New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Feasibility of satellite quantum key distribution

To cite this article: C Bonato *et al* 2009 *New J. Phys.* **11** 045017

View the article online for updates and enhancements.

New Journal of Physics
The open-access journal for physics

Feasibility of satellite quantum key distribution

C Bonato[1], A Tomaello, V Da Deppo, G Naletto and P Villoresi

Department of Information Engineering, University of Padova CNR-INFM
LUXOR Laboratory for Ultraviolet and X-Ray Optical Research,
via Gradenigo 6, 35131 Padova, Italy
E-mail: bonatocr@dei.unipd.it and paolo.villoresi@unipd.it

New Journal of Physics **11** (2009) 045017 (25pp)
Received 28 November 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045017

Abstract. In this paper, we present a novel analysis of the feasibility of quantum key distribution between a LEO satellite and a ground station. First of all, we study signal propagation through a turbulent atmosphere for uplinks and downlinks, discussing the contribution of beam spreading and beam wandering. Then we introduce a model for the background noise of the channel during night-time and day-time, calculating the signal-to-noise ratio for different configurations. We also discuss the expected error-rate due to imperfect polarization compensation in the channel. Finally, we calculate the expected key generation rate of a secure key for different configurations (uplink, downlink) and for different protocols (BB84 with and without decoy states, entanglement-based Ekert91 protocol).

[1] Author to whom any correspondence should be addressed.

Contents

1. Introduction

In the last decades, a strong research effort has been devoted to study how quantum effects may be employed to manipulate and transmit information, in what is called quantum information processing [1]–[3]. These research activities lead to new information-processing protocols with no classical counterpart, like quantum key distribution (QKD) [4]–[6], quantum teleportation [7] or quantum computing [8]. Quantum key distribution, in particular, is on its way from research laboratories into the real world. Fiber and free-space links have been realized linking nodes at larger and larger distances [9, 10] with higher and higher key generation rates. Network structures have also been demonstrated recently, for example, the DARPA network in Boston [5] and the SECOQC network in Vienna [11].

However, current fiber and free-space links cannot implement a real global-scale quantum key distribution system. Fiber links have the advantage that the photon transfer is scarcely affected by external conditions, like background light, weather or environmental obstructions. On the other hand the extension of fiber links beyond a few hundred kilometers is problematic, due to attenuation and polarization-preservation issues [4, 9]. Terrestrial free-space links show some advantages: the atmosphere provides low absorption and is essentially non-birefringent, allowing almost unperturbed propagation of polarization states. On the other hand, the optical mode is not confined in a waveguide, so it is sensitive to the external environment: objects interposed in the line of sight, beam distortion induced by atmospheric turbulence and weather conditions.

A solution to this problem can be the use of space and satellite technology. Space-based links can potentially lead to global-scale quantum networking since they can connect any two points on the Earth surface with reduced losses as compared with terrestrial channels. This is mainly due to the fact that most of the propagation path is in empty space, with no absorption and turbulence-induced beam spreading, and only a small fraction of the path (corresponding to less than 10 km) is in atmosphere. However, many technical problems must be overcome in order to realize a working quantum communication link between Earth and space. Geostationary satellites are too distant to implement a single photon link; therefore fast-moving low-orbit satellites (LEO orbit, from 500 to 2000 km above Earth surface) must be employed.

Several proof-of-principle experiments in this direction have been performed recently. In 2005, Peng *et al* reported the first distribution of entangled photon pairs over 13 km, beyond the effective thickness of the atmosphere [12]. This was a first significant step toward satellite-based global quantum communication, since it showed that entanglement can survive after propagating through the noisy atmosphere.

In 2007, two experiments were carried out at the Canary Islands by a European collaboration. Entanglement-based [10] and decoy-state [13] quantum key distribution was realized on a 144 km free-space path, linking La Palma with Tenerife. For these experiments the Optical Ground Station of the European Space Agency, developed for standard optical communication between satellites and Earth, was adapted for quantum communication. It is important to highlight that the twin-photon source was able to achieve coincidence production rates and entanglement visibility sufficient to bridge the attenuation expected for satellite-to-ground quantum channels.

In a successive experiment, the feasibility of single-photon exchange for a down-link between a LEO satellite and an optical ground station (Matera Laser Ranging Observatory, in the south of Italy) was experimentally demonstrated [14]. The researchers exploited the retroreflection of a weak laser pulse from a geodetic satellite covered with corner-cubes (Ajisai, orbiting at around 1400 km) to simulate a single photon source on a satellite. They showed that by implementing a strong filtering in the spatial, spectral and temporal domains emitted photons can be recognized against a very strong background.

In this paper, we present a novel analysis of the feasibility of satellite-based quantum communication. In particular, we investigate two crucial aspects pointed out in the experiment realized at Matera Observatory for the single photon link with an orbiting sender [14]: the conditions to achieve a good signal-to-noise ratio (SNR) and the control of polarization alignment during the satellite passage. As regards the SNR we will refine the models already presented in the literature by introducing a detailed analysis of the effect of atmospheric turbulence and of the background stray-light. As far as polarization control is concerned, we will discuss and compare different strategies to implement a polarization-conserving channel, showing that the error probability resulting from imperfect polarization compensation can be kept really low. Using the expected values for signal attenuation, noise and bit error rate we will finally discuss the possibility of implementing different quantum key distribution protocols (BB84, decoy-state BB84 and entanglement-based Ekert91 protocol).

2. Signal and noise

Two crucial points for any communication system are the amount of attenuation of the link and the noise introduced in the system. This is even more important for quantum communication since the signal transmitted by Alice is ideally one photon (or a weak coherent pulse with very low mean photon number in many realistic implementations). Therefore one cannot increase the signal power in order to have a good enough SNR: the only available tools are the reduction of the link attenuation and of the background noise. In this section, we will analyze a quantum channel between a ground station and a LEO satellite both in uplink and downlink, presenting a model for the expected attenuation and background noise.

2.1. Signal attenuation

The main factor limiting the performance of free-space optical communication is atmospheric turbulence, both for terrestrial horizontal links or for links between ground and satellites. Atmospheric turbulence induces refractive index inhomogeneities that increase the amount of spreading for traveling beams [15, 16] beyond the effect of diffraction. In particular, turbulent eddies whose size is large compared with the size of the beam induce a deflection of the beam (beam wandering), while smaller scale turbulent features induce beam broadening. In other words, observing a beam which propagates through turbulent atmosphere at different time instants, one can see a broadened beam randomly deflected in different directions. When integrating the observation over a timescale longer than the beam-wandering characteristic time, the global effect is a broadening of the beam.

2.1.1. Uplink. Models for optical beam propagation in the case of uplinks and downlinks between a satellite and a ground station have been discussed in the literature [17]–[19]. In the case of a Gaussian beam of waist w_0 and intensity I_0, the average long-term spot (which is a superposition of moving short-term spots), tends theoretically to a Gaussian spatial distribution of intensity [18]:

$$\langle I(r, L)\rangle = I_0 \mathrm{e}^{-2r^2/w_{\mathrm{LT}}^2} \tag{1}$$

with width w_{LT}, where

$$w_{\mathrm{LT}}^2 = w_{\mathrm{ST}}^2 + 2\left\langle \beta^2 \right\rangle. \tag{2}$$

Here w_{ST} is the short-term beam width, while β is the instantaneous beam displacement from the unperturbed position.

It can be shown that, for a collimated beam, the long-term beam width is [18]

$$w_{\mathrm{LT}}^2 = w_0^2\left(1+\frac{L^2}{Z_0^2}\right) + 2\left(\frac{4L}{kr_0}\right)^2, \tag{3}$$

where Z_0 is the Rayleigh parameter of the beam, L is the propagation distance and r_0 is the Fried parameter (for the uplink), given by

$$r_0 = \left[0.42k^2 \int_0^L C_n^2(z)\left(\frac{L-z}{L}\right)^{5/3} \mathrm{d}z\right]^{-3/5}. \tag{4}$$

The estimate of r_0 in equation (4) was made by integrating the turbulent contribution of the atmosphere along the whole optical path. The resulting w_{LT}^2 should then be considered a high bound, and the resulting conclusions as on the safe side. The refractive index structure constant $C_n^2(z)$ is taken from [17] to be

$$C_n^2(h) = 0.00594(v/27)^2(h\times 10^{-5})^{10}\mathrm{e}^{-h/1000} + 2.7\times 10^{-16}\mathrm{e}^{-h/1500} + A\mathrm{e}^{-h/100}, \tag{5}$$

where $A = 1.7\times 10^{-14}$ and $v = 21\,\mathrm{m\,s^{-1}}$. The expression for the short-term width is

$$w_{\mathrm{ST}}^2 = w_0^2\left(1+\frac{L^2}{Z_0^2}\right) + 2\left\{\frac{4.2L}{kr_0}\left[1-0.26\left(\frac{r_0}{w_0}\right)^{1/3}\right]\right\}^2. \tag{6}$$

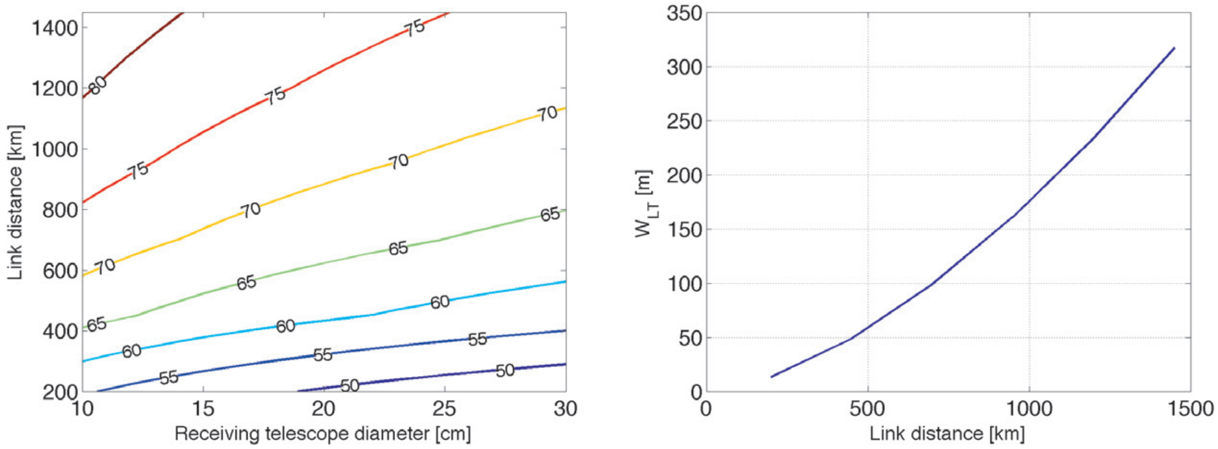

Figure 1. Attenuation η^{-1} (dB) for the uplink as a function of the link distance L and receiver telescope diameter $2R$ for the long-term beam spreading effect, which takes into account the effects of beam spreading and wandering. The operating wavelength is $\lambda = 800\,\text{nm}$ and the diameter of the Earth-based transmitting telescope is assumed to be $r_{\mathrm{T}} = 75\,\text{cm}$. On the right-hand side, plot of w_{LT} as a function of the uplink distance L. In the uplink, the beam propagates through the turbulent atmosphere in the first part of its path, resulting in a large spreading ($w_{\mathrm{LT}} \approx 50\,\text{m}$ at 500 km) and in a strong signal attenuation ($\approx$50 dB for telescope of diameter 30 cm on a satellite orbiting at $L = 500\,\text{km}$ above the Earth surface).

