Retraction

Retraction: The A Satellite-to-Ground Quantum Key Distribution Protocol Based on Orbital Angular Momentum of Light (J. Phys.: Conf. Ser. 1757 012173)

Sheng Wang¹, Yu Lin¹, Xun Ye¹, Tianbing Zhang²,³, Bao Feng²,³,⁎ and Xiang Bian Yu²,³

¹ State Grid Fujian Electric Power Information & Telecommunication Co., Ltd, Fuzhou 350003
² NARI information communication technology Co., Ltd, Nanjing 211000, China
³ NRGD Quantum CTEK, LTD, Nanjing 211000, China

Published 23 April 2021

IOP Publishing Limited ("IOPP") is retracting this paper following an investigation which has confirmed this work has significant overlap with a preprint written by another author group, without permission or acknowledgement to the original authors. IOP Publishing Limited request any citations to this article be redirected to the original work [1].

IOPP have made multiple attempts to contact the author but has not received a response. The author is encouraged to contact jpconf@ioppublishing.org.

[1] Wang Z, Malaney R and Burnett B 2020 https://arxiv.org/abs/2007.07748

Retraction published: 23 April 2021
The A Satellite-to-Ground Quantum Key Distribution Protocol Based on Orbital Angular Momentum of Light

Sheng Wang¹, Yu Lin¹, Xun Ye¹, Tianbing Zhang²,³, Bao Feng²,³*, Yu XiangBian²,³

¹State Grid Fujian Electric Power Information & Telecommunication Co., Ltd, Fuzhou 350003
²NARI information communication technology Co., Ltd, Nanjing 211000, China
³NRGD Quantum CTEK, LTD, Nanjing 211000, China

*1nrgd_lw@163.com

Abstract. The orbital angular momentum (OAM) of light has been considered as a promising degree of freedom (DoF) that gives access to a higher-dimensional Hilbert space, which may lead to potential higher capacity quantum communications. Due to the fragility of the OAM state, the traditional view is that turbulence will make OAM-QKD infeasible in satellite-to-ground channels. However, based on the detailed phase screen simulations of the expected atmospheric turbulence, we find that quantum key distribution (QKD) using OAM of the light is feasible in certain system configurations, especially if quantum channel information is utilized in the processing of post-selected states. Therefore, we propose a satellite-to-ground quantum key distribution protocol based on the orbital angular momentum of the light, which uses the principle that OAM-QKD can only be used in high-altitude ground stations with larger receiver apertures without using classic optical probes. At the same time, the classically entangled light is used as a probe of the quantum channel and reasonably-sized transmitter-receiver apertures are also employed. Numerical simulation results show that this protocol can lead to positive secret key rates even under circumstances where a sea-level ground station with a reasonable-sized aperture is used. We also found that quantum channel conjugation enables a key rate advantage provided by the higher dimensions of the protocol to be realized.

Keywords: Satellite-to-ground, Quantum Key Distribution, Orbital Angular Momentum

1. 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[2] have pointed the way towards global-scale and highly-secure quantum communication networks [3]. The originally proposed QKD protocols [1] mainly utilize 2-dimensional encoding. However, other QKD protocols have been generalized to the case of high-dimensional encoding [4], and their unconditional security has been proved[5]. Quantum information can be encoded in any degree of freedom (DoF) of the photon, but most of the mainstream implementations of QKD [2, 3] rely on polarization encoding - a typical 2-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. Unlike the polarization of light, the OAM of light can take arbitrary integer values. The corresponding OAM eigenstates form an orthonormal basis that allows for quantum coding within a theoretically infinite-dimensional Hilbert space, opening up new 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 [6]. The distribution of OAM-encoded entanglement through the turbulent atmosphere has been intensively investigated in terrestrial free-space optical (FSO) channels with some demonstrating distribution over 3 km. A recent experiment suggests that OAM entanglement distribution could be feasible over an FSO channel of more than 100 km [7]. Implementations of OAM-QKD have been demonstrated in laboratory conditions with 2-dimensional [8] and higher-dimensional [9] encoding. Considering other types of medium, OAM-QKD has also been demonstrated over a 3 m underwater link and a 1.2 km optical fiber. 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. Previously we have studied the OAM detection performance in satellite-to-ground communications [10], and the feasibility of OAM-based entanglement distribution via satellite [11]. In this work, we propose a satellite-to-ground quantum key distribution protocol based on the orbital angular momentum of the light. 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-ground 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-ground OAM-QKD is confined to large telescopes situated at high-altitude observatories.

