Performance analysis of d-dimensional quantum cryptography under state-dependent diffraction

Jiapeng Zhao,[1,*] Mohammad Mirhosseini,[2] Boris Braverman,[3] Yiyu Zhou,[1] Seyed Mohammad Hashemi Rafsanjani,[1] Yongxiong Ren,[4] Nicholas K. Steinhoff,[5] Glenn A. Tyler,[5] Alan E. Willner,[4] and Robert W. Boyd[1,3]

[1]*The Institute of Optics, University of Rochester, Rochester, New York 14627, USA*
[2]*California Institute of Technology, Pasadena, California 91125, USA*
[3]*Department of Physics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5*
[4]*University of Southern California, Los Angeles, California 90007, USA*
[5]*The Optical Science Company, Anaheim, California 92806, USA*

(Received 18 December 2018; published 13 September 2019)

Standard protocols for quantum key distribution (QKD) require that the sender be able to transmit in two or more mutually unbiased bases. Here, we analyze the extent to which the performance of QKD is degraded by diffraction effects that become relevant for long propagation distances and limited sizes of apertures. In such a scenario, different states experience different amounts of diffraction, leading to state-dependent loss and phase acquisition, causing an increased error rate and security loophole at the receiver. To solve this problem, we propose a precompensation protocol based on preshaping the transverse structure of quantum states. We demonstrate, both theoretically and experimentally, that when performing QKD over a link with known, state-dependent loss and phase shift, the performance of QKD will be better if we intentionally increase the loss of certain states to make the loss and phase shift of all states equal. Our results show that the precompensated protocol can significantly reduce the error rate induced by state-dependent diffraction and thereby improve the secure key rate of QKD systems without sacrificing the security.

DOI: 10.1103/PhysRevA.100.032319

I. INTRODUCTION

Quantum key distribution (QKD) is considered to be one of the most promising and practical applications of quantum information science [1–3]. It has been studied both theoretically and experimentally since it was proposed by Bennett and Brassard in 1984 [4], leading to many advances in the past decades, including protocols and technical prototypes [5]. In early works, researchers focused mainly on two-dimensional quantum systems, for example, the polarization states of individual photons [6]. In the past decade, effort has been dedicated to the investigation of higher-dimensional quantum systems [7–9]. The benefits of utilizing higher-dimensional quantum systems for QKD include higher information capacity and enhanced robustness against eavesdropping.

Orbital angular momentum (OAM) states are attractive candidates for QKD because they intrinsically span an infinitely large Hilbert space. Beams with an azimuthal phase dependence $\exp(i\ell\theta)$ carry an OAM of $\ell\hbar$ per photon, where ℓ is the integer OAM quantum number. After the breakthrough work by Allen *et al.* in 1992 [10], the properties and applications of OAM have been studied in both classical and quantum regimes [11–15].

One characteristic of an OAM state is its ℓ-dependent diffraction [16]. Because of the state-dependent diffraction (SDD), OAM states with higher ℓ will have larger far-field sizes, and acquire more propagation phase [for example, the Gouy phase of Laguerre Gaussian (LG) states]. Thus, in practical free-space communication links, different OAM states will suffer different amounts of loss for a given collection aperture of finite size [17,18], leading to ℓ-dependent detection efficiency. Similar problems occur for states in the complementary angular (ANG) basis, which consist of an equal superposition of OAM states with fixed relative phase between adjacent OAM components [8,19]. Due to the SDD, both the amplitude of each OAM state and the relative phase will be modified. Therefore, the received state will be different from the transmitted state, increasing the error rate at the receiver even in the absence of an eavesdropper. The adverse effects of SDD in both OAM and ANG bases result in QKD systems less robust against background noise, measurement errors, and eavesdropping. Although OAM-based QKD systems have been demonstrated in both laboratory and outdoor environments [8,9,20], the influence of SDD on QKD systems has not yet been adequately addressed in previous work [21].

Here, we investigate the performance of a d-dimensional QKD system under SDD using OAM states as the example. The SDD results in an efficiency mismatch in the OAM basis and an increased error rate in the ANG basis, which leads to a lower secure key rate. These SDD-induced defects are quantitatively studied as a function of the Fresnel product N_f in a vacuum, which is defined as $N_f = (\pi/4)D_A D_B/(\lambda z)$ [22]. D_A and D_B are the diameters of the circular transmitting and receiving apertures respectively, λ is the wavelength of the light, and z is the propagation distance. For a given free-space link, the parameter N_f shows how strong the diffraction is. A small N_f ($N_f \ll 1$) indicates a link suffering from a strong diffraction whereas the diffraction is negligible for

*jzhao24@ur.rochester.edu

links with $N_f \gg 1$. We then propose a precompensation protocol to minimize the SDD-induced defects. To validate the approach, we experimentally measure the crosstalk matrices for both the precompensated protocol and the original protocol, and then estimate the secure key rates in both cases. We find that for a quantum channel with a small Fresnel number product N_f but high-dimensional encoding space, the precompensated protocol can significantly reduce the error rate and provide a greater secure key rate per transmitted photon.

II. SECURITY LOOPHOLE INDUCED BY STATE-DEPENDENT DIFFRACTION

Because of the finite sizes of transmitter and receiver apertures, higher-order OAM states, which have stronger diffraction, will experience greater loss and acquire more propagation phase. To determine the channel transmission efficiency of a specific OAM state, we define a propagation operator $\hat{F}$ that transfers the OAM eigenstate prepared by Alice $|\ell\rangle_A$ to the state received by Bob $|\ell\rangle_B$ (which is also an OAM eigenstate but has a different radial amplitude distribution) as

$$|\ell\rangle_B = \hat{F}|\ell\rangle_A. \tag{1}$$

The operator $\hat{F}$ includes the effects of propagation in vacuum and the finite apertures at both transmitter and receiver sides. Note that $\hat{F}$ only results in different amounts of loss, but does not introduce any crosstalk between different OAM $|\ell\rangle$ states. Therefore, this is not a unitary transformation, and if we define the efficiency ε_ℓ as $\varepsilon_\ell = \langle\ell|\ell\rangle_B/\langle\ell|\ell\rangle_A$, we obtain the following eigenvalue relation:

$$\hat{H}|\ell\rangle_A = \varepsilon_\ell|\ell\rangle_A, \tag{2}$$

where $\hat{H} = \hat{F}^\dagger\hat{F}$, and the theoretical transmission efficiency of $|\ell\rangle_A$ in vacuum is represented by ε_ℓ which is a function of both OAM quantum number ℓ and Fresnel number product N_f (see Appendix A for details) [22].

In OAM-based QKD, the complementary ANG basis is the Fourier conjugate of the OAM basis. The ANG state of index j is defined as [8,19]

$$|j\rangle = \frac{1}{\sqrt{d}}\sum_{\ell=-L}^{L}|\ell\rangle e^{-i2\pi j\ell/d}, \tag{3}$$

where d is the dimension of the Hilbert space and L is the maximum OAM quantum number in use, which satisfies the relation $2L+1=d$. The ANG basis and the OAM basis form two mutually unbiased bases (MUBs), and the use of two or more sets of MUBs guarantees the unconditional security of QKD [23,24].

