Experimental Satellite Quantum Communications

Vallone, Giuseppe; Bacco, Davide; Dequal, Daniele; Gaiarin, Simone; Luceri, Vincenza; Bianco, Giuseppe; Villoresi, Paolo

Published in:
Physical Review Letters

Link to article, DOI:
10.1103/PhysRevLett.115.040502

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
Experimental Satellite Quantum Communications

Giuseppe Vallone,1 Davide Bacco,1 Daniele Dequal,1 Simone Gaiarin,1 Vincenza Luceri,2 Giuseppe Bianco,3 and Paolo Villoresi1,∗
1Dipartimento di Ingegneria dell’Informazione, Università degli Studi di Padova, Padova, Italy
2e-GEOS spa, Matera, Italy
3Matera Laser Ranging Observatory, Agenzia Spaziale Italiana, Matera, Italy

Quantum Communications on planetary scale require complementary channels including ground and satellite links. The former have progressed up to commercial stage using fiber-cables, while for satellite links, the absence of terminals in orbit has impaired theirs development. However, the demonstration of the feasibility of such links is crucial for designing space payloads and to eventually enable the realization of protocols such as quantum-key-distribution (QKD) and quantum teleportation along satellite-to-ground or intersatellite links. We demonstrated the faithful transmission of qubits from space to ground by exploiting satellite corner cube retroreflectors acting as transmitter in orbit, obtaining a low error rate suitable for QKD. We also propose a two-way QKD protocol exploiting modulated retroreflectors that necessitates a minimal payload on satellite, thus facilitating the expansion of Space Quantum Communications.

Quantum Physics protocols connecting separate operators call for Quantum Communications (QCs), whose essence is the fair transport of a generic quantum state along a channel [1]. For their implementation, quantum protocols may require short links, as in the case of Quantum Computing, or extended connections, as for the realization of Quantum Key Distribution (QKD), in which two distant parties generate a secret key to be used for data encryption [2–5]. In the case of QKD, the locations of these parties may be connected by optical cables, for which its implementation has already reached its maturity [6–8], or by two ground optical terminals [9]. However, a significant and crucial fraction of QKD applications require a free-space network including one or more nodes on a satellite, as it is occurring for classical communications (e.g. internet, phone and TV). More generally, Space QCs are needed to extend fundamental tests of Quantum Mechanics as the measure of Bell’s inequality in a relativistic scenario, as well as to establish a global network to distribute entanglement and provide secure communications [10, 11], as fostered in several continental Information-and-Communication-Technology (ICT) roadmaps [12, 13].

The envisaging and modelling of Space QCs started a dozen years ago [14–18]. Nevertheless, sources or detectors of quantum states have not been placed in orbit yet. Therefore, since 2008 the experimental studies of Space-to-ground links simulated a source of coherent pulses attenuated at the single photon level by exploiting satellites for geodetics laser ranging, which are equipped with corner-cube retroreflectors (CCRs) [19, 20]. However, a full quantum transmitter for polarization encoded QKD in Space also requires qubits prepared in different polarization states.

Here we show the operation of such quantum transmitter by sending toward selected satellites a train of laser pulses at the repetition rate of 100 MHz paced with an atomic clock and generated at the Matera Laser Ranging Observatory (MLRO) of the Italian Space Agency in Matera (Italy). The qubit signal is obtained by the pulses reflected by the CCRs (see FIG. 1). We set the outgoing laser intensity such that the qubit signal has an average photon number per pulse close to one, as required by QKD protocols. Then we demonstrate the faithful transmission of different polarization qubits between satellite and ground and provide a quantitative estimate of the mean photon number of the downward pulses. We will show at the end that, by using modulated CCRs, our technique can be exploited for a full QKD protocol along Space channels. Our results prove that quantum key distribution from an orbiting terminal and a base station is not only a promising idea but is nowadays realizable.

