematic layout of the measurement delays of the system. $x_{s,i}$: delay in the antenna for signal$i$; $x_{R,i}$: delay in RF section of receiver for signal$i$;x_c: delay in the RF cable (including amplifier and splitter); x_p: delay in the PPS cable;x_O: delay between PPS IN and internal receiver time reference

GNSS data acquisition

We have performed time-offset measurements between the OP PTF and the MA PTF. Both PTFs used a commercially available PolaRx5 receiver by Septentrio N.V. (https://www.septentrio.com/en), connected to a choke ring multiband GNSS-antenna (Novatel GNSS-750, Leica AR25). The receiver is synchronized to an external 10 MHz and 1 PPS signals from the local PTF and can automatically compute the difference between the local clock and the GNSS' one $\Delta t_{\text{clock,sat}}$ by applying standard ionospheric and tropospheric corrections. For simplicity, we did not calibrate the internal delays of the receiver system (antenna cables, RF-cables, etc.). The Septentrio receiver uses its own software to log the GNSS data (Septentrio Rx-control), including the navigation message for each observed satellite, the pseudoranges measured at both frequency bands, its power and signal-to-noise ratio and the Doppler shift.

Transfer of clock difference data via QKD-secured communication

In our demonstration, the data is sent unidirectionally from MA to OP and stored locally, so that the time offset between the two clocks can be computed at the OP PTF. Since the computation of the CGGTTS data requires at least 13 min of uninterrupted observation time, we decided to send a new update of the data once every 30 min.

The data collected from the MA laboratory are sent through the TCP/IP connection secured via QKD to the OP lab and a time window is determined to calculate the clock offsets. It is necessary that the CGGTTS data are available on both PTFs during the time window. This may not always be the case, for example, if one of the systems logging is stopped for a few hours or if it is necessary to reboot the system. Finally, the time difference between OP and MA measures is calculated as

$$\Delta t^{\text{meas}}_{OP,MA} \simeq t_{OP} - t_{MA} \tag{12}$$

where the procedures to evaluate the two local clocks t_{OP} and t_{MA} , as well as the time difference retrieval, are described in the Supplementary Information.

