


Satellite-To-Earth Quantum Key Distribution via Orbital Angular Momentum

Ziqing Wang^{1,*}, Robert Malaney^{1,†} and Benjamin Burnett^{2,‡}

¹*School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, New South Wales 2052, Australia*

²*Northrop Grumman Corporation, San Diego, California, USA*

 (Received 20 July 2020; revised 15 October 2020; accepted 4 November 2020; published 9 December 2020)

In this work, we explore the feasibility of performing satellite-to-earth quantum key distribution (QKD) using the orbital angular momentum (OAM) of light. Because of the fragility of OAM states the conventional wisdom is that turbulence would render OAM QKD nonviable in a satellite-to-earth channel. However, based on detailed phase screen simulations of the anticipated atmospheric turbulence we find that OAM QKD is viable in some system configurations, especially if quantum channel information is utilized in the processing of postselected states. More specifically, using classically entangled light as a probe of the quantum channel, and reasonably sized transmitter-receiver apertures, we find that nonzero QKD key rates are achievable on sea-level ground stations. We also determine the turbulence conditions under which the QKD key rate becomes effectively zero. Without using classical light probes, OAM QKD is relegated to high-altitude ground stations with large receiver apertures. Our work uses a quantitative assessment of the performance of OAM QKD from satellites to determine under what circumstances the much-touted higher dimensionality of OAM can be utilized in the context of secure communications.

DOI: [10.1103/PhysRevApplied.14.064031](https://doi.org/10.1103/PhysRevApplied.14.064031)

I. INTRODUCTION

As one of the most important applications in quantum communications, quantum key distribution (QKD) has been proven to provide unconditional security [1]. Recently, real-world implementations of satellite-based QKD (see, e.g., Refs. [2,3]) have pointed the way towards global-scale and highly secure quantum communication networks [4]. The originally proposed QKD protocols (see, e.g., Refs. [1,5,6]) mainly utilize two-dimensional encoding. However, other QKD protocols have been generalized to the case of high-dimensional encoding (see, e.g., Ref. [7]), and their unconditional security has been proved (see, e.g., Refs. [8–11]). Quantum information can be encoded in any degree of freedom (DOF) of the photon, but most of the mainstream implementations of QKD (see, e.g., Refs. [2–4]) rely on polarization encoding—a typical two-dimensional encoding scheme that limits the capacity of QKD systems due to an intrinsically bounded Hilbert space.

The orbital angular momentum (OAM) of light has been considered as a promising DOF for quantum communications [12]. Unlike the polarization of light, the OAM

of light can take arbitrary integer values [13]. The corresponding OAM eigenstates form an orthonormal basis that allows for quantum coding within a theoretically infinite-dimensional Hilbert space, opening up alternative possibilities for high-capacity quantum communications. As a key resource for quantum communications, entanglement can be encoded in OAM via the spontaneous parametric down-conversion (SPDC) process [14,15]. The distribution of OAM-encoded entanglement through the turbulent atmosphere has been intensively investigated in *terrestrial* free-space optical (FSO) channels (see, e.g., Refs. [16–21]) with some demonstrating distribution over 3 km [22]. A recent experiment suggests that OAM entanglement distribution could be feasible over a FSO channel of more than 100 km [23].

Besides the generation and distribution of OAM-encoded entanglement, other recent efforts have paved the way for the practical implementation of OAM QKD. Any OAM superposition state can be efficiently encoded in single photons thanks to the versatility of a spatial light modulator (see, e.g., Refs. [24,25]). The sorting of OAM photons has also been made possible (see, e.g., Refs. [26–28]), enabling the capability of performing multioutcome measurements. Implementations of OAM QKD have been demonstrated in laboratory conditions with two-dimensional (see, e.g., Ref. [29]) and higher-dimensional (see, e.g., Refs. [29–32]) encoding. Efforts have also been

*ziqing.wang1@unsw.edu.au

†r.malaney@unsw.edu.au

‡Benjamin.Burnett@ngc.com

made to investigate the practical feasibility of performing OAM QKD in turbulent *terrestrial* FSO channels [33,34]. Outside the laboratory, OAM QKD has been demonstrated over turbulent FSO channels of 210 m [35] and 300 m [36]. Considering other types of medium, OAM QKD has also been demonstrated over a 3 m underwater link [37] and a 1.2 km optical fiber [38]. However, most existing research on OAM QKD has not considered the context of a *satellite-based deployment*. As such, the feasibility of long-range OAM QKD via satellite is still not clear.

We have previously studied the OAM detection performance in satellite-to-earth communications [39], and the feasibility of OAM-based entanglement distribution via satellite [40]. In this work, we explore the feasibility of satellite-to-earth OAM QKD. Our main finding is that, contrary to conventional wisdom, such QKD is indeed feasible. More specifically, we find that utilizing quantum channel information enables satellite-to-earth OAM QKD over a wide range of dimensions under all anticipated circumstances, including the circumstance where a sea-level ground station with a reasonably sized receiver aperture is used. If channel information is not used then feasible satellite-to-earth OAM QKD is confined to large telescopes situated at high-altitude observatories.

The remainder of this paper is as follows. In Sec. II we introduce the necessary background knowledge on OAM eigenstates, atmospheric propagation of light, and the generalized OAM-QKD protocol. In Sec. III we detail the system model for satellite-to-earth OAM QKD. In Sec. IV we present our key results on satellite-to-earth OAM QKD. In Sec. V we explore the use of quantum channel information to improve the practical feasibility of satellite-to-earth OAM QKD. Finally, concluding remarks are provided in Sec. VI.

II. BACKGROUND

A. OAM eigenstates

OAM-QKD protocols utilize OAM eigenstates and their superpositions for quantum encoding. In cylindrical coordinates, the general form of an OAM eigenstate is given by

$$\varphi_{p,l}(r, \theta, z) = R_{p,l}(r, z) \frac{\exp(i l \theta)}{\sqrt{2\pi}}, \quad (1)$$

where r and θ are the radial and azimuthal coordinates, respectively, z is the longitudinal distance, l is the OAM quantum number, p is the radial node number, and $R_{p,l}(r, z)$ is the radial profile. OAM eigenstates with different l values are mutually orthogonal. In this paper, we choose $R_{p,l}(r, z)$ to be Laguerre-Gauss functions, making OAM eigenstates correspond to the Laguerre-Gaussian (LG)

mode set [41]. We express $R_{p,l}(r, z)$ as

$$R_{p,l}(r, z) = 2 \sqrt{\frac{p!}{(p+|l|)!}} \frac{1}{w(z)} \left[\frac{r\sqrt{2}}{w(z)} \right]^{|l|} \exp \left[\frac{-r^2}{w^2(z)} \right] \\ \times L_p^{|l|} \left(\frac{2r^2}{w^2(z)} \right) \exp \left[\frac{ikr^2z}{2(z^2 + z_R^2)} \right] \\ \times \exp \left[-i(2p + |l| + 1) \tan^{-1} \left(\frac{z}{z_R} \right) \right], \quad (2)$$

where $w(z) = w_0 \sqrt{1 + (z/z_R)^2}$, w_0 is the beam-waist radius, $z_R = \pi w_0^2/\lambda$ is the Rayleigh range, λ is the optical wavelength, $k = 2\pi/\lambda$ is the optical wave number, and $L_p^{|l|}(x)$ is the generalized Laguerre polynomial. We denote the single-photon OAM eigenstate of the $LG_{p,l}$ mode as $|p,l\rangle$, and this notation is further simplified to $|l\rangle$ as we only consider the $p = 0$ subspace [42]. We denote the set $\{|l\rangle, -\infty < l < \infty\}$ as the OAM basis and use it as the standard basis throughout this paper. Denoting the dimension as d , the standard basis of d -dimensional OAM QKD contains d mutually orthogonal OAM eigenstates and thus spans a d -dimensional Hilbert space. Throughout this work, we denote such a d -dimensional Hilbert space as the encoding subspace \mathcal{H}_d .

In this work, we consider a maximum OAM number of 4 to construct the encoding subspace \mathcal{H}_d . Specifically, we use the same approach adopted in Ref. [21] to construct the encoding subspace \mathcal{H}_d . For $d = 2$, we consider a two-dimensional encoding subspace spanned by a pair of OAM eigenstates with opposite OAM numbers (i.e., $\mathcal{H}_2 = \{-l_0, l_0\}$ with $l_0 \leq 4$). For $d = 3$, we consider a three-dimensional encoding subspace spanned by a pair of OAM eigenstates with opposite OAM numbers and the OAM eigenstate with zero OAM number (i.e., $\mathcal{H}_3 = \{-l_0, 0, l_0\}$ with $l_0 \leq 4$). For $d > 3$, more OAM numbers are involved. For example, for $d = 4$, the four-dimensional encoding subspace is spanned by two pairs of OAM eigenstates with opposite OAM numbers (i.e., $\mathcal{H}_4 = \{-l_2, -l_1, l_1, l_2\}$ with $l_1 < l_2 \leq 4$).

B. Mutually unbiased bases

Denoted by $\mathcal{M}_\beta = \{|\xi_{(\beta,s)}\rangle, \beta = 1, \dots, d+1, s = 0, \dots, d-1\}$, mutually unbiased bases (MUBs) are orthonormal bases defined on a d -dimensional Hilbert space such that

$$|\langle \xi_{(\beta,s)} | \xi_{(\beta',s')} \rangle|^2 = \begin{cases} \delta_{s,s'} & \text{if } \beta = \beta', \\ \frac{1}{d} & \text{if } \beta \neq \beta', \end{cases} \quad (3)$$

where δ denotes the Kronecker delta function. MUBs play an important role in QKD since any system prepared in a state in one MUB gives outcomes with equal probability

$1/d$ if measured in any other MUB. Therefore, if the eavesdropper measures the quantum signal in a wrong basis, she will acquire no information (in fact, she will introduce a disturbance).

It has been proven that, for a prime-power dimension d , there exists a complete set of $d + 1$ MUBs [43]. In this work we consider a variety of dimensions ranging from $d = 2$ to $d = 9$. When d is a prime number (i.e., 2, 3, 5, 7 in this work), a complete set of $d + 1$ MUBs is found as eigenstates of different Weyl operators in the set $\{Z, XZ^n \mid n = 0, 1, \dots, d - 1\}$. The Z operator is defined as

$$Z = \sum_{j=0}^{d-1} \vartheta^j |j\rangle\langle j|, \quad (4)$$

where $|j\rangle$ denotes the standard basis elements and $\vartheta = \exp(i2\pi/d)$. The X operator is defined as

$$X = \sum_{j=0}^{d-1} |(j + 1) \bmod d\rangle\langle j|. \quad (5)$$

When d is a prime-power number but not a prime number (i.e., 4, 8, 9 in this work), the construction of a complete set of $d + 1$ MUBs becomes a harder task. In this work we adopt the sets of MUBs given in Refs. [44,45] for these dimensions. The only nonprime-power dimension considered in this work is $d = 6$. Since the maximum number of MUBs is not known for an arbitrary dimension, for $d = 6$, we use only the two MUBs generated from the set $\{Z, X\}$ (note that this has a negligible impact on the findings of this work). In OAM QKD, the standard basis is the OAM basis; thus, any $|\xi_{(\beta,s)}\rangle$ is a superposition of OAM eigenstates that span the encoding subspace \mathcal{H}_d .

C. Optical propagation through the turbulent atmosphere

The turbulent atmosphere is a random medium with random inhomogeneities (turbulent eddies) of different size scales. These turbulent eddies give rise to small random refractive index fluctuations, causing continuous phase modulations on the optical beam. This leads to random refraction effects, imposing amplitude and phase distortions on the optical beam as it propagates through the atmospheric channel. The family of eddies bounded above by the outer scale L_{outer} and below by the inner scale l_{inner} form the inertial subrange [46].

