Characterization and mitigation of information loss in a six-state quantum-key-distribution protocol with spatial modes of light through turbulence

Bienvenu Ndagano* and Andrew Forbes
School of Physics, University of the Witwatersrand, Private Bag 3, Wits 2050, South Africa

(Received 10 July 2018; published 26 December 2018)

Quantum communication with structured photons is topical, owing to the multidimensional state space of spatial modes. However, spatial modes are fragile and their quality degrades when perturbed in traditional communication media such as free-space and optical fibers. Here, we illustrate the effects of atmospheric turbulence on a six-state quantum-key-distribution protocol with orbital angular momentum (OAM) modes. We experimentally characterize the fidelity decay as a function of turbulence strength, showing a concomitant decrease with increasing perturbation, and consider the influence of both mode order and mode size, showing that OAM modes with higher helicity are more resilient to turbulence for this protocol. We outline two approaches to mitigate the photon information loss. In the first, we show that by postselecting on a high-dimensional subspace at the detection side, we can recover information contained in the scattered modes. In the second, we measure the channel operator by means of classically entangled light and mitigate errors on the quantum state through entanglement concentration by means of one-party Procrustean filtering. The tools we provide here will be beneficial for realizing more robust quantum communication with OAM modes of light.

DOI: 10.1103/PhysRevA.98.062330

I. INTRODUCTION

Taking advantage of the fundamental principles of quantum mechanics, quantum key distribution (QKD) allows a sender and receiver to share information in order to build a secure key that would subsequently be used to encrypt further communication through traditional classical means [1,2]. This has been demonstrated in real-world environments over significant distances using polarization encoding [3–8].

Controlling the spatial degree of freedom of a photon has opened interesting avenues of research in the field of QKD. Indeed spatial modes, unlike polarization, allow one to pack more information per photon; the larger state space that spatial modes span offers a larger alphabet available for encoding [9,10]. Experimental demonstrations inside and outside laboratories have been reported [11–14], pushing the dimension of the protocol as high as 7 (inside the laboratory) and the range as far as 300 m.

While spatial modes offer the promise of higher bandwidth, they are adversely affected by perturbations in free-space and optical fibers [15–19]. In the presence of atmospheric turbulence, for example, random refractive index fluctuations in the atmosphere degrade the beam profile and steer the beam off axis, the combination of which results in a measured intermodal crosstalk; that is, the state detected is different from that which was sent, leading to (quantum) bit errors. The probability of error naturally depends on the strength of the perturbation and the properties of the modes, the effects of which have been studied at both the classical [20–24] and quantum levels [25–28]. In the context of QKD, intermodal scattering during transmission is one of the causes of quantum bit errors that reduce the amount of secret information carried by each photon, eventually compromising the viability of the link [29–33].

Here we study how turbulence affects the secret key rate of a six-state quantum-key-distribution protocol with orbital angular momentum (OAM) modes as the basis. Such modes may be indexed by their helicity (topological charge), ℓ, which takes on any integer value. We show experimentally that the secret key rate decreases below acceptable level as the turbulence increases due to the decay in detection fidelity. We consider the case of weak turbulence that can be approximated by a single phase screen, and neglect scintillations. In light of the above, we explore means to mitigate intermodal crosstalk and information loss resulting from turbulence perturbations.

In particular we note that previous work on the topic of QKD in turbulence did not account for the order-dependent spatial mode size, whereas the second moment radius of an OAM mode of helicity ℓ is given by $\omega_\ell = \omega_0\sqrt{|\ell| + 1}$, where ω_0 is the Gaussian mode radius and we assume a radial order of $p = 0$. Prior studies assumed all OAM modes have an effective scale of ω_0, quoting a dimensionless turbulence parameter of $W = \omega_0/r_0$, where r_0 is the Fried parameter (an indicator of the allowable size of an aperture before turbulence becomes pronounced). Such studies have shown that entanglement decreases monotonically with increasing W, suggesting that, for the same r_0, larger beams are more adversely affected than smaller beams, at least in the context of entanglement decay [28,29]. In the context of QKD, we show theoretically and numerically that when appropriately scaling the size of higher OAM modes, those with higher OAM separation are more resilient to turbulence, enabling a more robust link. As a comparison, we simulated the decay of fidelity in turbulence in the context of the six-state QKD protocol, using OAM modes with $\ell = 2$, 4, 6, 8, 10, and 20. We

*Corresponding author: nibienvenu@gmail.com

highlight that the demonstration here is a proof-of-principle experiment intended to provide insights for future real-world implementations. The choice of the six-state protocol rests on the fact that it is easy to implement and follows previous prepare-and-measure real-world QKD demonstrations with spatial modes [12,14].

Next, we revisit the fact that turbulence results in the spread of information into multiple subspaces through modal scattering. During measurement, only a fraction of the total information content is recovered because only preagreed subspaces are probed by the receiver, resulting in a lower channel capacity. We show that more information can be recovered by increasing the space of postselected modes. We parametrize the expression of the detection fidelity in the different subspaces as a function of OAM and turbulence strength, and derive an expression for the limit to which the recovery is possible.

Finally, we outline a scheme whereby errors due to turbulence can be mitigated by probing the channel with a classical beam. Error correction techniques using adaptive optics have been proposed and demonstrated as a viable solution to mitigate crosstalk and allow for forward error correction [34–37]. We take a different approach, using a process tomography to obtain the channel matrix using a bright classically entangled light source. The resultant conjugate channel operator is then used to implement in real time a Procrustean filter on the quantum state, resulting in a concentration of entanglement and a higher secure key rate in the quantum transmission.

