communications physics

ARTICLE

https://doi.org/10.1038/s42005-022-00814-5 OPEN

Quantum communications in a moderate-to-strong turbulent space

Masoud Ghalaii [1]✉ & Stefano Pirandola [1]

Since the invention of the laser in the 60s, one of the most fundamental communication channels has been the free-space optical channel. For this type of channel, a number of effects generally need to be considered, including diffraction, refraction, atmospheric extinction, pointing errors and, most importantly, turbulence. Because of all these adverse features, the free-space optical (FSO) channel is more difficult to study than a stable fiber-based link. For the same reasons, only recently it has been possible to establish the ultimate performances achievable in quantum communications via free-space channels, together with practical rates for continuous variable (CV) quantum key distribution (QKD). Differently from previous literature, mainly focused on the regime of weak turbulence, this work considers the FSO channel in the more challenging regime of moderate-to-strong turbulence, where effects of beam widening and breaking are more important than beam wandering. This regime may occur in long-distance free-space links on the ground, in uplink to high-altitude platform systems (HAPS) and, more interestingly, in downlink from near-horizon satellites. In such a regime we rigorously investigate ultimate limits for quantum communications and show that composable keys can be extracted using CV-QKD.

[1] Department of Computer Science, University of York, York YO10 5GH, UK. ✉email: masoud.ghalaii@york.ac.uk

Year-long chain of excellent work has stitched quantum communications and quantum cryptography into the science of quantum information technologies. In particular, QKD[1] has been developing rapidly, with the end goal of making distant individuals able to share a key, which must be inscrutable for an eavesdropper to learn about, and which, therefore, can be used for secure classical communications. Since 1980s that saw the début of QKD[2], optical fibres have been the main platform to perform and/or experiment most QKD protocols. However, the reach of fibre-based quantum communications is limited to only a few hundreds of kilometres[3–6] (because of the exponential decay of the transmissivity). Whereas, man seems to stand on the verge of building a quantum internet[7,8] to make global quantum communications viable.

As a possible solution, one may think of a harmonized use of quantum repeater stations (placed on ground and connected via optical fibres) and free-space communication links. The latter includes ground-to-ground free-space channels, HAPSs, downlink/uplink communications with satellites, and inter-satellite links. To make secure free-space and satellite QKD globally available, certain technological challenges must be addressed. There has been increasing attempts put by the community in this direction; many models have been proposed for free-space channels and several demonstrations have been performed (see, refs. [9,10] for review). The successful launch of the Micius QKD satellite in 2017 and the follow-up experiments[11–14], have particularly been pivotal.

Free-space QKD systems must fight the effects of loss and noise in the link. For instance, a satellite-to-ground link would also encounter additional problems due to atmospheric turbulence and pointing errors. Such issues have been addressed widely through studying fading channels[15,16], analysing FSO QKD protocols[17–21], and applying adaptive optics techniques, e.g., to suppress noise[22–24]. In the same direction, by focusing on the establishment of quantum communication and QKD links, probability distribution functions (PDFs) of the transmittance for slant propagation paths were derived, and models for atmospheric quantum channels with turbulence were proposed[25,26]. In addition, distant FSO atmospheric channels have been experimentally characterized[11,27], where optical loss and signal noise are measured. As well, attempts were made to stabilize transmittance fluctuations caused by beam wandering over free-space atmospheric channels[28].

On the other hand, it is desirable to find the limits of quantum communications and QKD in different types of free-space medium, such as the Earth's atmosphere and space. In fact, alike the PLOB bound[29] and quantum repeater capacities[30], one may work out bounds germane to free-space and satellite links, where the most detrimental phenomena is perhaps, not surprisingly, turbulence—fluctuations in the atmosphere refractive index due to the aerodynamics and temperature gradient of the Earth's surface[31,32]. Due to atmospheric turbulence the spatial coherence of an optical beam is gradually destroyed as it propagates. This loss of spatial coherence restricts the reach to which beams can be focused or collimated[33–35]. This in turn results in significant power level reductions in FSO communication and radar links. Equally fatal, the destruction of coherence can affect optical receivers, which are very sensitive to the loss of spatial coherence[36,37].

Accounting for realistic effects on optical beams, such as diffraction, extinction, background noise, and channel fading, the latter due to pointing errors and atmospheric turbulence, Pirandola investigated the ultimate quantum communication limits and the practical security of FSO links, considering ground-based communications[38] and uplink/downlink with satellites[39]. Even though the theory developed in ref. [38] is very general, the main focus was the regime of weak turbulence, suitable for short-range high-rate FSO links on the ground. Similarly, the main focus of[39] was quantum communications with satellites within 1 radiant from the zenith position, so to enforce the regime of weak fluctuations.

In this manuscript, we extend the investigation to the regime of moderate-to-strong turbulence[40–42], where optical waves can harshly be deformed and eventually broken up into multiple patches[37,43], such that one would observe a random multiplicity of spots distributed on the receiving aperture[44,45]. Of main tools in studying free-space links in the presence of atmospheric turbulence are PDFs, such as log-normal, extended Huygens-Fresnel, and the recently proposed elliptic-beam models[25,31]. Such functions are beneficial to the estimation of, e.g., transmissivity of FSO channels. However, they can be cumbersome to handle, even numerically, and therefore restrictive for a theoretical account of the system. As one key contribution to the body of the field, considering the purposes of quantum communications and QKD, we put a lower bound on the transmissivity of atmospheric links that alleviates security analysis of such systems. Not only the bound is manageable, but also it can be used at all turbulence regimes. Next, in the more challenging regime of moderate-to-strong turbulence, we provide information-theoretic bounds for the maximum rates that are achievable for key generation and entanglement distribution. We then study the composable finite-size key rates that can be achieved by protocols of CV-QKD, showing the feasibility of this approach in moderate-to-strong FSO links.

The considered stronger regime of turbulence occurs in long-distance free-space connections on the ground but also in communications with satellites at large zenith angles (beyond 1 radiant). When a satellite is close to the horizon, the optical path within Earth's atmosphere becomes long and turbulence becomes a major problem. At these angles, another problem is refraction, which creates an elongation of the atmospheric section of the path (and therefore further loss and turbulence occur). Accounting for all these adverse aspects, we bound the optimal performances and provide achievable key rates.

Results and discussion

We first present some preliminary aspects and physics of FSO communications in turbulent media. We shall use these in the rest of the paper in order to understand and establish both ultimate limits and practical security of quantum communications in a moderate-to-strong turbulent space.

Figure of merit for the strength of turbulence. Assume an optical-beam signal of wavelength λ that propagates through a turbulent path of length z. As widely accepted[31,37,40], we introduce the Rytov number to be the figure of merit for the strength of turbulence. Physically, the Rytov number, or Rytov variance, is a measure of the strength of light scintillations—fluctuations in received irradiance, or in the phase and amplitude of the light, resulting from propagation through a turbulent space[31,46]. The dimensionless Rytov number is defined for a plane wave as follows[47]

$$\sigma_{\mathrm{Ry}}^2 = 1.23 C_n^2 k^{\frac{7}{6}} z^{\frac{11}{6}}, \tag{1}$$

where $k = 2\pi/\lambda$ is the wavenumber and C_n^2 is known as the index-of-refraction structure constant, measuring the magnitude of the fluctuations in the index of refraction (the Rytov number for a spherical wave is $0.4\sigma_{\mathrm{Ry}}^2$). Note that the scintillation of an optical signal does not increase unlimitedly as predicted by Rytov approximation[47], but saturates for strong turbulence and long

propagation links[37]. It can nevertheless still specify turbulence regimes.

Values of $\sigma_{\rm Ry}^2 < 1$ refer to weak turbulent media, while $\sigma_{\rm Ry}^2 > 1$ indicate strong turbulence[40]. The regime of intermediate turbulent media hence is lying around $\sigma_{\rm Ry}^2 \sim 1$. Rytov number is very much similar to the dimensionless Reynolds number[48], *Re*, in fluid mechanics, where for a fluid flowing through a packed bed of particles $Re < 10$ corresponds to a laminar flow, whereas $Re > 2000$ indicates a turbulent stream[49]. According to the Rytov number, the specification of turbulence regimes involves not just the index-of-refraction structure constant C_n^2, but a combination of this parameter, the beam's wavelength and the propagation path length.

The positive power dependence of the Rytov number on path length z implies that the medium is indeed expected to be highly turbulent at longer distances[37]. It is hence helpful to introduce another quantity which is relevant to the propagation distance, which is[40,42,50]

$$z_i = \left(C_n^2 k^2 \ell_0^{5/3}\right)^{-1}. \tag{2}$$

Parameter z_i represents the propagation length at which the transverse coherence radius of the optical wave is comparable to the turbulence inner scale ℓ_0. The parameter ℓ_0, which is on the order of 1 mm, is a measure of the smallest distances over which fluctuations in the index of refraction are correlated. We will shortly discuss that z_i defines the minimum valid distance for some relevant quantities in studying stronger turbulence media; that is, some equations are sound only for $z > z_i$. Fortunately, apropos equations can be found in the literature for $z < z_i$, where we may expect a moderate or strong turbulence space. It is worth mentioning that, in the regime of weak turbulence, a similar quantity, known as the spatial coherence radius $\rho_0 = (iC_n^2 k^2 z)^{-\frac{3}{5}}$, is introduced, where $i = 0.55\,(1.46)$ corresponds to plane (spherical) waves[31].

Pure diffraction and optical loss in free space. A natural light's phenomenon is diffraction, which perennially spreads the wave's size while it propagates through free space. It also constantly increases the radius of curvature of the propagating beam[34,35]. In our study, we start with a Gaussian beam, with initial field spot size w_0, carrier wavelength λ, and radius of curvature R_0. At distance z of propagation, where a receiver is supposedly placed, free-space diffraction increases the beam's spot size to

$$w_z^2 = w_0^2\left[\left(1 - \frac{z}{R_0}\right)^2 + \left(\frac{z}{z_R}\right)^2\right], \tag{3}$$

with $z_R = \pi w_0^2/\lambda$ being the beam's Rayleigh length. A receiver with infinite radius would collect all the light. However, practically speaking, only a fraction of the light can be collected by a receiver with a realistic finite aperture with radius a_R. This defines the pure diffraction-induced transmissivity

$$\eta_{\rm dif} = 1 - e^{-\frac{2a_R^2}{w_z^2}}, \tag{4}$$

yet, in reality, this would not be the total loss in a turbulent atmosphere as we shall see below.