The receiving telescope can be described as a circular aperture of radius R, which collects part of the incoming beam and focuses it on a bucket single-photon detector. The power P received through a circular aperture of radius R centered on the beam is

$$P = 2\pi I_0 \int_0^R \rho \mathrm{e}^{-2(\rho^2/w_{\mathrm{LT}}^2)} \mathrm{d}\rho. \tag{7}$$

Therefore the link-efficiency η, which we define as the percentage of the received power with respect to the transmitted one is

$$\eta = \eta_0 \left(1 - \mathrm{e}^{-2R^2/w_{LT}^2}\right). \tag{8}$$

The factor η_0 comprises the detection efficiency, the pointing losses and the atmospheric attenuation; we take an empirical factor [20] $\eta_0 \approx 0.1$.

Some simulations for the link efficiency are shown in figure 1: the link attenuation (in dB) is shown as a function of the link distance L and the radius R of the receiving telescope. In the uplink, the beam first travels through the turbulent atmosphere and then propagates, aberrated, in the vacuum to the satellite. The initial atmosphere-induced aberrations greatly increase the beam spreading, resulting in a very strong attenuation. For a relatively low satellite, at 500 km above the Earth surface, the attenuation is of the order of more than 50 dB.

An interesting point is the relative contribution of the beam spreading due to smaller scale atmospheric turbulence (described by w_{ST}) and the beam-wandering induced by larger scale eddies (described by $\langle\beta^2\rangle$). In principle, the beam wandering could be compensated by means of an active tip/tilt mirror with some kind of feedback loop. To investigate this possibility, we

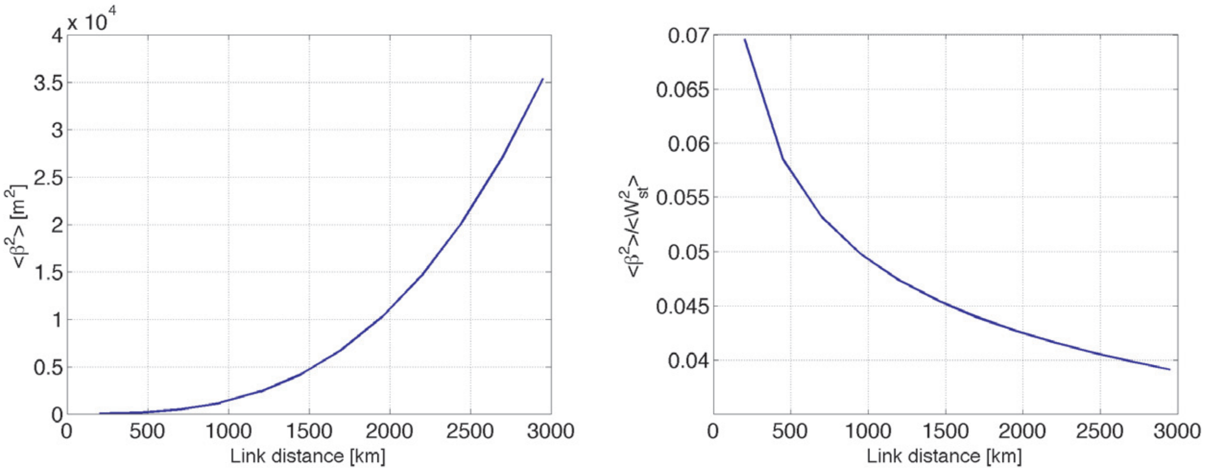

Figure 2. On the left, $\langle \beta^2 \rangle$ as a function of the ground-to-satellite distance (for the uplink). On the right, ratio between $\langle \beta^2 \rangle$ and $\langle \beta w^2_{\mathrm{ST}} \rangle$. In the case of a LEO satellite, the effect of beam wandering is limited to less than 10% with respect to the beam spreading; therefore its possible compensation with a tip/tilt active system might not significantly improve the overall performance of the link.

calculated the ratio between $\langle \beta^2 \rangle$, which describes the beam wandering, and $\langle W^2_{\mathrm{ST}} \rangle$, which describes the instantaneous beam spreading. The results, plotted in figure 2, show that the contribution of the beam wandering is smaller than the effect of the short-term beam spreading. Therefore the possible improvement due to a removal of the beam wandering with a tip/tilt active mirror is below 10%, making the benefits of the compensation quite limited.

2.1.2. Downlink. Beam displacement is induced by turbulent eddies whose size is much smaller than the beam diameter. For satellite downlinks the beam arrives at the atmosphere with a size much larger than any turbulent eddy, therefore there is no significant beam wandering. Moreover, the beam propagates through the turbulent atmosphere only in the final part of its path, resulting in a reduced beam spreading compared with the uplink. As shown in figure 3, the signal attenuation is much weaker, of the order of around 15 dB for a satellite at 500 km (as compared with 50 dB for the uplink).

Experimental data taken by means of a ground telescope are suitable to confirm the fact that the beam wandering for a downlink is negligible with respect to beam spreading. In our experiment we have acquired with a video recorder the flickering light from Vega (α-Lyrae, magnitude zero) by the Matera Laser Ranging Observatory of the Italian Space Agency (ASI) in Matera, Italy. The telescope has the primary mirror diameter of 1.5 m. The gathered light was spectrally filtered at 532 nm by the coated optical components of the telescope, and acquired on the focal plane by a bidimensional sensor whose square pixel size was of 6.7 μm. The collection of the frames was taken at 10 Hz and analyzed in order to extract the first two moments of the intensity distribution. By considering a sample of 81 frames of Vega, in figure 4 is shown the distribution in the telescope focal plane of the centers of each frame, derived as the first moment of each frame, together with two circles of radius equal to the centered second moment of two frames. The spatial scale shown in the figure is that of the detector, and corresponds approximately to 10 μrad of atmospheric seeing, which are good visibility conditions at MLRO.

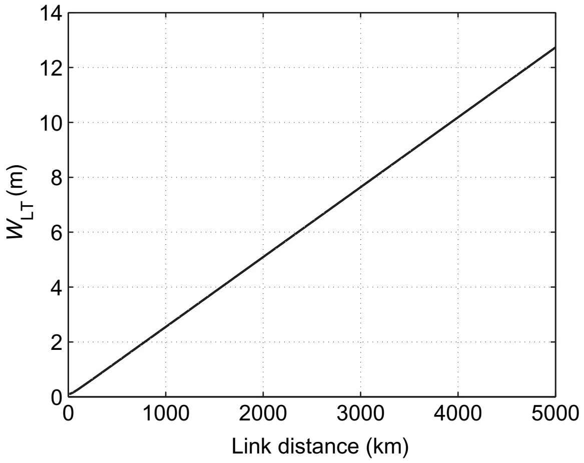

Figure 3. Beam width w_{LT} for the downlink as a function of the satellite-to-ground distance L. The long-term beam broadening is much smaller than it is for the uplink, resulting in a much weaker channel attenuation.

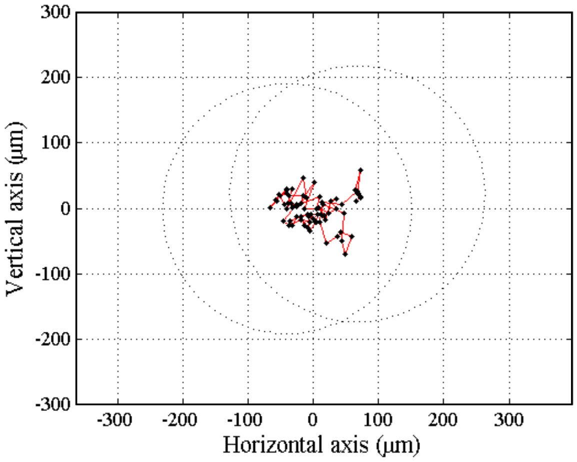

Figure 4. Analysis of light from Vega (α-Lyrae, magnitude zero): distribution of the centers in the telescope focal plane, combined with two circles of radius equal to the centered second moment of two frames.

The variation in the image diameter is shown in figure 5, where the radial centered second moment is plotted along the frames together with the two orthogonal components along the horizontal and vertical axes. Although rapid deformations of the image along one or the other components appear evidently in the figure, the radial second moment is fairly constant. The sequence of the sample images with the position of the center is shown in a video file available from stacks.iop.org/NJP/11/045017/mmedia.

