UNIVERSITY of York

This is a repository copy of *Satellite Quantum Communications : Fundamental Bounds and Practical Security*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/174369/

Version: Published Version

Article:
Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2021) Satellite Quantum Communications : Fundamental Bounds and Practical Security. Physical Review Research. 023130. ISSN 2643-1564

https://doi.org/10.1103/PhysRevResearch.3.023130

Reuse
This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here: https://creativecommons.org/licenses/

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Satellite quantum communications: Fundamental bounds and practical security

Stefano Pirandola
Department of Computer Science, University of York, York YO10 5GH, United Kingdom

(Received 7 November 2020; accepted 20 April 2021; published 19 May 2021)

Satellite quantum communications are emerging within the panorama of quantum technologies as a more effective strategy to distribute completely secure keys at very long distances, therefore playing an important role in the architecture of a large-scale quantum network. In this work, we apply and extend recent results in free-space quantum communications to determine the ultimate limits at which secret (and entanglement) bits can be distributed via satellites. Our study is comprehensive of the various practical scenarios, encompassing both downlink and uplink configurations, with satellites at different altitudes and zenith angles. It includes effects of diffraction, extinction, background noise, and fading, due to pointing errors and atmospheric turbulence (appropriately developed for slant distances). Besides identifying upper bounds, we also discuss lower bounds, i.e., achievable rates for key generation and entanglement distribution. In particular, we study the composable finite-size secret key rates that are achievable by protocols of continuous variable quantum key distribution, for both downlink and uplink, showing the feasibility of this approach for all configurations. Finally, we present a study with a sun-synchronous satellite, showing that its key distribution rate is able to outperform a ground chain of ideal quantum repeaters.

DOI: 10.1103/PhysRevResearch.3.023130

I. INTRODUCTION

Satellite quantum communications ([1], Sec. VI) represent a new collective endeavour of the scientific community, with pioneering experiments already demonstrated. A number of quantum protocols have been successfully realized, including satellite-to-ground quantum key distribution (QKD) [2–4], entanglement distribution [5], entanglement-based QKD [6,7], and ground-to-satellite quantum teleportation [8]. Further experiments have considered a space laboratory (Tiangong-2 [9]), and microsatellites, such as SOCRATES [10] and CubeSats [11].

An important driving reason behind the development of free-space quantum communications with satellites is the possibility to by-pass fundamental limitations that restrict rates and distances achievable by ground-based fiber communications. It is in fact well known that the amount of secret bits or entanglement bits (ebits) that can be distributed through a lossy communication channel with transmissivity η cannot exceed its secret key capacity $-\log_2(1-\eta)$ bits/use, also known as the repeaterless PLOB bound [12] (see also Ref. [13] for the very first investigation of the fundamental limits of quantum communication). In a ground-based fiber link, the transmissivity decays exponentially with the distance and so does the communication rate of any protocol for QKD or entanglement distribution.

One strategy to mitigate such a problem is the introduction of quantum repeaters or relays ([1], Sec. XII). In QKD, the cheapest solution is the use of a chain of trusted nodes between the two end-users. These nodes distribute pairs of keys with their neighbors, whose composition via one-time pad generates a final secret key for the remote users. Here a nontrivial issue is the fact that all the nodes need to be trusted, so that the longer is the chain, the higher is the probability that security could be compromised. An alternative strategy relies in the adoption of nodes able to distribute entanglement, which is then swapped to the remote users. However, this solution is rather expensive because it involves the development of quantum repeaters with long coherence times and distillation capabilities.

In this scenario, satellites open the way for new opportunities. Free-space connection with a satellite may have far less decibels of loss than a long ground-based fiber connection. Furthermore, most satellites are fast-moving objects, therefore able to physically travel between two far locations over the globe. These features have the potential to drastically reduce the complexity of a ground-based quantum network. In fact, a chain of nodes could just be replaced by a single satellite acting as a trusted QKD node or as a distributor of entanglement. In such an exciting new setting, it is crucial to understand the optimal performances allowed by quantum mechanics, and also what practical performances may be achieved with current technology. This work serves for this purpose.

Here we establish the information-theoretic limits of satellite quantum communications and also show their practical security on the basis of state-of-the-art technology. Our study extends the free-space analysis of Ref. [14], there developed for ground-to-ground free-space communications, to the more general setting of ground-satellite communications, where the

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

optical signals travel slant distances with variable altitudes and zenith angles (in uplink or downlink). This scenario involves more general models for the underlying physical processes occurring within the atmosphere (refraction, extinction and turbulence), and different descriptions for the background noise (planetary albedos besides sky brightness). Accounting for these accurate models, we study the ultimate rates for secret key generation and entanglement distribution with a satellite in all scenarios (uplink/downlink, night/day-time operations).

Once we established the ultimate converse rates for secret key and entanglement distribution, we also study lower bounds. In particular, we focus our investigation on the practical rates that are achievable by a coherent-state QKD protocol, suitably modified to account for the fading channel between satellite and ground station, and including the orbital dynamics of the satellite. Our security analysis considers finite-size effects and composable aspects. We show that high-rate ground-satellite QKD with continuous variable (CV) systems [15] is feasible for both downlink and uplink, during night and day.

Finally, we show that the number of secret key bits per day that can be distributed between two stations by a sun-synchronous satellite can be much larger than what achievable by a standard fiber connection between these stations, even when a substantial number of repeaters are employed in the middle and assumed to operate at their capacity level [16]. This analysis proves the potential advantages of satellite links over ground networks and strongly corroborates their role for near-future realization of large-scale quantum communications.

A. Structure of the paper

The paper has two main parts. In the first part, we investigate the fundamental bounds for satellite quantum communications (Sec. II). We start with some basic geometric considerations (Sec. II A) and then we present general upper bounds based on free-space diffraction (Sec. II B). We then increase the complexity of the description by introducing atmospheric extinction and setup inefficiencies (Sec. II C). Next we describe the fading process induced by pointing errors and turbulence (Sec. II D), followed by the corresponding expressions of the loss-limited upper bounds for key and entanglement distribution (Sec. II E). In our next generalization (Sec. II F), we consider the effect of background thermal noise and derive more advanced thermal-loss upper and lower bounds for key and entanglement distribution with the satellite.

Once we have established the ultimate performances, we then study the secret key rates that are achievable in satellite CV-QKD accounting for composable finite-size aspects, fading and orbital dynamics. This is the second part of the paper (Sec. III). We start with an overview of the problem (Sec. III A) and a discussion on the composable security at fixed transmissivity (Sec. III B). Then, we delve into the problem of free-space fading by discussing the use of pilots, post-selection, and a suitable defading technique (Sec. III C). Next we discuss how to perform parameter estimation and we provide the general forms of the composable key rates (Sec. III D). After important observations on the setup noise (Sec. III E), we analyze the performances of the key rates accounting for the orbital dynamics (Secs. III F and III G). Finally, we show how the satellite-based key rates can overcome the performance of a chain of quantum repeaters on the ground (Sec. III H). Section IV is for conclusions.

II. FUNDAMENTAL BOUNDS FOR SATELLITE QUANTUM COMMUNICATIONS

A. Geometric considerations

Consider a ground station (G), at some relatively low altitude $h_0 \simeq 0$ above the sea level, and a satellite (S), that is orbiting at some variable altitude h beyond the Kármán line ($h \geqslant 100$ km) with a variable zenith angle θ. The latter is the angle between the zenith point at the ground station and the direction of observation pointing at the satellite. It takes positive values between 0 (satellite at the zenith) and $\pi/2$ (satellite at the horizon). For a zenith-crossing orbit (studied later in Sec. III G), it may be useful to associate a sign to θ, so that $-\pi/2$ represents the "front" horizon and $+\pi/2$ is the "back" horizon. (Including the sign does not change the main geometric formulas since θ appears in cosine functions).

Calling $R_{\rm E} \simeq 6371$ km the approximate radius of the Earth, the slant distance z between the ground station and the satellite can be written as

$$z(h,\theta) = \sqrt{h^2 + 2hR_{\rm E} + R_{\rm E}^2 \cos^2\theta} - R_{\rm E}\cos\theta. \tag{1}$$

Equivalently, the altitude h of the satellite reads

$$h(z,\theta) = \sqrt{R_{\rm E}^2 + z^2 + 2zR_{\rm E}\cos\theta} - R_{\rm E}. \tag{2}$$

See Appendix A for more details on this geometry, which can be easily extended to the case of non-negligible atmospheric altitudes h_0 for the ground station. (We remark that, while this extension may be useful, in our main text, we investigate the basic scenario of a low-altitude ground station for which h_0 can be considered to be negligible with respect to the typical satellite altitudes.)

The formulas above are very good approximations for angles $\theta \lesssim 1$ (i.e., within about 60° from the zenith). For larger zenith angles, one needs to consider the apparent angle and the optical-path elongation induced by atmospheric refraction, which become more and more prominent close to the horizon. In such a case, the formulas above undergo some modifications as discussed in Appendix B. In our main text below, we omit this technicality for two reasons: (i) formulas above can still be used to provide (larger) upper bounds in the proximity of the horizon; (ii) when we treat achievable rates (lower bounds), we will restrict our study to the good window $\theta \lesssim 1$, an assumption which is also justified by the analysis of turbulence carried out later on in the manuscript.

In terms of configurations, we consider both uplink and downlink. In uplink, the ground station is the transmitter (Alice) and the satellite is the receiver (Bob); in downlink, it is the satellite to be the transmitter and the ground station to operate as a receiver. In these two configurations, the effects of free-space diffraction and atmospheric extinction are the same. Different is the case for the fading induced by turbulence (more relevant in uplink) and the thermal noise induced

by background sources (with further differences between day- and night-time operations). For the sake of simplicity, we start by accounting for diffraction and extinction only; then, we will introduce the other effects, which need to be treated quite differently with respect to the models that are valid for ground-to-ground free-space communications.

B. Free-space diffraction

We assume that free-space quantum communication is based on a quasi-monochromatic optical mode with temporal duration Δt and narrow bandwidth $\Delta\lambda$ around a carrier wavelength λ (so that the angular frequency is $\omega = 2\pi c/\lambda$ and the wave number is $k = \omega/c = 2\pi/\lambda$). This model is represented by a Gaussian beam with field spot size w_0 and curvature R_0 [17–20]. Spot size is sufficiently smaller than the transmitter's aperture so that the latter does not induce relevant diffraction. After free-space propagation for a distance z, the beam is detected by a receiver whose telescope has a circular aperture with radius a_R. To fix the ideas, one can assume that the propagation direction is uplink so that the ground station is the transmitter, but the model is completely symmetric and applies to downlink in exactly the same way.

Because of the inevitable free-space diffraction, the waist of the beam will broaden during propagation. After traveling for a distance z, the beam is intercepted by the receiver that will see an increased spot size

$$w_d(z) = w_0\sqrt{(1 - z/R_0)^2 + (z/z_R)^2}, \tag{3}$$

where $z_R := \pi w_0^2\lambda^{-1}$ is the Rayleigh range. Due to the finite aperture a_R of the receiving telescope, only a fraction of the initial beam will be detected, and this fraction is given by the diffraction-induced transmissivity

$$\eta_d(z) = 1 - e^{-2a_R^2/w_d^2}. \tag{4}$$

In the far field $z \gg z_R$, this can be approximated as

$$\eta_d \simeq \eta_d^{\rm far} := \frac{2a_R^2}{w_d^2} \ll 1. \tag{5}$$

Using η_d with the PLOB bound [12], one finds that the maximum number of secret bits that can be distributed by the most general (adaptive) QKD protocols over the free-space communication channel is upper bounded by [14]

$$\mathcal{U}(z) = \frac{2}{\ln 2}\frac{a_R^2}{w_d^2} \text{ bits per use.} \tag{6}$$

In other words, the secret key capacity K of the free-space channel must satisfy $K \leqslant \mathcal{U}$ and, similarly, this bound also holds for the channel's entanglement distribution capacity $E \leqslant K$ (which is the number of ebits per use of the channel that can be distributed by the most general adaptive protocols of entanglement distribution; see Ref. [12] for exact mathematical definitions).

Note that a focused beam ($R_0 = z$) optimizes the bound in Eq. (6) but, at long distances, optical focusing becomes a very challenging task. For this reason, a better strategy is to just generate a collimated beam ($R_0 = \infty$) so Eq. (6) is computed by assuming

$$w_d(z) = w_0\sqrt{1 + z^2/z_R^2}. \tag{7}$$

We will therefore use the specific case of a collimated Gaussian beam in our numerical investigations.

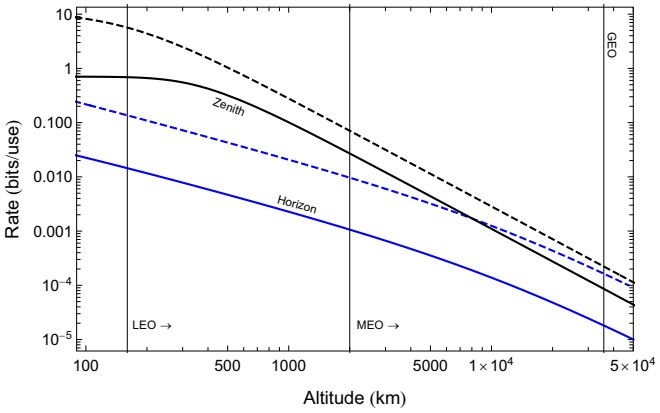

FIG. 1. Key rate between a ground station and a satellite at various altitudes h. In dashed we show the diffraction-based bound $\mathcal{U}(h,\theta)$ of Eq. (6) while, in solid, we show the upper bound $\mathcal{V}(h,\theta)$ of Eq. (15) which includes the combined effects of diffraction, extinction and quantum efficiency. The upper black curves refer to the satellite at the zenith position ($\theta = 0$), while the lower blue curves refer to the horizon position ($\theta = \pi/2$). We assume a collimated Gaussian beam with $\lambda = 800$ nm and $w_0 = 20$ cm, so that $z_{\rm R} \simeq 160$ km (LEO boundary). Then, we assume $a_R = 40$ cm and $\eta_{\rm eff} = 0.4$.

It is also clear that $\mathcal{U}(z)$ can be expressed in terms of the altitude h and zenith angle θ of the satellite. In fact, we may replace the function $z = z(h,\theta)$ of Eq. (1) in Eq. (6) to get the expression for $\mathcal{U}(h,\theta) = \mathcal{U}[z(h,\theta)]$. The diffraction-bound $\mathcal{U}(h,\theta)$ is numerically investigated in Fig. 1, for a collimated Gaussian beam and a typical choice of parameters. In particular, we show this ultimate bound in two extreme angles for the satellite, i.e., zenith position ($\theta = 0$) and horizon ($\theta = \pi/2$). The reduction of the rate at the horizon is due to the greater slant distance to be traveled by the beam. As mentioned before, in this case the bound is optimistic because the refraction-induced elongation of the optical path is here neglected.

C. Atmospheric extinction

Another important physical process that causes loss in the free-space propagation of an optical beam is atmospheric extinction; this is induced by both aerosol absorption and Rayleigh/Mie scattering. For a free-space communication at fixed altitude h, this effect is described by the simple Beer-Lambert equation

$$\eta_{\rm atm}(h) = \exp[-\alpha(h)z], \tag{8}$$

where $\alpha(h)$ is the extinction factor ([21], Ch. 11). This is given by $\alpha(h) = \alpha_0\exp(-h/\tilde{h})$, where h is expressed in meters, $\tilde{h} = 6600$ m, and the sea-level value α_0 takes the value $\simeq 5\times10^{-6}$ m^{-1} at $\lambda = 800$ nm ([22], Sec. III C).

It is clear that the model in Eq. (8) needs to be suitably modified in order to describe free-space optical communications at variable altitudes h. First suppose that the satellite is exactly at the zenith, so that its slant range z is equal to its altitude h. Then, we can easily compute

$$\begin{aligned}\eta_{\rm atm}^{\rm zen}(h) &= \exp\left[-\int_0^h dh'\alpha(h')\right] \\ &= \exp[\alpha_0\tilde{h}(e^{-h/\tilde{h}}-1)] \\ &\geqslant e^{-\alpha_0\tilde{h}} \simeq 0.967\ (\simeq 0.14\ {\rm dB}).\end{aligned} \tag{9}$$

The value in Eq. (9) is valid for any altitude and is already approximated at $h = 30$ km, in the middle of the stratosphere, after which the atmospheric density is negligible. For this reason, for any satellite at the zenith position, we can use the estimate $\eta_{\rm atm}^{\rm zen}(\infty) \simeq 0.967$.

Consider now a generic zenith angle θ. Neglecting refraction, we can therefore use the expressions in Eqs. (1) and (2), and write the following expression for the atmospheric transmissivity:

$$\eta_{\rm atm}(h,\theta) = \exp\left\{-\int_0^{z(h,\theta)} dy\,\alpha[h(y,\theta)]\right\} = e^{-\alpha_0 g(h,\theta)}, \tag{10}$$

where we have introduced the integral function

$$g(h,\theta) := \int_0^{z(h,\theta)} dy \exp\left[-\frac{h(y,\theta)}{\tilde{h}}\right]. \tag{11}$$

For zenith angles $\theta \lesssim 1$, one may check that Eq. (10) can be approximated as follows:

$$\eta_{\rm atm}(h,\theta) \simeq \left[\eta_{\rm atm}^{\rm zen}(h)\right]^{\sec\theta} \simeq \left[\eta_{\rm atm}^{\rm zen}(\infty)\right]^{\sec\theta}. \tag{12}$$

This approximation is already good at 30 km of altitude and becomes an almost exact formula beyond 100 km.

Combining atmospheric extinction with free-space diffraction and the inevitable internal loss $\eta_{\rm eff}$ affecting the setup of the receiver (due to nonunit quantum efficiency of the detector and other optical imperfections), we can write the total amount of fixed loss of the free-space channel from the generation of the Gaussian beam to its final detection. This is given by

$$\eta_{\rm tot}(h,\theta) := \eta_{\rm eff}\eta_{\rm atm}(h,\theta)\eta_d(h,\theta), \tag{13}$$

where $\eta_d(h,\theta) = \eta_d[z(h,\theta)]$ and we can assume $\eta_{\rm eff} \simeq 0.4$, i.e., about 4 dB (e.g., as in Ref. [23]). Using this transmissivity in the PLOB bound, we get an immediate extension of a result in Ref. [14], i.e.,

$$K \leqslant \mathcal{V}(h,\theta) := -\log_2[1-\eta_{\rm tot}(h,\theta)] \tag{14}$$

$$= -\log_2\left[1-\eta_{\rm eff}e^{-\alpha_0 g(h,\theta)}\left(1-e^{-\frac{2a_R^2}{w_d[z(h,\theta)]^2}}\right)\right] \tag{15}$$

$$\simeq \frac{2}{\ln 2}\frac{a_R^2\eta_{\rm eff}e^{-\alpha_0 g(h,\theta)}}{w_d[z(h,\theta)]^2}, \tag{16}$$

where the last approximation is valid for $\eta_{\rm tot}(h,\theta) \ll 1$ which is certainly true in the far field regime $z \gg z_R$.

From Fig. 1, we see that the combined effects of diffraction, extinction and nonideal quantum efficiency decrease (by about one order of magnitude) the ultimate communication bounds that are only based on free-space diffraction. As for $\mathcal{U}(h,\theta)$, also the value of the upper bound $\mathcal{V}(h,\theta)$ is overestimated at the horizon due to the fact that refraction has been neglected (see Appendix B for an extension of the bound which includes refraction). The ultimate performances discussed so far will further decrease when we include fading (turbulence/pointing errors) and then background noise.

D. Fading process induced by beam wandering: turbulence and pointing errors

The combined transmissivity $\eta_{\rm tot}$ in Eq. (13) is constant for a fixed geometry, h and θ, between ground station and satellite. At each time instant, it corresponds to the maximum transmissivity which can be reached by a beam that is perfectly aligned between transmitter and receiver. In a realistic scenario, such alignment is however not maintained and we need to consider a process of beam wandering; this inevitably induces a fading process for the communication channel whose instantaneous transmissivity will fluctuate [24–27].

Beam wandering is due to random errors in the pointing mechanism of the transmitter and also to the action of atmospheric turbulence on a section of the optical path. These two effects are independent and they sum up. In practice, they have a different weights depending on the configuration. In downlink, pointing error is quite relevant, since on-board optics is limited, while turbulence can be neglected, because it occurs in the final section of the optical path where the beam has been already spread by diffraction. In uplink, pointing error can be reduced, because ground stations may adopt more extensive and sophisticated optics; by contrast, turbulence represents a major effect in this case due to the fact that it affects the beam right after its generation.

In order to treat beam wandering and the corresponding fading process, we assume the regime of weak turbulence, which is appropriate for relatively small zenith angles $\theta \lesssim 1$. In this regime, we may separate effects occurring on fast and slow timescales. Turbulent eddies smaller than the beam waist act with a fast dynamics; these tend to broaden the beam, so that the diffraction-limited spot size w_d is replaced by a larger "short-term" spot size $w_{\rm st} = w_{\rm st}(z,\theta)$, also known as "hot spot." On the other hand, turbulent eddies that are larger than the beam waist act on a much slower time scale [28] (of the order of 10–100 ms [29]); these tend to deflect the beam, whose centroid will then wander according to a Gaussian distribution with variance $\sigma_{\rm TB}^2 = \sigma_{\rm TB}^2(z,\theta)$. This slow dynamics can be fully resolved and closely followed by a fast detector, e.g., with a realistic bandwidth of the order of 100 MHz. On top of this process, there are pointing errors whose dynamics is also slow and causes an additional Gaussian random walk with variance $\sigma_{\rm P}^2 \simeq (10^{-6}z)^2$ for a typical 1μrad error at the transmitter. Overall, the wandering of the beam centroid has variance $\sigma^2 = \sigma_{\rm TB}^2 + \sigma_{\rm P}^2$.

A crucial theoretical step in our treatment is the explicit derivation of $w_{\rm st}$ and $\sigma_{\rm TB}^2$ according to turbulence models that are appropriate for satellite communications. As discussed in detail in Appendix C, we start from the Hufnagel-Valley (H-V) model [30,31], which provides the atmospheric profile for the refraction-index structure constant $C_n^2(h)$ ([32], Sec. 12.2.1). This altitude-dependent constant measures the

strength of the fluctuations in the refraction index caused by spatial variations of temperature and pressure. Assuming this model, we then compute the scintillation index and the Rytov variance. The latter allows us to verify that the angular window $\theta \lesssim 1$ is compatible with the regime of weak turbulence, which is why we choose this angular window for quantum communication in both uplink and downlink.

From the structure constant $C_n^2(h)$, the wave number k of the beam and the geometry (slant distance z and zenith angle θ), one can define the spherical-wave coherence length $\rho_0 = \rho_0(z,\theta)$ for uplink (up) and downlink (down). Using the expression for generic z-long propagation [28,33] and accounting for the altitude function $h = h(z,\theta)$ in Eq. (2), this length takes the form

$$\rho_0^{\text{up/down}} = \left[1.46k^2 \int_0^z d\xi \left(1 - \frac{\xi}{z}\right)^{\frac{5}{3}} \gamma^{\text{up/down}}(\xi) \right]^{-\frac{3}{5}},$$
$$\gamma^{\text{up}}(\xi) = C_n^2[h(\xi,\theta)],\ \gamma^{\text{down}}(\xi) = C_n^2[h(z-\xi,\theta)]. \quad (17)$$

An analysis of ρ_0^{down} confirms that, within the good angular window and not-too large receiver apertures, downlink communication can be considered to be free of turbulence, so we can set $\sigma_{\text{TB}}^2 \simeq 0$ and $w_{\text{st}} \simeq w_d$. This assumption for downlink is well justified by examining the long-term spot-size of the beam

$$w_{\text{lt}}^2 = w_{\text{st}}^2 + \sigma_{\text{TB}}^2, \quad (18)$$

which takes the following form (valid in general conditions of turbulence) [28]

$$w_{\text{lt}}^2 \simeq w_d^2 + 2\left(\frac{\lambda z}{\pi \rho_0}\right)^2. \quad (19)$$

A quick calculation of ρ_0^{down} shows that one has $w_{\text{lt}} \simeq w_d$ in downlink at satellite altitudes (e.g., at the LEO lower border, the difference in these two standard deviations is basically in the third significative digit). This is equivalent to say that diffraction is the only relevant effect, i.e., we have the collapse $\sigma_{\text{TB}}^2 \simeq 0$ and $w_{\text{lt}} \simeq w_{\text{st}} \simeq w_d$.