We prove the feasibility of the BB84 protocol [21] with
FIG. 2. Top: Larets trajectory measured by the 10 Hz SLR pulses. The four selected 10 s intervals correspond to four different polarization input states. Bottom: the four histograms report the obtained counts at the receiver for each single photon detector in function of the measured detection time \( t_{\text{meas}} \), demonstrating an average QBER of 6.5 \%. The signal on the two detectors is blue for H/L polarization and green for V/R. Gray dashed lines represent the 1 \( \sigma \) selection interval around the expected time of arrival \( t_{\text{ref}} \).

The qubits encoded in four different polarization states, corresponding to two mutually unbiased basis. A secret key can be established between the transmitter (Alice, at the satellite) and the receiver (Bob, at MLRO) when the average Quantum Bit Error Rate (QBER) is below 11\%. In a transmission with polarization qubits, the QBER can be estimated as \( Q = (n_{\text{wrong}}+1)/(n_{\text{corr}}+n_{\text{wrong}}+2) \) where \( n_{\text{corr}} \) and \( n_{\text{wrong}} \) are the number of detections in the sent and orthogonal polarization respectively. The exploitation of CCRs with metallic coating on the three reflecting faces is crucial for preserving the imposed polarization state during the reflection. For this reason we could not use satellites mounting uncoated or dielectric coated CCRs. We selected five LEO (Low Earth Orbit, below 2000 km) satellites: Jason-2, Larets, Starlette and Stella with metallic coated CCRs and Ajisai, with uncoated CCRs, for comparison.

In order to reject the background and dark counts, a precise synchronization at Bob is needed. For this purpose we exploited the satellite laser ranging (SLR) signal. The latter is generated in a much coarser comb of strong pulses (10 Hz repetition rate and 100 mJ pulse energy) whose seed is taken from the same comb used for the qubits. Two non-polarizing beam splitters were used in the optical path in order to merge and split the outgoing and incoming SLR signal and qubit stream (see FIG. 1). For qubits discrimination, we synchronized the state analyser with the time-tagging of SLR pulses provided by the MLRO unit, which has few picosecond accuracy. Indeed, by dividing the intervals between two consecutive SLR detections in \( 10^7 \) equidistant subintervals, we determined the sequence of expected qubit times of arrival \( t_{\text{ref}} \). This technique compensates for the time scale transformation due to satellite motion with respect to the ground. Our detection accuracy \( \sigma \) was set equal to the detector time jitter (0.5 ns), as other contributions to time uncertainties coming from detection electronics or laser fluctuations are negligible. Counts registered within a 1 \( \sigma \) interval around \( t_{\text{ref}} \) were considered as signal, while the background is estimated from the counts outside 3 \( \sigma \). Details of the setup are described in Supplementary Material.

QCs of polarized photons QCs using generic polarization states from two mutually unbiased bases were realised with a single passage of Larets. The passage was divided in four intervals of 10 s in which we sent horizontal \( |H\rangle \), vertical \( |V\rangle \), circular left \( |L\rangle \) and circular right \( |R\rangle \) states. At the receiver the state analysis is performed by two single photon detectors measuring two orthogonal polarizations, from which the QBER is extracted. The results are summarized in FIG. 2. In the four intervals, we obtained 199 counts in the correct detector and 13 wrong counts, giving an average QBER of 6.5 \%. Once considered the average 3.6 \% duty cycle of our setup (see Supplementary Material), the mean return frequency in the selected intervals is 147 Hz.

A further analysis has been carried out to prove the preservation of the polarization state for the other coated satellites. These results will prove that low QBERs can be obtained in different conditions and satellite orbit, showing the stability and the reliability of our approach. We will also report the detection rates achievable with the different LEO satellites. In this analysis we divided the detection period in intervals of 5 seconds: for each interval the data were analyzed only if the signal of at least one detector was 5 standard deviations above the background. The QBERs resulting from this analysis are shown in FIG. 3 for Ajisai, having non polarization preserving CCRs, and for the polarization preserving satellites Jason-2, Larets, Starlette and Stella. We achieved a QBER below 10 \% for several tens of seconds in all the polarization maintaining conditions.

