Continuous-variable measurement-device-independent quantum key distribution in free-space channels

Masoud Ghalaii [1,2] and Stefano Pirandola[2]

[1]*School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, United Kingdom*
[2]*Department of Computer Science, University of York, York YO10 5GH, United Kingdom*

The field of space communications is the realm of communication technologies where diffraction and atmospheric effects, both of which contribute to loss and noise, become overriding. The pertinent questions here are how and at which rate information (secret keys) can be securely transferred (shared) among users under such supposedly severe circumstances. In the present work we study continuous-variable quantum key distribution in a measurement-device-independent configuration over free-space optical links. We assess the turbulence regime and provide a composable finite-size key rate analysis of the protocol for such links. We study both short-range, horizontal communication links as well as slant paths to, e.g., high-altitude platform station systems.

I. INTRODUCTION

Quantum cryptography [1], one of the oldest quantum technologies, has become a prominent candidate to counteract the challenge from quantum computers [2]. In particular, quantum key distribution (QKD) has been developing at a rapid pace, with the end goal of making distant users able to share a key that must be inscrutable for an eavesdropper to learn about and that therefore can provide highly secure encryption. Key challenges for QKD systems include channel loss and noise levels in the communication systems. These are the two main impediments that affect the performance of QKD and its realization, especially over long distances [3]. Until recently, optical fibers have been the main platform to study and experiment most QKD protocols. But their secure distance over long distances is limited, mostly due to the exponential decay of transmissivity in fiber links. In general, two solutions are introduced to conquer this limitation: using quantum repeaters [4–10] or using free-space and satellite links [11–17].

The reach of current terrestrial fiber-based quantum communications systems is limited to only a few hundreds of kilometers [18], whereas we seem to stand on the verge of building global quantum communication networks, i.e., quantum internet [19,20]. As a result, recent work has seen a substantial interest in space-borne QKD and space quantum communications [17] aimed at understanding in what way free-space, high-altitude platform station (HAPS) systems and satellite links may help with current distance limitations while guaranteeing that quantum safety will be achieved. Important steps have been taken, particularly on the limits and security of one-way space quantum communications [21–25], where

it is shown that secret bits can securely be distributed over a turbulent atmosphere, whether weak or strong [26].

At another distinct branch of the QKD science, measurement-device-independent (MDI) QKD [27,28] (see also Refs. [29–33] for related experiments), stands as one of the most interesting and well-studied schemes to relax trust assumptions in typical, point-to-point QKD protocols. More precisely, in MDI QKD one does not need to assume that the detection equipment of the legitimate parties, who are going to distribute a secret key between themselves, are trusted. This is owing to the fact that a third, allegedly untrusted party performs the crucial deed of measuring such that the protocol is immune to all attacks against the measurement modules.

Recently, an experiment implemented discrete-variable MDI, using single photons, over a 19.2-km urban free-space optical (FSO) link [34]. Feasibility studies [35,36] as well as parameter optimization [37] of space-based discrete-variable MDI QKD with photons were further appeared afterwards.

Nevertheless, full security analysis of a continuous-variable (CV) MDI protocol that includes parameter estimation and finite-size effects has not yet been presented for the free-space scenario, even though this protocol has been known since 2013 [38,39]. What's more, studying MDI protocols over free-space optical links is possibly the first step toward investigating space-based quantum repeaters and/or networks. Thus, here we develop the composable security of CV MDI QKD over short FSO links, which are generally affected by diffraction, atmospheric extinction, turbulence, and point errors. Further, we investigate slant paths to mobile devices by studying HAPS systems. For all cases we consider an asymmetric configuration, where one party is sufficiently close to the measurement station, and then compute the composable key rate in the finite-size regime.

II. SYSTEM DESCRIPTION

Take Alice and Bob to be two terrestrial parties who want to share a quantum-secure key between themselves over an

FSO link. In an MDI QKD configuration [39], they would use two transmitter (Tx) stations and an intermediate receiver station (Charlie, Rx), which is assumed untrusted; see Fig. 1(a). They would send their modulated (coherent-state) signals towards the relay Rx, which performs a joint measurement on the received signals and broadcasts the outcome, γ, through a public (classical) telecommunication channel to Alice and Bob. In an *asymmetric* MDI QKD setup, the relay is located at an unequal distance from Alice and Bob stations, say it is closer to Alice. We assume a Gaussian-modulated protocol, where Alice and Bob choose their quadrature values based on two bivariate Gaussian distributions. We also make certain assumptions about the physical FSO channel between the users' and relay's stations. Such assumptions are mainly concerned with the amount of diffraction, pointing error, and atmospheric turbulence.

In the entanglement-based (EB) scheme of the protocol, as schematically shown in Fig. 1(b), Alice and Bob use two two-mode squeezed vacuum (TMSV) sources that feed Charlie's relay over the corresponding FSO links. Charlie is supposed to perform a CV Bell measurement as before and reports the measurement outcome. Although the altitude of the three stations from sea level can be different, for now we assume that they all are located on top of communication towers with the same height, such that they share a constant-pressure atmospheric turbulence layer. Accordingly, Eve's attack on the FSO links can be modeled by two TMSV states ($e_1 e_1'$ and $e_2 e_2'$), one mode of each overlapping with Alice and Bob's signals on beam splitters η_A and η_B, respectively.

In practice, various effects, including beam-spreading and fading [40], result in high signal loss, which kills the key rate of air-QKD. A crucial step in our work is then channel modeling. Here we account for diffraction and beam spreading (short and long term, depending on the detectors being fast or slow), background thermal photons, pointing errors, and beam wandering. These contribute to have a realistic estimation of the channel loss as well as channel noise. We shall do this for single-layer free-space (ground-to-ground) atmospheric paths where we use specific existing models, such as log-normal. We also examine both techniques of measuring CV states, i.e., transmitted local oscillator (TLO) and local local oscillator (LLO).

A. Path loss

The overall optical loss that can occur in a turbulent atmospheric channel can be defined in terms of the multiplication of several types of optical transmissivity,

$$\eta(z) = \eta_{\text{eff}} \eta_{\text{atm}}(z) \eta_{\text{TB}}(z), \tag{1}$$

where η_{eff} is the receiver's efficiency and η_{atm} describes the atmospheric loss, which is modeled by the Beer-Lambert equation

$$\eta_{\text{atm}}(z) = \exp[-\alpha(\lambda, h)z], \quad \alpha(\lambda, h) = \alpha_0(\lambda) e^{-h/6600}, \tag{2}$$

where h is the altitude, in meters, and $\alpha_0(\lambda)$ is the extinction factor at sea level [41,42]. The term η_{TB} is the turbulence-induced transmissivity which, depending on the strength of turbulence, can be computed by several means, as we shall discuss in this section.
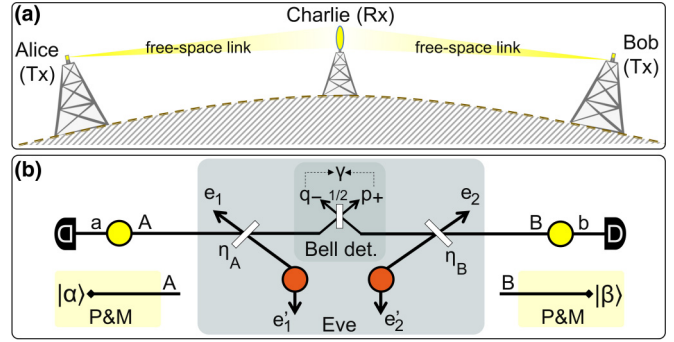

FIG. 1. Schematic of CV MDI QKD in free space. (a) Two parties, Alice and Bob, transmit encoded signals to an untrusted, intermediate party, Charlie, who jointly measures the signals. (Note that the whole setup, including the relay measurement, is assumed to be performed in free space.) (b) The entanglement-based schematic of a CV protocol with details of the sources and the middle node. Alice and Bob heterodyne one mode of their two-mode squeezed vacuum (TMSV) states, denoted by yellow circles, while subsequently sending the conjugate modes A and B (this is equivalent to the P&M scheme, where they send a Gaussian-modulated coherent states, e.g., $|\alpha\rangle$ and $|\beta\rangle$). Eve implements an attack by utilizing two TMSV states, denoted by orange circles, and interacting with carrier modes A and B. This is modeled via beam splitters of transmissivities η_A and η_B.