Under the paraxial approximation, the propagation of a monochromatic optical beam ψ through the turbulent atmosphere is governed by the stochastic parabolic equation [46]

$$\nabla_T^2 \psi(\mathbf{R}) + i2k\partial_z \psi(\mathbf{R}) + 2\delta n(\mathbf{R})k^2 \psi(\mathbf{R}) = 0, \quad (6)$$

where $\mathbf{R} = [x, y, z]^T$ denotes the three-dimensional position vector [in Eq. (6) we use Cartesian coordinates for simplicity], $\nabla_T^2 = \partial^2/\partial x^2 + \partial^2/\partial y^2$ is the transverse Laplacian operator, and $\delta n(\mathbf{R}) = n(\mathbf{R}) - \langle n(\mathbf{R}) \rangle$ represents the small refractive index fluctuation, with $n(\mathbf{R})$ being the refractive index at \mathbf{R} . Note that the turbulent atmosphere satisfies $\langle n(\mathbf{R}) \rangle = 1$ and $\delta n(\mathbf{R}) \ll 1$ [46]. In this work we numerically solve Eq. (6) using the *split-step* method [47–49], which has been widely used to study atmospheric optical propagation under a variety of conditions. This method models the atmospheric channel using multiple slabs with a phase screen located in the midway of each slab. Two free-space (vacuum) propagations with one random phase modulation in between are repeatedly performed for each slab until the beam reaches the receiver plane [48]. The split-step method has also been used to study the entanglement evolution of OAM-photon pairs in horizontal atmospheric channels, providing quantitative agreement with analytical results [19,20].

D. Generalized OAM-QKD protocol

QKD protocols can be described and implemented in both the prepare-and-measurement (P&M) paradigm and the entanglement-based (EB) paradigm. Although most implementations of QKD are based on the P&M scheme, all P&M QKD protocols have their EB equivalences (note that EB QKD has also been demonstrated over the satellite-to-earth channel; see, e.g., Ref. [3]). Furthermore, the EB paradigm is usually adopted to simplify the security analysis. Throughout this work, we adopt the EB paradigm for OAM QKD. Here we briefly recall the procedures of a d -dimensional OAM-QKD protocol utilizing N_B ($N_B \geq 2$) MUBs.

(1) Alice first generates entangled photon pairs. For every pair of the entangled photons, Alice keeps one photon at her side and sends the other photon to Bob through a quantum channel.

(2) For every photon pair, Alice and Bob randomly (and independently) choose one of the N_B MUBs and perform a d -outcome measurement on their corresponding photon, giving each of them a d -ary symbol.

(3) Alice and Bob start the sifting process where they reveal the MUBs that they used for their photon measurements. Specifically, they generate a sifted key by only keeping the symbols from the photon pairs jointly measured in the same MUB.

(4) In the parameter estimation process, Alice and Bob compare a small subset of their sifted data to estimate the average error rate Q .

(5) With the knowledge on Q , the two parties then carry out subsequent processes, including reconciliation (which

mainly includes error correction) and privacy amplification, to produce a final secret key that Eve has no knowledge on.

III. SYSTEM MODEL

A. System settings

Throughout this work, we denote the satellite and the ground station as Alice and Bob, respectively. In this section, we describe the system settings for satellite-to-earth OAM QKD [as illustrated in Fig. 1(a)]. The ground-station altitude is denoted as h_0 , the satellite zenith angle at the ground station is denoted as θ_z , and the satellite altitude at $\theta_z = 0$ is denoted as H . The channel distance L is given by $L = (H - h_0) / \cos \theta_z$. We denote the aperture radius at the ground station receiver as r_a . To perform OAM QKD, Alice is equipped with an on-board SPDC source that generates entangled OAM-photon pairs. Both Alice and Bob are equipped with versatile OAM mode sorters that can randomly switch between all available MUBs and perform the corresponding d -outcome measurements.

The schematic diagram in Fig. 2 illustrates our deployment strategy for satellite-to-earth OAM QKD, in addition to all effects we consider. These include turbulence-induced crosstalk, loss (due to a finite-sized aperture), misalignment (due to imperfect beam tracking), and tomography noise (which leads to imperfect channel conjugation when classically entangled light is used as a probe to characterize the quantum channel).

Unless otherwise specified, the following assumptions are adopted throughout this work.

(1) We assume that Alice and Bob are perfectly time synchronized, and that they will discard any event where the photon sent by Alice does not click any of Bob's detectors.

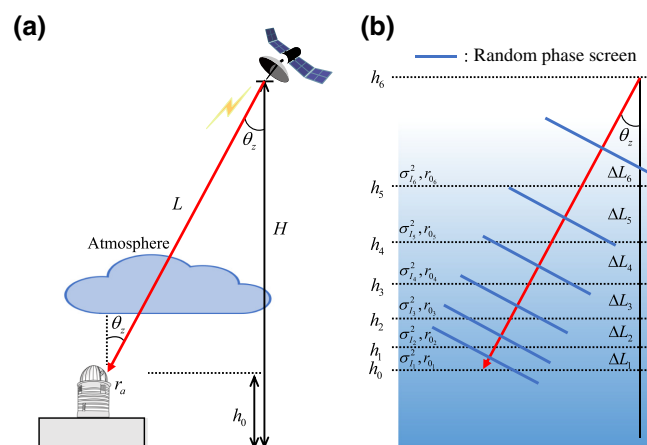


FIG. 1. (a) System model for satellite-to-earth OAM QKD. (b) The modeling of a satellite-to-earth atmospheric channel.

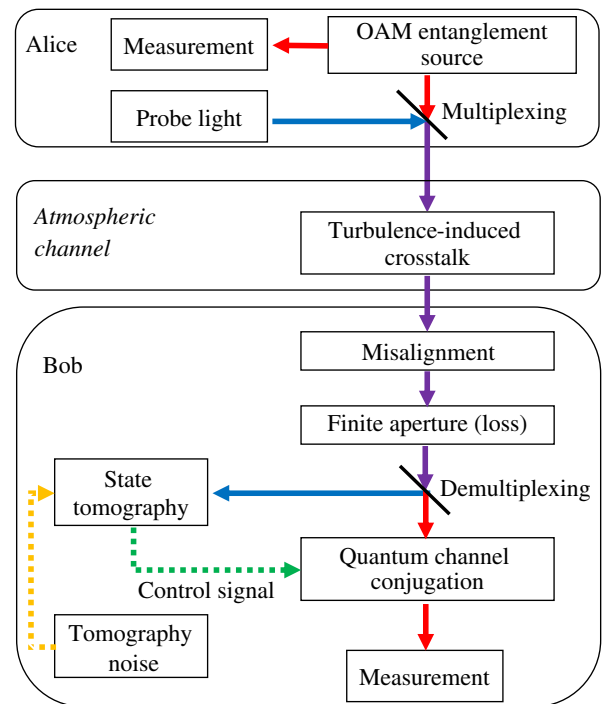


FIG. 2. Schematic diagram for satellite-to-earth OAM QKD.

(2) We assume that the OAM mode sorters used for measurement have a separation efficiency of unity and introduce no additional loss.

(3) For any specific dimension d , we only consider OAM-QKD protocols utilizing all $(d + 1)$ MUBs. We restrict ourselves to the infinite key limit; therefore, the sifting efficiency is set to 1. We also assume a reconciliation efficiency of 1.

(4) In the security analysis we assume that Eve controls the quantum channel and performs a collective attack.

B. Satellite-to-earth atmospheric channel

1. Turbulence characterization

The strength of the optical turbulence within a satellite-based atmospheric channel can be described by the structure parameter $C_n^2(h)$ as a function of altitude h . We can describe $C_n^2(h)$ by the widely used Hufnagel-Valley (HV) model [46]

$$C_n^2(h) = 0.00594(v_{\text{rms}}/27)^2(h \times 10^{-5})^{10} \exp(-h/1000) + 2.7 \times 10^{-16} \exp(-h/1500) + A \exp(-h/100), \quad (7)$$

where A is the ground-level (i.e., sea-level, $h = 0$) turbulence strength in $\text{m}^{-2/3}$. In the above equation, v_{rms} is the root-mean-square (rms) wind speed in m/s, which is given

by

$$v_{\text{rms}} = \left[\frac{1}{15 \times 10^3} \int_{5 \times 10^3}^{20 \times 10^3} V^2(h) dh \right]^{1/2}, \quad (8)$$

where $V(h)$ is the altitude-dependent wind speed profile. In this paper we adopt the Bufton wind speed profile [46]

$$V(h) = V_g + 30 \exp \left[- \left(\frac{h - 9400}{4800} \right)^2 \right], \quad (9)$$

where V_g is the ground-level wind speed [50].

The effect of the atmospheric turbulence on a propagating beam is quantified by two parameters, namely the scintillation index σ_I^2 and the Fried parameter r_0 . The scintillation index is the normalized variance of the intensity. For satellite-to-earth channels under weak-to-strong turbulence, this parameter is given by [46]

$$\sigma_I^2 = \exp \left[\frac{0.49 \sigma_R^2}{(1 + 1.11 \sigma_R^{12/5})^{7/6}} + \frac{0.51 \sigma_R^2}{(1 + 0.69 \sigma_R^{12/5})^{5/6}} \right] - 1 \quad (10)$$

with σ_R^2 being the Rytov variance,

$$\sigma_R^2 = 2.25 k^{7/6} \sec^{11/6}(\theta_z) \int_{h_0}^H C_n^2(h) (h - h_0)^{5/6} dh. \quad (11)$$

The Fried parameter quantifies the coherence length of the turbulence-induced phase errors in the transverse plane. For satellite-to-earth channels, this parameter is given by [46]

$$r_0 = \left[0.423 k^2 \sec \theta_z \int_{h_0}^H C_n^2(h) dh \right]^{-3/5}. \quad (12)$$

The detailed channel modeling used to perform the split-step method is illustrated in Fig. 1(b), and is further discussed in the Appendix.

2. Quantum state evolution

To illustrate the undesirable decoherence effects caused by the atmospheric turbulence, we formally describe the evolution of an OAM eigenstate within a satellite-to-earth channel. Assuming that Alice sends a single-photon OAM eigenstate $|l\rangle$ to Bob's ground station through an atmospheric channel, the evolution of such a single-photon OAM eigenstate can be described by a unitary operator $U_{\text{turb}}(L)$ [21].

Denoting the received state as $|\psi_{l_t}\rangle$, we have

$$|\psi_{l_t}\rangle = U_{\text{turb}}(L) |l\rangle. \quad (13)$$

The received single-photon state can be expanded in the OAM basis as

$$|\psi_{l_t}\rangle = \sum_l c_{l,l_t}(L) |l\rangle, \quad (14)$$

where $c_{l,l_t}(L) = \langle l | U_{\text{turb}}(L) | l_t \rangle$.

In this work, the evolution of a single-photon OAM eigenstate is simulated by the atmospheric propagation of the corresponding classical LG beam via the split-step method. In Fig. 3 we plot the intensity and phase profiles of a LG₀₃ beam after vacuum propagation (i.e., propagation without atmospheric turbulence) and one realization of atmospheric propagation. After a vacuum propagation, we have $c_{l,l_t} = \delta_{l,l_t}$ due to the orthogonality of OAM eigenstates. After atmospheric propagation, however, the turbulence-induced distortions lead to crosstalk. At the receiver, $|\psi_{l_t}\rangle$ is generally a superposition of OAM eigenstates, and thus it is no longer orthogonal to any OAM eigenstate. The resulting crosstalk causes entanglement decay and thus degrades the performance of OAM QKD. A good quantitative measurement of the resulting crosstalk is the OAM spectrum that can be considered as a set of crosstalk probabilities (i.e., the probabilities that an original OAM eigenstate $|l\rangle$ scatters into other OAM eigenstates $|l_t\rangle$; see, e.g., Refs. [21,51]). The crosstalk probabilities under a single channel realization can be simply calculated as $P(l_t \rightarrow l) = |c_{l,l_t}|^2$. The crosstalk matrix can

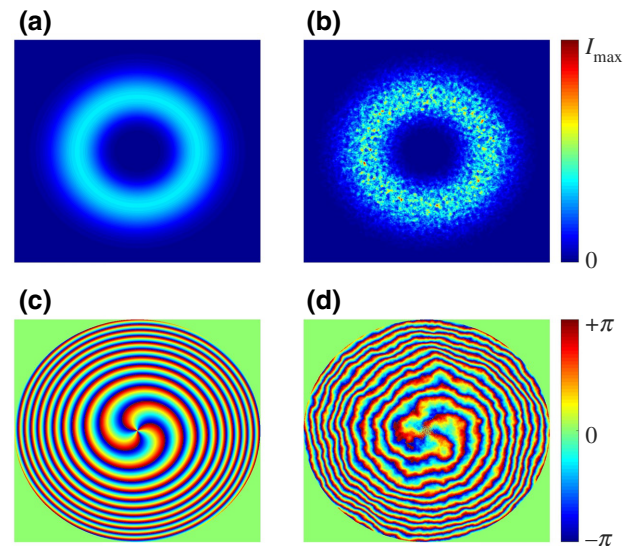


FIG. 3. (a),(b) Intensity and (c),(d) phase profiles for a LG₀₃ beam after a vacuum propagation (left) and a realization of atmospheric propagation (right). For illustration purposes, the ground-station altitude is set to $h_0 = 3000$ m.