---

1 By using the post-selection techniques introduced in [22], QBER up to 20\% can be tolerated for secret key generation.

2 We used the Bayesian estimator of the QBER.
satellites.

**Link budget and μ estimate** A real earth-satellite QKD system is based on faint laser pulses with a mean photon number of the Poisson process μ close to 1. Indeed the BB84 protocol with decoy states [23, 24] in a realistic scenario requires μ ≪ 2 [25]. We demonstrate in the following that our experiment was carried out in this regime.

An estimation of the average number of photons per pulse leaving the satellites μsat is obtained by dividing the average number of photons per pulse detected at the receiver, μrx, by the transmission of the quantum channel. A general formula to predict the detected number of photons per pulse is the radar equation

\[ \mu_{rx} = \mu_{tx} \eta_{tx} G_t \Sigma \left( \frac{1}{4\pi R^2} \right)^2 T_a^2 A_t \eta_{rx} \eta_{det} \]

where \( \mu_{tx} \) is the source mean photon per pulse, \( \eta_{tx} \) is the optical transmission efficiency, \( G_t \) is the transmission gain, \( \Sigma \) and \( R \) the satellite cross-section and slant distance, \( T_a \) the atmospheric transmissivity, \( A_t \) the telescope area, \( \eta_{rx} \) the optical receiving efficiency and \( \eta_{det} \) the single photon detector efficiency [26]. To estimate \( \mu_{sat} \) it is necessary to factorise the radar equation into an uplink and a downlink factors. While most of the parameters of the radar equation can be easily separated into uplink and downlink factors, the satellite cross section \( \Sigma \) plays a role in both and must be split according to \( \Sigma = \rho A_{eff} G_{down} \). The parameters \( \rho \) and \( A_{eff} \), corresponding to the CCR reflectivity and the effective satellite retroreflective area, contribute to the uplink, while \( G_{down} \) gathers all the downlink contributions into an effective downlink gain. Then, the downlink factor, corresponding to the quantum channel transmission, is given by

\[ \mu_{rx} = \mu_{sat} \Sigma \rho A_{eff} \left( \frac{1}{4\pi R^2} \right) T_a A_t \eta_{rx} \eta_{det} \]  

The values of \( \mu_{sat} \) in FIG. 4 were calculated by using (1).
with the following parameters $\eta_{det} = 0.1$, $P_s = 0.11W$, $\eta_{xs} = 0.1$, $A_t = 1.73m^2$, $\eta_{xx} = 0.13$. We used the satellite cross-section reported in [27,29]. For the Larets passage of FIG.2 we obtained $\mu_{sat} = 3.4 \pm 0.2$ and a corresponding downlink transmissivity of $\sim 4.3 \times 10^{-7}$ (63 dB of attenuation). The resulting $\mu_{sat}$ is of the order of unity for the four satellites with metallic CCRs. The reflectivity $\rho$ of these latter was taken as unitary, setting a higher bound on $\mu_{sat}$. The atmospheric absorbance is proportional to the air-mass (AM), defined as the optical path length through atmosphere normalized to the zenith. In our model we considered 87% of transmissivity for the zenith for all the days. This value refers to good sky conditions [26] which were effectively selected for the experiment.

For a consistency check of our $\mu_{sat}$ estimation, the full radar equation has been used to extrapolate the transmitter gain $G_t$, which depends on the upward beam divergence, the beam wandering due to the atmospheric turbulence and the pointing errors. By averaging the data obtained in different passages of Ajisai, Jason and Starlette, an effective gain $G_t = 1.1 \times 10^9$ was obtained (see Supplementary Material). The resulting value of $G_t$ has been used in the radar equation to estimate the number of received photons. The theoretical predictions and the experimental data are compared in FIG.4. The results show that radar equation model [26] and eq. (1) provides a precise fit for the measured counts and the $\mu_{sat}$ values derived in FIG.4.