Let us introduce the dimensionless Rytov variance, which is defined for a plane wave as [43,44]

$$\sigma_{\text{R}}^2(z) = 1.23 C_n^2 k^{7/6} z^{11/6}, \tag{3}$$

where $k = 2\pi/\lambda$ is the wave number, and C_n^2 is known as the index-of-refraction structure constant (for a spherical wave the Rytov variance is $0.4\sigma_{\text{R}}^2$). For a multiple-layer path, e.g., a slant path from ground to space, the Rytov variance has a more complex expression. For now we restrict our links to be short and within a constant-pressure atmospheric layer, where Eq. (3) would suffice. It is well accepted that the regime of weak turbulence can be defined by the condition

$$\sigma_{\text{R}}^2(z) < 1. \tag{4}$$

In terms of free-space length z, a more lenient condition,

$$z \lesssim z_{\max} := k \min\{4a_{\text{rec}}^2, \rho_0^2(z)\}, \tag{5}$$

where a_{rec} is the receiver's aperture radius, can be used to describe the strength of the turbulence. Here

$$\rho_0(z) = \left[0.423 k^2 \int_0^z dz' C_n^2(z') \right]^{-3/5} \tag{6}$$

is the Fried's coherence length, which for a constant-pressure atmospheric layer, where C_n^2 is constant, reduces to $\rho_0(z) = (0.423 k^2 C_n^2 z)^{-3/5}$ [44, Chap. 6].

We assume a Gaussian beam with initial field spot size $w_0 = w(0)$, carrier wavelength λ, and radius of curvature F_0. At distance z of propagation, where a receiver is supposedly placed, free-space diffraction increases the beam's spot size to

$$w(z) = w_0 \sqrt{\left(1 - \frac{z}{F_0}\right)^2 + \left(\frac{z}{z_{\text{R}}}\right)^2}, \tag{7}$$

with $z_{\mathrm{R}} = \pi w_0^2 / \lambda$ being the beam's Rayleigh length [44, Chap. 4]. Practically, only a fraction of the light can be collected by the receiver, such that the pure diffraction-induced transmissivity is defined as follows:

$$\eta_{\mathrm{DIF}}(z) = 1 - \exp\left[-\frac{2a_{\mathrm{rec}}^2}{w^2(z)} \right]. \tag{8}$$

However, the presence of turbulence affects the amount of loss. For the range of distances that we consider in the present paper we do not expect strong turbulence, but wandering of the beam centroid as well as pointing errors can affect the performance. On a fast timescale the smaller turbulent eddies deflect the beam. This widens the beam size in Eq. (7) to the short-term spot size, w_{ST}. This also causes the random Gaussian wandering of the beam centroid with variance σ_{TB}^2. In addition, pointing errors from jitter and imprecise tracking could cause centroid wandering, such that the centroid quivers with total variance,

$$\sigma^2(z) = \sigma_{\mathrm{TB}}^2(z) + \sigma_{\mathrm{PE}}^2(z). \tag{9}$$

In other words, the position of the centroid can be taken as a stochastic variable with a Gaussian distribution with variance σ^2 [45]. We find that the geometric variance of the pointing error at the receiver can be approximated by

$$\sigma_{\mathrm{PE}}^2(z) = \pi \tan^2(\delta/2) z^2, \tag{10}$$

where δ, in rad, is the error at the transmitter. For small amounts of δ one can write $\sigma_{\mathrm{PE}}^2(z) \simeq (\delta z)^2$. We remark that in practice one would collectively estimate the effects of pointing and turbulence on beam wandering [46].

Figure 2 reveals that the atmospheric turbulence regime we are considering in the present study is indeed weak. Such an atmospheric regime is verified by the help of both conditions given in Eqs. (4) and (5). While at all distances considered we have $\sigma_{\mathrm{R}} < 1$, we see that $z < z_{\mathrm{max}}$ is also verified. This allows us to use Yura's set of equations.

From Yura's theory [47], under weak turbulence conditions we have that

$$w_{\mathrm{ST}}^2(z) = w^2(z) + \Sigma_{\mathrm{TB}}^2(z), \tag{11}$$

where

$$\Sigma_{\mathrm{TB}}^2(z) = 2(1 - \phi)^2 \left(\frac{\lambda z}{\pi \rho_0(z)} \right)^2 \tag{12}$$

accounts for the contribution of turbulence to beam widening. We note that Yura's formulation of weak turbulence regimes requires that $\phi(z) := 0.33(\rho_0(z)/w_0)^{1/3} \ll 1$. In the present work we consider a weak satisfaction of this condition ($\phi < 0.4$, assuming distances $z < 250$ m) so that Yura's expansion has to be considered approximate. Also, the amount of beam wandering due to turbulence is given by

$$\sigma_{\mathrm{TB}}^2(z) = \frac{0.1337 \lambda^2 z^2}{w_0^{1/3} \rho_0(z)^{5/3}}. \tag{13}$$

From the above description, one infers that atmospheric turbulence affects the beam in two ways: the first is by worsening the beam wandering, as described by Eq. (9); the second is a diffraction-type effect, as Eq. (11) suggests, that results in increasing the beam waist.
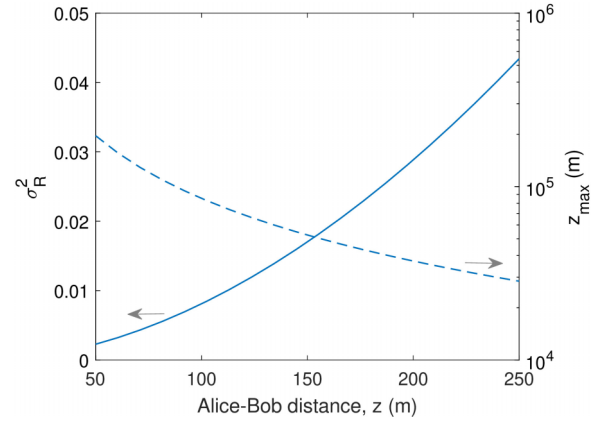

FIG. 2. Identifying the regime of turbulence. Rytov variance (σ_{R}^2, solid curve) and maximum free-space length (z_{max}, dashed curve) vs free-space distance z. For these plots we have assumed night-time conditions, with $C_n^2 = 1.28 \times 10^{-14}$ m$^{-2/3}$, wavelength $\lambda = 800$ nm, and aperture size $a_{\mathrm{rec}} = 20$ cm.