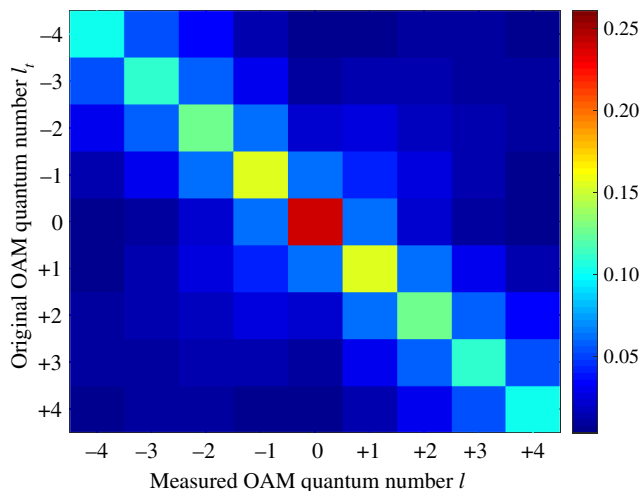


FIG. 4. The crosstalk matrix under the same settings of Figs. 3(b) and 3(d). The crosstalk probabilities are averaged over 4000 channel realizations. As an intuitive illustration of the turbulence-induced crosstalk, only the data for $|l_i| \leq 4$ and $|l| \leq 4$ are presented. Note that the probabilities in any row do not sum to 1 because of the small data extraction range, and the projection onto the $p = 0$ subspace.

be acquired by combining the OAM spectra for different original l_i values and extracting the data within a certain interested range of l . In Fig. 4 we present the crosstalk matrix (averaged over 4000 channel realizations) as a quantitative illustration of crosstalk under the same settings of Figs. 3(b) and 3(d). For detailed analyses of the OAM crosstalk behaviors and the OAM crosstalk matrix, we refer the reader to, e.g., Refs. [39,51,52].

C. OAM QKD over the satellite-to-earth channel

Now let us analyze the performance of OAM-QKD protocols introduced in Sec. IID over the satellite-to-earth channel. Specifically, we are interested in the achievable QKD performance over the satellite-to-earth channel. The QKD performance is quantified by the secret key rate K in *bits per sent photon*, and throughout this work we use the unit *bits per photon* for short.

For a d -dimensional OAM-QKD protocol, Alice generates OAM-photon pairs, each pair being in the maximally entangled state

$$|\Phi_0\rangle = \sum_{l_i \in \mathcal{H}_d} \frac{1}{\sqrt{d}} |l_i\rangle |l_i\rangle, \quad (15)$$

where \mathcal{H}_d is a d -dimensional encoding subspace. From each pair, one photon is sent to Bob through a satellite-to-earth quantum channel. At the output, the quantum state shared between Alice and Bob *before any measurement* is

given by

$$|\Phi_{\text{turb}}\rangle = \{\mathbb{1} \otimes U_{\text{turb}}(L)\} |\Phi_0\rangle = \sum_{l_i \in \mathcal{H}_d} \sum_{l \in \mathcal{H}_\infty} \frac{c_{l,l_i}}{\sqrt{d}} |l_i\rangle |l\rangle, \quad (16)$$

where $\mathbb{1}$ denotes an identity operator acting on Alice's photon and \mathcal{H}_∞ denotes an infinite-dimensional Hilbert space.

Although the initial state $|\Phi_0\rangle$ can be considered as a finite-dimensional state living in the $\mathcal{H}_d \otimes \mathcal{H}_d$ subspace, due to the crosstalk it spreads over the entire infinite-dimensional Hilbert space. Since a practical system can only utilize a finite-dimensional encoding subspace, a necessary procedure is to project the output state $|\Phi_{\text{turb}}\rangle$ onto the original $\mathcal{H}_d \otimes \mathcal{H}_d$ subspace. This procedure is realized by a postselection at Bob's side, giving a postselected (and unnormalized) state

$$|\Phi_{\text{ps}}\rangle = (\mathbb{1} \otimes O) |\Phi_{\text{turb}}\rangle, \quad (17)$$

where O is the filtering operator acting on Bob's photon. Since Bob has no information on $U_{\text{turb}}(L)$, his filtering operator O is equal to $\Pi_d = \sum_{l_p \in \mathcal{H}_d} |l_p\rangle \langle l_p|$. By setting $O = \Pi_d$, the postselected state in Eq. (17) can be explicitly given as [53]

$$|\Phi_{\text{ps}}\rangle = (\mathbb{1} \otimes \Pi_d) |\Phi_{\text{turb}}\rangle = \sum_{l_i \in \mathcal{H}_d} \sum_{l \in \mathcal{H}_d} \frac{c_{l,l_i}}{\sqrt{d}} |l_i\rangle |l\rangle. \quad (18)$$

Note that $|\Phi_{\text{ps}}\rangle$ is not normalized. In fact, the atmospheric propagation and the postselection together form a completely positive (and nontrace-preserving) map $\Pi_d U_{\text{turb}}(L)$. It is obvious that the postselection results in a loss of photons. However, this operation will not give Eve any information, since the lost photons are simply discarded by Alice and Bob and will not be used in key generation.

Since we are not interested in any specific realization of the atmospheric channel, we perform an ensemble average of $|\Phi_{\text{ps}}\rangle$ over different channel realizations. After averaging over channel realizations and performing renormalization, the averaged state shared between Alice and Bob can be given as a mixed state described by

$$\rho_{AB} = \frac{\langle |\Phi_{\text{ps}}\rangle \langle \Phi_{\text{ps}}| \rangle}{\mathcal{T}}, \quad (19)$$

where $\langle \cdot \rangle$ denotes an ensemble average and $\mathcal{T} = \text{tr}(\langle |\Phi_{\text{ps}}\rangle \langle \Phi_{\text{ps}}| \rangle)$ is the trace required for renormalization. Note that \mathcal{T} quantifies the *photon survival fraction* after postselection.

Now we briefly recall how security analysis is performed and how the key rate is calculated for our OAM-QKD protocols (for a complete and rigorous security

analysis, we refer the reader to Refs. [10,11]). Utilizing the photons that survive the postselection, the secret key rate K_1 can be expressed as [54]

$$K_1 = I(A : B) - \chi(A : E), \quad (20)$$

where $I(A : B)$ is the classical mutual information between Alice and Bob, and $\chi(A : E)$ is the quantum mutual information between Alice and Eve. Considering the fact that Eve holds a purification of ρ_{AB} , $\chi(A : E)$ can be explicitly given as

$$\chi(A : E) = S(\rho_{AB}) - \sum_a p(a) S(\rho_B|a), \quad (21)$$

where $S(\cdot)$ denotes the von Neumann entropy, $a = 0, \dots, d-1$ denotes Alice's measurement outcome, $p(a)$ denotes the probability distribution of a , and $\rho_B|a$ is the state of Bob's photon conditioned on a . In the security analysis it is assumed that all errors are caused by Eve's eavesdropping attempts. The average error rate Q can be expressed as

$$Q = \frac{1}{N_B} \sum_{\beta=1}^{N_B} \sum_{\substack{s,s' \\ s \neq s'}} \text{tr}(|\xi_{(\beta,s)}^*\rangle \langle \xi_{(\beta,s)}^*| \otimes |\xi_{(\beta,s')} \rangle \langle \xi_{(\beta,s')} | \rho_{AB}). \quad (22)$$

Starting from Eqs. (20) and (21), K_1 is found to be a function of Q [10,11]. For a d -dimensional QKD protocol utilizing all $(d+1)$ MUBs, K_1 can be calculated as

$$K_1 = \log_2 d + \frac{d+1}{d} Q \log_2 \left(\frac{Q}{d(d-1)} \right) + \left(1 - \frac{d+1}{d} Q \right) \log_2 \left(1 - \frac{d+1}{d} Q \right). \quad (23)$$

Recalling a nonunity photon survival fraction \mathcal{T} , the achievable secret key rate K is given by

$$K = \mathcal{T} K_1. \quad (24)$$

IV. NUMERICAL EVALUATION OF QKD PERFORMANCE

In this section, we numerically evaluate the performance of the satellite-to-earth OAM-QKD protocols analyzed in Sec. III C. We carry out Monte Carlo simulations to numerically evaluate the secret key rate K . First, we generate 4000 independent realizations of the satellite-to-earth channel. For each channel realization, we perform a series of atmospheric propagations using the split-step method to obtain a realization of $|\Psi_{\text{ps}}\rangle$ [see Eq. (17)]. Afterwards,

realizations of $|\Psi_{\text{ps}}\rangle$ are used to obtain \mathcal{T} and ρ_{AB} [see Eq. (19)]. Then Q is evaluated from ρ_{AB} [see Eq. (22)], and K_1 is then evaluated from Q [see Eq. (23)]. Finally, K can be evaluated using K_1 and \mathcal{T} [see Eq. (24)].

A. General settings

We restrict ourselves to the case of a low-Earth-orbit (LEO) satellite with a maximum satellite altitude $H = 500$ km. We consider two zenith angles, $\theta_z = 0^\circ$ and $\theta_z = 45^\circ$, giving a maximum channel distance of $L \sim 500$ km and $L \sim 700$ km, respectively [55]. Note that a higher H leads to worse performance. This is because the beam radius on atmospheric entry increases with H (due to diffraction), and this in turn results in increased distortion on the beam. A larger θ_z also leads to worse performance, since the photon travels a longer distance within the turbulent atmosphere. Unless otherwise stated, when we refer to our results, we mean for all considered H values (i.e., from 200 to 500 km) and for all considered θ_z values (i.e., 0° and 45°). Also, throughout this work, QKD performances are compared at the same satellite altitudes under the same zenith angles.

For the atmospheric parameters, we set $A = 9.6 \times 10^{-14} \text{ m}^{-2/3}$, which accords with a realistic setting adopted in Ref. [56]. We set $V_g = 3$ m/s, giving a value of $v_{\text{rms}} = 21$ m/s. We set $L_{\text{outer}} = 5$ m and $l_{\text{inner}} = 1$ cm for the atmospheric turbulence [57]. For the optical parameters, we set $\lambda = 1064$ nm in accord with existing entanglement sources (see, e.g., Ref. [58]), and set w_0 to 15 cm.

The loss of signal at the receiver will be a function of several system parameters as well as the atmospheric conditions [59]. The beam width at the receiver is critical in determining the loss of signal, and is largely dependent on system parameters such as transmitter aperture (sets the beam waist w_0), and the distance between the satellite and the ground station. For a given optical wavelength, a given beam width at the receiver, and a given channel distance, the transmitter beam waist required can be easily determined. However, in our calculations we simply set the beam waist (in effect the transmitter aperture). To orientate ourselves, we note that the Micius satellite (which orbits at an altitude of about 500 km), with an aperture size of 0.3 m, provided a beam width of 12 m at ground level at a channel distance of 1200 km [2,3]. For a satellite altitude of 500 km, the smallest beam width at ground level we will have in our calculations will be 2.2 m, corresponding to a 1 dB loss at a receiver aperture of 1 m radius (for a sea-level receiver, and a zenith angle of 0° , this corresponds to our $w_0 = 15$ cm).

