UNIVERSITY of York

This is a repository copy of *Continuous-Variable Measurement-Device-Independent Quantum Key Distribution in Free-Space Channels*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/204661/

Version: Accepted Version

Article:
Ghalaii, Masoud and Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2023) Continuous-Variable Measurement-Device-Independent Quantum Key Distribution in Free-Space Channels. Physical Review A. 042621. ISSN 1094-1622

https://doi.org/10.1103/PhysRevA.108.042621

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

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/

arXiv:2212.06687v1 [quant-ph] 13 Dec 2022

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 (CV) quantum key distribution (QKD) in a measurement-device-independent (MDI) configuration over free-space optical (FSO) links. We assess the turbulence regime and provide a composable finite-size key rate analysis of the protocol for FSO links. We study both short-range, horizontal communication links as well as slant paths to, e.g., high-altitude platform station (HAPS) 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 fibre-based quantum communication 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 spaceborne 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, in particular on the limits and security of one-way space quantum communications [21–23], where it is shown that secret bits can securely be distributed over a turbulent atmosphere, whether weak or strong [24].

At another distinct branch of the QKD science, measurement-device-independent (MDI) QKD [25, 26] (see also Refs. [27–29] 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 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. What's more, studying MDI protocols over free-space optical (FSO) links is possibly the first step toward investigating space-based quantum repeaters/networks. Recently, an experiment implemented discrete-variable MDI, using single photons, over a 19.2 km urban FSO link [30]. Feasibility studies [31, 32] as well as parameter optimization [33] of space-based discrete-variable MDI QKD with photons were further appeared afterwards.

Nevertheless, a full security analysis of 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 is known since 2013 [34, 35]. 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 the asymmetric configuration where one party is sufficiently close to the MDI station and we 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 FSO links. In an MDI configuration [35], they would use two transmitter (Tx) stations and an intermediate receiver station (Charlie, Rx), which is assumed untrusted; see Fig. 1a. They send their modulated coherent-state signals towards the relay Rx, which performs a joint measurement on the received signals and broadcasts the outcome to Alice and Bob. In an *asymmetric* MDI 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, as well as atmospheric turbulence.

In the entanglement-based (EB) scheme of the protocol, as schematically shown in Fig. 1b, Alice and Bob use two two-mode squeezed vacuum (TMSV) sources that feed Charlie's relay over the FSO links. Charlie is supposed to perform a CV Bell measurement and reports the measurement outcome, γ, through a public (classical) telecommunication channel. 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. In practice, various effects, including beam-spreading and fading, result in high signal loss which kills the key rate of air-QKD.

A crucial step in our work is channel modelling. Here we account for diffraction and beam spreading (short/long-term depending on the detectors being fast/slow), background thermal photons, pointing errors and beam wandering. These contribute to have a realistic estimation of the channel loss and channel noise. Accordingly, Eve's attack on the FSO links can be modelled by two TMSV states (e_1e_1' and e_2e_2'), one mode of each overlapping with Alice and Bob's signals on beam splitters η_A and η_B, respectively. 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

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

where $\eta_{\rm eff}$ is the receiver's efficiency and $\eta_{\rm atm}$ describes the atmospheric loss, which is modelled by the Beer-Lambert equation

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

where h is the altitude, in metres, and $\alpha_0(\lambda)$ is the extinction factor at sea level [36, 37]. The term $\eta_{\rm TB}$ 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.

Let us introduce the dimensionless Rytov variance, which is defined for a plane wave as [38, 39]

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

where $k = 2\pi/\lambda$ is the wavenumber and C_n^2 is known as the index-of-refraction structure constant (for a spherical wave the Rytov variance is $0.4\sigma_{\rm R}^2$). For a multiple-layer path, e.g., a slant path form 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

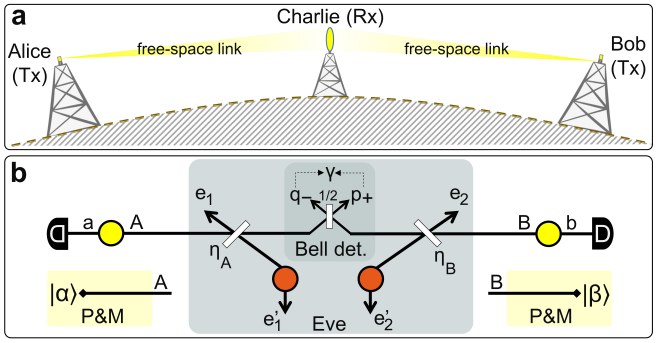

FIG. 1. **Schematic of MDI QKD in free space. a,** Two parties, Alice and Bob, transmit encoded signals to an untrusted, intermediate party, Charlie, who jointly measures the signals. **b,** The entanglement-based schematic of a continuous-variable protocol with details of the sources and the middle 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.