Difference in time offsets and clock synchronization in post-processing

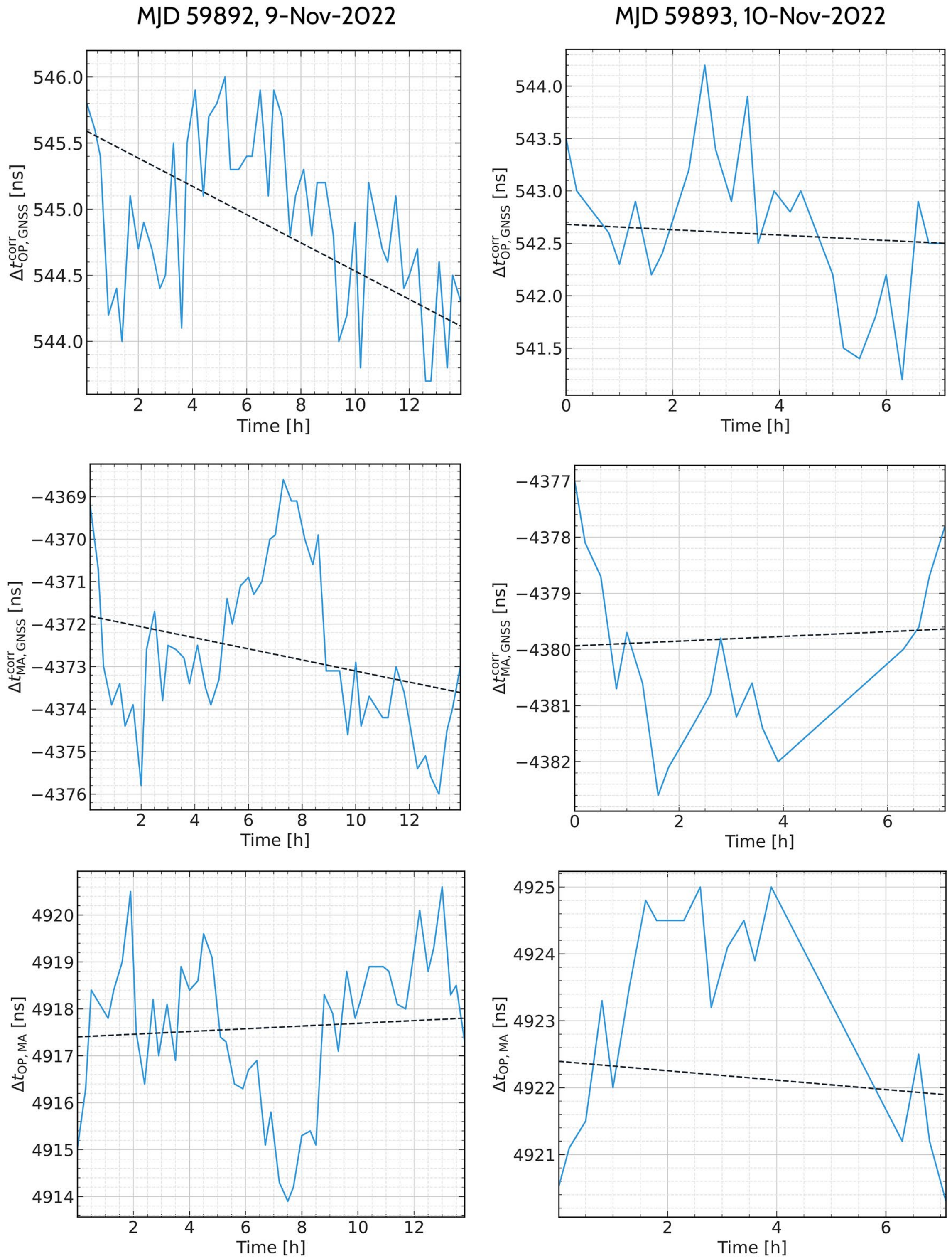
For this measurement campaign, we considered only the GNSS satellites from the European Galileo constellation, which are kept synchronized to the Galileo System Time (GST) by the ground station. From the CGGTTS files, it is possible to display the relative clock offset between the local PTF and a given Galileo satellite. Typically, there are at least 5 Galileo satellites that are observed at both laboratories at the same time.

As shown in the left column of Fig. 7, the relative drift between the OP PTF and the GST is about −2.6 ns/day, while the drift between MA PTF and GST is −3.1 ns/day (measured on MJD-59892 in which we have the largest number of measurements available). By computing the difference between the relative offset between the PTF clocks and the GST this is about 4917 ns on MJD-59892 with a relative drift of 0.7 ns/day which is, as expected, a very low value.

Once the clock offset data have been measured, a re-calibration procedure could be performed to synchronize the local and remote clock. In alternative, the measured clock difference can be saved locally and used to track the relative clock drift over time.

Conclusions and outlook

In this experiment, we have demonstrated the deployment of an integrated network allowing the transfer of time difference data secured by QKD. The experiment required the configuration and coordination of the operation of several subsystems, all of which were critical to the success of the experiment. These included atomic clocks both in MA and OP side, together with GNSS receivers, in order to perform an all-in-view time offset measurement; a fiber-based QKD system in MA and one in OP, each allowing the last-mile


MJD 59892, 9-Nov-2022

MJD 59893, 10-Nov-2022

Fig. 7 Time offsets measured during the experiment realization at MA and OP, and their difference $\Delta t_{OP,MA}$. The first day of the measurement campaign (MJD 59892, 9-Nov-2022) is shown in the left column, with daily trend of the time offsets (dashed lines) $t_{OP} = -2.6$ ns/day, $t_{MA}= -3.1$ ns/day, and $\Delta t_{OP,MA} = 0.7$ ns/day. The second day of the measurement campaign (MJD 59893, 10-Nov-2022) is shown in the right column, with daily trend of the time offsets (dashed lines) $t_{OP} = -0.6$ ns/day, $t_{MA} = 1.0$ ns/day, and $\Delta t_{OP,MA} = -1.7$ ns/day

secure relaying of a quantum generated key, and finally the real-time secure transmission of the time difference data over an encrypted and authenticated internet connection. Besides the satellite QKD links that have been only simulated due to the unavailability of the satellites, all the other critical subsystems were all simultaneously functional during the experimental campaign, successfully demonstrating the use-case.