In practice, as we mentioned above, different OAM states will suffer different amounts of diffraction, as do the OAM components of an ANG state. As shown in Fig. 1(a), for a low Fresnel number product ($N_f \ll 1$), there are huge efficiency differences between lower-order and higher-order OAM states. This difference results in a nonuniform probability of detecting the OAM states. The ANG basis for Bob will thus be modified as

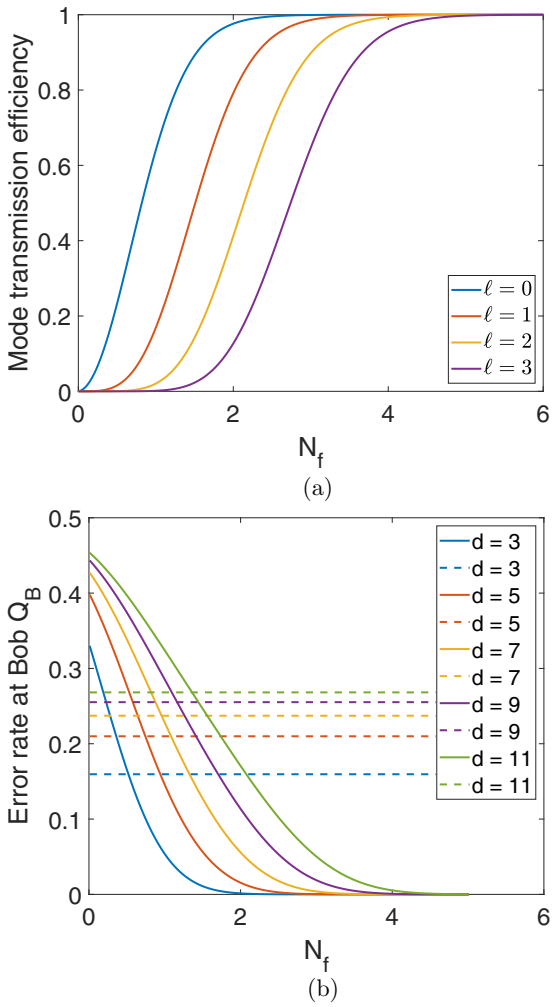


FIG. 1. (a) Theoretical transmission efficiency ε_ℓ of different OAM states as a function of Fresnel number product N_f in a $d=7$ quantum system. (b) QSER at Bob as a function of Fresnel number product N_f. The solid lines show the QSER induced by the effects of SDD. The dashed lines show the maximum value of the QSER for which a secure channel can be obtained in the limit where the effects from SDD are negligible ($N_f \gg 1$). When the QSER goes above the corresponding upper bounds, the communication system is not secure and the secure data rate goes to zero.

$$|j\rangle_B = \frac{1}{\sqrt{\varepsilon_j}}\hat{F}|j\rangle_A = \sum_{p=0}^{d-1}\sqrt{P_{j,p}}|j+p\rangle_A$$
$$= \sum_{\ell=-L}^{L}\sqrt{P_\ell}|\ell\rangle_A e^{-i\ell[2\pi j/d-\psi(z)]}, \tag{4}$$

where $1/\sqrt{\varepsilon_j}$ is the normalization constant given by $\varepsilon_j = \sum_\ell^d \varepsilon_\ell/d$, which describes the transmission efficiency of ANG states. The state $|j\rangle_A$ is the ANG state j prepared by Alice, which has the same form as Eq. (3). The state $|j\rangle_B$ is the ANG state received by Bob after being modified by SDD. The quantity $P_{j,p}$ characterizes the crosstalk between ANG states, and is equal to the probability of finding the ANG state $|j+p\rangle_A$ prepared by Alice in the ANG state $|j\rangle_B$ received by

Bob which has been modified by SDD. The quantity P_ℓ, which can be calculated from transmission efficiency ε_ℓ, is the probability of finding the OAM component $|\ell\rangle$ in the modified ANG state $|j\rangle_B$. The quantities $\sqrt{P_{j,p}}$ and $\sqrt{P_\ell/d}$ are related by a discrete Fourier transform, and one can also show that $P_{j,p}$ is independent of j (see Appendix B for details). The propagation phase $\psi(z)$ is the phase acquired by each OAM state after propagating a distance z. One can notice that the state-dependent loss gives rise to a nonuniform probability distribution of the OAM spectrum, while the state-dependent phase terms introduce an extra relative phase between the different OAM components in each ANG state. Both of these effects lead to the crosstalk in the ANG basis, which will be further exacerbated in current methods for sorting ANG states [25].

One direct consequence of the increased crosstalk is an increase in the quantum symbol error rate (QSER) at Bob's side (Q_B). Here we define the QSER as the probability of detecting a photon in a state other than the launched state [26]: $Q_B = 1 - (F_{\mathrm{OAM}} + F_{\mathrm{ANG}})/2$, where F_{OAM} and F_{ANG} are the fidelities of the OAM basis and the ANG basis respectively, defined as $F_{\mathrm{OAM}} = |_A\langle\ell|\ell\rangle_B|^2$ and $F_{\mathrm{ANG}} = |_A\langle j|j\rangle_B|^2$. Note that here we already exclude all the other errors. In our case, assuming there is no eavesdropping, F_{OAM} equals unity while F_{ANG} equals P_j, which means that only the ANG basis suffers an increased QSER [27]. To quantitatively show how the QSER changes with diffraction, we have numerically calculated the probability distribution of P_ℓ for Fresnel number product N_f ranging from 0.01 to 5 under different quantum space dimensions in Fig. 1(a). When N_f is close to 0, only the fundamental Gaussian state ($|\ell = 0\rangle$) can be transmitted. Therefore, the OAM spectrum at Bob will be very narrow, and the ANG spectrum will become uniform, leading to a complete loss of information. As N_f increases, the efficiency of all OAM states will be closer and finally become near 1, indicating that state-dependent loss is reduced and then negligible at the high N_f regime. The QSER as a function of N_f is shown in Fig. 1(b). For a given dimension d, small N_f can significantly increase the QSER even if there is no quantum attack. This will lead to a lower information capacity (see Appendix B for details), and make the system more vulnerable to eavesdropping and quantum cloning since the upper bound for the QSER is fixed for each given dimension d [28,29]. Moreover, for a given N_f, a higher dimensional system will suffer from more crosstalk introduced by SDD. For instance, in Fig. 1(b), the crosstalk for $d = 11$ is three times larger than the crosstalk for $d = 7$ in a $N_f = 2$ system. In addition to the loss of information, a higher error rate means that one needs to sacrifice a greater fraction of the raw key to detect the existence of eavesdroppers, because the legitimate parties cannot distinguish the errors generated by eavesdroppers' attack from other errors in the system.