II. SIX-STATE PROTOCOL WITH ENTANGLED PHOTONS

The appeal of QKD lies in the ability to securely exchange information between two parties in the presence of external perturbations, solely by exploiting the laws of physics. These perturbations reduce the ability of the receiver, Bob, to correctly measure the states encoded by the sender, Alice. Some common sources of perturbations include measurements from an eavesdropper, dark counts in the detectors, or noise that is present in the quantum channel (atmospheric turbulence for example). The extent to which these perturbations affect Bob's measurements determine the secure key rate of the QKD link.

We considered a scenario where Alice generates a pair of entangled photons through spontaneous parametric down-conversion, retains one photon (photon A) of each pair, and sends the other (photon B) to Bob through a turbulent channel, as shown in Fig. 1(a). In order to generate the secret key, Alice and Bob enact an entanglement-based variant of the 1984 Bennett and Brassard protocol (BB84) [38]. For every photon pair, Alice and Bob perform joint projective measurements onto states from a set of mutually unbiased bases (MUBs). While BB84 with qubits states is traditionally performed with two MUBs (four states in total), the six-state protocol uses three MUBs, a total of six states, hence the name. On one hand, the six-state protocol carries higher inherent losses compared to the original BB84, given that, in the former, $2/3$ of the photons are lost during sifting as opposed to $1/2$ in the latter. On the other hand, using more MUBs enhances the tolerance to noise with a higher error rate threshold [39]. At the end of the transmission, Alice and Bob broadcast the measurement bases for each of the N generated pairs. Upon

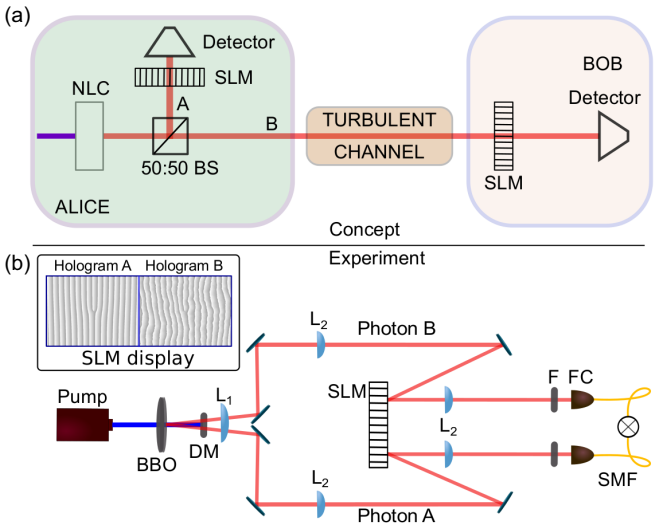

FIG. 1. (a) Alice generates a pair of entangled photons (A and B) using a pumped nonlinear crystal (NLC) and sends one of the photons to Bob through a turbulent channel. Alice and Bob enact a quantum-key-distribution protocol, whereby they perform joint measurements on the photon pair using spatial light modulators (SLMs) in order to build the key. (b) In the experimental realization one SLM is used to encode the spatial projections of both Alice and Bob. Turbulence is encoded as a phase screen, superimposed on the tomography holograms as shown on the inset. The plane of the BBO crystal was relayed onto the SLM and then the fibers using $4f$ imaging systems. $F = 10$ nm bandpass filters; $L1 = 10$ mm; $L2 = 750$ mm; FC is a fiber coupler with 2 mm focal length lens integrated; SMF is a single mode fiber; DM is a dichroic mirror.

comparison, Alice and Bob discard measurement outcomes where the encoding and decoding bases disagree to distill a key that is further refined through error correction and privacy amplification [40].

The secret key rate, R, is the amount of information that can be securely exchanged between Alice and Bob in the presence of perturbations. The exact expression of R depends on the QKD protocol used. In the six-state protocol it is given by [41]

$$R = 1 + \frac{3}{2}Q\log_2\left(\frac{Q}{2}\right) + \left(1 - \frac{3}{2}Q\right)\log_2\left(1 - \frac{3}{2}Q\right), \tag{1}$$

where $Q = 1 - F$ is the qubit error rate and F is the measurement fidelity, i.e., the ability of Bob to correctly distinguish the states sent by Alice. The secret key rate reaches its maximum $R_{\max} = 1$ for $Q = 0$ or $F = 1$. The QKD link between Alice and Bob is viable so long as the secret key rate is positive; this is satisfied for $Q < 0.126$ or $F > 0.874$. By comparison, the secret key rate in the original BB84 protocol is given by [41]

$$R = 1 + 2Q\log_2(Q) + 2(1 - Q)\log_2(1 - Q) \tag{2}$$

and admits a lower error threshold of $Q < 0.11$ and a higher fidelity threshold $F > 0.89$. We use the six-state protocol to demonstrate the importance of mode order and size, information retrieval, and entanglement concentration schemes, with

OAM as the spatial mode of choice. Although we use OAM as a topical example, the framework provided here can easily be extended to other spatial modes.

III. DECAY OF MEASUREMENT FIDELITY IN TURBULENCE

In the scenario depicted in Fig. 1(a), the entangled photons are initially correlated in OAM. Ideally Alice and Bob would like to share the following maximally entangled two-photon state:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|\ell_1\rangle_A|\ell_2\rangle_B + |-\ell_1\rangle_A|-\ell_2\rangle_B). \tag{3}$$

In the presence of turbulence, the correlations between the two photons are weakened, resulting in a lower photon detection probability [20,21,24] and loss of entanglement and measurement fidelity with respect to the initial state [27,28,42]. This is because the OAM spectrum of photon B is altered as it propagates through the turbulent channel. From previous work it was found that the spectral broadening arising from turbulence perturbations is peaked around the initially transmitted state [21–24,42–44]. Thus for simplicity we model the effect of turbulence as follows:

$$|\ell\rangle \xrightarrow{\text{turbulence}} \sum_m b^{|\ell-m|}|m\rangle, \tag{4}$$

where $0 \leqslant b < 1$. The spectral broadening is symmetric about the initially transmitted OAM state $|\ell\rangle$. The two-photon state in Eq. (3) is then modified due to the turbulent channel acting on photon B, to produce

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{N}}\left(\sum_m b^{|\ell_2-m|}|\ell_1\rangle_A|m\rangle_B + \sum_n b^{|-\ell_2-n|}|-\ell_1\rangle_A|n\rangle_B\right), \tag{5}$$

where

$$N = \sum_m b^{2|\ell_2-m|} + \sum_n b^{2|-\ell_2-n|} = 2\sum_m b^{2|\ell_2-m|}. \tag{6}$$

In the absence of turbulence, $b \to 0$ and the distribution is sharply peaked around the initial OAM state. Conversely, in very strong turbulence, the OAM spectrum flattens and $b \to 1^-$ (the negative superscript is used here to refer to b approaching 1 from the left).