By replacing Eq. (11) in the expression for diffraction-induced transmissivity of Eq. (8), we derive

$$\eta_{\mathrm{ST}}(z) = 1 - \exp\left[-\frac{2a_{\mathrm{rec}}^2}{w_{\mathrm{ST}}^2(z)} \right]. \tag{14}$$

However, further modifications are required, e.g., the effect of deflection, which defines wandering of the beam centroid on the receiver's plane following a Gaussian distribution with variance σ^2. Deflection, with the value $r := |x_C - x_R|$, where x_C is the location of beam's centroid on the receiver plane and x_R is the aperture center of the receiver, results in an instantaneous transmissivity [48]

$$\eta_{\mathrm{ST}}(z, r) = \eta_{\mathrm{ST}}(z) \exp\left[-\left(\frac{r}{r_0} \right)^\gamma \right]. \tag{15}$$

Here we have that

$$\gamma = \frac{4\eta_{\mathrm{ST}}^{\mathrm{ff}} \Lambda_1(\eta_{\mathrm{ST}}^{\mathrm{ff}})}{1 - \Lambda_0(\eta_{\mathrm{ST}}^{\mathrm{ff}})} \left[\ln \frac{2\eta_{\mathrm{ST}}}{1 - \Lambda_0(\eta_{\mathrm{ST}}^{\mathrm{ff}})} \right]^{-1}, \tag{16}$$

$$r_0 = a_{\mathrm{rec}} \left[\ln \frac{2\eta_{\mathrm{ST}}}{1 - \Lambda_0(\eta_{\mathrm{ST}}^{\mathrm{ff}})} \right]^{-1/\gamma}, \tag{17}$$

with $\eta_{\mathrm{ST}}^{\mathrm{ff}} := 2a_{\mathrm{rec}}^2 / w_{\mathrm{ST}}^2(z)$ being the transmissivity at far field and $\Lambda_n(x) = e^{-2x} I_n(2x)$ (where I_n denotes a modified Bessel function of the first kind with order n [49, Chap. 14]). As a result, total transmissivity η becomes a function of r:

$$\eta(z, r) = \eta_{\mathrm{eff}} \eta_{\mathrm{atm}}(z) \eta_{\mathrm{ST}}(z, r). \tag{18}$$

Consequently, for any physical quantity that is a function of the total transmissivity, such as the key generation rate $K(\eta)$, we have to compute their average [21],

$$\overline{K}(z) = \int_0^{a_{\mathrm{rec}}} dr P_{\mathrm{WB}}(z, r) K(\eta(z, r)), \tag{19}$$

where the expression

$$P_{\mathrm{WB}}(z, r) = \frac{r}{\sigma^2(z)} \exp\left(-\frac{r^2}{2\sigma^2(z)} \right) \tag{20}$$

is a Weibull distribution for the deflection r and σ^2.

B. Path noise

In general, a receiver sees a total mean number of thermal photons [21],

$$\bar{n} = \eta_{\text{eff}} \bar{n}_{\text{bg}} + \bar{n}_{\text{ex}}, \tag{21}$$

where $\bar{n}_{\text{bg}}$ and $\bar{n}_{\text{ex}}$ are the number of background thermal photons per mode and extra photons generated within the receiver box, respectively. The number $\bar{n}_{\text{bg}}$ depends on several factors related to both the sky and the receiver and is given by [50,51]

$$\bar{n}_{\text{bg}} = \frac{\pi \Gamma_{\text{rec}} B_{\lambda}^{\text{sky}}}{\hbar \omega}, \tag{22}$$

where $\hbar$ is the reduced Planck constant, ω is the angular frequency of light, and B_{λ}^{sky} is the brightness of the sky in the range of 10^{-6}–$10^{-1}\,\text{W}\,\text{m}^{-2}\,\text{nm}^{-1}\,\text{sr}^{-1}$ from night to day. All traces of the receiver are given in

$$\Gamma_{\text{rec}} = \Delta\lambda \Delta t \Omega_{\text{fov}} a_{\text{rec}}^2, \tag{23}$$

where Ω_{fov}, $\Delta\lambda$, and Δt are the angular field of view, spectral filter, and time window of the detector, respectively. The nominal values that we use in the present study are $\Omega_{\text{fov}} = 10^{-10}\,\text{sr}$, $\Delta\lambda = 0.1\,\text{pm}$, and $\Delta t = 10\,\text{ns}$.

We note that the natural interferometric effect of coherent detection, where the signal and local oscillator (LO) pulse overlap, imposes an effective filter of $\Delta\lambda = \lambda^2 \Delta\nu/c$, such that assuming $\lambda = 800$ nm, a LO of $\Delta t = 10$ ns, and a bandwidth $\Delta\nu = 50 \geqslant 0.44/\Delta t$ MHz applies an effective filter of $\Delta\lambda = 0.1$ pm. This would suppress the background noise $\bar{n}_{\text{bg}}$ to the order of 10^{-12} (10^{-7}) at night (day) time. In the asymmetric configuration that we assume in the present study we assume that $\bar{n}_A = \bar{n}_{\text{ex}}$ and $\bar{n}_B = \bar{n}$, given by Eq. (21). This is because the distance from Bob to the relay covers almost all the total distance.

Continuous-variable signals, i.e., their quadratures, are measured by means of a homodyne or heterodyne detection, both of which require a reference light, the so-called local oscillator, to perform the detection. The LO can be transmitted along with the signal, hence called transmitted LO (TLO), or locally created at the receiver side, hence called local LO (LLO). The TLO and LLO schemes add different amounts of noise photons within the receiver. Those generated by LLO, $\bar{n}_{\text{LLO}}$, are a linear function of the link transmissivity, while that generated by TLO, $\bar{n}_{\text{TLO}}$, is an inverse function of transmissivity. Strictly speaking, we have [21, Eq. (62)]

$$\bar{n}_{\text{LLO}} = \mathcal{N} + \frac{\pi l_{\text{w}} V_A \eta(z)}{C} \quad \text{and} \quad \bar{n}_{\text{TLO}} = \frac{\mathcal{N}}{\eta(z)}, \tag{24}$$

where

$$\mathcal{N} = \frac{\nu_{\text{det}}(\text{NEP})^2 W \Delta t_{\text{LO}}}{2\hbar\omega P_{\text{LO}}},$$

with V_A being the modulation variance, P_{LO} the LO power, C the clock, l_{w} the linewidth, W the detector bandwidth, NEP the noise equivalent power, Δt_{LO} the LO pulse duration, and ν_{det} the detection noise variance ($\nu_{\text{det}} = 1$ and $\nu_{\text{det}} = 2$ for a homodyne and heterodyne detection, respectively).