We remark that the addition of a QKD security layer does not hinder the quality or timeliness of the time synchronization of the PTFs: the synchronization routines are typically performed only on a daily or weekly basis, since several hours of integration time are needed to measure a significant time offset between the local clocks (Defraigne and Petit 2003). The clock offset between the two remote PTFs can then be determined by comparing the local time-difference data. This operation is not time-critical: data processing can be performed later to recover what was the clock offset at any given previous time. Further developments of this use-case can be envisioned. Most prominently, it would be of uttermost importance to demonstrate the integration of real satellite QKD systems in the network for the long-haul relaying of the quantum generated keys. This may be done relatively soon, since several satellite experimental platforms are scheduled for launch in the upcoming years (Sidhu et al. 2021).

Furthermore, it could be of interest to strengthen the security of the classical communication link, by replacing the AES-secured connection with information-theoretic secure encryption and authentication. On a longer-term perspective, it would be of high scientific (and practical) interest to be able to use QKD to secure all the steps in time synchronization, including the GNSS segment. Using the methods demonstrated in the work by Dai et al. (2020) one could use QKD signals, together with precise and authentic satellite ranging data, to authenticate the validity of clock signals of future GNSS constellations.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10291-023-01580-9.

Acknowledgements We would like to thank Michele Paradiso of e-Geos s.p.a., Catia Benedetto and Vincenzo Buompane of the Italian Space Agency for the collaboration and support at the Matera Laser Ranging Observatory. This work was supported by: European Union's Horizon 2020 research and innovation programme, project OpenQKD (grant agreement No 857156); Agenzia Spaziale Italiana, project Q-SecGroundSpace (Accordo n. 2018- 14-HH.0, CUP: E16J16001490001); European Union's PON Ricerca e Innovazione 2014-2020 FESR/FSC—Project ARS01-00734 QUANCOM.

Author contributions All authors contributed to the study conception and design. Management and coordination responsibility for the research activity were performed by Davide Orsucci, Francesco Picciariello, Francesco Vedovato, Giuseppe Vallone, Paolo Villoresi, Amita Shrestha, and Florian Moll. The experiment realization and the data collection were performed by Francesco Picciariello, Francesco Vedovato, Davide Orsucci, Marco Avesani, Matteo Padovan, Luca Calderaro, Pablo Nahuel Dominguez, and Thomas Zechel. The data analysis was performed by Francesco Picciariello, Francesco Vedovato, Matteo Padovan, Giulio Foletto, Pablo Nahuel Dominguez, and Thomas Zechel. The software used was developed by Francesco Picciariello, Francesco Vedovato, Matteo Padovan, Giulio Foletto, Marco Avesani, Luca Calderaro, Pablo Nahuel Dominguez, and Thomas Zechel. The following authors provided technical equipment for the realization of the experiment: Daniele Dequal, Ludwig Blümel, Tobias Schmidt, Luca Calderaro, Marco Avesani, Francesco Vedovato, Giuseppe Vallone, and Paolo Villoresi. The first draft of the manuscript was written by Francesco Picciariello, Francesco Vedovato, Davide Orsucci, Matteo Padovan, Pablo Nahuel Dominguez, and Thomas Zechel. Acquisition of the financial support for the project leading to this publication was performed by Florian Moll, Johann Furthner, Tobias Schmidt, Giuseppe Vallone, and Paolo Villoresi. All authors read and approved the final manuscript.

Funding Open access funding provided by Università degli Studi di Padova.

Declarations

Competing interests The authors declare no competing interests.