Eq. (3) would suffice. It is well accepted that the regime of weak turbulence can be defined by the condition

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

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

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

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

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

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

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

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

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

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

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, $w_{\rm ST}$. This also causes the random Gaussian wandering of the beam centroid with variance $\sigma^2_{\rm TB}$. In addition, pointing errors from jitter and imprecise tracking could cause centroid wandering, such that the centroid quivers with total variance

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

In other words, the position of the centroid can be taken as a stochastic variable with a Gaussian distribution with variance σ^2 [40]. The geometric variance of the pointing error at the receiver can be approximated by

$$\sigma^2_{\rm PE}(z) = \pi \tan^2(\delta/2) z^2, \tag{10}$$

where δ, in rad, is the error at the transmitter. For small amounts of δ one can write $\sigma^2_{\rm PE}(z) \simeq (\delta z)^2$. We remark that in practice one would collectively estimate the effects of pointing and turbulence on beam wandering [41].

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 $\sigma_{\rm R} < 1$ we see that $z < z_{\rm max}$ is also verified. This allows us to use Yura's set of equations.

From Yura's theory [42], under weak turbulence conditions we have that

$$w^2_{\rm ST}(z) = w^2(z) + \Sigma^2_{\rm TB}(z), \tag{11}$$

where

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

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 ($\phi < 0.4$) so that Yura's expansion has to be considered approximate. Also, the amount of beam wandering due to turbulence is given by

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

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.

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

$$\eta_{\rm ST}(z) = 1 - \exp\left[-\frac{2a^2_{\rm rec}}{w^2_{\rm ST}(z)}\right]. \tag{14}$$

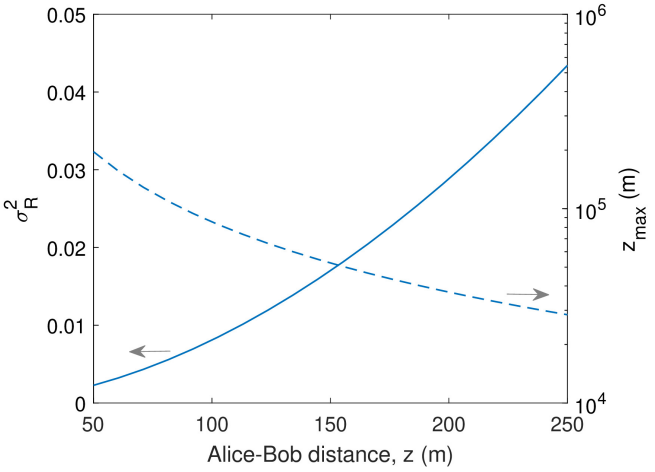

FIG. 2. **Identifying the regime of turbulence.** For the plots we have assumed night-time conditions, with $C_n^2 = 1.28 \times 10^{-14}$ m$^{-2/3}$, wavelength $\lambda = 800$ nm, and aperture size $a_{\rm rec} = 20$ cm.

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 [43]

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

Here, we have that

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

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

with $\eta^{\rm ff}_{\rm ST} := 2a^2_{\rm rec}/w^2_{\rm ST}(z)$ being the transmissivity at far field and $\Lambda_n(x) = e^{-2x} I_n(2x)$ (I_n denotes a modified Bessel function of the first kind with order n [44, Chap. 14]).

As a result, total transmissivity η becomes a function of r

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

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

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

where the expression

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

is a Weibull distribution for the deflection r and σ^2 [21].