Meanwhile, the nonuniform efficiencies induced by SDD in the OAM basis introduces a detection efficiency mismatch in Bob's detectors, which can be utilized by Eve to control the information received by Bob. The security of QKD in the presence of efficiency mismatch has been both theoretically and experimentally studied [30–32]. Fortunately, measurement-device-independent QKD protocols have been developed to eliminate the loopholes from side channels including efficiency mismatch [33–35], and one can implement these protocols to remove this SDD induced security loophole. However, these strategies cannot eliminate the effect of SDD (the increased QSER) in the ANG basis. Therefore, a new protocol that can reduce the effect of SDD in both bases needs to be developed.

III. WAIST PRECOMPENSATION PROTOCOL

From the discussion above, one can conclude that the nonuniform efficiency induced by SDD leads to a security loophole, which is caused by the increased error rates from the state-dependent loss in both OAM and ANG bases, as well as the state-dependent phase in the ANG basis. Therefore, to reduce the adverse effects of SDD, a uniform efficiency for all encoding states is desirable, which requires adjusting the efficiencies of low-order states to match the high-order states.

Here, we propose a precompensation protocol to mitigate these adverse effects. Alice first selects one set of states that she is going to use for encoding, and measures the efficiency of state $|L\rangle$. To adjust the efficiencies of all low-order states to match the efficiency of $|L\rangle_A$, she can change the beam radius of each low-order state so that each state has a same divergence angle α_ℓ: $\alpha_\ell \propto (|\ell| + 1)/r_{\mathrm{rms}}(0)$, where $r_{\mathrm{rms}}(0)$ is the root-mean-square (rms) beam radius defined by Ref. [16]. That is to say, Alice intentionally increases the loss of the low-order states to reduce the state-dependent loss. We call this set of OAM states uniform-energy-loss (UEL) states. Alice then uses these specially prepared OAM states to construct the corresponding ANG basis j. After this, a uniform efficiency has been achieved for both OAM and ANG states, and both the efficiency mismatch and the increased QSER for Bob can be significantly reduced. Since the two bases are orthogonal and mutually unbiased throughout the entire propagation distance, the security analysis of this protocol is identical to the one for the BB84 protocol but with a higher uniform channel loss. We name the approach we have just described *waist precompensation* (WPC).

IV. EXPERIMENTAL RESULTS

To implement our protocol in a laboratory setting, we measure the crosstalk matrix for a Fresnel number product $N_f = 3.96$ and dimension $d = 7$. A HeNe laser is coupled into a single-mode fiber (SMF) to generate a single spatial mode at 633 nm. The first spatial light modulator (SLM1), together with lenses 2 (L2, $f = 0.75$ m) and 3 (L3, $f = 0.5$ m), is used to generate the desired input states $|\ell\rangle_A$ and $|j\rangle_A$ [19]. Aperture 1 (A1) is used to select the first diffraction order. The distance (Z1 = 3.12 m) between transmitter's aperture (the diameter of A2 is 3.07 mm) and receiver's aperture (the diameter of A3 is 3.25 mm) constitute the link with Fresnel number product $N_f = 3.96$. Both A2 and A3 are implemented by round apertures written onto SLM1 and SLM2 respectively. The second SLM scans the OAM and ANG spectra, and projects the desired state onto the fundamental Gaussian state, which can be coupled into the second SMF. The details of the projective measurement are included in Appendix E. A power meter (PM) is used to measure the transmitted intensity coupled into the second SMF.

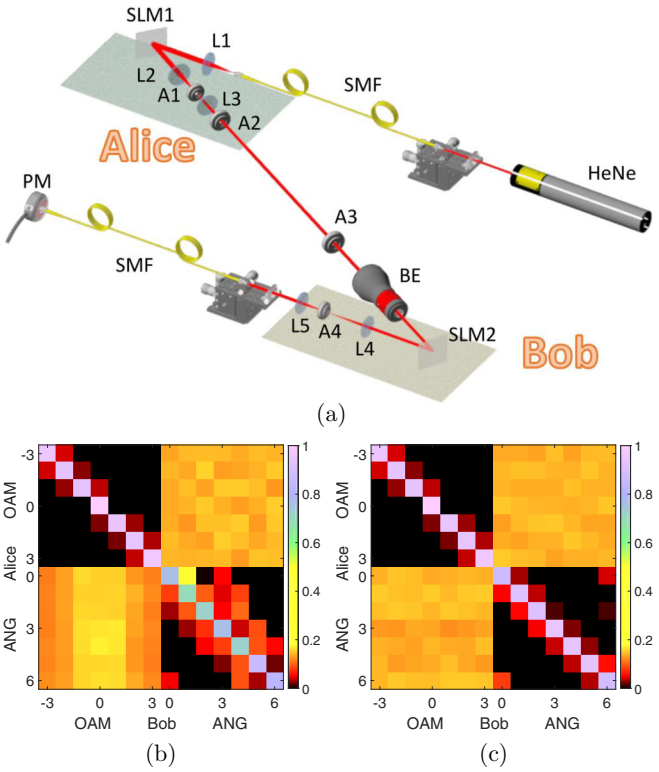


FIG. 2. (a) Experimental setup. L1 to L5 are lenses while SLM denotes the spatial light modulator. A1 to A4 are apertures, and BE is beam expander. Z1 represents the propagation distance from transmitter aperture A2 to the receiver aperture A3. (b) Measured probability distribution with no precompensation. (c) Experimental result of WPC protocol. The tables showing the probabilities in these matrices can be found in Appendix F. We can see that the diagonal elements in (c), which represents the fidelity of the states, have less error than in (b). The worst fidelity in (b) is less than 70% while the average fidelity is only 85.8%. As the comparison, the worst fidelity in (c) is 86.8% and the average fidelity is 93.3%. Therefore, the crosstalk in (c) is less than the crosstalk in (b). One should also note that, through the use of WPC, measuring the ANG states in the OAM basis will have a more uniform distribution, which can be found as the bottom left corners in (b) and (c).

To quantitatively show the benefits of the WPC protocol, we measure the conditional probability of finding each state received by Bob for each state transmitted by Alice, and display the results in a crosstalk matrix [Fig. 2(c)]. One can see that the crosstalk in the ANG basis is very small, in particular when compared with the crosstalk of no compensation protocol, which is shown in Fig. 2(b). The average QSER measured in the case of no compensation is 14.2% while the average QSER with WPC is 6.7%. The mutual information with the WPC protocol equals 2.56 bits per photon, an improvement over 2.22 bits per photon in the case of no compensation. From the QSER above, we can then find the secure key density using the following equation based on two MUB protocols [29,36]:

$$r = \log_2 d + 2\left[Q_B \log_2 \frac{Q_B}{d-1} + (1-Q_B)\log_2(1-Q_B)\right], \tag{5}$$

where Q_B represents QSER at Bob's side. The secure key density r is then found to be 1.76 bits per received photon with WPC protocol, a significant improvement from 0.89 bits per photon in the no compensation case.