By contrast, for uplink communication, the value of ρ_0^{up} becomes rather small (of the order of 1 cm at $\lambda = 800$ nm), meaning that turbulence is relevant in this scenario. In this case, we can resort to Refs. [28,34] and write analytical formulas for the short-term spot size and the variance of the centroid wandering.

For satellite distances one can easily check the validity of Yura's condition for uplink $\phi := 0.33(\rho_0^{\text{up}}/w_0)^{1/3} \ll 1$, which allows us to write [34]

$$w_{\text{st}}^2 \simeq w_d^2 + 2\left(\frac{\lambda z}{\pi \rho_0^{\text{up}}}\right)^2 \Psi,\ \ \sigma_{\text{TB}}^2 \simeq 2\left(\frac{\lambda z}{\pi \rho_0^{\text{up}}}\right)^2 (1-\Psi), \quad (20)$$

where $\Psi := (1-\phi)^2 \simeq 1 - 2\phi$. For satellites in the LEO region and beyond, we can adopt the asymptotic planar approximation

$$\rho_0^{\text{up}} \simeq \rho_p^{\text{up}} \simeq [1.46k^2(\sec\theta) I_\infty]^{-3/5}, \quad (21)$$

$$I_\infty := \int_0^\infty d\xi C_n^2(\xi), \quad (22)$$

where ρ_p^{up} bounds the value of ρ_0^{up} from below at any relevant altitude and any $\theta \lesssim 1$ (e.g., see the comparison in Fig. 16 of Appendix C). This leads to the simpler expressions

$$w_{\text{st}}^2 \simeq w_d^2 + z^2 \Delta(\theta), \quad (23)$$

$$\sigma_{\text{TB}}^2 \simeq \frac{7.71 I_\infty}{w_0^{1/3}} z^2 \sec\theta, \quad (24)$$

where we have set

$$\Delta(\theta) := \frac{26.28(I_\infty \sec\theta)^{6/5}}{\lambda^{2/5}} - \frac{7.71 I_\infty \sec\theta}{w_0^{1/3}}. \quad (25)$$

In these formulas, I_∞ takes different values depending on the parameters chosen for the H-V model. In particular, we compute $I_\infty \simeq 2.2354 \times 10^{-12}$ m$^{1/3}$ for the standard H-V$_{5/7}$ model ([32], Sec. 12.2.1), which is good for describing night-time operation. During the day, turbulence on the ground is higher and we consider a typical day-time version of the H-V model, for which $I_\infty \simeq 3.2854 \times 10^{-12}$ m$^{1/3}$ (see Appendix C for more details). Numerical investigations at $\lambda = 800$ nm show that w_{st} exceeds w_d by one order of magnitude in uplink, with an almost constant gap in the far field (e.g., see Fig. 17 in Appendix C). Finally, note that we can re-obtain the downlink diffraction-limited values by setting $I_\infty = 0$ in Eqs. (23) and (24).

E. Bounds for the satellite fading channels in uplink and downlink

Following the theory of the previous section, it follows that we can adopt a unified approach to treat fading in uplink and downlink. In fact, we may consider the general parameters w_{st} and $\sigma^2 = \sigma_{\text{TB}}^2 + \sigma_{\text{P}}^2$, which can then be simplified for the specific case of downlink, for which we may set $w_{\text{st}} \simeq w_d$ and $\sigma^2 \simeq \sigma_{\text{P}}^2$.

In general, the broader short-term spot size w_{st} decreases the maximum value of the transmissivity. In fact, the diffraction-induced transmissivity η_d has to be replaced by the (lower) short-term transmissivity

$$\eta_{\text{st}}(z,\theta) = 1 - e^{-2a_R^2/w_{\text{st}}^2}, \quad (26)$$

with far-field approximation

$$\eta_{\text{st}} \simeq \eta_{\text{st}}^{\text{far}} := \frac{2a_R^2}{w_{\text{st}}^2}. \quad (27)$$

As a result the combined expression η_{tot} of Eq. (13) has to be replaced by the more general parameter

$$\eta(h,\theta) := \eta_{\text{eff}} \eta_{\text{atm}}(h,\theta) \eta_{\text{st}}(h,\theta), \quad (28)$$

where $\eta_{\text{st}}(h,\theta) := \eta_{\text{st}}[z(h,\theta),\theta]$ using Eq. (1).

At any fixed geometry h and θ, the loss parameter $\eta(h,\theta)$ describes the maximum transmissivity that is achievable in the communication through the generally turbulent free-space channel, which corresponds to the case where the incoming beam is perfectly aligned with the receiver's aperture. Note that, more generally, one may assume the case of a constant deflection for the beam; here we omit this technicality for two reasons: we are interested in the optimal rate performance of the communication and such a deflection can anyway be compensated by using adaptive optics.

As a consequence of beam wandering, the actual instantaneous value of the transmissivity will be $\tau \leqslant \eta$ and this value will depend on how far the beam is deflected from the center of the receiver's aperture. The Gaussian random walk of the beam centroid [35] results in a Weibull distribution for the instantaneous deflection which, in turn, leads to a probability distribution $P_\sigma(\tau)$ for the instantaneous transmissivity. Let us introduce the two functions

$$f_0(x) := [1 - \exp(-2x) I_0(2x)]^{-1}, \tag{29}$$

$$f_1(x) := \exp(-2x) I_1(2x), \tag{30}$$

in terms of the modified Bessel function I_n of the first kind with order $n = 0, 1$. These are useful to introduce the geometry-dependent positive parameters [27]

$$\gamma(z,\theta) = \frac{4\eta_{\rm st}^{\rm far} f_0\left(\eta_{\rm st}^{\rm far}\right) f_1\left(\eta_{\rm st}^{\rm far}\right)}{\ln\left[2\eta_{\rm st} f_0\left(\eta_{\rm st}^{\rm far}\right)\right]}, \tag{31}$$

$$r_0(z,\theta) = \frac{a_R}{\left\{\ln\left[2\eta_{\rm st} f_0\left(\eta_{\rm st}^{\rm far}\right)\right]\right\}^{1/\gamma}}. \tag{32}$$

Using these parameters, we may then write

$$P_\sigma(\tau) = \frac{r_0^2}{\gamma\sigma^2\tau}\left(\ln\frac{\eta}{\tau}\right)^{\frac{2}{\gamma}-1} \exp\left[-\frac{r_0^2}{2\sigma^2}\left(\ln\frac{\eta}{\tau}\right)^{\frac{2}{\gamma}}\right]. \tag{33}$$

The free-space fading channel $\mathcal{E}_{\rm fad}$ can therefore be described by an ensemble $\{P_\sigma(\tau), \mathcal{E}_\tau\}$ of pure-loss channels $\mathcal{E}_\tau$ whose transmissivity τ is chosen with probability $P_\sigma(\tau)$. From the PLOB bound and the convexity of the relative entropy of entanglement [12], one has that the secret-key capacity of the fading channel $\mathcal{E}_{\rm fad}$ is bounded by the average

$$K \leqslant -\int_0^\eta d\tau\, P_\sigma(\tau) \log_2(1-\tau). \tag{34}$$

Repeating the steps of Ref. [14], we get

$$K \leqslant \mathcal{B}(\eta,\sigma) := -\Delta(\eta,\sigma)\log_2(1-\eta), \tag{35}$$

where $\Delta(\eta,\sigma)$ is defined by the expression

$$\Delta(\eta,\sigma) := 1 + \frac{\eta}{\ln(1-\eta)}\int_0^{+\infty} dx \frac{\exp\left(-\frac{r_0^2}{2\sigma^2}x^{2/\gamma}\right)}{e^x - \eta}. \tag{36}$$

Note that, while Eq. (35) has exactly the same analytical form of the free-space bound in Ref. [14], it is here implicitly extended from the setting of ground-based communications to that of satellite communications. In $\mathcal{B}(\eta,\sigma)$, the component $-\log_2(1-\eta) \simeq \eta/\ln 2$ upper bounds the key rate achievable with a perfectly aligned link between ground station and receiver, while $\Delta(\eta,\sigma)$ is a correction factor accounting for beam wandering, induced by turbulence and/or pointing errors. In order to investigate this bound for satellite communications, we need to include the necessary geometry and distinguish between downlink and uplink.

By replacing $z = z(h,\theta)$ in the formulas of γ, r_0 and the total variance σ^2, we can express all these parameters in terms of h and θ. We may then use these functionals together with $\eta = \eta(h,\theta)$ of Eq. (28) in Eq. (35), so as to obtain a geometry-dependent expression for the bound $\mathcal{B} = \mathcal{B}(h,\theta)$. In Fig. 2, we investigate the behavior of $\mathcal{B}(h,\theta)$ in uplink and downlink for a satellite at various altitudes h and for zenith angles equal to zero or 1. Besides the effects of free-space diffraction, atmospheric extinction and limited quantum efficiency, the downlink bound $\mathcal{B}_{\rm down}(h,\theta)$ includes the centroid wandering due to pointing error $\sigma_{\rm P}^2$, while the uplink bound $\mathcal{B}_{\rm up}(h,\theta)$ also includes turbulence-induced beam spreading ($w_{\rm st}$) and wandering (so that $\sigma^2 = \sigma_{\rm P}^2 + \sigma_{\rm TB}^2$).

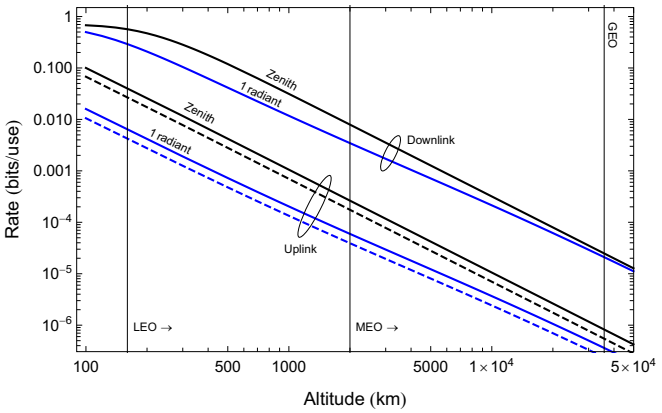

FIG. 2. Key rate between a ground station and a satellite at various altitudes h. We consider the upper bound in Eq. (35) specified for downlink ($\mathcal{B}_{\rm down}$) and uplink ($\mathcal{B}_{\rm up}$), the latter being presented for night time (solid) and day time (dashed). In each case, we show the performance both at the zenith position ($\theta = 0$) and at $\theta = 1$ radiant. In the various configurations, the lines upper bound the maximum number of secret (and entanglement) bits that can be distributed per use of the channel, considering the combined effects of diffraction, atmospheric extinction, quantum efficiency, pointing error (1 μrad) and atmospheric turbulence (night-/day-time H-V model, only for uplink). As in Fig. 1, we assume a collimated beam with $\lambda = 800$ nm and $w_0 = 20$ cm. Receiver has aperture $a_R = 40$ cm and total efficiency $\eta_{\rm eff} = 0.4$.

By comparing the zenith-performance of $\mathcal{B}_{\rm down}$ in Fig. 2 and that of $\mathcal{V}$ in Fig. 1, we can see how the pointing error decreases the rate already from the beginning of the LEO region. Then, by comparing the downlink bound $\mathcal{B}_{\rm down}$ with the uplink bound $\mathcal{B}_{\rm up}$ in Fig. 2, we see how turbulence induces a further nontrivial decrease, which is about one-two orders of magnitude. Also note that $\mathcal{B}_{\rm up}$ is additionally decreased during day time (while $\mathcal{B}_{\rm down}$ does not depend on the operation time).

Several important considerations are in order about Eq. (35). The first is that, as long as the free-space fading channel $\mathcal{E}_{\rm fad}$ can indeed be described by an ensemble of instantaneous pure-loss channels $\mathcal{E}_\tau$, i.e., $\mathcal{E}_{\rm fad} = \{P_\sigma(\tau), \mathcal{E}_\tau\}$, then the bound $\mathcal{B}$ in Eq. (35) is also achievable. As discussed in Ref. [14], this bound is achieved by optimal protocols of CV-QKD, either based on the use of quantum memories or employing largely squeezed states to be transmitted in an extremely biased manner. The bound can also be achieved by optimal protocols of entanglement distribution, where distillation is assisted by one-way backward classical communication. The performance of these protocols is equal to the (bosonic) reverse coherent information [13], which achieves $-\log_2(1-\tau)$ for each $\mathcal{E}_\tau$. As a result, we may write $E = K = \mathcal{B}$ for both the entanglement distribution (E) and the secret key (K) capacities of the fading channel $\mathcal{E}_{\rm fad}$.

The pure-loss assumption $\mathcal{E}_{\rm fad} = \{P_\sigma(\tau), \mathcal{E}_\tau\}$, which implies the achievability of the bound $\mathcal{B}$, is appropriate for night-time operation at typical satellite altitudes. Different is the case for day-time operation, where the background noise becomes nontrivial. In this setting, the quantity $\mathcal{B}$ in Eq. (35) is still an upper bound but no longer guaranteed to be achievable. In the following (Sec. II F), we will therefore consider a more refined upper bound and a corresponding lower bound in the presence of noise. These two bounds are useful for the study of day-time operation and also clarify the validity of the pure-loss assumption for night-time operation.

A final observation regards the potential use of slow detection strategies, so that the wandering of the centroid is not time-resolved but averaged over long acquisition times of the order of 100 ms or more, i.e., beyond the typical timescales associated with turbulence and pointing error. In such a case, the transmissivity of the ground-satellite link has to be averaged over the fading process and is given by

$$\eta_{\rm slow} = \eta_{\rm eff}\eta_{\rm atm}\big[1 - e^{-2a_R^2/(w_{\rm lt}^2+\sigma_{\rm P}^2)}\big], \tag{37}$$

where $w_{\rm lt}$ is the long-term spot size of the beam given in Eq. (18). As a result, the upper bound takes the simple form [14]

$$K_{\rm slow} \leqslant -\log_2(1-\eta_{\rm slow}) \leqslant \frac{2}{\ln 2}\frac{a_R^2}{w_{\rm lt}^2+\sigma_{\rm P}^2}. \tag{38}$$

This detection strategy may be helpful to increase the detection efficiency, but it has the downside to reduce the clock rate and also involves a larger amount of noise to be collected by the receiver.

F. Satellite bounds with background noise

Let us account for the presence of background noise. First of all, it is important to adopt an appropriate model for the input-output number of photons. Call $\bar{n}_T$ the mean number of photons in the beam at the transmitter. For an instantaneous transmissivity τ, the mean number of photons reaching the receiver can be written as

$$\bar{n}_R = \tau\bar{n}_T + \bar{n}, \tag{39}$$

where $\bar{n}$ is the mean number of thermal photons describing the overall noise affecting the propagation.

It is natural to decompose the thermal number $\bar{n}$ as follows [14]

$$\bar{n} := \eta_{\rm eff}\bar{n}_B + \bar{n}_{\rm ex}, \tag{40}$$

where $\bar{n}_B$ is the background thermal noise collected by the receiver's aperture, whose detector has quantum efficiency $\eta_{\rm eff}$ and extra setup noise $\bar{n}_{\rm ex}$. The noise contribution from the setup $\bar{n}_{\rm ex}$ is sometimes considered to be trusted. It is assumed to be negligible ($\bar{n}_{\rm ex} \simeq 0$) in our numerical investigation of the ultimate bounds since we aim at analyzing optimal/almost-optimal performances. (A realistic estimate of $\bar{n}_{\rm ex}$ for a practical receiver setup will be explicitly taken into account in our subsequent analysis of the composable QKD rates.)

The value of the background noise $\bar{n}_B$ depends on the operational setting (time of the day/direction of the link), besides features of the receiver, such as its aperture a_R, field of view $\Omega_{\rm fov}$, detection time Δt, carrier frequency λ and spectral filter $\Delta\lambda$. Let us evaluate $\bar{n}_B$ in the various settings. It is convenient to define the parameter

$$\Gamma_R := \Delta\lambda\Delta t\Omega_{\rm fov}a_R^2. \tag{41}$$

Assuming $\Delta\lambda = 1$ nm and $\Delta t = 10$ ns for the detector, and $\Omega_{\rm fov} = 10^{-10}$ sr and $a_R = 40$ cm for the receiving telescope, we compute $\Gamma_R = 1.6 \times 10^{-19}$ m^2 s nm sr.

TABLE I. Environmental noise in satellite communications (mean number of thermal photons $\bar{n}_B$ per mode). This is shown for uplink and downlink in various conditions, considering a typical receiver ($\Gamma_R = 1.6 \times 10^{-19}$ m^2 s nm sr).

	Day	Night
Downlink	$\simeq 0.3$ (cloudy) $\simeq 3 \times 10^{-3}$ (clear)	$\simeq 3 \times 10^{-6}$
Uplink	$\simeq 0.22$	$\simeq 5.4 \times 10^{-7}$

Then, for uplink we may write

$$\bar{n}_B^{\rm up} = \kappa H_\lambda^{\rm sun}\Gamma_R, \tag{42}$$

where $H_\lambda^{\rm sun}$ is the solar spectral irradiance at the relevant wavelength λ, e.g., $H_\lambda^{\rm sun} = 4.61 \times 10^{18}$ photons m^{-2} s^{-1} nm^{-1} sr^{-1} at $\lambda = 800$ nm. In the formula above, the dimensionless parameter κ depends on the geometry and albedos of the Earth and the Moon. Its value is $\kappa_{\rm day} \simeq 0.3$ for day-time and $\kappa_{\rm night} \simeq 7.36 \times 10^{-7}$ for full-Moon night time (see Appendix D for more details). For downlink, we instead have

$$\bar{n}_B^{\rm down} = H_\lambda^{\rm sky}\Gamma_R, \tag{43}$$

where $H_\lambda^{\rm sky}$ is the spectral irradiance of the sky in units of photons m^{-2} s^{-1} nm^{-1} sr^{-1}. At $\lambda = 800$ nm, its value ranges from 1.9×10^{13} (full-Moon clear night) to 1.9×10^{16} (clear day time) and 1.9×10^{18} (cloudy day time).

A summary of the resulting values for the mean number of photons is provided in Table I. These values confirm that background noise is practically negligible at night time, while it plays an important role for day time. Under general sky conditions, day-time operations need to be described by thermal-loss channels, where loss and fading effects are combined with the thermal bath collected by the field of view of the receiver.

1. Noise filtering

It is important to observe that these values strongly depend on the filter $\Delta\lambda$. At 800 nm, the filter $\Delta\lambda = 1$ nm corresponds to a bandwidth of $\Delta\nu = c\lambda^{-2}\Delta\lambda \simeq 470$ GHz (here c is the speed of light). This value for the filter is certainly appropriate for GEO satellites, while it may become a bit more challenging for fast-moving satellites in the LEO region where the Doppler shift need to be compensated by adaptive optics [36] (so that the central frequency of the beam is suitably tracked during the flyby of the satellite, with generally different speeds at different zenith angles). However, due to other observations, the value of $\Delta\lambda = 1$ nm can also be considered

TABLE II. Day-time noise $\bar{n}_B$ with a narrow filter $\Delta\lambda = 0.1$ pm (corresponding to $\Gamma_R = 1.6 \times 10^{-23}$ m^2 s nm sr).

Day downlink	$\simeq 3 \times 10^{-5}$ (cloudy)
	$\simeq 3 \times 10^{-7}$ (clear)
Day uplink	$\simeq 2.2 \times 10^{-5}$

to be relatively large, since it can be reduced by employing specific detection techniques at the receiver. In other words, the effective value of $\Delta\nu$ can be greatly reduced by suitable interferometric measurements at the receiver.

In fact, an important ingredient of CV quantum communications is the local oscillator (LO). In the method of "transmitted LO" (TLO), each signal is multiplexed in polarization with a bright classical LO pulse, carrying phase information. Signal and LO pulse are de-multiplexed at the receiver via a polarizing beam splitter and made to interfere on balanced beam-splitter(s) in a homodyne or heterodyne setup. Alternatively, one can use the method of the "local LO" (LLO) [37]. Here there is the transmission of bright reference pulses regularly interleaved with the signal pulses (time multiplexing). The reference pulses are detected and used to digitally reconstruct the LO at the receiver. Each signal is homodyned/heterodyned by using an independent LO which is then rotated according to the phase reconstruction.

In both cases, the output of homodyne is proportional to $\sqrt{\bar{n}_{\rm LO}}\hat{x}$, where $\hat{x}$ is signal's generic quadrature and $\bar{n}_{\rm LO} \gg 1$ is the number of photons of the LO pulse interfering with the signal. Only thermal noise mode-matching with the LO will be detected (together with the signal), while all the other noise will be filtered out. For this reason, the actual filter of the receiver will be limited by the bandwidth of the LO pulses. Compatibly with the time-bandwidth product (which is $\Delta t\,\Delta\nu \geqslant 0.44$ for Gaussian pulses), the bandwidth of the LO can be made very narrow so that very small values of $\Delta\lambda$ are indeed accessible. For $\Delta t = 10$ ns, one can consider $\Delta\nu = 50$ MHz, which corresponds to $\Delta\lambda = 0.1$ pm around 800 nm. Such small bandwidths can certainly be generated by current lasers, whose line-widths can easily go down to 1 KHz (e.g., for continuous-wave lasers).

From this point of view, the value of $\Delta\nu \simeq 470$ GHz is pessimistic in the setting of LO-based CV quantum communications. For this reason, we also account for the possibility of receiver designs that may have such ultranarrow filters. An effective filter of $\Delta\lambda = 0.1$ pm is 10^{-4} narrower than the value considered above in Table I. With such a filter, we have a corresponding 10^{-4} suppression of thermal noise $\bar{n}_B$, implying that its day-time values become almost negligible as reported in Table II (where we do not report the night-time values since they become $\lesssim 10^{-10}$). In our following analysis, we therefore include this better regime.

As also noted in Ref. [14], when thermal noise is non-negligible, there is a general trade-off associated with the receiver aperture a_R. If we increase a_R we certainly increase the transmissivity of the link according to Eqs. (4) and (26). However, larger values of a_R also lead to higher values of background noise collected by the receiver as is also clear from Eqs. (41)-(43). As a result, an optimal value for a_R can be determined by optimizing over the rate [or the thermal bound in Eq. (47) of the next sub-section]. In this regard, it is clear that the use of an ultra-narrow filter able to suppress the noise would mitigate this problem and give access to large apertures for the receiver. However, even in total absence of thermal noise, too large apertures would encounter other problems related to enhanced turbulence, in terms of increasing off-axis scintillation and number of short-term speckles (see Appendix C for more details on these effects).

2. *Accounting for the untrusted noise*

It is important to observe that the total input-output relation of Eq. (39) from transmitter to receiver is equivalent to the action of a thermal-loss channel $\mathcal{E}_{\tau,\bar{n}}$ with transmissivity τ and environmental number of photons

$$\bar{n}_e = \bar{n}/(1-\tau). \tag{44}$$

From the point of view of the generic quadrature $\hat{x}$ of the mode (i.e., position $\hat{q}$ or momentum $\hat{p}$), Eq. (39) corresponds to the following transformation:

$$\hat{x}_T \to \hat{x}_R = \sqrt{\tau}\hat{x}_T + \xi_{\rm add}, \tag{45}$$

where the additive-noise variable $\xi_{\rm add}$ can be written as $\xi_{\rm add} = \sqrt{1-\tau}\hat{e}$, and $\hat{e}$ is the quadrature of an environmental mode with $\bar{n}_e$ mean thermal photons. Therefore the overall process can be represented as an effective beam-splitter of transmissivity τ mixing the input mode of the transmitter with an environmental thermal mode. At the output of the beam splitter, one mode is detected by the receiver, while the other mode goes back into the environment.