B. Path noise

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

$$\overline{n} = \eta_{\rm eff}\overline{n}_{\rm bg} + \overline{n}_{\rm ex}, \tag{21}$$

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

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

where $\hbar$ is the reduced Planck constant, ω is the angular frequency of light, and $B_{\lambda}^{\rm sky}$ is the brightness of the sky in the range of 10^{-6} – 10^{-1} $\rm Wm^{-2}nm^{-1}sr^{-1}$ from night to day [45, 46]. All traces of the receiver are given in

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

where $\Omega_{\rm fov}$, $\Delta\lambda$, and Δt are the angular field of view, spectral filter, and time window of the detector, respectively. The nominal values that we use in the present study are $\Omega_{\rm fov} = 10^{-10}$ sr, $\Delta\lambda = 0.1$ pm, and $\Delta t = 10$ 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 $\Delta\nu = 50 \geq 0.44/\Delta t$ MHz, applies an effective filter of $\Delta\lambda = 0.1$ pm. This would suppress the background noise $\overline{n}_{\rm bg}$ to the order of 10^{-12} (10^{-7}) at night (day) time. In the asymmetric MDI configuration that we assume in the present study we assume that $\overline{n}_A = \overline{n}_{\rm ex}$ and $\overline{n}_B = \overline{n}$, 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 (LO), 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, $\overline{n}_{\rm LLO}$, is a linear function of the link transmissivity, while that generated by TLO, $\overline{n}_{\rm TLO}$, is an inverse function of transmissivity. Strictly speaking we have [21, Eq. (62)]

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

where

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

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

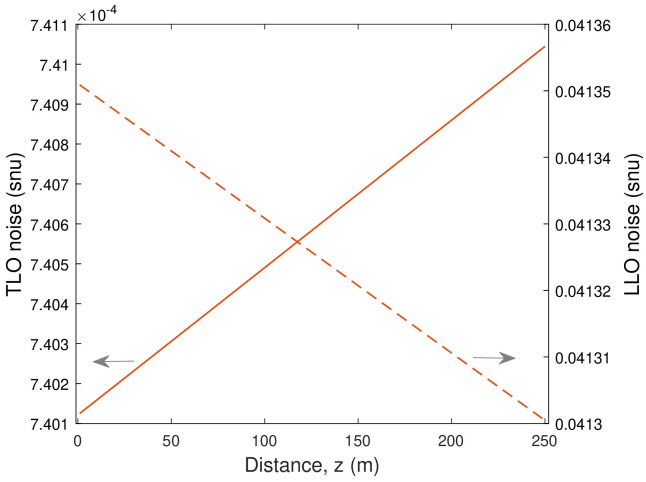

FIG. 3. **Noise photons generated by a homodyne receiver.** We consider night-time, with $C_n^2 = 1.28\times10^{-14}$ $\rm m^{-2/3}$, when a TLO and LLO scheme is used. We have $\lambda = 800$ nm NEP = 6 pW/$\sqrt{\rm Hz}$, $W = 100$ MHz, $\Delta t_{\rm LO} = 10$ ns, $P_{\rm LO} = 100$ mW, $V_A = 44$, $l_{\rm w} = 1.6$ KHz, $C = 5$ MHz, $H_A = H_B = 20$ m, $\alpha_0 = 5\times10^{-6}$, $w_0 = 10$ cm, $a_{\rm rec} = 20$ cm, $\eta_{\rm eff} = 0.98$ and $\hbar = 1.054\times10^{-34}$ Js.

Figure 3 shows the number of extra photons generated at a homodyne receiver. Although at long distances one expects that LLO results in less noise than the TLO [24], at short distances TLO introduces about 2 order 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 $\overline{n}_{\rm LLO} = 0.04$ SNU.

III. SECURITY ANALYSIS

By using the outcomes of our modelling in the previous sections we can now convey a security analysis by computing achievable key rates for an asymmetric 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 modelled 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. 1b)

$$\mathbf{V}_{ee'} = \begin{pmatrix} \omega_A \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B \mathbf{I} \end{pmatrix}, \ \mathbf{G} = \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{29}$$

where ω_A and ω_B quantify Eve's injected thermal noise while g and g' respect bona fide conditions [35]. The parameters $\omega_A = 2\overline{n}_A + \nu_{\text{det}}$ and $\omega_B = 2\overline{n}_B + \nu_{\text{det}}$ are total thermal noise variance at Alice-relay and Bob-relay links, respectively, with ν_{det} being the detection noise variance ($\nu_{\text{det}} = 1$ SNU for homodyne and $\nu_{\text{det}} = 2$ SNU for heterodyne detection). Also, one can argue that the larger $|g|$ and $|g'|$, with $|g| = |g'|$, the stronger the correlation between the modes. Then, as the worst-case scenario we can consider an attack with

$$\mathbf{G}_{\max} = \begin{pmatrix} -g_{\max} & 0 \\ 0 & g_{\max} \end{pmatrix}, \tag{30}$$

where $g_{\max} = \max\{|g|, |g|\}$.