Turbulence-induced beam spread. Equation (4) can lead to incorrect estimations because of Eq. (3), which may underestimate the effective spot size of the beam. This is because a different physics setting may apply in many real-world scenarios due to atmospheric turbulence. Therefore, we need to provide a proper estimation of the z-dependent spot size in order to modify

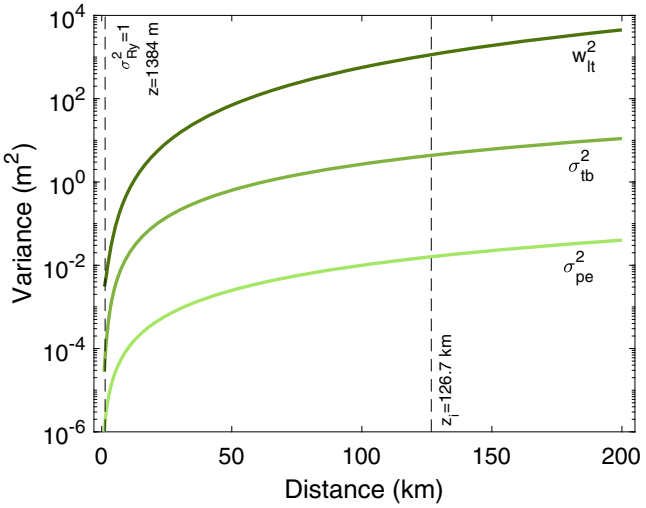

Fig. 1 Beam widening in the presence of strong turbulence. Here, we compare the variance of the centroid wandering induced by turbulence ($\sigma_{\rm tb}^2$, middle line) to that of pointing error ($\sigma_{\rm pe}^2$, lower line) and the long-term beam waist ($w_{\rm lt}^2$, upper line). We assume a collimated beam ($R_0 = +\infty$) with initial radius $w_0 = 5$ cm and wavelength $\lambda = 800$ nm. Other parameters are the outer scale of turbulence $L_0 = 1$ m and index-of-refraction structure constant $C_n^2 = 1.28 \times 10^{-14}$ m$^{-2/3}$ (night-time operation). Rytov variance ranges from $\sigma_{\rm Ry}^2 = 1$ at $z = 1384$ m to $\sigma_{\rm Ry}^2 > 9.12 \times 10^3$ at $z = 200$ km.

$\eta_{\rm dif}$ in Eq. (4). In a moderate-to-strong turbulent regime, a beam can break up into multiple patches and this primarily happens at longer propagation distances, where it is expected to have a large Rytov number. In this case, the patches of the beam will be in an area with mean square radius $w_{\rm lt}^2$, also known as the long-term beam waist[37]. Note that the relevant beam spread in the regime of weak turbulence is the short-term beam waist, $w_{\rm st}^2$[42]. In general, one has the decomposition $w_{\rm lt}^2 = w_{\rm st}^2 + \sigma_{\rm tb}^2$[38,40,42], where $\sigma_{\rm tb}^2$ is the variance associated with the wandering of the beam centroid. However, for stronger turbulence, wandering becomes negligible with respect to beam widening, i.e., we have the collapse $\sigma_{\rm tb}^2 \ll w_{\rm st}^2 \simeq w_{\rm lt}^2$. See Fig. 1 for a study of these quantities.

Let us now assume a Gaussian beam with initial spot radius w_0 and curvature R_0. After travelling through a path of length z, such a beam is characterized by a pair of parameters[31,51]

$$\Omega_0 = 1 - \frac{z}{R_0},\ \Lambda_0 = \frac{2z}{kw_0^2}. \tag{5}$$

For example, the pair $\Omega_0 = 0$ and $\Lambda_0 = 0$ corresponds to a spherical wave, whereas $\Omega_0 = 1$ and $\Lambda_0 = 0$ represents a plane wave. Alternatively, in the plane of the receiver, such a Gaussian beam can be described by the similar pair of parameters

$$\Omega = \frac{\Omega_0}{\Omega_0^2 + \Lambda_0^2} = 1 + \frac{z}{R},\ \Lambda = \frac{\Lambda_0}{\Omega_0^2 + \Lambda_0^2} = \frac{2z}{kw_z^2}, \tag{6}$$

where R is the phase front radius of curvature at the receiver. It is then shown that, at distances $z > z_i$, where a strong turbulent space is experienced[37], the long-term beam waist at the receiver is given by (ref. [31], Chap. 8)

$$w_{\rm lt} = w_z\sqrt{1 + \frac{4}{3}q\Lambda}, \tag{7}$$

with the q parameter equal to

$$q = 0.74\sigma_{\rm Ry}^2 Q_m^{1/6},\ Q_m = 35.05z/(k\ell_0^2). \tag{8}$$

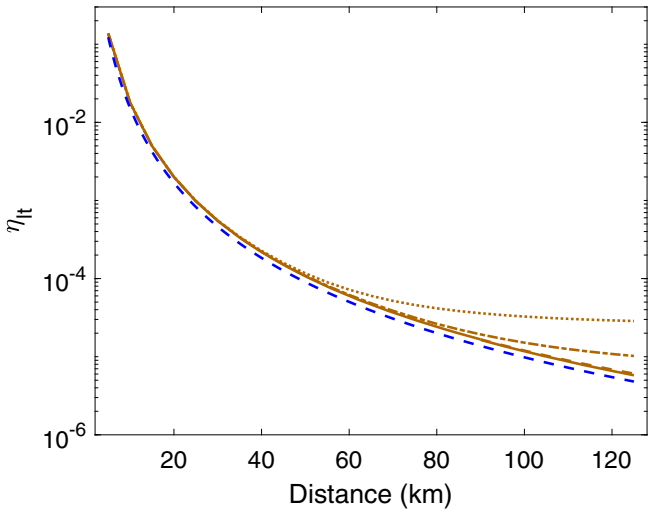

Fig. 2 Turbulence-induced transmissivity versus distance. By assuming the same parameters of Fig. 1, here we plot turbulence-induced transmissivity versus distance $z < z_i$, where $z_i = 126.7$ km. Brown curves from top to bottom correspond to the Huygens-Fresnel long-term transmissivity numerically computed for a_R^{∞} =10, 20, 50 and 100 m. The lower (dashed blue) curve is the long-term transmissivity analytically computed from Eqs. (16) and (9). The latter can be assumed as limiting lower value at all distances.

In Eq. (7), we see how the diffraction-limited beam waist w_z is revised into the long-term beam waist $w_{\rm lt}$ via an additional spread factor associated with scattering by turbulent eddies.

Note that even through a short propagation distance the beam may experience a moderate or strong turbulence space. In this case ($z < z_i$) the effective beam waist is

$$w_{\rm lt} = w_z\sqrt{1 + 1.63(\sigma_{\rm Ry}^2)^{\frac{6}{5}}\Lambda}. \tag{9}$$

The above equation is also considered to be adequately precise for weak turbulence so that it can generally be used to estimate the long-term beam waist under almost all turbulence conditions. Thus, we may use Eq. (9) at all distances $0 \simeq z < z_i$, no matter the strength of turbulence.

In this study, Eqs. (7) and (9) provide the main quantities that we shall use to bound the rate of quantum communications in a moderate-to-strong turbulent space.

More details on beam wandering. While transmitting an optical signal through free space, it is observed that position of the instantaneous centroid of the signal (point of maximum irradiance or "hot spot") is randomly displaced. This instantaneous quivering in the plane of the receiver, which supposedly happens according to a Gaussian distribution with variance σ^2, is commonly called beam or centroid wandering. Overall, this wandering is caused by pointing error $\sigma_{\rm pe}^2$, due to Gaussian jitter and off-target tracking, and atmospheric turbulence $\sigma_{\rm tb}^2$. These two effects are independent and sum up such that the total variance of the wandering is given by $\sigma^2 = \sigma_{\rm pe}^2 + \sigma_{\rm tb}^2$. The amount of wandering for a typical 1 μrad off-tracking error at the transmitter is given by $\sigma_{\rm pe}^2 \simeq 10^{-12}z^2$. But, the contribution of atmospheric turbulence is more elaborate.

Different mathematical expressions have been developed to estimate wandering in strong turbulent media[31,40,41,43]. Here, we use the following estimation (ref. [31], Chap. 8)

$$\sigma_{\rm tb}^2 = 7.25C_n^2 w_0^{-\frac{1}{3}} z^3 \int_0^1 d\xi\xi^2\left[\frac{1}{f^{\frac{1}{6}}(\xi)} - \frac{\kappa_0^{\frac{1}{3}} w_0^{\frac{1}{3}}}{\left[1+\kappa_0^2 w_0^2 f(\xi)\right]^{\frac{1}{6}}}\right], \tag{10}$$

where $\kappa_0 = 2\pi/L_0$, with $L_0 \simeq 1{-}100$ m being the outer scale of turbulence and

$$f(\xi) = [\Omega_0 + (1-\Omega_0)\xi]^2 + 1.63(\sigma_{\rm Ry}^2)^{6/5}\Lambda_0(1-\xi)^{16/5}. \tag{11}$$

This is applicable in moderate-to-strong atmospheric turbulence, and is shown to be consisting of experimental data.

As previously discussed, it turns out that centroid wandering is a negligible effect when turbulence is sufficiently strong. In Fig. 1, we plot the turbulence-induced centroid wandering $\sigma_{\rm tb}^2$, the pointing-error wandering $\sigma_{\rm pe}^2$ and the long-term beam waist $w_{\rm lt}^2$. While at short distances, where $\sigma_{\rm Ry}^2 \sim 1$, they tend towards each other, they diverge at longer distances, where $\sigma_{\rm Ry}^2 \gg 1$. Nevertheless, it is clear that at all distances considered, we have $w_{\rm lt}^2 \gg \sigma_{\rm tb}^2 \gg \sigma_{\rm pe}^2$. In fact, the beam may break up into smaller patches in a very wide area, while the wandering of the centroid becomes negligible.

Turbulence-induced transmissivity. In FSO communication, turbulence can cause power fading and sometimes complete loss of signal. In addition, communication links can experience severe signal degradation as well as spatial/temporal irradiance scintillations in the beam wavefront. To accurately estimate the signal fading and behaviour at some propagation distance, and to learn a true picture of how these affect crucial performance parameters such as the communication rate, it is important to analyze the distribution of the irradiance and/or transmittance at the receiver. In addition, having a theoretical distribution that accurately models these fluctuations under propagation conditions is desirable. This can be achieved through the knowledge of the statistical properties of the intensity fluctuations of the beams. In particular, the probability distribution of the transmittance most thoroughly characterizes the statistics of these fluctuations. Several models have been introduced to deal with this problem, including the log-normal model, the parabolic equation model, Feynman path integral, extended Huygens-Fresnel principle (see, ref. [31]), and the recently proposed elliptic-beam model[25].