To determine the effect of turbulence on the secure key rate of the QKD protocol, we chose to focus on the decay of measurement fidelity as a function of the turbulence strength; that is, the probability that, after turbulence, Alice and Bob measure their photons in the correlated state described in Eq. (3). Given that the target state is a pure state, the fidelity takes the form [45]

$$F = \langle\Phi^+|\rho|\Phi^+\rangle = |\langle\Phi^+|\Phi\rangle|^2 = \frac{1}{\sum_m b^{2|\ell_2-m|}}. \tag{7}$$

In the two-dimensional case where Alice and Bob use states $|\pm\ell_1\rangle$ and $|\pm\ell_2\rangle$, respectively, the measurement fidelity within the postselected subspaces is given by

$$F_\ell = \frac{1}{\sum_{m=\pm\ell_2} b^{2|\ell_2-m|}} = \frac{1}{1+b^{4|\ell_2|}}. \tag{8}$$

Note that the measurement fidelity is dependent on the turbulence strength: F_ℓ decreases as b increases. However, the fidelity is bounded below by $F_\ell = 0.5$. This is logical when one considers the overlap in Eq. (7). In the specific case where $|\langle\Phi^+|\Phi\rangle|^2 = 1/2$, the states $|\Phi\rangle$ and $|\Phi^+\rangle$ can be said to belong to mutually unbiased bases. Hence no information can be extracted from the projection of $|\Phi\rangle$ onto $|\Phi^+\rangle$, and the mutual information between Alice and Bob, I_{AB}, vanishes.

The decay in fidelity is experimentally demonstrated in Fig. 2. Information is encoded into OAM modes with a transverse electric field expressed as [46]

$$U_\ell(r,\phi) = \sqrt{\frac{1}{\pi|\ell|!}}\frac{1}{\omega_0}\left(\frac{r\sqrt{2}}{\omega_0}\right)^{|\ell|}\exp\left(-\frac{r^2}{\omega_0^2}\right)\exp(i\ell\phi). \tag{9}$$

For ease of notation, we will refer to the OAM state in Eq. (9) with the ket $|\ell\rangle$. The projections performed by Alice and Bob in the six-states protocol are made into the following bases: $\{|-\ell\rangle,\ |\ell\rangle\}$, $\{(|\ell\rangle+|-\ell\rangle)/\sqrt{2},\ (|\ell\rangle-|-\ell\rangle)/\sqrt{2}\}$, and $\{(|\ell\rangle+i|-\ell\rangle)/\sqrt{2},\ (|\ell\rangle-i|-\ell\rangle)/\sqrt{2}\}$. Interestingly, the joint measurements in the six-state protocol coincide with those required for an overcomplete quantum state tomography [45,47], and are shown in Fig. 2(a). Projections in the same basis fully discriminate the states prepared by Alice, while measurements in conjugate bases produce a uniform probability distribution. These projective measurements can be used to reconstruct the density matrix of the state after the turbulence and compute the fidelity. Note that the region enclosed with red-dashed lines highlights a set of measurements that would be required in BB84.

We generated entangled photons through type-I spontaneous parametric down-conversion by pumping a 3 mm BBO crystal with a picosecond laser with wavelength 355 nm and average power 350 mW, as shown in Fig. 1(b). For each down-converted pump photon, a pair of entangled photons is emitted, each with a wavelength of 710 nm that were then directed onto a spatial light modulator (SLM). On one half of the SLM, we encoded the spatial projections required for the six-state protocol. On the other half, the same projections were superimposed with turbulence phase screens to simulate one photon propagating through turbulence. The substitution of a turbulent channel by a single phase screen is justified by the fact that we have assumed a weak scintillation regime, i.e., phase-only perturbations. The down-converted photons were then passed through 10 nm bandpass filters and coupled into single-mode fibers connected to single-photon detectors (Excelitas SPCM-AQRH-13-FC) with dark count rates of 250 counts per s and a 70% photon detection efficiency. Using holograms encoded on the SLM, we performed a state tomography of the two-photon state as a function of turbulence.

We modeled turbulence based on Kolmogorov's theory. We used the Strehl ratio (SR) as our measure of the turbulence