2. Background

2.1. Choice of mutually unbiased bases

Under Two orthonormal bases, \( M_1 = \{ |\phi_{1,i}\rangle, i = 0,1,...,d-1 \} \) and \( M_2 = \{ |\phi_{2,j}\rangle, j = 0,1,...,d-1 \} \), of a \( d \)-dimensional Hilbert space \( \mathcal{H}_d \), are said to be mutually unbiased if, and only if, all pairs of basis vectors \( |\phi_{1,i}\rangle \) and \( |\phi_{2,j}\rangle \) satisfy

\[
\left| \langle \phi_{2,j} | \phi_{1,i} \rangle \right|^2 = \frac{1}{d}.
\]

The smallest prime dimension is 2, and for that, an example of a complete set of MUBs consists of the eigenstates of the three Pauli spin operators \( s_x, s_y, s_z \), i.e.,

\[
\{ |0\rangle, |1\rangle \};
\]

\[
\left\{ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right\};
\]

\[
\left\{ \frac{1}{\sqrt{2}} (|0\rangle + i |1\rangle), \frac{1}{\sqrt{2}} (|0\rangle - i |1\rangle) \right\}.
\]

Pauli operators can be generalized to a higher dimension, known as the Weyl operators. These are unitary operators of the form \( X^k Z^l \) for \( k,l \in \{0,1,...,d-1\} \). The operator \( Z \) is diagonal in the standard basis \( \{ |0\rangle, |1\rangle, ..., |d-1\rangle \} \),
\[ Z = \sum_{j=0}^{d-1} \omega^j |j\rangle \langle j| \]  

(5)

with \( \omega = \exp(i2\pi / d) \), whereas the operator \( X \) reads

\[ X = \sum_{j=0}^{d-1} |j+1 \text{mod} d\rangle \langle j| \]  

(6)

The eigenbases belonging to the different operators in the set \( \{Z, X^Z, X \} \) \text{ for } \{0, 1, \ldots, d-1\} \text{ form a complete set of MUBs for any prime number } d \text{ as the dimension of the underlying Hilbert space. For } d = 3 \text{, our choice of the standard basis corresponds to Laguerre-Gaussian (LG) modes with OAM values } l = -1, 0, 1:

\[ |l\rangle = \begin{cases} 1, & |0\rangle, \quad |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \\ 0, & |1\rangle, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}. \end{cases} \]  

(7)

The remaining three bases are given in matrix notation with respect to the standard basis as

\[ \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \]

\[ \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \]

\[ \frac{1}{\sqrt{3}} \begin{pmatrix} \omega & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega^2 & \omega & 1 \end{pmatrix}. \]  

(8)

Examples of the LG modes and their super-positions are given in Fig. 1, which contains images of the measurement holograms and their corresponding intensity profiles. The first row represents the standard basis as given by Eq. (7), while rows 2–4 show the remaining three bases for \( d = 3 \), as given by Eq. (8).

2.2. Optical propagation through turbulent atmosphere

Turbulence in the Earth’s atmosphere is caused by random fluctuations in temperature and pressure. These variations alter the air’s refractive index both spatially and temporally, distorting any optical waves propagating through the atmosphere. In Kolmogorov’s [12] theory the turbulence is induced by eddies in the atmosphere characterized by an inner-scale \( l_s \), and an outer-scale \( L_s \). When using beam propagation to quantify atmospheric turbulence, a useful quantity is the scintillation index \( (s^2) \), defined as the normalized variance of the irradiance fluctuations,

\[ \sigma^2 = \frac{\left\langle I(x_0, y_0)^2 \right\rangle}{\left\langle I(x_0, y_0)^2 \right\rangle} - 1, \]  

(9)
where $I(x_0, y_0)$ is the optical irradiance evaluated at a single point of the detector plane $D$, and the mean over all the measurements performed. While normally $\sigma^2$ is defined using a sole point, here we consider the total power $P$ over $D$,

$$P = \int_{x,y} |I(x,y)|^2 \, dx \, dy \quad (10)$$

where $I(x,y)$ is expressed in Cartesian coordinates.