Figure 3 shows the number of extra photons generated at a homodyne receiver. Although at long distances one expects
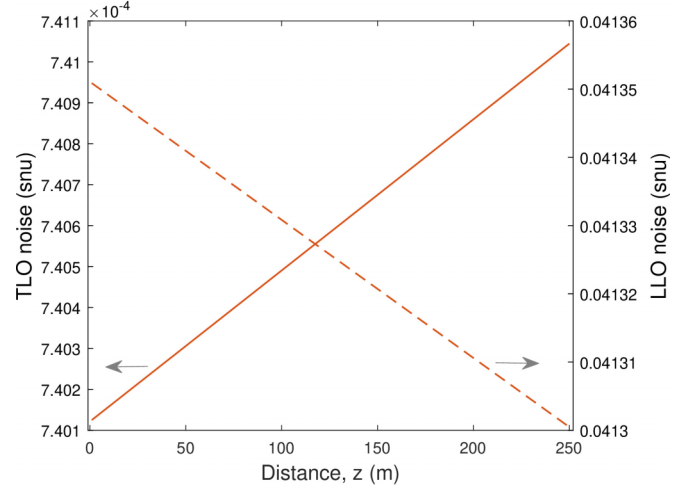

FIG. 3. Noise photons generated by a homodyne receiver. TLO noise (solid curve) and LLO noise (dashed curve) vs free-space distance z. We consider night time, with $C_n^2 = 1.28 \times 10^{-14}\,\text{m}^{-2/3}$, when a TLO and LLO scheme is used. We have $\lambda = 800$ nm, NEP $= 6\,\text{pW}/\sqrt{\text{Hz}}$, $W = 100$ MHz, $\Delta t_{\text{LO}} = 10$ ns, $P_{\text{LO}} = 100$ mW, $V_A = 44$, $l_{\text{w}} = 1.6$ kHz, $C = 5$ MHz, $H_A = H_B = 20$ m, $\alpha_0 = 5 \times 10^{-6}$, $w_0 = 10$ cm, $a_{\text{rec}} = 20$ cm, $\eta_{\text{eff}} = 0.98$, and $\hbar = 1.054 \times 10^{-34}$ J s.

that LLO results in less noise than the TLO [26], at short distances TLO introduces about two orders of magnitudes less noise. For the regime of operation we will use in this study, we assume the maximum amount of extra noise photons generated at the receiver, that is, we assume $\bar{n}_{\text{LLO}} = 0.04$ SNU.

III. SECURITY ANALYSIS

By using the outcomes of our modeling in the previous sections, we can now convey a security analysis by computing achievable key rates for an asymmetric CV MDI QKD protocol over FSO links. In the EB representation we assume that Alice and Bob hold two TMSV states with the following covariance matrices (CMs):

$$\mathbf{V}_{aA} = \begin{pmatrix} \mu_A \mathbf{I} & \sqrt{\mu_A^2 - 1}\mathbf{Z} \\ \sqrt{\mu_A^2 - 1}\mathbf{Z} & \mu_A \mathbf{I} \end{pmatrix} \tag{25}$$

and

$$\mathbf{V}_{bB} = \begin{pmatrix} \mu_B \mathbf{I} & \sqrt{\mu_B^2 - 1}\mathbf{Z} \\ \sqrt{\mu_B^2 - 1}\mathbf{Z} & \mu_B \mathbf{I} \end{pmatrix}, \tag{26}$$

where $\mu_{A(B)}$ defines Alice's (Bob's) TMSV variance. By applying heterodyne detection modules to their local modes a and b, they project the carrier modes A and B to known Gaussian-modulated coherent states $|\alpha\rangle$ and $|\beta\rangle$, respectively. In other words, Alice and Bob encode the variables $\alpha = (q_A, p_A)$ and $\beta = (q_B, p_B)$ with Gaussian distributions

$$G(\alpha) = \frac{1}{2\pi\sigma_A^2} \exp\left[-\frac{q_A^2 + p_A^2}{2\sigma_A^2}\right] \tag{27}$$

and

$$G(\beta) = \frac{1}{2\pi\sigma_B^2} \exp\left[-\frac{q_B^2 + p_B^2}{2\sigma_B^2}\right] \tag{28}$$

on the modes A and B, such that $\sigma_A^2 = \mu_A - 1$ and $\sigma_B^2 = \mu_B - 1$. In the present work we assume equal variances for Alice and Bob, i.e., $\mu_A = \mu_B = \mu$.

On their way through free space, these states experience Eve's attack, which is modeled by means of two beam splitters with transmissivities η_A and η_B. She applies a two-mode attack for each channel by interacting Alice and Bob modes with those of hers that are described by the following CM [see Fig. 1(b)] [39]:

$$\mathbf{V}_{ee'} = \begin{pmatrix} \omega_A \mathbf{I} & g_{\max} \mathbf{Z} \\ g_{\max} \mathbf{Z} & \omega_B \mathbf{I} \end{pmatrix}, \tag{29}$$

where ω_A and ω_B quantify Eve's injected thermal noise, while $g_{\max} = \max\{\sqrt{(\omega_A + 1)(\omega_B - 1)}, \sqrt{(\omega_A - 1)(\omega_B + 1)}\}$. The parameters $\omega_A = 2\bar{n}_A + \nu_{\det}$ and $\omega_B = 2\bar{n}_B + \nu_{\det}$ are total thermal noise variance at Alice-relay and Bob-relay links, respectively, with $\nu_{\det}$ being the detection noise variance ($\nu_{\det} = 1$ SNU for homodyne and $\nu_{\det} = 2$ SNU for heterodyne detection).

The execution of Charlie's Bell measurement (elaborated in Ref. [52]) gives the outcome $\gamma = q_C + ip_C$, where q_C and p_C are dependent on the variables α and β:

$$q_C = -\tau_A q_A + \tau_B q_B + x_N, \tag{30}$$

$$p_C = +\tau_A p_A + \tau_B p_B + p_N, \tag{31}$$

where $\tau_{A(B)} = \sqrt{\eta_{\mathrm{eff}}\eta_{A(B)}/2}$. The variables x_N and p_N are noise variables with variance

$$\Sigma_N^2 = \Xi + \nu_{\mathrm{el}} + 1, \tag{32}$$

which includes 1 SNU vacuum noise, electronic noise ν_{el}, and excess noise

$$\Xi = \frac{\eta_{\mathrm{eff}}}{2}[(1 - \eta_A)(\omega_A - 1) + (1 - \eta_B)(\omega_B - 1)]$$
$$+ \eta_{\mathrm{eff}} g_{\max}\sqrt{(1 - \eta_A)(1 - \eta_B)}. \tag{33}$$

It can be shown that the conditional CM for Alice and Bob is given by

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \zeta_a \mathbf{I} & \zeta_c \mathbf{Z} \\ \zeta_c \mathbf{Z} & \zeta_b \mathbf{I} \end{pmatrix}, \tag{34}$$

where

$$\begin{cases} \zeta_a = \mu_A - \frac{\eta_A(\mu_A^2 - 1)}{\eta_A(\mu_A - 1) + \eta_B(\mu_B - 1) + 2\Sigma_N^2/\eta_{\mathrm{eff}}}, \\ \zeta_b = \mu_B - \frac{\eta_B(\mu_B^2 - 1)}{\eta_A(\mu_A - 1) + \eta_B(\mu_B - 1) + 2\Sigma_N^2/\eta_{\mathrm{eff}}}, \\ \zeta_c = \frac{\sqrt{\eta_A(\mu_A^2 - 1)\eta_B(\mu_B^2 - 1)}}{\eta_A(\mu_A - 1) + \eta_B(\mu_B - 1) + 2\Sigma_N^2/\eta_{\mathrm{eff}}}. \end{cases} \tag{35}$$

In addition, a heterodyne detection at Bob's side, with the outcome $\tilde{\beta}$, gives the conditional CM at Alice's side:

$$\mathbf{V}_{a|\gamma\tilde{\beta}} = \left(\zeta_a - \frac{\zeta_c^2}{\zeta_b + 1}\right)\mathbf{I}. \tag{36}$$