The execution of Charlie's Bell measurement gives the outcome $\gamma = q_C + ip_C$, where q_C and p_C are dependent on the variables α and β

$$q_C = -\tau_A q_A + \tau_B q_B + x_N, \tag{31}$$

$$p_C = +\tau_A p_A + \tau_B p_B + p_N, \tag{32}$$

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

$$\Sigma_N^2 = \Xi + \nu_{\text{el}} + 1, \tag{33}$$

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

$$\Xi = \frac{\eta_{\text{eff}}}{2}\left[(1-\eta_A)(\omega_A - 1) + (1-\eta_B)(\omega_B - 1)\right] + \eta_{\text{eff}} g_{\max}\sqrt{(1-\eta_A)(1-\eta_B)}. \tag{34}$$

It can be shown that the conditional CM for Alice and Bob is given by [47]

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \zeta_a \mathbf{I} & \zeta_c \mathbf{Z} \\ \zeta_c \mathbf{Z} & \zeta_b \mathbf{I} \end{pmatrix}, \tag{35}$$

where

$$\begin{cases} \zeta_a = \mu_A - \frac{\eta_A(\mu_A^2 - 1)}{\eta_A(\mu_A - 1) + \eta_B(\mu_B - 1) + 2\Sigma_N^2/\eta_{\text{eff}}}, \\ \zeta_b = \mu_B - \frac{\eta_B(\mu_B^2 - 1)}{\eta_A(\mu_A - 1) + \eta_B(\mu_B - 1) + 2\Sigma_N^2/\eta_{\text{eff}}}, \\ \zeta_c = \frac{\sqrt{\eta_A(\mu_A^2 - 1)\eta_B(\mu_B^2 - 1)}}{\eta_A(\mu_A - 1) + \eta_B(\mu_B - 1) + 2\Sigma_N^2/\eta_{\text{eff}}}. \end{cases} \tag{36}$$

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

$$\mathbf{V}_{a|\gamma\widetilde{\beta}} = \left(\zeta_a - \frac{\zeta_c^2}{\zeta_b + 1}\right)\mathbf{I}. \tag{37}$$

The secret key rate of CV MDI QKD at the asymptotic limit is then given by

$$K_\infty(\eta_A, \eta_B, \Xi) = \beta I_{AB}(\eta_A, \eta_B, \Xi) - \chi_E(\eta_A, \eta_B, \Xi), \tag{38}$$

where β is the reconciliation efficiency,

$$I_{AB}(\eta_A, \eta_B, \Xi) = \frac{1}{2}\log_2 \frac{1 + \det \mathbf{V}_{a|\gamma} + \text{tr}\mathbf{V}_{a|\gamma}}{1 + \det \mathbf{V}_{a|\gamma\widetilde{\beta}} + \text{tr}\mathbf{V}_{a|\gamma\widetilde{\beta}}} \tag{39}$$

is mutual information, and

$$\chi_E(\eta_A, \eta_B, \Xi) = g(\nu_+) + g(\nu_-) + g(\nu_c) \tag{40}$$

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 $\mathbf{V}_{b|\gamma\widetilde{\alpha}}$, and we define

$$g(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{41}$$

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 time scales, such that the probability distribution for the deflected transmissivity is [21]

$$P_0(\tau) = \frac{r_0^2}{\gamma\sigma^2\tau}\left(\ln\frac{\eta}{\tau}\right)^{2/\gamma - 1} \exp\left[-\frac{r_0^2}{2\sigma^2}\left(\ln\frac{\eta}{\tau}\right)^{2/\gamma} \right], \tag{42}$$

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. (38). The details of such an issue was 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 in the case of free-space CV MDI QKD protocols.

Pilot pulses are relatively intense pulses that help to track and measure/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 $m_{\rm PE}$ samples that are sacrificed for parameter estimation (PE), $m_{\rm PL}$ of the signals are energetic pilot signals that are used to estimate the instantaneous transmissivity, such that $N = n + (m_{\rm PE} + m_{\rm PL})$, where n will be consumed for building the raw key.