V. DISCUSSION AND CONCLUSION

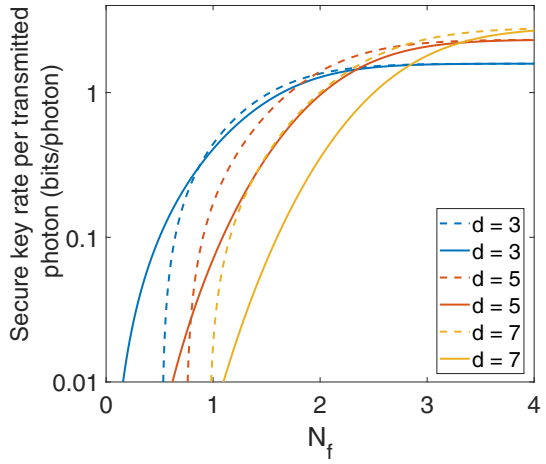
Although the WPC protocol will ensure the robustness of the quantum system and provide higher information encoded per photon, it will lower the overall efficiency and may result in a lower secure key rate because of a lower average transmission probability [8]. However, for practical quantum encoding systems with higher dimensionality and lower Fresnel number products, the crosstalk introduced by SDD can be much larger than in the ideal case. In such circumstances, the external errors from either modal dispersion (from turbulence, optical fiber, etc.) or imperfect mode sorting can be severe, which makes it even more necessary to implement the precompensation protocol for a better QKD performance.

The simulated comparison of the secure key rate per transmitted photon between WPC protocol and no compensation protocol with different error rates from external errors are shown in Fig. 3 as a function of Fresnel number product N_f. For a given system with fixed transmitting and receiving apertures, N_f is inversely proportional to the transmission distance z. Therefore, when N_f is small, usually indicating a larger z, we see that WPC protocol can significantly improve the performance of high-dimensional QKD systems in realistic links, especially in the presence of external errors. Even for our in-laboratory measurements, which have low external errors, the secure key rate is increased from 0.86 to 1.63 bits per transmitted photon when WPC is implemented (see Appendix C for details). Therefore, in realistic QKD systems, intentionally sacrificing some efficiency for low-order states to get a lower but uniform efficiency can significantly benefit the system.

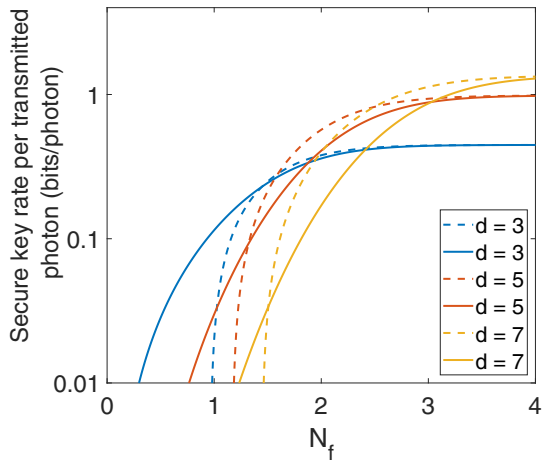
Another concern regarding the WPC protocol is how practical it will be in a realistic QKD scenario. As we discussed above, in most cases, the WPC protocol is superior to no compensation protocols only when N_f is limited. In realistic scenarios, most current free-space QKD systems have Fresnel number products less than 1, especially the satellite-to-ground system ($N_f = 0.23$) [2,37]. Thus the WPC protocol could be useful in optimizing the performance of future global high-dimensional QKD systems. Furthermore, implementing the WPC protocol is simple: one only needs to take the N_f of the system into consideration, and employ the optimal set of beam waists, which requires no extra apparatus.

We assumed OAM encoding and circular apertures in the discussion given above. However, SDD is expected to be a problem for any type of spatial-mode encoding, and for a given system, we can always find a set of eigenstates with uniform transmission efficiency. Therefore, our new protocol is generic for realistic high dimensional quantum encoding scenarios utilizing spatial degrees of freedom [38–40].

In summary, we have analyzed the performance of a high-dimensional QKD system based on OAM encoding in the presence of SDD. In practical free-space quantum links with finite aperture sizes and long transmission distance, SDD can introduce a high error rate and security loopholes, which can



(a)



(b)

FIG. 3. (a),(b) Simulated secure key rate per transmitted photon as a function of Fresnel number product N_f with 0% and 10% external errors respectively. The solid lines represent the secure key rate using WPC protocol while the dashed lines represent the secure key rate with no compensation. Note that the Fresnel number product N_f is inversely proportional to the transmission distance z.

significantly reduce the information capacity of the quantum link and its robustness against quantum attacks. To overcome this threat, we propose the WPC protocol based on the use of UEL states, which have a uniform loss for all encoding states. We implemented this approach experimentally and showed that it can appreciably reduce the QSER and improve the secure key rate per transmitted photon. Since the two bases in the WPC protocol are orthogonal and mutually unbiased, the security of this new approach is the same as the conventional BB84 protocol. Therefore, by intentionally increasing the loss for certain states to get a uniform efficiency, we can significantly reduce the adverse effects induced by SDD, and improve the secure key rate in QKD systems. Considering that in the near future, high-dimensional QKD systems will be a promising platform for increasing the channel information capacity of free-space communication systems, our WPC protocol will aid in improving the performance of these systems, and increase their robustness to eavesdropping.

ACKNOWLEDGMENTS

We acknowledge helpful discussions with B. Gao, C. Liu, and K. Pang. This work was supported by the U.S. Office of Naval Research. R.W.B. acknowledges support from Canada Research Chairs Program and the National Science and Engineering Research Council of Canada. B.B. acknowledges the support of a Banting postdoctoral fellowship.

APPENDIX A: DERIVATION OF THE EIGENVALUE EQ. (2) IN THE MAIN PAPER

We employ the same notation as in the main paper. The $|\ell\rangle_A$ represents the state prepared by Alice while $|\ell\rangle_B$ denotes the state received by Bob. The propagation operator $\hat{F}$ includes both the effects of diffraction and limited aperture size at the receiver. That is, this operator is not unitary and includes the loss of the link. Therefore, if we define the power sent out by Alice as $P_A = {}_A\langle\ell|\ell\rangle_A$ and the power received by Bob as $P_B = {}_B\langle\ell|\ell\rangle_B$, we can write the efficiency $\varepsilon_\ell = P_B/P_A = \langle\ell|\ell\rangle_B/\langle\ell|\ell\rangle_A$. We can then rewrite this equation in the following form:

$$\begin{aligned} {}_B\langle\ell|\ell\rangle_B &= {}_A\langle\ell|\hat{F}^\dagger\hat{F}|\ell\rangle_A \\ &= {}_A\langle\ell|\varepsilon_\ell|\ell\rangle_A. \end{aligned} \tag{A1}$$

If we define a new operator $\hat{H} = \hat{F}^\dagger\hat{F}$, we can get the following relation:

$$P_B = {}_A\langle\ell|\hat{H}|\ell\rangle_A. \tag{A2}$$

Therefore, to find the optimal field maximizing the efficiency, we need to maximize the P_B for a given P_A. Then, we use a Lagrange multiplier by introducing an additional scalar variable ε_ℓ, and rewrite this optimization problem as

$$\widetilde{P} = {}_A\langle\ell|\hat{H}|\ell\rangle_A - \varepsilon_\ell[{}_A\langle\ell|\ell\rangle_A - P_A]. \tag{A3}$$

By differentiating $\widetilde{P}$ with respect to ${}_A\langle\ell|$, we have

$$\frac{\partial\widetilde{P}}{\partial\,{}_A\langle\ell|} = \hat{H}|\ell\rangle_A - \varepsilon_\ell|\ell\rangle_A. \tag{A4}$$

By optimizing the $\widetilde{P}$, Eq. (4) should be 0. Therefore, we have the following eigenfunction:

$$\hat{H}|\ell\rangle_A = \varepsilon_\ell|\ell\rangle_A. \tag{A5}$$

Hence, the resulting eigenvalue ε_ℓ is the efficiency of the eigenstate $|\ell\rangle_A$ which maximizes the transmission efficiency of a given link.