To describe the fluctuations of the refractive index we use a spectral density function [13]

$$\Phi_{s}(\kappa) = 0.49 r_{0}^{-5/3} \exp\left(-\kappa^2 / \kappa_{s}^2\right) \left(\kappa^2 + \kappa_{s}^2\right)^{3/4} \quad (11)$$

with $\kappa$ the radial spatial frequency on a plane orthogonal to the propagation direction, $\kappa_{s} = 5.92 / L_0$, $\kappa_{s} = 2\pi / L_0$ and $r_{0}$ the Fried parameter for a propagation length $\Delta z$. In the case of a horizontal propagation path at ground level

$$r_{0} = \left(0.423k^2C_{s}^2(0)\Delta z\right)^{3/5} \quad (12)$$

with $C_{s}^2(0)$ the refractive index structure constant at ground level and $k$ the wavenumber.

To model the effects of the atmosphere over a propagating beam we use the phase screen model. The phase screen model consists of subdividing the atmosphere into regions of length $L_D$. For each region, the random phase changes of the beam are compressed into a thin phase screen, placed at the start of the propagation path, and the rest of the atmosphere is taken to have a constant refractive index. In order to simulate beam propagation, we use the software package PROPER [14], which is an optical propagation library capable of simulating the propagation of electromagnetic waves.

3. Satellite-to-ground QKD protocol based on orbital angular momentum

Throughout this work, we denote the satellite and the ground station as Alice and Bob, respectively. We describe the system settings for satellite-to-ground OAM-QKD which is illustrated in Fig.1. The ground-station altitude is denoted as $h_0$, the satellite zenith angle at the ground station is denoted as $\theta_s$, and the satellite altitude at $\theta_s = 0$ is denoted as $H$. The channel distance $L$ is given by $L = (H - h_0) / \cos \theta_s$. 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-ground OAM-QKD, in addition to all effects we consider.
In this section, we briefly introduce the procedures of a $d$-dimensional OAM-QKD protocol utilizing $N_s (N_s \geq 2)$ MUBs.

Step 1: State preparation 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. For a $d$-dimensional OAM-QKD protocol, Alice generates OAM-photon pairs, each pair being in the maximally entangled state

$$|\Phi_{\text{tot}}\rangle = \sum_{l=0}^{d-1} \frac{1}{\sqrt{d}} |l\rangle |l\rangle$$  \hspace{1cm} (13)$$

where $H_d$ is a $d$-dimensional encoding subspace. At the output, the quantum state shared between Alice and Bob before any measurement is given by

$$|\Phi_{\text{tot}}\rangle = (I \otimes U_{\text{sub}}(L))|\Phi_{\phi}\rangle = \sum_{l_1=0}^{d-1} \sum_{l_2=0}^{d-1} C_{l_1 l_2} \sqrt{d} |l_1\rangle |l_2\rangle$$  \hspace{1cm} (14)$$
where \( I \) denotes an identity operator acting on Alice’s photon, and \( H_\infty \) denotes an 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 \( |\Phi_{\text{out}}\rangle \) onto the original \( H_x \otimes H_y \) subspace. This procedure is realized by a post-selection at Bob’s side, giving a post-selected (and unnormalized) state

\[
|\Phi_p\rangle = (I \otimes O)|\Phi_{\text{out}}\rangle
\]

(15)

where \( O \) is the filtering operator acting on Bob’s photon. Since Bob has no information on \( U_{\text{out}}(L) \), his filtering operator \( Q = \Pi_x \) is equal to \( \sum_{j} |j\rangle\langle j| \). By setting \( Q = \Pi_x \) the post-selected state in Eq. (15) can be explicitly given as

\[
|\Phi_p\rangle = (I \otimes \Pi_x)|\Phi_{\text{out}}\rangle = \sum_{j} \sum_{l} \frac{1}{\sqrt{d}} |j\rangle |l\rangle |O_l\rangle.
\]

(16)

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

\[
\rho_{AB} = \langle \Phi_p | \Phi_p \rangle
\]

(17)

where \( \langle \cdot \cdot \rangle \) denotes an ensemble average, and \( = \text{tr}(\langle \Phi_p | \Phi_p \rangle) \) is the trace required for renormalization.

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

Step 3: Sifting 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.