We perform all simulations using a numerical grid of 2048×2048 points with a spatial resolution [60] of 5 mm. In generating the random phase screens using the FFT-based method, 3 orders of subharmonics are added using

the method introduced in Ref. [61] to accurately represent the low-spatial-frequency components contributed by large-scale turbulent eddies.

B. Ideal circumstances

We first explore a rather ideal circumstance for the receiver. Adopting all settings of Sec. IV A, we initially set the ground-station altitude to $h_0 = 3000$ m to avoid the strong atmospheric turbulence near the sea level. We also first adopt a large receiver aperture of $r_a = 4$ m, thus providing a zero-loss scenario.

First we investigate the performances of two-dimensional and three-dimensional OAM QKD for different l_0 values under such an ideal circumstance. For two-dimensional OAM QKD, we find that a large l_0 value generally leads to a higher secret key rate. Under $\theta_z = 0^\circ$, positive key rates of 0.03, 0.05, 0.06 bits/photon can be achieved at $H = 500$ km for $l_0 = 2, 3, 4$, respectively. Under $\theta_z = 45^\circ$, we observe a reduction in the secret key rate ranging from 70% to 100%. Specifically, only $l_0 = 4$ leads to a positive key rate of 10^{-3} bits/photon at $H = 500$ km. For three-dimensional OAM QKD, we find that a larger l_0 value does not always lead to a higher secret key rate. Under $\theta_z = 0^\circ$, despite the observation that $l_0 = 1$ does not lead to any positive key rate, there is no significant correlation between the achievable secret key rate and l_0 for $l_0 = 2, 3, 4$. Moreover, no positive key rate can be achieved at $H = 500$ km for any considered l_0 value. Under $\theta_z = 45^\circ$, we find that no positive key rate can be achieved by three-dimensional OAM QKD. By comparing the QKD performances, we find that the performance of three-dimensional OAM QKD is overall inferior to the performance of two-dimensional OAM QKD over the satellite-to-earth channel for a given l_0 value.

We then compare the performances of OAM QKD of dimensions ranging from 2 to 9 under $\theta_z = 0^\circ$, and find that the QKD performance decreases as the dimension increases [62]. Specifically, we find that no performance advantage can be achieved, by OAM QKD of any dimension, against two-dimensional OAM QKD at $H > 200$ km. Furthermore, we find that OAM QKD of dimensions larger than 5 achieve no positive key rate at all considered satellite altitudes and under all considered zenith angles. No positive key rate can be achieved by OAM QKD of dimensions larger than 2 under $\theta_z = 45^\circ$.

It is widely anticipated that the use of higher-dimensional QKD can improve noise resistance and lead to a higher secret key rate. However, all the observations reported in this subsection clearly indicate that an increased dimension *cannot* improve the performance of OAM QKD over the satellite-to-earth channel, even under the ideal circumstance. This finding can be explained by the fact that the maximally OAM-entangled state of a higher dimension is less robust against turbulence (note

that the similar phenomenon has been observed in, e.g., Ref. [21]). This will lead to an increased error rate that can be large enough to nullify the advantage of higher-dimensional QKD. Therefore, a lower secret key rate is achieved in spite of a higher photon survival fraction (due to an enlarged encoding subspace). In other words, the theoretical capacity advantage provided by increasing the dimension in OAM QKD is negated by the atmospheric turbulence over the satellite-to-earth channel.

C. Realistic circumstances

Now we extend our scope to more realistic circumstances. Specifically, we discuss the impact of loss, and a lower ground-station (receiver) altitude, on the feasibility of satellite-to-earth OAM QKD.

1. Loss

The main source of loss in a satellite-to-earth channel is diffraction loss. Generally, diffraction loss becomes more significant as the channel distance increases. Diffraction loss is also *state dependent* in OAM QKD since OAM eigenstates with different (absolute values of) OAM numbers experience different amounts of diffraction [63]. Specifically, an OAM eigenstate with a larger OAM number results in a larger beam size after free-space propagation [64], and thus suffers from a heavier diffraction loss when a limited-sized receiver aperture is used. Diffraction loss generally reduces the photon survival fraction, leading to a reduced QKD performance. For OAM QKD with a dimension larger than 2, the state-dependent nature of diffraction loss further modifies the (relative) amplitudes of the OAM eigenstates that span the encoding subspace, leading to an increased error rate and performance degradation. In order to investigate the impact of loss on the feasibility of satellite-to-earth OAM QKD, we adopt all settings of Sec. IV B except setting the radius of the receiver aperture to $r_a = 1$ m. At $H = 500$ km and under $\theta_z = 0^\circ$, setting $r_a = 1$ m gives losses of 1, 3.4, 6.9, 11.3, 16.7 dB to OAM eigenstates with OAM numbers 0, 1, 2, 3, 4, respectively. We then re-evaluate the performances of two-dimensional and higher-dimensional OAM QKD.

In Fig. 5 we compare the performances of two-dimensional OAM QKD, achieved with $r_a = 1$ m and $r_a = 4$ m (zero loss), under $\theta_z = 0^\circ$ and $h_0 = 3000$ m. From this figure, we see that loss degrades the performance of two-dimensional OAM QKD. We further note that the trends of curves are opposite for $r_a = 4$ m (solid curves) and $r_a = 1$ m (dashed curves). Specifically, compared to a smaller l_0 value, a larger l_0 value generally leads to a higher (lower) performance when $r_a = 4$ m ($r_a = 1$ m) is used. Such an observation indicates that the performance degradation due to loss is more significant for a larger l_0 value than for a smaller l_0 value. This is mainly because, for a given aperture size (under the presence of loss), a

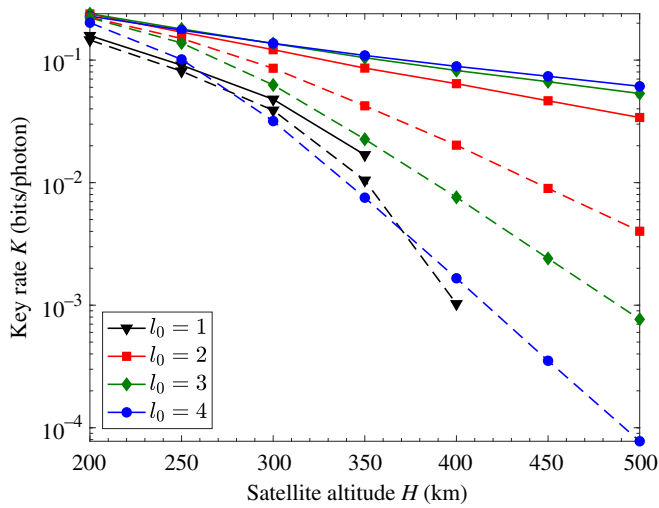


FIG. 5. Secret key rates K of two-dimensional satellite-to-earth OAM QKD, achieved with $r_a = 1$ m (dashed) and $r_a = 4$ m (solid). These results are achieved under $h_0 = 3000$ m and $\theta_z = 0^\circ$. Note that some curves end before reaching $H = 500$ km due to a zero key rate. This happens when the average error rate Q surpasses the tolerable error rate.

larger l_0 value leads to a lower photon survival fraction, and thus results in a lower secret key rate.

Higher-dimensional OAM QKD is more sensitive to loss. For three-dimensional OAM QKD, after setting $r_a = 1$ m we find that no positive key rate can be achieved at $H > 300$ km under $\theta_z = 0^\circ$. For OAM QKD of dimensions larger than 3, setting $r_a = 1$ m we find that no positive key rate can be achieved at $H > 250$ km. Comparing the performances of OAM QKD of different dimensions under loss, we find that two-dimensional OAM QKD is more robust against loss compared to higher-dimensional OAM QKD. Indeed, the loss has a greater impact on higher-dimensional OAM QKD due to its state-dependent nature (see related discussions in, e.g., Ref. [65]).

2. Receiver altitude

Lowering the ground-station altitude increases the turbulence strength, and intuitively this can degrade QKD performance. To see whether satellite-to-earth OAM QKD is feasible under lower ground-station altitudes, we adopt all settings of Sec. IV B except for lower h_0 values. In Fig. 6 we compare the performances of two-dimensional OAM QKD, under $\theta_z = 0^\circ$, under different ground-station altitudes h_0 . From this figure, we clearly see that the use of a lower ground-station altitude degrades the performance of two-dimensional OAM QKD at a given satellite altitude. The offset between the $l_0 = 1$ results and the other results is because $l_0 = 1$ gives the smallest separation between the two states (i.e., l_0 and $-l_0$) that span the two-dimensional encoding subspace \mathcal{H}_2 . This leads to the most severe OAM crosstalk (within the encoding subspace) and therefore the

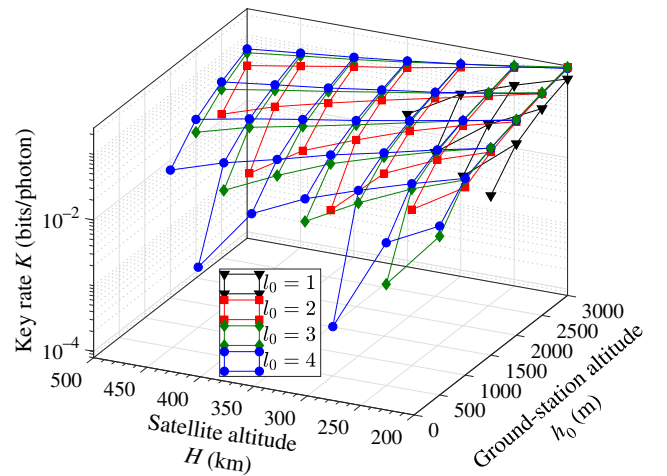


FIG. 6. Secret key rates K of two-dimensional satellite-to-earth OAM QKD under different ground-station altitudes h_0 . These results are achieved with $r_a = 4$ m under $\theta_z = 0^\circ$. Again, some curves end before reaching $H = 500$ km due to a zero key rate.

worst performance (note that similar phenomena have also been observed in, e.g., Refs. [20,21,33,40]). We see that a positive key rate can still be achieved for $l_0 = 4$ at $H = 500$ km under $h_0 = 1500$ m. Under $\theta_z = 45^\circ$, we find that no positive key rate can be achieved at $H > 300$ km under $h_0 = 2000$ m.

OAM QKD of a higher dimension is more sensitive to h_0 . For three-dimensional OAM QKD, we find that a larger l_0 value is not more robust against performance degradation. We also find that, for $h_0 = 2000$ m, no positive key rate can be achieved by three-dimensional OAM QKD at $H > 250$ km even under $\theta_z = 0^\circ$. For OAM QKD of dimensions larger than 3, for $h_0 = 2000$ m, we find that no positive key rate can be achieved at $H > 200$ km even under $\theta_z = 0^\circ$.

3. Sea-level receiver with a reasonably sized aperture

Then we adopt all settings of Sec. IV A and jointly set $r_a = 1$ m and $h_0 = 0$ m to reflect a more realistic scenario where a sea-level receiver with a reasonably sized aperture is used. Unfortunately, we find that no positive key rate can be achieved by OAM QKD of any dimension, even under $\theta_z = 0^\circ$.

V. FEASIBILITY THROUGH CHANNEL INFORMATION

In all previous sections we have assumed that channel knowledge is unavailable. It is intuitive to think that channel information can be used to improve QKD performance. Indeed, in quantum communications a natural paradigm is to characterize the quantum channel through quantum process tomography (QPT) [66,67], and cancel

out the turbulence-induced effects accordingly [68]. However, QPT is performed at the single-photon level, making the real-time characterization of quantum channels a challenging job. Recently, it has been discovered that the state evolution of the classically entangled degrees of freedom is equivalent to the state evolution of quantum entangled photons [68]. Such an equivalence allows for the use of nonseparable (i.e., DOF-entangled) states of classical light to characterize the quantum channel (see, e.g., Refs. [33,68–70]). By performing a state tomography on the output classical light, the quantum channel can be readily characterized in real time (for a comprehensive tutorial, see, e.g., Ref. [71]).