In the worst-case scenario, one assumes that the eavesdropper (Eve) controls the input environmental mode, assumed to be part of a TMSV state in her hands (which realizes a purification of the channel, unique up to local isometries on the environment). One also assumes that all environmental modes after interaction are stored by Eve in a quantum memory to be subject to an optimal joint measurement. This active strategy is known as collective entangling-cloner attack and represents the most typical collective Gaussian attack [38]. According to Ref. [12], the relative entropy of entanglement suitably computed over the asymptotic Choi matrix of the thermal-loss channel $\mathcal{E}_{\tau,\bar{n}}$ provides an upper bound for its secret key capacity K. For each instantaneous channel $\mathcal{E}_{\tau,\bar{n}}$ describing the satellite link, we have $K(\mathcal{E}_{\tau,\bar{n}}) \leqslant \Phi_{\tau,\bar{n}}$, where [12]

$$\Phi_{\tau,\bar{n}} = \begin{cases} -\log_2[(1-\tau)\tau^{\bar{n}_e}] - h(\bar{n}_e), & \text{for} \quad \bar{n} \leqslant \tau, \\ 0 \quad \text{for} \quad \bar{n} > \tau, \end{cases} \tag{46}$$

and we have set $h(x) := (x+1)\log_2(x+1) - x\log_2 x$.

For the analysis of the ultimate bounds, we may assume that $\bar{n}$ does not depend on τ. Indeed, the external background noise $\bar{n}_B$ does not depend on the transmissivity affecting the signals, since it is noise collected by the field of view of the receiver. Then, in the presence of non-negligible values for the setup noise $\bar{n}_{\rm ex}$ that may depend on τ, we can always optimize $\bar{n}_{\rm ex}$ over τ (and, in particular, minimize its value for the study of upper bounds, and maximize it for that of the lower bounds).

Thus we can represent the satellite fading channel in the presence of background noise by means of the channel ensemble $\mathcal{E}_{\rm fad}^{\rm noi} = \{P_\sigma(\tau), \mathcal{E}_{\tau,\bar{n}}\}$. By averaging $\Phi_{\tau,\bar{n}}$ over the fading process in τ, Ref. [14] computed the general free-space upper bound

$$K \leqslant \int_{\bar{n}}^{\eta} d\tau\, P_\sigma(\tau)\Phi_{\tau,\bar{n}} \leqslant \mathcal{B}(\eta,\sigma) - \mathcal{T}(\bar{n},\eta,\sigma), \tag{47}$$

for $\bar{n} \leqslant \eta$ and where the thermal correction $\mathcal{T}$ is given by

$$\mathcal{T}(\bar{n},\eta,\sigma) = \left\{1 - e^{-\frac{r_0^2}{2\sigma^2}[\ln(\eta/\bar{n})]^{2/\gamma}}\right\} \times \left[\frac{\bar{n}\log_2\bar{n}}{1-\bar{n}} + h(\bar{n})\right] + \mathcal{B}(\bar{n},\sigma). \tag{48}$$

Similarly, one may write the lower bound [14]

$$K \geqslant E \geqslant \mathcal{B}(\eta,\sigma) - \int_0^{\eta} d\tau\, P_\sigma(\tau) h\left(\frac{\bar{n}}{1-\tau}\right) \tag{49}$$

$$\geqslant \mathcal{B}(\eta,\sigma) - h\left(\frac{\bar{n}}{1-\eta}\right), \tag{50}$$

which is based on the RCI and can be approximated by ideal implementations of CV-QKD protocols [14,39].

The application of these formulas to the specific satellite models developed above allows us to bound the ultimate rates for key (and entanglement) distribution that are achievable in the presence of background noise.

3. Maximum ranges

The presence of thermal noise restricts the maximum slant distance for secure key generation to some finite value $z_{\rm max}$. From Eq. (47), we see that no key (or entanglement) distribution is possible in correspondence to the entanglement-breaking condition $\bar{n} = \eta$, which automatically leads to an upper bound for $z_{\rm max}$. If we assume ideal conditions, where all the effects are negligible with the exception of diffraction and thermal noise, the over-optimistic threshold condition $\bar{n} = \eta_d$ would still restricts the range to some finite value. In fact, the latter leads to

$$\bar{n} \leqslant \sqrt{f_{0R}(z_{\rm max})}, \quad f_{0R}(z) := [\pi w_0 a_R/(\lambda z)]^2, \tag{51}$$

where $f_{0R}(z)$ is the Fresnel number product of the beam and the receiver. Then, using Eqs. (42) and (43), we get the following bounds for the maximum ranges in uplink and downlink:

$$z_{\rm max}^{\rm up} \leqslant \frac{\Sigma}{\kappa H_\lambda^{\rm sun}}, \; z_{\rm max}^{\rm down} \leqslant \frac{\Sigma}{H_\lambda^{\rm sky}}, \tag{52}$$

where we have set $\Sigma := \pi w_0/(\lambda\Delta\lambda\Delta t\,\Omega_{\rm fov} a_R)$. It is also clear that $\bar{n} \geqslant 1$ leads to entanglement breaking, so that no key or entanglement can be distributed when $\Gamma_R \geqslant (\kappa H_\lambda^{\rm sun})^{-1}$ in uplink or $\Gamma_R \geqslant 1/H_\lambda^{\rm sky}$ in downlink.

While the conditions in Eq. (52) are particularly simple, tighter bounds on $z_{\rm max}$ can be obtained by directly imposing $\mathcal{B}(\eta,\sigma) = \mathcal{T}(\bar{n},\eta,\sigma)$ in Eq. (47), and using Eqs. (42) and (43). For typical parameters, the situation is the one depicted in Table III, where we observe that thermal noise represents quite an important limitation for day-time operation. As a matter of fact, day-time uplink does seem to be particularly challenging for satellite QKD. For the regime considered, the security range is roughly limited to the Kármán line. In downlink, day-time limitations appear to be less severe. For the considered regime, secret key generation is confined to the LEO region in a cloudy day, but may access MEO altitudes in a clear-sky day.

TABLE III. Bounds on maximum ranges for secure key distribution in uplink and downlink, considering a typical receiver with $\Gamma_R = 1.6 \times 10^{-19}$ m^2 s nm sr (with filter $\Delta\lambda = 1$ nm).

	Day	Night
Downlink	$\lesssim 650$ km (cloudy) $\lesssim 6300$ km (clear)	$\lesssim 2 \times 10^5$ km
Uplink	$\lesssim 110$ km	$\lesssim 9 \times 10^4$ km

In order to reach higher altitudes we need to consider better setup parameters. For instance, a faster detector working at 1 GHz (instead of 100 MHz) will reduce Γ_R and $n_B^{\rm up}$ by a factor of 10. As a result, we get a larger bound for the maximum range in day uplink, i.e., $z_{\rm max} \lesssim 340$ km, so that LEO altitudes are reached. It is clear that a strong mitigation for this problem comes from the use of ultra-narrow filters $\Delta\lambda$, so that the amount of background thermal noise entering the detector becomes negligible, even for day-time operation. With an effective filter of $\Delta\lambda = 0.1$ pm around 800 nm, day-time ranges are sensibly increased. Night-time values of the bounds go well beyond satellite applications, while the bounds for day-time ranges become large as in Table IV.

4. Analysis of the thermal-loss bounds

Following our preliminary analysis on the security ranges, we now explicitly study the thermal-loss upper bound in Eq. (47) and the corresponding lower bound in Eq. (50). Because we are here interested in investigating optimal performances, we assume the ideal case of negligible setup noise ($\bar{n}_{\rm ex} \simeq 0$, noiseless receiver), even though we allow for nonunit quantum efficiency $\eta_{\rm eff}$. We start with the investigation of the optimal rates that are achievable by using a relatively large filter ($\Delta\lambda = 1$ nm) in low-noise conditions of night-time downlink/uplink and day-time downlink with clear sky (see Fig. 3).

For night-time downlink/uplink, one can numerically check that the thermal correction $\mathcal{T}(\bar{n},\eta,\sigma)$ is practically negligible, so the thermal-loss upper bound coincides with the loss-limited bound $\mathcal{B}(\eta,\sigma)$ of Eq. (35), with only small deviations at GEO altitudes. Furthermore, as we can see from Figs. 3(a) and 3(b), the thermal-loss upper bound of

TABLE IV. Bounds on maximum ranges for day-time secure key distribution in uplink and downlink, with a narrow filter $\Delta\lambda = 0.1$ pm, corresponding to $\Gamma_R = 1.6 \times 10^{-23}$ m^2 s nm sr.

Day downlink	$\lesssim 6.2 \times 10^4$ km (cloudy) $\lesssim 6.2 \times 10^5$ km (clear)
Day uplink	$\lesssim 10^4$ km

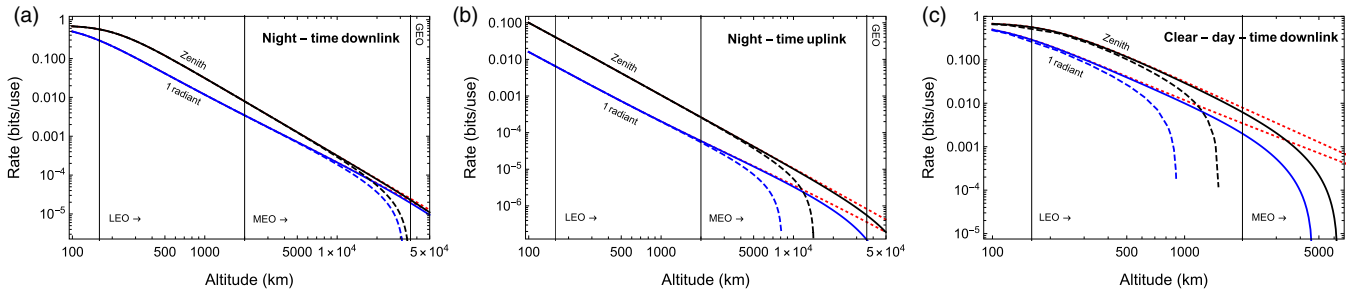

FIG. 3. Optimal key rate between a ground station and a satellite at altitude h, in low-noise configurations of: (a) night-time downlink, (b) night-time uplink, and (c) clear-day-time downlink. In each configuration we consider the thermal-loss upper bound $\mathcal{B}-\mathcal{T}$ of Eq. (47) (solid lines) and the thermal-loss lower bound of Eq. (50) (lower dashed lines), specified for the zenith position (black lines) and 1 radiant (blue lines). We also plot the loss-limited upper bound $\mathcal{B}$ of Eq. (35) (red dashed lines). We account for diffraction, extinction, quantum efficiency, pointing error (1 μrad) and atmospheric turbulence (H-V model). Collimated beam has $\lambda = 800$ nm and $w_0 = 20$ cm. Receiver has a telescope with $a_R = 40$ cm and $\Omega_{\rm fov} = 10^{-10}$ sr, and a detector with filter $\Delta\lambda = 1$ nm, $\Delta t = 10$ ns, $\eta_{\rm eff} = 0.4$ and $\bar{n}_{\rm ex} = 0$ (no extra setup noise). Therefore the receiver has $\Gamma_R = 1.6 \times 10^{-19}$ m^2 s nm sr and the background thermal photons $\bar{n}_B$ are those specified in Table I. For a receiver implementing a narrow filter $\Delta\lambda = 0.1$ pm, the thermal-loss upper and lower bounds in (a), (b) and (c) collapse and coincide with the corresponding loss-limited bounds at the zenith and 1 radiant (red dashed lines).

Eq. (47) numerically coincides with the lower bound of Eq. (50) at LEO altitudes. This means that, for LEO satellites, the two bounds collapse into the loss-limited bound $\mathcal{B}(\eta,\sigma)$ which therefore represents the secret key capacity K (and entanglement-distribution capacity E) of the satellite channel [40]. Said in other words, for night-time downlink/uplink and LEO altitudes, the free-space fading channel can certainly be approximated by an ensemble of pure-loss channels and we can write the achievability result $E \simeq K \simeq \mathcal{B}$. At higher altitudes in the MEO region, the presence of a gap does not allow us to enforce the pure-loss assumption and claim achievability with respect to the chosen parameters (in particular, for the value $\Delta\lambda = 1$ nm).

For clear-day-time downlink in Fig. 3(c), the gap between the two thermal-loss bounds of Eqs. (47) and (50) already appears in the LEO region, even though at low altitudes (of the order of 160 km) there is a substantial coincidence. We can appreciate how, for increasing altitudes, not only the gap increases but the thermal-loss upper bound also substantially departs from the loss-limited bound $\mathcal{B}(\eta,\sigma)$, confirming the relevant role of the background thermal noise in limiting the rate performance for day-time operation.

As expected, the role of the thermal background noise can be strongly mitigated by the use of a narrow filter, e.g., $\Delta\lambda = 0.1$ pm (as in homodynelike setups at the receiver). In conditions of low background noise, our numerical investigation shows that the use of such a narrow filter enables the parties to achieve the loss-limited bound $\mathcal{B}$ at the relevant altitude and zenith angle, expressed by the red dashed lines in Fig. 3. In other words, the thermal-loss upper and lower bounds collapse into the loss-limited bound $\mathcal{B}$ at all satellite altitudes, so the remote parties can distribute ebits and secret bits at the capacity value $E \simeq K \simeq \mathcal{B}$. Such a collapse is more limited in conditions of stronger background noise, as typical in cloudy-day-time downlink and day-time uplink, but yet the use of a narrow filter would allow to reach good communication rates in such scenarios as shown in Fig. 4. As we can see from the figure, we can match the loss-limited bound $\mathcal{B}$ in all the LEO region for day-time downlink with cloudy sky, and for the first part of LEO in day-time uplink. Extending the achievability of $\mathcal{B}$ to all altitudes would require an even narrower filter.

Before concluding this section, it is important to remark that, in the various scenarios studied above, the achievability of the upper bound refers to a satellite *at a fixed* geometry, i.e., with fixed altitude and zenith angle. This means that we ignore the orbital dynamics or we assume that such a dynamics is much slower than the timescale of the quantum communication, so the channel is used many times before the satellite has substantially moved (fast-clock limit/large repetition rate). However, apart from GEO satellites, the orbital dynamics is relevant and, for realistic clocks, we need to modify the lower bound in order to account for this process. In fact, suppose that the rate in Eq. (50) can approximately be achieved after N pulses. For some realistic clock, such a block of N pulses corresponds to a slice of the orbit over which we identify the worst-case values for h and θ. An achievable rate would certainly be given by Eq. (50) computed over such values, but this rate will no longer match the upper bound in the slice (to be computed on the best-case values for h and θ). In the following, we will consider the problem of orbital slicing more carefully for the derivation of a composable secret key rate.

III. COMPOSABLE FINITE-SIZE SECURITY FOR SATELLITE CV-QKD

Once we have clarified the ultimate limits for distributing keys (and entanglement) with satellites, we study the rates that are achievable by practical CV-QKD protocols, where we explicitly account for finite-size and composable aspects. We adopt the pilot-based post-selected protocol studied in Ref. [14], here suitably applied and extended to considering the underlying physical models valid for satellite communications.

A. Overview

The idea is to use a coherent-state protocol, where Gaussian-modulated signal pulses (used to encode the

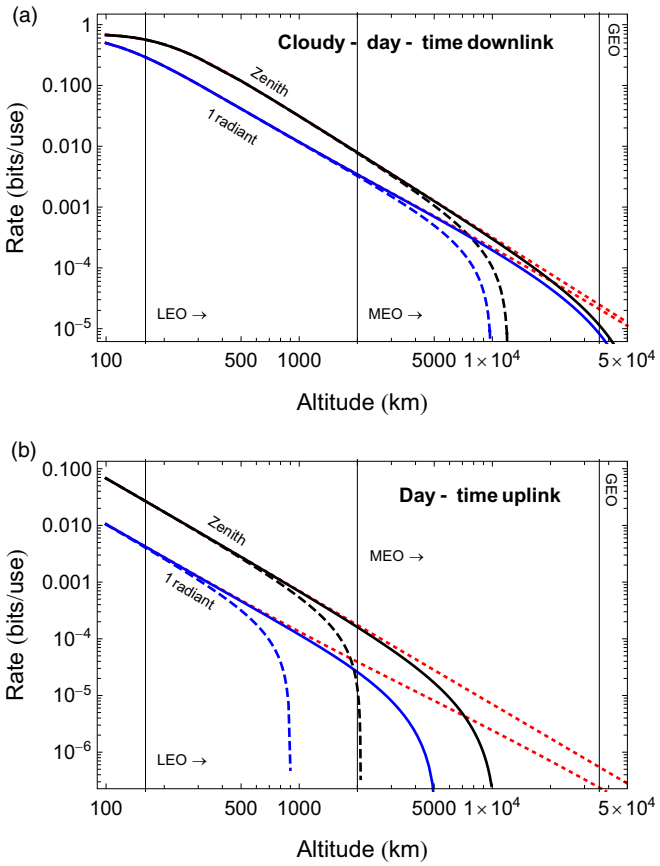

FIG. 4. Optimal performances in day-light conditions with a narrow filter. As in Fig. 3, we consider the key rate between a ground station and a satellite at various altitudes h. In each configuration, we consider the thermal-loss upper bound $\mathcal{B}-\mathcal{T}$ of Eq. (47) (solid lines) and the thermal-loss lower bound of Eq. (50) (lower dashed lines), specified for the satellite at the zenith position (black lines) or at 1 radiant (blue lines). We also plot the loss-limited upper bound $\mathcal{B}$ of Eq. (35) (red dashed lines). In particular, we consider cloudy-day-time downlink in (a), and day-time uplink in (b). We account for diffraction, extinction, quantum efficiency, pointing error (1 μrad) and atmospheric turbulence (H-V model). Collimated beam has $\lambda = 800$ nm and $w_0 = 20$ cm. Receiver has a telescope with $a_R = 40$ cm and $\Omega_{\rm fov} = 10^{-10}$ sr, and a detector with narrow filter $\Delta\lambda = 0.1$ pm, $\Delta t = 10$ ns, $\eta_{\rm eff} = 0.4$, and $\bar{n}_{\rm ex} = 0$ (no extra setup noise). Therefore the receiver has $\Gamma_R = 1.6\times 10^{-23}$ m^2 s nm sr and the background thermal photons $\bar{n}_B$ are strongly suppressed as in Table II.

information) are randomly interleaved with more energetic pilot pulses, that are used to monitor the instantaneous transmissivity of the satellite link in real-time. In this way, the parties are able to allocate the distributed data to slots of transmissivity and to perform classical post-processing slot-by-slot. In general, one may divide the interval $[0,\eta]$ by introducing a lattice with step $\delta\tau$, so that we have $M = \eta/\delta\tau$ slots $[\tau_k,\tau_{k+1}]$ with $\tau_k := (k-1)\delta\tau$ and $k = 1,\ldots,M$. When the kth slot is selected, with probability

$$p_k = \int_{\tau_k}^{\tau_{k+1}} d\tau\, P_\sigma(\tau), \tag{53}$$

the corresponding data points are associated to its minimum transmissivity τ_k.

A more practical post-selection strategy consists of introducing a threshold value $\eta_{\rm th}$ and only accepting data points with $\tau > \eta_{\rm th}$, i.e., within the post-selection interval $\Delta = [\eta_{\rm th},\eta]$. This happens with success probability

$$p_{\rm th} = \int_{\eta_{\rm th}}^{\eta} d\tau\, P_\sigma(\tau). \tag{54}$$

The data points are then associated with the value of the threshold transmissivity $\eta_{\rm th}$. In our work, we adopt this post-selection strategy from Ref. [14], which is more robust, especially in terms of collecting enough statistics for parameter estimation. This approach is different from the clusterization method of Ref. [41] which may instead be affected by poor statistics.

In the next subsections, we first discuss the security of the link for a fixed value of the transmissivity, as if there were no fading and with a satellite in a fixed geometry. Then, we introduce the fading process, for which we use the post-selection strategy above, and we subsequently account for orbital dynamics in the key rate. These derivations will provide realistic rates for satellite quantum communications and will also be used for our comparison with a ground network.

B. Composable key rate at fixed transmissivity

Let us start by considering the link to be a thermal-loss channel $\mathcal{E}_{\tau,\bar{n}}$ with fixed transmissivity τ and thermal noise $\bar{n}_e = \bar{n}/(1-\tau)$, where $\bar{n}$ may take the form in Eq. (40). In a coherent-state protocol [42,43], the transmitter generates an input mode with generic quadrature $\hat{x}_T = x + \hat{v}$, where $\hat{v}$ is the vacuum quadrature and x is a Gaussianly modulated variable with variance $\sigma_x^2 = \mu - 1$ (with μ being the variance of the average thermal state generated by the transmitter). At the output of the thermal-loss channel $\mathcal{E}_{\tau,\bar{n}}$, the receiver gets a mode with generic quadrature $\hat{x}_R$ as given in Eq. (45). Assuming that the output is homodyned (randomly in $\hat{q}$ or $\hat{p}$), then the receiver's classical outcome takes the form

$$y = \sqrt{\tau}x + z, \tag{55}$$

where z is a random noise variable, distributed according to a Gaussian with zero mean and variance $\sigma_z^2 = 2\bar{n}+1$. If heterodyne is used, then the outcome y (for each of the two quadratures) is affected by thermal noise with larger variance $\sigma_z^2 = 2\bar{n}+2$. Compactly, we may therefore write

$$\sigma_z^2 = 2\bar{n} + \nu_{\rm det}, \tag{56}$$

where $\nu_{\rm det} = 1$ holds for homodyne, and $\nu_{\rm det} = 2$ for heterodyne detection.

For fixed τ and $\bar{n}$, one computes the mutual information $I(x:y|\tau,\bar{n})$ which takes simple expressions for the two types of output detections, i.e.,

$$I^{\rm hom}(x:y|\tau,\bar{n}) = \frac{1}{2}\log_2\left(1+\frac{\tau\sigma_x^2}{2\bar{n}+1}\right), \tag{57}$$

$$I^{\rm het}(x:y|\tau,\bar{n}) = \log_2\left(1+\frac{\tau\sigma_x^2}{2\bar{n}+2}\right). \tag{58}$$

In reverse reconciliation, it is easy to compute Eve's Holevo bound $\chi(E:y|\tau,\bar{n})$ with corresponding expressions for χ^{hom} and χ^{het} (see Ref. ([14], Sec. III C) for details). Therefore one may write the asymptotic key rate against collective Gaussian attacks, which takes the form

$$R_{\text{asy}}(\tau,\bar{n}) = \beta I(x:y|\tau,\bar{n}) - \chi(E:y|\tau,\bar{n}), \tag{59}$$

where $\beta \in [0,1]$ is the reconciliation parameter (here βI corresponds to the effective rate of the code which is employed in the step of error correction).

In an actual practical implementation, there is a number N of transmitted signals, whose m are randomly selected by the parties and used for the estimation of the channel parameters τ and $\bar{n}$. From $m_p := m\nu_{\text{det}}$ pairs of data points $\{x_i, y_i\}$ related by Eq. (55), the parties build the following unbiased estimators $\widehat{\tau} = \widehat{T}^2$ and $\widehat{\bar{n}} = (\widehat{\sigma_z^2} - \nu_{\text{det}})/2$, where [14]

$$\widehat{T} = \frac{\sum_{i=1}^{m_p} x_i y_i}{m_p \sigma_x^2}, \ \widehat{\sigma_z^2} := \frac{1}{m_p}\sum_{i=1}^{m_p}(y_i - \widehat{T}x_i)^2. \tag{60}$$

Up to $\mathcal{O}(m_p^{-2})$, these have variances

$$\sigma_\tau^2 := \text{var}(\widehat{\tau}) \simeq \frac{4\tau^2}{m_p}\left(2 + \frac{\sigma_z^2}{\tau\sigma_x^2}\right), \tag{61}$$

$$\sigma_{\bar{n}}^2 := \text{var}(\widehat{\bar{n}}) \simeq \frac{\sigma_z^4}{2m_p}. \tag{62}$$

We can therefore build the worst-case parameters

$$\tau' := \widehat{\tau} - w\sigma_\tau \simeq \tau - 2w\sqrt{\frac{2\tau^2 + \tau\sigma_z^2/\sigma_x^2}{m_p}}, \tag{63}$$

$$\bar{n}' := \widehat{\bar{n}} + w\sigma_{\bar{n}} \simeq \bar{n} + \frac{w\sigma_z^2}{\sqrt{2m_p}}. \tag{64}$$

Each of them bounds the corresponding actual value up to an error probability ε_{pe}, with

$$w = \sqrt{2}\,\text{erf}^{-1}(1 - 2\varepsilon_{\text{pe}}). \tag{65}$$

Alternatively, one may write a more robust tail bound which leads to the same expressions as above but with

$$w = \sqrt{2\ln(1/\varepsilon_{\text{pe}})}, \tag{66}$$

which can be used in the cases where ε_{pe} is very small, e.g., less than 10^{-17} ([14], Sec. III D).