QKD satellite protocol using retroreflector

We note that, if the outgoing and incoming beam travel through the same optical path, the polarization transformation induced in the uplink by the telescope movements is compensated in the downlink (see Supplementary Material). Therefore, by transforming the state during the retroreflection, we drive the qubit state received on the ground. On this base, we propose a two-way QKD protocol, working as follows. In the ground station, the qubit is sent to the satellite forming the state during the retroreflection, we drive the qubit upward by the telescope movements is compensated in the downlink. From the satellite, the qubit is propagated toward the ground telescope, and thanks to the properties of the Coudé path, a polarization rotated by $\theta$ with respect to the horizontal will be received. By this scheme, a decoy state BB84 protocol can be realised between satellite and ground. The experimental results shown above demonstrate that such protocol is currently realizable using few centimetres CCRs and that the MLRO station is suitable for Space QCs.

In conclusion, QCs were demonstrated experimentally from several satellites acting as quantum transmitter and with MLRO as the receiver. QBER was found low enough to demonstrate the feasibility of quantum information protocols such as QKD along a Space channel. Moreover, we propose that a very simple trusted device in orbit, formed by an active CCR mounted on spacecraft and operated in the two-way scheme may provide a simple alternative to a full space terminal, fostering a faster expansion of QCs around the planet and beyond.

We would like to thank Francesco Schiavone, Giuseppe Nicoletti and the MRLO technical operators and Prof. Cesare Barbieri, Andrea Tomaello and Alberto Dall’Arche (University of Padova) for the collaboration and support. This work has been carried out within the Strategic-Research-Project QUANTUMFUTURE of the University of Padova and the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova.

*paolo.villoresi@dei.unipd.it*

[28] V.P. Vasilev, I.S. Gashkin, Presented at One-way and

Supplementary Information

SETUP

The detailed scheme used in the experiment is shown in figure 5.

A mode-locking laser oscillator subjugated at the MLRO atomic clock is used as event generator. It produces pulses of 100 ps duration at the wavelength of 1064 nm, with 100 MHz of repetition rate and about 400 mW of average power. The laser output is split to provide the seed for the SLR signal and the pump pulse for the qubits. The SLR pulse is obtained by selecting with a pulse picker one pulse every $10^{-7}$ and then using a regenerative amplifier and two single-pass amplifiers followed by a Second Harmonic Generation (SHG) stage, obtaining a pulse at 532 nm with 100 mJ energy and 10 Hz repetition rate. The beam used to generate the qubits is obtained by sending the rest of the master oscillator laser to a suitable SHG unit, whose output is 110 mW. The beam divergence is controlled by a collimator and the polarization state is controlled by two waveplates and a modulator. Two non-polarizing beam splitters (NPBS) are used to combine SLR with qubit combs in the upward beam that is directed via the Coudé path to the MLRO telescope, from which it propagates toward the satellites.

The beams received from the satellites by the MLRO telescope propagate backward via the Coudé path and are split by the same two NPBS also used in the uplink. The qubit receiver is composed by a focalizing lens, a rotating waveplate, an optical shutter and two single photon photomultipliers (PMTs) placed at the outputs of a Polarizing Beam Splitter (PBS). The signals detected by the PMTs are fed into a time tagger with 81 ps resolution. A rotating waveplate, controlled by software, is used to change between two receiving bases, $\{\ket{H}, \ket{V}\}$ and $\{\ket{L}, \ket{R}\}$.

The pulses generated by the transmitter, passing through the first NPBS produce a scattering that elevates the background noise at the quantum receiver. To prevent this effect, we implemented a time division protocol by using two fast mechanical optical shutters. In the first half of the 100 ms slot between two SLR pulses, the transmitter shutter is opened in order to send the qubit pulses toward the satellite, while the reception shutter is closed to protect the receiver PMTs. In the second half of the slot the transmitter shutter is closed, and, once the receiver shutter is fully open, the detection phase begin (see FIG. 6). By using this protocol, the effective transmission time during a slot cannot be larger than the round trip time (RTT); however, since the
shutters require about 2 ms to fully open and 2.5 ms to fully close, the effective period is further reduced by 4.5 ms. Considering that for a LEO satellite the RTT varies between 5 and 20 ms, the effective duty cycle can vary between 0 and 15%. Moreover, the effective duty cycle varies also in a single satellite passage, approaching its minimum when the satellite reaches its maximum elevation.

FIG. 6. Temporal slot between two SLR pulses. TX and RX indicate the transmitter and receiving phase respectively. RTT is the satellite round trip time. The green zone represents the effective time of qubit detection.