From the statistical analysis of the frames we deduce that the center-of-mass displacement is less extended as compared to the radius of the spots, evaluated by means of the square root of the second moment. Indeed, by referring to the radius of the mean distribution, that is the average over all the 81 frames, of 197 μm, the standard deviation of the center-of-mass displacement results of 23 and 38 μm for the two axes while the mean radius of the single frame is 193 μm. The two radii are quite similar, indicating that the effect of wandering is of

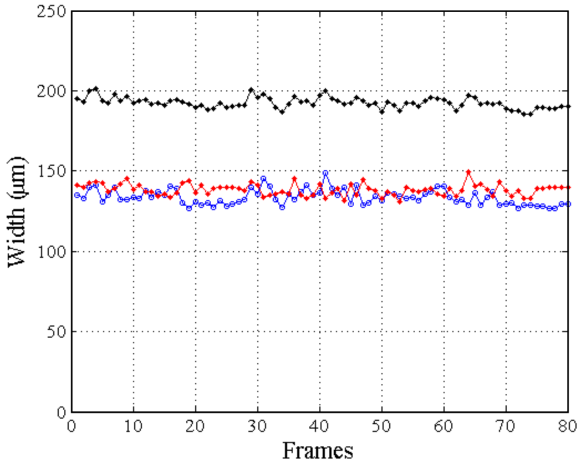

Figure 5. Analysis of light from Vega (α-Lyrae, magnitude zero): radial centered second moment is plotted along the frames and the two orthogonal components along the horizontal and vertical axes. Although rapid deformations of the image along one or the other components appear, the radial second moment is fairly constant. From the statistical analysis of the frames we deduce that the center-of-mass displacement is less extended as compared to the radius of the spots, evaluated by means of the square root of the second moment.

significantly lower importance. From this observation we can deduce that the wandering can be considered as weak, according to the seminal work of Fante [15] and following ones. This condition is encouraging for the effective achievement of the space quantum channel.

2.2. Background noise

2.2.1. Up-link (day-time operation). During the day the main source of background noise is the sunlight reflected by the Earth's surface into the telescope field-of-view (see figure 6). Let H_{sun} be the solar spectral irradiance (photons s^{-1} nm^{-1} m^{-2}) at one astronomical unit and a_E the Earth albedo. Assuming Lambertian diffusion, for which the radiance is independent of the angle, the spectral radiant intensity reflected by the Earth in number of photons per s, nm and steradian (sr) is

$$J_{\mathrm{E}} = \frac{1}{\pi} a H_{\mathrm{sun}} \Sigma, \tag{9}$$

where Σ is the emitting area seen by the telescope and $H_{\mathrm{sun}} = 4.61 \cdot 10^{18}$ photons s^{-1} nm^{-1} m^{-2} at $\lambda = 800$ nm. Such photons are collected by an optical system having entrance aperture radius R and instantaneous field-of-view (IFOV), at distance L from the Earth surface. Therefore the emitting area is

$$\Sigma = (\mathrm{IFOV})^2 L^2 \tag{10}$$

and the solid angle from which the telescope on the satellite can be seen from Earth is:

$$\Omega = \frac{\pi R^2}{L^2}. \tag{11}$$

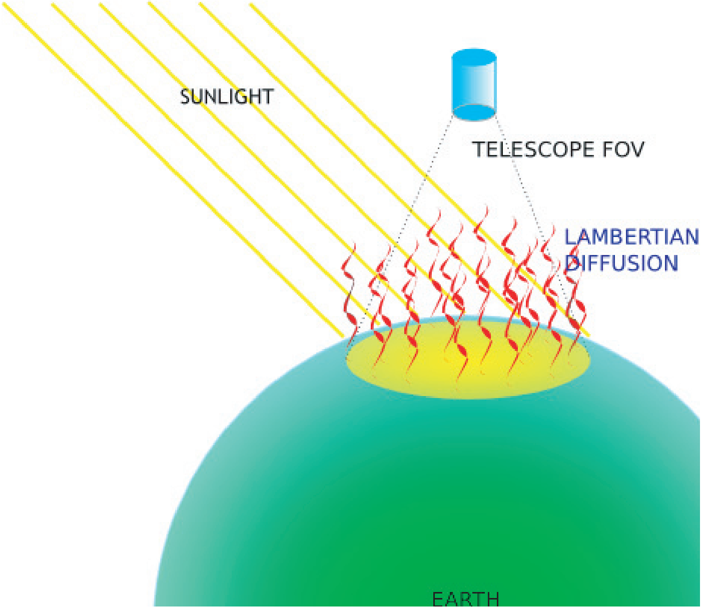

Figure 6. Scheme to calculate the background noise in the uplink. Sun (or Moon) light is reflected by the Earth surface (with Lambertian diffusion) into the receiving telescope field-of-view.

The number of background photons collected by the optical system per units of $\Delta\nu$ and Δt is

$$N_{\mathrm{day}} = \frac{1}{\pi} a_{\mathrm{E}} H_{\mathrm{sun}} \Sigma\Omega = a_{\mathrm{E}} r^2 (\mathrm{IFOV})^2 H_{\mathrm{sun}}. \tag{12}$$

2.2.2. Uplink (night-time operation). The dominant sources of background radiation from the Earth surface during night are its black-body emission, the reflected moonlight and the scattered light from human activities.

Let us start by calculating the radiance due to moonlight reflection on the Earth. Given the solar spectral irradiance H_{sun}, the number of photons per s and nm which hit the Moon's surface is: $H_{\mathrm{sun}} \cdot \pi R_{\mathrm{M}}^2$ where R_{M} is the Moon's radius. Assuming Lambertian diffusion, the number of photons s^{-1} nm^{-1} sr^{-1} reflected by the Moon is

$$\tilde{J}_{\mathrm{M}} = \frac{1}{\pi} a_{\mathrm{M}} H_{\mathrm{sun}} \pi R_{\mathrm{M}}^2, \tag{13}$$

where a_{M} is the Moon albedo. Assuming the Moon at normal incidence, the solid angle to the area on Earth Σ seen by the telescope is

$$\Omega_{\Sigma} = \frac{\Sigma}{d_{\mathrm{EM}}^2}, \tag{14}$$

where d_{EM} is the Earth–Moon distance. The spectral radiant intensity after Lambertian reflection from the Earth's surface is

$$J_{\mathrm{E}}^{(M)} = \frac{1}{\pi} a_{\mathrm{M}} \tilde{J}_{\mathrm{M}} \Omega_{\Sigma} = \frac{1}{\pi} a_{\mathrm{E}} a_{\mathrm{M}} R_{\mathrm{M}}^2 \frac{\Sigma}{d_{\mathrm{EM}}^2} H_{\mathrm{sun}}. \tag{15}$$

The number of photons per second and nm of bandwidth entering the receiving telescope (radius R, field-of-view IFOV) is

$$N_{\text{night}} = J_{\text{E}}^{(M)}\Omega = a_{\text{E}} a_{\text{M}} R_{\text{M}}^2 R^2 \frac{(\text{IFOV})^2}{d_{\text{EM}}^2} H_{\text{sun}} = \alpha N_{\text{day}}, \tag{16}$$

where

$$\alpha = a_{\text{M}} \left(\frac{R_{\text{M}}}{d_{\text{EM}}}\right)^2 \tag{17}$$

is the ratio between the background radiance at night-time (full Moon) and day-time. Assuming the Moon albedo to be $a_{\text{M}} \approx 0.12$ we have that α is of the order of 10^{-6}: during the night, in full Moon conditions, we have approximately a reduction of six orders of magnitudes in the amount of background noise.

As far as the Earth's black-body emission is concerned, according to Planck's law, the energy emitted at frequency ν by unit area, time, bandwidth and solid angle by a black body at temperature T is

$$I(\nu)\mathrm{d}\nu = \frac{2h\nu^3}{c^2} \frac{1}{\mathrm{e}^{h\nu/k_B T} - 1} \mathrm{d}\nu. \tag{18}$$

The spectral radiance (in photons $\mathrm{s}^{-1}\,\mathrm{m}^{-2}\,\mathrm{m}^{-1}\,\mathrm{sr}^{-1}$) as a function of the wavelength is

$$N_0(\lambda) = \frac{2c}{\lambda^4} \frac{1}{\mathrm{e}^{hc/\lambda kT} - 1}. \tag{19}$$

For $T = 293\,\mathrm{K}$, $\lambda = 800\,\mathrm{nm}$ and $\Delta\lambda = 1\,\mathrm{nm}$, $N_0 = 3.1 \times 10^6$ photons $\mathrm{s}^{-1}\,\mathrm{nm}^{-1}\,\mathrm{m}^{-2}\,\mathrm{sr}^{-1}$. The number of photons which enters the Earth-pointing telescope is, as before:

$$N_{\text{Planck}} = N_0 \Sigma \Omega \Delta\lambda. \tag{20}$$

For a telescope of radius $r = 15\,\mathrm{cm}$ and field-of-view $100\,\mu\mathrm{rad}$ the Earth's blackbody contribution is around 10^{-12} photons per ns and nm of bandwidth, at least three orders of magnitude less than that of moonlight.

As regards light pollution due to human activities, the amount of background photons collected depends strongly on the ground-station site. In the case of scientific experiments based on astronomical observatories located in remote regions very far from intense human lighting, this is not a problem. However, in the case of practical QKD systems connecting real world activities, the effect of light pollution at specific sites and at different wavelength must be assessed with good accuracy.

The expected number of background photons per second, nm of bandwidth and ns of gating window is plotted in figure 7. During the day around 10^{-1}–10^{-2} photons $\mathrm{s}^{-1}\,\mathrm{nm}^{-1}\,\mathrm{ns}^{-1}$ are expected, while at night-time (full Moon), the number is six order of magnitudes lower, around 10^{-7}–10^{-9} photons $\mathrm{s}^{-1}\,\mathrm{nm}^{-1}\,\mathrm{ns}^{-1}$.

2.2.3. Down-link. The background noise for a satellite-to-ground link was examined in detail by Miao *et al* [21]. The noise power P_{b} received by a ground-based telescope pointing at a satellite in the sky can be expressed as

$$P_{\text{b}} = H_{\text{b}} \Omega_{\text{fov}} \pi R^2 \Delta\nu, \tag{21}$$

where H_{b} is the brightness of the sky background in $\mathrm{W\,m}^{-2}\,\mathrm{sr}^{-1}\,\mu\mathrm{m}^{-1}$, Ω_{fov} the field of view of the telescope in sr and R its radius; $\Delta\nu$ is the filter bandwidth. H_{b} is strongly related to the weather conditions.