In this section we explore the use of quantum channel information to improve the practical feasibility of satellite-to-earth OAM QKD. Inspired by Refs. [33,68], we utilize the quantum channel information acquired through a real-time quantum channel characterization utilizing nonseparable states of classical light, and apply a quantum channel conjugation at the ground station. By quantum channel information we mean the Kraus operator of the channel, and by quantum channel conjugation we mean the application of a quantum conjugate filter that cancels out the turbulence-induced crosstalk.

A. General method

In this section, we demonstrate how a conjugate filter could be found, and we also analyze the impact of using that filter on OAM QKD. The nonseparable states of classical light we use for channel characterization are given in the general form [69]

$$|\Phi_0^C\rangle = \sum_m \alpha_m |D_m^{(1)}\rangle |D_m^{(2)}\rangle, \quad (25)$$

where the first DOF $D_m^{(1)}$ is a DOF that is not affected by the turbulent atmosphere (e.g., polarization or wavelength), the second DOF $D_m^{(2)}$ denotes the OAM DOF of light, m indicates different basis elements in these degrees of freedom, and α_m denotes the expansion coefficients such that $\sum_m |\alpha_m|^2 = 1$. We denote the encoding subspaces of $D_m^{(1)}$ and $D_m^{(2)}$ as $\mathcal{H}^{(1)}$ and $\mathcal{H}^{(2)}$, respectively. To faithfully characterize the quantum channel under study, it is required that $\dim(\mathcal{H}^{(1)}) = \dim(\mathcal{H}_d)$ and $\mathcal{H}^{(2)} = \mathcal{H}_d$.

In an OAM QKD protocol Alice prepares OAM-photon pairs in the maximally entangled state $|\Phi_0\rangle$ described by Eq. (15). To help characterize the quantum channel, Alice also generates classical light in the corresponding nonseparable state $|\Phi_0^C\rangle$ described by Eq. (25). While sending one photon of each entangled photon pair to Bob, Alice simultaneously sends the classical light through the same channel [72]. Since the state evolution of $|\Phi_0^C\rangle$ is equivalent to the state evolution of $|\Phi_0\rangle$, under a specific channel realization, Bob can characterize the one-sided OAM quantum

channel in the encoding subspace \mathcal{H}_d by performing a state tomography on the received classical light. Specifically, Bob finds the Kraus operator M that satisfies

$$(\mathbb{1} \otimes M)|\Phi_0^C\rangle = (\mathbb{1} \otimes \Pi_d)|\Phi_{\text{turb}}^C\rangle, \quad (26)$$

where $|\Phi_{\text{turb}}^C\rangle = \{\mathbb{1} \otimes U_{\text{turb}}(L)\}|\Phi_0^C\rangle$ denotes the state of the received classical light at Bob's side. Note that the right-hand side of Eq. (26) is known to Bob via his state tomography.

The Kraus operator M can be expressed in its polar decomposition as

$$M = U|M|, \quad (27)$$

where U is a unitary operator and $|M| = \sqrt{M^\dagger M}$ is a positive Hermitian operator. We can express $|M|$ in its spectral decomposition

$$|M| = \sum_{j=1}^d \gamma_j |v_j\rangle \langle v_j|, \quad (28)$$

where γ_j and $|v_j\rangle$ denote the eigenvalues of $|M|$ and their corresponding eigenvectors, respectively. Note that $|v_j\rangle$ can be expressed as superpositions of the standard basis elements.

Considering the fact that the γ_j are smaller than 1, the conjugate filter cannot be directly constructed as M^{-1} . This is because $|M|^{-1}$ has eigenvalues larger than 1 and thus cannot be physically implemented due to a violation of the no-cloning theorem [73]. To construct a conjugate filter that does not violate the no-cloning theorem, inspired by the idea in Ref. [33] we consider a conjugate filter \tilde{M} that achieves $\tilde{M}M \propto \mathbb{1}$. Specifically, we construct the conjugate filter as

$$\tilde{M} = \left(\sum_{j=1}^d \frac{\gamma_{\min}}{\gamma_j} |v_j\rangle \langle v_j| \right) U^\dagger, \quad (29)$$

where $\gamma_{\min} = \min\{\gamma_j, j = 1, \dots, d\}$. Note that \tilde{M} in Eq. (29) is a *local Procrustean filter* that can be physically implemented (see experimental demonstrations of OAM Procrustean filters in, e.g., Refs. [15,74,75]).

Under every channel realization, Bob constructs the Kraus operator M , constructs the conjugate filter \tilde{M} , and applies \tilde{M} on his photon. Therefore, Alice and Bob share a postselected state of the form

$$|\Phi'_{\text{ps}}\rangle = (\mathbb{1} \otimes \tilde{M})|\Phi_{\text{turb}}\rangle = \gamma_{\min}|\Phi_0\rangle. \quad (30)$$

Note that $|\Phi'_{\text{ps}}\rangle$ is not normalized. From Eq. (30), it can be seen that the quantum channel conjugation results in a probabilistic entanglement distillation. After averaging

over channel realizations and performing renormalization, ρ_{AB} is now given by

$$\rho'_{AB} = \frac{\langle |\Phi'_{ps}\rangle \langle \Phi'_{ps}| \rangle}{\mathcal{T}'} = |\Phi_0\rangle \langle \Phi_0|, \quad (31)$$

where $\mathcal{T}' = \langle \gamma_{\min}^2 \rangle$ is the photon survival fraction when the quantum channel conjugation is applied. Note that \mathcal{T}' can be interpreted as the probability of success of the quantum channel conjugation (which can be as low as 10^{-4} in extreme cases). Following the descriptions in Sec. III C, ρ'_{AB} and \mathcal{T}' can be then used to evaluate the secret key rate K . It can be inferred from Eq. (31) that $Q = 0$ is achieved by the quantum channel conjugation at the cost of a low photon survival fraction.

Here we summarize the assumptions made, regarding the quantum channel characterization and the quantum channel conjugation, in this section. For simplicity, we assume that the channel Kraus operator M is constructed without error (i.e., perfect state tomography on classical light), and the exact conjugate filter \tilde{M} is applied to Bob's photon without error. Furthermore, these operations are assumed to be performed in real time. Such an assumption indicates that the time taken to perform a state tomography on the classical light is less than the coherence time of the atmospheric channel (typically of the order of milliseconds [46]). Although no experiment has been demonstrated so far to indicate how fast such a state tomography can be done, in principle all the projective measurements required by such a state tomography can be done simultaneously with high signal-to-noise ratio. In addition, a recent work [76] has demonstrated that a complete state tomography can be done in one shot if the classical light is in a pure state (note that this is valid under every specific channel realization). We further note that the paradigm adopted here resembles the concept of adaptive optics (AO) where a servo loop system tracks (with a wavefront sensor) and corrects (with a deformable mirror) the turbulence effect in a real-time fashion. Given the fact that current AO systems have no significant trouble keeping up with the temporal evolution of turbulence, we believe that the quantum channel characterization and the following quantum channel conjugation can also be performed in real time.

B. QKD performance with quantum channel conjugation

To numerically investigate the impact of the quantum channel conjugation on QKD performance, we adopt the settings of Secs. IV B and IV C, and re-evaluate the performances of satellite-to-earth OAM QKD of different dimensions. In two-dimensional OAM QKD, we assume that the vector vortex beam is used for quantum channel characterization (for a detailed review on vector vortex beams, we refer the reader to, e.g., Ref. [77]). Specifically,

Eq. (25) is explicitly given by

$$|\Phi_0^C\rangle = \frac{1}{\sqrt{2}}(|R\rangle|l_0\rangle + |L\rangle|-l_0\rangle), \quad (32)$$

where $|R\rangle, |L\rangle$ denote right and left circular polarization states, respectively. In three-dimensional OAM QKD, the vector vortex beam cannot be used due to the constraint of the two-dimensional Hilbert space imposed by the polarization DOF. It has been proposed in Ref. [69] that the wavelength DOF of light is a promising candidate to replace the polarization DOF of light in $|\Phi_0^C\rangle$. Specifically, Eq. (25) is explicitly given by

$$|\Phi_0^C\rangle = \frac{1}{\sqrt{3}}(|\lambda_1\rangle|l_0\rangle + |\lambda_2\rangle|0\rangle + |\lambda_3\rangle|-l_0\rangle), \quad (33)$$

where the λ_m denote different wavelengths. Although no experiment has been demonstrated so far, the use of classical light in a state described by Eq. (33) is theoretically feasible [69]. Since there is no fundamental limitation on dimension if the wavelength DOF is adopted, we also use this paradigm for quantum channel characterization in OAM QKD of higher ($d > 3$) dimensions.

First, we compare the QKD performances achieved with and without the quantum channel conjugation under the ideal circumstances in Sec. IV B. We find that, with the help of the quantum channel conjugation, positive (and improved) secret key rates can be achieved by OAM QKD of all considered dimensions at all considered satellite altitudes under all considered zenith angles. We also find that the use of smaller OAM numbers leads to a higher secret key rate. For two-dimensional and three-dimensional OAM QKD, this means a smaller l_0 value leads to better performance. For OAM QKD of dimensions larger than 3, this means using OAM numbers as small as possible to construct the encoding subspace leads to a better performance. Comparing the performances achieved by OAM QKD of different dimensions, we find that an increased dimension can improve the performance of OAM QKD over the satellite-to-earth channel when the quantum channel conjugation is applied. This observation holds under both $\theta_z = 0^\circ$ and $\theta_z = 45^\circ$ (results not shown). Specifically, we find that five-dimensional OAM QKD achieves the highest performance at $H \geq 300$ km under $\theta_z = 0^\circ$. Under $\theta_z = 45^\circ$, three-dimensional OAM QKD achieves the highest performance at $H \geq 250$ km.

Then, we adopt the settings in Sec. IV C 3 and evaluate the performance of OAM QKD achieved with the quantum channel conjugation under the realistic circumstance where a sea-level (i.e., $h_0 = 0$ m) ground station and a reasonably sized (i.e., $r_a = 1$ m) receiver aperture is used. We find that, with the help of the quantum channel conjugation, positive secret key rates can be achieved by OAM QKD of all considered dimensions. Such an

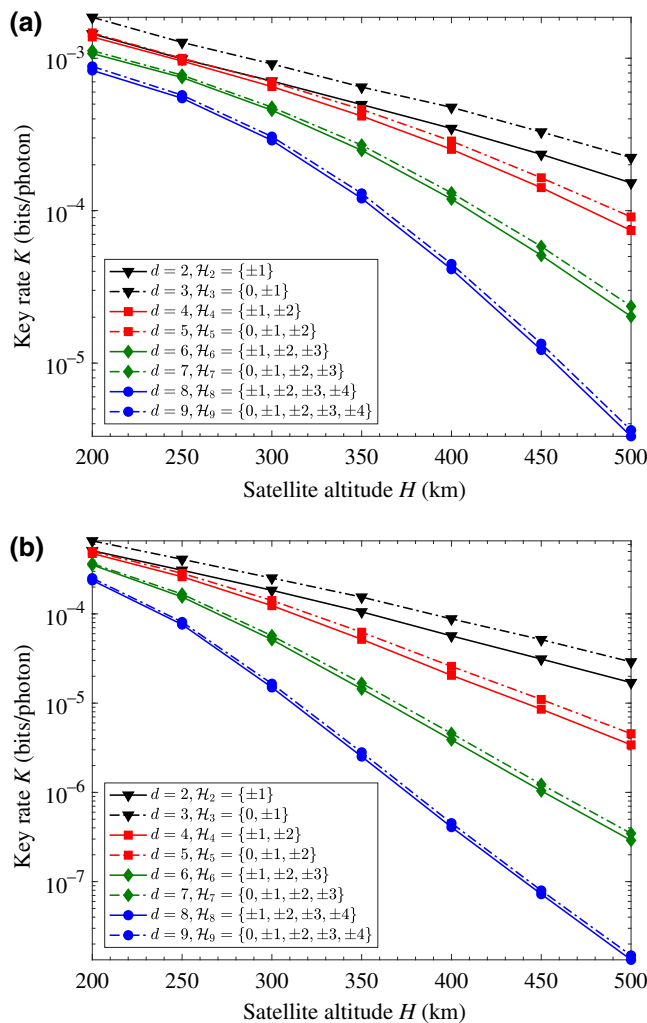


FIG. 7. Performances of satellite-to-earth OAM QKD of different dimensions achieved with the quantum channel conjugation. These results are achieved with $r_a = 1$ m, under $h_0 = 0$ m, and under (a) $\theta_z = 0^\circ$ and (b) $\theta_z = 45^\circ$. A specific encoding subspace \mathcal{H}_d is chosen to maximize the key rate for each dimension d .