**RADAR EQUATION**

As said in the main text, in order to have an additional confirmation that the obtained values of $\mu_{sat}$ are correct, the full radar equation has been used to extrapolate the transmitter gain, given by

$$G_t = \frac{8}{\theta_t^2} \exp \left[ -2 \left( \frac{\theta}{\theta_t} \right)^2 \right].$$

In the previous equation $\theta_t$ is the divergence angle of the upgoing beam (including the beam broadening due to turbulence), while $\theta$ is the pointing error. Since the two parameters $\theta$ and $\theta_t$ cannot be directly and separately measured, we obtained an estimate for $G_t$ by comparison the data obtained in different passages of the several LEO satellites. As a consequence of the pointing error, the detection frequency of the 100 MHz laser varies strongly with time, thus producing localized peaks of detection for few tens of seconds, followed by the absence of signal. Because of this several periods of at least 10 seconds, in which the detection frequency was significantly above the background, have been isolated and only the peak frequency within these periods has been taken into account. To best approximate of $G_t$, we averaged the most stable data taken for Ajisai, Jason and Starlette, thus obtaining an effective gain of $G_t = 1.1 \times 10^9$. This value for $G_t$ has been used in the link budget equation to estimate the received photons frequency and then the fit has been compared with the collected data as shown in FIG. 4.

**POLARIZATION COMPENSATION IN THE DOWNLINK**

The polarization state generated on the optical table of the MLRO observatory in subjected to a unitary transformation due to the Coudé path of the telescope. Indeed, the Coudé path is composed of mirrors $M_1 \cdots M_7$ as in figure 7 with $M_1$ and $M_2$ the primary and secondary mirror of the telescope. If the mirrors are coated to have $\pi$ phase shift between s- and p- polarization (corresponding to a $\sigma_z$ transformation), the transformation in the uplink channel is given by

$$U_{up} = \sigma_z R \left( \frac{\pi}{2} - \theta_{el} \right) \sigma_z R(\theta_{az}) \sigma_z R \left( \frac{\pi}{2} \right),$$

where $\theta_{az}$ and $\theta_{el}$ are the azimuth and elevation angles of the telescope and $R(\theta)$ is a rotation of the reference frame given by:

$$R(\theta) = e^{-i\theta \sigma_y} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}.$$
FIG. 7. Coudé path of the MLRO telescope

With an input polarization $|\psi\rangle = \begin{pmatrix} \cos \alpha \\ e^{i\phi} \sin \alpha \end{pmatrix}$, the polarization at the output of the telescope is given by $|\psi'\rangle = U_{up}|\psi\rangle$. Since the CCR induce a transformation of $\sigma_z$ and the downlink channel can be written as

$$U_{down} = R\left(\frac{\pi}{2}\right) \sigma_z R(\theta_{az}) \sigma_z R\left(\frac{\pi}{2} - \theta_{el}\right) \sigma_z,$$

the receiving polarization state is given by

$$|\psi_{rec}\rangle = U_{down} \sigma_z U_{up}|\psi\rangle.$$

By using the property $\sigma_z R(\theta) = R(\theta) \sigma_z$, it is easy to demonstrate that

$$|\psi_{rec}\rangle = \sigma_z |\psi\rangle,$$

showing that the uplink rotation is compensated by the downlink transformation.

This compensation is at the base of our proposed two-way protocol. Indeed, if the CCR is equipped with an active element like a Faraday Rotator at the entrance face, the transformation induced by the CCR is given by $U_{CCR}(\phi) = R(-\phi) \sigma_z R(\phi)$ with $R(\phi) = e^{-i\phi \sigma_x}$. The overall transformation is then obtained as

$$|\psi_{rec}(\phi)\rangle = U_{down} U_{CCR}(\phi) U_{up}|\psi\rangle = R(2\phi) \sigma_z |\psi\rangle.$$

If the input state is horizontally polarized, the received state is thus rotated by an angle of $2\phi$ in the laboratory reference frame. By modulating $\phi$, the two-way QKD protocol can be realized.