The extended Huygens-Fresnel model is considered to be rather easier to use than other methods, especially when it comes to stronger turbulent media. For a Gaussian beam defined by the set of parameters given in Eqs. (5) and (6), and long-term waist given in Eqs. (7) and (9), the turbulence-induced transmissivity can be computed from

$$\eta_{\rm lt} = \frac{1}{\mathcal{N}}\int_{\mathcal{A}} d^2r\langle I(r,z)\rangle, \tag{12}$$

where the integration is performed over the area $\mathcal{A}$ of the circular aperture, and

$$\mathcal{N} = \lim_{\mathcal{A}\to\infty}\int_{\mathcal{A}} d^2r\langle I(r,z)\rangle \tag{13}$$

is a normalization factor. The mean irradiance $\langle I(r,z)\rangle$ is provided by the extended Huygens-Fresnel model (ref. [31], Chapt. 7)

$$\langle I(r,z)\rangle = \frac{w_0^2}{w_{\rm lt}^2}\exp\left\{-\frac{2r^2}{w_{\rm lt}^2}\right\}, \quad z > z_i, \tag{14}$$

and

$$\langle I(r,z)\rangle = \frac{2w_0^2}{w_z^2}\int_0^\infty dt\, t J_0\left(\frac{2\sqrt{2}rt}{w_z}\right) e^{-t^2-yt^{5/3}}, \quad z<z_i, \tag{15}$$

where $J_0(x)$ is a Bessel function and $y = 1.41\sigma_{\rm Ry}^2\Lambda^{\frac{5}{6}}$.

For $z>z_i$, we replace Eq. (14) in Eqs. (12) and (13). Solving the integration, we can find an explicit analytical form for the transmissivity, given by

$$\eta_{\rm lt} = 1 - e^{-\frac{2a_R^2}{w_{\rm lt}^2}}, \tag{16}$$

where $w_{\rm lt}^2$ is given in Eq. (7). Thus Eq. (16) should be used instead of the pure diffraction transmissivity in Eq. (4).

For $z<z_i$, we cannot find a closed-form but nevertheless we can compute the result numerically by replacing Eq. (15) in Eqs. (12) and (13), and noting that the limit for unlimited area $\mathcal{A}$ can be treated by assuming $a_R = a_R^\infty$ for sufficiently large a_R^∞. Notwithstanding, we can check that the formula in Eq. (16), where we replace the long-term waist of Eq. (9), provides a limiting lower bound to such numerical values, as shown in Fig. 2. Thus, we may use an analytical expression for the turbulence-induced transmissivity at all distances, as given by Eq. (16) where we replace either Eq. (7) (for $z>z_i$) or Eq. (9) (for $z<z_i$).

Another theoretical model is the log-normal model, where the beam follows a log-normal distribution rather than a Gaussian one. Using this model, we get a similar formula

$$\eta_{\rm lt,LN} = 1 - e^{-\frac{2a_R^2}{w_{\rm lt,LN}^2}}, \tag{17}$$

where $w_{\rm lt,LN}^2$ is given in 'Methods'. The validity of the formula holds for all propagation values z and it has been experimentally verified[52]. In addition, it is shown to match recently developed descriptions of atmospheric transmissivity, such as the elliptic-beam model[25]. However, the computation of $w_{\rm lt,LN}^2$ is cumbersome to handle even numerically. An heuristic choice is to combine Eq. (17) with the calculation of the beam waist from other models, in particular, from the previous Huygens-Fresnel model. Thus, we may consider a *hybrid* log-normal model where we replace $w_{\rm lt,LN}^2$ with $w_{\rm lt}^2$, whose expression is given in Eqs. (7) and (9). This is completely equivalent to the previous approach. For this reason, in our study, we consider $\eta_{\rm lt}$ of Eq. (16) with long-term waist $w_{\rm lt}$ given by Eqs. (7) and (9).

Bounds and security of quantum communications in a moderate-to-strong turbulent space. Now we are in a position to account for the overall optical loss that can occur in a strong turbulence regime. The overall transmissivity includes the multiplication of three types of optical transmissivity

$$\eta = \eta_{\rm lt}\eta_{\rm eff}\eta_{\rm atm}, \tag{18}$$

where we include the receiver's efficiency $\eta_{\rm eff}$ and atmospheric loss $\eta_{\rm atm}$. The latter is modelled by the Beer-Lambert equation

$$\eta_{\rm atm} = \exp\{-\alpha(\lambda,h_0)z\}, \;\; \alpha(\lambda,h_0) = \alpha_0(\lambda)e^{-\frac{h_0}{6600}}, \tag{19}$$

where h_0 is the altitude (measured in metres) and $\alpha_0(\lambda)$ is the extinction factor at sea level[53,54].

By replacing the combined transmissivity of Eq. (18) in the repeaterless PLOB bound $\Phi(\eta) = -\log_2(1-\eta)$[29], one gets the following upper bound for the rate R of any QKD protocol over the FSO link

$$R \le \Phi(\eta) := -\log_2\left[1 - \eta_{\rm eff}e^{-\alpha(\lambda,h_0)z}\left(1 - e^{-\frac{2a_R^2}{w_{\rm lt}^2}}\right)\right]. \tag{20}$$

We remark that, as shown in Fig. 1, in the moderate-to-strong turbulence regime ($\sigma_{\rm Ry}^2 \ge 1$) the variance of long-term beam widening is several orders of magnitude larger than that associated with the centroid wandering. Therefore, we can neglect the short-term fading process and assume a fixed transmissivity between the sender and the detector plane at each distance. This is different from the weak turbulence regime where beam widening and wandering are equally important[38].

Apart from loss, the other key element that must be considered in FSO quantum communications is the number of thermal-noise photons, which may find their way into the receiver's aperture. They come from the sky brightness and can also be generated within the receiver itself. To involve the effect of thermal noise into the communications bound, we follow and apply the technique introduced in ref. [38].

The receiver sees a total mean number of thermal photons equal to $\bar{n} = \eta_{\rm eff}\bar{n}_B + \bar{n}_{\rm ex}$, where $\bar{n}_B$ and $\bar{n}_{\rm ex}$ are the number of background thermal photons per mode and extra photons generated within the receiver box, respectively. The number $\bar{n}_B$ depends on several factors coupled to the sky and the receiver. It is given by $\bar{n}_B = \pi\Gamma_R B_\lambda^{\rm sky}/(\hbar\omega)$, where $\hbar$ is the reduced Planck constant, ω is the angular frequency of light, and $B_\lambda^{\rm sky}$ is the brightness of the sky, which is in the range of 10^{-6}–$10^{-1}\,{\rm Wm^{-2}\,nm^{-1}\,sr^{-1}}$ from night to cloudy day[55,56]. The effects of the receiver is gathered in a single parameter $\Gamma_R = \Delta\lambda\Delta t\Omega_{\rm fov}a_R^2$, where $\Omega_{\rm fov}$, $\Delta\lambda$ and Δt are the angular field of view, spectral filter, and time window of the detector, respectively. The nominal values that we use in this study are $\Omega_{\rm fov} = 10^{-10}$ sr, $\Delta\lambda = 0.1$ pm, and $\Delta t = 10$ ns. The natural interferometric effect of coherent detection, where the signal and LO pulse overlap, imposes an effective filter of $\Delta\lambda = \lambda^2\Delta\nu/c$, such that assuming $\lambda = 800$ nm, a LO of $\Delta t = 10$ ns, and a bandwidth $\Delta\nu = 50 \ge 0.44/\Delta t$ MHz, applies an effective filter of $\Delta\lambda = 0.1$ pm. This would suppress the background noise $\bar{n}_B$ to the order of 10^{-12} (10^{-7}) at night (day) time, which in turn allow for positive rates that could not have been obtained otherwise. Precisely, for a receiver with $a_R = 5$cm, we estimate $\bar{n}_B = 4.75\times10^{-12}$ (10^{-7}) background photons per optical mode at night (day).

The total Alice-Bob FSO link is modelled as a thermal-loss channel with transmissivity η and overall thermal noise $\bar{n}$. The worst-case scenario is when the eavesdropper (Eve) has control over all the input noise. Such a scenario can be simulated by her using a beam splitter with transmissivity η that combines Alice's signal mode with an input thermal mode with $\bar{n}_e = \bar{n}/(1-\eta)$ mean photons. We then use the thermal-loss version of the PLOB bound. For $\bar{n} \le \eta$, the secret-key capacity in Eq. (20) can be revised to

$$R \le K_{\rm UB}(\eta,\bar{n}) := \Phi(\eta) - \frac{\bar{n}}{1-\eta}\log_2\eta - h\left(\frac{\bar{n}}{1-\eta}\right), \tag{21}$$

where $h(x) = (1+x)\log_2(1+x) - x\log_2 x$. One may also find the achievable lower bound given by the reverse coherent information[57,58], i.e., there is an optimal rate R such that

$$R \ge K_{\rm LB}(\eta,\bar{n}) := \Phi(\eta) - h\left(\frac{\bar{n}}{1-\eta}\right). \tag{22}$$

We present numerical simulations of the limits on communication rates in Fig. 3 showing the pure-loss bound of Eq. (20) and the thermal-loss bound of Eqs. (21) and (22). One first, and important, conclusion one may make is that we can obtain positive communication rates even in a strong turbulence regime.

Each curve in Fig. 3a is made of two parts because we have used two different equations in our simulation, i.e., Eq. (7) for $z \le z_i$ and Eq. (9) for $z \ge z_i$. The distance $z = z_i$ is indicated by a

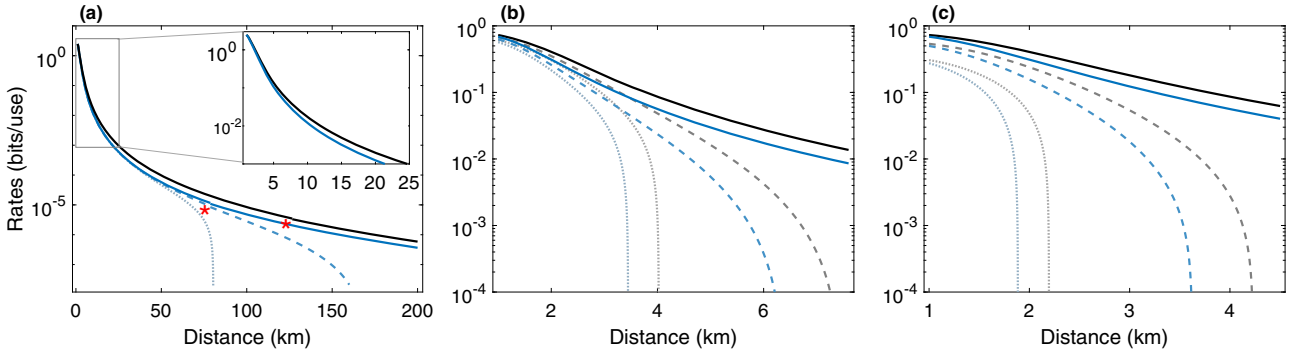

Fig. 3 Free-space optical quantum communications in a moderate-to-strong turbulent space. We indicate night- and day-time conditions by black and blue curves, respectively. In **a**, we plot the ultimate pure-loss bound of Eq. (20) with an ideal receiver, $\eta_{\rm eff}=1$ and $\bar{n}_{\rm ex}=0$, at night-time (solid black curves) and day-time (solid blue curve). The dashed (dotted) curves are thermal upper (achievable lower) bounds for an ideal receiver with $\eta_{\rm eff}=1$ and $\bar{n}_{\rm ex}=0$ [cf. Eqs. (21) and (22)]. The red star indicates the distance z_i (connecting plots from different equations and therefore presenting small discontinuities). Here, the following set of parameters are considered: $\lambda=800$ nm, $\alpha_0(\lambda)=5\times10^{-6}\,{\rm m}^{-1}$, $w_0=a_R=5$ cm, $\Omega_{\rm fov}=10^{-10}$ sr, $\Delta t=10$ ns, $\Delta\lambda=0.1$ pm, $h_0=30$ m, so that $C_n^2=1.28\,(2.06)\times10^{-14}\,{\rm m}^{-2/3}$ for night (day). Also, we have thermal noise $\bar{n}_B=4.75\times10^{-12}\,(\times10^{-7})$ photons per mode at night (day). In **b** and **c**, we assume a lossy and noisy receiver with $\eta_{\rm eff}=0.5$ and, respectively, $\bar{n}_{\rm ex}=0.01$ and $\bar{n}_{\rm ex}=0.05$. As in panel (**a**), we compare the pure-loss rates (solid) with the thermal-noise bounds (dashed) and the achievable lower bounds (dotted).