The secret key rate at the asymptotic limit is then given by [39]

$$K_\infty(\eta_A, \eta_B, \Xi) = \beta I_{AB}(\eta_A, \eta_B, \Xi) - \chi_E(\eta_A, \eta_B, \Xi), \tag{37}$$

where β is the reconciliation efficiency,

$$I_{AB}(\eta_A, \eta_B, \Xi) = \frac{1}{2}\log_2 \frac{1 + \det \mathbf{V}_{a|\gamma} + \mathrm{tr}\mathbf{V}_{a|\gamma}}{1 + \det \mathbf{V}_{a|\gamma\tilde{\beta}} + \mathrm{tr}\mathbf{V}_{a|\gamma\tilde{\beta}}} \tag{38}$$

is mutual information, and

$$\chi_E(\eta_A, \eta_B, \Xi) = g(\nu_+) + g(\nu_-) - g(\nu_c) \tag{39}$$

is Holevo information, with $\nu_\pm$ being eigenvalues of the CM $\mathbf{V}_{ab|\gamma}$ and ν_c being the eigenvalue of the conditional CM $\mathbf{V}_{b|\gamma\tilde{\alpha}}$, and we define

$$g(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{40}$$

The stochastic nature of free-space channels causes fluctuations that result in free-space fading. Hence, the transmissivities, as well as the level of noise, become unstable and vary with time over certain timescales such that the probability distribution for the deflected transmissivity is [21]

$$P_0(\tau) = \frac{r_0^2}{\gamma\sigma^2\tau}\left(\ln\frac{\eta}{\tau}\right)^{2/\gamma - 1}\exp\left[-\frac{r_0^2}{2\sigma^2}\left(\ln\frac{\eta}{\tau}\right)^{2/\gamma}\right], \tag{41}$$

where γ and r_0 are given in Eqs. (16) and (17), respectively, and the mean value of deflection is assumed to be zero. Thus estimated parameters and the key rate would take different values than that given in Eq. (37). The details of such an issue were introduced in Refs. [21,23] for one-way CV QKD protocols. Also, as a possible solution, the pilot pulses were introduced. In the following we explain how one can use the pilot solution, presented in Refs. [21,23], in the case of free-space CV MDI QKD protocols.

Pilot pulses are relatively intense pulses that help to track and measure or estimate the instantaneous transmissivity. The pilots are weak enough to be measured via LO signals but much brighter than quantum signals to provide a good estimate of the transmissivity. In fact, they help to collect signals within a lattice of suitable time bins with almost equal transmissivity. Therefore, in a free-space scenario, apart from m_{PE} samples that are sacrificed for parameter estimation (PE), m_{PL} of the signals are energetic pilot signals that are used to estimate the instantaneous transmissivity, such that $N = n + (m_{\mathrm{PE}} + m_{\mathrm{PL}})$, where n will be consumed for building the raw key.

For our MDI QKD setup, let us assume that both Alice and Bob send coherent-state pilots $|\bar{n}_{\mathrm{PL}}\rangle$ towards the relay, which treats pilots as normal quantum signals, i.e., it outcomes γ_{PL}. This would allow Alice and Bob to build the estimators for the instantaneous transmissivities $\tau_{A(B)} = \sqrt{\eta_{\mathrm{eff}}\eta_{A(B)}/2}$. In a fading interval $[\tau, \tau + \delta\tau]$, a fraction of the pilots $p_\delta m_{\mathrm{PL}}$, where

$$p_\delta := \int_\tau^{\tau+\delta\tau} P_0(\tau)d\tau, \tag{42}$$

can be used for estimating τ_A and τ_B. From the pilots the number of $p_\delta m_{PL} \nu_{det}$ outcome pairs $(q_{C,i}, p_{C,i})$ of the relay, i.e.,

$$q_{C,i} = -\tau_A q_{A,i} + \tau_B q_{B,i} + x_{N,i}, \qquad (43)$$

$$p_{C,i} = +\tau_A p_{A,i} + \tau_B p_{B,i} + p_{N,i}, \qquad (44)$$

where $q_{A,i} = p_{A,i} = q_{B,i} = p_{B,i} = \sqrt{2\bar{n}_{PL}}$, can be derived. Alice and Bob can then build the estimators

$$\hat{T}_{A,PL} := \frac{1}{p_\delta m_{PL} \nu_{det}} \sum_i \frac{-q_{C,i} + p_{C,i}}{2\sqrt{2\bar{n}_{PL}}}, \qquad (45)$$

$$\hat{T}_{B,PL} := \frac{1}{p_\delta m_{PL} \nu_{det}} \sum_i \frac{q_{C,i} + p_{C,i}}{2\sqrt{2\bar{n}_{PL}}}, \qquad (46)$$

with mean τ_A and τ_B, respectively, and variance $\sigma_N^2/(8 p_\delta m_{PL} \nu_{det} \bar{n}_{PL})$. It can be argued that real-time tracking of the transmissivities is possible with negligible error for a sufficiently large $\bar{n}_{PL}$, even if m_{PL} is small.

While it is possible to introduce postselection intervals $[\tau_{A,min}, \tau_{A,max}]$ and $[\tau_{B,min}, \tau_{B,max}]$, the parties can choose the minimum achievable values $\tau_{A,min}$ and $\tau_{B,min}$ to wipe out the fading and build a stable link. Following Refs. [21,23], we take $\tau_{B,min} = f_{th}\eta_B$, where f_{th} is a fixed postselection threshold. At the same time, for a very asymmetric MDI protocol, one can assume that $\tau_{A,min} = \eta_A$. These values can also modify associated noise values given in Eq. (24), as well as the excess noise given in Eq. (33). Therefore the secret key rate at the asymptotic limit in Eq. (37) will be given by $K_\infty(\eta_{A,min}, \eta_{B,min}, \Xi_{max})$.

To deliver a more rigorous account of the key rate analysis, in the following we compute the composable finite-size key rate analysis by also presenting the PE step. We assume that Alice and Bob use m_{PE} samples for PE. Accepting an error ϵ_{PE}, which is the error probability associated with each estimator, one can provide the following worst-case scenario values for the transmissivities and the excess noise (here, for convenience, we drop the "min" and "max" subscripts from the transmissivities and the noise) [52]:

$$\tilde{\eta}_A = \eta_A - w\sqrt{\sigma_{\eta_A}^2}, \qquad (47)$$

$$\tilde{\eta}_B = \eta_B - w\sqrt{\sigma_{\eta_B}^2}, \qquad (48)$$

$$\tilde{\Xi} = \Xi + w\sqrt{\sigma_N^2}, \qquad (49)$$

where $w = \sqrt{2}\,\text{erf}^{-1}(1 - \epsilon_{PE})$, $\Xi = \Sigma_N^2 - \nu_{el} - 1$, and

$$\sigma_{\eta_A}^2 \simeq \frac{16\eta_A}{m_{PE}} \left[\eta_A + \frac{\eta_B \sigma_B^2}{2\sigma_A^2} \right] \left\{ 1 + \frac{\Sigma_N^2/\eta_{eff}}{\eta_A \sigma_A^2 + \eta_B \sigma_B^2/2} \right\}, \qquad (50)$$

$$\sigma_{\eta_B}^2 \simeq \frac{16\eta_B}{m_{PE}} \left[\eta_B + \frac{\eta_A \sigma_A^2}{2\sigma_B^2} \right] \left\{ 1 + \frac{\Sigma_N^2/\eta_{eff}}{\eta_B \sigma_B^2 + \eta_A \sigma_A^2/2} \right\}, \qquad (51)$$

$$\sigma_N^2 \simeq \frac{2(\Sigma_N^2)^2}{m_{PE}}. \qquad (52)$$

Thus the worst-case, minimum secret key rate based on the PE scheme is given by

$$K_{PE}(\tilde{\eta}_A, \tilde{\eta}_B, \tilde{\Xi}) = \beta I_{AB}(\tilde{\eta}_A, \tilde{\eta}_B, \tilde{\Xi}) - \chi_E(\tilde{\eta}_A, \tilde{\eta}_B, \tilde{\Xi}). \qquad (53)$$