APPENDIX B: CALCULATION OF MUTUAL INFORMATION I_{AB} IN THE ABSENCE OF EAVESDROPPER

First we prove that the $\sqrt{P_{j,p}}$ and $\sqrt{P_\ell/d}$ are related by a quantum Fourier transform, and $P_{j,p}$ is independent of ANG state index j. From Eq. (4) in the main paper, we can find the following inner products:

$$\begin{aligned} {}_A\langle j+p|j\rangle_B &= \sqrt{P_{j,p}} \\ &= {}_A\langle j+p|\sum_{\ell=-L}^{L}\sqrt{P_\ell}|\ell\rangle_A e^{-i\ell[2\pi j/d-\psi(z)]}. \end{aligned} \tag{B1}$$

Therefore, we can find the following relation:

$$\begin{aligned}\sqrt{P_{j,p}} &= \sum_{m=-L}^{L} \sqrt{\frac{1}{d}}_A \langle m| e^{i2\pi(j+p)m/d} \\ &\quad \times \sum_{\ell=-L}^{L} \sqrt{P_\ell}|\ell\rangle_A e^{-i\ell[2\pi j/d-\psi(z)]} \\ &= \sum_{\ell=-L}^{L} \sqrt{\frac{P_\ell}{d}} e^{i2\pi(j+p)\ell/d} e^{-i2\pi j\ell/d} e^{i\ell\psi(z)} \\ &= \sum_{\ell=-L}^{L} \sqrt{\frac{P_\ell}{d}} e^{i\ell 2\pi(p/d+\frac{\psi(z)}{2\pi})}. \end{aligned} \tag{B2}$$

Therefore we can find that $P_{j,p}$ is independent of j and equals the Fourier transform of $\sqrt{P_\ell/d}$.

We then show how to get Eq. (5) in the paper. The probability of Alice sending out each symbol is still equal, but due to the state-dependent loss, the probabilities of finding each symbol at Bob's side are different. Therefore, as discussed in our paper, for the photons which are registered by both parties, we have the following probabilities:

$$\begin{aligned} P(\mathrm{OAM}_{\ell,B}) &= P_\ell, \\ P(\mathrm{ANG}_{j,B}) &= 1/d, \\ P(\mathrm{OAM}_{\ell,A}) &= P_\ell, \\ P(\mathrm{ANG}_{j,A}) &= 1/d. \end{aligned} \tag{B3}$$

$P(\mathrm{OAM}_{\ell,B}$ represents the probability that Bob receives a photon in the $|\ell\rangle$ state, while $P(\mathrm{OAM}_{\ell,A}) = P_\ell$ represents the probability that Alice sends out a photon in the $|\ell\rangle$ state. This is because those events in which Alice sends out one symbol but Bob receives nothing have been discarded.

The definition of mutual information is

$$I_{AB} = \sum_{a\in A}\sum_{b\in B} p(a,b)\log_2 \frac{p(a,b)}{p(a)p(b)}, \tag{B4}$$

where $p(a,b)$ is the joint probability. The relation between joint probability and conditional probability is $p(a,b) = p(a)p(b|a)$. In our case, even if Alice is sending out each symbol with equal probability, the photon statistics at Bob's side are not uniformly distributed because of the state-dependent loss. Therefore, we have the following probability relations:

$$p(\ell_A, i_B) = P_\ell \delta_{i\ell},\ p(j_A, k_B) = P_{j,p}/d. \tag{B5}$$

Therefore, considering Alice randomly chooses her basis, the mutual information between Alice and Bob I_{AB} is

$$I_{\mathrm{AB}} = \tfrac{1}{2} I_{\mathrm{AB,OAM}} + \frac{1}{2} I_{\mathrm{AB,ANG}}, \tag{B6}$$

where $I_{\mathrm{AB,OAM}}$ represents the mutual information using the OAM basis while $I_{\mathrm{AB,ANG}}$ is the mutual information using the ANG basis. The final form of I_{AB} can be found as

$$I_{\mathrm{AB}} = \frac{1}{2}\sum_p P_{j,p}\log_2 P_{j,p} d - \frac{1}{2d}\sum_\ell \log_2 P_\ell. \tag{B7}$$

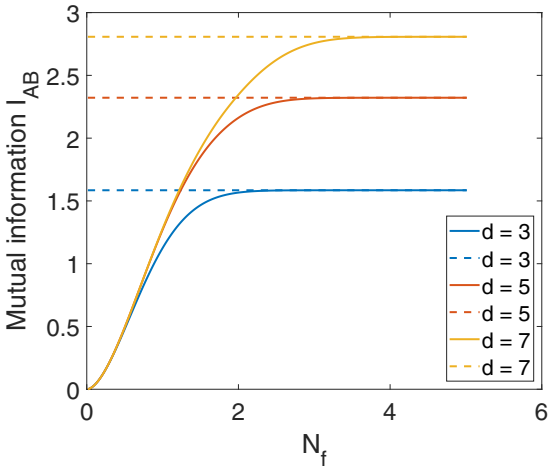


FIG. 4. The mutual information between Alice and Bob as a function of N_f. The solid lines represent the mutual information with SDD while the dashed lines indicate the mutual information $\log_2(d)$ in the limit where SDD can be ignored ($N_f \gg 1$).

As shown in Fig. 4, it is not difficult to verify that I_{AB} is smaller than the ideal value $\log_2 d$. When N_f is near zero, the information encoded is almost lost, while in the high N_f region, the information capacity gets close to the ideal value. Another interesting result is that the information carried by the two bases is not equal, and that the information encoded in the OAM basis is always larger than that carried in the ANG basis because of the absence of crosstalk in the OAM basis.