It is therefore clear that the effect of parameter estimation is to modify the asymptotic rate in Eq. (59) as follows

$$R_{\text{asy}} \to \frac{n}{N}R_{\text{pe}}, \ R_{\text{pe}} = R_{\text{asy}}(\tau', \bar{n}') \tag{67}$$

where $n = N - m$ is the number of signals remaining for key generation. This is valid up to a total error $\simeq 2\varepsilon_{\text{pe}}$. The rate R_{pe} takes specific formulas for the homodyne ($R_{\text{pe}}^{\text{hom}}$) and the heterodyne ($R_{\text{pe}}^{\text{het}}$) protocol by using Eqs. (57) and (58) together with corresponding expressions for the Holevo information χ^{hom} and χ^{het}.

Parameter estimation provides the parties with crucial information about the amount of loss and noise present in the channel, so they can apply a suitable code to correct their data. The procedure of error correction is successful with a probability p_{ec} which depends on the rate βI of the code and a pre-established ε-correctness ε_{cor}, which bounds the residual probability that the local strings are different after passing a hashing test. Thus only np_{ec} pulses are successfully error-corrected and further processed into a key. This means that secret-key rate R_{pe} needs to be rescaled by the pre-factor np_{ec}/N.

The next step is that of privacy amplification which is also not perfect. This means that there will be some nonzero distance between the final strings (composing the shared key) and an ideal classical-classical-quantum state where the eavesdropper is completely decorrelated from the parties. Such a distance is bounded by some target value of the ε secrecy of the protocol, which is further decomposed as $\varepsilon_{\text{sec}} = \varepsilon_{\text{s}} + \varepsilon_{\text{h}}$, where ε_{s} is a smoothing parameter ε_{s} and ε_{h} is a hashing parameter. Overall, all these imperfections are composed into a single global parameter which is the ε security of the protocol, and given by $\varepsilon = 2p_{\text{ec}}\varepsilon_{\text{pe}} + \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$ [14].

For a Gaussian-modulated coherent-state protocol [42,43] with success probability p_{ec} and ε security against collective (Gaussian) attacks [38], we may write the composable finite-size key rate [14]

$$R \geqslant \frac{np_{\text{ec}}}{N}\left(R_{\text{pe}} - \frac{\Delta_{\text{aep}}}{\sqrt{n}} + \frac{\Theta}{n}\right), \tag{68}$$

where

$$\Delta_{\text{aep}} := 4\log_2\left(2\sqrt{d}+1\right)\sqrt{\log_2\frac{18}{p_{\text{ec}}^2\varepsilon_{\text{s}}^4}}, \tag{69}$$

$$\Theta := \log_2\left[p_{\text{ec}}\left(1-\varepsilon_{\text{s}}^2/3\right)\right] + 2\log_2\sqrt{2}\varepsilon_{\text{h}}, \tag{70}$$

and d is the size of the alphabet after analog-to-digital conversion of the continuous variables of the parties (typically $d = 2^5$ for a five-bit digitalization).

For the specific case of the heterodyne protocol, one can extend the security to general coherent attacks by combining Eq. (68) with the approach of Ref. [44]. This involves a suitable symmetrization of the data and performing $m_{\text{et}} = f_{\text{et}}n$ local energy tests, where they check if their local mean number of photons is $\lesssim \bar{n}_T + \mathcal{O}(m_{\text{et}}^{-1/2})$. This test is certainly passed for large enough m_{et} and for typical communication conditions with small values of excess noise (as is the case here, so that we certainly have $\bar{n}_R = \tau\bar{n}_T + \bar{n} \lesssim \bar{n}_T$ at the receiver).

Thus the parties achieve the rate [14]

$$R_{\text{gen}}^{\text{het}} \geqslant \frac{np_{\text{ec}}}{N}\left[R_{\text{pe}}^{\text{het}} - \frac{\Delta_{\text{aep}}}{\sqrt{n}} + \frac{\Theta - 2\left\lceil \log_2\binom{K_n+4}{4}\right\rceil}{n}\right], \tag{71}$$

where the number of key-generation pulses is now

$$n = N - (m + m_{\text{et}}) = \frac{N-m}{1+f_{\text{et}}}, \tag{72}$$

and we have set

$$K_n = \max\{1, 2n\bar{n}_T\Sigma_n\}, \tag{73}$$

$$\Sigma_n := \frac{1 + 2\sqrt{\frac{\ln(8/\varepsilon)}{2n}} + \frac{\ln(8/\varepsilon)}{n}}{1 - 2\sqrt{\frac{\ln(8/\varepsilon)}{2f_{\text{et}}n}}}. \tag{74}$$

The final security here is $\varepsilon' = K_n^4\varepsilon/50$.

In a practical implementation, the parties exchange many pulses [45], which are split into $n_{\rm b} \gg 1$ blocks of suitable size N for data processing; typically, $N = \mathcal{O}(10^6)$ or more. Assuming that the channel parameters are stable, one can write Eq. (68) for the generic block, i.e., for $N = \mathcal{O}(10^6)$. The success probability $p_{\rm ec}$ provides the fraction of blocks that are successfully processed into key generation. Under conditions of stability, parameter estimation can be performed in one-go over the entire set of sacrificed pulses $mn_{\rm b}$, so that the worst-case estimators are expected to be quite close to the actual values. However, if the channel is not stable, but slowing varying with respect to the time-frame associated with a single block, then parameter estimation has to be done block-by-block and the final rate will be averaged over the blocks. In the following, we will assume that parameter estimation is based over the single-block statistics, so that we encompass the possibility of variability.

C. Pilots, post-selection, lattice allocation, and defading

In a fading scenario where the value of the transmissivity τ fluctuates, as is the case of a free-space quantum communication, it is useful to use bright pilot pulses to track τ so as to create a lattice where signals with almost-equal transmissivity are grouped together. Assume that Alice randomly interleaves her signals with $m_{\rm PL}$ pilots. These are prepared in an energetic coherent-state $|\sqrt{\bar{n}_{\rm PL}}e^{i\pi/4}\rangle$, with $\bar{n}_{\rm PL}$ mean photons and fixed $\pi/4$ phase, so as to provide components for both q and p measurements. The first moments of the pilots follow Eq. (55), where the magnitude of the noise z is negligible with respect to that of $\sqrt{\tau}x$. As discussed in Ref. [14], they allow to achieve an almost perfect estimation of the instantaneous value of τ.

The high energy regime is easily accessible using 10 ns-long pulses from a 100 mW laser source. At $\lambda = 800$ nm, each 1 nJ pulse contains an average of $x^2 \simeq 4 \times 10^9$ photons. Such energy can be used for the TLO multiplexed with each signal or pilot. A fraction of this energy, say $x^2 \simeq 10^6$ photons can be used for the pilots. Considering $\simeq 30$ dB loss, i.e., $\tau \simeq 10^{-3}$, which is the worst-case scenario in the LEO region (reached in uplink with a 2000-km-high satellite at 1 radiant), we have that $>10^6$ photons are collected for the LO, and about 10^3 for the pilots. The LO is bright enough to allow for shot-noise limited measurements, and the pilots are also bright enough to provide an almost perfect estimation of τ. It is clear that, in the case of an LLO, the LO is even brighter since it is not even attenuated by the transmission.

On the basis of the pilots, Alice and Bob determine a post-selection interval $\Delta = [\eta_{\rm th}, \eta]$ where η is the maximum transmissivity and $\eta_{\rm th} = f_{\rm th}\eta$ is computed for some fixed $f_{\rm th} < 1$. As a result, only a fraction $p_{\rm th}$ of the pulses will be post-selected [cf. Eq. (54)]. Within Δ, they introduce a regular lattice of M bins/slots with step $\delta\tau = (\eta - \eta_{\rm th})/M$ and generic bin/slot $\Delta_k = [\tau_k, \tau_{k+1}]$, with $\tau_k := \eta_{\rm th} + (k-1)\delta\tau$ and $k = 1, \ldots, M$. The generic slot Δ_k is populated with probability p_k computed according to Eq. (53), i.e., it is associated with (an integer approximation of) $S_k := (N - m_{\rm PL})p_k$ signals and corresponding $\nu_{\rm det}S_k$ pairs of data points $\{x_i, y_i^k\}$. For a sufficiently small step $\delta\tau$, these points satisfy the input-output relation

$$y^k \simeq \sqrt{\tau_k}x + z^k, \tag{75}$$

for a Gaussian noise variable z^k whose variance $\sigma_z^2(\tau_k) = 2\bar{n}(\tau_k) + \nu_{\rm det}$ generally depends on τ_k.

Instead of processing each slot independently from the others (with limited statistics), the parties may adopt a defading procedure mapping all the slots into the first one, with minimum transmissivity $\eta_{\rm th}$. To the points in slot Δ_k, Bob applies the classical channel

$$y^k \to \tilde{y}^k := \sqrt{\frac{\eta_{\rm th}}{\tau_k}}y^k + \sqrt{1 - \frac{\eta_{\rm th}}{\tau_k}}\xi_{\rm add}, \tag{76}$$

where $\xi_{\rm add}$ is a Gaussian variable with variance equal to $\nu_{\rm det}$. By repeating this mapping for all the slots, Bob creates a new variable

$$\tilde{y} = \sqrt{\eta_{\rm th}}x + \tilde{z}, \tag{77}$$

where $\tilde{z}$ is non-Gaussian with variance

$$\sigma_{\tilde{z}}^2 = 2\bar{n}_* + \nu_{\rm det},\ \bar{n}_* := \frac{\eta_{\rm th}}{p_{\rm th}}\sum_k \frac{p_k}{\tau_k}\bar{n}(\tau_k). \tag{78}$$

Using the optimality of Gaussian attacks, Alice and Bob assume that $\tilde{z}$ is Gaussian, thus overestimating Eve's strategy and underestimating their performance. In this way, the entire defading procedure reduces the initial non-Gaussian fading channel into a worst-case thermal-loss Gaussian channel $\mathcal{E}_{\eta_{\rm th},\bar{n}_*}$ with fixed minimum transmissivity $\eta_{\rm th}$ and thermal number equal to $\bar{n}_*$.

D. Parameter estimation and composable key rate

Once they have reduced the problem to a worst-case thermal loss channel $\mathcal{E}_{\eta_{\rm th},\bar{n}_*}$, Alice and Bob build the worst-case estimators, $\eta'_{\rm th}$ and $\bar{n}'_*$, for the parameters $\eta_{\rm th}$ and $\bar{n}_*$ associated with the channel, by using $m_p p_{\rm th}$ pairs of data points (coming from $mp_{\rm th}$ sacrificed signals). Each of these worst-case estimators is correct up to an error $\varepsilon_{\rm pe}$, related to the confidence parameter w according to Eq. (65) or (66). See also Ref. ([14], Sec. IV.F).

Note that also the threshold transmissivity $\eta_{\rm th}$ needs to be estimated, even though this is agreed by the parties via the pilots. In this way, in fact, Alice and Bob can detect and account for Eve's potential strategies that are aimed at discriminating signals and pilots, and then applying different interactions. As a matter of fact, any potential error associated with the slot allocation of the signals (due to Eve's action or coarse-graining imperfections) will be detected and accounted by directly estimating $\eta_{\rm th}$ over the signals ([14], Sec. IV.E).

Assume the realistic case where signals and pilots undergo the same interaction with the environment, so that the estimation of $\eta_{\rm th}$ via the signals confirms the threshold value agreed by the parties using the pilots. (As said above, in the potential presence of signal-pilot discrepancies, our general formalism still applies by generating the corresponding worst-estimators from the signals.) Then, the worst-case estimators satisfy the bounds [14]

$$\eta'_{\rm th} \gtrsim \eta_{\rm LB} := \eta_{\rm th} - 2w\sqrt{\frac{2\eta_{\rm th}^2 + \eta_{\rm th}\sigma_{\rm wc}^2/\sigma_x^2}{m_p p_{\rm th}}}, \tag{79}$$

$$\bar{n}'_* \lesssim \bar{n}_{\rm UB} := \bar{n}_{\rm wc} + w\frac{\sigma_{\rm wc}^2}{\sqrt{2m_p p_{\rm th}}}, \tag{80}$$

where $\sigma_{\rm wc}^2 = 2\bar{n}_{\rm wc} + \nu_{\rm det}$ is the worst-case value for the total thermal noise. This value upper bounds $\sigma_{\tilde{z}}^2$ and is computed by taking $\bar{n}_{\rm wc} \geqslant \bar{n}(\tau)$ for any $\tau \in \Delta$. In order to compute $\bar{n}_{\rm wc}$, i.e., maximize the thermal noise over the transmissivity, we need to introduce a practical expression for the setup noise (see the next subsection).

Using $\eta_{\rm LB}$ and $\bar{n}_{\rm UB}$, we can lower-bound Alice and Bob's key rate affected by parameter estimation

$$R_{\rm pe} = R_{\rm asy}(\eta'_{\rm th}, \bar{n}'_{*}) \geqslant R_{\rm LB} := R_{\rm asy}(\eta_{\rm LB}, \bar{n}_{\rm UB}). \tag{81}$$

Then, the composable key rate is a direct modification of Eq. (68) and takes the form [14]

$$R \geqslant \frac{np_{\rm th}p_{\rm ec}}{N}\left(R_{\rm LB} - \frac{\Delta_{\rm aep}}{\sqrt{np_{\rm th}}} + \frac{\Theta}{np_{\rm th}}\right), \tag{82}$$

with $n = N - (m + m_{\rm PL})$ and security $\varepsilon = 2p_{\rm ec}\varepsilon_{\rm pe} + \varepsilon_{\rm cor} + \varepsilon_{\rm sec}$ against collective (Gaussian) attacks.

For the heterodyne version of the protocol, we can again extend the security from collective to general attacks by performing a similar modification as in Eq. (71). In this case, the secret-key rate becomes [14]

$$R_{\rm gen}^{\rm het} \geqslant \frac{np_{\rm th}p_{\rm ec}}{N}\left[R_{\rm LB}^{\rm het} - \frac{\Delta_{\rm aep}}{\sqrt{np_{\rm th}}} + \frac{\Theta - 2\left\lceil \log_2 \binom{K_{np_{\rm th}}+4}{4}\right\rceil}{np_{\rm th}}\right], \tag{83}$$

where K_n is given in Eq. (73) and the total number of key-generation pulses is now given by

$$n = N - (m + m_{\rm PL} + m_{\rm et}) = \frac{N - (m + m_{\rm PL})}{1 + f_{\rm et}}. \tag{84}$$

Final security is equal to $\varepsilon' = K_{np_{\rm th}}^4 \varepsilon/50$.

E. Setup noise and observations about the LO

The setup noise $\bar{n}_{\rm ex}$ strictly depends on what type of LO is used. In fact, in the case of a TLO, there is no phase error, but the electronic noise of the detector becomes nontrivial due to the attenuation that the LO undergoes during its transmission. By contrast, in the case of an LLO, the electronic noise is lower due to the fact that the LO is always bright, independently from the transmissivity; however, there will be some nontrivial phase noise that comes from the imperfect digital reconstruction of the rotating reference frame at the receiver.

The electronic noise can be described by an additive Gaussian channel with associated variance $\nu_{\rm el}$ or equivalent number of photons $\bar{n}_{\rm el} = \nu_{\rm el}/2$. Its value depends on various quantities, namely the noise equivalent power (NEP) of the amplifiers/photodiodes in the homodyne detectors, the detection bandwidth W, the duration of the LO pulses $\Delta t_{\rm LO}$, the LO power at the detector $P_{\rm LO}^{\rm det}$, and the frequency of the light ν. Let us consider the power $P_{\rm LO}$ at which the LO is generated, so that we have $P_{\rm LO}^{\rm det} = \tau P_{\rm LO}$ for the TLO and $P_{\rm LO}^{\rm det} = P_{\rm LO}$ for the LLO. Then, let us introduce the parameter (see also Ref. [14])

$$\Theta_{\rm el} := \frac{\nu_{\rm det}{\rm NEP}^2 W \Delta t_{\rm LO}}{2h\nu P_{\rm LO}}. \tag{85}$$

In our notation, we may write

$$\bar{n}_{\rm el}^{\rm TLO} = \Theta_{\rm el}/\tau, \quad \bar{n}_{\rm el}^{\rm LLO} = \Theta_{\rm el}. \tag{86}$$

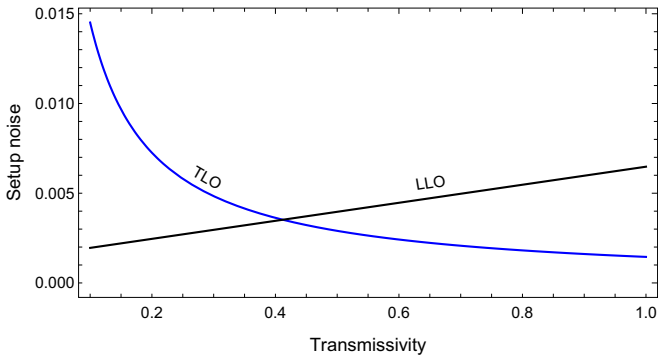

FIG. 5. Comparison of the setup noise (in terms of equivalent number of thermal photons $\bar{n}_{\rm el}$) versus channel transmissivity τ, for the LLO (black line) and the TLO (blue line). These are computed using Eq. (88). Parameters are chosen as in the text, i.e., $\lambda = 800$ nm, $l_{\rm W} = 1.6$ KHz, $W = 100$ MHz, NEP $= 6$ pW/$\sqrt{\rm Hz}$, $P_{\rm LO} = 100$ mW, $\Delta t_{\rm LO} = 10$ ns, $C = 10$ MHz, $\sigma_x^2 = 10$, and $\nu_{\rm det} = 2$ (heterodyne detection).

For a detector with bandwidth $W = 100$ MHz, we may consider NEP $= 6$ pW/$\sqrt{\rm Hz}$. Then, let us take an LO power $P_{\rm LO} = 100$ mW. At 800 nm and using LO pulses of duration $\Delta t_{\rm LO} = 10$ns, we get $\Theta_{\rm el} \simeq 1.45 \times 10^{-3}$ for the case of an heterodyne setup ($\nu_{\rm det} = 2$). It is clear the advantage of the LLO in reducing the electronic noise.

Such a reduction of the electronic noise induced by the LLO comes at the price of introducing phase errors. In our notation, we quantify this contribution as follows:

$$\bar{n}_{\rm phase}^{\rm LLO} = \frac{\pi\sigma_x^2 l_{\rm W}}{C}\tau, \tag{87}$$

where C is the clock of the system and $l_{\rm W}$ is the laser linewidth [14]. In our investigations we have $\sigma_x^2 \lesssim 10$ and $C = 10$ MHz, so a low value $\bar{n}_{\rm phase}^{\rm LLO}$ can be reached with a linewidth $l_{\rm W} \simeq 1.6$ KHz.

Overall, we have that the setup noise for the TLO and LLO takes the following expressions:

$$\bar{n}_{\rm ex}^{\rm TLO}(\tau) = \frac{\Theta_{\rm el}}{\tau}, \quad \bar{n}_{\rm ex}^{\rm LLO}(\tau) = \Theta_{\rm el} + \frac{\pi\sigma_x^2 l_{\rm W}}{C}\tau, \tag{88}$$

where we see the different monotonic behavior of these quantities versus the transmissivity τ. In particular, the TLO seems to be preferable for short distances (high values of τ), while the LLO is better for long distances (low value of τ). See also Fig. 5.

In order to maximize $\bar{n}_{\rm ex}$ over the post-selection interval Δ, we therefore compute $\bar{n}_{\rm ex}^{\rm TLO}(\tau)$ at the minimum border value $\tau = \eta_{\rm th}$, and $\bar{n}_{\rm ex}^{\rm LLO}(\tau)$ at the maximum border value $\tau = \eta$. Thus the worst-case value for the setup noise will be given by

$$\bar{n}_{\rm wc} = \eta_{\rm eff}\bar{n}_B + \bar{n}_{\rm ex,wc}, \tag{89}$$

where we have set

$$\bar{n}_{\rm ex,wc}^{\rm TLO} = \Theta_{\rm el}/\eta_{\rm th}, \quad \bar{n}_{\rm ex,wc}^{\rm LLO} = \Theta_{\rm el} + \frac{\pi\sigma_x^2 l_{\rm W}}{C}\eta. \tag{90}$$

As already mentioned, an LLO is more convenient for long-distance quantum communications (low values of the

transmissivity). In fact, in such a case, the associated phase error decreases to zero, and the total setup noise tends to the constant term $\Theta_{\rm el}$. For this reason, in the following we specifically investigate the performances achievable with an LLO, but we stress that both approaches of TLO and LLO are encompassed by our theory. We also stress that an LLO requires a more sophisticated hardware than that needed by a TLO.

As already mentioned in Sec. II F 1, an important aspect in the use of an LLO is that each pulse (signal or pilot) must be transmitted in the middle of two reference pulses, so that there is a regular interleaving between these bright references and all the other pulses. From the detection of the references, Bob reconstructs Alice's rotating frame and therefore suitably rotates the outcomes he has obtained from the measurements of the signals and the pilots (for which a locally generated LO was employed for the homodyne/heterodyne detection). It is clear that, in this process, the free-space link is half of the time used by the phase-synchronizing references. This means that, in terms of actual throughput (bits/second), there is a factor of $1/2$ to account for the LLO. However, it is also true that such a time-multiplexing of the LO enables Alice to use both polarizations for the transmission of the signals, which therefore leads to a compensation of the $1/2$ extra factor. We assume this scenario.

F. Key rate analysis with orbital dynamics

With all the ingredients in our hands, we now study the numerical behavior of the composable key rate, accounting not only for the fading process but also for the variability associated with the orbital dynamics of the satellite. In fact, there are two basic reasons why the channel is not stable in satellite communications: One is the inevitable fading process affecting the free-space transmission, which occurs even when the satellite is assumed to be 'frozen' at some fixed altitude and zenith angle; the other is the temporal variation of the zenith angle (and altitude) due to the specific orbit. Even if we assume the satellite to be at some fixed (or approximately fixed) altitude, the variation of the zenith angle is inevitable for all orbits in the LEO and MEO regions.

Assume that the satellite is on an orbit with a constant altitude h, which is an assumption valid for polar orbits and approximately valid for sun-synchronous orbits. Then, during the quantum communication of a block of size N, the satellite performs a corresponding slice of its orbit, spanning a range of different zenith angles. The angular size of this slice depends on various factors, including the clock of the system C and the speed of the satellite (which depends on its altitude h). As a result, we have that the value of the maximum transmissivity η (and that of the threshold transmissivity $\eta_{\rm th}$) sensibly changes during the quantum communication. It is clear that this problem also affects the thermal noise $\bar{n}$, due to the general dependence of the setup noise $\bar{n}_{\rm ex}$ on the instantaneous transmissivity.