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

$$p_\delta := \int_{\tau}^{\tau+\delta\tau} P_0(\tau) d\tau, \tag{43}$$

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

$$q_{C,i} = -\tau_A q_{A,i} + \tau_B q_{B,i} + x_{N,i}, \tag{44}$$

$$p_{C,i} = +\tau_A p_{A,i} + \tau_B p_{B,i} + p_{N,i}, \tag{45}$$

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

$$\hat{T}_{A,\rm PL} := \frac{1}{p_\delta m_{\rm PL} \nu_{\rm det}} \sum_i \frac{-q_{C,i} + p_{C,i}}{2\sqrt{2\overline{n}_{\rm PL}}}, \tag{46}$$

$$\hat{T}_{B,\rm PL} := \frac{1}{p_\delta m_{\rm PL} \nu_{\rm det}} \sum_i \frac{q_{C,i} + p_{C,i}}{2\sqrt{2\overline{n}_{\rm PL}}}, \tag{47}$$

with mean τ_A and τ_B, respectively, and variance $\sigma_N^2/(8p_\delta m_{\rm PL}\nu_{\rm det}\overline{n}_{\rm PL})$. It can be argued that real-time tracking of the transmissivities is possible with negligible error for a sufficiently large $\overline{n}_{\rm PL}$, even if $m_{\rm PL}$ 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 $\tau_{B,\min} = f_{\rm th}\eta_B$, where $f_{\rm th}$ 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. (34). Therefore, the secret key rate at the asymptotic limit in Eq. (38) 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 $m_{\rm PE}$ samples for PE. Accepting an error $\epsilon_{\rm PE}$, 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)

$$\widetilde{\eta}_A = \eta_A - w\sqrt{\sigma^2_{\eta_A}}, \tag{48}$$

$$\widetilde{\eta}_B = \eta_B - w\sqrt{\sigma^2_{\eta_B}}, \tag{49}$$

$$\widetilde{\Xi} = \Xi + w\sqrt{\sigma_N^2}, \tag{50}$$

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

$$\sigma^2_{\eta_A} \simeq \frac{16\eta_A}{m_{\rm PE}}\left[\eta_A + \frac{\eta_B\sigma_B^2}{2\sigma_A^2}\right]\left\{1 + \frac{\Sigma_N^2/\eta_{\rm eff}}{\eta_A\sigma_A^2 + \eta_B\sigma_B^2/2}\right\}, \tag{51}$$

$$\sigma^2_{\eta_B} \simeq \frac{16\eta_B}{m_{\rm PE}}\left[\eta_B + \frac{\eta_A\sigma_A^2}{2\sigma_B^2}\right]\left\{1 + \frac{\Sigma_N^2/\eta_{\rm eff}}{\eta_B\sigma_B^2 + \eta_A\sigma_A^2/2}\right\}, \tag{52}$$

$$\sigma_N^2 \simeq \frac{2(\Sigma_N^2)^2}{m_{\rm PE}}. \tag{53}$$

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

$$K_{\rm PE}(\widetilde{\eta}_A, \widetilde{\eta}_B, \widetilde{\Xi}) = \beta I_{AB}(\widetilde{\eta}_A, \widetilde{\eta}_B, \widetilde{\Xi}) - \chi_E(\widetilde{\eta}_A, \widetilde{\eta}_B, \widetilde{\Xi}). \tag{54}$$

What's more, the key rate must be composably secure [1], including imperfections in the data processing [48]. Assuming that the free-space link is used N times, the composable finite-size is given by [21]

$$K(z,r) = \frac{np_{\rm EC}}{N}\left(K_{\rm PE}(\widetilde{\eta}_A, \widetilde{\eta}_B, \widetilde{\Xi}) - \frac{\Delta_{\rm AEP}}{\sqrt{n}} + \frac{\Theta}{n}\right), \tag{55}$$

where [21, 23]

$$\Delta_{\rm AEP} := 4\log_2(\sqrt{d}+2)\sqrt{\log_2(18p_{\rm EC}^{-2}\epsilon_{\rm S}^{-4})}, \tag{56}$$

$$\Theta := \log_2\left[p_{\rm EC}(1 - \frac{\epsilon_{\rm S}^2}{3})\right] + 2\log_2(\sqrt{2}\epsilon_{\rm H}). \tag{57}$$