References

Allan DW, Weiss MA (1980) Accurate time and frequency transfer during common-view of a gps satellite. In: 34th Annual Symposium on Frequency Control, Philadelphia, PA, USA. https://doi.org/10.1109/FREQ.1980.200424

Andrews LC, Phillips RL (2005) Laser Beam Propagation through Random Media. SPIE. https://doi.org/10.1117/3.626196

Avesani M, Agnesi C, Stanco A, Vallone G, Villoresi P (2020) Stable, low-error, and calibration-free polarization encoder for free-space quantum communication. Opt Lett 45:4706–4709. https://doi.org/10.1364/OL.396412

Avesani M et al (2022) Deployment-ready quantum key distribution over a classical network infrastructure in Padua. J Lightwave Technol 40(6):1658–1663. https://doi.org/10.1109/JLT.2021.3130447

Bennet CH, Brassard G (1984) Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the international conference on computers, systems & signal processing, Bangalore, India, pp 175–179. https://doi.org/10.48550/arXiv.2003.06557

Bernstein DJ, Lange T (2017) Post-quantum cryptography. Nature 549:188–194. https://doi.org/10.1038/nature23461

Calderaro L, Stanco A, Agnesi C, Avesani M, Dequal D, Villoresi P, Vallone G (2020) Fast and simple qubit-based synchronization for quantum key distribution. Phys Rev Appl 13:054041. https://doi.org/10.1103/PhysRevApplied.13.054041

Ceccato S, Formaggio F, Caparra G, Laurenti N, Tomasin S (2018) Exploiting side-information for resilient GNSS positioning in mobile phones. IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, pp 1515–1524. https://doi.org/10.1109/PLANS.2018.8373546

Daemen J, Rijmen V (2000) The Block Cipher Rijndael. In: Quisquater JJ, Schneier B (eds) Smart Card Research and Applications. CARDIS 1998. Lecture Notes in Computer Science, vol 1820. Springer, Berlin, Heidelberg. https://doi.org/10.1007/10721064_26

Dai H et al (2020) Towards satellite-based quantum-secure time transfer. Nat Phys 16:848–852. https://doi.org/10.1038/s41567-020-0892-y

Defraigne P, Petit G (2003) Time transfer to TAI using geodetic receivers. Metrologia 40:184. https://doi.org/10.1088/0026-1394/40/4/307

Defraigne P, Petit G (2015) CGGTTS-Version 2E: an extended standard for GNSS Time Transfer. Metrologia 52:G1. https://doi.org/10.1088/0026-1394/52/6/G1

Fante RL (1975) Electromagnetic beam propagation in turbulent media. Proc IEEE 63(12):1669–1692. https://doi.org/10.1109/PROC.1975.10035

Fung C-HF, Lo H-K (2006) Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. Phys Rev A 74:042342. https://doi.org/10.1103/PhysRevA.74.042342

Götzelmann M, Köller E, Viciano-Semper I, Oskam D, Gkougkas E, Simon J (2023) Galileo open service navigation message authentication: preparation phase and drivers for future service provision. Navigation. https://doi.org/10.33012/navi.572

Kneizys F, Shettle E, Abreu L, Chetwynd J and Anderson G (1988) Users Guide to LOWTRAN 7ADA206773 Air Force Geophysics Laboratory AFB MA. https://apps.dtic.mil/sti/citations/ADA206773

Lewis A, Travagnin M (2022) A secure quantum communications infrastructure for Europe: technical background for a policy vision. Publ off Eur Union. https://doi.org/10.2760/180945

Liao S-K et al (2018) Satellite-relayed intercontinental quantum network. Phys Rev Lett 120:030501. https://doi.org/10.1103/PhysRevLett.120.030501

Lim CB et al (2019) Single-mode fiber coupling with adaptive optics for free-space optical communication under strong scintillation. In: IEEE International Conference on Space Optical Systems and Applications (ICSOS), Portland, OR, USA. https://doi.org/10.1109/ICSOS45490.2019.8978978

Miller VS (1986) Use of elliptic curves in cryptography. In: Williams HC (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39799-X_31