What's more, the key rate must be composably secure [1], including imperfections in the data processing [53]. Assuming that the free-space link is used N times, the composable finite size is given by [21]

$$K(z, r) = \frac{n p_{EC}}{N} \left(K_{PE}(\tilde{\eta}_A, \tilde{\eta}_B, \tilde{\Xi}) - \frac{\Delta_{AEP}}{\sqrt{n}} + \frac{\Theta}{n} \right), \qquad (54)$$

where [21,23]

$$\Delta_{AEP} := 4\log_2(\sqrt{d} + 2)\sqrt{\log_2 \left(18 p_{EC}^{-2} \epsilon_s^{-4} \right)}, \qquad (55)$$

$$\Theta := \log_2 \left[p_{EC} \left(1 - \frac{\epsilon_s^2}{3} \right) \right] + 2\log_2(\sqrt{2}\epsilon_H). \qquad (56)$$

Equation (54) gives the rate for a protocol with overall security parameter $\epsilon = \epsilon_c + \epsilon_s + \epsilon_H + 3 p_{EC}\epsilon_{PE}$. Assuming reverse reconciliation, the hash comparison step of the finite-key analysis requires Bob to send $\lceil \rceil \log_2(1 - \epsilon_c)$ bits to Alice for proper values of ϵ_c (called ϵ_c correctness) and bounds the probability that Alice's and Bob's sequences differ even if their hashes match. Also, ϵ_H and ϵ_s describe errors that occur during the hashing and the smoothing stages, respectively. It is also convenient to define the frame error rate $\text{FER} = 1 - p_{EC}$. Further, it is assumed that by using an analog-to-digital conversion each continuous-variable symbol is encoded with d bits of precision. We remark that since the transmissivities are dependent on the deflection parameter r, such that the rate in Eq. (54) is a function of r, one needs to use the integral in Eq. (19) to compute an average rate.

Figure 4 partly reveals the performance of CV MDI QKD in a free-space setup. Here, we assume a horizontal path between Alice and Bob, both located at $H_A = H_B = 20$ m. We refer to the caption for the nominal (reasonably realistic) parameters that we have used. As we discussed under Fig. 2, here we can use Yura's weak turbulence theory. However, let us emphasis that Yura's condition ($\phi \ll 1$) has to be considered approximate as we consider a weak satisfaction of it, i.e., at all distances considered in Fig. 4 we have that $\phi < 0.4$.

In Fig. 4(a) we plot the average rate versus distance at fixed block size $N = 5 \times 10^8$ by assuming the postselection threshold $f_{th} = 0.9$ to build a stable channel. It is interesting to see that, similar to the one-way CV QKD protocol studied in, e.g., Ref. [21], one can extract a secure key string with relatively high generation rate. Indeed, one could obtain higher rates with a higher value of postselection threshold. This is shown in Fig. 4(b), where in order to see the effect of block size, too, we plot the average rate versus block size at a fixed distance $z = 100$ m. It is observed that smaller values of postselection threshold would result in very poor performance of the system, or it requires a very high, impractical block size. For instance, with the same set of parameters given in Fig. 4, the protocol is incapable of delivering a positive rate at $f_{th} = 0.85$. Nevertheless, as one can imagine, there are several parameters involved in this problem that, considering the realization of the protocol, can be opted and/or tuned to result in a positive rate, even higher than presented here. In particular, as one would expect, we have observed that both the transmitter and receiver telescopes' size effect the final rate greatly.
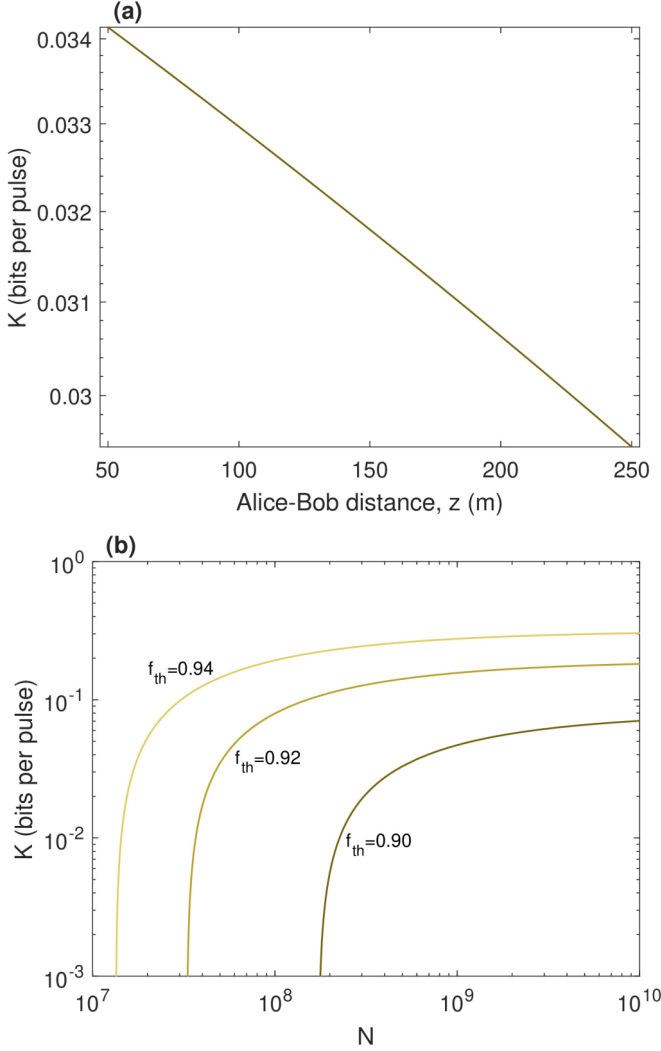
FIG. 4. Free-space CV MDI QKD performance. (a) Secret key rate vs total distance at $N = 5 \times 10^8$ and $f_{th} = 0.9$. (b) Secret key rate vs block size at $z = 100$ m. Set of parameters used: $w_0 = 10$ cm, $a_{rec} = 20$ cm, $\beta = 0.98$, $\mu_A = \mu_B = 45$, $\eta_A = 0.98$, $\eta_{eff} = 0.98$, $\nu_{el} = 0.01$, $\nu_{det} = 1$, $\alpha_0 = 5 \times 10^{-6}$, $C_n^2 = 1.28 \times 10^{-14}$, $\bar{n}_{bg} = 4.8 \times 10^{-12}$, $\delta = 10 \, \mu$m, and $\bar{n}_{ex} = 0.04$. Other parameters related to pilots and parameter estimation are $m_{PL} = 0.1N$, $m_{PE} = 0.1N$, $d = 2^6$, FER $= 0.1$, $\varepsilon_s = \varepsilon_h = \varepsilon_{pe} = 10^{-10}$, $w = 6.34$, and $\varepsilon = 4.5 \times 10^{-10}$. Note that realistic block sizes are up to 10^8 with current data processing facilities.