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

\[
Q = \frac{1}{N_s} \sum_{s} \sum_{i,j} \text{tr}(|\xi(i,s)\rangle |\xi(i,s)\rangle \langle \xi(i,s) | \langle \xi(i,s) | \rho_{AB} \rangle.
\]

(18)

Step 5: Reconciliation and privacy amplification 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. For a \( d \)-dimensional QKD protocol utilizing all \( d+1 \) MUBs, the key length can be calculated as
\[ K_i = \log_2 d + \frac{d+1}{d} Q \log_2 \left( \frac{Q}{d(d-1)} \right) + \left( 1 - \frac{d+1}{d} Q \right) \log_2 \left( 1 - \frac{d+1}{d} Q \right) \]  

(19)

Recalling a non-unity photon survival fraction \( T \), the achievable secret key rate \( K \) is given by

\[ K = T \times K_i \]  

(20)

4. Performance evaluation

In this section, we numerically evaluate the performance of the satellite-to-ground OAM-QKD protocols analyzed in Section 3. We carry out Monte Carlo simulations to numerically evaluate the secret key rate \( K \). First, we generate 4000 independent realizations of the satellite-to-ground channel. For each channel realization we perform a series of atmospheric propagations using the split step method to obtain a realization of \( \psi_{\mu} \) as shown in Eq. (15). Afterward, realizations of \( \psi_{\mu} \) are used to obtain \( T \) and \( \rho_{\text{sat}} \) as Eq. (17). Then \( Q \) is evaluated from \( \rho_{\text{sat}} \) as Eq. (18), and \( K_i \) is then evaluated from \( Q \) as shown in Eq. (19). Finally, \( K \) can be evaluated using \( K_i \) and \( T \) as described in Eq. (20).

4.1. General settings

We restrict ourselves to the case of a low-Earth-orbit (LEO) satellite with a maximum satellite altitude \( H = 500 \text{ km} \). We consider two zenith angles, \( \theta_z = 0^\circ \) and \( \theta_z = 45^\circ \), giving a maximum channel distance of \( L \approx 500 \text{ km} \) and \( L \approx 700 \text{ km} \), respectively. Unless otherwise stated, when we refer to our results we will mean for all considered \( H \) values, i.e., from 200 km to 500 km, and for all considered \( \theta_z \) values, i.e., \( 0^\circ \) and \( 45^\circ \). Also, throughout this work QKD performances are compared at the same satellite altitudes under the same zenith angles.

For the atmospheric parameters, we set \( A = 9.6 \times 10^{-37} \text{ m}^{-2/3} \) which accords with a realistic setting [15]. We set \( V_g = 3 \text{ m/s} \), giving a value of \( \sigma_{\text{rms}} = 21 \text{ m/s} \). We set \( L_{\text{core}} = 5 \text{ m} \) and \( L_{\text{max}} = 1 \text{ cm} \) for the atmospheric turbulence [16]. For the optical parameters, we set \( \lambda = 1064 \text{ nm} \) in accord with existing entanglement sources [17] and set \( \sigma_{\theta} \) to 15 cm.

We perform all simulations using a numerical grid of \( 2048 \times 2048 \) points with a spatial resolution of 5 mm. In generating the random phase screens using the FFT-based method, 3 orders of subharmonics are added using this method [18] to accurately represent the low spatial frequency components contributed by large scale turbulent eddies.

4.2. Realistic circumstances

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

4.2.1. Loss

The main source of loss in a satellite-to-ground channel is diffraction loss. We set the radius of the receiver aperture \( r_\text{r} = 1 \text{ m} \). At \( H = 500 \text{ km} \) and under \( \theta_z = 0^\circ \), setting \( r_\text{r} = 1 \text{ m} \) gives losses of 1 dB, 3.4 dB, 6.9 dB, 11.3 dB, 16.7 dB to OAM eigenstates with OAM numbers 0, 1, 2, 3, 4, respectively. We then re-evaluate the performances of 2-dimensional and higher-dimensional OAM-QKD. In Fig. 3 we compare the performances of 2- dimensional OAM-QKD, achieved with \( r_\text{r} = 1 \text{ m} \) (dashed) and \( r_\text{r} = 4 \text{ m} \) (solid), under \( \theta_z = 0^\circ \) and \( h_\text{g} = 3000 \text{ m} \). From this Fig, we see that the loss degrades the performance of 2-dimensional OAM-QKD, and such a performance degradation is more significant
for a larger $l_0$ value. At the same time, we also see that some curves end before reaching $H = 500\text{km}$ due to a zero key rate. This happens when the average error rate $Q$ surpasses the tolerable error rate.