red star, which is different for night and day operation (the right is for night). We observe a very slight inconsistency at $z=z_i$, which is due to using different expressions. Notwithstanding it is clear that the second part of the rate after z_i follows exactly the same trend as the first part. In Fig. 3a, we compare the performances at night and day with an ideal receiver having $\eta_{\rm eff}=1$ and $\bar{n}_{\rm ex}=0$. For night-time operation, all curves coincide because of absolutely low background noise ($\bar{n}_B=4.75\times10^{-12}$). However, for day-time, with $\bar{n}_B=4.75\times10^{-7}$, the deviation between the rates becomes distinct at large link distances, so that the thermal lower bound and upper bound drop at nearly 80 and 150 km, respectively. Nevertheless, the plot suggests that high rates can still be achieved at relatively shorter distances at both night and day.

Then we account for a realistic lossy and noisy receiver with $\eta_{\rm eff}=0.5$ and $\bar{n}_{\rm ex}=0.01$ in Fig. 3b, while $\eta_{\rm eff}=0.5$ and $\bar{n}_{\rm ex}=0.05$ in Fig. 3c. It is observed that the thermal photons generated at the receiver suppress the rates so that distances are of the order of a few kilometres. As we shall show later, this can be partially alleviated by using a receiver with a larger aperture size.

Long free-space distances that we are considering here, e.g., $z=100$ km, may not seem so practical, especially because Earth's geometry, in particular its curvature, does not allow two terrestrial stations to actually "see" each other. For example, the maximum distance between two communications towers with height 30 m is about 40 km. Although this can be true for terrestrial stations, we allow for a wider variety of FSO links, including HAPS. Otherwise, a long-distance link could basically be an equivalent section of the atmosphere with a shorter length but stronger turbulence.

The key rates for a moderate-to-strong turbulence regime can be seen as the tail of the rates found in ref. [38] for weak turbulence. This is where, at about 1384 m distance, we have $\sigma_{\rm Ry}^2=1$ and longer distances induce a stronger turbulence regime (for sake of comparison, we have used the same set of parameters used in ref. [38]). The main reason is that Eq. (9) is sufficiently precise even in weak turbulence regimes. Let us also remark the reason behind choosing $\Delta\lambda=0.1$ pm, which is discussed in detail in ref. [38].

Composable finite-key security analysis. Equation (22) gives the achievable lower bound for key distribution rate when, ideally, an infinite number of signals are used for key extraction. However, in a real-world scenario, communication links can only be used a finite number of times. Hence, we may expect a poorer key rate than the asymptotic one. In addition, the security of a QKD protocol is desirable to be composable, i.e., the protocol must not be distinguished from an ideal protocol which is secure by construction[1]. Mathematically, a composable security proof can be provided by incorporating proper error parameters (ε's) for each segment of the protocol, namely, error correction, smoothing and hashing[59,60]. To address this finiteness and composability, we study a QKD protocol based on coherent states for which we compute the composable finite-size key rate.

We consider the homodyne-based coherent-state QKD protocol[61,62], the GG02 protocol, where Alice prepares N Gaussian-modulated signals, with variance V, and sends them through a quantum channel to Bob. The latter performs a homodyne measurement, whereby he randomly measures one of the light quadratures. A number n of signals will be used for key extraction, while the rest $m_{\rm pe}=N-n$ are left for parameter estimation. It can then be shown that the composable finite-size secret-key rate is given by[38,39]

$$R_\varepsilon\geq p_{\rm ec}(1-r_{\rm pe})\left(R_{\rm pe}-\frac{\Delta_{\rm aep}}{\sqrt{n}}+\frac{\Omega}{n}\right),\tag{23}$$

where $p_{\rm ec}$ is the success probability of error correction connected to the frame error rate by $FER=1-p_{\rm ec}$, $r_{\rm pe}=m_{\rm pe}/N$ is the fraction of signals used for parameter estimation, $R_{\rm pe}$ is the asymptotic key rate accounting for parameter estimation, and (ref. [63], Sec. F)

$$\Delta_{\rm aep}:=4\log_2(\sqrt{d}+2)\sqrt{\log_2(18p_{\rm ec}^{-2}\varepsilon_{\rm s}^{-4})},\tag{24}$$

$$\Omega:=\log_2\left[p_{\rm ec}(1-\varepsilon_{\rm s}^2/3)\right]+2\log_2(\sqrt{2}\varepsilon_{\rm h}).\tag{25}$$

In Eq. (23), the asymptotic rate $R_{\rm pe}$ is calculated for the worst-case values of transmissivity and excess noise to be evaluated at the parameter estimation stage. These values are chosen within w confidence intervals so that they are correct up to an error probability of $\varepsilon_{\rm pe}(w)=\left[1-{\rm erf}\,(w/\sqrt{2})\right]/2$. See 'Methods' for the calculation of $R_{\rm pe}$. Equation (23) is valid for a protocol with overall security $\varepsilon=\varepsilon_{\rm cor}+\varepsilon_{\rm s}+\varepsilon_{\rm h}+2p_{\rm ec}\varepsilon_{\rm pe}$[38], where $\varepsilon_{\rm h(s)}$ is the hashing (smoothing) parameter and $\varepsilon_{\rm cor}$ is the ε-correctness bounding the probability that Alice's and Bob's sequences are different even if they pass error correction. Finally, one needs to

account for the analogue-to-digital conversion so that each continuous-variable symbol is encoded in d bits.

One further consideration regards the measurement techniques in CV-QKD. The received signals can be detected by using a coherent (homodyne or heterodyne) detection with the help of an either transmitted local oscillator (TLO) or local local oscillator (LLO). It turns out that at long distances the amount of detection noise is much lower for the LLO case. But, at the same time, the signal, which propagates through a turbulent path, and the LO, which is produced locally at the receiver, would not be spatially matched. As we show in 'Methods', this introduces even more loss to the system during the detection process. Therefore, we modify the overall transmissivity in Eq. (18) by a further factor $\eta_{\rm cd}$, i.e.,

$$\eta = \eta_{\rm lt}\eta_{\rm eff}\eta_{\rm cd}\eta_{\rm atm}. \tag{26}$$

Our estimate is that at long distances we roughly have $\eta_{\rm cd} = 0.63$, which is the value used in our simulation.

Figure 4 shows the composable finite-size key rate versus (a) block size and (b) receiver aperture size in a strong turbulence space. The link's length is $z = 10$ km, equivalent to 7.84 dB, and the Rytov number is $\sigma^2_{\rm Ry} = 37.56\,(60.45)$ at night (day).

In Fig. 4a, we have fixed the receiver aperture size to $a_R = 30$ cm. The rates at night-time operation can be obtained with a typical block size of ~10^8, while the system demands a larger block size, which is still acceptable. We observe that one main parameter that substantially affects the rates, at fixed distance and block size, is the aperture size. From Fig. 4b we see that, at fixed length of $z = 10$ km, positive rates can be achieved with a relatively large receiver. However, note that the aperture cannot be made too large. In fact, increasing the receiver size lets more thermal photons into the detection system, e.g., we get $\bar{n}_B = 1.71\times 10^{-10}(10^{-5})$ for $a_R = 30$ cm, versus $\bar{n}_B = 4.75\times 10^{-12}(10^{-7})$ for $a_R = 5$ cm, at night (day).

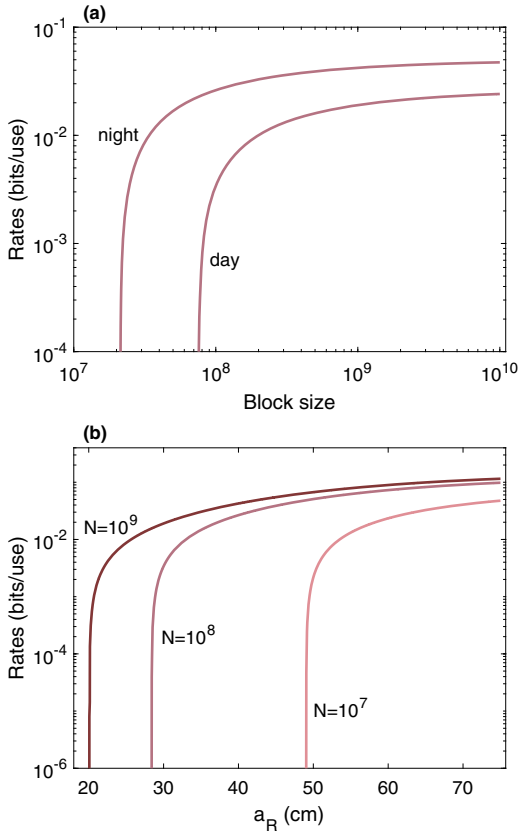

Fig. 4 Numerical results for the composable secret-key rate of a free-space CV-QKD protocol in turbulent space. The rate is plotted versus **a** block size and **b** receiver aperture size. In (**a**), an aperture size $a_R = 30$ cm is fixed. In (**b**), assuming night-time operation, we plot the rate for various block-size values. In both plots we assume a lossy and noisy receiver with $\eta_{\rm eff} = 0.5$, $\eta_{\rm cd} = 0.63$, and $\bar{n}_{\rm ex} = 0.001$. Distance is $z = 10$ km. Other physical parameters are set as given in Fig. 3, except $\bar{n}_B$ which varies with a_R. Protocol parameters are $\mu = 10$, $r_{\rm pe} = 0.1$, $d = 2^5$, frame error rate (*FER*) is 0.1, $\varepsilon_{\rm s} = \varepsilon_{\rm h} = \varepsilon_{\rm cor} = 10^{-10}$, $w = 6.34$, $\varepsilon = 4.5\times 10^{-10}$, and $\beta = 0.98$.