There are various strategies to deal with this situation. One strategy is to minimize $\eta_{\rm LB}$ and maximize $\bar{n}_{\rm UB}$ over the slice, and then use these values to lower bound the achievable key rate (for an LLO, one could also use a constant maximum value of $\bar{n}_{\rm UB}$, as computed at the Kármán line or at the lower LEO boundary). Another method, which is more practical, is to directly minimize the key rate over the orbital slice. Under typical conditions, the fixed-geometry rate $R(h,\theta)$ decreases for increasing θ, i.e., from the zenith towards the horizon. For this reason, we can lower bound the actual rate by taking the value of $R(h,\theta)$ at the largest zenith angle θ (for any fixed altitude h). In particular, assume that the slice associated with the block has zenith angles $\theta \lesssim 1$. We can therefore lower bound the key rate by taking the value $R(h,\theta=1)$. We call this the "one-radiant" key rate [46].

TABLE V. Protocol parameters adopted with respect to collective attacks and general attacks.

Protocol parameter	Symbol	Collective attacks	General attacks
Total pulses	N	10^8	10^8
Pilot pulses	$m_{\rm PL}$	$0.01\times N$	$0.01\times N$
PE signals	m	$0.1\times N$	$0.1\times N$
Energy tests	$f_{\rm et}$	–	0.2
KG signals	n	$0.89\times N$	$\simeq 7.4\times 10^7$
Digitalization	d	2^5	2^5
Rec. efficiency	β	0.96	0.96
EC success prob	$p_{\rm ec}$	0.9	0.1
Epsilons	$\varepsilon_{\rm h,s,\ldots}$	$2^{-33}\simeq 10^{-10}$	10^{-43}
Confidence	w	$\simeq$6.34	$\simeq$14.07
Security	ε,ε'	$\simeq 5.6\times 10^{-10}$	$\lesssim 2.6\times 10^{-10}$
Modulation	μ	optimized	7
Threshold	$f_{\rm th}$	optimized	0.75

Let us analyze the one-radiant key rates that are achievable by a pilot-guided post-selected heterodyne protocol with LLO at various satellite altitudes for the various configurations. In particular, we choose the protocol parameters specified in Table V. We assume a 1% quota for the pilots [47]. The values of the input modulation μ (i.e., $\bar{n}_T$) and the threshold transmissivity $f_{\rm th}$ (i.e., $\eta_{\rm th}$) are implicitly optimized at each altitude. This is the case for rates under collective attacks (plotted for each configuration). For the study of the general attacks (only done in the best configuration of night-time downlink), we have made the sub-optimal choices of $\mu=7$ and $f_{\rm th}=0.75$. Also note that the security ε' versus general attacks depends on the altitude; its maximum value shown in Table V is achieved for the minimum altitude of $h=100$ km.

Then, we follow all the physical parameters and theoretical models considered so far, explicitly listed in Table VI. However, we allow for the possibilities of different setups on the basis of the spot-size w_0 and receiver aperture a_R. With setup 1, we reproduce the physical conditions adopted for the study of the ultimate bounds presented in Fig. 3 (under the assumption of a narrow filter $\Delta\lambda=0.1$pm). The other setups offer a more generous hardware that allows us to improve the key rates in the various configurations.

In Fig. 6, we show the performances that are achievable in downlink with setup 1, which clearly improve when the better setup 2 is considered, with positive key rates in the LEO region. By contrast, we need to assume the expensive setup 3 for enabling uplink, whose key rates appear to be restricted to the sub-LEO region (between 100 and 160 km). Note that, thanks to the narrow homodyne filter, we may achieve positive

TABLE VI. Physical parameters and theoretical models.

Physical parameter	Symbol	Value
Beam curvature	R_0	∞
Wavelength	λ	800 nm
Beam spot size	w_0	20 cm (setup 1) 40 cm (setup 2) 60 cm (setup 3)
Receiver aperture	a_R	40 cm (setup 1) 1 m (setup 2) 2 m (setup 3)
Receiver field of view	$\Omega_{\rm fov}$	10^{-10} sr
Homodyne filter	$\Delta\lambda$	0.1 pm
Detector shot-noise	$\nu_{\rm det}$	2 (heterodyne)
Detector efficiency	$\eta_{\rm eff}$	0.4
Detector bandwidth	W	100 MHz
Noise equivalent power	NEP	6 pW/$\sqrt{\rm Hz}$
Linewidth	$l_{\rm W}$	1.6 KHz
LO power	$P_{\rm LO}$	100 mW
Clock	C	10 MHz
Pulse duration	Δt, $\Delta t_{\rm LO}$	10 ns
Extinction (at 1 rad)	$\eta_{\rm atm}$	$\simeq$0.94
Pointing error	$\sigma_{\rm P}^2$	$\simeq (10^{-6}z)^2$ (1 μrad)
Structure constant	C_n^2	night/day H-V model
Turbulence parameters	$w_{\rm st}$, $\sigma_{\rm TB}^2$	Appendix C
Background noise	$\bar{n}_B$	Eqs. (42) and (43)

key rates for day-time operation. In particular, in downlink, the suppression of the background is such that the day-time rate coincides with the night-time rate. For uplink, there is still a gap though, which is due to the effects of the ground-level turbulence on the beam. These effects reduce the transmissivity and are higher during the day.

According to our investigation, all the configurations allow for secure quantum communications with a satellite in the LEO/sub-LEO region, even though with different hardware requirements. The homodyne filter largely suppresses the background noise, paving the way for day-light implementations under various weather conditions.

G. Orbital slicing

The one-radiant key rates are pessimistic estimates of what we can actually achieve with a satellite orbiting at an approximately constant altitude. For this reason, we now consider a more accurate treatment where we explicitly account for the fact that different blocks of data correspond to different slices of the orbit within the one-radiant sector. For each slice we consider the corresponding minimum rate, which is achieved at the largest zenith angle along that particular slice. The overall orbital rate is given by an average over the slices.

Before presenting the improved results, we need to make some preliminary considerations about an ideal modus operandi for the ground-satellite link.

In fact, we identify the following ideal conditions.

(i) The transit time of the satellite should allow the parties to distribute many quantum data points.

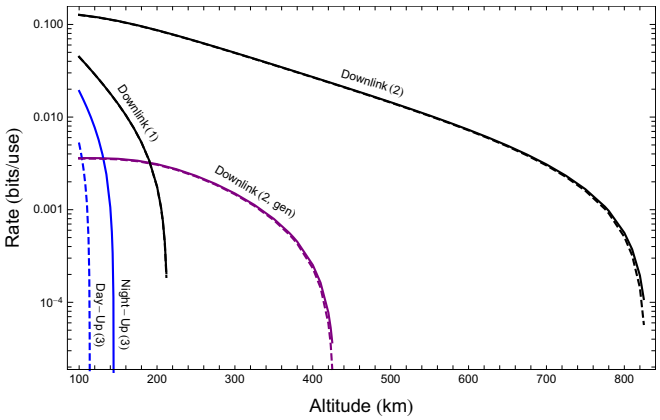

FIG. 6. One-radiant composable key rates (bits/use) achievable by a pilot-guided post-selected heterodyne protocol with LLO at various satellite altitudes h (km). We consider downlink with setups 1 and 2 from Table VI. Black lines refer to the key rate of Eq. (82) while the purple line is the rate of Eq. (83) against general attacks. Solid lines refer to night time, while the overlapping/almost-overlapping dashed lines refer to day time (difference becomes appreciable only for longer distances). We also show the performance in uplink (blue lines), considering Eq. (82) and setup 3 from Table VI. In particular, we compare the night-time uplink (solid blue) with day-time uplink (dashed blue).

(ii) There should be additional time for classical communication and data-processing, in such a way that a secret key is generated before the end of the fly by.

(iii) There should be time for an encrypted communication, exploiting part of the key already distributed.

To satisfy these ideal conditions, it is better to have a satellite that is able to reach small zenith angles. Clearly, an optimal solution is a satellite crossing the zenith point above the ground station (zenith-crossing orbit). For simplicity, assume that its orbit is circular, with constant radius $R_{\rm S} = R_{\rm E} + h$ from the center of the Earth. Examples of circular orbits are polar and near-polar sun-synchronous orbits.

For a zenith-crossing orbit, it is useful to introduce a sign for the zenith angle θ, so that a negative θ corresponds to the zenith angle with respect to a satellite which is arising from the "front" horizon and moving towards the zenith, while a positive θ corresponds to a satellite that has passed the zenith point and it is descending towards the "back" horizon (see Fig. 7).

For a zenith-crossing circular orbit, the slant distance $z = z(R_{\rm S}, \alpha)$ can be expressed as $z(R_{\rm S}, \alpha) = \sqrt{R_{\rm E}^2 + R_{\rm S}^2 - 2R_{\rm E}R_{\rm S}\cos\alpha}$ in terms of $R_{\rm S} = R_{\rm E} + h$ and the orbital angle α (which may also be negative). See also Eq. (A7) and Fig. 12 in Appendix A. Then, we may write the orbital period (in seconds)

$$T_{\rm S} = 2\pi\sqrt{\frac{R_{\rm S}^3}{\mu_{\rm G}}}, \tag{91}$$

where $\mu_{\rm G} = GM_{\rm E}$ is the standard gravitational parameter, with $G = 6.674 \times 10^{-11}$ N m^2 kg^{-2} being the gravitational constant and $M_{\rm E} \simeq 5.972 \times 10^{24}$ kg the approximate Earth's mass. As a result, the orbital angle α varies over time t

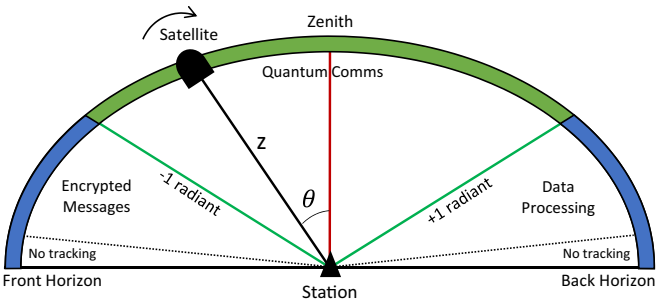

FIG. 7. Orbital sectors for a zenith-crossing circular orbit. Zenith angle θ has an associated sign and we identify the front and the back horizons. Quantum communication occurs within the (green) good sector associated with the angular window $-1 \leqslant \theta \leqslant 1$ (where the angle is negative on the left, i.e., for a rising satellite). There is a transit time $t_{\rm Q}$ associated with this sector. Total transit time $t_{\rm T}$ is associated with the entire flyby from the front to the back horizon. The right blue sector $1 < \theta < \pi/2$ can be used for data processing and key generation. The left blue sector $-\pi/2 < \theta < -1$ can be used for encrypted communication using a previously generated key (e.g., the satellite may download the key exchanged with another station). In practical scenarios, the satellite is not tracked within $5^\circ - 10^\circ$ of the horizon (depending on the urban setting etc.). In other words, there is an effective "mask" angle $\theta_{\rm m}$ (or minimum acceptable elevation above the horizon) for the satellite. In the text, we assume $\theta_{\rm m} = 10^\circ$.

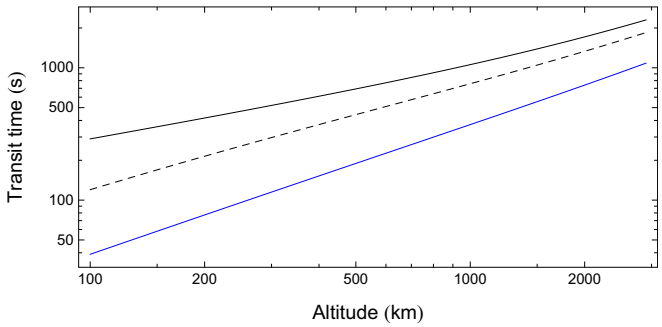

FIG. 8. Transit times (seconds) versus altitudes (kms) for a satellite passing through the zenith in a circular orbit. We plot the total transit time $t_{\rm T}$ from horizon to horizon (solid black), the effective transit time $t_{\rm E}$ accounting for the mask angle (dashed black) and the quantum transit time $t_{\rm Q}$ within the window $-1 \leqslant \theta \leqslant 1$ (solid blue).

according to the law

$$\alpha(t,h) = \frac{2\pi t}{T_{\rm S}} = t\sqrt{\frac{\mu_{\rm G}}{R_{\rm S}^3}}, \tag{92}$$

where we have implicitly set $\alpha = 0$ (satellite at the zenith) for $t = 0$. Correspondingly, the time-varying zenith angle $\theta = \theta(t,h)$ can be computed from

$$\sin\theta = \frac{R_{\rm S}\sin\alpha}{z(R_{\rm S},\alpha)}. \tag{93}$$

We can divide the orbit in different sectors as depicted in Fig. 7. Assuming that the quantum communication occurs within 1 radiant from the zenith (good sector), we compute a corresponding *quantum transit time* $t_{\rm Q}$. Within $|\theta| \leqslant \pi/2$, we may certainly invert $\theta = \theta(t,h)$ into $t = t(\theta,h)$. In fact, we may write

$$t(\theta,h) = \sqrt{\frac{(R_{\rm E}+h)^3}{GM_{\rm E}}}\arccos\left[\frac{R_{\rm E}+z(h,\theta)\cos\theta}{R_{\rm E}+h}\right], \tag{94}$$

where $z(h,\theta)$ is given in Eq. (1) and the initial condition is $t(0,h) = 0$. We then compute the quantum transit time $t_{\rm Q}(h) = 2t(1,h)$, the total transit time $t_{\rm T}(h) := 2t(\pi/2,h)$ of the satellite from horizon to horizon, and the effective transit time $t_{\rm E}(h) := 2t(\pi/2-\theta_{\rm m},h)$, where $\theta_{\rm m}$ is the mask angle (here assumed to be of 10°). Their behaviors are plotted in Fig. 8.

As we can see, at 530 km, the total transit time is about 716 seconds, of which 200 seconds are within 1 radiant. Assuming $t_{\rm Q} \simeq 200$ and a clock of $C = 10$ MHz, we have the quantum communication of $Ct_{\rm Q} \simeq 2\times 10^9$ pulses. Assuming blocks of size $N = 10^8$ (each corresponding to $2N$ pairs of data points for the heterodyne protocol), we have 20 blocks distributed within the one-radiant window of each passage. Since we assume that the protocol runs with an LLO, we also assume that both polarizations are used for the signals (so that we compensate for the time multiplexing associated with the transmission of the reference pulses). Thus condition (i) above can be met.

In order to realize condition (ii), we exploit the orbital sector after the one-radiant window (see Fig. 7) where a 530 km satellite spends $(t_{\rm T}-t_{\rm Q})/2 \simeq 258$ seconds. In particular, accounting for the mask angle $\theta_{\rm m} = 10^\circ$, we have that the satellite is visible for $(t_{\rm E}-t_{\rm Q})/2 \simeq 131$ seconds. During this time, the parties can implement the classical procedures of error correction and privacy amplification, e.g., using the high-speed methods of Refs. [48,49]. Ideally, by using optimal LDPC codes over a 1GHz GPU, the processing of $\simeq 2\times 10^9$ data points may take $\simeq 120$ seconds [45,50]. Such performances for data processing require an highly performant computing hardware. High speed data processing is achievable because of the relatively high signal-to-noise ratio (so that the number of iterations for syndrome extraction in the error correcting procedure is low). As a matter of fact, for downlink from about 500 km, the total loss is less than 10 dB. Note that there is also a latency time in communications with the satellite, of the order of 1.6 ms at that altitude. However, because the procedures can be implemented with limited sessions of one-way CC, this is negligible.

Finally, there is the condition (iii) which is about having enough time for an encrypted communication between the satellite and the ground station. This session can be used for authentication and/or for downloading the key of another ground station via one-time pad. This step can be implemented during the first sector of the orbit, i.e., at zenith angles $-\pi/2 < \theta < -1$. In the basic scenario of Fig. 7, this phase is symmetric to that discussed above and the satellite is visible for about 131 seconds, clearly sufficient for the encrypted communication.

Let us now slice the good sector for quantum communication $(-1 \leqslant \theta \leqslant 1)$ for a zenith-crossing circular orbit. Assume that $n_{\rm bks}$ blocks are transmitted during the flyby. Dividing the quantum transit time $t_{\rm Q}$ by $n_{\rm bks}$, we get the time δt that is needed for each block to be transmitted. These time

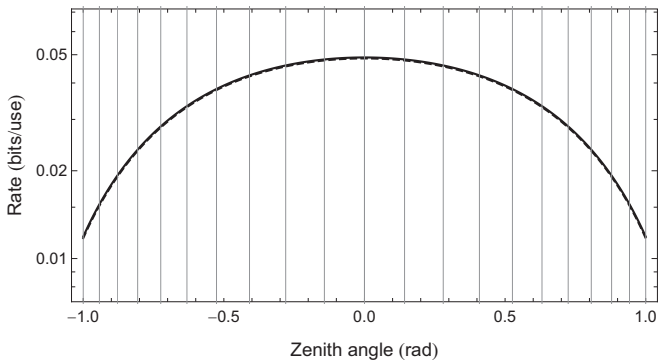

FIG. 9. Composable finite-size key rate R of Eq. (82) for a pilot-guided post-selected heterodyne protocol with LLO. This is plotted versus the zenith angle θ for downlink from a satellite which is in a zenith-crossing circular orbit at $h = 530$ km. We plot the performance for night time (solid) and day time (dashed, overlapping). Parameters are specified in Table V for collective attacks, and Table VI for setup 2. In particular, we choose $\mu = 7.18$ and $f_{\rm th} = 0.76$. Besides the rates we explicitly show the angular lattice in Eq. (97).

intervals identify corresponding angular slices $\{\theta_i, \theta_{i+1}\}$ along the orbit, that can be computed using Eqs. (92) and (93) for any fixed altitude h. For slice $i = 1, \ldots, n_{\rm bks}$ we consider the minimum value

$$R_i = \min_{\theta\in[\theta_i,\theta_{i+1}]} R(\theta), \tag{95}$$

where $R(\theta)$ is the θ-dependent key rate for the considered altitude. Thus the average orbital rate is equal to

$$R_{\rm orb} = \frac{1}{n_{\rm bks}} \sum_{i=1}^{n_{\rm bks}} \max\{0, R_i\} \geqslant R_{\text{1-rad}}, \tag{96}$$

where the bound $R_{\text{1-rad}} := \max\{0, R(\theta = \pm 1)\}$ is the rate associated with the border values (considered in the previous subsection and Fig. 6).

As previously said, for a zenith-crossing circular orbit at $h = 530$ km, the quantum transit time is about 200 seconds. Therefore we may consider $n_{\rm bks} = 20$ blocks, where each block of size $N = 10^8$ corresponds to a transmission time of $\delta t = 10$ seconds for a $C = 10$ MHz clock. This configuration identifies angular slices

$$\{\theta_i, \theta_{i+1}\} \simeq \{-1, -0.942\}, \ldots, \{0.942, 1\}, \tag{97}$$

that are shown in Fig. 9 together with the rate $R(\theta)$ of Eq. (82) specified for night-time and day-time downlink.

For the angle-dependent rate $R(\theta)$, we assume the protocol parameters in Table V for collective attacks, and the physical parameters in Table VI, by choosing spot size and receiver aperture according to setup 2. The values for the modulation and the threshold are chosen in such a way to maximize the lowest rate in the ensemble $\{R_i\}_{i=1}^{n_{\rm bks}}$ which coincides with $R_{\text{1-rad}}$. Thus, in the figure, we have chosen $\mu = 7.18$ and $f_{\rm th} = 0.76$.

Using Eqs. (82) and (97) in Eq. (95) and then Eq. (96), we compute the average orbital rate for downlink, which is approximately the same for night and day, i.e.,

$$R_{\rm orb}^{\rm down} \simeq \begin{cases} 3.066 \times 10^{-2} \text{ bits/use (night time)} \\ 3.041 \times 10^{-2} \text{ bits/use (day time).} \end{cases} \tag{98}$$

Here "per use" means per use of the quantum communication channel, occurring within 1 radiant. When we plug a clock $C = 10$ MHz, we have a rate of $R_{\rm orb}^{\rm down} \simeq 307$ kbits/s during night time, and $R_{\rm orb}^{\rm down} \simeq 304$ kbits/s during day time. Accounting for the time of the quantum communication (200 s), each night-time zenith-crossing passage distributes $\simeq 6.13 \times 10^7$ secret bits, while a day-time zenith-crossing passage distributes $\simeq 6.08 \times 10^7$ secret bits. Considering that, within 24 hours, there will also be non-zenith-crossing passages (exploitable for QKD), the above estimates lowerbound the number of bits that can be distributed per day via night- and day-time operation. (Alternatively, in a less-performant hardware, the other passages can be used for data processing by the parties).

Now consider uplink to a satellite in the sub-LEO region. We take $h = 103$ km, just after the Kármán line. As we have already mentioned, the main reason for the inferior performance in uplink is the nontrivial effect of the atmospheric turbulence, with bigger impact during the day. We consider the rate $R(\theta)$ of Eq. (82) for the case of a pilot-guided post-selected heterodyne protocol with LLO, specified for night-time and day-time uplink. We assume the protocol parameters given in Table V for collective attacks, and the physical parameters in Table VI, where we assume the more demanding setup 3. The values for the modulation μ and the threshold $f_{\rm th}$ are chosen to maximize the lowest rate ($R_{\text{1-rad}}$). In particular, we choose $\mu = 6.5$ and $f_{\rm th} = 0.74$.

Because of the lower altitude, we have a total transit time of just $t_{\rm T} \simeq 295$ s, an effective transit time of $t_{\rm E} \simeq 123$ s, and a quantum transit time of $t_{\rm Q} \simeq 40$ s. The latter allows the parties to distribute 4 blocks of size 10^8 with a clock of $C = 10$ MHz (and these blocks may be data-processed in $\simeq 24$ s, which is enough for the last sector of the orbit by assuming highly performant error-correcting codes). The orbital slices associated with the 10 s-long blocks are

$$\{\theta_i, \theta_{i+1}\} \simeq \{-1, -0.65\}, \{-0.65, 0\}, \{0, 0.65\}, \{0.65, 1\}. \tag{99}$$

Both the rate $R(\theta)$ and the slices are shown in Fig. 10.

Using Eqs. (82) and (99) in Eq. (95) and then Eq. (96), we compute the average orbital rate in uplink, which is equal to

$$R_{\rm orb}^{\rm up} \simeq \begin{cases} 4.244 \times 10^{-2} \text{ bits/use (night time)} \\ 2.737 \times 10^{-2} \text{ bits/use (day time)} \end{cases}. \tag{100}$$

At 10 MHz this rate corresponds to about 424 kbit/s at night and 273 kbit/s during the day. Accounting for a quantum transit time of 40 s, we have that each zenith-crossing passage distributes $\simeq 1.69 \times 10^7$ secret bits for night uplink, and $\simeq 1.09 \times 10^7$ secret bits for day uplink.

According to our analysis, it is indeed feasible to use CV-QKD protocols to distribute keys with a satellite orbiting in the LEO/sub-LEO region, accounting not only for the fading process due to turbulence and pointing errors, but also for the fast orbital dynamics (which creates additional problems for the transmission of reasonably large block sizes). Our analysis

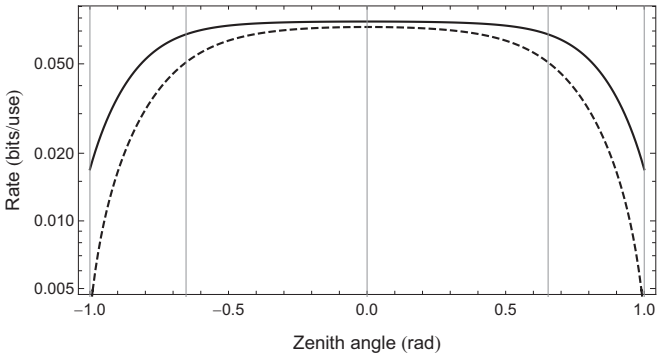

FIG. 10. Composable finite-size key rate R of Eq. (82) for a pilot-guided post-selected heterodyne protocol with LLO. This is plotted versus the zenith angle θ for uplink to a satellite which is in a zenith-crossing circular orbit at $h = 103$ km. We plot the performance for night (solid) and day (dashed) time. Parameters are specified in Table V for collective attacks, and Table VI for setup 3. In particular, we choose $\mu = 6.5$ and $f_{\rm th} = 0.74$. Besides the rates we show the angular lattice generated by the slices of Eq. (99).

shows this possibility not only for the best-considered scenario of night-time downlink, but also for day-time downlink and for the more challenging scenarios of night- and day-time uplink.