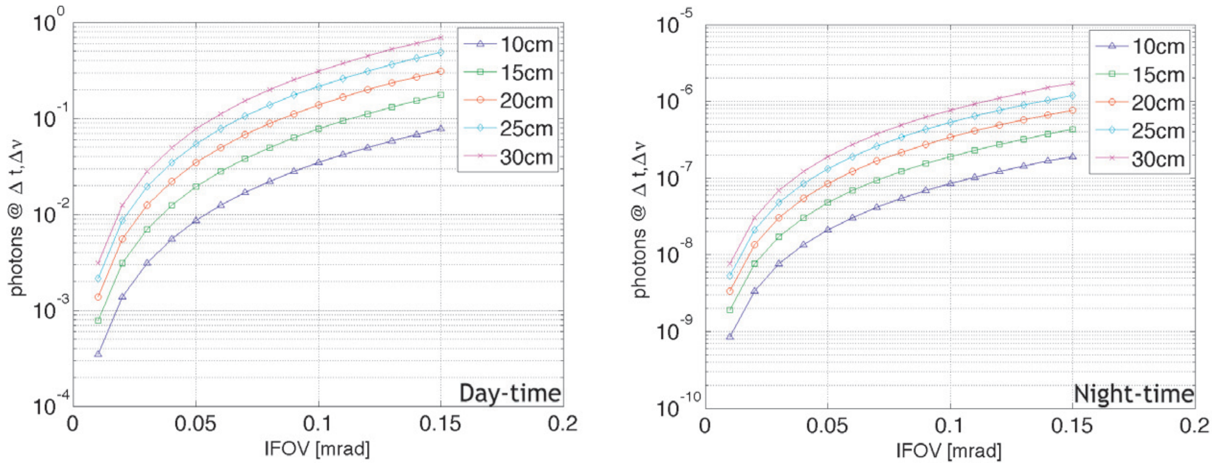

Figure 7. Number of photons in the day (left side) and at night-time (right side) as a function of telescope field-of-view for different values of the receiving telescope radius R. All simulations are performed for $\Delta\nu = 1$ nm and $\Delta t = 1$ ns. The number of background photons entering the telescope at night-time in full-Moon conditions is approximately six orders of magnitude smaller than the value for day-time operation.

2.3. SNR

In this paragraph we will study the SNR contribution, due to the signal and background noise count rate; we will therefore neglect the contribution due to imperfections in the quantum state transmission (i.e. problems in polarization maintenance), which will be addressed in the next section. Suppose we have a source emitting single photons in a channel with efficiency η given by (8). If the radius of the receiving telescope R is much smaller than the beam width w_{LT}, as is the case for the uplink (see figure 1), the signal at the telescope is

$$\epsilon_S = \eta \approx 2\eta_0 \frac{R^2}{w_{\mathrm{LT}}^2}. \tag{22}$$

Assuming to spectrally filter a bandwidth $\Delta\nu$ and to open the detector gate for a time Δt when a photon is expected to arrive, given N noise photons per second and nm of bandwidth, the number of noise photons is $\epsilon_{\mathrm{N}} = N\Delta\nu\Delta t$. From (12) and (16)

$$\epsilon_{\mathrm{N}} \propto R^2(\mathrm{IFOV})^2\Delta\nu\Delta t. \tag{23}$$

The SNR is

$$\mathrm{SNR} = \frac{\epsilon_S}{\epsilon_N} \propto \frac{\eta_0}{w_{\mathrm{LT}}^2(\mathrm{IFOV})^2\Delta\nu\Delta t}. \tag{24}$$

In the first approximation, the SNR does not depend on the radius R of the receiving telescope: for a larger telescope entrance area both the numbers of collected signal and noise photons increase consistently. The SNR is inversely proportional to the beam area, the telescope field-of-view, the filter bandwidth and the gating window of the detector.

Results for the uplink are shown in figure 8 for day-time and night-time operation, assuming $\Delta\nu = 1$ nm and $\Delta t = 1$ ns. In the case of day-time operation the SNR is much less than one (around $1:10^4$), implying that a sufficient SNR is not within reach, even improving

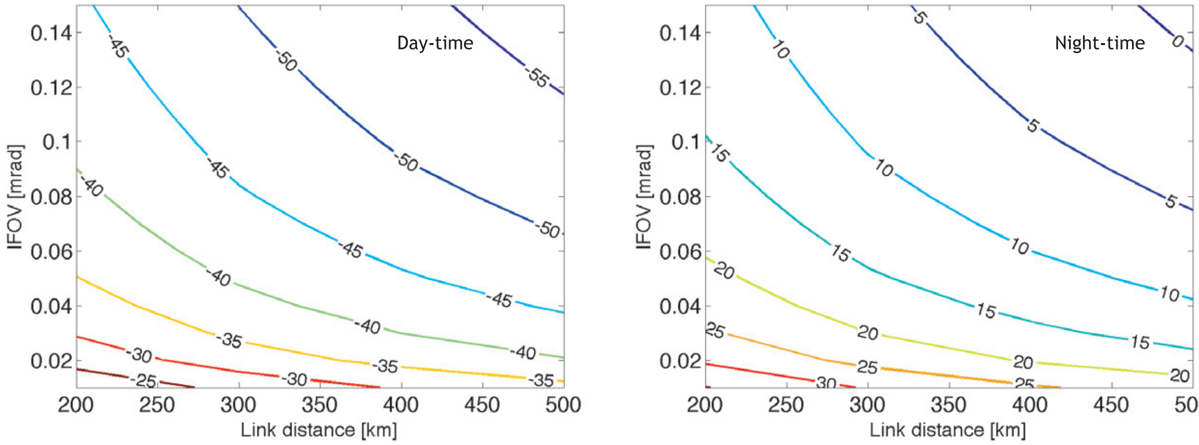

Figure 8. SNR (in dB) at day-time (left side) and night-time (right side) as a function of telescope field of view and satellite distance for the uplink. The curves on the left sign show negative values (in decibels), corresponding to a SNR lower than 1. This is clearly too low to establish a quantum communication link. On the other hand, SNR as high as 100 : 1 or 1000 : 1 can be envisaged during night-time. The operating wavelength is $\lambda = 800$ nm and the transmitting telescope diameter is 1.5 m. We assume a filtering bandwidth $\Delta\nu = 1$ nm and a gating time of $\Delta t = 1$ ns for the detectors.

the temporal and spectral filtering. On the other hand, at night-time (full Moon conditions), a SNR of the order of 10 : 1 can be obtained and can be further improved acting on the filter bandwidth and on the telescope field-of-view.

We calculated the SNR for the downlink using our results for the signal attenuation in a turbulent atmosphere and the noise parameters given in [21]. The results are shown in figure 9. On the left-hand side, the down-link attenuation is shown as a function of the link distance L and the radius r_T of the satellite-based transmitting telescope. Two factors result in an increased performance for the downlink with respect to the uplink. Firstly, on Earth we can have larger receiving telescopes than in space. Secondly, the beam first propagates in the vacuum with just diffraction spreading and is in contact with the turbulent atmosphere only in the final stage of propagation. Therefore the aberrations introduced by turbulence only affect weakly the wavefront before it enters the telescope.

On the right-hand side of figure 9, we plotted the SNR as a function of the sky brightness ($\Delta\nu = 1$ nm). The SNR is greater than one only at night-time.

3. Polarization control

A second crucial point for the implementation of quantum communication schemes based on polarization-encoded qubits is, of course, the preservation of polarization states in the channel.

As was shown in [22], propagation in the atmosphere does not affect significantly the polarization states, nor does the Faraday effect due to the Earth's magnetic field. This was experimentally confirmed in a recent experiment [23] where an entangled photon pair

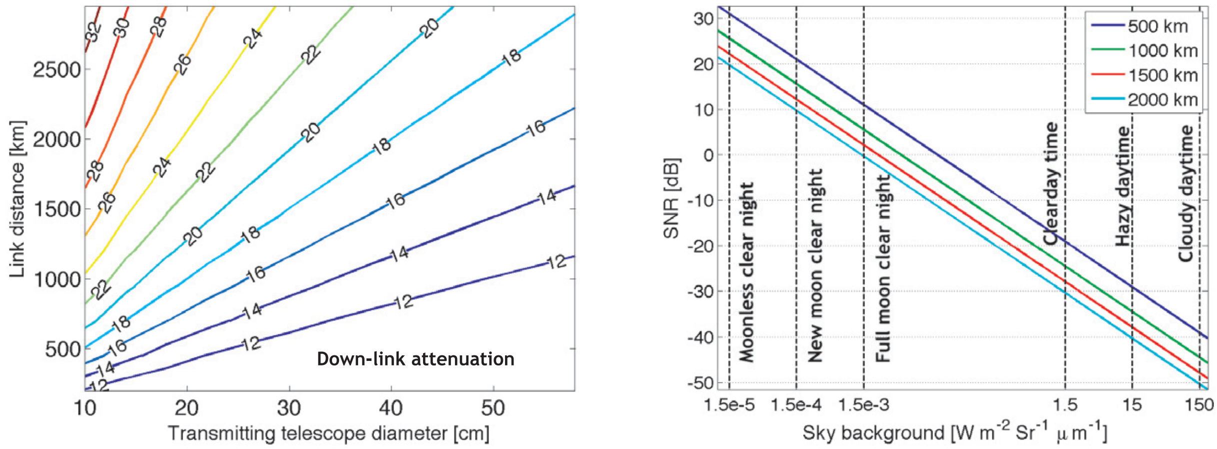

Figure 9. Simulations for the downlink. On the left-hand side, link attenuation (in dB), as a function of the diameter of the satellite-based transmitting telescope and of the link distance L. On the right-hand side, SNR of the link as a function of the sky background noise for different link distances, assuming a diameter of the transmitting telescope $r_T = 15$ cm. All simulations are performed assuming a diameter of the Earth-based receiving telescope $R = 1.5$ m, with field-of-view 0.016° (corresponding to MLRO, Matera).

was shown to violate Bell inequalities after propagating through a 144 km free-space link, demonstrating that the propagation through the atmosphere does not induce decoherence on polarization-encoded photonic qubits. The use of curved optics in an off-axis configuration introduces some spatially dependent polarization effects [24], which can lead to global decoherence of the polarization-encoded qubits. However, the effect is small for on-axis optics and it can be neglected, just having some care in the design of optical systems.