APPENDIX C: SIMULATION RESULTS OF WPC PROTOCOL

Figure 5 shows simulation results comparing the WPC protocol and transmission without the use of compensation, which we will refer to as the no-compensation protocol. Figure 5(a) shows the simulated intensity and phase distributions of the ANG state $|j=0\rangle$ prepared by Alice in the no-compensation and WPC protocols, while Fig. 5(b) shows the corresponding results for the received ANG state $|j=0\rangle$. One can notice that both the intensity and phase profiles for the two protocols are very different at Alice's and Bob's sides. Diffraction distorts the intensity distribution of the received state in the no-compensation case; after propagating through the link, the one single main lobe on Alice's side, which indicates the angular position and the value of j, becomes two main lobes on Bob's side. In contrast, the intensity profile in the WPC case remains similar even after diffraction. The simulated crosstalk matrices of no compensation protocol and WPC protocol are shown in Figs. 5(c) and 5(d), respectively. Compared to the experimental data in Figs. 2(b) and 2(c), it is obvious that in the no compensation case, the SDD gives a nonuniform probability distribution when we measure the ANG states in the OAM spectrum with higher probabilities in lower orders but lower probabilities in the higher orders, and nonzero off-diagonal elements in the ANG spectrum [the fidelity of ANG states shown in Fig. 5(c) is 95.1% since the Fresnel number product is chosen to be 3.96]. However, with the WPC protocol, an almost uniform probability

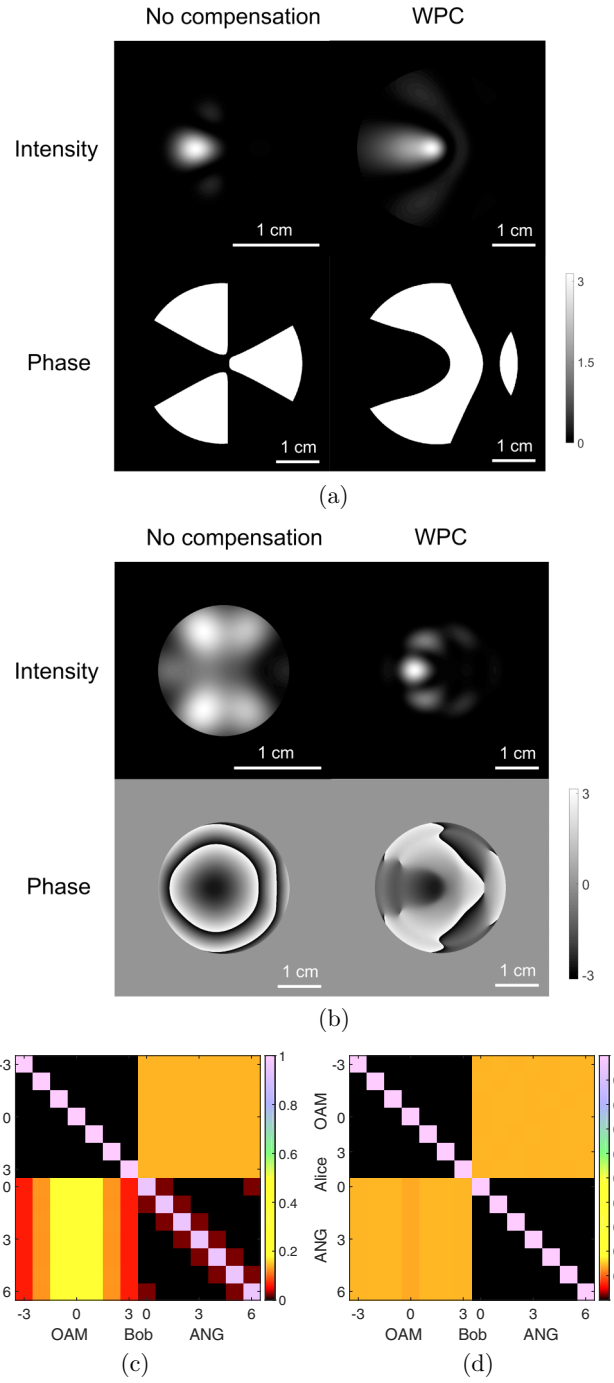


FIG. 5. (a),(b) Simulation results of transmitted and received $|j=0\rangle$ states respectively, both with WPC and without compensation. (c),(d) probability distributions of finding each OAM component in the received ANG state $|j=0\rangle$, in the no-compensation protocol (c) and WPC protocol (d). The simulated link has a Fresnel number product equal to 3.96.

distribution can be found when ANG states are measured in the OAM basis, and there are no nonzero off-diagonal elements in the ANG basis [the fidelity of ANG states in Fig. 5(d) is 99.99%]. Therefore, the simulation results show the ability of the WPC protocol to reduce the adverse effects of SDD.

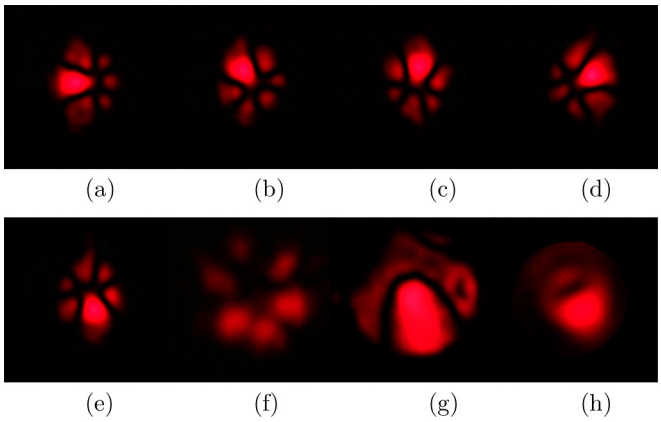


FIG. 6. (a)–(d) Four ANG states generated experimentally with no compensation with $N_f = 3.96$ at transmitter's side. The ANG quantum number of these states is $j = 0,\ 1,\ 2$, and 3 respectively. (e),(f) Prepared and received ANG states $|j=5\rangle$ in the no compensation protocol. (g),(h) Prepared and received states in the WPC protocol. All images are taken under identical acquisition parameters. Note that in panel (f) the dominant lobe of (e) has disappeared, but that it is retained in (h) through the use of precompensation.

APPENDIX D: PREPARED AND RECEIVED STATES

Figure 6 shows the images of experimentally realized ANG states after transmitting and receiving apertures for $d = 7$, $\ell_{\max} = 3$. The top row gives the ANG states with ANG quantum number j from 0 to 3 prepared by the transmitter. All the states in the top row are prepared with no compensation while the figures in the bottom row are the comparison between no compensation and WPC. Figures 6(e) and 6(f) are prepared and received ANG states $|j=5\rangle$ with no compensation, and Figs. 6(g) and 6(h) are prepared and received states in the WPC case. After diffracting in the link, the spatial profile of ANG state $|j=5\rangle$ in the no compensation case changes greatly, such that it is intractable to identify the angular position of the main lobe of the state. However, in the WPC case, the received ANG state has a similar spatial profile as the launched state.