Equation (55) gives the rate for a protocol with overall security parameter $\epsilon = \epsilon_{\rm C} + \epsilon_{\rm S} + \epsilon_{\rm H} + 3p_{\rm EC}\epsilon_{\rm PE}$. Assuming reverse reconciliation, the hash comparison step of the finite-key analysis requires Bob to send $\lceil \log_2(1-\epsilon_{\rm C}) \rceil$ bits to Alice for proper values of $\epsilon_{\rm C}$ (called $\epsilon_{\rm C}$-correctness) and bounds the probability that Alice's and Bob's sequences differ even if their hashes match. Also, the $\epsilon_{\rm H}$ and $\epsilon_{\rm S}$ describe errors that occur during the hashing and the smoothing stages, respectively. It is also convenient to define the frame error rate $\mathrm{FER} = 1 - p_{\rm EC}$. 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. (55) 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, 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. 4a we plot the average rate versus distance at fixed block size $N = 5 \times 10^8$ by assuming postselection threshold $f_{\rm th} = 0.9$ to build a stable channel. Next, in order to see the effect of block-size, and point out the difference between different values of $f_{\rm th}$, we plot the average rate versus block size at

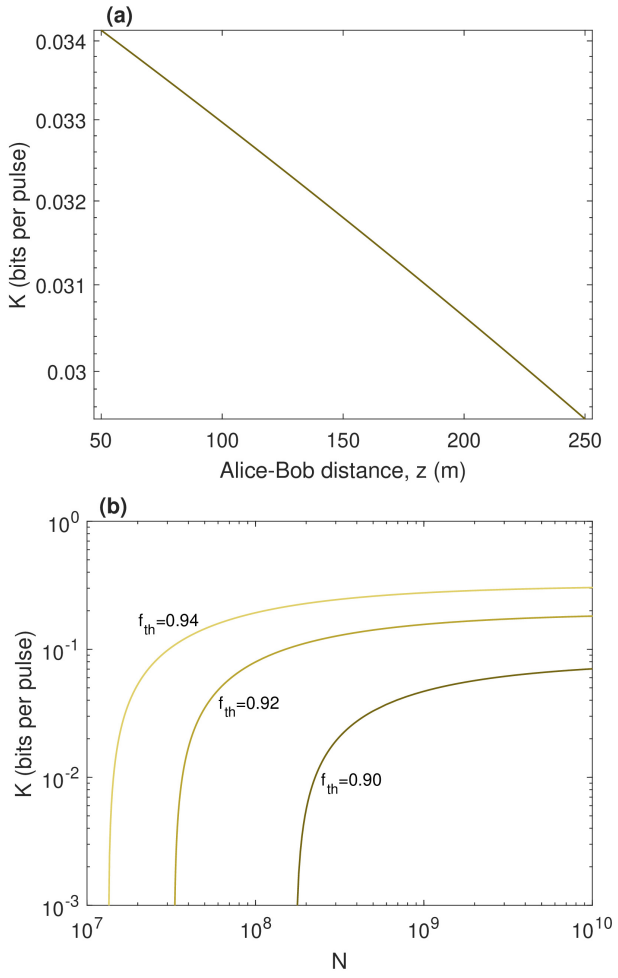

FIG. 4. **Free-space MDI QKD performance. a,** Secret key rate versus total distance at $N = 5 \times 10^8$ and $f_{\rm th} = 0.9$. **b,** Secret key rate versus block size at $z = 100$ m. Set of parameters used are $w_0 = 10$ cm, $a_{\rm rec} = 20$ cm, $\beta = 0.98$, $\mu_A = \mu_B = 45$, $\eta_A = 0.98$, $\eta_{\rm eff} = 0.98$, $\nu_{\rm el} = 0.01$, $\nu_{\rm det} = 1$, $\alpha_0 = 5 \times 10^{-6}$, $C_n^2 = 1.28 \times 10^{-14}$, $\overline{n}_{\rm bg} = 4.8 \times 10^{-12}$, $\delta = 10$ μm, and $\overline{n}_{\rm ex} = 0.04$. Other parameters related to pilots and parameter estimation are $m_{\rm PL} = 0.1N$, $m_{\rm PE} = 0.1N$, $d = 2^6$, FER $= 0.1$, $\varepsilon_{\rm s} = \varepsilon_{\rm h} = \varepsilon_{\rm pe} = 10^{-10}$, $w = 6.34$ and $\varepsilon = 4.5 \times 10^{-10}$. Note that realistic block sizes are up to 10^8 with current data processing facilities.

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 $f_{\rm th} = 0.85$.