On the other hand, the relative motion of the satellite and the ground station induces a time-dependent transformation on the polarization state as seen by the receiver [22]. Consider, for example, a source on a satellite which emits a stream of single photons, directed to ground by a moving pointing mirror (see figure 10). A second pointing mirror on the ground receives the photons and whatever direction they come from, it sends them to the detection apparatus. Due to the relative motion between the satellite and the ground station, there is a relative rotation of the polarization axes between satellite and ground. Moreover, the movement of the pointing mirrors changes the incidence angles over time, resulting in a variation of the reflection Fresnel coefficients

$$\begin{aligned} r_s(\lambda, \theta_i) &= \frac{\cos\,\theta_i - n(\lambda)\cos\,\theta_t}{\cos\,\theta_i + n(\lambda)\cos\,\theta_t}, \\ r_p(\lambda, \theta_i) &= \frac{\cos\,\theta_t - n(\lambda)\cos\,\theta_i}{\cos\,\theta_t + n(\lambda)\cos\,\theta_i}, \end{aligned} \tag{25}$$

where $n(\lambda)$ is the surface refractive index, θ_i is the incidence angle and $n(\lambda)\sin\theta_t = \sin\theta_i$. The effect, in the case of a single passage of a LEO satellite orbiting at 400 km from the Earth surface, is shown in figure 11. Given a photon which is emitted with polarization orthogonal to the orbit plane vertical-polarization in the satellite reference frame, the evolution of the Stokes

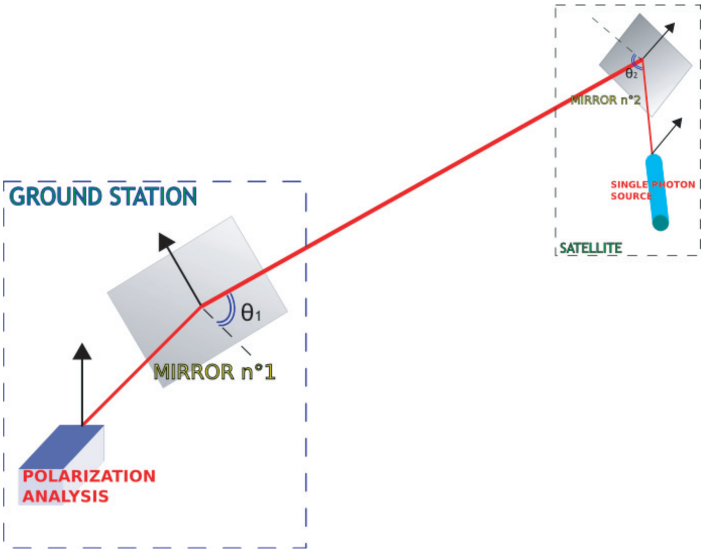

Figure 10. Scheme of the satellite tracking system and its effect on polarization, as discussed in [22].

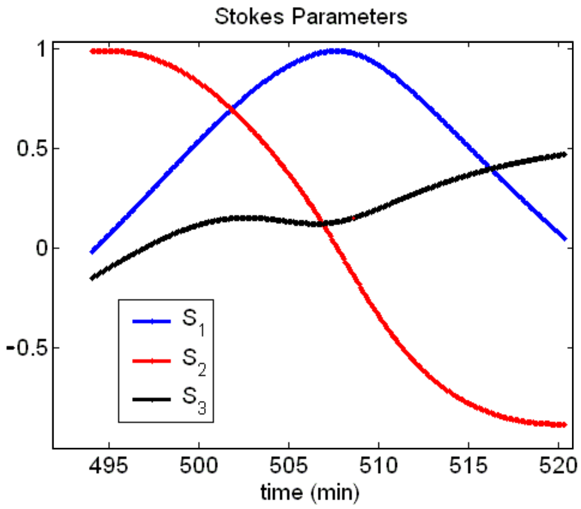

Figure 11. Example of temporal evolution of the Stokes parameters at the receiver for a fixed vertically polarized state (electric field orthogonal to the satellite orbit) emitted on the satellite. In a few minutes passage the values of the Stokes parameters change dramatically in a smooth way.

parameter seen by the ground-based receiver is plotted as a function of time. The transformation of the polarization state received on ground is dramatic; therefore a characterization of the channel and a compensation technique is needed.

If we can neglect channel depolarization effects, as is the case for atmospheric propagation, polarization states can be represented by normalized Jones vectors

$$\begin{bmatrix} A \\ B\mathrm{e}^{\mathrm{i}\varphi} \end{bmatrix}, \qquad A, B, \varphi \in R, \qquad A^2 + B^2 = 1. \tag{26}$$

The channel properties are described by a 2×2 time-dependent Jones matrix $C(t)$, which transforms the polarization states according to $J(t) = C(t)J_0$. To establish a successful quantum link based on polarization-encoded qubits, such transformation must be compensated. This can be done characterizing the channel without interfering with the single-photon exchange, in order to measure such matrix $C(t)$. Then, applying the inverse transformation $C^{-1}(t)$ for every time instant t to the incoming photons, the correct state can be restored before detection.

However, in general, not to interfere with the single photon exchange, the characterization of the channel Jones matrix is to be performed with different parameters than the photon exchange. For example, a different wavelength may be employed, or the two operations of channel-probing and quantum communication can be performed in different time-slots. Defining $C_\mathrm{P}(t)$ as the experimentally measured channel Jones matrix, we have

$$C_\mathrm{P}^{-1}(t)C(t) = E(t). \tag{27}$$

In the case of ideal compensation, $E(t)$ will be the identity matrix.

In this section, we will examine some polarization-compensation schemes, discussing their effectiveness in the case of the model presented in [22]. This is just one of the possible configurations of the optical link. For example, one could envisage a scheme in which the receiver rotates together with the receiving telescope, removing the need for a second pointing mirror: in this situation the expected polarization change is reduced. However, here we concentrate in the configuration with two moving mirrors, to show that a compensation is possible in the worst case.

Consider photons transmitted in two non-orthogonal bases, for example, the horizontal/vertical one (states $|H\rangle$ and $|V\rangle$) or the diagonal one (states linearly polarized at ±45°, that we will indicate, respectively, with $|+\rangle$ and $|-\rangle$). The average error probability is

$$P_\mathrm{E} = 1 - P_\mathrm{HH} - P_\mathrm{VV} - P_{++} - P_{--}, \tag{28}$$

where P_{ij} is the temporal average of the conditional probability of measuring the state i once j has been transmitted ($P_{ij} = \langle p(r = i|t = j) \cdot p(t = j)\rangle$). The *a priori* probability of transmitting each of the states is equal for all the states

$$p(t = j) = \tfrac{1}{4}, \qquad j = \mathrm{H, V, +, -} \tag{29}$$

Suppose, for example, to have a horizontally polarized state, parallel to the satellite orbit, transmitted at time t_i. After compensation, the state at the receiver is

$$J(t_i) = \begin{bmatrix} E_{11}(t_i) & E_{12}(t_i) \\ E_{21}(t_i) & E_{22}(t_i) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} E_{11}(t_i) \\ E_{21}(t_i) \end{bmatrix}, \tag{30}$$

so that the probability of obtaining the correct result is $|E_{11}(t_i)|^2$. Therefore

$$P_\mathrm{HH} = \tfrac{1}{4}\left\langle |E_{11}|^2 \right\rangle. \tag{31}$$

With similar arguments one can find expressions for the other conditional probabilities so that

$$P_\mathrm{E} = 1 - \tfrac{1}{8}\langle\{3|E_{11}|^2 + 3|E_{22}|^2 + |E_{21}|^2 + |E_{12}|^2 + E_{11}^*E_{22} + E_{11}E_{22}^* + E_{12}^*E_{21} + E_{12}E_{21}^*\}\rangle. \tag{32}$$

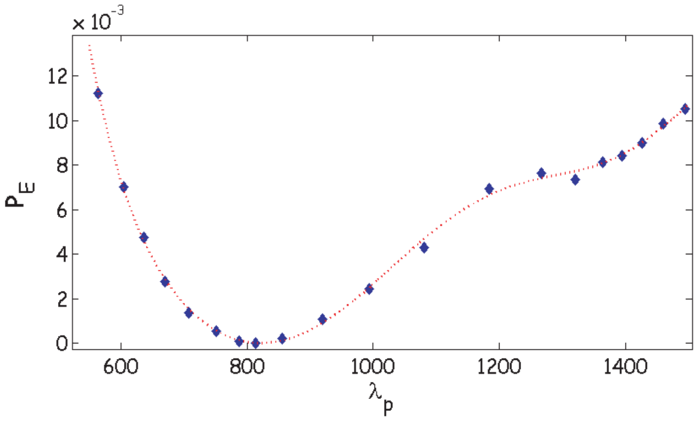

Figure 12. Polarization-state preservation in the satellite-based quantum channel, in the case of a channel-probing beam at a different wavelength with respect to the signal. The bit error rate due to imperfect compensation is negligible even for probing wavelengths quite far from the signal one ($\lambda_s = 800\,\text{nm}$).

3.1. Probe beam at a different wavelength

One possible way of measuring the channel Jones matrix without perturbing the single-photon exchange is using a probe beam at a wavelength λ_p different from the one of the signal beam (λ_s). In this case, the signal transformation Jones matrix is $C(\lambda_s)$, while the compensation matrix is $C(\lambda_p)$. Therefore

$$E = C^{-1}(\lambda_p)C(\lambda_s). \tag{33}$$

To have a statistical evaluation of the degree of compensation that can be achieved with this technique we performed a simulation for 1000 passages of a LEO satellite orbiting at 500 km. We used the model described in [22] to calculate the matrices $C(\lambda_s)$ and $C(\lambda_p)$ for a uniform temporal sampling of each passage ($\Delta t = 1$ s). Then we computed for each time the matrix E and the error probability P_E, finally averaging over time. The results are reported in figure 12, showing the probability error P_E due to imperfect polarization compensation as a function of λ_P. Perfect compensation is possible using a wavelength for the probe beam very close to that of the signal beam. However, an acceptable error rate (below 1%) is possible for wavelengths much more distant from the signal one.