APPENDIX E: PROJECTIVE MEASUREMENT

Here, we explain how we experimentally realize the projective measurement in OAM and ANG bases. For the OAM states, as the first step, we use SLM2 to apply diffraction gratings with the same OAM quantum number as the incident beam onto the SLM2. In this case, we couple the Gaussian states which are selected from the first negative diffraction order from SLM2 into the SMF. Since the negative first diffraction order adds the opposite phase we added onto the SLM2, in cases where the OAM quantum number in the incident beam match the OAM value on the SLM2, the beam in the first negative order should be a Gaussian. Therefore, we can record the coupling efficiencies of each incident OAM state by switching the OAM quantum number in the diffraction grating. The single mode coupling efficiency for the fundamental Gaussian state is about 40%. All these calibrations are done with an infinitely large collection aperture. Then, to do the projective measurement of the incident beam

in the OAM basis, we sequentially implement the diffraction gratings with different OAM quantum numbers through the use of SLM2, and then record the powers coupled into SMF. These powers are divided by the corresponding coupling efficiencies of each OAM state to get the exact power of each OAM component in the incident state before coupling. To get the probability distribution we show in the main paper, one needs to normalize the measured power of each incident OAM state. In theory, if the incident beam is in an OAM state, there will be no crosstalk in the OAM basis in both the conventional protocol and WPC. This is because the grating on the second SLM only modulates the phase of the incident beam but not the amplitude. Therefore, the projective measurement can be described by the following equation:

$$P(\ell_i, \ell_m) = \frac{\int_0^R \int_0^{2\pi} |A_i(r)\exp(i\ell_i\theta)\exp(-i\ell_m\theta)|^2 r dr d\theta}{\sum_{\ell_m=-\ell_{\max}}^{\ell_{\max}} \int_0^R \int_0^{2\pi} |A_i(r)\exp(i\ell_i\theta)\exp(-i\ell_m\theta) r|^2 dr d\theta}, \tag{E1}$$

where $P(\ell_i, \ell_m)$ is the probability of finding the OAM ℓ_m component in the incident beam which has an OAM equal to ℓ_i. $A_i(r)$ is the radial field distribution of the incident beam. Since the integral over azimuthal degree of freedom gives a Kronecker delta, Eq. (E1) will finally reduce to $P(\ell_i, \ell_m) = \delta_{\ell_i,\ell_m}$. Therefore, the radial field distribution of the incident beam has no influence on the crosstalk in the OAM basis when the incident beam is in an OAM state. For the ANG states, the measurement we did is not a complete projective measurement since ANG states have both amplitude and phase information, but one single SLM can only manipulate one of them. However, we find out that if we use the same method as what we use in the OAM basis, we will only get light coupled into SMF when the ANG quantum added on the SLM2 matches the ANG quantum number of the incident beam in the no SDD case. Even though this method provides a very low coupling efficiency (around 10%), we can still scan the ANG space and get the crosstalk matrix. However, when the SDD is taken into consideration, one can still find some coupling in the SMF when the ANG quantum numbers mismatch so that we have errors in the ANG basis (i.e., the errors induced by SDD only). This gives the off-diagonal terms in the crosstalk matrices.

APPENDIX F: SECURE KEY RATE CALCULATION BASED ON EXPERIMENTAL DATA

Equation (5) in the main text gives the secure key density per detected photon, while the product of the secure key density and the transmission efficiency of the states yields the secure key density per transmitted photon. The secure key rate is then simply the product of the secure key rate per transmitted photon and the photon rate. In the simulation, the QSER at Bob's side (Q_B) comes from the external error (Q_{ex}) and the error induced by the SDD (Q_{s}). Therefore, the QSER at Bob's side is expressed as $Q_B = Q_{\text{s}} + Q_{\text{ex}} - Q_{\text{s}}Q_{\text{ex}}$, where Q_{s} stands for the error induced by SDD and Q_{ex} is the external error. Here we have assumed that the Q_{ex} is independent of the state which is measured by Bob. This assumption is valid since the external error Q_{ex} comes from the environment but not the state itself. With this Q_B, we can easily find the secure key density r from Eq. (5) in the main text, and the secure key density per transmitted photon r_t can be found as $r_t = r\eta$, where η is the experimental transmission efficiency.

In the experiments, the external error Q_{ex} usually comes from measurement devices, which is not easy to estimate. Therefore, to calculate r, we directly use Q_B for calculation, which can be found from the crosstalk matrices. From the experimental data, the measured efficiency η for the $\ell = 3$ state is 92.4% which is the transmission efficiency of WPC using UEL states. The average efficiency η_{avg} of all seven states is 97.1%, which is the transmission efficiency of the conventional protocol. Therefore, the secure key density with WPC can be calculated as 1.63 bits per transmitted photon, as compared to 0.86 bits per transmitted photon with no compensation. We can see that a uniform efficiency distribution for all spatial modes, even though it is low, can provide an improved key rate over maximum transmission efficiency. Note that there is a discrepancy in the secure key rate comparison for a $N_f = 4$ system between simulation and laboratory data [Figs. 5(c), 5(d) 2(b), and 2(c)]. In theory, the WPC is advantageous only when N_f is small, since for

TABLE I. Experimental crosstalk matrix in the no compensation protocol when Alice prepares her states in the ANG basis while Bob measures in the ANG basis. The typical uncertainty of these elements is under 3% of each given value, mainly coming from the power fluctuation in the laser. The dark noise of the detector has been subtracted, leading to the zero terms in the table, with corresponding uncertainty typically equal to 0.0001.

	$\|j_0\rangle_B$	$\|j_1\rangle_B$	$\|j_2\rangle_B$	$\|j_3\rangle_B$	$\|j_4\rangle_B$	$\|j_5\rangle_B$	$\|j_6\rangle_B$
$\|j_0\rangle_A$	0.7646	0.1786	0.0048	0.0520	0.0000	0.0000	0.0000
$\|j_1\rangle_A$	0.0824	0.6913	0.0980	0.0444	0.0839	0.0000	0.0000
$\|j_2\rangle_A$	0.0318	0.0952	0.7182	0.0508	0.1040	0.0000	0.0000
$\|j_3\rangle_A$	0.0000	0.0301	0.0740	0.7650	0.0404	0.0904	0.0000
$\|j_4\rangle_A$	0.0000	0.0000	0.0504	0.0822	0.7222	0.0919	0.0533
$\|j_5\rangle_A$	0.0000	0.0000	0.0000	0.0258	0.0919	0.8599	0.0223
$\|j_6\rangle_A$	0.0492	0.0000	0.0000	0.0000	0.0926	0.0339	0.8243

TABLE II. Experimental crosstalk matrix in the WPC when Alice prepares her states in the ANG basis while Bob measures in the ANG basis. The typical uncertainty of these elements is under 3% of each given value, mainly coming from the power fluctuation in the laser. The dark noise of the detector has been subtracted, leading to the zero terms in the table, with corresponding uncertainty typically equal to 0.0001.