Satellite communications at large zenith angles. Here we apply the theory to a satellite communication link beyond 1 rad up to the horizon, where turbulence is strong. In particular, we focus on the mask (or cutoff) angle, $\theta_{\rm m}$, which is the minimum acceptable elevation above the horizon that a satellite has to be at to avoid blockage of line-of-sight. This is important because the key rates that will be derived for the mask angle represent lower bounds for the entire satellite quantum communication system. One can set a mask angle that tells the receiver to ignore the satellite at zenith angles larger than $\theta_{\rm m}$, i.e., lower elevations. The mask angle is roughly 80 deg ($4\pi/9$ rad) that is 10 deg from the horizon.

In this study, we consider a zenith-crossing satellite at altitude h, whose slant distance to the ground station, located at h_0 above sea level, is given by

$$z = \sqrt{(R_E + h)^2 + (R_E + h_0)^2(\cos^2\theta - 1)} - (R_E + h_0)\cos\theta, \tag{27}$$

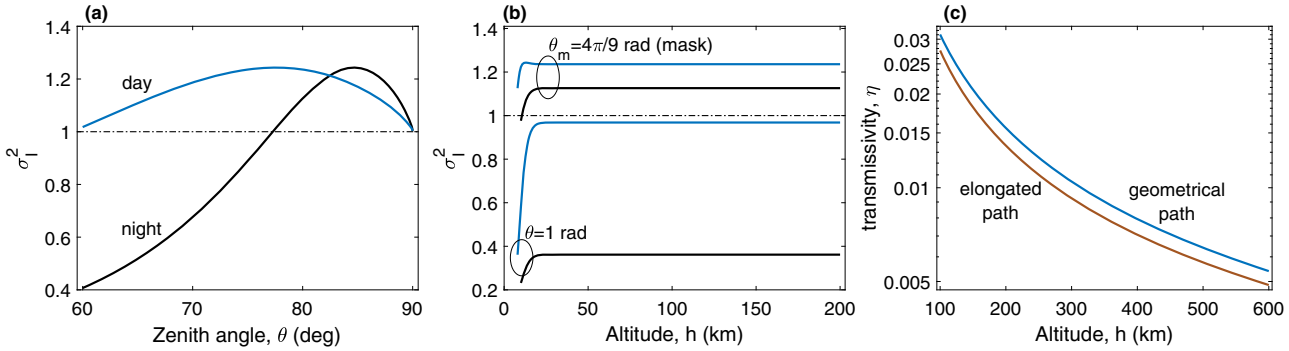

Fig. 5 Satellite communications at large zenith angle. In (**a**), we show the scintillation index of Eq. (28) versus the zenith angle, at fixed $z = 400$ km. In (**b**), we plot the scintillation index of Eq. (28) versus altitude, at $\theta = 1$ rad and $\theta_{\rm m} = 4\pi/9$ rad. In (**a**) and (**b**) black curves are for clear-night turbulence conditions, while blue curves are for day-time and high-wind conditions. In (**c**) we illustrate the non-trivial difference between the elongated and geometrical paths at the mask angle $\theta_{\rm m} = 4\pi/9$. In (**c**) we have set $w_0 = 20$ cm, $a_R = 40$ cm, $\lambda = 800$ nm, $h_0 = 30$, $\alpha_0(\lambda) = 5\times 10^{-6}\,{\rm m}^{-1}$, and $\eta_{\rm eff} = 0.5$.

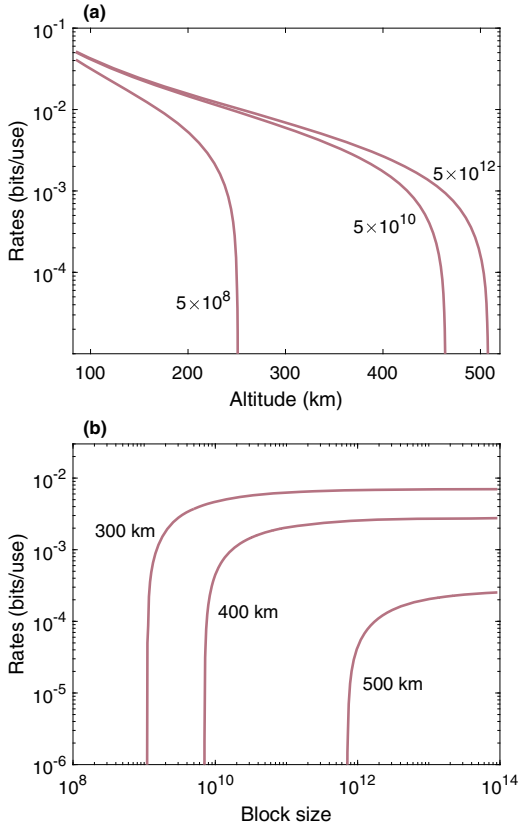

Fig. 6 Performance of satellite quantum communications at large zenith angles. In (**a**), we have finite-size key rates versus altitude (for fixed values of block size). In (**b**), we have similar rates versus block-size (for fixed values of altitude). Both figures consider a mask angle $\theta_{\rm m}=4\pi/9$ at night-time, and windspeed $v=21$ m/s and $A=1.7\times10^{-14}\,{\rm m}^{-2/3}$ used in Eq. (29). Here we have set $w_0=20$ cm, $a_R=70$ cm, $\bar{n}_B=4.75\times10^{-10}$, $\bar{n}_{\rm ex}=0.001$, and $\eta_{\rm cd}=0.63$. Other parameters chosen as given in Fig. 5. Protocol parameters are taken as follows: $\mu=10$, $\beta=0.98$, $r_{\rm pe}=0.1$, $d=2^5$, frame error rate (*FER*) is 0.1, $\varepsilon_{\rm s}=\varepsilon_{\rm h}=\varepsilon_{\rm cor}=10^{-10}$, $w=6.34$, and $\varepsilon=4.5\times10^{-10}$.

where $R_E\simeq6370$ km is Earth's radius and θ the zenith angle. To continue, we first need to identify the regime of operation. Replacing the above equation in the Rytov number of Eq. (1) cannot be used for a slant link out to the space because the index-of-refraction structure C_n^2 is not anymore constant and varies with the altitude h. We then require a more general, altitude-dependent, theory that stands as a measure for atmospheric scintillations and the turbulence regime. Assuming a downlink path from space, we take the following expression for scintillation index[64]

$$\sigma_I^2(h,\theta)=\exp\left[\frac{0.49\sigma_{\rm Ry}^2(h,\theta)}{\left(1+1.11\sigma_{\rm Ry}^{12/5}(h,\theta)\right)^{7/6}}+\frac{0.51\sigma_{\rm Ry}^2(h,\theta)}{\left(1+0.69\sigma_{\rm Ry}^{12/5}(h,\theta)\right)^{5/6}}\right]-1, \tag{28}$$

where

$$\sigma_{\rm Ry}^2(h,\theta)=2.25k^{\frac{7}{6}}\sec^{\frac{11}{6}}(\theta)\int_{h_0}^{h}dh'\,(h'-h_0)^{\frac{5}{6}}C_n^2(h').$$

In fact, $\sigma_I^2(h,\theta)$ is the modified version of a typical Rytov number that is now a function of altitude, zenith angle, as well as varying properties of the atmosphere. According to the Hufnagel–Valley (H-V) atmospheric model (ref. [31], Sec. 12.2), the index-of-refraction structure is a function of the altitude

$$C_n^2(h)=5.94\times10^{-53}(v/27)^2h^{10}e^{-h/1000}+2.7\times10^{-16}e^{-h/1500}+Ae^{-h/100}, \tag{29}$$

where v is the windspeed [m/s] and A is the nominal value of $C_n^2(0)\,[{\rm m}^{-2/3}]$ at the ground. In our simulation, we consider low-wind night-time by assuming $v=21$ m/s and $A=1.7\times10^{-14}\,{\rm m}^{-2/3}$, and high-wind day-time by assuming $v=57$ m/s and $A=2.75\times10^{-14}\,{\rm m}^{-2/3}$ [31,39].

As it is seen in Fig. 5a, for zenith angles larger than 1 (1.32) rad for day (night), we have $\sigma_I^2>1$, which means that signals will experience a moderate/strong turbulent space in such operational regimes. As $\theta\to90$ deg scintillation drops to 1; precisely, to 1.0033. In addition, Fig. 5b shows σ_I^2 versus altitude h, at the zenith angle $\theta=1$ rad as well as at the mask angle $\theta_{\rm m}=4\pi/9$ rad. At $\theta=1$ rad, the turbulence is weak for both night- and day-time operation, as also argued previously in ref. [39]. Whereas, at relatively high zenith angle, such as a mask angle of 80 deg, the turbulence in the link is strong at all values of altitude $h>20$ km.

Another important factor that plays a role in a slant satellite path at large zenith angles is geometrical elongation of the communication links. This is due to the refraction on interfaces of atmospheric layers, which introduces even more optical loss. It accounts for the apparent position of celestial objects toward the zenith, and is measured as the elongation factor, which is defined by the quotient of the (bent) optical trajectory and the (direct) geometrical slant path. We account for the elongation factor via the methodology introduced in ref. [26]. It uses the so-called standard atmosphere model and distinguishes 10 atmospheric layers above the Earth's surface (within each layer the latitude dependence of refractive index is to be assumed linear). In Fig. 5c, we plot the optical loss for an elongated path, at night and at mask angle $\theta_{\rm m}=4\pi/9$ rad, and compare it with that without elongation. It is seen that the elongated path imposes more optical loss.

Let us now apply all the above consideration to the evaluation of finite-size key rates. In Fig. 6a, for several block-size values, we have plotted key rates at night-time operation and at mask angle $\theta_{\rm m}=4\pi/9$ rad, where turbulence is strong (cf. Fig. 5). Here we have set $w_0=20$ cm, $a_R=70$ cm, which constrains $\bar{n}_B=4.75\times10^{-10}$, and $\bar{n}_{\rm ex}=0.001$. For the sake of comparison, we have also shown the pure-loss upper bound, which continue to offer higher rates with increasing the satellite altitude, whereas the finite-size rates drop at relatively lower altitudes. Furthermore, in Fig. 6b, for several altitudes, we have plotted composable finite-size key rates versus block size, at night and at mask angle $\theta_{\rm m}=4\pi/9$ rad. Our simulation illustrates that with a reasonable block size and receiver size quantum satellite communication is feasible for altitudes up to 500 km. At the same time, we note that the lifetime of low Earth orbit satellites with altitudes between 200 and 400 km is considerably short (fewer than 3 years) due to atmospheric drag, which eventually deorbits the satellites[65]. This reads roughly 75 years for a satellite at 700 km altitude.