Pirandola S et al (2020) Advances in quantum cryptography. Adv Opt Photon 12:1012–1236. https://doi.org/10.1364/AOP.361502

Ricklin JC, Davidson FM (2002) Atmospheric turbulence effects on a partially coherent Gaussian beam: implications for free-space laser communication. J Opt Soc Am A 19:1794–1802. https://doi.org/10.1364/JOSAA.19.001794

Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126. https://doi.org/10.1145/359340.359342

Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H (2018) Finite-key analysis for the 1-decoy state QKD protocol. Appl Phys Lett 112:171104. https://doi.org/10.1063/1.5023340

Scriminich A, Foletto G, Picciariello F, Stanco A, Vallone G, Villoresi P, Vedovato F (2022) Optimal design and performance evaluation of free-space quantum key distribution systems. Quantum Sci Technol 7:045029. https://doi.org/10.1088/2058-9565/ac8760

Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA. https://doi.org/10.1109/SFCS.1994.365700

Sidhu JS et al (2021) Advances in space quantum communications. IET Quant Comm 2:182–217. https://doi.org/10.1049/qtc2.12015

Stanco A, Santagiustina FBL, Calderaro L, Avesani M, Bertapelle T, Dequal D, Vallone G, Villoresi P (2022) Versatile and concurrent FPGA-based architecture for practical quantum communication systems. IEEE Trans Quant Eng 3:1–8. https://doi.org/10.1109/TQE.2022.3143997

Wegman MN, Carter JL (1981) New hash functions and their use in authentication and set equality. J Comput Syst Sci 22(3):265–279. https://doi.org/10.1016/0022-0000(81)90033-7

Xu F, Ma X, Zhang Q, Lo H-K, Pan J-W (2020) Secure quantum key distribution with realistic devices. Rev Mod Phys 92:025002. https://doi.org/10.1103/RevModPhys.92.025002

Yin J et al (2020) Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature 582:501–505. https://doi.org/10.1038/s41586-020-2401-y

Francesco Picciariello received the M.Sc. degree in Telecommunication Engineering and the Ph.D. degree in Information Engineering from Universitá degli Studi di Padova, Padua, Italy, in 2018 and 2023, respectively. He currently holds a postdoctoral research grant where he works in free-space quantum communication and quantum key distribution at the Department of Information Engineering.

Francesco Vedovato received the M.Sc. degree in physics and the Ph.D. degree in space sciences and technologies from Universitá degli Studi di Padova, Padua, Italy, in 2015 and 2019, respectively. He is currently a Researcher with the Department of Information Engineering at the University of Padova, where he works on experimental quantum optics, quantum communication, and quantum key distribution, with particular focus on free-space and satellite applications.

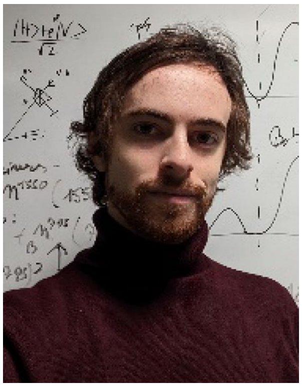
Davide Orsucci is a theoretical physicist working in the Institute of Communications and Navigation at the German Aerospace Center (DLR) on quantum key distribution, free-space optical communication, atmospheric channel modeling, and quantum repeater architectures.

Pablo Nahuel Dominguez is member of the German Aerospace Center (DLR) in Oberpfaffenhofen. His fields of interest are optical time and frequency distribution systems and phase stabilization of optical oscillators.

Thomas Zechel is an experimental physicist working in the Institute of Communications and Navigation at the German Aerospace Center (DLR) on time generation and distribution as well as systems engineering and project management for space projects.

Marco Avesani received the M.Sc. degree in physics and the Ph.D. degree in information and communication technologies from Universitá degli Studi di Padova, Padua, Italy, in 2015 and 2020, respectively. He is currently a Researcher with the Department of Information Engineering, where he works on experimental quantum optics, quantum random number generation, and quantum communication, with a particular focus on quantum key distribution and semi-device-independent quantum random number generators.