observation not only holds under $\theta_z = 0^\circ$, but also holds under $\theta_z = 45^\circ$ (where a higher loss and more severe turbulence effect is anticipated). Specifically, in Fig. 7 we present the QKD performances achieved with the quantum channel conjugation under $\theta_z = 0^\circ$ and $\theta_z = 45^\circ$. We first observe that the secret key rate becomes higher when the dimension of OAM QKD is increased by one via the inclusion of the $l = 0$ state in the encoding subspace (the same phenomenon can also be observed from Fig. 8). This is not only due to an increased dimension, but also due to an enhanced photon survival fraction resulting from the stability of the $l = 0$ state in turbulence (note that the enhanced photon survival fraction in turbulence provided by the inclusion of the $l = 0$ state has also been observed in Ref. [21]). From both subfigures, we can see that OAM

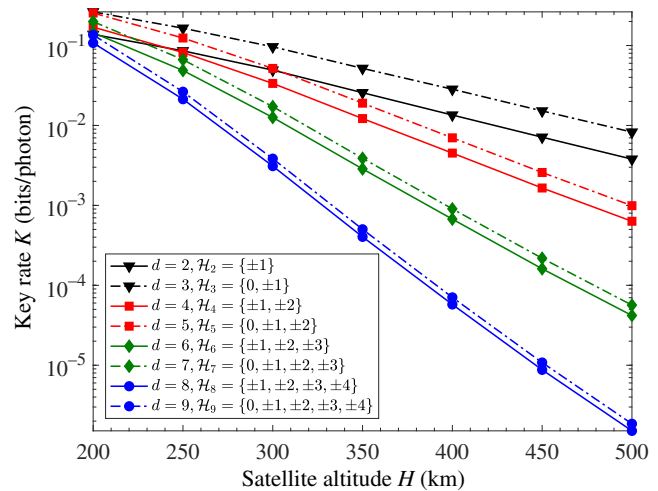


FIG. 8. Performances of satellite-to-earth OAM QKD of different dimensions achieved with the quantum channel conjugation. These results are achieved with $r_a = 1$ m, under $h_0 = 3000$ m and $\theta_z = 45^\circ$. A specific encoding subspace \mathcal{H}_d is chosen to maximize the key rate for each dimension d .

QKD of dimension 3 outperforms OAM QKD of all other considered dimensions.

Finally, we move to a better circumstance where a high-altitude ($h_0 = 3000$ m) ground station with a reasonably sized (i.e., $r_a = 1$ m) receiver aperture is used, and we evaluate the performance of OAM QKD achieved with the quantum channel conjugation. In Fig. 8 we plot the resulting QKD performances under $\theta_z = 45^\circ$. We first again find that the quantum channel conjugation leads to positive secret key rates for all dimensions at all considered satellite altitudes, and that three-dimensional OAM QKD achieves the highest QKD performance. Comparing the results in Figs. 8 and 7(b), we clearly see the significant performance improvements provided by a higher ground-station altitude.

According to the widely used HV model [recall Eq. (7)], the turbulence profile of a satellite-to-earth channel is determined by the ground-level turbulence strength A and the rms wind speed v_{rms} (we refer to these two parameters as the *turbulence conditions*). We have explored the feasibility of OAM QKD (with the help of the quantum channel conjugation) under a set of typical turbulence conditions (i.e., $A = 9.6 \times 10^{-14} \text{ m}^{-2/3}$ and $v_{\text{rms}} = 21$ m/s). However, it is useful to remark on how sensitive our results are to variations in these assumed conditions. As discussed in, e.g., Refs. [46,56], A mainly varies within the range 10^{-15} to $10^{-12} \text{ m}^{-2/3}$ and v_{rms} within the range 3 to 30 m/s. Sometimes $v_{\text{rms}} = 57$ m/s is used for stronger wind conditions (see, e.g., Ref. [78]).

We now pose the practically important question: *under what range of turbulence conditions does the practical feasibility of OAM QKD hold?* To answer this question, we

explore the feasibility of OAM QKD (with the quantum channel conjugation) under a wider range of turbulence conditions. We choose seven different A values ranging from 1×10^{-15} to $3 \times 10^{-12} \text{ m}^{-2/3}$ to represent weak to strong ground-level turbulence strengths. We also choose four typical v_{rms} values of 10, 21, 30, and 57 m/s to represent different moderate to strong wind speeds. In Fig. 9 we plot the performance of three-dimensional OAM QKD, achieved with the quantum channel conjugation, against the seven considered A values for the four considered v_{rms} values. The other settings are for a satellite altitude of 500 km, and a sea-level (i.e., $h_0 = 0 \text{ m}$) ground station with $r_a = 1 \text{ m}$ under $\theta_z = 45^\circ$. The considered three-dimensional OAM-QKD protocol utilizes the encoding subspace $\mathcal{H}_3 = \{-1, 0, 1\}$. From this figure we clearly observe that the secret key rate decreases as the ground-level turbulence strength A , or the rms wind speed v_{rms} , increases. However, the performance degradation caused by an increased v_{rms} value becomes negligible when A becomes large enough. We further observe that, although positive secret key rates can be achieved under all considered turbulence conditions, the secret key rate becomes effectively zero (too low to be useful, i.e., less than 10^{-6} bits/photon) when the ground-level turbulence strength A becomes larger than $1.8 \times 10^{-12} \text{ m}^{-2/3}$. We emphasize that no positive key rate can be achieved, without the help of the quantum channel conjugation, under any of the considered turbulence conditions in Fig. 9.

It should be noted that, despite the potential benefits, higher-dimensional OAM QKD is generally more resource intensive (and harder to carry out) in practice. In the EB implementation, the key resource (i.e., maximally OAM-entangled states) of a higher-dimensional OAM QKD is generally produced at a reduced rate (this is because the distribution of higher-order modes from the SPDC process is nonuniform; see, e.g., Ref. [12]). In the P&M implementation, the fast and precise generation of OAM-encoded MUB states in a higher-dimensional space could also be harder due to efficiency and computation issues (see, e.g., Ref. [24]). Additionally, although the near-perfect sorting of OAM-encoded MUBs has been made possible, a trade-off between dimension, acceptable levels of loss, separation efficiency, and optics complexity inevitably exists (see, e.g., Ref. [28]). Although all these practical issues do not directly compromise the security of OAM QKD, it is anticipated that the secret key rate will be scaled down mainly due to efficiency and complexity issues as the dimension increases.

On the other hand, our results indicate that, when the quantum channel conjugation is applied, a moderate dimension (e.g., $d = 3$) and an encoding subspace spanned by low-order OAM eigenstates (e.g., $\mathcal{H}_3 = \{-1, 0, 1\}$ for $d = 3$) are generally preferred in a typical satellite-to-earth OAM-QKD scenario. Furthermore, the recent seven-dimensional OAM-QKD experiment [32] implies use

of a moderate dimension should be practically feasible. Although a practical implementation under turbulence may be challenging and costly, we believe that the gain in the secret key rate should justify the rise in the implementation cost as long as a moderate dimension and an encoding subspace spanned by low-order OAM eigenstates are used.

In summary, the quantum channel conjugation leads to positive (and improved) secret key rates at all considered satellite altitudes under all considered zenith angles, even under loss and a low ground-station altitude of 0 m. The quantum channel conjugation also enables the theoretically predicted secret key rate advantage provided by an increased dimension in OAM QKD over the satellite-to-earth channel.

C. Additional noise contributions

We note that in our calculations we have assumed perfect tomography implemented in real time. Of course, in practice this perfect outcome can never be realized. The accuracy and timescale for implementation of any tomography are a function of the specific measurements pursued and the number of signals analyzed; see, e.g., Ref. [79]. However, given that the coherence timescale of the channel is of the order of a millisecond, and that we are using classical light as the probe (in effect no limit on the sample size), it could be anticipated that enough signals could be analyzed in real time providing infidelities between

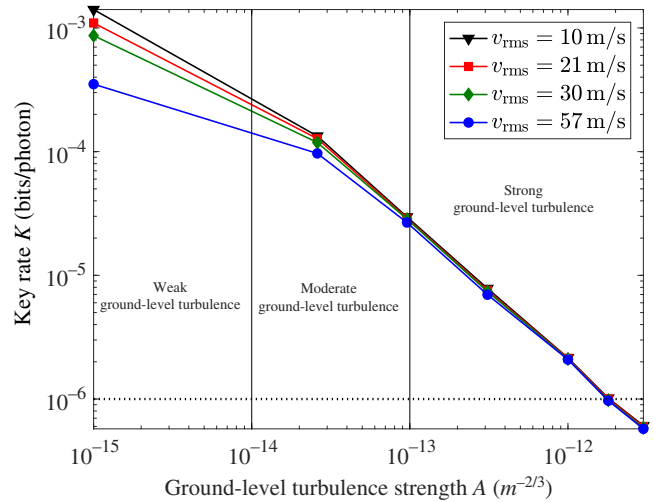


FIG. 9. Performance of three-dimensional satellite-to-earth OAM QKD achieved with the quantum channel conjugation, plotted against the ground-level turbulence strength A , for different rms wind speeds v_{rms} . The satellite altitude is fixed to $H = 500 \text{ km}$, and the results are achieved with $r_a = 1 \text{ m}$, under $h_0 = 0 \text{ m}$ and $\theta_z = 45^\circ$. The encoding subspace $\mathcal{H}_3 = \{-1, 0, 1\}$ is chosen to maximize the key rate. The dotted line indicates the key rate of 10^{-6} bits/photon. We consider a key rate less than 10^{-6} bits/photon to be too low to be useful, since a 100 MHz pulsed source results in less than 100 bits/second.

the true and reconstructed quantum states less than 5% [79]. The presence of tomography noise will manifest itself in our key rate calculations through the design of a conjugate filter targeted at a different (erroneous) state, which ultimately leads to the state produced possessing less than maximal entanglement. The error rate Q , therefore, becomes nonzero, which in turn impacts our final key rate [see Eq. (23)].

We also have assumed that our channel noise is entirely a consequence of phase perturbations and loss (the latter leading to vacuum contributions to the state). Although beam misalignment caused by turbulence-induced beam wander is negligible in the downlink from satellite to earth, direction tracking errors in the transmitter and/or receiver may also cause misalignment (recall that the satellite is in low orbit and moving across the sky in timescales of minutes). The presence of beam misalignment will lead to additional crosstalk in the received state, which will manifest itself in our key rate equations through a smaller survival fraction in the measurement process [see Eq. (24)].