Finally, let us compare a part of our findings with actual measured data. For the Chinese Micius satellite[11], at altitude 500 km and zenith angle around 70 deg (that is a slant path of 1200 km), the loss was measured to be about 25 dB (using a transmitter telescope with 30 cm aperture size and a receiver telescope with 1 m aperture size placed at 890 m above ground level). There, with a repetition rate of 100 MHz, they could achieve a few kHz key rate from the satellite to ground by discrete-variable QKD protocols. This is comparable to our findings, at the same altitude and repetition rate, but a larger zenith angle (80 deg), which from Fig. 6b and at block size of 10^{12} reads 4.4 kHz key rate by CV-QKD protocols. In addition, by

assuming an Alphasat-like satellite in a LEO orbit at 500 km[27], estimates the total channel losses from a satellite up to the receiving aperture, with an aperture of 1 m, to be about 20 dB (note that this is based on extrapolated data and not actual measured data). This is comparable to our results, read from Fig. 5c, that for the same orbit the channel loss is 16.4 dB. The difference may come from the choice of wavelength, which reads 1064 nm for their setup and 800 nm for ours, or the error in the extrapolation.

In this work, we have extended the field of FSO quantum communications to a moderate-to-strong turbulent space where atmospheric conditions can be harsh and fatal to optical signals. Despite the possibility that the signals could be severely degraded and subjected to high optical loss, our results demonstrated that it is possible to obtain positive key rates. After introducing a figure of merit for the strength of turbulence, we showed that in stronger turbulence regimes the beam spread dominates pointing errors and beam wandering, so that the latter effects can be ignored. We have then justified that the transmissivity estimated by a hybrid log-normal model can safely be used as a lower bound to the more elaborate extended Huygens-Fresnel model.

With these tools in hand, we have computed the ultimate bounds for FSO quantum communication in moderate-to-strong turbulence regimes. Besides establishing these ultimate limits, we have also derived practical and composable finite-key rates for CV-QKD operated in such a strong turbulent space. An important feature is the level of excess noise generated at the receiver which may greatly reduce the key rates and reduce the distance for secure communication. However, our analysis also shows that increasing the aperture of the receiver can mitigate the problem and revive the rates. As a main application of our results, we have then investigated satellite quantum communications at large zenith angles, specifically at the mask angle where not only turbulence is strong but also the elongation induced by refraction becomes relevant. This analysis allowed us to show that CV-QKD is feasible even in satellite links affected by strong turbulence, therefore removing the necessity and the restrictions associated with the weak turbulence regime which is at the basis of previous literature.

Methods

We here present the main techniques that are needed to prove or support the results of our main text.

Transmissivity in a turbulence media: log-normal atmospheric model. In the log-normal model the probability distribution for the transmissivity is given by[25]

$$\mathcal{P}(\eta)=\frac{1}{\eta\sigma\sqrt{2\pi}}\exp\left\{-\frac{(-\ln\eta-\mu)^2}{2\sigma^2}\right\}, \tag{30}$$

where $\mu=-\ln(\eta^2/\sqrt{\langle\eta^2\rangle})$ and $\sigma^2=\ln(\langle\eta^2\rangle/\eta^2)$ are parameters of the log-normal distribution. They are functions of the first and second moments of the transmissivity

$$\eta=\int_{\mathcal{A}}d^2\boldsymbol{r}\langle I(\boldsymbol{r},z)\rangle=\int_{\mathcal{A}}d^2\boldsymbol{r}\Gamma_2(\boldsymbol{r}) \tag{31}$$

and

$$\langle\eta^2\rangle=\int_{\mathcal{A}}d^2\boldsymbol{r}_1d^2\boldsymbol{r}_2\Gamma_4(\boldsymbol{r}_1,\boldsymbol{r}_2), \tag{32}$$

where the integration is performed over the circular aperture opening area $\mathcal{A}$. In the above equations, $\boldsymbol{r}=(xy)^T$ is the vector of transverse coordinates on the receiver plane.

The field coherence functions Γ_2 and Γ_4 are respectively given by[25]

$$\Gamma_2(\boldsymbol{r})=\frac{k^2}{4\pi^2z^2}\int_{\mathbb{R}^2}d^2\boldsymbol{r}'e^{-\frac{g^2|\boldsymbol{r}'|^2}{2w_0^2}-2i\frac{\Upsilon}{w_0^2}\boldsymbol{r}.\boldsymbol{r}'-\frac{1}{2}D_S(0,\boldsymbol{r}')} \tag{33}$$

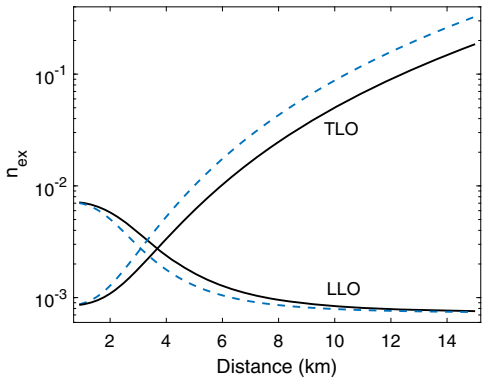

Fig. 7 Extra noise photons generated within a coherent receiver (homodyne detection). Here, we consider night- (solid black curves) and daytime (dashed blue curves) when a TLO/LLO technique is used. We have $\nu_{\rm det}=1$ SNU, NEP$=6\,{\rm pW}/\sqrt{\rm Hz}$, $W=100$ MHz, $\Delta t_{\rm LO}=10$ ns, $P_{\rm LO}=100$ mW, $V_A=8$ SNU, $l_{\rm w}=1.6$ KHz, $C=5$ MHz, and $hc=1.986\times10^{-25}$ J.m. Other parameters related to η are set as in Fig. 3.

and

$$\begin{aligned}\Gamma_4(\boldsymbol{r}_1,\boldsymbol{r}_2)=&\frac{2k^4}{\pi^2(2\pi)^3z^4w_0^2}\int_{\mathbb{R}^6}d^2\boldsymbol{r}_1'd^2\boldsymbol{r}_2'd^2\boldsymbol{r}_3'\\&\times e^{-\frac{1}{w_0^2}(|\boldsymbol{r}_1'|^2+|\boldsymbol{r}_2'|^2+|\boldsymbol{r}_3'|^2)}\\&\times e^{+2i\frac{\Upsilon}{w_0^2}[(1-z/R_0)\boldsymbol{r}_1'.\boldsymbol{r}_2'-(\boldsymbol{r}_1-\boldsymbol{r}_2).\boldsymbol{r}_2'-(\boldsymbol{r}_1+\boldsymbol{r}_2).\boldsymbol{r}_3']}\\&\times\exp\left[\frac{1}{2}\sum_{j=1,2}\{D_S(\boldsymbol{r}_1-\boldsymbol{r}_2,\boldsymbol{r}_1'+(-1)^j\boldsymbol{r}_2')\right.\\&\left.-D_S(\boldsymbol{r}_1-\boldsymbol{r}_2,\boldsymbol{r}'+(-1)^j\boldsymbol{r}_3')-D_S(0,\boldsymbol{r}_2'+(-1)^j\boldsymbol{r}_3')\}\right],\end{aligned} \tag{34}$$

where $\Upsilon=kw_0^2/(2z)$ is the Fresnel number of the transmitter aperture and $g^2=1+\Upsilon^2(1-z/R_0)^2$ is the generalized diffraction beam parameter. Here,

$$D_S(\boldsymbol{r},\boldsymbol{r}')=2\rho_0^{-5/3}\int_0^1d\xi\left|r\xi+r'(1-\xi)\right|^{5/3} \tag{35}$$

is the phase structure function, where ρ_0 is the radius of spatial coherence of the wave in the atmosphere.

The first moment of the transmissivity in Eq. (31) can be evaluated explicitly

$$\eta=1-e^{-\frac{2a_R^2}{w_{\rm lt,LN}^2}}, \tag{36}$$

where

$$\begin{aligned}w_{\rm lt,LN}^2&=S_{xx}+4\langle x_0^2\rangle\\&\equiv w_{\rm st,LN}^2+\sigma_{\rm tb}^2\end{aligned} \tag{37}$$

is the long-term beam size, with

$$\begin{aligned}S_{xx}=&4\left[\int_{\mathbb{R}^2}d^2\boldsymbol{r}x^2\Gamma_2(\boldsymbol{r},z)\right.\\&\left.-\int_{\mathbb{R}^4}d^2\boldsymbol{r}_1d^2\boldsymbol{r}_2x_1x_2\Gamma_4(\boldsymbol{r}_1,\boldsymbol{r}_2,z)\right]\end{aligned} \tag{38}$$

and

$$\langle x_0^2\rangle=\int_{\mathbb{R}^4}d^2\boldsymbol{r}_1d^2\boldsymbol{r}_2x_1x_2\Gamma_4(\boldsymbol{r}_1,\boldsymbol{r}_2,z). \tag{39}$$

Extra photons generated within the receiver. Considering a CV-QKD experiment, there are two techniques whereby one can measure the received signals through a coherent (homodyne or heterodyne) detection: transmitted local oscillator (TLO) and local local oscillator (LLO). In refs. [38,39], it is shown that these two may lead to generating totally different amounts of noisy photons within the coherent receiver system. This is mostly because extra photons generated by LLO, $\bar{n}_{\rm ex}^{\rm LLO}$, is a linear function of the link transmissivity, η, whereas extra photons generated by TLO, $\bar{n}_{\rm ex}^{\rm TLO}$, is an inverse function of it. Precisely, it reads (ref. [38], Eq. (62))

$$\bar{n}_{\rm ex}^{\rm LLO}=\Theta+\pi\eta V_Al_{\rm w}C^{-1}\ \text{and}\ \bar{n}_{\rm ex}^{\rm TLO}=\frac{\Theta}{\eta}, \tag{40}$$

where

$$\Theta = \frac{\nu_{\rm det} \mathrm{NEP}^2 W \Delta t_{\rm LO}}{2\hbar\omega P_{\rm LO}}, \tag{41}$$

with V_A being the modulation variance, $P_{\rm LO}$ the LO power, C the clock, $l_{\rm w}$ the linewidth, W the detector bandwidth, NEP the noise equivalent power, $\Delta t_{\rm LO}$ the LO pulse duration, and $\nu_{\rm det}$ the detection noise variance—$\nu_{\rm det} = 1(2)$ for a homodyne (heterodyne) measurement. We refer to ref. [38] for more detail.