H. Satellites versus ground-based repeaters

Once we have computed the secret key rates that are achievable in the most relevant configurations for satellite and ground station, we now show that satellite quantum communications are able to provide a nontrivial advantage with respect to the use of quantum repeaters on the ground, when the aim is to connect two remote end-users that are sufficiently far apart on Earth's surface.

An example of circular orbit is a polar orbit, i.e., with orbital inclination $\iota = 90^\circ$. However, a more practical scenario is considering a near-polar satellite in sun-synchronous orbit (which is approximately circular). This type of orbit guarantees that the satellite passes over any point on Earth's surface at the same local mean solar time. This clearly implies the possibility of stable conditions for night-time or day-time operation, so that the quantum communication with the satellite occurs at roughly the same time of the night or the day.

For a sun-synchronous satellite at altitude h, the orbital inclination is given by

$$\iota = \frac{360}{2\pi} \arccos\left[-\left(\frac{R_{\rm E}+h}{12352}\right)^{7/2}\right], \tag{101}$$

where $h \leqslant 5980$ is expressed in km. At $h = 530$ km, this corresponds to $\iota \simeq 97.5^\circ$. Because the orbital period is $T_{\rm S} \simeq 95$ minutes, the satellite performs 15 orbits a day, before returning above the initial point. Note that the Micius satellite is sun-synchronous with $\iota \simeq 97.4^\circ$ and with altitude between 488 and 584 km. At $h = 103$ km, we have $\iota \simeq 96^\circ$, $T_{\rm S} \simeq 86$ minutes and 16 orbits a day.

Assume that two ground stations are along the orbital path, so that the satellite crosses both their zenith positions, which happens once per day. We assume the worst-case scenario in which the stations interact with the satellite only during the sections of the orbit where the zenith positions are crossed (of course this assumption can be relaxed and the ground stations could also use other passages that are not zenith-crossing). Also assume that the stations are in similar operational conditions, so that we can simultaneously adopt the results for night time or day time for both of them. Finally, assume that the satellite may have the option to communicate with two stations simultaneously (e.g., using two quantum transmitters or receivers); this is assumed to address the particular case where the stations are close, so that the satellite appears within their one-radiant angular windows roughly at the same time (clearly this is not the case for very distant ground stations).

Start with the satellite at the zenith of the first station ($t = 0$) and assume that it reaches the zenith of the second station after time Δt. For $\Delta t \leqslant T_{\rm S}/2$, the distance between the two stations is equal to

$$d_{\rm st} = \alpha(\Delta t, h) R_{\rm E} = \frac{2\pi\,\Delta t R_{\rm E}}{T_{\rm S}} \in [0, \pi R_{\rm E}], \tag{102}$$

where we have used Eq. (92) and accounted for Earth's curvature. Then, assume that the two stations are also connected by an optical fiber with standard loss rate of $\alpha_{\rm fib} = 0.2$dB/km, so that we have a total fiber transmissivity of $\eta_{\rm fib} = 10^{-\alpha_{\rm fib} d_{\rm st}/10}$. The maximum fiber-based repeater-less rate (bits per use) is given by the PLOB bound $R_{\rm fib} = -\log_2(1-\eta_{\rm fib})$ [12]. Multiplying by the clock $C = 10$ MHz and the number of seconds in one day $\#_{\rm day} \simeq 8.6 \times 10^4$, we may compute the maximum number of secret bits that can the distributed in one day $CR_{\rm fib}\#_{\rm day}$ as a function of the station-to-station ground distance. We also assume the situation where a number $N_{\rm rep} \geqslant 1$ of ideal repeaters are inserted along the fiber line, so that we have the fiber-based rate becomes $R_{\rm fib}^{\rm rep} = -\log_2(1 - \sqrt[N_{\rm rep}+1]{\eta_{\rm fib}})$ [16]. We have a corresponding number of secret bits $CR_{\rm fib}^{\rm rep}\#_{\rm day}$ per day.

In Fig. 11, we consider the maximum number of secret bits per day (versus ground distance) that can be distributed by a repeaterless fiber link between the stations and also by fiber links assisted by ideal quantum repeaters. Assuming the same clock, we compare these ground-based performances with the secret-bits per day that can be distributed by using a satellite moving between the two stations, the latter operating in the same way with respect to the satellite, i.e., via night/day-time downlink [Eq. (98)] or night/day-time uplink [Eq. (100)].

We can see how a satellite can beat the fiber-based repeaterless bound when the stations are separated by more than 215 km, and how it can achieve the same rate of 30 ideal quantum repeaters when the station-to-station ground separation is about 6675 km. This performance is achievable in downlink no matter if during the day or the night (solid red line in Fig. 11). As expected, in uplink, the performances are worse than downlink (despite the better setup). That being said, via uplink to the satellite, the remote users are still able to beat ground chains of quantum repeaters after similar distances.

IV. CONCLUSIONS

In this work, we have established the ultimate limits and the practical rates that can be achieved in secure quantum communications with satellites, assuming various configurations

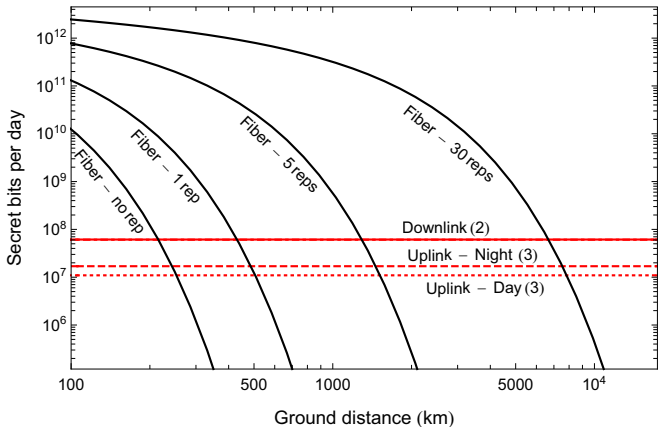

FIG. 11. Secret-key bits per day versus ground distance (km) between two stations, assuming a clock of 10 MHz. We consider the maximum performances achievable by a repeaterless fiber-connection (PLOB bound) and repeater-based fiber-connections assisted by 1, 5, and 30 ideal quantum repeaters (solid lines). These are compared with the constant performances achievable by connecting the two ground stations via a near-polar sun-synchronous satellite. We consider $h = 530$ km in downlink [Eq. (98) based on setup 2 in Table VI] and $h = 103$ km in uplink [Eq. (100) based on setup 3 in Table VI]. In particular, from the top to the bottom, we show downlink at night-time (solid red) and day-time (dot-dashed red, overlapping with the solid line). Then we show uplink at night (dashed red) and during the day (dotted red).

(downlink/uplink) and operational settings (night or day time). While our study is based on ideas and tools developed in Ref. [14] for free-space quantum communications, it also required a number of nontrivial generalizations in order to account for the slant propagation at variable altitudes and beyond the atmosphere. As a matter of fact, the underlying physical models for atmospheric turbulence and background noise have crucial differences with respect to the models adopted for free-space communications on the ground.

We have started our work by establishing information-theoretic upper limits to the maximum number of secret bits (and ebits) that can be achieved per use of the satellite link in all scenarios. Our theoretical analysis considers all relevant effects, as due to diffraction, atmospheric extinction, limited efficiency, pointing error, turbulence, thermal background, and setup noise.

In uplink, turbulence is very important because it affects the beam close to the transmitter where the spot size is small. In this case, both pointing error and turbulence effects must be accounted for. By contrast, in downlink, the spot size is already very large when it enters the atmosphere, compared to the typical size of the turbulent eddies. For this reason, turbulence is negligible and the only relevant effect is the pointing error.

A further asymmetry is introduced by the background noise that is induced by sky brightness and planetary albedos (Moon and Earth), even though this background can be greatly suppressed by using narrow frequency filters. Such filters are indeed created by the interferometric process occurring in homodyne-like setups where the signals are mode-matched with a strong local oscillator.

For all configurations, we have studied the numerical behavior of the ultimate key rates when the satellite is at the zenith position or at 1 radiant from the zenith, showing that a large range of altitudes are possible for secure key generation (and entanglement distribution) when we adopt optimal protocols. For the same configurations, we have then studied secret key rates that are achievable in practice by accounting for finite-size effects and composable security. Our analysis therefore addresses the problem of block size, which is particularly relevant for satellite quantum communications (see also Ref. [51] for the setting of discrete-variable QKD).

In our paper, the use of a pilot-guided post-selected heterodyne protocol, combined with a careful consideration for the orbital dynamics, enables the implementation of CV-QKD between station and satellite in all configurations of night-time downlink/uplink and day-time downlink/uplink. It is interesting that all these scenarios represent indeed a viable option for secure quantum communications, whereas only the setting of night-time downlink has been considered in other works [52].

As a further analysis beyond this work, it would be interesting to compare the QKD rates that are achievable by CV protocols with those of discrete-variable protocols in the various configurations of communication with the satellite. Since discrete-variable QKD is more robust for long-distance implementations on the ground, we would expect this approach to be particularly suitable for the far-LEO and MEO regions. By contrast, CV-QKD is generally better for high-rate implementations at shorter ground distances, so it appears an approach specifically suitable for the LEO and sub-LEO regions.

Finally, we have shown that a sun-synchronous satellite, exchanging keys with ground stations, is able to distribute more secret bits per day than a direct fiber-connection between the stations, even if the latter communicate at the ultimate PLOB bound. Remarkably, the satellite is also able to outperform a chain of many ideal quantum repeaters operating between the remote stations. These results are obtained when the distance between the remote stations surpasses certain thresholds, which depend on the hardware available for the satellite together with the adopted configuration (downlink/uplink) and operational setting (night/day time).

ACKNOWLEDGMENTS

The author acknowledges funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 820466 (Quantum-Flagship Project CiViQ: "Continuous Variable Quantum Communications").

APPENDIX A: BASIC GEOMETRY FOR SATELLITE COMMUNICATIONS

Here we discuss some geometrical elements about communications with satellites. The slant distance z between a sea-level ground station and a satellite can be connected with other two important parameters. The first one is the (positive) zenith angle θ which is defined as the angle between the vertical direction (zenith) and the pointing direction from the ground station to the satellite. The second one is the altitude

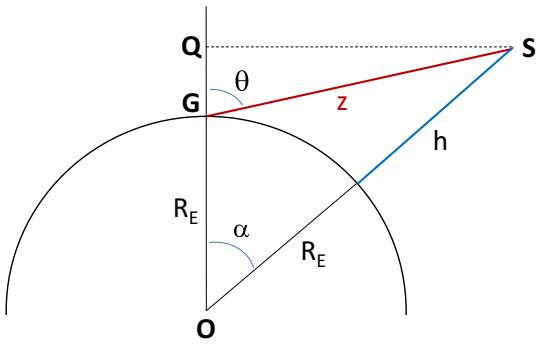

FIG. 12. Basic geometry for satellite communications. A satellite (S) is at slant distance z from a sea-level ground station (G). The satellite is at zenith angle θ and altitude h over the Earth's surface. Clearly, $z = h$ only at the zenith ($\theta = 0$). The satellite is also at the orbital angle α and orbital radius $R_S = h + R_E$, where R_E is the radius of the Earth. Note that $\overline{OQ} = R_E + \overline{QG} = \overline{OS}\cos\alpha$ leads to (1) $R_E + z\cos\theta = R_S\cos\alpha$. Now, from $\overline{QS}$ have (2) $z\sin\theta = R_S\sin\alpha$. By taking the squared in (1) and (2) and using $\cos^2\alpha = 1 - \sin^2\alpha$, we derive $h^2 + 2R_E h - z(z + 2R_E\cos\theta) = 0$ whose positive solution gives Eq. (A1). In a similar way, one can use $\cos^2\theta = 1 - \sin^2\theta$ and derive Eq. (A7).

h of the satellite, which is defined as the distance from the satellite to the ground (sea-level) orthogonally to the surface of the Earth. Slant distance z, altitude h, and positive zenith angle $\theta \in [0, \pi/2]$ can be easily connected by means of simple trigonometric observations. (Note that the following geometric formulas do not change if we include a sign in the zenith angle, so that $\theta \in [-\pi/2, \pi/2]$, as considered for the study with the zenith-crossing orbit in the main text).

It is easy to express the altitude h as a function of z and θ. A simple trigonometric calculus provides

$$h(z,\theta) = \sqrt{R_E^2 + z^2 + 2zR_E\cos\theta} - R_E, \tag{A1}$$

where $R_E \simeq 6371$ km is the approximate radius of the Earth (see Fig. 12). In particular, at small angles $\theta \simeq 0$, we can write the simplified "flat-Earth" approximation

$$h(z,\theta) \simeq z\cos\theta_z + \mathcal{O}(\theta^3),\ \theta_z := \theta\sqrt{\frac{R_E}{R_E + z}}. \tag{A2}$$

For $\theta \leqslant 1$ and relatively small h (of the order of the atmospheric thickness, i.e., 20 km), one finds that $h \simeq z\cos\theta$ and $z \simeq h\sec\theta$ represent excellent approximations.

It is easy to see that Eq. (A1) can be inverted into

$$\cos\theta = \frac{h}{z} + \frac{h^2 - z^2}{2zR_E}, \tag{A3}$$

which gives the zenith angle θ in terms of z and h (see also Ref. ([53], Ch. 13)). Similarly, the slant range z can be expressed as a simple function of h and θ, i.e., we may write the slant distance functional (see also Ref. [22])

$$z(h,\theta) = \sqrt{h^2 + 2hR_E + R_E^2\cos^2\theta} - R_E\cos\theta. \tag{A4}$$

Note that $z(h,\theta) \leqslant h\sec\theta$ for any h and $\theta \in [0, \pi/2]$.

It is easy to verify that the previous formulas can immediately be generalized to the scenario where the ground station is located at some nonzero altitude h_0. Setting $R_G := R_E + h_0$ and $R_S = R_E + h$, we may in fact write

$$h(z,\theta) = \sqrt{R_G^2 + z^2 + 2zR_G\cos\theta} - R_E, \tag{A5}$$

$$z(h,\theta) = \sqrt{R_S^2 + R_G^2(\cos^2\theta - 1)} - R_G\cos\theta. \tag{A6}$$

Another parametrization is in terms of orbital radius R_S and the orbital angle α, i.e., the angle between the position of the ground station and the position of the satellite as seen from the center of the Earth. It is immediate to see that

$$z(R_S,\alpha) = \sqrt{R_E^2 + R_S^2 - 2R_E R_S\cos\alpha}. \tag{A7}$$

This parametrization is useful for circular orbits, where R_S is constant. In this case, we can write $\alpha = 2\pi t/T_S$, where t is time and T_S is the orbital period, i.e., the time needed for a complete revolution around the Earth.

APPENDIX B: REFRACTION EFFECTS

In a more refined description, we need to consider atmospheric refraction. Assuming the atmosphere to be modeled as a set of thin uniform slabs provides the same result of an atmosphere modeled as a single uniform slab with surface refractive index n_0 ([53], Ch. 13, Fig. 13.4). Therefore atmospheric refraction creates an apparent zenith angle θ_{app} satisfying Snell's law

$$\sin\theta_{app} = n_0^{-1}\sin\theta, \tag{B1}$$

where $n_0 \simeq 1.00027$ is the surface value of the refractive index. We see that the angle of refraction $\Delta\theta := \theta - \theta_{app}$ exceeds one degree when the satellite is at the horizon, where $\theta = \pi/2$ corresponds to $\theta_{app}^{max} \simeq 1.548$ ($\simeq 88.7^\circ$). Besides the apparent angle, refraction also increases the optical path by an elongation factor $\varepsilon_{elo} = \varepsilon_{elo}(\theta_{app})$.

Replacing $\theta = \theta(\theta_{app}) := \arcsin(n_0\sin\theta_{app})$ in $z(h,\theta)$ and multiplying by ε_{elo}, one gets the refracted slant range

$$z_{ref}(h,\theta_{app}) = \varepsilon_{elo}(\theta_{app})z[h,\theta(\theta_{app})], \tag{B2}$$

as a function of the altitude h and the apparent angle θ_{app}. Replacing $\theta = \theta(\theta_{app})$ and $z = z_{ref}/\varepsilon_{elo}(\theta_{app})$ in $h(z,\theta)$, we get the altitude in terms of the refracted parameters, i.e.,

$$h = h_{ref}(z_{ref},\theta_{app}) := h[z_{ref}/\varepsilon_{elo}(\theta_{app}),\theta(\theta_{app})]. \tag{B3}$$

With these modifications in hand, we can formulate the refracted version of the atmospheric extinction in Eq. (10) of the main text. We need to integrate $\alpha(h) = \alpha_0\exp(-h/\tilde{h})$ (with α_0 and $\tilde{h}$ given in the main text) using the modified expression for the slant distance $z_{ref}(h,\theta_{app})$ and the expression of the altitude $h_{ref}(z_{ref},\theta_{app})$. We get

$$\eta_{atm}^{ref}(h,\theta_{app}) = \exp\left\{-\int_0^{z_{ref}(h,\theta_{app})} dy\,\alpha[h_{ref}(y,\theta_{app})]\right\} = e^{-\alpha_0 g_{ref}(h,\theta_{app})}, \tag{B4}$$

where we have defined

$$g_{ref}(h,\theta_{app}) := \int_0^{z_{ref}(h,\theta_{app})} dy\exp\left[-\frac{h_{ref}(y,\theta_{app})}{\tilde{h}}\right]. \tag{B5}$$

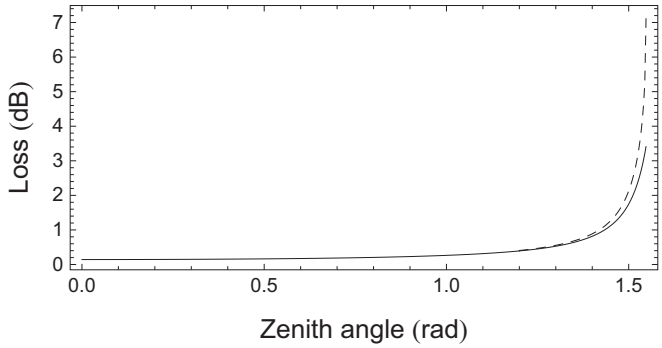

FIG. 13. Atmospheric loss (decibels) versus zenith angle (radiants) in the link between a sea-level ground station and a satellite at $h = 780$ km, for $\lambda = 800$ nm. We plot the refraction-free model for atmospheric loss $-10\log_{10}\eta_{\rm atm}$ [given by Eq. (10) of the main text] with respect to the zenith angle θ (solid line), and the refraction-based model $-10\log_{10}\eta_{\rm atm}^{\rm ref}$ of Eq. (B4) with respect to the apparent zenith angle $\theta_{\rm app}$ (dashed line).

Correspondingly, we can modify the bound in Eq. (15) of the main text to account for refraction. We obtain

$$\mathcal{B}_{\rm ref}(h,\theta_{\rm app}) = -\log_2\Big[1-\eta_{\rm eff}e^{-\alpha_0 g_{\rm ref}(h,\theta_{\rm app})} \times\left(1-e^{-\frac{2a_R^2}{w_d[z_{\rm ref}(h,\theta_{\rm app})]^2}}\right)\Big]. \tag{B6}$$

For low transmissivity, which is certainly the case in the far field regime $z \gg z_R$, we can approximate

$$\mathcal{B}_{\rm ref}(h,\theta_{\rm app}) \simeq \frac{2}{\ln 2}\frac{a_R^2\eta_{\rm eff}e^{-\alpha_0 g_{\rm ref}(h,\theta_{\rm app})}}{w_d[z_{\rm ref}(h,\theta_{\rm app})]^2}. \tag{B7}$$

In Fig. 13, we investigate the effects of refraction on the channel loss. For typical parameters, we see that refraction is negligible within $\simeq 1$ radiant from the zenith, while it becomes more and more relevant in the proximity of the horizon. For a sea-level ground station communicating with a satellite at $h = 780$ km and apparent zenith angle $\theta_{\rm app}^{\rm max}$, we compute $\eta_{\rm atm}^{\rm ref} \simeq 7.1$dB from Eq. (B4) instead of $\eta_{\rm atm} \simeq 3.4$ dB from Eq. (10) of the main text (setting $\theta = \theta_{\rm app}^{\rm max}$). This discrepancy leads to differences between $\mathcal{B}$ and its refraction-based version $\mathcal{B}_{\rm ref}$ for large angles, i.e., close to the horizon.

Finally, it is worth mentioning that the formula in Eq. (B6) can also be applied to the case where the ground station is at some non-negligible altitude h_0. In fact, it is sufficient to use Eqs. (A5) and (A6) in all the previous expressions that lead to Eq. (B6).

APPENDIX C: ATMOSPHERIC TURBULENCE

1. Weak turbulence

Atmospheric turbulence leads different treatments depending on its strength. From a physical point of view, turbulence effects are due to eddies affecting the traveling beam. In a regime of weak turbulence, one can clearly distinguish the action of small and large turbulent eddies. Those smaller than the beam waist tend to broaden the beam (on a fast time scale), while those larger than the beam waist tend to deflect the beam, randomly but on a slower time scale [28]. As a result, the broadening of the beam can be decomposed into a sum of two contributions, the short-term spot size $w_{\rm st}^2$ plus the random wandering of the beam centroid with variance $\sigma_{\rm TB}^2$, so that there is a long-term spot size ([28], Eq. (32))

$$w_{\rm lt}^2 = w_{\rm st}^2 + \sigma_{\rm TB}^2. \tag{C1}$$

The slower time scale is of the order of 10–100 ms [29], which means that this dynamics can be resolved by a fast-enough detector.

For long-distance communication, if turbulence becomes stronger, the motion of the centroid becomes negligible ($\sigma_{\rm TB}^2 \simeq 0$). At some point, strong beam deformation comes into place as a major effect, and the beam will eventually break up in multiple patches [28,54].

The first step is therefore the correct characterization of the relevant regime of turbulence, which requires the introduction of parameters from the theory of optical propagation through turbulent media. The most important of these parameters is the refraction index structure constant C_n^2 [32,55], since this is at the basis of the others and, in particular, the scintillation index [32], that characterizes the strength of turbulence, and the spherical-wave coherence length [28], that directly enters in the expressions of the spot sizes of Eq. (C1).

2. Refraction index structure constant

The structure constant C_n^2 measures the strength of the fluctuations in the refraction index, due to spatial variations of temperature and pressure. We need to consider an adequate model for the structure constant $C_n^2(h)$, so that this quantity can be suitably averaged over different altitudes for up- and down-link communication.

Assuming the Hufnagel-Valley (H-V) model of atmospheric turbulence [30,31], the structure constant reads

$$C_n^2(h) = 5.94\times10^{-53}\left(\frac{v}{27}\right)^2 h^{10}e^{-h/1000} + 2.7\times10^{-16}e^{-h/1500} + Ae^{-h/100}, \tag{C2}$$

where $h > 0$ is expressed in meters, v is the windspeed (m/s) and A is the nominal value of $C_n^2(0)$ at the ground in units $\mathrm{m}^{-2/3}$ (MKS units are implicitly assumed in all these formulas). These parameters depend on the atmospheric conditions and the time of the day.

Similarly to Ref. [29], one can assume the typical night-time value $A = 1.7\times10^{-14}\,\mathrm{m}^{-2/3}$ and low-wind $v = 21$ m/s [56]. This is also known as the H-$V_{5/7}$ model ([32], Sec. 12.2.1). However, during the day, parameter A can be of the order of $2.75\times10^{-14}\ \mathrm{m}^{-2/3}$ [57] and, for high-wind conditions, v can be of the order of $v = 57$ m/s [23]. In our work, we adopt H-$V_{5/7}$ as night-time model, and H-V with parameters $A = 2.75\times10^{-14}\,\mathrm{m}^{-2/3}$ and $v = 21$ m/s as day-time model. Finally, we may also consider H-V with parameters $A = 2.75\times10^{-14}\,\mathrm{m}^{-2/3}$ and $v = 57$ m/s as the worst-case day-time model.