3.2. Time-multiplexing of signal and probe beam

A different compensation scheme can be time-multiplexing of signal and probe pulses at the same wavelength in the channel. In this case, suppose to send the probe pulses with repetition rate f_P, so that the mth probe pulse will be emitted at time $t_m = mT_0$ with $T_0 = 1/f_P$. Between any two probe pulses, N single-photon pulses will be transmitted, each at the time $t_{imi,i} = t_m + i\delta$, where $i = 0, \ldots, N$ and $\delta = T_0/(N+1)$. In other words, we measure the channel Jones matrix $C(t_m)$ and use it to compensate N subsequent single-photon pulses

$$J\,(t_m + i\delta) = C^{-1}(t_m)J_0\,(t_m + i\delta)\,. \tag{34}$$

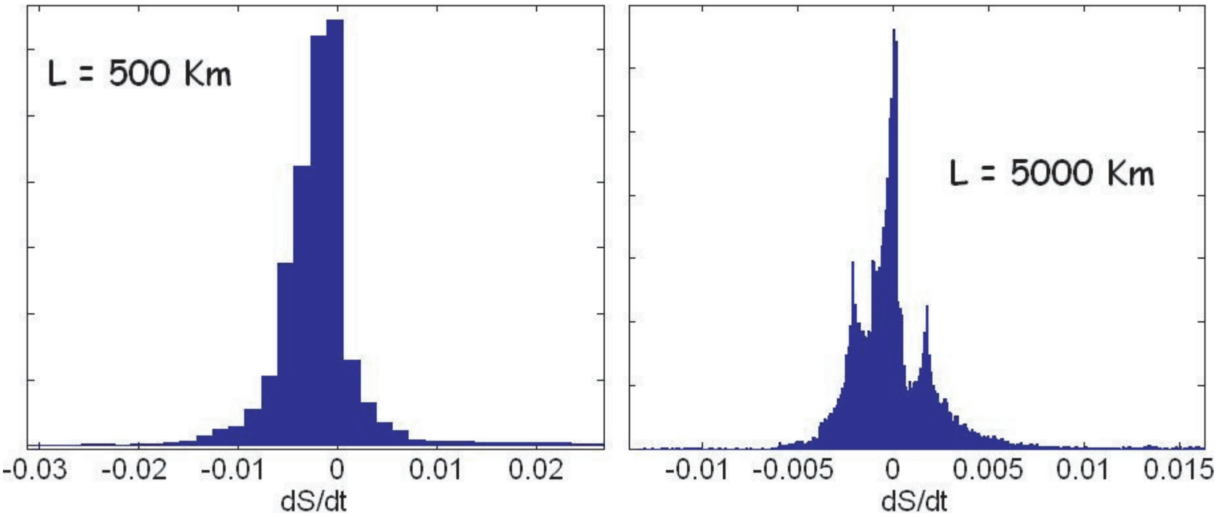

Figure 13. Statistics of the time-derivative of the Stokes parameter S_2 for 1000 passages of two satellites with different orbits (500 km for the picture on the left, 5000 km for the one on the right). The temporal evolution of the transformation is faster for the lower orbit satellite (the absolute value of the time derivative is within 0.015 s^{-1}). For the higher satellite the transformation is slower (within 0.005 s^{-1} for the figure on the right).

The repetition rate of such pulses must be fast enough to characterize in real-time the evolution of the channel properties. Assuming that this is the case, the amount of change for a Stokes parameter $S_j(t)$ where $j = 1, \ldots, 3$ at a time Δt slightly after t_m is small and can be expressed with a Taylor expansion to the first order

$$\Delta S_j(t_m) = S_j(t_m + \Delta t) - S_j(t_m) \approx \left.\frac{\mathrm{d}S_j}{\mathrm{d}t}\right|_{t=t_m} \Delta t. \tag{35}$$

If we want to keep the error on $\Delta S_j(t)$ under a certain value $\Delta S_{\max}$, the repetition rate of the probing pulses must be:

$$f_{\mathrm{P}} \geqslant \frac{1}{\Delta S_{\max}} \left.\frac{\mathrm{d}S}{\mathrm{d}t}\right|_{\max}. \tag{36}$$

Assuming a maximum value for the time-derivative of the Stokes parameters of 0.02 (see figure 13), and stating for the maximum acceptable error on the Stokes parameters $\Delta S_{\max} = 10^{-5}$, we get a value of $f_{\mathrm{P}} = 2$ kHz for the probe repetition rate. This value is a large bound on the error, since $|\mathrm{d}S/\mathrm{d}t|$ is in general much smaller than the maximum value we took.

The average error probability can be statistically evaluated performing some simulations similar to what we did for the different-wavelengths scheme. In this case, we computed the probability error as a function of the repetition rate of the probe pulses. The results are shown in figure 14, for three values of the satellite distance ($L = 200$, 500 and 1000 km). Increasing the repetition rate f_{P} of the compensation pulses the error probability decreases. Very low QBER values can be obtained with a reasonably slow compensation rate (with $f_{\mathrm{P}} = 1$ Hz we can get an error probability around 10^{-3}–10^{-4}). This indicates that the higher bound for the repetition rate we had found using the maximum temporal derivative of the Stokes parameter is at least

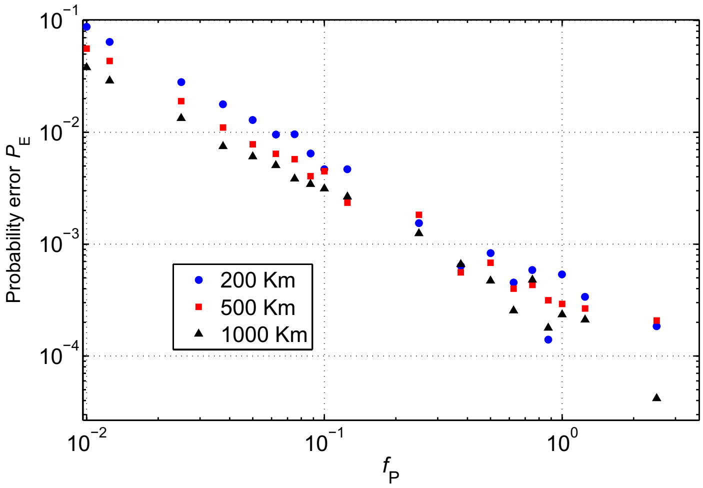

Figure 14. Simulated error probability P_{E} due to imperfect polarization compensation in the case of a temporal-multiplexing scheme, as a function of the channel-characterization pulses repetition rate. Data are shown for satellites at different altitudes.

a couple of orders of magnitude larger than its real value. Higher QBER is obtained for lower orbit satellites, since their orbit time is shorter and the polarization evolution is faster.

4. Discussion

In this section, we will analyze the possibility of establishing a quantum key distribution link in different configurations employing a LEO satellite and an optical ground station, for different protocols. Throughout the whole section, formulae for key-generation rate in the asymptotic limit of a long key will be employed. This is not true for real world QKD experiments, in particular for links between a LEO satellite and Earth which have a very limited duration (a few minutes at best) and high channel attenuation. The analysis of the security of quantum key distribution for finite key lengths is a recently developed area in quantum information science: a brief discussion of its implication for satellite-based QKD will be given in section 4.2.

4.1. BB84

The secret key rate per pulse for the BB84 protocol in the case of an ideal single-photon source is

$$R_{\mathrm{BB84}}^{(\mathrm{ideal})} \geqslant \frac{S}{2}\left[1 - f(e)H_2(e) - H_2(e)\right], \qquad (37)$$

where S is the probability that a non-empty pulse is detected by Bob, e is the QBER, $f(e)$ is the efficiency of error correction and $H_2(x)$ is the binary entropy function: $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$. The efficiency of the classical error correction algorithm is described by the factor $f(e)$: we take $f(e) \approx 1.22$.

In most practical quantum communication experiments, single photons are implemented with weak coherent pulses, for which there is a nonzero probability to produce multiphoton states. On such multiphoton pulses Eve could perform a photon-number-splitting (PNS) attack [25]–[27]. She can split a photon from the multiphoton pulse, store it and measure it in the correct basis after Alice and Bob have publicly announced their bases. If she sends the rest of the multiphoton pulse to Bob no noise will be introduced in the channel and she can get complete information about the bit without being discovered. Such bits, that have leaked information to the eavesdropper, are called tagged bits. Inamory *et al* [28] and Gottesmann *et al* [29] showed that in this situation a secure key can still be distilled and the key generation rate is given by

$$R_{\mathrm{BB84}} \geqslant \frac{S}{2}\left[(1-\Delta) - f(e)H_2(e) - (1-\Delta)H_2\left(\frac{e}{1-\Delta}\right)\right]. \tag{38}$$

In the case of an uplink to a LEO satellite the channel is extremely lossy and almost all the single-photon pulses may be wasted, resulting in basically only multiphoton pulses being detected by Bob. Therefore, increasing the channel losses, the fraction of secure bits decreases. If the losses are so strong that only multiphoton pulses are detected by Bob, no secure key can be generated.

As a worst-case estimate of the fraction of tagged bits Δ we can take the fraction of multiphoton pulses over the fraction of non-empty pulses detected by Bob [26]

$$\Delta \approx \frac{1-\mathrm{e}^{-\mu}-\mu\mathrm{e}^{-\mu}}{1-\mathrm{e}^{-\eta\mu}}. \tag{39}$$

In general, given a link attenuation η the key generation rate is of the order of $O(\eta^2)$ (see [30]).

Simulations for the key generation rate as a function of the link distance are shown in figure 15. In the case of the uplink the attenuation is so high that the secure key generation rate is extremely low (of the order of 10^{-12}), on the other hand it is not possible to increase the value of μ in order to avoid PNS attacks.

For the downlink, on the contrary, a successful establishment of a BB84 QKD link is possible. Assuming $\mu = 0.01$ (see figure 15) and a source repetition rate of 10 MHz, for a satellite at 500–600 km we can get around 1 kbit of secure key per second.

4.2. Decoy-state

To improve the performance of coherent-state weak-pulse QKD, the decoy state method has been heuristically proposed [31]–[33]. For BB84 protocol, the security analysis is performed using a worst-case estimate on the fraction of bits that are known to the eavesdropper. The decoy-state technique, on the other hand, exploits states with different light intensities to probe the channel transmissivity and error probability, giving a more accurate bound on the amount of tagged bits.