In Fig. 7, we plot $\bar{n}_{\rm ex}$ versus distance. As seen at relatively large distances, i.e., the regime of strong turbulence, the LLO technique is the better detection scheme. However, the quality of LLO detection may be poorer due to overlapping a fresh LO with the signal. In TLO, both the signal and the LO undergo the same (atmospheric turbulent) conditions, so that when they are recombined at the receiver, ideally, no mismatch is expected. This is not the case of LLO which we discuss in more detail in the following.

LLO-induced loss. Suppose two continuous-wave optical beams—the signal E_S and the LO E_L—of the same frequency are incident on a beam splitter τ. Let us consider a balanced homodyne detection, i.e., $\tau = 1/\sqrt{2}$, where the output number of photons is given by[36,66]

$$\begin{aligned} n_- = \eta_{\rm eff} \int_0^T dt \int_{\mathcal{A}} d^2 r \big[& E_L^-(r,z,t) E_S^+(r,z,t) \\ & + E_S^-(r,z,t) E_L^+(r,z,t) \big], \end{aligned} \tag{42}$$

with spatial-temporal modes defined as follows

$$E_S^+(r,z,t) = i\hat{a}_S f_S(t) u_S(r,z), E_L^+(r,z,t) = i\hat{a}_L f_L(t) u_L(r,z), \tag{43}$$

and $\hat{a}$ being the corresponding annihilation operator.

Usually, for quantum tomography purposes and phase-sensitive detection, the LO field is assumed a monochromatic coherent state, with the on-axis amplitude $|\alpha_L|$, $f_L(t) = e^{-i\omega t}$, and $u_L(r,0)e^{i\phi_L}$ (plane wave) or $u_L(r,0) = e^{ikr}$ (spherical wave)[36,66–68]. This then follows

$$n_- \propto \eta_{\rm eff} |\alpha_L| \left(\hat{a}_S e^{i\Delta\phi} + \hat{a}_S^\dagger e^{-i\Delta\phi} \right) = \eta_{\rm eff} |\alpha_L| \hat{q}_S(\Delta\phi), \tag{44}$$

where $\hat{q}_S(\Delta\phi)$ is signal's quadrature with $\Delta\phi = \phi_S - \phi_L$.

Back to the coherent detection in a free-space scenario, in the following, we show that some loss is expected in the case of LLO, where signal's shape is different from that of the LO. We consider coherent Gaussian beams, which in the plane of the exit aperture of the transmitter are described by

$$u(r,0) = e^{-\frac{r^2}{w_0^2} \frac{-ikr^2}{2R_0}}, \tag{45}$$

where w_0 is the beam spot radius and R_0 is its phase front radius of curvature. For simplicity, we assume a collimated beam with $R_0 \to \infty$, such that

$$u(r,0) = e^{-\frac{r^2}{w_0^2}}. \tag{46}$$

At distance z a Gaussian beam may or may not keep its Gaussian form. If it does, the beam width w_0 will be replaced with $W(z)$—short- or long-term beam size according to the turbulence regime. However, in general, $u(r,z)$ can be distorted, or even completely destroyed, during a turbulent path. In that case, proper functions $u(r,z)$ should be used that reflect the effects of turbulence. We assume far-field conditions where Gaussian beams can be approximated by plane waves[31]. Therefore, in the case of TLO, the signal and the LO can be taken as pane waves that reduces the problem to previous (usual) coherent detection scenarios[36,66–68], with the expectation value of photocurrent from Eq. (42) as follows:

$$\langle n_- \rangle_{\rm TLO} \propto \eta_{\rm eff} |\alpha_S(z)| |\alpha_L(z)| \cos(\Delta\phi). \tag{47}$$

When it comes to LLO, we should consider the Gaussian shape of the fresh LO generated locally at the receiver, while we assume the signal has the form of a plane wave. By replacing Eq. (46) for the LO into Eq. (42), and assuming that signal and the LO are frequency matched, it is straightforward to find

$$\langle n_- \rangle_{\rm LLO} \propto \eta_{\rm eff} |\alpha_S(z)| |\alpha_L(0)| \cos(\Delta\phi) \frac{1}{\mathcal{N}_0} \int_{\mathcal{A}} dr\, r e^{-\frac{r^2}{W_L^2(0)}}, \tag{48}$$

which is also normalized by $\mathcal{N}_0 = \int_{\mathcal{A}\to\infty} dr\, r e^{-\frac{r^2}{W_L^2(0)}}$ (the receiver does not collect all the light). It is evident that the expression

$$\eta_{\rm LLO} := \frac{1}{\mathcal{N}_0} \int_{\mathcal{A}} dr\, r e^{-\frac{r^2}{W_L^2(0)}} \tag{49}$$

has the same nature as the quantum efficiency of the detectors $\eta_{\rm eff}$; hence, can be considered as extra loss. One can implicitly find that

$$\eta_{\rm LLO} = 1 - e^{-\frac{a_R^2}{W_L^2(0)}}. \tag{50}$$

For the special case where the aperture size (or equivalently the lenses that collect and focus the beam on the detection's beam splitter) is equal to the LO's initial size, we have $\eta_{\rm LLO} = 1 - e^{-1} = 0.63$.

The overall transmissivity can then be written as follows:

$$\eta = \eta_{\rm lt} \eta_{\rm eff} \eta_{\rm cd} \eta_{\rm atm}, \tag{51}$$

where $\eta_{\rm cd}$ represents $\eta_{\rm TLO}$ or $\eta_{\rm LLO}$. In our estimation of composable CV-QKD rates, we use $\eta_{\rm cd} = 0.63$.

We remark that a more precise evaluation involves working out a more precise shape of the beam after propagating through a turbulent medium, where $u_{S/LO}(r,z)$ functions that include the effects of turbulent are known. One possible procedure is as follows: due to the extended Huygens-Fresnel principle the optical wave field after propagating a distance z through a turbulent space is given by solving ref. [31] (Eq. (21), Chapt. 7), where the most complex function seems to be the complex phase perturbation of the field[69,70]. One can then compute a more accurate loss coherent detection $\eta_{\rm cd}$ from the above methodology.

Details of key rate analysis and parameter estimation. For the secret-key rate analysis, we use to consider the entanglement-based representation of the coherent-state QKD protocol. We assume a collective Gaussian entangling-cloner attack[71]. At each run of the protocol Alice shares one leg of a two-mode squeezed vacuum (TMSV) state, with variance μ, through a communications link with Bob. This is equivalent to the prepare and measure version of the protocol, where Alice prepares coherent states by a bivariate Gaussian modulation with variance $\sigma_x^2 = \mu - 1$. Assuming that the link is a thermal-loss channel, characterized by the transmissivity η and thermal noise $\bar{n}$, the end-to-end covariance matrix between Alice and Bob has the form

$$\mathbf{V}_{AB} = \begin{pmatrix} a\mathbb{1} & c\mathbb{Z} \\ c\mathbb{Z} & b\mathbb{1} \end{pmatrix}, \tag{52}$$

where $a = \mu$, $b = \eta(\mu - 1) + 2\bar{n} + 1$, $c = \sqrt{\eta(\mu^2 - 1)}$, $\mathbb{1} = \mathrm{diag}(1,1)$ and $\mathbb{Z} = \mathrm{diag}(1,-1)$.

Having the triplet (a,b,c), and assuming a homodyne measurement at Bob's side, the asymptotic key rate in the reverse reconciliation case is given by

$$R_{\rm asy}(\eta,\bar{n}) = \beta I_{AB}(\eta,\bar{n}) - \chi_{EB}(\eta,\bar{n}) \tag{53}$$

where

$$I_{AB}(\eta,\bar{n}) = \frac{1}{2}\log_2\left(1 + \frac{\eta(\mu-1)}{2\bar{n}+1}\right), \tag{54}$$

also, assuming that the eavesdropper purifies the entangled state between Alice and Bob, one finds

$$\chi_{BE}(\eta,\bar{n}) = h\left(\frac{\nu_+ - 1}{2}\right) + h\left(\frac{\nu_- - 1}{2}\right) - h\left(\frac{\nu_c - 1}{2}\right). \tag{55}$$

with $h(x)$ given in the main text, $\nu_\pm = \left(\sqrt{(a+b)^2 - 4c^2} \pm (b-a)\right)/2$, and $\nu_c = \sqrt{a(ab-c^2)/b}$.

In a realistic setting, Alice and Bob should compute the values of η and $\bar{n}$ in order to estimate the key rate in Eq. (53). This computation is carried out by using only a finite number of runs, which inevitably reduces the rate to $R_{\rm pe}(\eta_{\rm wc}, \bar{n}_{\rm wc})$, for the worst-case values are $\eta_{\rm wc} \le \eta$ and $\bar{n}_{\rm wc} \ge \bar{n}$[72,73].

Before discussing the worst-case scenario parameters, let us point out a matter that eases the parameter estimation in the case of moderate-to-strong turbulence. Unlike the case of a weak turbulence medium[38], where the link transmissivity varies instantaneously, we can assume a fixed loss and a fixed number of thermal photons in the moderate-to-strong turbulence regime due to the fact that beam wandering is negligible here; see Fig. 1. Therefore, we assume a thermal-loss channel that is characterised by transmissivity η and mean number of thermal photons $\bar{n}$. This channel induces an input–output relation $y = \sqrt{\eta}x + z$ between the input Gaussian variable x and the output variable y, with z being a Gaussian noise variable; the variables x and z have zero mean with variances $\mu - 1$ and $\sigma_z^2 = 2\bar{n} + 1$, respectively.

Back to the estimation of the worst-case parameters, by revealing m pairs of corresponding data, i.e., $[x]_i$ and $[y]_i$, Alice and Bob can build an estimator $\widehat{T}$ of the square root of transmissivity $T = \sqrt{\eta}$, that is $\widehat{T} := m^{-1}\sigma_x^{-2}\sum_{i=1}^m x_i y_i$, with variance $\mathrm{Var}(\widehat{T}) = m^{-1}(2\eta + \sigma_x^{-2}\sigma_z^2)$, where $\sigma_x^2 = \sum_{i=1}^m x_i^2 \simeq \mu - 1$. Then, the estimator for transmissivity is $\widehat{\eta} = (\widehat{T})^2$, with variance $\mathrm{Var}(\widehat{\eta}) = 4m^{-1}\eta^2\left(2 + \eta^{-1}\sigma_x^{-2}\sigma_z^2\right) + \mathcal{O}(m^{-2})$. Similarly, Alice and Bob can construct the estimator for $\bar{n}$, that is, $\widehat{\bar{n}} := (\widehat{\sigma_z^2} - 1)/2$, with variance $\mathrm{Var}(\widehat{\bar{n}}) = \sigma_z^4/(2m)$. Here, $\widehat{\sigma_z^2} = m^{-1}\sum_{i=1}^m z_i^2$ is the estimator for the variance of the thermal noise σ_z^2.