It is important to remark that there are other models for $C_n^2(h)$. These include the VanZandt model [58], with a simplified version proposed by Dewan *et al.* [59], and the Walters and Kunkel model [60]. For instance, they have been used in Ref. ([22], Appendix D). These other approaches and the H-V model are in good agreement with thermosonde data in

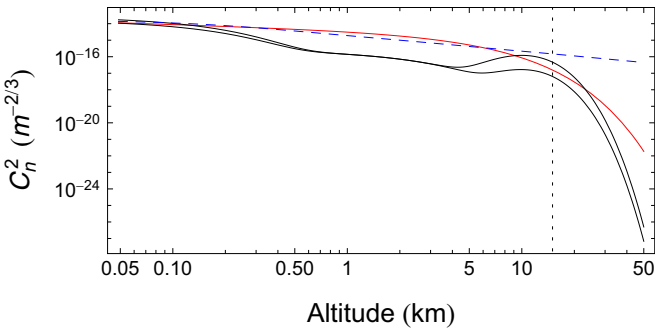

FIG. 14. Optical turbulence profile in the atmosphere, quantified by the refraction index structure constant C_n^2 as a function of the altitude h. More precisely, we plot the predictions of the Hufnagel-Valley model of Eq. (C2) (black curves) considering the typical night-time parameters (H-$V_{5/7}$, lower black curve) and the worst-case day-time parameters (i.e., the worst-case day-time model, upper black curve). We compare these predictions with the simplified model of Eq. (C3) (red curve), which is an approximate upper bound at most altitudes. We can clearly see the exponential fall of $C_n^2(h)$ after $\simeq 15$ km (vertical dotted line), compared with the single-layer average value $\bar{C}_n^2(h)$ of Eq. (C5) (dashed blue line).

Ref. [61] (see also Ref. ([22], Fig. 13)). Here we also consider a simplified version of this model, as originally proposed by Hufnagel and Stanley ([30], Fig. 6). This is given by ([62], Eq. (3.1))

$$C_n^2(h) \simeq c_1 h^{-1/3} \exp\left(-\frac{h}{c_2}\right), \tag{C3}$$

$$c_1 = 4.2 \times 10^{-14},\ c_2 = 3200, \tag{C4}$$

so that $C_n^2 \simeq 10^{-14}\,\mathrm{m}^{-2/3}$ a few meters high. See also Ref. ([63], Ch. 3) and Ref. ([64], Ch. 8).

In Fig. 14, we show the H-V model of Eq. (C2) and the simplified Hufnagel-Stanley model in Eq. (C3) which are in good agreement. We can see that, at higher altitudes, C_n^2 starts to decrease exponentially. As a matter of fact, it can be considered to be negligible beyond $h_{\max} \simeq 20$ km. This altitude corresponds to the upper edge of the tropopause, below which most of the mass of the atmosphere is contained. Taking $h_{\max}$ as effective thickness of the atmosphere can also be justified by the following argument. Let us treat the atmosphere as a single layer of thickness h and structure constant given by the average

$$\bar{C}_n^2(h) = h^{-1} \int_0^h d\xi C_n^2(\xi), \tag{C5}$$

computed according to the standard H-$V_{5/7}$ model. From Fig. 14, we can see how this quantity exponentially departs from the previous models after 15 km. At $\simeq 20$ km, the difference is about two orders of magnitude.

For a satellite at altitude h and zenith angle $\theta \lesssim 1$ communicating with a sea-level ground station, the effective section of the atmosphere which is crossed by the beam is given by $z_{\mathrm{atm}}(\theta) = z(h_{\max}, \theta)$ using the slant functional in Eq. (A4). At one radiant, we have $z_{\mathrm{atm}}(1) \simeq 37$ km, which is of the same order of magnitude of $h_{\max}$. For larger angles, refraction comes into place and one needs to use the elongated slant distance in Eq. (B2). At the horizon, the section becomes large even neglecting the elongation by refraction. In fact, we have

$$z_{\mathrm{atm}}(\pi/2) = \sqrt{h_{\max}^2 + 2h_{\max}R_{\mathrm{E}}} \simeq 505\ \mathrm{km}. \tag{C6}$$

An important observation is that, for $\theta \lesssim 1$ and $h \leqslant h_{\max}$, we may certainly use the approximations

$$z(h, \theta) \simeq h \sec\theta,\ \ h(z, \theta) \simeq z \cos\theta, \tag{C7}$$

since the relative error $[z(h, \theta) - h \sec\theta]/z(h, \theta)$ remains less than 0.4%. In the integral of Eq. (C5), the structure constant C_n^2 is non-negligible only for values $\xi \leqslant h_{\max}$, so we may write

$$\bar{C}_n^2(h) \simeq h^{-1} \int_0^{h_{\max}} d\xi C_n^2(\xi) \simeq h^{-1} \int_0^{\infty} d\xi C_n^2(\xi). \tag{C8}$$

This observation leads to a simplification when we write $\bar{C}_n^2$ and similar integrals in terms of the slant distance $z = z(h, \theta)$. In fact, for zenith angles $\theta \lesssim 1$, we may write the approximation

$$\bar{C}_n^2(z, \theta) := z^{-1} \int_0^z dz' C_n^2[h(z', \theta)] \tag{C9}$$

$$\simeq z^{-1} \sec\theta \int_0^h d\xi C_n^2(\xi). \tag{C10}$$

3. Scintillation index and Rytov variance

An important issue in free-space communication with turbulence is the evaluation of the scintillation effects. In general, scintillation corresponds to irradiance fluctuations, causing variations of the field intensity across the aperture of the receiver, both temporally (twinkles) and spatially (speckles). As a result, for an input Gaussian beam, the intensity profile at the receiver will not be simply given by

$$I(z, r) = \frac{w_0^2}{w_d(z)^2} \exp[-2r^2/w_d(z)^2], \tag{C11}$$

but there will be some instantaneous random profile $I(z, \mathbf{r})$, where $\mathbf{r} = (x, y)$ is the radial coordinate at the receiver and z the longitudinal coordinate.

Mathematically, one defines the scintillation index as the normalized variance of the field intensity [65]

$$\sigma_I^2(z, \mathbf{r}) := \frac{\langle I(z, \mathbf{r})^2 \rangle}{\langle I(z, \mathbf{r}) \rangle^2} - 1, \tag{C12}$$

where the average is taken over the random fluctuations. This index is usually decomposed into a longitudinal (on-axis) and transverse (off-axis) parts [32,65]

$$\sigma_I^2(z, \mathbf{r}) = \sigma_I^2(z, \mathbf{0}) + \sigma_{I,r}^2(z, \mathbf{r}). \tag{C13}$$

The condition of weak fluctuation (weak turbulence) corresponds to $\sigma_I^2(z, \mathbf{r}) < 1$ throughout the beam profile. If this is the case, the mean intensity can be closely approximated by a Gaussian spatial profile [66–68].

According to previous studies [65,69], the regime of weak turbulence holds for zenith angles smaller than 1 radiant (i.e., about 60°) assuming the standard H-$V_{5/7}$ atmospheric model. For downlink, this is true for any beam waist w_0. For uplink, the off-axis scintillation index $\sigma_{I,r}^2(z, \mathbf{r})$ increases with w_0, but

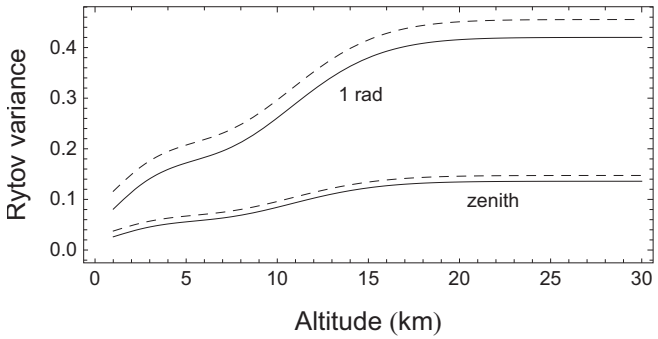

FIG. 15. Rytov variance versus altitude h (km) for $\theta = 0$ (zenith) and $\theta = 1$, considering $\lambda = 800$ nm. We plot the Rytov variance assuming the H-V model with night-time parameters (H-$V_{5/7}$ model, solid lines) and the H-V model with typical day-time parameters (dashed lines). In all cases, the Rytov variance saturates at values that are <1.

still remains reasonably small over the receiver's aperture if this is not too large (condition which is typically satisfied at the satellite). Under the assumption of weak fluctuations, one can use Rytov approximation for the beam field [70], together with the Kolmogorov power-law spectrum [71], and develop a simple formalism for the theory of turbulence.

In a weak-fluctuation theory, the longitudinal scintillation index $\sigma_L^2 := \sigma_I^2(z, \mathbf{0})$ can be easily written for both downlink and uplink. For a downlink path from a satellite at altitude h and zenith angle $\theta \lesssim 1$, this index equals the Rytov variance for a plane wave $\sigma^2_{R,\text{plane}}$, i.e. [32,69]

$$\sigma^2_{L,\text{down}} = \sigma^2_{\text{Rytov}} := 2.25k^{7/6}h^{5/6}(\sec\theta)^{11/6}\mu(h), \tag{C14}$$

$$\mu(h) := \int_0^h d\xi C_n^2(\xi)\left(\frac{\xi}{h}\right)^{5/6}. \tag{C15}$$

Note that, if we impose C_n^2 to be constant in the integral of Eq (C15), then σ^2_{Rytov} becomes $1.23C_n^2k^{7/6}z^{11/6}$, which is the expression for the Rytov variance that is valid for fixed-altitude z-long propagation.

For an uplink path, we may instead write [72]

$$\sigma^2_{L,\text{up}} = \sigma^2_{L,\text{down}}\frac{\tilde{\mu}(h)}{\mu(h)}, \tag{C16}$$

$$\tilde{\mu}(h) := \int_0^h d\xi C_n^2(\xi)\left(\frac{\xi}{h}\right)^{5/6}\left(1-\frac{\xi}{h}\right)^{5/6}. \tag{C17}$$

As noted in Ref. [69], one can approximate $\tilde{\mu}(h) \simeq \mu(h)$, implying $\sigma^2_{L,\text{up}} \simeq \sigma^2_{\text{Rytov}}$ also for uplink.

For these reasons the Rytov variance for a plane wave in Eq. (C14) can be used as a measure of the scintillation (in the weak fluctuation regime) and, most importantly, as a parameter to check if the condition of weak turbulence is indeed satisfied, corresponding to $\sigma^2_{\text{Rytov}} < 1$. As we can see from Fig. 15, the value of the Rytov variance quickly saturates within the atmosphere and its values are below unity for zenith angles within 1 radiant. It is easy to check that the Rytov variance exceeds 1 for larger zenith angles; for instance, at $h = 20$ km, we have that $\sigma^2_{\text{Rytov}} > 1$ for $\theta \gtrsim 1.2$, i.e., beyond 69°. One can also check that, if we assume not typical but worst-case day-time parameters for the H-V model (i.e., high-wind conditions, see Appendix C 2), the Rytov variance tends to values that are below the unity at the zenith ($\simeq 0.6$), but quickly violate the unity for increasing zenith angle, e.g., $\simeq 2$ already at $\theta = 1$.

4. Coherence length

Once we have clarified the working regime of weak turbulence, we introduce the spherical-wave coherence length ρ_0, which directly enters in the explicit expressions of the spot sizes of Eq. (C1). This is related to the well known Fried's parameter r_{F} [62,73], that can be written as $r_{\text{F}} = 2.088\rho_0$ [33], and describes the transverse spatial separation at the receiver over which the field phase correlations decay by $1/e$. At the optical frequencies, typical values of ρ_0 or r_{F} are in cm. When this value is particularly large, e.g., of the order of meters, then the effects of turbulence are completely negligible from the point of view of the receiver. In this regard, we will see a stark difference between uplink and downlink.

For wavenumber k and propagation distance z, the spherical-wave coherence length is given by ([28], Eq. (38))

$$\rho_0 = [1.46k^2I_0(z)]^{-3/5}, \tag{C18}$$

$$I_0(z) := \int_0^z d\xi\left(1-\frac{\xi}{z}\right)^{5/3}C_n^2(\xi), \tag{C19}$$

where the explicit functional dependence of $C_n^2(\xi)$ needs to be specified and depends on the type of propagation. For free-space propagation at a fixed altitude, the value of C_n^2 is constant and we have the simple form

$$\rho_0^{\text{fix}} = \left(0.548k^2C_n^2z\right)^{-3/5}. \tag{C20}$$

For uplink communications where the altitude h increases with the beam propagation, we assume the H-$V_{5/7}$ model for $C_n^2(h)$ and we write ρ_0 in terms of the slant distance z and the zenith angle θ, by replacing $I_0(z)$ with the following integral:

$$I_0^{\text{up}}(z,\theta) := \int_0^z d\xi\left(1-\frac{\xi}{z}\right)^{5/3}C_n^2[h(\xi,\theta)], \tag{C21}$$

where $h(z,\theta)$ is given in Eq. (A1). For downlink, the altitude decreases with the propagation. This is accounted by replacing $\xi \to z - \xi$ in the structure constant, so we replace $I_0(z)$ with the following integral:

$$I_0^{\text{down}}(z,\theta) := \int_0^z d\xi\left(1-\frac{\xi}{z}\right)^{5/3}C_n^2[h(z-\xi,\theta)]. \tag{C22}$$

In downlink, the term $(1-\xi/z)^{5/3}$ goes to zero in the region where C_n^2 has the higher values (close to the ground). For this reason, the downlink coherence length ρ_0^{down} becomes large very quickly, for any object beyond the tropopause ($\simeq$ 20 km). For instance, consider an object at the slant distance of $z = 100$ km sending down a beam with wavelength $\lambda =$ 800 nm. We compute $\rho_0^{\text{down}} \simeq 1.8$m at the zenith (compared to the uplink value $\rho_0^{\text{up}} \simeq 4.2$ cm) and $\rho_0^{\text{down}} \simeq 68$ cm at $\theta = 1$ (compared to $\simeq 2.9$ cm in uplink). At $\lambda = 1\,\mu$m, we compute $\rho_0^{\text{down}} \simeq 2.4$ m at the zenith, and $\rho_0^{\text{down}} \simeq 0.9$ m at $\theta = 1$. Note that these values increase both in distance z and wavelength. In particular, one has $\rho_0 \propto \lambda^{6/5}$.

It is clear that, within 1 radiant from the zenith (weak scintillation regime), the effect of the atmospheric turbulence is practically negligible in downlink paths. More precisely, this is true as long as the receiver's aperture a_R does not become too large (e.g., of the order of 2 meters). In fact, recall that the number of turbulence-induced short-term speckles from a point source is of the order of $N_s = 1 + (a_R/\rho_0)^2$ [32]. Assuming $a_R = 40$ cm and an object at altitude $h = 100$ km communicating at $\lambda = 800$ nm, we compute $N_s \simeq 1.05$ at the zenith and $\simeq 1.35$ at $\theta = 1$ radiant. These values are very close to the perfect coherent limit ($N_s = 1$).

Then, consider an increased aperture $a_R = 1$ m and a satellite in the LEO region, so that $h \geqslant 160$ km, we compute $N_s \lesssim 1.11$ at the zenith and $\lesssim 1.82$ at $\theta = 1$ radiant. In particular, for a satellite at $h = 530$ km (as the one studied in the main text), we get $N_s \lesssim 1.01$ at the zenith and $\lesssim 1.07$ at $\theta = 1$ radiant. For these reasons, turbulence-induced beam spreading and wandering are negligible in downlink. This means that long- and short-term spot sizes are both equal to the diffraction-limited spot size, i.e., we can set $w_{\rm lt} \simeq w_{\rm st} \simeq w_d$.

For uplink the situation is completely different, and turbulence effects cannot be neglected even at the zenith position. Before proceeding further, it is important to note some simplifications which can be enforced for zenith angles $\theta \lesssim 1$ (that are useful for the spot sizes in uplink discussed in the next section). First of all, we may simplify the expression of the slant distance as in Eq. (C10) and write

$$\rho_0^{\rm up} \simeq \left[1.46k^2 \sec\theta \int_0^h d\xi \left(1 - \frac{\xi}{h}\right)^{5/3} C_n^2(\xi)\right]^{-3/5}. \quad \text{(C23)}$$

Then, we observe that, for $\theta \lesssim 1$, any satellite slant distance z is much larger than the thickness of the atmosphere (20 − 37 km). As a result, the term $(1 - \xi/z)^{5/3}$ in Eq. (C23) is $\simeq 1$ for all values of ξ falling in the atmosphere, where the quantity C_n^2 is non-negligible.

For this reason, we can approximate the spherical-wave coherence length $\rho_0^{\rm up}$ with a plane-wave coherence length ([28], Eq. (51)), which is given by

$$\rho_p^{\rm up} = [1.46k^2 I_p(z,\theta)]^{-3/5}, \quad \text{(C24)}$$

$$I_p(z,\theta) = \int_0^z d\xi C_n^2[h(\xi,\theta)] \quad \text{(C25)}$$

$$\simeq \sec\theta \int_0^h d\xi C_n^2(\xi). \quad \text{(C26)}$$

This planar approximation is numerically investigated in Fig. 16, where we see how $\rho_0^{\rm up}$ rapidly approaches $\rho_p^{\rm up}$ already in the LEO region. These coherence lengths are computed using the exact integrals in Eqs. (C21) and (C25). The secant approximations in Eqs. (C23) and (C26) provide curves that are very close to those based on the exact integrals. As a matter of fact, they practically overlap with them at the zenith position. (Note that, while Fig. 16 is plotted for the night-time H-V model, an equivalent behavior is found for the day-time H-V model, but with different asymptotic values).

It is therefore clear that we can set $\rho_0^{\rm up} \simeq \rho_p^{\rm up}$ and use the integral in Eq. (C26). We can further simplify the formulas above by directly replacing the asymptotic value of the

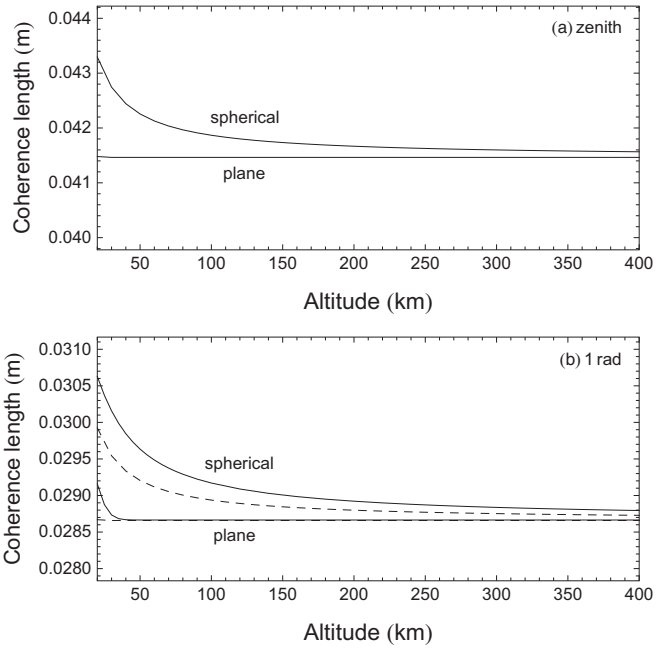

FIG. 16. Coherence length (m) versus altitude h (km) for uplink communication with a collimated Gaussian beam at $\lambda = 800$ nm. Turbulence is modelled by H-$V_{5/7}$. We compare the spherical-wave coherence length $\rho_0^{\rm up}$ (upper curve) and its plane-wave approximation $\rho_p^{\rm up}$ (lower curve). In (a), we consider the zenith position, while in (b) we consider $\theta = 1$. In both panels, the solid curves are computed with the exact integrals in Eqs. (C21) and (C25). The dashed curves are associated with the secant approximations in Eqs. (C23) and (C26). The latter are not shown in (a) because they overlap with the solid curves. Note that $\rho_0^{\rm up}$ rapidly converges to $\rho_p^{\rm up}$, and the asymptotic (lower bound) value in Eq. (C27) is approximately achieved already in the LEO region, i.e., for $h \geqslant h_{\rm LEO} = 160$ km.

coherence lengths. In other words, we may extend the integral in Eq. (C26) to infinity, and write

$$\rho_0^{\rm up} \simeq \rho_p^{\rm up} \simeq \left[1.46k^2(\sec\theta) I_\infty\right]^{-3/5}, \quad \text{(C27)}$$

$$I_\infty := \int_0^\infty d\xi C_n^2(\xi). \quad \text{(C28)}$$

Assuming the H-$V_{5/7}$ model of atmosphere ($A = 1.7 \times 10^{-14}\,{\rm m}^{-2/3}$ and $v = 21$ m/s), particularly appropriate for night-time operation, we compute $I_\infty \simeq 2.2354 \times 10^{-12}\,{\rm m}^{1/3}$, leading to

$$\rho_0^{\rm up} \simeq \rho_p^{\rm up} \simeq 8.59 \times 10^5 \lambda^{6/5} (\sec\theta)^{-3/5}, \quad \text{(C29)}$$

which is an excellent approximation for any slant distance $z \geqslant h_{\rm LEO} = 160$km and zenith angle $\theta \lesssim 1$. For the day-time H-V model ($A = 2.75 \times 10^{-14}\,{\rm m}^{-2/3}$ and $v = 21$ m/s), we compute the different value $I_\infty \simeq 3.2854 \times 10^{-12}\,{\rm m}^{1/3}$, so the approximation in Eq. (C29) holds with a different prefactor.

5. Spot sizes for uplink

Consider a Gaussian beam with wavelength λ, spot size w_0 and curvature radius R_0, which freely propagates in uplink for a distance z with a zenith angle $\theta \lesssim 1$, so that we are in the regime of weak turbulence. In particular, we may assume

a collimated beam ($R_0 = +\infty$), even though this assumption is not necessary for the following theory. The associated spherical-wave coherence length $\rho_0^{\rm up}$ is based on the integral in Eq. (C21) which can be closely approximated by Eq. (C27).

We now impose Yura's condition [28,34]

$$0.33\left(\frac{\rho_0^{\rm up}}{w_0}\right)^{\frac{1}{3}} \ll 1. \tag{C30}$$

Using Eq. (C29), it is easy to show that Eq. (C30) is implied by $w_0^{1/3} \gg 31\lambda^{2/5}$, which is compatible with typical satellite communications. For instance, at $\lambda = 800$ nm, it means to considering spot sizes $w_0 \gg 1.4$ mm. Furthermore, the condition in Eq. (C30) could also be imposed more weakly as $\rho_0^{\rm up}/w_0 < 1$, in which case the resulting expressions (discussed below) will be valid with a higher degree of approximation.

The satisfaction of Yura's condition in Eq. (C30) allows us to write the decomposition in Eq. (C1) with analytical expressions for the long- and short-term spot sizes. Specifically, we have the formulas [28,34]

$$w_{\rm lt}^2 \simeq w_d^2 + 2\left(\frac{\lambda z}{\pi \rho_0^{\rm up}}\right)^2, \tag{C31}$$

$$w_{\rm st}^2 \simeq w_d^2 + 2\left(\frac{\lambda z}{\pi \rho_0^{\rm up}}\right)^2 \Psi, \tag{C32}$$

where w_d is the diffraction-limited field spot size and Ψ is given by [34]

$$\Psi = \left[1 - 0.33\left(\frac{\rho_0^{\rm up}}{w_0}\right)^{1/3}\right]^2 \simeq 1 - 0.66\left(\frac{\rho_0^{\rm up}}{w_0}\right)^{1/3}. \tag{C33}$$

As a consequence, the variance associated to the centroid wandering is given by [34]

$$\sigma_{\rm TB}^2 = w_{\rm lt}^2 - w_{\rm st}^2 \simeq \frac{0.1337\lambda^2 z^2}{w_0^{1/3}\left(\rho_0^{\rm up}\right)^{5/3}}. \tag{C34}$$

Note that the expressions in Eqs. (C31) and (C32) are derived from Ref. ([34], Eqs. (16)–(18)) and Ref. ([28], Eq. (37)), changing their notation from intensity spot size ($w_{\rm int}$) to field spot size ($w = \sqrt{2} w_{\rm int}$). See also Refs. [74–77] for related derivations.