In Fig. 10 we illustrate the impact on our final key rate as a function of the additional noise terms discussed above. Here, the performance of OAM QKD is shown for a dimension of 3, and with the noisy channel conjugation and misalignment in the beam applied [80]. The settings are for a satellite altitude of 500 km, and a sea-level ground station with $r_a = 1$ m under $\theta_z = 45^\circ$. The considered three-dimensional OAM-QKD protocol utilizes the encoding subspace $\mathcal{H}_3 = \{-1, 0, 1\}$. The losses are 2.7 and 7.4 dB to OAM eigenstates with OAM numbers

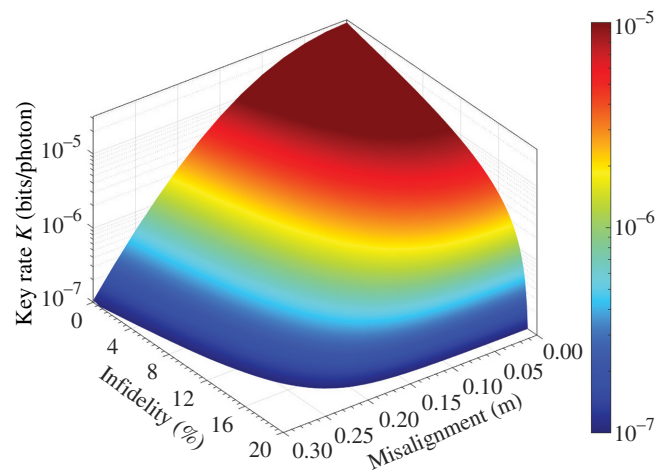


FIG. 10. Performance of three-dimensional satellite-to-earth OAM QKD achieved with the quantum channel conjugation, plotted against the channel conjugation error (in terms of infidelity) and misalignment. The satellite altitude is fixed to $H = 500$ km, and the results are achieved with $r_a = 1$ m, under $h_0 = 0$ m and $\theta_z = 45^\circ$. The encoding subspace $\mathcal{H}_3 = \{-1, 0, 1\}$ is chosen to maximize the key rate.

0 and 1, respectively. We can see that nonzero key rates can be found for a wide range of noise conditions. Beyond misalignment of 0.225 m or infidelity of 18% the key rate rapidly falls to less than 10^{-6} bits/photon. The region of nonzero key rates is at noise levels within current experimental reach. Note that other detector noise components not explicitly mentioned, such as shot noise, dark counts, and losses, are anticipated to be small relative to real-world misalignment noise; see, e.g., Ref. [81]. Any additional detector noise can be readily mapped to an equivalent misalignment error of Fig. 10. Recall that the classical signal is to be set by the system at much stronger intensity than the quantum signal. As such, most additional detector noise components can be made to have an impact on QKD rates well below the impact caused by a 0.05 m misalignment error.

It should be noted that the quantum channel conjugation investigated in this work is not the only technique that can aid satellite-to-earth OAM QKD. It has been shown that AO techniques could improve the performance of OAM-based entanglement distribution in FSO channels (see, e.g., Refs. [20,21]). AO techniques use a nonentangled classical light source as a probe, and their ability to negate turbulence heavily depends on the number of movable elements used for the required receiver-mirror deformation. But we note that phase perturbations across the transverse plane of the beam, when coupled to diffraction, lead to scintillation, and this cannot be completely negated by AO techniques. However, it is certainly the case that AO applied before any channel conjugation will only lead to improvement in the above results, particularly with regard to corrections of beam wander and direction tracking. No report on the actual use of AO within the context of OAM entanglement distribution through long FSO channels is currently available. In practice, we anticipate the channel conjugation method used here will lead to better negation of the atmospheric turbulence relative to AO, if either technique is used on its own. However, further research on the coupling of quantum channel conjugation and advanced AO techniques may prove fruitful.

VI. CONCLUSIONS

The OAM of light has been considered as a promising DOF that gives access to a higher-dimensional Hilbert space, leading to potential higher capacity quantum communications. In this work we explore the feasibility of performing satellite-to-earth QKD utilizing the OAM of light. Specifically, we numerically investigate the performances of OAM QKD of different dimensions achieved with different OAM numbers at different satellite altitudes H under different zenith angles θ_z . We find that utilizing the OAM of light in satellite-to-earth QKD is indeed feasible between a LEO satellite and a high-altitude ground station.

First, we consider an ideal circumstance where a high-altitude ground station with a large receiver aperture (no loss) is used. We then move to less ideal circumstances and discuss the feasibility of satellite-to-earth OAM QKD under loss and a lower ground-station altitude. However, we find that no positive secret key rate can be achieved at a sea-level ground station when a reasonably sized aperture is used. We then explore the use of quantum channel information as a means to improve the feasibility of satellite-to-earth OAM QKD. We assume that such information is acquired through a real-time quantum channel characterization utilizing nonseparable states of classical light, and we use this information to perform a quantum channel conjugation at the ground station. We find that the quantum channel conjugation significantly improves the feasibility of OAM QKD, and leads to positive secret key rates even under circumstances where a sea-level ground station with a reasonably sized aperture is used. We also find that the quantum channel conjugation enables a key rate advantage (provided by the higher dimensions of OAM QKD) to be realized.

ACKNOWLEDGMENTS

We thank the four anonymous referees whose comments significantly improved the presentation of this paper.

APPENDIX: CHANNEL MODELING

To perform the split-step method we divide the satellite-to-earth atmospheric channel into N_S slabs bounded by specific altitudes h_j with j ranging from 1 to N_S (note that h_0 is the ground-station altitude, and a larger j indicates a higher altitude). For the j th ($j \geq 1$) slab bounded by h_j and h_{j-1} , its thickness can be estimated as $\Delta L_j = (h_j - h_{j-1}) / \cos(\theta_z)$ (note that $\sum_j \Delta L_j = L$). In order to characterize the turbulence within each slab, both σ_I^2 and r_0 are evaluated locally (for the turbulent volume of their corresponding slab). We denote the scintillation index and the Fried parameter for the j th slab as $\sigma_{I_j}^2$ and r_{0_j} , respectively. To accurately model the atmospheric channel using multiple slabs with a phase screen located in the midway of each slab, we meet the two conditions described in Ref. [47] (i.e., $\sigma_{I_j}^2 < 0.1$ and $\sigma_{I_j}^2 < 0.1\sigma_I^2$) by setting N_S and h_j through a numerical search. A schematic illustration of our channel modeling (with $N_S = 6$) is provided in Fig. 1(b). In our simulations N_S ranges from 6 to 17 depending on specific settings.

After determining the widths of the atmospheric slabs, the realizations of the corresponding phase screens are generated using the fast-Fourier-transform (FFT)-based spectral domain algorithm [82]. This method involves the filtering of a complex Gaussian random field using the phase power spectral density (PSD) function of the atmospheric turbulence. In this paper, we adopt the modified

von Karman model, giving the phase PSD function for the j th slab

$$\Phi_{\phi_j}^{\text{mvK}}(f) = 0.023r_{0_j}^{-5/3} \frac{\exp(-f^2/f_m^2)}{(f^2 + f_0^2)^{11/6}}, \quad (\text{A1})$$

where f is the magnitude of the two-dimensional spatial frequency vector in the transverse plane in cycles/ m , $f_0 = 1/L_{\text{outer}}$, and $f_m = 0.9422/l_{\text{inner}}$ [49].

For the free-space propagation, we utilize the FFT-based angular spectrum method (for details of this method, we refer the reader to, e.g., Refs. [49,83]). In this study we utilize a physical optics propagation library named PROPER [84] to perform this method.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Bangalore, India, 1984).
 - [2] S.-K. Liao, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
 - [3] J. Yin, Satellite-To-Ground Entanglement-Based Quantum key Distribution, *Phys. Rev. Lett.* **119**, 200501 (2017).
 - [4] S.-K. Liao, Satellite-Relayed Intercontinental Quantum Network, *Phys. Rev. Lett.* **120**, 030501 (2018).
 - [5] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [6] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with six States, *Phys. Rev. Lett.* **81**, 3018 (1998).
 - [7] M. Bourennane, A. Karlsson, and G. Björk, Quantum key distribution using multilevel encoding, *Phys. Rev. A* **64**, 012306 (2001).
 - [8] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, Quantum key distribution using multilevel encoding: Security analysis, *J. Phys. A: Math. Gen.* **35**, 10065 (2002).
 - [9] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum key Distribution Using d -Level Systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
 - [10] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, *Phys. Rev. A* **82**, 030301 (2010).
 - [11] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, *Phys. Rev. A* **85**, 052310 (2012).
 - [12] A. Vaziri, G. Weihs, and A. Zeilinger, Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication, *Phys. Rev. Lett.* **89**, 240401 (2002).
 - [13] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes, *Phys. Rev. A* **45**, 8185 (1992).
 - [14] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Entanglement of the orbital angular momentum states of photons, *Nature* **412**, 313 (2001).
 - [15] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities, *Nat. Phys.* **7**, 677 (2011).

- [16] N. D. Leonhard, V. N. Shatokhin, and A. Buchleitner, Universal entanglement decay of photonic-orbital-angular-momentum qubit states in atmospheric turbulence, *Phys. Rev. A* **91**, 012345 (2015).
- [17] A. Hamadou Ibrahim, F. S. Roux, M. McLaren, T. Konrad, and A. Forbes, Orbital-angular-momentum entanglement in turbulence, *Phys. Rev. A* **88**, 012312 (2013).
- [18] F. S. Roux, T. Wellens, and V. N. Shatokhin, Entanglement evolution of twisted photons in strong atmospheric turbulence, *Phys. Rev. A* **92**, 012326 (2015).
- [19] A. H. Ibrahim, F. S. Roux, and T. Konrad, Parameter dependence in the atmospheric decoherence of modally entangled photon pairs, *Phys. Rev. A* **90**, 052115 (2014).
- [20] N. Leonhard, G. Sorelli, V. N. Shatokhin, C. Reinlein, and A. Buchleitner, Protecting the entanglement of twisted photons by adaptive optics, *Phys. Rev. A* **97**, 012321 (2018).
- [21] G. Sorelli, N. Leonhard, V. N. Shatokhin, C. Reinlein, and A. Buchleitner, Entanglement protection of high-dimensional states by adaptive optics, *New J. Phys.* **21**, 023003 (2019).
- [22] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, Twisted photon entanglement through turbulent air across Vienna, *Proc. Natl. Acad. Sci. USA* **112**, 14197 (2015).
- [23] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, Twisted light transmission over 143 km, *Proc. Natl. Acad. Sci. USA* **113**, 13648 (2016).
- [24] E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram, *Opt. Lett.* **38**, 3546 (2013).
- [25] M. Mirhosseini, O. S. Magaña-Loaiza, C. Chen, B. Rodenburg, M. Malik, and R. W. Boyd, Rapid generation of light beams carrying orbital angular momentum, *Opt. Express* **21**, 30196 (2013).
- [26] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, Efficient separation of the orbital angular momentum eigenstates of light, *Nat. Commun.* **4**, 2781 (2013).
- [27] H. Larocque, J. Gagnon-Bischoff, D. Mortimer, Y. Zhang, F. Bouchard, J. Upham, V. Grillo, R. W. Boyd, and E. Karimi, Generalized optical angular momentum sorter and its application to high-dimensional quantum cryptography, *Opt. Express* **25**, 19832 (2017).
- [28] R. Fickler, F. Bouchard, E. Giese, V. Grillo, G. Leuchs, and E. Karimi, Full-field mode sorter using two optimized phase transformations for high-dimensional quantum cryptography, *J. Opt.* **22**, 024001 (2020).
- [29] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons, *Quantum* **2**, 111 (2018).
- [30] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, Experimental quantum cryptography with qutrits, *New J. Phys.* **8**, 75 (2006).
- [31] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, *Phys. Rev. A* **88**, 032305 (2013).
- [32] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, *New J. Phys.* **17**, 033033 (2015).
- [33] B. Ndagano and A. Forbes, Characterization and mitigation of information loss in a six-state quantum-key-distribution protocol with spatial modes of light through turbulence, *Phys. Rev. A* **98**, 062330 (2018).
- [34] S. K. Goyal, A. H. Ibrahim, F. S. Roux, T. Konrad, and A. Forbes, The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum, *J. Opt.* **18**, 064002 (2016).
- [35] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Free-Space Quantum key Distribution by Rotation-Invariant Twisted Photons, *Phys. Rev. Lett.* **113**, 060503 (2014).
- [36] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, High-dimensional intracity quantum cryptography with structured photons, *Optica* **4**, 1006 (2017).
- [37] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, Quantum cryptography with twisted photons through an outdoor underwater channel, *Opt. Express* **26**, 22563 (2018).
- [38] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rot-twitz, S. Ramachandran, and L. K. Oxenløwe, Orbital Angular Momentum States Enabling Fiber-Based High-Dimensional Quantum Communication, *Phys. Rev. Appl.* **11**, 064058 (2019).
- [39] Z. Wang, R. Malaney, and J. Green, in *2019 IEEE Global Communications Conference (GLOBECOM)* (IEEE, Waikoloa, Hawaii, United States, 2019).
- [40] Z. Wang, R. Malaney, and J. Green, in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)* (IEEE, Dublin, Ireland, 2020).
- [41] A. M. Yao and M. J. Padgett, Orbital angular momentum: Origins, behavior and applications, *Adv. Opt. Photon.* **3**, 161 (2011).
- [42] Similar to other works, here we restrict ourselves to the $p = 0$ subspace for simplicity. However, we do note that turbulence-induced crosstalk will also produce $p \neq 0$ modes. Intuitively, more initial signal could be retrieved by summing over the radial index p instead of performing a single projection onto the $p = 0$ subspace (as we have done in this work) for every OAM index at the receiver. In this sense, the results presented here can be considered as lower bounds on the key rates for the assumed noise levels.
- [43] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, A new proof for the existence of mutually unbiased bases, *Algorithmica* **34**, 512 (2002).