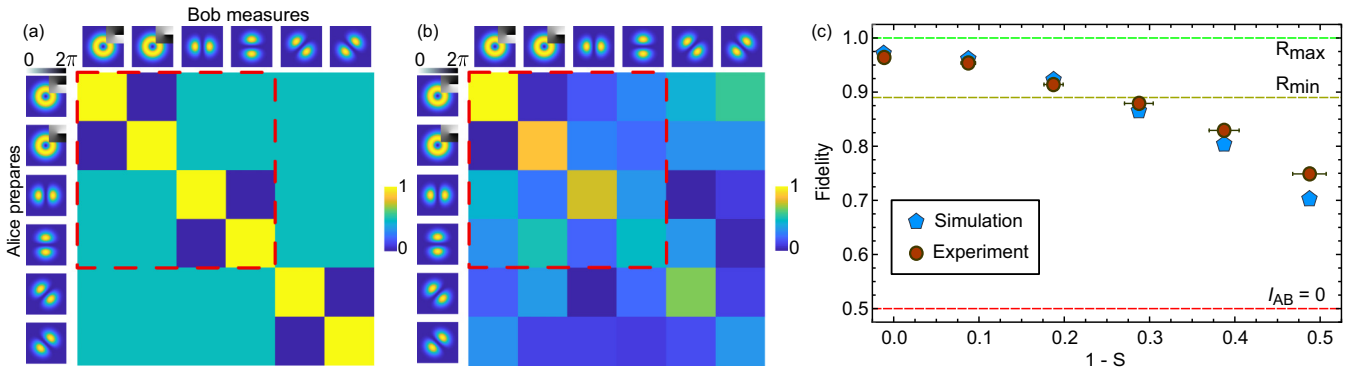

FIG. 2. Fidelity decay in turbulence. Alice and Bob perform joint measurements on the two-photon state for an entanglement based six-state protocol with OAM states carrying $\hbar$ of OAM per photon. These tomographic measurements are shown (a) in the absence of turbulence ($S = 1$) and (b) in the presence of turbulence with $S = 0.5$ for a mode size $\omega_0 = 800\ \mu$m. The regions enclosed by the red dashed lines (top left corner) show the measurements required for the traditional BB84. (c) The simulation matches experimental measurements of the decay of fidelity as a function of turbulence for OAM states with $|\ell| = 1$ and postselected beam width $\omega_0 = 200\ \mu$m.

strength

$$S = \frac{1}{1 + 6.88(\omega_0/r_0)^2}, \tag{10}$$

where ω_0 is the beam size and r_0 is Fried's parameter, expressed in terms of the refractive index structure C_n^2, wavelength λ, and propagation distance z as

$$r_0 = 0.185\left(\frac{\lambda^2}{C_n^2 z}\right)^{3/5}. \tag{11}$$

The above expression in Eq. (10) was obtained by applying the quadratic structure function approximation [48] to the general definition of SR presented in [49]. To generate the turbulence phase screen, we multiply the Kolmogorov power spectral density with a random complex function, then inverse Fourier transform the product following the method detailed in [28]. The effects of turbulence on the projective measurements are, by means of example, graphically depicted in Fig. 2(b) for a single turbulence phase screen with strength $S = 0.5$. Note that here the Strehl ratio is defined with respect to the Gaussian mode and only serves to define controlled turbulence conditions.

We chose to perform the experiment using two OAM states with $\ell = \pm 1$, as well as the corresponding MUBs. The fidelity measurement results, averaged over a total of 50 single turbulence phase screens per turbulence strength SR, are presented in Fig. 2(c). The uncertainty in the turbulence strength arises from the prior calibration measurements we performed to ensure the accuracy of the turbulence strength that was digitally encoded.

IV. DECAY OF FIDELITY AS A FUNCTION OF MODE SEPARATION

As predicted by Eq. (8), the measured fidelity decays with increasing turbulence strength. Interestingly, the fidelity in Eq. (8) is also seen to depend on the OAM used to encode the qubit information. For a given turbulence strength, states with higher helicity, ℓ, have higher fidelities, allowing for more robust quantum communication due to higher tolerance to noise. To illustrate the advantage of using higher values of OAM for robust QKD, we simulated the measurements that Alice and Bob would perform to build a key in the six-state protocol, using OAM modes with different topological charges.

The intensities of the OAM modes used are shown in Fig. 3 for $\ell = \{2, 4, 6, 8, 10, 20\}$. Each point on the graph corresponds to the fidelity of Bob's measurements at a given turbulence strength, averaged over 200 turbulence screens. Observe that the decay in fidelity is faster when using OAM states with lower OAM values, compared to those with larger OAM values. This is indeed consistent with the expected behavior of the fidelity deduced in Eq. (8). Note that the minimum fidelity for which the channel is still secure, that is $R > 0$, is chosen here to be $F = 0.89$. This is because for $F > 0.89$ the channel is viable for both the BB84 and the six-state protocol. The mutual information I_{AB} between Alice and Bob, given by

$$I_{AB} = 1 + Q\ \log_2(Q) + (1 - Q)\log_2(1 - Q), \tag{12}$$

vanishes for $Q = F = 0.5$.

It could be argued that the comparison between these modes is not a fair one due to the difference in mode size. Indeed, the size of an OAM mode depends on the OAM value according to the relation $\omega_\ell = \omega_0\sqrt{|\ell| + 1}$ [50]. The higher the OAM content, the larger the mode size. However, note that the strength of turbulence SR in Eq. (10) is inversely proportional to the square of the mode size; given fixed turbulence conditions (that is we fix r_0), larger beams would experience higher turbulence compared to smaller beams, and hence will experience higher OAM scattering. The results shown in Fig. 3 thus show that, despite experiencing higher turbulence, higher OAM modes still show more robustness compared to lower OAM modes due to their higher mode separation. To remove the dependence on beam size, we ran a second simulation where we normalized each OAM mode to the same size; that is, rather than encoding the same scale parameter ω_0 for all the modes, we assign each mode the OAM-dependent scale parameter $\omega_\ell = \omega_0/\sqrt{|\ell| + 1}$. This way, all OAM modes have identical beam size ω_0. The newly normalized states, together with the results of the simulation, are shown in Fig. 3(b). Observe that the rescaled modes now have a smaller radius.