Fig.3 Secret key rates $K$ of 2-dimensional satellite-to-ground OAM-QKD

Higher-dimensional OAM-QKD is more sensitive to loss. For 3-dimensional OAM-QKD, after setting $r_s = 1\text{m}$ we find that no positive key rate can be achieved at $H > 300\text{km}$ under $\theta_i = 0^\circ$. For OAM-QKD of dimensions larger than 3, setting $r_s = 1\text{m}$ we find that no positive key rate can be achieved at $H > 250\text{km}$. Comparing the performances of OAM-QKD of different dimensions under loss, we find that 2-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 [19].

4.2.2. Sea-level receiver with reasonably-sized aperture

Then we adopt all settings of Section 4.1 and jointly set $r_s = 1\text{m}$ and $h_q = 0\text{m}$ 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 $\theta_i = 0^\circ$.

4.3. QKD performance with quantum channel conjugation

To numerically investigate the impact of the quantum channel conjugation on QKD performance, we adopt the settings of Sections 4.1 and re-evaluate the performances of satellite-to-ground OAM-QKD of different dimensions. In 2-dimensional OAM-QKD, we assume that the vector vortex beam is used for quantum channel characterization. Specifically, the non-separable states of classical light we use for channel characterization is given in the general form
where \(|R\rangle, |L\rangle\) denote right and left circular polarization states, respectively. In 3-dimensional OAM-QKD, the vector vortex beam cannot be used due to the constraint of the 2-dimensional Hilbert space imposed by the polarization DoF. Specifically, Eq. (21) is explicitly given by

\[
\Phi_0^c = \frac{1}{\sqrt{2}} (|R\rangle |l_0\rangle + |L\rangle |l_0\rangle)
\]

(22)

where \(\lambda_m\) denote different wavelengths. 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 Section 4.2. 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 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 2-dimensional and 3-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 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-ground channel when the quantum channel conjugation is applied. Specifically, we find that 5-dimensional OAM-QKD achieves the highest performance at \(H \geq 300\) km under \(\theta_z = 0^\circ\). Under \(\theta_z = 45^\circ\), 3-dimensional OAM-QKD achieves the highest performance at \(H \geq 250\) km.

Then, we adopt the settings in Section 4.2 and evaluate the performance of OAM-QKD achieved with the quantum channel conjugation under the realistic circumstance where a sea-level ground station and a reasonably-sized 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 observation not only holds under \(\theta_z = 0^\circ\), but also holds under \(\theta_z = 45^\circ\). Specifically, in Fig. 4 we present the QKD performances achieved with the quantum channel conjugation under \(\theta_z = 45^\circ\). From this Fig., we can see that OAM-QKD of dimension 3 outperforms OAM-QKD of all other considered dimensions.
Fig. 4 Performances of satellite-to-ground OAM-QKD of different dimensions achieved with the quantum channel conjugation. These results are achieved with \( r_s = 1 \text{m} \), under \( h_0 = 0 \text{m} \) and \( \theta = 45^\circ \). A specific encoding subspace \( H_j \) is chosen to maximize the key rate for each dimension \( d \).

Fig. 5 Performances of satellite-to-ground OAM-QKD of different dimensions achieved with the quantum channel conjugation. These results are achieved with \( r_s = 1 \text{m} \), under \( h_0 = 3000 \text{m} \) and \( \theta = 45^\circ \). A specific encoding subspace \( H_j \) is chosen to maximize the key rate for each dimension \( d \).

Finally, we move to a better circumstance where a high-altitude (\( h_0 = 3000 \text{m} \)) ground station with a reasonably-sized receiver aperture is used, and we evaluate the performance of OAM-QKD achieved with the quantum channel conjugation. In Fig. 5 we plot the resulting QKD performances under...
$\theta = 45^\circ$. 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 3-dimensional OAMQKD achieves the highest QKD performance. Comparing the results in Fig. 5 and Fig. 4, we clearly see the significant performance improvements provided by a higher ground-station altitude.

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-ground channel.

5. Conclusion
The OAM of light has been considered as a promising DoF that gives access to a higher-dimensional Hilbert space, leading to potentially higher capacity quantum communications. In this work, we propose a satellite-to-ground quantum key distribution protocol based on the orbital angular momentum of the light. We numerically investigated the performances of OAM-QKD of different dimensions achieved with different OAM numbers at different satellite altitudes $H$ under different zenith angles $\theta$. We found that utilizing the OAM of light in satellite-to-ground QKD is indeed feasible between an LEO satellite and a high-altitude ground station.