The formulas above undergo a great simplification by explicitly accounting for the asymptotic expression of the coherence length $\rho_0^{\rm up}$ given in Eq. (C27). Thus, for uplink satellite communications with zenith angle $\theta \lesssim 1$, we may write the following approximations:

$$w_{\rm lt}^2 \simeq w_d^2 + a\lambda^{-2/5} z^2 (\sec\theta)^{6/5}, \tag{C35}$$

$$\Psi \simeq 1 - b w_0^{-1/3} (\lambda^2 \cos\theta)^{1/5}, \tag{C36}$$

$$\sigma_{\rm TB}^2 \simeq c w_0^{-1/3} z^2 \sec\theta, \tag{C37}$$

where we set $a = 26.28 I_\infty^{6/5}$, $b = 0.2934 I_\infty^{-1/5}$ and $c = ab \simeq 7.71 I_\infty$, whose numerical values depend on the specific atmospheric profile (e.g., for the H-V$_{5/7}$ model, they become $a \simeq 2.75 \times 10^{-13}$, $b \simeq 63$, and $c \simeq 1.72 \times 10^{-11}$). Then, for the short-term spot size, we may write the following simple expression:

$$w_{\rm st}^2 = w_{\rm lt}^2 - \sigma_{\rm TB}^2 \simeq w_d^2 + z^2 \Delta(\theta), \tag{C38}$$

$$\Delta(\theta) := a\lambda^{-2/5} (\sec\theta)^{6/5} - c w_0^{-1/3} \sec\theta. \tag{C39}$$

By using the geometric expression of the slant distance $z = z(h, \theta)$ from Eq. (A4) in Eqs. (C35), (C37), and (C38), we can study the behavior of the spot sizes and that of the centroid wandering as a function of the altitude h and zenith angles $\theta \lesssim 1$. For a typical optical frequency, it is easy to see that their values practically coincide with those that can be computed from Eqs. (C31), (C32), and (C34), while providing much simpler analytical expressions.

For uplink communication with a collimated beam with $w_0 = 20$ cm and $\lambda = 800$ nm, we perform a numerical study in Fig. 17. Here we note that the short-term spot size $w_{\rm st}$ becomes considerably larger than the diffraction-limited spot size w_d, and the standard deviation of the centroid wandering $\sigma_{\rm TB}$ increases from about $0.5 - 1$ m at the Kármán line to about 200–300 m at the GEO altitude ($\simeq 36\,000$ km), depending on the value of the zenith angle.

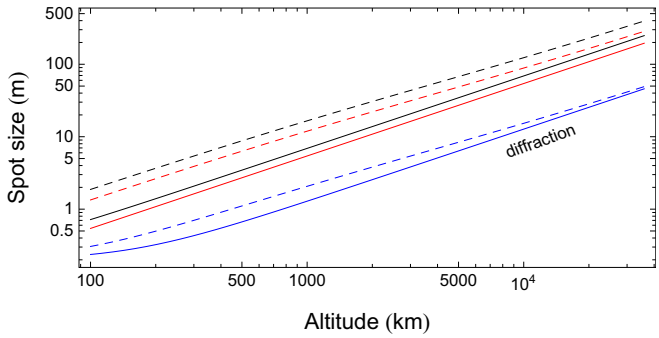

FIG. 17. Spot sizes (m) versus altitude h (km) for uplink communication by means of a collimated Gaussian beam with $\lambda = 800$ nm and $w_0 = 20$ cm. Here, turbulence is described by the H-V$_{5/7}$ model (night time). At the zenith position, we plot the short-term spot size $w_{\rm st}$ (black solid) and the standard deviation of the centroid wandering $\sigma_{\rm TB}$ (red solid), to be compared with the diffraction-limited spot size w_d (blue solid). Dashed lines refer to a zenith angle of $\theta = 1$.

APPENDIX D: BACKGROUND NOISE IN SATELLITE COMMUNICATIONS

Let us discuss the basic theoretical models which describe the background noise affecting satellite communications. With good approximation, both the Moon and the Earth can be considered to be Lambertian disks [78,79]. This means that the scattering from their surfaces can be approximated to be uniform (radiance independent from the angle), which in turn implies that the intensity detected by the satellite's receiver strictly depends on its angular field of view $\Omega_{\rm fov}$.

First consider uplink. In day-time operation, the main source of noise comes from the sunlight directly reflected by the Earth towards the satellite. The total amount depends on the solar spectral irradiance $H_\lambda^{\rm Sun}$ at the relevant wavelength λ and the albedo of the Earth ($A_{\rm E} \simeq 0.3$). During night-time operation, the noise is mainly due to the sunlight reflected

by the Moon towards the Earth, and then from the Earth towards the satellite. Therefore this noise also depends on the albedo of the Moon ($A_{\rm M} \simeq 0.12$), the radius of the Moon ($R_{\rm M} \simeq 1.737 \times 10^6$ m), and the average Earth-Moon distance ($d_{\rm EM} \simeq 3.84 \times 10^8$ m).

Considering these parameters, the mean number of environmental thermal photons impinging on the satellite's receiver with aperture a_R and (solid) angular field of view $\Omega_{\rm fov}$, within the time window Δt and the spectral filter $\Delta\lambda$, is given by [80] $\bar{n}_B^{\rm up} = \kappa H_\lambda^{\rm sun} \Gamma_R$. Here the parameter $\Gamma_R = \Delta\lambda \Delta t \Omega_{\rm fov} a_R^2$ only depends on the specific features of the receiver, while the dimensionless factor κ is equal to $\kappa_{\rm day} = A_{\rm E} \simeq 0.3$ for day-time and to $\kappa_{\rm night} = A_{\rm E} A_{\rm M} R_{\rm M}^2 d_{\rm EM}^{-2} \simeq 7.36 \times 10^{-7}$ for full-Moon night time (roughly 10^{-6} of the day-time value).

At the optical regime, the typical values of $\bar{n}_B^{\rm up}$ are orders of magnitude higher than the photon numbers due to the black-body thermal radiation emitted by the Earth. Recall that the spectral radiance of a black body at temperature T and wavelength λ is given by

$$N(\lambda, T) = 2c\lambda^{-4}[e^{hc/(\lambda k_{\rm B} T)} - 1]^{-1}, \tag{D1}$$

in terms of number of photons per unit area, time, wavelength, and solid angle (photons $\mathrm{m}^{-2}\,\mathrm{s}^{-1}\,\mathrm{nm}^{-1}\,\mathrm{sr}^{-1}$). In the formula above, it is understood that c is the speed of light and $k_{\rm B}$ is the Boltzmann constant. Therefore the total number of photons impinging on the receiver is given by $\bar{n}_{\rm body}^{\rm up} = N(\lambda, T)\Gamma_R$. Considering the optical wavelength $\lambda = 800$ nm and assuming the average surface temperature of the Earth ($T \simeq 288$ K), one has $N(\lambda, T) \simeq 3 \times 10^6$ photons $\mathrm{m}^{-2}\,\mathrm{s}^{-1}\,\mathrm{nm}^{-1}\,\mathrm{sr}^{-1}$. For a receiver with $\Gamma_R = 1.6 \times 10^{-19}\,\mathrm{m}^2$ s nm sr, we compute $\bar{n}_{\rm body}^{\rm up} \simeq 4.8 \times 10^{-13}$ mean photons, which is clearly negligible with respect to the values of $\bar{n}_B^{\rm up}$ given in Table I of the main text.

In downlink, the transmitter is the satellite and the receiver is a ground station with aperture a_R and angular field of view $\Omega_{\rm fov}$. In this case, the number of environmental photons reaching the receiver within the time window Δt and the spectral filter $\Delta\lambda$ is given by [23,81] $\bar{n}_B^{\rm down} = H_\lambda^{\rm sky} \Gamma_R$, where $H_\lambda^{\rm sky} := \pi \tilde{H}_\lambda^{\rm sky}/(\hbar\omega)$ and $\tilde{H}_\lambda^{\rm sky}$ is the background spectral irradiance of the sky in units $\mathrm{W}\,\mathrm{m}^{-2}\,\mathrm{nm}^{-1}\,\mathrm{sr}^{-1}$. In these units, its value ranges between 1.5×10^{-6} (full-Moon clear night) to 1.5×10^{-3} (clear day time) and 1.5×10^{-1} (cloudy day time) ([81], Table 1), assuming that the field of view of the receiver does not include the Moon or the Sun [82,83]. At $\lambda = 800$ nm, we have $\pi/(\hbar\omega) \simeq 1.27 \times 10^{19}\ \mathrm{W}^{-1}\ \mathrm{s}^{-1}$ sr, which means that $H_\lambda^{\rm sky}$ ranges between 1.9×10^{13} and 1.9×10^{18} photons $\mathrm{m}^{-2}\ \mathrm{s}^{-1}\ \mathrm{nm}^{-1}\ \mathrm{sr}^{-1}$. Using the same parameters for the receiver as above ($\Gamma_R = 1.6 \times 10^{-19}\,\mathrm{m}^2$ s nm sr), we find that $\bar{n}_B^{\rm down}$ ranges between $\simeq 3 \times 10^{-6}$ and $\simeq 0.3$ mean photons, which are the values for downlink reported in Table I of the main text.

Let us conclude by noticing that these estimates for the background thermal noise can be made more precise by employing dedicated programs. For instance, a more detailed calculation of sky brightness can be achieved by using software such as MODTRAN [84], LIBRADTRAN [85,86], or 6SV [87].

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[2] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Experimental Satellite Quantum Communications, Phys. Rev. Lett. **115**, 040502 (2015).

[3] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).

[4] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120**, 030501 (2018).

[5] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, Satellite-based entanglement distribution over 1200 kilometers, Science **356**, 1140 (2017).

[6] J. Yin, Y. Cao, Y. H. Li, J. G. Ren, S. K. Liao, L. Zhang, W. Q. Cai, W. Y. Liu, B. Li, H. Dai *et al.*, Satellite-to-Ground Entanglement-Based Quantum Key Distribution, Phys. Rev. Lett. **119**, 200501 (2017).

[7] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, *et al.*, Entanglement-based secure quantum cryptography over 1, 120 kilometres, Nature (London) **582**, 501 (2020).

[8] J. G. Ren, P. Xu, H. L. Yong, L. Zhang, S. K. Liao, J. Yin, W. Y. Liu, W. Q. Cai, M. Yang, L. Li *et al.*, Ground-to-satellite quantum teleportation, Nature (London) **549**, 70 (2017).

[9] S. K. Liao, J. Lin, J. G. Ren, W. Y. Liu, J. Qiang, J. Yin, Y. Li, Q. Shen, L. Zhang, X. F. Liang *et al.*, Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab, Chin. Phys. Lett. **34**, 090302 (2017).

[10] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Satellite-to ground quantum-limited communication using a 50-kgclass microsatellite, Nat. Photon. **11**, 502 (2017).

[11] A. Villar, A. Lohrmann, X. Bai, T. Vergoossen, R. Bedington, C. Perumangatt, H. Y. Lim, T. Islam, A. Reezwana, Z. Tang, *et al.*, Entanglement demonstration on board a nano-satellite, Optica **7**, 734 (2020).

[12] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[13] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and Reverse Secret-Key Capacities of a Quantum Channel, Phys. Rev. Lett. **102**, 050503 (2009).

[14] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Res. **3**, 013279 (2021).

[15] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[16] S. Pirandola, End-to-end capacities of a quantum communication network, Commun. Phys. **2**, 51 (2019).

[17] O. Svelto, *Principles of Lasers*, 5th ed. (Springer, New York 2010).

[18] L. C. Andrews, W. B. Miller, and J. C. Ricklin, Geometrical representation of Gaussian beams propagating through complex paraxial optical systems, Appl. Opt. **32**, 5918 (1993).

[19] M. Born and E. Wolf, *Principles of Optics* (Cambridge University Press, Cambridge, 2013).

[20] A. Siegman, *Lasers* (University Science Books, Sausalito, California, 1986).

[21] C. F. Bohren and D. R. Huffman, *Absorption and Scattering of Light by Small Particles* (John Wiley & Sons, Inc., New York, 2008).

[22] D. Vasylyev, W. Vogel, and F. Moll, Satellite-mediated quantum atmospheric links, Phys. Rev. A **99**, 053830 (2019).

[23] C. Liorni, H. Kampermann, and D. Bruß, Satellite-based links for quantum key distribution: beam effects and weather dependence, New J. Phys. **21**, 093055 (2019).

[24] R. Esposito, Power Scintillations Due to the Wandering of the. Laser Beam, Proc. IEEE **55**, 1533 (1967).

[25] D. Fried, Statistics of laser beam fade induced by pointing jitter, App. Opt. **12**, 422 (1973).

[26] P. Titterton, Power reduction and fluctuations caused by narrow laser beam motion in the far field, Appl. Opt. **12**, 423 (1973).

[27] D. Yu. Vasylyev, A. A. Semenov, W. Vogel, Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality, Phys. Rev. Lett. **108**, 220501 (2012).

[28] R. L. Fante, Electromagnetic beam propagation in turbulent media, Proc. IEEE **63**, 1669 (1975).

[29] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, New J. Phys. **15**, 023006 (2013).

[30] R. E. Hufnagel and N. R. Stanley, Modulation transfer function associated with image transmission through turbulent media, J. Opt. Soc. Am. **54**, 52 (1964).

[31] G. C. Valley, Isoplanatic degradation of tilt correction and short-term imaging systems, Appl. Opt. **19**, 574 (1980).

[32] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Medium*, 2nd ed. (SPIE, Bellinghan, 2005).

[33] R. L. Fante, Electromagnetic beam propagation in turbulent media: An update, Proc. IEEE **68**, 1424 (1980).

[34] H. Yura, Short term average optical-beam spread in a turbulent medium, J. Opt. Soc. Am. **63**, 567 (1973).

[35] J. Dowling and P. Livington, Behavior of focused beams in atmospheric turbulence: Measurements and comments on the theory, J. Opt. Soc. Am. **63**, 846 (1973).

[36] M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, K. E. Stoltenberg, J. F. Morris, M. Bareian, M. A. Harris, D. W. Oesch, M. D. Oliker, M. B. Flanagan, B. T. Kay, J. D. Schiller, and R. N. Lanning, Adaptive-optics-enabled daytime field experiment for satellite-earth quantum networking, arXiv:2006.07745.

[37] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection, Phys. Rev. X **5**, 041009 (2015).

[38] S. Pirandola, S. L. Braunstein, S. Lloyd, Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography, Phys. Rev. Lett. **101**, 200504 (2008).

[39] Note that, under the hypothesis that the environmental noise is assumed to be trusted, then Eqs. (47) and (50) do not apply. In that case, the optimal QKD rate is still bounded by the pure-loss bound in Eq. (35).

[40] It is understood that we refer to an "extended" quantum channel which includes imperfections of the transmitter (pointing error $\sigma_{\rm P}^2$) and the receiver (quantum efficiency $\eta_{\rm eff}$). By assuming an optimal value for these setup parameters ($\sigma_{\rm P}^2 = 0$ and $\eta_{\rm eff} = 1$), one retrieves the bounds/capacity that are associated with the "external" quantum channel (accounting for diffraction, extinction and turbulence).

[41] L. Ruppert, C. Peuntinger, B. Heim, K. Günthner, V. C. Usenko, D. Elser, G. Leuchs, R. Filip, and C. Marquardt, Fading channel estimation for free-space continuous-variable secure quantum communication, New J. Phys. **21**, 123036 (2019).

[42] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[43] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography Without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[44] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[45] Y.-C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[46] From an operational point of view, the parties may approximately reach the one-radiant rate by applying a de-fading procedure which maps all their data points (collected along the slice) into the threshold transmissivity $\eta_{\rm th}$ associated with the angle $\theta = 1$.

[47] At reasonably high values of the clock, just a small percentage of the pulses needs to be employed for the pilots. Indeed, for a 10-MHz clock, we have 10^7 pulses per second. Assume that 1% of the pulses are pilots. Then, within the typical timescale associated with beam-wandering (10–100 ms), we have $10^3 - 10^4$ pilots. On average these allow the parties to create a very fine lattice in transmissivity, with a small step $\simeq 10^{-3}$–10^{-4}. Also note that the dynamics of the pilots is fast with respect to the orbital dynamics. In fact, within a timescale of 10 ms, a fast object in circular orbit at $h = 100$ km travels a zenith angle of about 8×10^{-4} rad, so that the post-selection interval Δ can be considered to be approximately constant.

[48] X. Wang, Y. Zhang, S. Yu, and H. Guo, High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code, Sci. Rep. **8**, 10543 (2018).

[49] X. Wang, Y. Zhang, S. Yu, and H. Guo, High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution, IEEE Photon. J. **10**, 7600309 (2018).

[50] Y. Zhang (private communication).

[51] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, Security Analysis of Quantum Key Distribution with Small Block Length and Its

Application to Quantum Space Communications, Phys. Rev. Lett. **126**, 100501 (2021).

[52] D. Dequal, L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, Feasibility of satellite-to-ground continuous-variable quantum key distribution, npj Quantum Inf **7**, 3 (2021).

[53] A. R. Thompson, J. M. Moran, and G. W. Swenson, Jr., *Interferometry and Synthesis in Radio Astronomy*, 3rd ed. (Springer Nature, Cham, Switzerland, 2017).

[54] V. Klyatskin and A. Kon, On the displacement of spatially bounded light beams in a turbulent medium in the Markovian random-process approximation, Radiophys. Quantum Electron. **15**, 1056 (1972).

[55] H. Kaushal, V. K. Jain, and S. Kar, *Free Space Optical Communication* (Springer, New York, 2017).

[56] D. H. Tofsted, S. G. O'Brien, and G. T. Vaucher, An atmospheric turbulence profile model for use in army war gaming applications I, Technical Report ARL-TR-3748 US Army Research Laboratory (2006).

[57] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, Free-space quantum links under diverse weather conditions, Phys. Rev. A **96**, 043856 (2017).

[58] T. W. VanZandt, J. L. Green, K. S. Gage, and W. L. Clark, Vertical profiles of refractivity turbulence structure constant: Comparison of observations by the Sunset Radar with a new theoretical model, Radio Sci. **13**, 819 (1978).

[59] E. M. Dewan, R. E. Good, R. Beland, and J. Brown, A model for C_n^2 (optical turbulence) profiles using radiosonde data, Environmental Research Papers, Report No. **1121**, PL-TR-93-2043, 1993 (unpublished).

[60] D. L. Walters and K. E. Kunkel, Atmospheric modulation transfer function for desert and mountain locations: The atmospheric effects on r_0, J. Opt. Soc. Am. **71**, 397 (1981).

[61] R. Frehlich, R. Sharman, F. Vandenberghe, W. Yu, Y. Liu, and J. Knievel, Estimates of C_n^2 from numerical weather prediction model output and comparison with thermosonde data, J. Appl. Meteor. Climatol. **49**, 1742 (2010).

[62] D. L. Fried, Limiting resolution looking down through the atmosphere, J. Opt. Soc. Am. **56**, 1380 (1966).

[63] A. K. Majumdar and J. C. Ricklin, *Free-Space Laser Communications* (Springer New York, 2008).

[64] J. W. Goodman, *Statistical Optics* (John Wiley & Sons, Inc., New York, 1985).

[65] L. C. Andrews, R. L. Phillips, and P. T. Yu, Optical scintillations and fade statistics for a satellite-communication system, Appl. Opt. **34**, 7742 (1995).

[66] P. A. Lightsey, Scintillation in ground-to-space and retroreflected laser beams, Opt. Eng. **33**, 2535 (1994).

[67] A. M. Prokhorov, F. V. Bunkin, K. S. Gochelashvily, and V. I. Shishov, Laser irradiance propagation in turbulent media, Proc. IEEE **63**, 790 (1975).

[68] L. C. Andrews, W. B. Miller, and J. C. Ricklin, Spatial coherence of a Gaussian-beam wave in weak and strong optical turbulence, J. Opt. Soc. Am. A **11**, 1653 (1994).

[69] L. C. Andrews, R. L. Phillips, and C. Y. Young, Scintillation model for a satellite communication link at large zenith angles, Opt. Eng. **39**, 3272–3280 (2000).

[70] S. M. Rytov, Diffraction of light by ultrasonic waves, Izvestiya Akademii Nauk SSSR, Seriya Fizicheskaya (Bulletin of the Academy of Sciences of the USSR, Physical Series) **2**, 223–259 (1937).

[71] A. N. Kolmogorov, The local structure of turbulence in an incompressible viscous fluid for very large Reynolds numbers, C. R. (Doki) Acad. Sci. U. S. S. R. **30**, 301–305 (1941).

[72] H. T. Yura and W. G. McKinley, Optical scintillation statistics for IR ground-to-space laser communication systems, Appl. Opt. **22**, 3353 (1983).

[73] B. Beland, *The Infrared and Electro-Optical System Handbook* (SPIE Press, Bellingham, Washington, 1993), Vol. 2.

[74] J. Poirier and D. Korff, Beam spreading in a turbulent medium, J. Opt. Soc. Am. **62**, 893 (1972).

[75] F. Bunkin and K. Gochelashvily, Spreading of a light beam in a turbulent medium, Radiophys. Quantum Electron. **13**, 811 (1970).

[76] F. Dios, J. A. Rubio, A. Rodríguez, and A. Comerón, Scintillation and beam-wander analysis in an optical ground station-satellite uplink, Appl. Opt. **43**, 3866 (2004).

[77] A. Belmonte, Feasibility study for the simulation of beam propagation: consideration of coherent lidar performance, Appl. Opt. **39**, 5426 (2000).

[78] J. H. Lambert, *Photometria, Sive de Mensura et Gradibus Luminis, Colorum et Umbrae* (Augsburg: Eberhard Klett, 1760).

[79] F. L. Pedrotti and L. S. Pedrotti, *Introduction to Optics* (Prentice Hall, 1993).

[80] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, Feasibility of satellite quantum key distribution, New J. Phys **11**, 045017 (2009).

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

[82] C. Leinert, S. Bowyer, L. K. Haikala, M. S. Hanner, M. G. Hauser, A.-C. Levasseur-Regourd, I. Mann, K. Mattila, W. T. Reach, W. Schlosser, H. J. Staude, G. N. Toller, J. L. Weiland, J. L. Weinberg, and A. N. Witt, The 1997 reference of diffuse night sky brightness, Astron. Astrophys. Suppl. Ser. **127**, 1 (1998).

[83] V. Hansen, Spectral distribution of solar radiation on clear days: A comparison between measurements and model estimates, J. Clim. Appl. Meteorol. **23**, 772 (1984).

[84] A. Berk, P. Conforti, R. Kennett, T. Perkins, F. Hawes, and J. van den Bosch, MODTRAN6: a major upgrade of the MODTRAN radiative transfer code, Proc. SPIE 9088, Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XX, 90880H (2014).

[85] B. Mayer and A. Kylling, Technical note: The libRadtran software package for radiative transfer calculations - description and examples of use, Atmos. Chem. Phys. **5**, 1855 (2005).

[86] C. Emde, R. Buras-Schnell, A. Kylling, B. Mayer, J. Gasteiger, U. Hamann, J. Kylling, B. Richter, C. Pause, T. Dowling, and L. Bugliaro. The libradtran software package for radiative transfer calculations (version 2.0.1), Geosci. Model Dev. **9**, 1647 (2016).

[87] E. F. Vermote, D. Tanré, J. L. Deuzé, M. Herman, J.-J. Morcrette, Second simulation of the satellite signal in the solar spectrum, 6S: An overview, IEEE Trans. Geosci. Remote Sens **35**, 675 (1997).