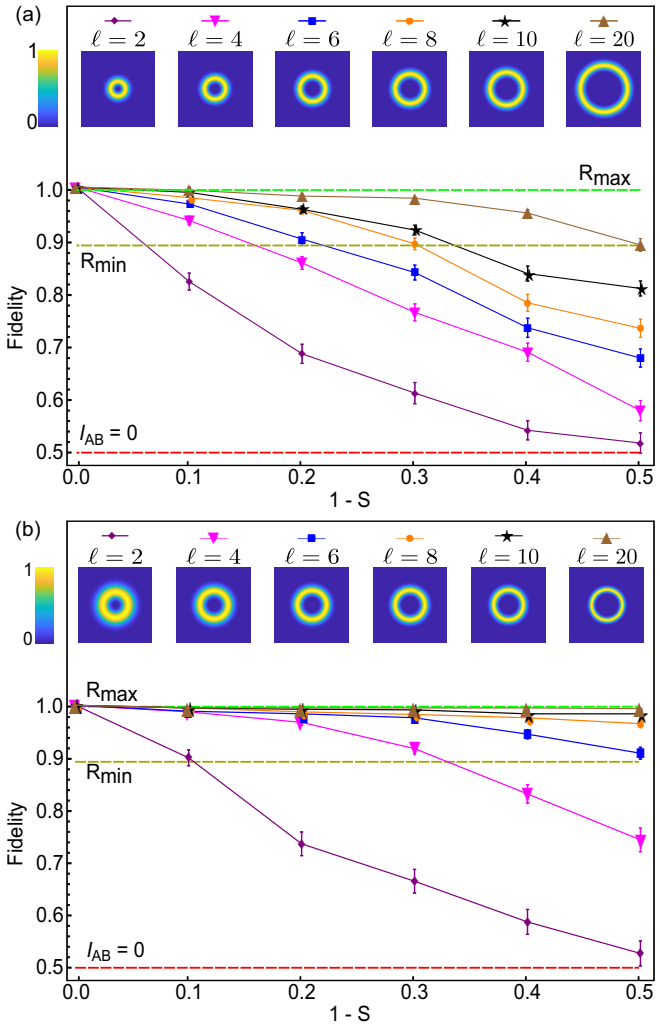

FIG. 3. (a) Simulated measurement of fidelity decay as a function of turbulence for OAM states with $\ell = 2$, 4, 6, 8, 10, and 20. The minimum secure key rate $R_{\min} = 0$ is attained for a fidelity of 0.89, while the mutual information I_{AB} vanishes for $F = 0.5$. (b) Simulated measurement of fidelity decay as a function of turbulence for OAM states with $\ell = 2$, 4, 6, 8, 10, and 20 with the modes all renormalized to the same size.

Hence they would experience less turbulence than in the cases presented in Fig. 3(a). Indeed, reducing the beam size has increased the robustness to turbulence as shown in Fig. 3. Similar to the previous simulation, modes with higher OAM content are even more resilient to turbulence.

Though QKD with higher-order modes is desirable due to the reduced crosstalk, there are some design challenges that need to be considered. In the case of photon pairs produced by parametric down conversion, as is the case here, the OAM correlation signal decays with increasing OAM index. This reduces the speed at which secure keys can be generated. A possible avenue that has been explored involves shaping the down-converted spectrum at the source. By changing the spatial profile of the pump laser, one is able to change the nature and amplitude of the spatial (OAM) correlations [51,52]. In this manner, one could engineer the OAM spectrum so that higher-order modes have higher correlation signals compared to the lower-order modes.

V. RECOVERY OF INFORMATION IN ADDITIONAL SUBSPACES

Atmospheric turbulence causes modal scattering, resulting in the broadening of the mode spectrum, transforming the maximally entangled qubit state in Eq. (3) into a high-dimensional entangled state as described in Eq. (4). However, when implementing the BB84 or six-state protocol, Alice and Bob postselect on a given OAM subspace, say $|\ell|$. The consequence of this postselection is the loss of information and therefore the decay of entanglement. Could Bob extend the postselected mode space to gain more information? Consider the scenario depicted in Fig. 4, where a quantum router that separates even and odd OAM modes [53] is placed after the turbulent channel but before Bob's detector. In this scenario, Alice projects her photon in the $|\ell| = 1$ subspace, while Bob makes his projections in both the $|\ell| = 1$ and $|\ell| = 2$ subspaces. Let $|\Phi\rangle_{ABo}$ and $|\Phi\rangle_{ABe}$ be the two-photon state shared by Alice and Bob at the detectors for odd and even $|\ell|$, respectively, as depicted in Fig. 4. Then

$$|\Phi\rangle_{ABo} = \frac{1}{\sqrt{\mathcal{N}_1}}(|1\rangle|1\rangle + |-1\rangle|-1\rangle) + \frac{b^2}{\sqrt{\mathcal{N}_1}}(|1\rangle|-1\rangle + |-1\rangle|1\rangle), \tag{13}$$

$$|\Phi\rangle_{ABe} = \frac{b}{\sqrt{\mathcal{N}_2}}(|1\rangle|2\rangle + |-1\rangle|-2\rangle) + \frac{b^3}{\sqrt{\mathcal{N}_2}}(|1\rangle|-2\rangle + |-1\rangle|2\rangle), \tag{14}$$

where $\mathcal{N}_1 = 2(1 + b^4)$ and $\mathcal{N}_2 = 2b^2(1 + b^4)$ are normalization constants.