	$\|j_0\rangle_B$	$\|j_1\rangle_B$	$\|j_2\rangle_B$	$\|j_3\rangle_B$	$\|j_4\rangle_B$	$\|j_5\rangle_B$	$\|j_6\rangle_B$
$\|j_0\rangle_A$	0.8680	0.0328	0.0000	0.0000	0.0000	0.0000	0.0429
$\|j_1\rangle_A$	0.0504	0.6913	0.9138	0.0379	0.0000	0.0000	0.0000
$\|j_2\rangle_A$	0.0000	0.0535	0.9130	0.0151	0.0000	0.0000	0.0141
$\|j_3\rangle_A$	0.0000	0.0000	0.0491	0.9454	0.0251	0.0000	0.0000
$\|j_4\rangle_A$	0.0000	0.0000	0.0000	0.0395	0.9373	0.0281	0.0000
$\|j_5\rangle_A$	0.0000	0.0000	0.0000	0.0000	0.0376	0.9368	0.0576
$\|j_6\rangle_A$	0.0816	0.0000	0.0000	0.0000	0.0000	0.0351	0.08855

systems with $d = 7$ and $N_f = 4$, the QSER in the ANG basis is very small (less than 1%). However, our experimental data show a 14.2% QSER for the no compensation case. This is due to the imperfect measurements in the experiments. In the no compensation protocol, a perfect measurement should lead to less than 1% QSER in the ANG basis while the compensation case should have no QSER. There should be no QSER in the OAM basis in both cases as well. In the laboratory, the QSER in the ANG basis is much larger than our prediction (average QSER is 23.6% without compensation, and 8.57% with compensation), and the QSER in the OAM basis also exists (about 4.74%). Therefore, these imperfect measurements lead to the discrepancy between theoretical prediction and experimental data. Regarding the QSER in two bases, one should note that, for the current state of the art, the measurement error in the ANG basis is usually larger than that in the OAM basis, which requires a technical improvement in the future [8,25]. As shown in Tables I and II, the crosstalk matrices from the experiments, which correspond to the data in Figs. 2(b) and 2(c) respectively, have off-diagonal terms larger than the theoretical predictions, which indicates the imperfect measurement in our experiments. Even with these imperfections, the WPC protocol can significantly reduce the QSER in the ANG basis, which matches our prediction in Fig. 3 .

[1] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Continuous operation of high bit rate quantum key distribution, Appl. Phys. Lett. **96**, 161102 (2010).

[2] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution Over 144 km, Phys. Rev. Lett. **98**, 010504 (2007).

[3] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. OBrien, and M. G. Thompson, Integrated silicon photonics for high-speed quantum key distribution, Optica **4**, 172 (2017).

[4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in Quantum Cryptography, arXiv:1906.01645v1.

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptology **5**, 3 (1992).

[7] J. P. Torres, G. Molina-Terriza, and L. Torner, Twisted photons: new classical and quantum applications, in *Lasers and Applications* (International Society for Optics and Photonics, Warsaw, 2005), Vol. 5958, p. 59581O.

[8] 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).

[9] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Gunthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, High-dimensional intracity quantum cryptography with structured photons, Optica **4**, 1006 (2017).

[10] 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).

[11] J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. X. Ren, Y. Yue, S. Dolinar, M. Tur *et al.*, Terabit free-space data transmission employing orbital angular momentum multiplexing, Nat. Photon. **6**, 488 (2012).

[12] M. Mirhosseini, O. S. Magaña-Loaiza, C. Chen, S. M. Hashemi Rafsanjani, and R. W. Boyd, Wigner Distribution of Twisted Photons, Phys. Rev. Lett. **116**, 130402 (2016).

[13] L. Gao, S. Mohammad Hashemi Rafsanjani, Y. Zhou, Z. Yang, O. S. Magaña-Loaiza, M. Mirhosseini, J. Zhao, B. Gao, and R. W. Boyd, Distributed angular double-slit interference with pseudo-thermal light, Appl. Phys. Lett. **110**, 071107 (2017).

[14] Y. Ren, Z. Wang, P. Liao, L. Li, G. Xie, H. Huang, Z. Zhao, Y. Yan, N. Ahmed, A. Willner *et al.*, Experimental characterization of a 400 gbit/s orbital angular momentum multiplexed free-space optical link over 120 m, Opt. Lett. **41**, 622 (2016).

[15] Y. Ren, C. Liu, K. Pang, J. Zhao, Y. Cao, G. Xie, L. Li, P. Liao, Z. Zhao, M. Tur *et al.*, Spatially multiplexed orbital-angular-momentum-encoded single photon and classical channels in a free-space optical communication link, Opt. Lett. **42**, 4881 (2017).

[16] M. J. Padgett, F. M. Miatto, M. P. Lavery, A. Zeilinger, and R. W. Boyd, Divergence of an orbital-angular-momentum-carrying beam upon propagation, New J. Phys. **17**, 023011 (2015).

[17] M. P. J. Lavery, C. Peuntinger, K. Günthner, P. Banzer, D. Elser, R. W. Boyd, M. J. Padgett, C. Marquardt, and G. Leuchs, Free-space propagation of high-dimensional structured optical fields in an urban environment, Sci. Adv. **3**, e1700552 (2017).

[18] 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. U.S.A. **113**, 13648 (2016).

[19] M. Mirhosseini, O. S. Magana-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).

[20] 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).

[21] F. Wang, P. Zeng, X. Wang, H. Gao, F. Li, and P. Zhang, Towards practical high-speed high dimensional quantum key distribution using partial mutual unbiased basis of photon's orbital angular momentum. arXiv:1801.06582.

[22] G. A. Tyler, Spatial bandwidth considerations for optical communication through a free space propagation link, Opt. Lett. **36**, 4650 (2011).

[23] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, Rev. Mod. Phys. **89**, 015002 (2017).

[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[25] 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).

[26] The QSER is not equal to the quantum bit error rate (QBER) because one error symbol can yield more than one bit error in high dimensional QKD. The QBER is equal to QSER only in two-dimensional encoding since one error symbol gives one bit error.

[27] The SDD does not change the OAM value upon propagation. Although each OAM state suffers a different amount of loss and acquires a different phase, the azimuthal phase vortex of each OAM state is maintained during propagation. Therefore, there is no spread in the OAM spectrum but only loss.

[28] 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).

[29] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301(R) (2010).

[30] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov *et al.*, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[31] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, Phys. Rev. A **91**, 062301 (2015).

[32] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, Quantum **2**, 77 (2018).

[33] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[34] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

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

[36] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, Finite-key security analysis for multilevel quantum key distribution, New J. Phys. **18**, 073030 (2016).

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

[38] G. Xie, Y.-X. Ren, Y. Yan, H. Huang, N. Ahmed, L. Li, Z. Zhao, C.-J. Bao, M. Tur, S. Ashrafi *et al.*, Experimental demonstration of a 200-gbit/s free-space optical link by multiplexing laguerre–gaussian beams with different radial indices, Opt. Lett. **41**, 3447 (2016).

[39] Y. Zhou, M. Mirhosseini, D. Fu, J. Zhao, S. M. Hashemi Rafsanjani, A. E. Willner, and R. W. Boyd, Sorting Photons by Radial Quantum Number, Phys. Rev. Lett. **119**, 263602 (2017).

[40] Y. Zhou, M. Mirhosseini, S. Oliver, J. Zhao, S. M. H. Rafsanjani, M. P. J. Lavery, A. E. Willner, and R. W. Boyd, Using all transverse degrees of freedom in quantum communications based on a generic mode sorter, Opt. Express **27**, 10383 (2019).