For the above numerical analysis, we assumed a highly asymmetric configuration CV MDI QKD setup where we have considered the relay literally placed at Alice's laboratory to let the Bob relay link, covering the total distance. The reason is that, whether in the fiber-based or free-space case, CV MDI protocols offer a reasonable key rate mostly in such regimes.

IV. SLANT PATHS

It is conceivable that either of the stations of Alice and Bob is located at a higher altitude than the other, e.g., on top of a mountain. Furthermore, they can be moving objects such as HAPSs. In either case we face a slanted atmospheric path between Alice and Bob. Supposedly, in such scenarios, the

beam light propagates through different atmospheric layers; hence, a more elaborate consideration may be required. For instance, we note that the index-of-refraction structure C_n^2 is no longer constant and changes with the altitude.

To begin with, let us assume a slant path between a HAPS, say Bob's station at altitude H_B and Alice's platform on the ground, located at $H_A < H_B$ above sea level. The length of the path is given by

$$
\begin{aligned}
z = & \sqrt{(R_E + H_B)^2 + (R_E + H_A)^2(\cos^2\theta - 1)} \\
& - (R_E + H_A)\cos\theta,
\end{aligned}
\tag{57}
$$

where $R_E \simeq 6371$ km is the earth's radius and θ the zenith angle. As the first consideration, in the following we try to identify the regime of turbulence that is determinant of the choice of equations to be used.

A more general, altitude-dependent expression for the scintillation index, to be used instead of the Rytov variance, is [44,54]

$$
\begin{aligned}
\sigma_{SI}^2(\theta, H_B) = & -1 + \exp\left[\frac{0.49\beta_R^2(\theta, H_B)}{\left(1 + 1.11\beta_R^{12/5}(\theta, H_B)\right)^{7/6}}\right. \\
& \left. + \frac{0.51\beta_R^2(\theta, H_B)}{\left(1 + 0.69\beta_R^{12/5}(\theta, H_B)\right)^{5/6}}\right],
\end{aligned}
\tag{58}
$$

where

$$
\beta_R^2(\theta, H_B) = 2.25k^{7/6}\sec^{11/6}(\theta)\int_{H_A}^{H_B} dh \, (h - H_A)^{5/6}C_n^2(h),
$$

and a downlink path is (from Bob to Alice) assumed. According to the Hufnagel-Valley (H-V) atmospheric model [44, Sec. 12.2], the index-of-refraction structure is a function of the altitude h and the wind speed v,

$$
\begin{aligned}
C_n^2(h) = & \, 5.94 \times 10^{-53}(v/27)^2 h^{10} e^{-h/1000} \\
& + 2.7 \times 10^{-16} e^{-h/1500} + A e^{-h/100},
\end{aligned}
\tag{59}
$$

where A is the nominal value of $C_n^2(0)$ at the ground.

From Fig. 5 it is seen that the regime of turbulence can be assumed weak. Here we have considered low wind, $v = 21$ ms^{-1}, and night time with $A = 1.7 \times 10^{-14}$ m$^{-2/3}$ [22,44]. Consequently, in such slant-path regimes, we can still make use of the Yura's recipe for a weak turbulent atmosphere. Let us now get back to our CV MDI QKD protocol and apply the above considerations to the analysis.

The performance of CV MDI QKD with slant paths can be seen in Fig. 6, where for several values of zenith angle we have plotted a composable finite-size key rate at night-time operation. Here we have set the same parameters as given in Fig. 4, including initial beam size $w_0 = 10$ cm, receiver size $a_{rec} = 20$ cm, block size $N = 5 \times 10^8$, and pilot postselection threshold $f_{th} = 0.9$. Our simulation illustrates that with a reasonable block size and receiver size, quantum communications through CV MDI protocols is feasible for altitudes up to $H_B = 200$ m (note that Alice's altitude is fixed at $H_A = 20$ m).
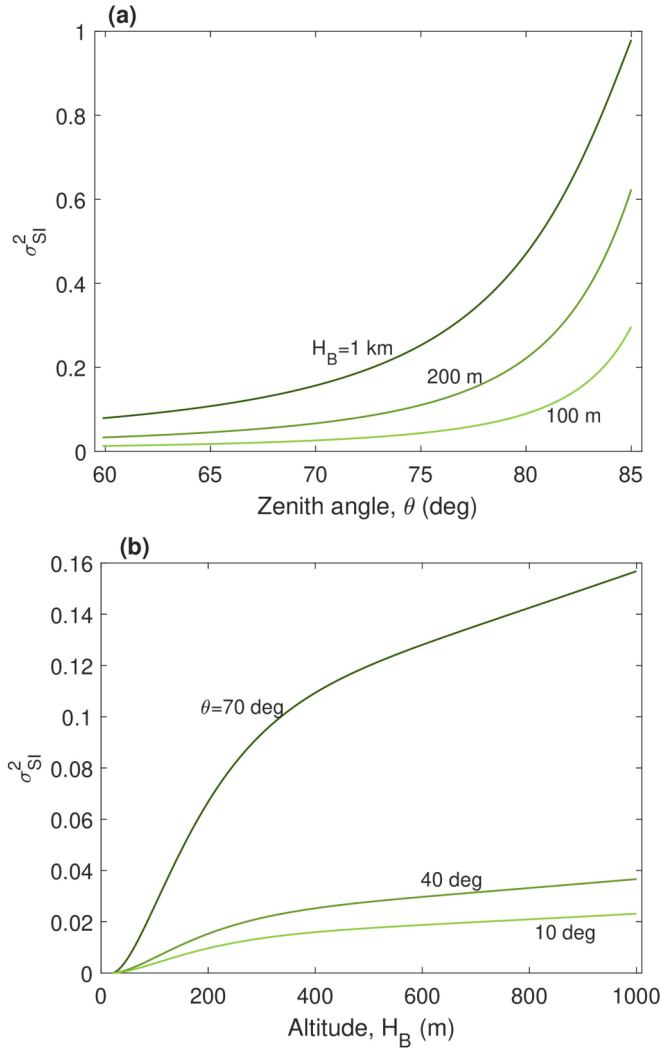
FIG. 5. High-altitude platform systems. (a) Scintillation index vs the zenith angle at different altitudes of Bob's station. (b) Scintillation index vs Bob's altitude at different zenith angles. We assume a fixed of $H_A = 20$ m for Alice's station.
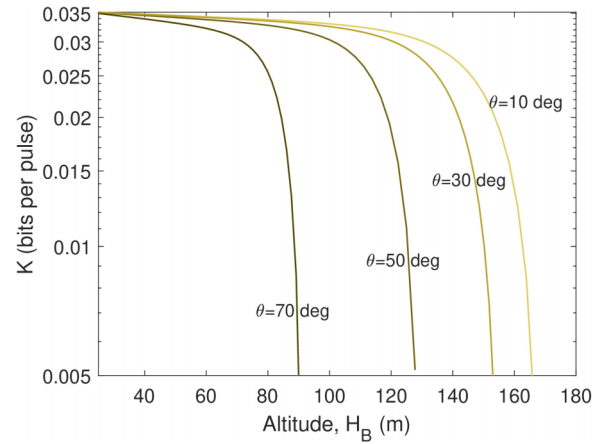