One can compute the fidelity between Alice and Bob within the respective subspaces and show that they are given by Eq. (8). Thus for b sufficiently small (enough to guarantee that the secret key rate is positive) Bob can extract useful information by probing additional subspaces. However, here the measurement in the higher OAM subspace will only occur at a rate proportional to b^2. The effect of turbulence on the photon detection probability is shown in Fig. 4(c). As a quantitative illustration, the probabilities were normalized with respect to the two measuring subspaces. Losses resulting from turbulence in the primary channel $|\pm 1\rangle_A \otimes |\pm 1\rangle_B$ are accompanied by gains in the other channel $|\pm 1\rangle_A \otimes |\pm 2\rangle_B$, up to a limit defined by the turbulence parameter b. In the range of acceptable values for b ($F > 0.874$), postselecting on the additional OAM subspace allows a fraction of the decohered information to be recovered. We highlight that, while we have normalized the detection probability to only the measured subspaces, that is, we have assumed that scattering is limited to those two subspaces, one should expect a lower fraction of photons recovered when accounting for the full high-dimensional space after scattering. In the above, photon loss during sifting is not accounted for (1/2 in BB84 and 2/3 for the six-state protocol). Nevertheless, postselecting on additional subspaces would allow Bob to extract more

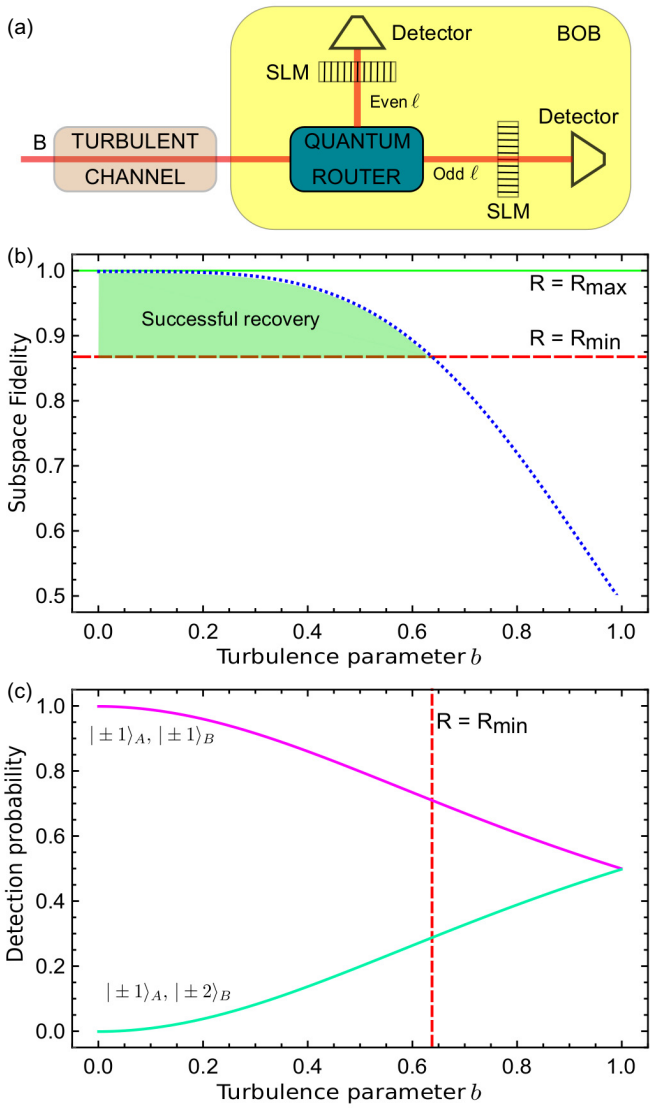

FIG. 4. Recovering information in higher OAM subspaces. (a) To increase photon recovery during QKD, Bob uses a quantum router to separate photon states according to their parity and postselects two OAM subspaces: $|\ell| = 1$ and $|\ell| = 2$. (b) The measurement fidelity of Alice and Bob, normalized to each of the two subspaces (dotted blue line). The range of turbulence parameter b for which information recovery is still possible is shown as the green shaded region enclosed by the $R_{\max}$, $R_{\min}$ and the fidelity curve. (c) The impact of turbulence on the relative photon detection probability in two measuring subspaces for Alice and Bob.

information from the QKD link, at a rate inversely proportional to the turbulence strength.

We also considered the possibility that the quantum router in Fig. 4 could have been introduced by an eavesdropper to extract the photons with $|\ell| = 2$ that would have otherwise been discarded by Bob through postselection. The eavesdropper, Eve, could for example attempt an intercept-and-resend strategy. This approach would however not be successful because of sifting losses: Eve would send photons to Bob with at least a 50% error in BB84 and over 66% in the six-state protocol. Hence probing additional subspaces would only benefit Bob and not the eavesdropper.

VI. CONVERSION OF NOISE INTO LOSS

The intermodal scattering incurred by an OAM state in the presence of turbulence can be represented as

$$|\Phi\rangle_{AB} = \mathbb{1} \otimes \hat{M}|\Phi^+\rangle_{AB}, \tag{15}$$

where $\hat{M}$ is an operator acting on Bob's qubit. In the context of QKD, it is not possible to obtain an exact picture of $\hat{M}$ by quantum state tomography given that multiple projections cannot be performed on a single photon. However, it has recently been shown that, in a one-sided channel, the decay of entanglement of a quantum state is identical to the decay of nonseparability in a classical vector beam [42]. As such, one could employ a nonseparable classical beam, sometimes called classically entangled, to reconstruct the channel operator. Because of the abundance of photons in the classical beam, the necessary projections for the quantum state tomography can be realized simultaneously with high signal-to-noise ratio. This would allow for real-time measurement of the channel and mitigation of errors on the quantum states measured. Importantly, this approach can be implemented optically as we outline next.

For a given realization of turbulence, i.e., a single phase screen in this case, the channel operator $\hat{M}$ admits the following polar decomposition:

$$\hat{M} = \hat{U}|\hat{M}| = \hat{U}(\lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|), \tag{16}$$

where $\hat{U}$ is a unitary operator and λ_i are the eigenvalues of the positive operator $|\hat{M}|$, with corresponding eigenstates $|i\rangle$. Note that if Alice and Bob encode information as shown in the previous sections, then the eigenstates $|i\rangle$ would correspond to superposition of the basis OAM states.