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 slant 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 not anymore 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

$$z = \sqrt{(R_E + H_B)^2 + (R_E + H_A)^2(\cos^2\theta - 1)} - (R_E + H_A)\cos\theta, \tag{58}$$

where $R_E \simeq 6371$ km is 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 scintillation index, to be used instead of the Rytov variance is [39, 49]

$$\sigma_{\rm SI}^2(\theta, H_B) = -1 + \exp\left[\frac{0.49\beta_{\rm R}^2(\theta, H_B)}{\left(1 + 1.11\beta_{\rm R}^{12/5}(\theta, H_B)\right)^{7/6}} + \frac{0.51\beta_{\rm R}^2(\theta, H_B)}{\left(1 + 0.69\beta_{\rm R}^{12/5}(\theta, H_B)\right)^{5/6}}\right] \tag{59}$$

where

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

and a downlink path is (from Bob to Alice) assumed. According to the Hufnagel-Valley (H-V) atmospheric model [39, Sec. 12.2], the index-of-refraction structure is a function of the altitude h and the windspeed v

$$C_n^2(h) = 5.94 \times 10^{-53}(v/27)^2 h^{10} e^{-h/1000} + 2.7 \times 10^{-16} e^{-h/1500} + Ae^{-h/100}, \tag{60}$$

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, 39]. 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 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 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 $a_{\rm rec} = 20$ cm, block size $N = 5 \times 10^8$, and pilot postselection threshold $f_{\rm th} = 0.9$. 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).

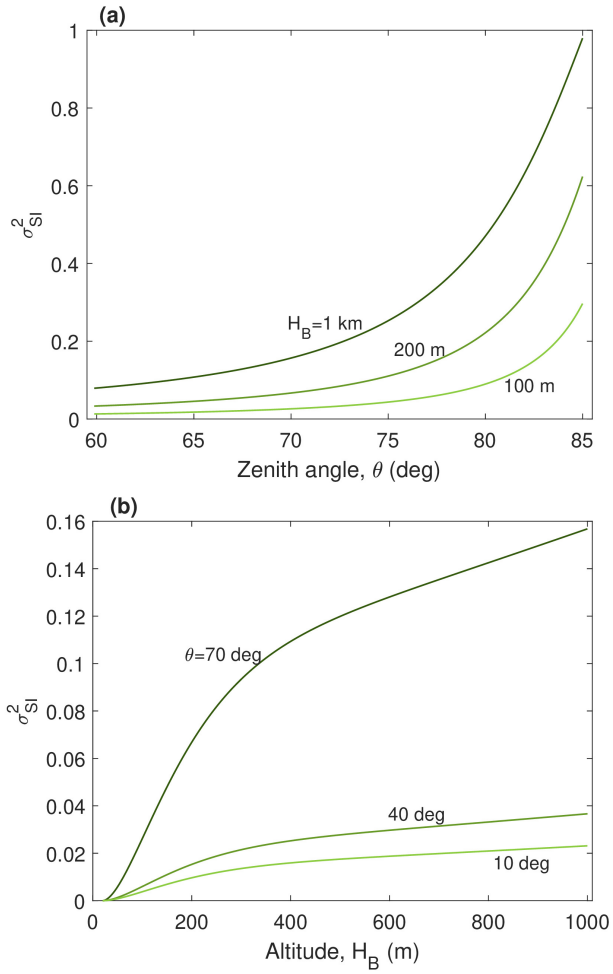

FIG. 5. **High-altitude platform systems. a,** Scintillation index versus the zenith angle at different altitudes of Bob's station. **b,** Scintillation index versus Bob's altitude at different zenith angles. We assume a fixed of H_A = 20m for Alice's station.

V. SUMMARY

In the present work, we have developed a composable security analysis of CV-MDI-QKD over free-space optical links that can include 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 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 hundred meters, where the regime of turbulence is weak.

ACKNOWLEDGMENTS

This work has been funded by the EPSRC via the UK Quantum Communications Hub (Grant No. EP/T001011/1). SP would like to thank G. Mortzou.