FIG. 6. Free-space CV MDI QKD performance with high-altitude platform systems. Secret key rate vs Bob's altitude at different zenith angles with $H_A = 20$ m at all cases. The curves represent the rate at $f_{th} = 0.9$, and the set of parameters used here are the same as reported in Fig. 4, except for the index-of-refraction structure C_n^2, which varies.

several types of noise and experimental inefficiencies. We have demonstrated that asymmetric CV MDI QKD protocols can be used to extract a composably-secure key over FSO links. This can be achieved in the powerful collective eavesdropping scenario with the protocol offering substantially high rates. We have considered physical space-related phenomena such as light-beam diffraction, deflection, turbulence, and beam widening, all of which degrade transmissivity. We have also accounted for several types of noise, including background noise, excess noise, and receiver noise, that free-space CV QKD suffers from. Furthermore, we have studied the usefulness of the protocol for a slant path through an atmospheric turbulent space. In all cases we show that high-rate CV MDI QKD is possible over short FSO links of the order of hundreds of meters, where the regime of turbulence is weak.

V. SUMMARY

In the present work we have developed a composable security analysis of CV MDI QKD over FSO links that can include

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. 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] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

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

[4] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, Phys. Rev. Lett. **81**, 5932 (1998).

[5] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification, Phys. Rev. A **59**, 169 (1999).

[6] W. Dür, H.-J. Briegel, P. Zoller, and P. v. Loock, Quantum repeater, in *Quantum Information* (John Wiley & Sons, Ltd., 2016), Chap. 30, pp. 691–700.

[7] F. Furrer and W. J. Munro, Repeaters for continuous-variable quantum communication, Phys. Rev. A **98**, 032335 (2018).

[8] J. Dias, M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, Quantum repeater for continuous-variable entanglement distribution, Phys. Rev. A **102**, 052425 (2020).

[9] K. P. Seshadreesan, H. Krovi, and S. Guha, Continuous-variable quantum repeater based on quantum scissors and mode multiplexing, Phys. Rev. Res. **2**, 013310 (2020).

[10] M. Ghalaii and S. Pirandola, Capacity-approaching quantum repeaters for quantum communications, Phys. Rev. A **102**, 062412 (2020).

[11] 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, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).

[12] 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, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He *et al.*, Ground-to-satellite quantum teleportation, Nature (London) **549**, 70 (2017).

[13] 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, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia *et al.*, Satellite-based entanglement distribution over 1200 kilometers, Science **356**, 1140 (2017).

[14] R. Bedington, X. Bai, E. Truong-Cao, Y. C. Tan, K. Durak, A. V. Zafra, J. A. Grieve, D. K. Oi, and A. Ling, Nanosatellite experiments to enable future space-based QKD missions, EPJ Quantum Technology **3**, 12 (2016).

[15] 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).

[16] L. Mazzarella, C. Lowe, D. Lowndes, S. K. Joshi, S. Greenland, D. McNeil, C. Mercury, M. Macdonald, J. Rarity, and D. K. L. Oi, QUARC: Quantum research cubesat—A constellation for quantum communication, Cryptography **4**, 7 (2020).

[17] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone, P. Villoresi, A. Ling, T. Jennewein, M. Mohageg, J. G. Rarity, I. Fuentes, S. Pirandola, and D. K. L. Oi, Advances in space quantum communications, IET Quant. Commun. **2**, 182 (2021).

[18] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Large scale quantum key distribution: Challenges and solutions, Opt. Express **26**, 24260 (2018).

[19] H. J. Kimble, The quantum internet, Nature (London) **453**, 1023 (2008).

[20] S. Pirandola and S. L. Braunstein, Unite to build the quantum internet, Nature (London) **532**, 169 (2016).

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

[22] S. Pirandola, Satellite quantum communications: Fundamental bounds and practical security, Phys. Rev. Res. **3**, 023130 (2021).

[23] S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks, Phys. Rev. Res. **3**, 043014 (2021).

[24] I. Derkach and V. C. Usenko, Applicability of squeezed- and coherent-state continuous-variable quantum key distribution over satellite links, Entropy **23**, 55 (2021).

[25] N. Hosseinidehaj, M. S. Winnel, and T. C. Ralph, Simple and loss-tolerant free-space quantum key distribution using a squeezed laser, Phys. Rev. A **105**, 032602 (2022).

[26] M. Ghalaii and S. Pirandola, Quantum communications in a moderate-to-strong turbulent space, Commun. Phys. **5**, 38 (2022).

[27] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[28] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[29] A. A. E. Hajomer, U. L. Andersen, and T. Gehring, Real-world data encryption with continuous-variable measurement device-independent quantum key distribution, arXiv:2303.01611.

[30] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks, Phys. Rev. Lett. **111**, 130501 (2013).

[31] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum key distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[32] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (2013).

[33] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution, Phys. Rev. Lett. **112**, 190503 (2014).

[34] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, W.-Y. Liu, X. Jiang, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, C.-Y. Lu, X.-B. Wang *et al.*, Long-distance free-space measurement-device-independent quantum key distribution, Phys. Rev. Lett. **125**, 260503 (2020).

[35] X. Wang, C. Dong, S. Zhao, Y. Liu, X. Liu, and H. Zhu, Feasibility of space-based measurement-device-independent quantum key distribution, New J. Phys. **23**, 045001 (2021).

[36] X. Wang, W. Liu, T. Wu, C. Guo, Y. Zhang, S. Zhao, and C. Dong, Free space measurement device independent quantum key distribution with modulating retro-reflectors under correlated turbulent channel, Entropy **23**, 1299 (2021).

[37] Q. Dong, G. Huang, W. Cui, and R. Jiao, Parameter optimization in satellite-based measurement-device-independent quantum key distribution, Quantum Sci. Technol. **7**, 015014 (2022).

[38] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, and S. L. Braunstein, Continuous-variable quantum cryptography with untrusted relays, arXiv:1312.4104v1.

[39] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photonics **9**, 397 (2015).

[40] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, Entanglement of Gaussian

states and the applicability to quantum key distribution over fading channels, New J. Phys. **14**, 093048 (2012).

[41] S. Q. Duntley, The reduction of apparent contrast by the atmosphere, J. Opt. Soc. Am. **38**, 179 (1948).

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

[43] 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 (1937).

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

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

[46] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics, npj Quantum Inf. **7**, 93 (2021).

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

[48] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, Toward global quantum communication: Beam wandering preserves nonclassicality, Phys. Rev. Lett. **108**, 220501 (2012).

[49] G. B. Arfken, H. J. Weber, and F. E. Harris, *Mathematical Methods for Physicists*, 7th ed. (Elsevier, Waltham, MA, 2013).

[50] M. Er-long, H. Zheng-fu, G. Shun-sheng, Z. Tao, D. Dasheng, and G. Guang-can, Background noise of satellite-to-ground quantum key distribution, New J. Phys. **7**, 215 (2005).

[51] 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).

[52] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables, Phys. Rev. A **96**, 042332 (2017).

[53] P. Papanastasiou, A. G. Mountogiannakis, and S. Pirandola, Composable security of CV-MDI-QKD with secret key rate and data processing, Sci. Rep. **13**, 11636 (2023).

[54] 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 (2000).