- [44] A. Klappenecker and M. Rötteler, in *Finite Fields and Applications*, edited by G. L. Mullen, A. Poli, and H. Stichtenoth (Springer, Berlin, Heidelberg, 2004).
- [45] C. Spengler and B. Kraus, Graph-state formalism for mutually unbiased bases, *Phys. Rev. A* **88**, 052323 (2013).
- [46] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation through Random Media* (SPIE, Bellingham, WA, 2005), 2nd ed.
- [47] J. M. Martin and S. M. Flatté, Intensity images and statistics from numerical simulation of wave propagation in 3-D random media, *Appl. Opt.* **27**, 2111 (1988).
- [48] A. Belmonte, Feasibility study for the simulation of beam propagation: Consideration of coherent lidar performance, *Appl. Opt.* **39**, 5426 (2000).
- [49] J. D. Schmidt, *Numerical Simulation of Optical Wave Propagation with Examples in MATLAB* (SPIE, Bellingham, WA, 2010).
- [50] Note that the most general form of the wind speed profile includes an additional velocity term, which is related to the slew rate that is associated with a satellite moving with respect to the ground station. The slew rate becomes important in making temporal calculations [46]. Since all the calculations are time independent in this work, here we follow the common practice and drop the slew-rate-related velocity term.
- [51] B. Rodenburg, M. Mirhosseini, M. Malik, O. S. Magaña-Loaiza, M. Yanakas, L. Maher, N. K. Steinhoff, G. A. Tyler, and R. W. Boyd, Simulating thick atmospheric turbulence in the lab with application to orbital angular momentum communication, *New J. Phys.* **16**, 033020 (2014).
- [52] J. A. Anguita, M. A. Neifeld, and B. V. Vasic, Turbulence-induced channel crosstalk in an orbital angular momentum-multiplexed free-space optical link, *Appl. Opt.* **47**, 2414 (2008).
- [53] We later show in Sec. V A that, with channel information available, Bob can adopt a different choice of O , giving a different form of $|\Phi_{ps}\rangle$.
- [54] Note here the key rate is per photon actually used in the key generation. For every photon sent (transmitted), it can be “lost” either by not hitting the receiver, or by not being postselected via the projection operation. The parameter T states the fraction of sent photons that survive both these loss events. Effectively, the finite-sized receiver aperture is absorbed into the postselection process.
- [55] Note that the path elongation due to the spatial variability of the refractive index is ignored in this work. We expect the path elongation factor to be very close to 1 in all our considered scenarios [85].
- [56] Y. Guo, C. Xie, P. Huang, J. Li, L. Zhang, D. Huang, and G. Zeng, Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution, *Phys. Rev. A* **97**, 052326 (2018).
- [57] For simplicity, we set the inner scale and the outer scale to fixed values. The 1 cm inner scale adopted is a value commonly used (see, e.g., Ref. [86]). We choose the 5 m outer scale since some empirical profiles indicate that typical values for this are less than or equal to 5 m for slant atmospheric channels (see, e.g., Refs. [85,87]). Note that sometimes the outer scale in a real-world scenario might not perfectly agree with the empirical profiles. A larger outer scale will generally lead to a degraded performance (see, e.g., degraded entanglement in Ref. [88]). However, the main conclusions of this work should still hold for larger outer scales (e.g., 10–100 m).
- [58] S. Magnitskiy, D. Frolovstev, V. Firsov, P. Gostev, I. Protosenko, and M. Saygin, A SPDC-based source of entangled photons and its characterization, *J. Russ. Laser Res.* **36**, 618 (2015).
- [59] In this work we assume a clear-sky condition, and neglect any losses caused by absorption and scattering. Such losses are strongly wavelength dependent, and can be substantially mitigated by an appropriate choice of the communication wavelength (note that our choice of 1064 nm lies within the atmospheric transmission window). Within this transmission window, the small remnant absorption and scattering losses present will not significantly affect our results.
- [60] Note that the spatial resolution (i.e., the grid spacing in the transverse plane) could be adaptively varied along the propagation path to minimize numerical errors in FFT-based wave propagation methods [49]. However, in this work we fix the spatial resolution throughout the simulation. To validate this, we perform a vacuum propagation over the length of the channel and compare the resulting simulated beam profile with an independently derived analytical profile at the same channel distance. Such a test is performed for all considered channel distances and for LG beams with all considered OAM numbers, and we find that all numerical errors are negligible. We also note that, when no phase modulation is set at the phase screens, our simulation results give $U_{\text{turb}}(L) = \mathbb{1}$.
- [61] R. G. Lane, A. Glindemann, and J. C. Dainty, Simulation of a Kolmogorov phase screen, *Waves in Random Media* **2**, 209 (1992).
- [62] When OAM QKD of dimension larger than 3 is involved in a performance comparison, for each dimension d , we choose a specific encoding subspace \mathcal{H}_d that maximizes the key rate.
- [63] M. J. Padgett, F. M. Miatto, M. P. J. Lavery, A. Zeilinger, and R. W. Boyd, Divergence of an orbital-angular-momentum-carrying beam upon propagation, *New J. Phys.* **17**, 023011 (2015).
- [64] Considering the fact that an increased OAM number leads to a larger beam size, one might be concerned that this property might lead to additional side-channel information leakage and thus might compromise the security of OAM QKD. However, it can be shown that Eve cannot, in principle, gain any information by utilizing such a property (see related discussions in, e.g., Ref. [32]).
- [65] J. Zhao, M. Mirhosseini, B. Braverman, Y. Zhou, S. M. Hashemi Rafsanjani, Y. Ren, N. K. Steinhoff, G. A. Tyler, A. E. Willner, and R. W. Boyd, Performance analysis of d -dimensional quantum cryptography under state-dependent diffraction, *Phys. Rev. A* **100**, 032319 (2019).
- [66] I. L. Chuang and M. A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box, *J. Mod. Opt.* **44**, 2455 (1997).
- [67] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O’Brien, M. A. Nielsen, and A. G. White, Ancilla-Assisted Quantum Process Tomography, *Phys. Rev. Lett.* **90**, 193601 (2003).

- [68] B. Ndagano, B. Perez-Garcia, F. S. Roux, M. McLaren, C. Rosales-Guzman, Y. Zhang, O. Mouane, R. I. Hernandez-Aranda, T. Konrad, and A. Forbes, Characterizing quantum channels with non-separable states of classical light, *Nat. Phys.* **13**, 397 (2017).
- [69] C. M. Mabena and F. S. Roux, High-dimensional quantum channel estimation using classical light, *Phys. Rev. A* **96**, 053860 (2017).
- [70] C. M. Mabena and F. S. Roux, Quantum channel correction with twisted light using compressive sensing, *Phys. Rev. A* **101**, 013807 (2020).
- [71] E. Toninelli, B. Ndagano, A. Vallés, B. Sephton, I. Nape, A. Ambrosio, F. Capasso, M. J. Padgett, and A. Forbes, Concepts in quantum state tomography and classical implementation with intense light: A tutorial, *Adv. Opt. Photon.* **11**, 67 (2019).
- [72] We assume that the classical light is made orthogonal to the quantum signal using polarization or wavelength multiplexing techniques. For example, if the polarization (wavelength) DOF is used to construct the nonseparable state in Eq. (25), the wavelength (polarization) DOF should be used for multiplexing. We note that the turbulence effect on a propagating beam is wavelength dependent, and this can potentially cause errors in quantum channel characterization. For simplicity, we assume that the wavelengths used for multiplexing and for constructing the nonseparable state are chosen to be close enough to the wavelength of the quantum signal. Under such an assumption, the wavelength-dependent nature of the turbulence effect becomes negligible (see the discussions in, e.g., Ref. [69]).
- [73] One can show that directly applying M^{-1} leads to a *noiseless amplification*. Such an operation is *not* allowed in a deterministic fashion by the no-cloning theorem.
- [74] A. Vaziri, J.-W. Pan, T. Jennewein, G. Weihs, and A. Zeilinger, Concentration of Higher Dimensional Entanglement: Qutrits of Photon Orbital Angular Momentum, *Phys. Rev. Lett.* **91**, 227902 (2003).
- [75] L. X. Chen and Q. P. Wu, High-dimensional entanglement concentration of twisted photon pairs, *Laser Phys. Lett.* **9**, 759 (2012).
- [76] Z. Zhu, D. Hay, Y. Zhou, A. Fyffe, B. Kantor, G. S. Agarwal, R. W. Boyd, and Z. Shi, Single-Shot Direct Tomography of the Complete Transverse Amplitude, Phase, and Polarization Structure of a Light Field, *Phys. Rev. Appl.* **12**, 034036 (2019).
- [77] C. Rosales-Guzmán, B. Ndagano, and A. Forbes, A review of complex vector light fields and their applications, *J. Opt.* **20**, 123001 (2018).
- [78] 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).
- [79] A. Youssry, C. Ferrie, and M. Tomamichel, Efficient online quantum state estimation using a matrix-exponentiated gradient method, *New J. Phys.* **21**, 033006 (2019).
- [80] The effect of misalignment is modeled as a deterministic misalignment operator acting on Bob's photon before the quantum channel conjugation. In other words, the magnitude (ranging from 0 to 0.3 m) and direction (fixed at $+45^\circ$) of misalignment are constant under all channel realizations. The effect of a noisy channel conjugation is modeled as a deterministic depolarizing channel acting on Bob's photon after a perfect quantum channel conjugation, and the infidelity of such a depolarizing channel is used to quantify the channel conjugation error. However, we point out that any practical correction system can only work within a finite-dimensional subspace, any turbulence-induced crosstalk into the space outside such a subspace is not probed and is essentially converted into photon loss. We recognize our modeling of additional noise terms will not be an exact match to the real-world noise contributions.
- [81] S. Kish, E. Villaseñor, R. Malaney, K. Mudge, and K. Grant, Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel, *Quantum Engineering* **2**, e50 (2020).
- [82] B. L. McGlamery, Restoration of turbulence-degraded images, *J. Opt. Soc. Am.* **57**, 293 (1967).
- [83] J. W. Goodman, *Introduction to Fourier Optics* (McGraw-Hill, New York, 1996), 2nd ed.
- [84] J. E. Krist, in *Optical Modeling and Performance Predictions III*, edited by M. A. Kahan, International Society for Optics and Photonics (SPIE, San Diego, California, United States, 2007), Vol. 6675, p. 66750P.
- [85] D. Vasylyev, W. Vogel, and F. Moll, Satellite-mediated quantum atmospheric links, *Phys. Rev. A* **99**, 053830 (2019).
- [86] A. Belmonte, Coherent return turbulent fluctuations in ground lidar systems profiling along slant paths, *Opt. Express* **13**, 9598 (2005).
- [87] C. E. Coulman, J. Vernin, Y. Coqueugniot, and J. L. Caccia, Outer scale of turbulence appropriate to modeling refractive-indexstructure profiles, *Appl. Opt.* **27**, 155 (1988).
- [88] X. Yan, P. F. Zhang, J. H. Zhang, H. Q. Chun, and C. Y. Fan, Decoherence of orbital angular momentum tangled photons in non-Kolmogorov turbulence, *J. Opt. Soc. Am. A* **33**, 1831 (2016).