Next, by assuming a certain number w of confidence of intervals, Alice and Bob compute the worst-case estimators up to some probability of error $\varepsilon_{\rm pe}(w) = \left[1 - \mathrm{erf}(w/\sqrt{2})\right]/2$, i.e.,

$$\eta_{\rm wc} = \eta - 2w\sqrt{\frac{2\eta^2 + \eta\sigma_x^{-2}\sigma_z^2}{m}}, \ \bar{n}_{\rm wc} = \bar{n} + w\frac{\sigma_z^2}{\sqrt{2m}}. \tag{56}$$

Data availability

All data in this paper can be reproduced by using the methodology described.

Code availability

Code is available at https://github.com/softquanta/Strong_Turbulence.

Received: 27 July 2021; Accepted: 19 January 2022;
Published online: 10 February 2022

References

1. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
2. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* 175–179 (IEEE, New York, Bangalore, India, 1984).
3. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
4. Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z. & Pan, J.-W. Large scale quantum key distribution: challenges and solutions. *Opt. Express* **26**, 24260–24273 (2018).
5. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
6. Pittaluga, M. et al. 600 km repeater-like quantum communications with dual-band stabilisation. Preprint at https://arxiv.org/abs/2012.15099 (2020).
7. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
8. Pirandola, S. & Braunstein, S. L. Unite to build the quantum internet. *Nature* **532**, 169 (2016).
9. Sidhu, J. S. et al. Advances in space quantum communications. *IET Quant. Commun.* **2,** 182–217 (2021).
10. Belenchia, A. et al. Quantum physics in space. *Physics Reports* **951,** 1–70 (2022).
11. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
12. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
13. Liao, S.-K. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photon* **311**, 509 (2017).
14. Ren, J.-G. et al. Ground-to-satellite quantum teleportation. *Nature* **549**, 70 (2017).
15. Usenko, V. C. et al. Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels. *N. J. Phys.* **14**, 093048 (2012).
16. Papanastasiou, P., Weedbrook, C. & Pirandola, S. Continuous-variable quantum key distribution in uniform fast-fading channels. *Phys. Rev. A* **97**, 032311 (2018).
17. Wang, S., Huang, P., Wang, T. & Zeng, G. Atmospheric effects on continuous-variable quantum key distribution. *N. J. Phys.* **20**, 083037 (2018).
18. Derkach, I., Usenko, V. C. & Filip, R. Squeezing-enhanced quantum key distribution over atmospheric channels. *N. J. Phys.* **22**, 053006 (2020).
19. Derkach, I. & Usenko, V. C. Applicability of squeezed- and coherent-state continuous-variable quantum key distribution over satellite links. *Entropy* **23**, 55 (2020).
20. Dequal, D. et al. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Inf.* **7**, 3 (2021).
21. Gyongyosi, L. Multicarrier continuous-variable quantum key distribution. *Theor. Computer Sci.* **816**, 67–95 (2020).
22. Chai, G., Huang, P., Cao, Z. & Zeng, G. Suppressing excess noise for atmospheric continuous-variable quantum key distribution via adaptive optics approach. *N. J. Phys.* **22**, 103009 (2020).
23. Zheng, D. et al. Free space to few-mode fiber coupling efficiency improvement with adaptive optics under atmospheric turbulence. in *Optical Fiber Communication Conference*, Th3C.2 (Optical Society of America, 2017).
24. Cao, J., Zhao, X., Liu, W. & Gu, H. Performance analysis of a coherent free space optical communication system based on experiment. *Opt. Express* **25**, 15299–15312 (2017).
25. Vasylyev, D., Semenov, A. A. & Vogel, W. Atmospheric quantum channels with weak and strong turbulence. *Phys. Rev. Lett.* **117**, 090501 (2016).
26. Vasylyev, D., Vogel, W. & Moll, F. Satellite-mediated quantum atmospheric links. *Phys. Rev. A* **99**, 053830 (2019).
27. Günthner, K. et al. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica* **4**, 611–616 (2017).
28. Usenko, V. C. et al. Stabilization of transmittance fluctuations caused by beam wandering in continuous-variable quantum communication over free-space atmospheric channels. *Opt. Express* **26**, 31106–31115 (2018).
29. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
30. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019).
31. Andrews, L. C. & Phillips, R. L. *Laser Beam Propagation Through Random Medium*, 2nd edn (SPIE, 2005).
32. Kaushal, H, Jain, V. K & Kar, S. *Free Space Optical Communication* (Springer, 2017).
33. Goodman, J. W. *Statistical Optics* (John Wiley & Sons, Inc., 1985).
34. Siegman, A. *Lasers* (University Science Books, 1986).
35. Svelto, O. *Principles of Lasers*. 5th (Springer, 2010).
36. Fried, D. L. Optical heterodyne detection of an atmospherically distorted signal wave front. *Proc. IEEE* **55**, 57–77 (1967).
37. Murty, S. S. R. Electromagnetic beam propagation in turbulent media. *Proc. Indian Acad. Sci.* **2**, 179–195 (1979).
38. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).
39. Pirandola, S. Satellite quantum communications: fundamental bounds and practical security. *Phys. Rev. Res.* **3**, 023130 (2021).
40. Fante, R. L. Electromagnetic beam propagation in turbulent media. *Proc. IEEE* **63**, 1669–1692 (1975).
41. Mironov, V. L. & Nosov, V. V. On the theory of spatially limited light beam displacements in a randomly inhomogeneous medium. *J. Opt. Soc. Am.* **67**, 1073–1080 (1977).
42. Yura, H. T. Short-term average optical-beam spread in a turbulent medium. *J. Opt. Soc. Am.* **63**, 567–572 (1973).
43. Klyatskin, V. I. & Kon, A. I. On the displacement of spatially-bounded light beams in a turbulent medium in the markovian-random-process approximation. *Radiophys. Quantum Electron* **15**, 1056–1061 (1972).
44. Kerr, J. R. & Dunphy, J. R. Experimental effects of finite transmitter apertures on scintillations. *J. Opt. Soc. Am.* **63**, 1 (1973).
45. Raidt, H. & Höhn, D. H. Instantaneous intensity distribution in a focused laser beam at 0.63 μm and 10.6 μm propagating through the atmosphere. *Appl. Opt.* **14**, 2747–2749 (1975).
46. Andrews, L. C., Phillips, R. L. & Hopen, C. Y. *Laser Beam Scintillation with Applications*, 2nd edn (SPIE, 2001).
47. Rytov, S. M. Diffraction of light by ultrasonic waves. *Izvestiya Akademii Nauk SSSR, Seriya Fizicheskaya* **2**, 223–259 (1937).
48. Sommerfeld, A. Ein beitrag zur hydrodynamischen erkläerung der turbulenten flüssigkeitsbewegüngen (a contribution to hydrodynamic explanation of turbulent fluid motions). *Int. Congr. Mathematicians* **3**, 116–124 (1908).
49. Rhodes, M. J. *Introduction to Particle Technology*, 2nd edn (John Wiley & Sons Ltd., 2008).
50. Yura, H. T. Atmospheric turbulence induced laser beam spread. *Appl. Opt.* **10**, 2771–2773 (1971).
51. Andrews, L. C., Miller, W. B. & Ricklin, J. C. Spatial coherence of a gaussian-beam wave in weak and strong optical turbulence. *J. Opt. Soc. Am. A* **11**, 1653–1660 (1994).
52. Capraro, I. et al. Impact of turbulence in long range quantum and classical communications. *Phys. Rev. Lett.* **109**, 200502 (2012).
53. Duntley, S. Q. The reduction of apparent contrast by the atmosphere. *J. Opt. Soc. Am.* **38**, 179–191 (1948).
54. Bohren, C. F. & Huffman, D. R. *Absorption and Scattering of Light by Small Particles* (John Wiley & Sons Inc., 2008).
55. Er-long, M. et al. Background noise of satellite-to-ground quantum key distribution. *N. J. Phys.* **7**, 215–215 (2005).
56. Liorni, C., Kampermann, H. & Bruß, D. Satellite-based links for quantum key distribution: beam effects and weather dependence. *N. J. Phys.* **21**, 093055 (2019).
57. García-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102**, 210501 (2009).
58. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
59. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
60. Furrer, F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **109**, 100502 (2012).
61. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
62. Grosshans, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
63. Pirandola, S. Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.* **3**, 043014 (2021).

64. Andrews, L. C., Phillips, R. L. & Young, C. Y. Scintillation model for a satellite communication link at large zenith angles. *Optical Eng.* **39**, 3272–3280 (2000).
65. Cappelletti, C., Battistini, S. & Malphrus, B. K. *CubeSat Handbook: From Mission Design to Operations* (Academic Press, 2021).
66. Raymer, M. G., Cooper, J., Carmichael, H. J., Beck, M. & Smithey, D. T. Ultrafast measurement of optical-field statistics by dc-balanced homodyne detection. *J. Opt. Soc. Am. B* **12**, 1801–1812 (1995).
67. Leonhardt, U. *Measuring the Quantum State of Light* (Cambridge University Press, 1997).
68. Milburn, D. W. G. J. *Quantum Optics*, 2nd edn (Springer, 2008).
69. Lutomirski, R. F. & Yura, H. T. Propagation of a finite optical beam in an inhomogeneous medium. *Appl. Opt.* **10**, 1652–1658 (1971).
70. Yura, H. T. & Hanson, S. G. Second-order statistics for wave propagation through complex optical systems. *J. Opt. Soc. Am. A* **6**, 564–575 (1989).
71. Pirandola, S., Braunstein, S. L. & Lloyd, S. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 200504 (2008).
72. Ruppert, L., Usenko, V. C. & Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **90**, 062310 (2014).
73. Ruppert, L. et al. Fading channel estimation for free-space continuous-variable secure quantum communication. *N. J. Phys.* **21**, 123036 (2019).

Acknowledgements

M.G. would like to thank Dmytro Vasylyev for helpful discussion regarding trajectory elongation. This work has been funded by the European Union via "Continuous Variable Quantum Communications" (CiViQ, Grant Agreement No. 820466).

Author contributions

All authors contributed to the scientific discussions and the theoretical developments of the work. M.G. studied properties of optical beams in the presence of strong turbulence, performed analysis security of the CV-QKD protocols in the presence of practical imperfections, obtained the analytical results, and wrote the paper. S.P. proposed the core idea, analysed the outcomes, edited the paper and supervised the entire project.

Competing interests

The authors declare no competing interests. S.P. is an Editorial Board Member for *Communications Physics*, but was not involved in the editorial review of, or the decision to publish this article.

Additional information

Correspondence and requests for materials should be addressed to Masoud Ghalaii.

Peer review information *Communications Physics* thanks the anonymous reviewers for their contribution to the peer review of this work.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.