Suppose to use a three-state decoy technique, which exploits vacuum states and two coherent states with mean photon number μ and μ'. Let S_μ be Bob's counting rate when Alice transmits pulses with mean photon number μ and S_0 be Bob's counting rate in the case of vacuum-state transmission (therefore due to dark counts and background noise). The bound for Δ is [30]:

$$\Delta \leqslant \frac{\mu}{\mu'-\mu}\left(\frac{\mu\mathrm{e}^{-\mu}S_{\mu'}}{\mu'\mathrm{e}^{-\mu'}S_\mu} - 1\right) + \frac{\mu\mathrm{e}^{-\mu}S_0}{\mu' S_\mu}. \tag{40}$$

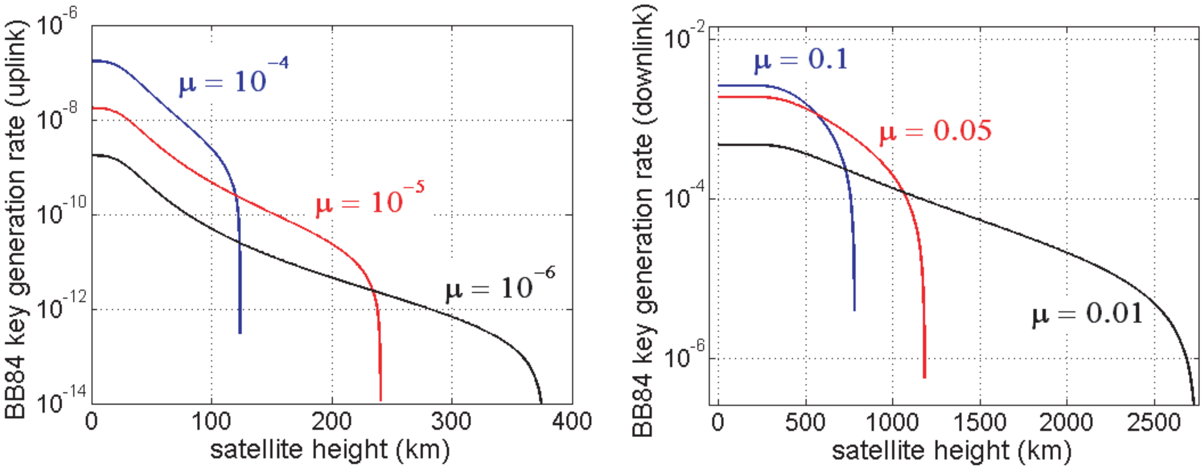

Figure 15. Key generation rate for the BB84 protocol using weak laser pulses as an approximate single-photon source. On the left-hand side, results for the up-link, in the right-hand side results for the downlink. For the uplink, the channel attenuation is so high that a QKD session with significant key generation rates cannot be implemented, while for the downlink a key generation rate of 10^{-4} for a satellite orbiting at around 500 km can be obtained using a source with mean photon number $\mu = 0.01$.

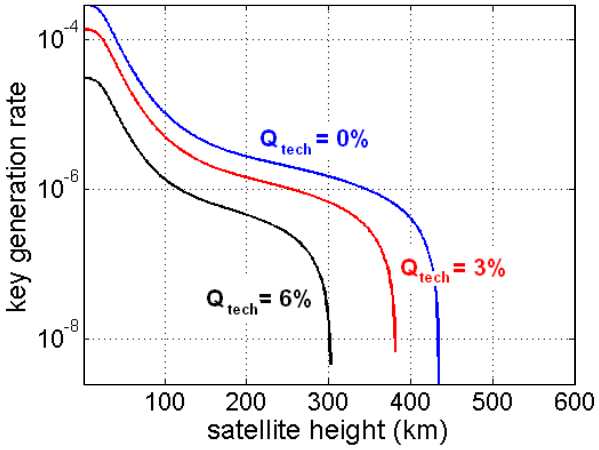

Figure 16. Key generation rate for the BB84 protocol using a three-level decoy-state protocol (vacuum, $\mu = 0.27$, $\mu' = 0.4$) for different values of the technical QBER. A secure key rate of 10^{-6} can be obtained for an uplink to a satellite orbiting at around 400 km (in the case of $Q_{\mathrm{tech}} = 0$).

Probing the channel with different light intensities we can get a more accurate estimate of Δ. Consequently, we can guarantee unconditional security without reducing the mean photon number of the pulses too much.

In figure 16, we show some simulations performed for a three-state decoy method, which employs the vacuum and two coherent-beam intensities $\mu = 0.27$ and $\mu' = 0.4$. For the QBER we summed the expected contribution due to spurious events (as calculated in the previous sections) to a technical QBER (Q_{tech}) due to alignment errors and imperfection in the polarization analyzers. The order of magnitude of Q_{tech}, taken from [13], is around 3–4%. The key generation rate, as a function of the uplink distance L is plotted for three different values of the technical QBER (Q_{tech}). Clearly there is a significant improvement in the key generation rate, from $O(\eta^2)$ to $O(\eta)$. For a source repetition rate of 10 MHz, in the case of an uplink to a satellite at 400 km, we would still be able to get a key generation rate of 10 bps, as compared with the value of 10^{-5} bps one would get for the BB84 protocol with no decoy states.

The cut-off distance, beyond which no key generation is possible, is around 400 km with no technical QBER. Such distance reduces to around 350 km for $Q_{\mathrm{tech}} \approx 3\%$ and to less than 300 km for $Q_{\mathrm{tech}} \approx 6$ percent. Therefore decoy-state technique can help in the establishment of a quantum key distribution uplink to a satellite, but only for very low-altitude orbits (not more than 400 km).

The main problem in the practical implementation of the decoy-state technique in a satellite link is the unavoidable intensity fluctuations in the channel due to the fast relative motion of the communication terminals and to scintillation effects.

In general, two distinctive features of satellite-based links are the low link efficiency η and the short duration, which result in a short expected key length. The infinite-key assumption is not valid and security proofs for finite key size QKD are of great importance. Recently, Scarani and Renner [34] showed that at least $\sim 10^5$ signals need to be exchanged and processed for BB84 with one-way post-processing in order to get a nonzero key generation rate. In general, a LEO satellite is visible from a ground-station for a few minutes. For example, assuming a link duration of 200 s, to reach the 10^5 signal photons limit, an average key generation rate of around 500 bps must be ensured. In the case of a BB84 downlink, with a key generation rate of 10^{-4}, a transmission frequency of at least 5 MHz is needed. On the other hand, in the case of a decoy-state BB84 uplink, with a key generation rate of 10^{-6} the situation is much more demanding: a transmission frequency of 500 MHz is required to guarantee unconditional key security.

4.3. Entangled photons

A detailed analysis of the conditions to violate Bell inequalities and implement a quantum key distribution experiment based on Ekert's protocol has been presented in [20]. As a minimum requirement, they assume the SNR needed to violate a Bell inequality [35]. For the case of polarization-entangled photons this necessitates a coincidence visibility of at least 71%, corresponding to a SNR of 6 : 1. Below that ratio it is possible to model the observed correlation with a local realistic theory, allowing unobserved eavesdropping.

The rate of accidental coincidences is

$$C_{\mathrm{acc}} = N_1 N_2 \Delta t, \tag{41}$$

where N_1 and N_2 are the count rates for the detectors due to background noise and dark counts. The rate of good coincidences is

$$C = P_0 \eta_1 \eta_2, \tag{42}$$

where η_i is the efficiency of the link i. In our simulations, we used the link efficiencies and the noise values calculated in section 2 for satellite links and $\eta_i \approx 0.5$ in the case of local detection. In the latter case, we assume as photon noise the detector dark counts ($N_i \approx 200$ counts per second). P_0 is the emission rate of the entangled-photon pairs: values of the order of 10^6–10^7 pairs per second are currently available using for examples periodically poled nonlinear crystals.

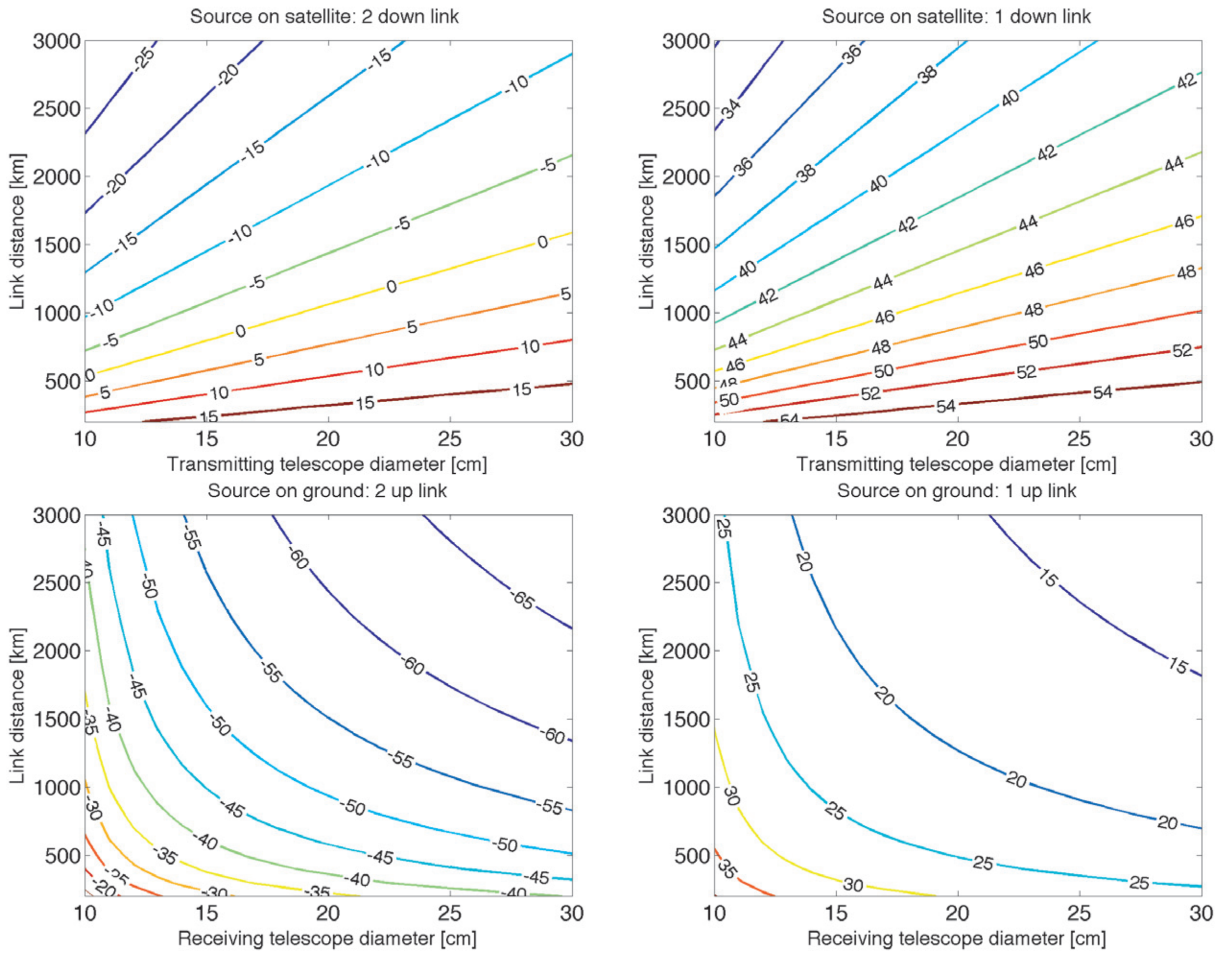

Figure 17. SNR (in dB) for entanglement-based experiments in different configurations. For all the simulations, the diameter of the Earth-based telescope used either in transmitting or receiving mode, is assumed to be 1.5 m. The detector gating window is 1 ns and the spectral filtering bandwidth is 1 nm.