Given that $\lambda_i \leqslant 1$, implementing an inverse transformation is in general not always physically feasible; this is because the eigenvalues of $|\hat{M}|^{-1}$, $1/\lambda_i$, are larger than 1. Thus implementing the inverse channel transformation would imply adding identical copies of the photons to the system, something that is prohibited by the no-cloning theorem [54]. Alternatively, one can engineer a conjugate filter $\tilde{M}$, given by

$$\tilde{M} = |\tilde{M}|\hat{U}^\dagger = (\lambda_1|0\rangle\langle 0| + \lambda_0|1\rangle\langle 1|)\hat{U}^\dagger, \tag{17}$$

such that $\tilde{M}\hat{M} = \lambda_0\lambda_1\mathbb{1}$. Alice and Bob can then distill the initial state $|\Phi^+\rangle_{AB}$ at a rate proportional to $\lambda_0\lambda_1$, thus increasing the measurement fidelity of the QKD link. Interestingly, the state measured after applying the conjugate filter will have higher fidelity with respect to the initial state and, in our case, a higher degree of entanglement. This concentration of entanglement by means of local operations was first proposed in [55], where a set of maximally entangled singlet states could be filtered from an ensemble of nonmaximally entangled states. This process was later extended to mixed states [56] and experimentally demonstrated in two and higher dimensions [57–60]. In all these demonstrations, the entanglement concentration was achieved through Procrustean filtering, performed on both photons from an entangled pair. However, unlike the previous demonstrations, the method

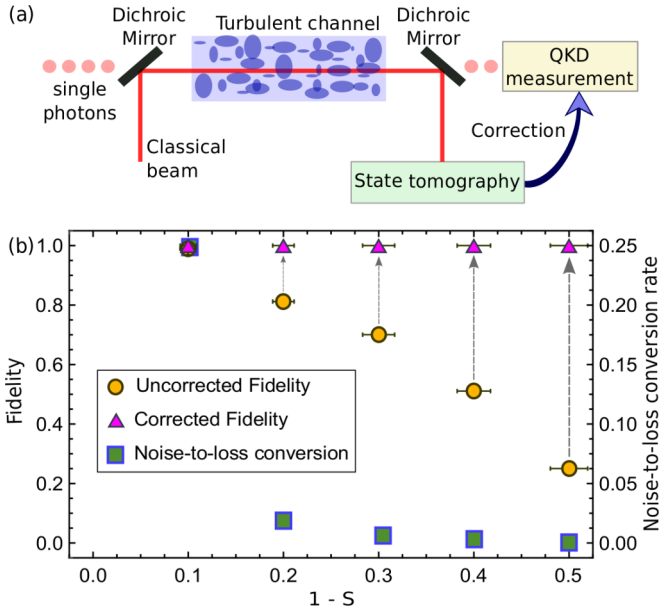

FIG. 5. Noise to loss conversion scheme with classical light. (a) Single photons, together with a bright classical beam, are sent through the same channel and analyzed separately. A state tomography of the classical beam is performed to reconstruct the channel operator. The classical data are subsequently used to perform a Procrustean filtering on the quantum state in real time. (b) The detection fidelity is computed from the measured two-photon density matrix in the presence of turbulence (uncorrected data). The channel matrix is reconstructed using a bright classical source and used to engineer a filter that cancels out the effect of turbulence, increasing the fidelity to unit (corrected).

we present here achieves entanglement distillation with local operations performed on only one of the entangled parties.

Let us demonstrate the scheme using a particular example from our simulation. Alice prepares the entangled state $|\Phi^+\rangle_{AB}$ and sends one qubit to Bob through a turbulent channel. Simultaneously, Alice sends a vector beam $|\Psi\rangle$ through the same channel, as shown in Fig. 5(a). The initial quantum and classical states are expressed as follows:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|\ell\rangle_A|\ell\rangle_B + |-\ell\rangle_A|-\ell\rangle_B), \tag{18}$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\ell\rangle|R\rangle + |-\ell\rangle|L\rangle), \tag{19}$$

where $|R\rangle$ and $|L\rangle$ are right- and left-circular polarization states.

In the presence of turbulence, the classical beam is transformed by a unitary phase screen, causing intermodal scattering. We assume that Alice and Bob postselect a particular OAM subspace for both the classical and quantum state. As a result of postselection, Bob receives the following classical state:

$$|\Psi_{\text{out}}\rangle = 0.53|\ell\rangle|R\rangle + 0.18e^{i\pi/3}|-\ell\rangle|R\rangle + 0.24e^{i\pi/5}|\ell\rangle|L\rangle + 0.47e^{-i\pi/8}|-\ell\rangle|L\rangle. \tag{20}$$

Note that the probabilities do not add to unity since we are projecting onto a particular OAM subspace. While the state could easily be normalized, we have purposely not done so to demonstrate the effect of postselection. The channel operator then reads

$$\hat{M} = \begin{pmatrix} 0.47e^{-i\pi/8} & 0.18e^{i\pi/3} \\ 0.24e^{i\pi/5} & 0.53 \end{pmatrix}. \tag{21}$$

We denote V and D the matrix of eigenvectors and eigenvalues, respectively, of the operator $\hat{M}^\dagger\hat{M}$. The positive operator $|\hat{M}|$ is computed as follows:

$$|\hat{M}| = V\sqrt{D}V^{-1} = \begin{pmatrix} 0.5167 & 0.1069+0.0085i \\ 0.1069-0.0085i & 0.5494 \end{pmatrix}.$$

One can then show that the positive operator $|\hat{M}|$ admits the following spectral decomposition:

$$|\hat{M}| = 0.4246|0\rangle\langle 0| + 0.6415|1\rangle\langle 1|,$$

where

$$|0\rangle = \begin{pmatrix} 0.7584 \\ -0.6497+0.0519i \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0.6497+0.0519i \\ 0.7584 \end{pmatrix}.$$

Note that the above eigenvectors are represented in the OAM basis where $|-\ell\rangle = (1\ 0)^T$ and $|\ell\rangle = (0\ 1)^T$.