First, we considered a realistic circumstance where a high-altitude ground station with a large receiver aperture (no loss) is used. We then discussed the feasibility of satellite-to-ground OAM-QKD under loss and a lower ground-station altitude and explored the use of quantum channel information as a means to improve the feasibility of satellite-to-ground OAM-QKD. We assumed such information is acquired through a real-time quantum channel characterization utilizing non-separable states of classical light, and we used this information to perform a quantum channel conjugation at the ground station. We found 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 reasonable-sized aperture is used. We also found that the quantum channel conjugation enables a key rate advantage provided by the higher dimensions of the protocol to be realized.

Of course, the protocol also has some flaws, such as the protocol is only correct in certain specific system settings. Next, we will improve the protocol in response to this problem.

6. Acknowledgments
The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work is support by Scientific Project of Fujian Electric Power Co., Ltd. of SGCC under Grant No. 52130M19000Y and National key R & D project under Grant No. 2018YFE0200603.

References
[1] Bennett C H and Brassard G 2020 Quantum cryptography: Public key distribution and coin tossing arXiv preprint arXiv: 2003 pp06-557
[2] Shengkai L, Wenqi C, Weiyue L, Liang Z, Yang L, Jigang R, Juan Y, Qi S, Yuan C, Zhengping L and et al 2017 Satellite-to-ground quantum key distribution Nature 549 pp 43-47
[3] Liao S K, Cai W Q, Handsteiner J and et al 2018 Satellite-relayed intercontinental quantum network Phys. Rev. Lett 120 pp03-501
[4] Bourennane M, Karlsson A and Bjork G 2001 Quantum key distribution using multilevel encoding Phys. Rev. A 64 pp012-306
[5] Bourennane M, Karlsson A and Gisin N 2002 Quantum key distribution using multilevel encoding: security analysis J. Phys. A: Math. Gen 35 pp10-65
[6] Mair A, Vaziri A and Weihs G 2001 Entanglement of the orbital angular momentum states of photons Nature 412 pp3-13
[7] Krenn M, Handsteiner J, Fink M, Fickler R, Ursin R, Malik M, and Zeilinger A 2016 Twisted light transmission over 143 km Proc. Natl. Acad. Sci. U.S.A 113 pp 13648-136485

[8] Bouchard, Frédéric, Heshami K, England, Duncan, Fickler, Robert, Boyd, Robert W, Englert and et al 2018 Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons Quantum 2 pp1-11

[9] Gröblacher S, Jennewein T, Vaziri A, Weihs G and Zeilinger A 2006 Experimental quantum cryptography with qutrits New J. Phys 8 p5

[10] Wang Z, Malaney R and Green J 2019 Detecting orbital angular momentum of light in satellite-to-ground quantum communications 2019 IEEE Global Communications Conf. (GLOBECOM) pp 1-6

[11] Wang Z, Malaney R and Green J 2020 Satellite-based entanglement distribution using orbital angular momentum of light 2020 IEEE International Conf. on Communications Workshops (ICC Workshops) pp 1-6

[12] Kolmogorov A N 1991 The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers Proc. Mathematical & Physical ences 434 pp 9-13

[13] Schmidt J D 2010 Numerical Simulation of Optical Wave Propagation with Examples in MATLAB SPIE press

[14] Krist J E 2007 PROPER: an optical propagation library for IDL. Proc. of SPIE - The Int. Society for Optical Engineering pp 66-75

[15] Ying G, Cailang X, Peng H, Jiawei L, Ling Z, Duan H, and Guihua Z 2018 Channel parameter estimation for satellite-to-submarine continuous-variable quantum key distribution Phys. Rev. A 97 pp26-523

[16] Belmonte A 2005 Coherent return turbulent fluctuations in ground lidar systems profiling along slant paths Opt. Express 13 pp95-98

[17] Magnitskiy S, Frolovtsev D, Firsov V, Gostev P, Protsenko I and Saygin M 2015 A SPDC-based source of entangled photons and its characterization J. Russ. Laser Res 36 pp6-18

[18] Lane R G, Glindemann A and Dainty J C 1992 Simulation of a Kolmogorov phase screen Waves in Random Media 2 pp9-20

[19] Jiapeng Z, Mohammad M, Boris B, Yiyu Z and Robert W B 2019 Performance analysis of d-dimensional quantum cryptography under state dependent diffraction Phys. Rev. A 100 pp19-323