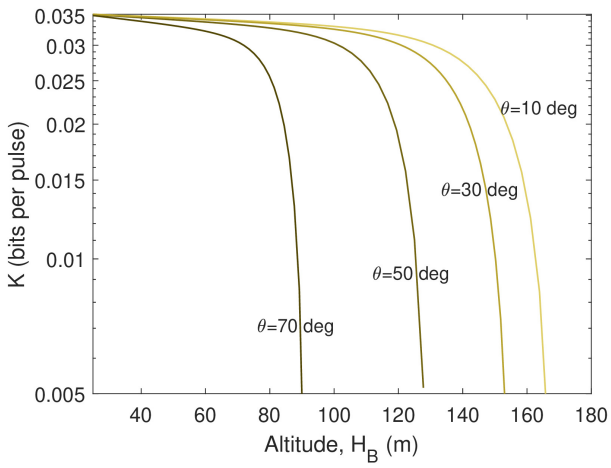

FIG. 6. **Free-space MDI QKD performance with high-altitude platform systems.** Secret key rate versus Bob's altitude at different zenith angles with H_A = 20 m at all cases. The curves represent the rate at f_{th} = 0.9 and the set of parameters used here are the same as reported in Fig. 4, except for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

[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, Adv. Opt. Photon. **12**, 1012 (2020).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

[4] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[5] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, 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, Phys. Rev. A **98**, 032335 (2018).

[8] J. Dias, M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, Phys. Rev. A **102**, 052425 (2020).

[9] K. P. Seshadreesan, H. Krovi, and S. Guha, Phys. Rev. Research **2**, 013310 (2020).

[10] M. Ghalaii and S. Pirandola, 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, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Nature **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, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Nature **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, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, 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, EPJ Quantum Technology **3**, 12 (2016).

[15] D. Dequal, L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, 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, Cryptography **4(1)**, 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, IET Quantum Communication (2021).

[18] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Opt. Express **26**, 24260 (2018).

[19] H. J. Kimble, Nature **453**, 1023 (2008).

[20] S. Pirandola and S. L. Braunstein, Nature **532**, 169 (2016).

[21] S. Pirandola, Phys. Rev. Research **3**, 013279 (2021).

[22] S. Pirandola, Phys. Rev. Research **3**, 023130 (2021).

[23] S. Pirandola, Phys. Rev. Research **3**, 043014 (2021).

[24] M. Ghalaii and S. Pirandola, Communications Physics **5**, 38 (2022).

[25] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[26] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[27] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[28] 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, Phys. Rev. Lett. **111**, 130502 (2013).

[29] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[30] 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, Q. Zhang, C.-Z. Peng, and J.-W. Pan, Phys. Rev. Lett. **125**, 260503 (2020).

[31] X. Wang, C. Dong, S. Zhao, Y. Liu, X. Liu, and H. Zhu, New Journal of Physics **23**, 045001 (2021).

[32] X. Wang, W. Liu, T. Wu, C. Guo, Y. Zhang, S. Zhao, and C. Dong, Entropy **23** (2021), 10.3390/e23101299.

[33] Q. Dong, G. Huang, W. Cui, and R. Jiao, Quantum Science and Technology **7**, 015014 (2021).

[34] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, and S. L. Braunstein, (2013), arXiv:1312.4104v1.

[35] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photonics **9**, 397 (2015).

[36] S. Q. Duntley, J. Opt. Soc. Am. **38**, 179 (1948).

[37] C. F. Bohren and D. R. Huffman, *Absorption and scattering of light by small particles* (John Wiley & Sons Inc., 2008).

[38] S. M. Rytov, Izvestiya Akademii Nauk SSSR, Seriya Fizicheskaya (Bulletin of the Academy of Sciences of the USSR, Physical Series) **2**, 223 (1937).

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

[40] J. A. Dowling and P. M. Livingston, J. Opt. Soc. Am. **63**, 846 (1973).

[41] 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, npj Quantum Inf **7**, 93 (2021).

[42] H. T. Yura, J. Opt. Soc. Am. **63**, 567 (1973).

[43] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, Phys. Rev. Lett. **108**, 220501 (2012).

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

[45] M. Er-long, H. Zheng-fu, G. Shun-sheng, Z. Tao, D. Da-sheng, and G. Guang-can, New Journal of Physics **7**, 215 (2005).

[46] C. Liorni, H. Kampermann, and D. Bruß, New Journal of Physics **21**, 093055 (2019).

[47] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).

[48] P. Papanastasiou, A. G. Mountogiannakis, and S. Pirandola, To appear (2022).

[49] L. C. Andrews, R. L. Phillips, and C. Y. Young, Optical Engineering **39**, 3272 (2000).