We consider four different scenarios:

- the source is on the satellite, with two ground receivers (the scheme proposed for the SpaceQUEST experiment [36]);
- source on the satellite, with one local receiver and the other on the ground;
- source on the ground, with two satellite-based receivers;
- source on the ground with one local receiver and the other on satellite.

All simulations were performed for night-time new Moon conditions. The results are shown in figure 17. Entanglement-based experiments with one photon measured locally at the source and the other one propagating either in the uplink or downlink are feasible, due to sufficient SNR. On the other hand a ground-based source with two satellite uplinks is unfeasible. The situation with a source on the satellite and two Earth-based receiving telescopes is feasible, but only under some stringent requirements on the experimental parameters (telescope diameter, link distance, filtering, etc).

Even in the case of entanglement-based QKD, the available sources are not exactly sources of single-photon pairs. For example, in the case of spontaneous parametric downconversion, the probability to get an $n-$photon pair is [36]:

$$P(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}, \tag{43}$$

where $\lambda = \sinh^2\chi$ and χ is the second-order nonlinear coefficient of the SPDC crystal. Therefore, as in the case of coherent-state QKD, the key generation rate is limited by the channel attenuation.

Ma *et al* [37] performed an interesting analysis of the key generation rate one can achieve for entanglement-based QKD using a parametric downconversion source. Performing simulations with the parameters of the experiments performed in the Canary Islands [10] (repetition rate 249 MHz, $\eta_{\text{Alice}} = 0.14$, $\eta_{\text{Bob}} = 0.14$, $e = 0.015$ and $Y_0 = 6.02 \times 10^{-6}$) showed that the maximum tolerable link loss is around 60 dB. This limit can be increased to 70 dB when applying post-processing with two-way classical communication. If statistical fluctuations due to finite-size key are considered, the maximum link attenuation is reduced to around 50 dB.

This makes the establishment of an entanglement-based QKD uplink problematic, since the single channel losses for a LEO satellite are around 50–70 dB. On the other hand, the establishment of a down-link both in the single and in the double channel case seems within reach.

5. Conclusions

In this paper we discussed some aspects of the feasibility of satellite-based quantum key distribution which we believe were not yet well addressed in the literature.

Firstly, we discussed signal propagation through a turbulent atmosphere, refining the models presented in [20, 38]. In particular, for the uplink, we analyzed the relative contribution of beam spreading and wandering, showing that the former is more important than the latter for low-altitude satellites. Then we introduced a model for the background noise of the channel during night-time and day-time, and we discussed the SNR for different configurations.

Secondly, we discussed the polarization properties of a satellite-based quantum channel, discussing two possible compensation techniques for the effects illustrated in [22]. For both techniques (channel-probing at a different wavelength and time-multiplexing of signal and probe pulses at the same wavelength) we showed that the bit error rate can be kept at really low levels.

Finally we discussed the generation rate of a secure key for different configurations and for different protocols. For the standard BB84 protocol (with Poissonian-distributed source) we showed that a QKD link can be established for the downlink with a good generation rate, but not for the uplink. On the other hand, a QKD uplink can be realized with the more accurate estimate of the fraction of bits for which an eavesdropper could have complete information without introducing any disturbance, provided by the decoy-state techniques. Two points are still not sufficiently clear: the effect of the finite duration of the satellite link to the secure key generation and the possibility of implementing the decoy-state technique in a channel with strong and random intensity fluctuations. We also discussed the implementation of entanglement-based links, showing that configurations with one photon detected locally at the source and one propagating either in uplink or in downlink are feasible with realistic experimental parameters.

The situation with a source on satellite and two ground-based receivers is also feasible, but with particular care on the choice of the relevant hardware parameters.

In conclusion, satellite-based quantum key distribution is certainly feasible with present technology. We believe that space technology can provide a rich environment for experiments on foundational quantum mechanics and on quantum-information applications.

Acknowledgments

We thank Dr Enrico Grisan of DEI—University of Padova for the help in the image analysis, Professor Cesare Barbieri, Professor Gianfranco Cariolaro, Dr Ivan Capraro, Dr Tommaso Occhipinti, Dr Fabrizio Tamburini, Dr Gabriele Anzolin and Ing. Filippo Ratti of University of Padova for helpful discussions. This work has been carried out within the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[2] Bouwmeester D, Ekert A and Zeilinger A 2000 *The Physics of Quantum Information* (Berlin: Springer)

[3] Jaeger G 2006 *Quantum Information: An Overview* (Berlin: Springer)

[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95

[5] Sergienko A V 2005 *Quantum Communication and Cryptography* (Boca Raton, FL: CRC Press)

[6] Lo H-K and Zhao Y 2008 Quantum cryptography arXiv:0803.2507

[7] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9

[8] Kaye P, Laflamme R and Mosca M 2007 *An Introduction to Quantum Computing* (New York: Oxford University Press)

[9] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors *Nat. Photonics* **1** 343–8

[10] Ursin R *et al* 2007 Entanglement based quantum communication over 144 km *Nat. Phys.* **3** 481–6

[11] http://www.secoqc.net/

[12] Peng C-Z *et al* 2005 Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication *Phys. Rev. Lett.* **94** 150501

[13] Schmitt-Manderbach T *et al* 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98** 010504

[14] Villoresi P *et al* 2008 Experimental verification of the feasibility of a quantum channel between space and earth *New J. Phys.* **10** 033038

[15] Fante R 1975 Electromagnetic beam propagation in turbulent media *Proc. IEEE* **63** 1669–2

[16] Fante R 1980 Electromagnetic beam propagation in turbulent media: an update *Proc. IEEE* **68** 1424–43

[17] Andrews L C, Philips R L and Yu P T 1995 Optical scintillation and fade statistics for a satellite-communication system *Appl. Opt.* **34** 7742–5164

[18] Dios F, Rubio J A, Rodriguez A and Comeron A 2004 Scintillation and beam-wander analysis in an optical ground station-satellite uplink *Appl. Opt.* **43** 3866–73

[19] Toyoda M 2005 Intensity fluctuations in laser links between ground and a satellite *Appl. Opt.* **44** 7364

[20] Aspelmeyer M, Jennewein T, Pfennigbauer M, Leeb W R and Zeilinger A 2003 Long distance quantum communication with entangled photons using satellites *IEEE J. Sel. Top. Quantum Electron.* **9** 1541

[21] Miao E-L, Han Z-F, Gong S-S, Zhang T, Diao D-S and Guo G-C 2005 Background noise of satellite-to-ground quantum key distribution *New J. Phys.* **7** 215

[22] Bonato C, Aspelmeyer M, Jennewein T, Pernechele C, Villoresi P and Zeilinger A 2006 Influence of satellite motion on polarization qubits in a space–Earth quantum communication link *Opt. Express* **14** 10050–9

[23] Fedrizzi A, Ursin R, Herbst T, Nespoli M, Prevedel R, Scheidl T, Tiefenbacher F, Jennewein T and Zeilinger A 2009 High-fidelity transmission of entanglement over a high-loss free-space channel arXiv:0902.2015

[24] Bonato C, Pernechele C and Villoresi P 2007 Influence of all-reflective optical systems in the transmission of polarization-encoded qubits *J. Opt. A: Pure Appl. Opt.* **9** 899

[25] Dusek M, Haderka O and Hendrych M 1999 Generalized beam-splitting attack in quantum cryptography with dim coherent states *Opt. Commun.* **169** 103

[26] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography *Phys. Rev. Lett.* **85** 1330–3

[27] Luetkenhaus N 2000 Security against individual attacks for realistic quantum key distribution *Phys. Rev.* A **61** 052304

[28] Inamori H, Luetkenhaus N and Mayers D 2001 Unconditional security for practical quantum key distribution *Eur. Phys. J.* D **41** 599 (arXiv:quant-ph/0107017)

[29] Gottesmann D, Lo H-K, Luetkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Quantum Inf. Comput.* **4** 325–60

[30] Wang X-B, Hiroshima T, Tomita A and Hayashiv M 2007 Quantum information with gaussian states *Phys. Rep.* **448** 1–111

[31] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901

[32] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504

[33] Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503

[34] Scarani V and Renner R 2008 Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing *Phys. Rev. Lett.* **100** 200501

[35] Fuchs C A, Gisin N, Griffiths R B, Niu C-S and Peres A 1997 Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy *Phys. Rev.* A **56** 1163–72

[36] Ursin R *et al* 2008 Space-quest: experiments with quantum entanglement in space arXiv:0806.0945v1

[37] Ma X, Fred Fung C-H and Lo H-K 2007 Quantum key distribution with entangled photons *Phys. Rev.* A **76** 012307

[38] Rarity J G, Tapster P R, Gorman P M and Knight P 2002 Ground to satellite secure key exchange using quantum cryptography *New J. Phys.* **4** 82