Matteo Padovan received the M.Sc. degree in internet communication technology in 2020 from Universitá degli Studi di Padova, Padua, Italy, where he is currently working toward the Ph.D. degree in space sciences and technologies. His main research interests include quantum weak measurements for quantum information, experimental quantum optics, and quantum key distribution.



Giulio Foletto is a post-doctoral fellow at KTH, Sweden, and previously at Università degli Studi di Padova, Italy. His main research interests are the quantum weak measurement and quantum key distribution.

Luca Calderaro received the B.S. and M.S. degrees in physics and the Ph.D. degree in space sciences and technology from the University of Padova, Padua, Italy, in 2013, 2015, and 2018, respectively. Before entering into ThinkQuantum as a Quantum System Architect, he worked on the following research topics: experimental satellite quantum communication, quantum key distribution, and quantum entanglement.

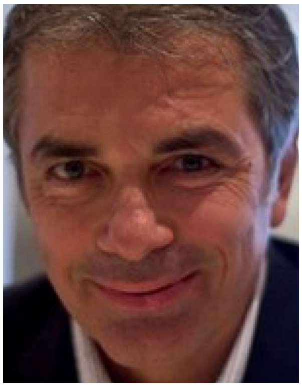
Daniele Dequal graduated in Physics at the University of Padua where he continued his studies with a Ph.D. focused on the development of a trigger system for ICARUS T-600, an innovative neutrino detector operating at the Gran Sasso National Laboratories of the INFN. He continues his post-doctoral research activity by joining the quantum communications group of the Information Engineering Department of Padua. During this research activity, the first satellite quantum communication is demonstrated. Since 2017, he has been a researcher at ASI, where he deals with quantum communications and satellite, lunar and space debris laser ranging.

Amita Shrestha has a masters' degree in Communications Systems and Electronics and is working in the Institute of Communications and Navigation at the German Aerospace Center (DLR). She has been involved in the development of real-time tracking software of institute's optical ground stations and is actively involved in several other projects related to free-space optical classical and quantum communications.

Ludwing Blümel received a diploma degree in microsystems engineering in 2005 and a diploma degree in physics in 2013. Since 2019, he works at the Institute of Communications and Navigation at the German Aerospace Center (DLR). His fields of interest are optical clocks, time references, and optical frequency combs.

Johann Furthner received his Ph.D. in laser physic in 1994 and is working since 1995 at the German Aerospace Center (DLR) in the area of GNSS design, simulation, and performance analysis. Since 2019, he is head of the department Signal Analysis and Timing Systems of the Galileo Competence Center of DLR.

Giuseppe Vallone received the M.S. degree in physics and the Ph.D. degree in theoretical physics from the University of Torino, Turin, Italy, in 2002 and 2006, respectively. Since 2019, he has been an Associate Professor with the Department of Information Engineering, University of Padova, Padua, Italy. He has coauthored more than 150 articles and participated in more than 30 scientific research projects. His research interests include quantum information, experimental quantum optics, and quantum communication.



Paolo Villoresi born in Treviso, Italy, in 1962. He studied physics and applied mathematics with the University of Padova, Padua, Italy. He is currently a Full Professor of physics with the University of Padova, where he currently teaches quantum optics and related subjects. He is the author of more than a 170 publications on peer-refereed journals and editor of two books. He is the coauthor of more than 200 congresses contribution in the areas of quantum communication, quantum optics, laser–matter interaction, and atomic and plasma physics.

Tobias D. Schmidt received his Ph.D. in molecular physics in 2013 from the University of Augsburg. He began work at the Institute of Communications and Navigation at the German Aerospace Center (DLR) in 2017. His fields of interests are (optical) atomic clocks, time reference frames, and optical time transfer for navigation applications.

Florian Moll received his M.Sc. degree in electrical engineering in 2009 and has been a member of the German Aerospace Centre (DLR) Institute of Communications and Navigation since then. His work area is free-space optical quantum communications for aircraft and satellites. He is involved in several research projects as project and team leader.