The unitary matrix U is given by

$$U = \hat{M}|\hat{M}|^{-1} = \begin{pmatrix} 0.8356-0.4211i & -0.0053+0.3527i \\ 0.1836+0.3012i & 0.9337-0.0615i \end{pmatrix}, \tag{22}$$

such that $U^\dagger U = \mathbb{1}$.

One can then read off the expression of the positive conjugate filter to apply in the correction

$$|\tilde{M}| = 0.6415|0\rangle\langle 0| + 0.4246|1\rangle\langle 1|, \tag{23}$$

and show that $\tilde{M}\hat{M} = (0.6415 \times 0.4246)\ \mathbb{1}$. The result of the correction in this case is a conversion of noise from crosstalk, into loss: the identity operator obtained by applying the conjugate filter shows that the effect of turbulence can be completely removed from the final quantum state, resulting in entanglement distillation. The corresponding constant term quantifies the photon losses during the filtering process. A simulation of the noise-to-loss conversion on the fidelity is shown in Fig. 5(b) for single phase screen at various turbulence strengths. The observed increase in fidelity postfiltering comes at the cost of a reduced key generation rate, shown in Fig. 5(b).

VII. CONCLUSION

Spatial modes have shown promising potential to realize high-bandwidth quantum communication beyond the qubit. In free space, spatial modes are adversely affected by external perturbations during propagation, as a result of turbulence. Here we have considered a six-state protocol with OAM, showed the deleterious effects of turbulence on the secret key rate, and proposed two approaches to mitigate errors and losses. Unlike in previous studies, we have carefully accounted for mode-dependent size when comparing the decay in detection fidelity between OAM states.

To mitigate the effects of turbulence, we have proposed two schemes. On one hand, we have shown that, depending on

the strength of turbulence, more information can be recovered by postselecting a state space larger than the encoding one. However, the frequency of a viable detection in the additional subspaces increases with turbulence strength, a behavior not desired given that detection fidelity decreases with increasing turbulence strength. On the other hand, we have introduced an entanglement concentration scheme based on a classical measurement of the channel. We exploited the fact that entanglement dynamics of quantum and classically entangled states in a one-sided channel are indistinguishable to show that the classical beam can be used to probe the channel in real time. Reconstruction of the channel matrix in real time can be performed through a process tomography and used to perform Procrustean filtering on one party in the entangled pair shared by Alice and Bob. It is our opinion that the tools presented here will be useful in supplementing existing methods of turbulence mitigation for robust quantum (and classical) communication.

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

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[4] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, Opt. Exp. **12**, 3865 (2004).

[5] A. Mirza and F. Petruccione, J. Opt. Soc. Am. B **27**, A185 (2010).

[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Opt. Express **19**, 10387 (2011).

[7] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Science **356**, 1140 (2017).

[8] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Nature (London) **549**, 43 (2017).

[9] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).

[10] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[11] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Phys. Rev. A **88**, 032305 (2013).

[12] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Phys. Rev. Lett. **113**, 060503 (2014).

[13] 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, New J. Phys. **17**, 033033 (2015).

[14] 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, Optica **4**, 1006 (2017).

[15] B. Ndagano, R. Brüning, M. McLaren, M. Duparré, and A. Forbes, Opt. Express **23**, 17330 (2015).

[16] R. Brüning, B. Ndagano, M. McLaren, S. Schröter, J. Kobelke, M. Duparré, and A. Forbes, J. Opt. **18**, 03LT01 (2016).

[17] H. Huang, G. Milione, M. P. J. Lavery, G. Xie, Y. Ren, Y. Cao, N. Ahmed, T. An Nguyen, D. a. Nolan, M.-J. Li, M. Tur, R. R. Alfano, and A. E. Willner, Sci. Rep. **5**, 14931 (2015).

[18] G. Milione, M. P. J. Lavery, H. Huang, Y. Ren, G. Xie, T. A. Nguyen, E. Karimi, L. Marrucci, D. A. Nolan, R. R. Alfano, and A. E. Willner, Opt. Lett. **40**, 1980 (2015).

[19] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, New J. Phys. **16**, 113028 (2014).

[20] C. Gopaul and R. Andrews, New J. Phys. **9**, 94 (2007).

[21] C. Paterson, Phys. Rev. Lett. **94**, 153901 (2005).

[22] J. A. Anguita, M. A. Neifeld, and B. V. Vasic, Appl. Opt. **47**, 2414 (2008).

[23] B. Rodenburg, M. P. J. Lavery, M. Malik, M. N. O'Sullivan, M. Mirhosseini, D. J. Robertson, M. Padgett, and R. W. Boyd, Opt. Lett. **37**, 3735 (2012).

[24] G. A. Tyler and R. W. Boyd, Opt. Lett. **34**, 142 (2009).

[25] B. J. Smith and M. G. Raymer, Phys. Rev. A **74**, 062104 (2006).

[26] F. S. Roux, Phys. Rev. A **83**, 053822 (2011).

[27] F. S. Roux, T. Wellens, and V. N. Shatokhin, Phys. Rev. A **92**, 012326 (2015).

[28] A. Hamadou Ibrahim, F. S. Roux, M. McLaren, T. Konrad, and A. Forbes, Phys. Rev. A **88**, 012312 (2013).

[29] M. Malik, M. O'Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. J. Lavery, M. J. Padgett, and R. W. Boyd, Opt. Express **20**, 13195 (2012).

[30] F. M. Spedalieri, Opt. Commun. **260**, 340 (2006).

[31] F. Bouchard, F. Hufnagel, D. Koutný, A. Abbas, A. Sit, K. Heshami, R. Fickler, and E. Karimi, arXiv:1806.08018.

[32] L. Wang, S.-M. Zhao, L.-Y. Gong, and W.-W. Cheng, Chin. Phys. B **24**, 120307 (2015).

[33] S. K. Goyal, A. H. Ibrahim, F. S. Roux, T. Konrad, and A. Forbes, J. Opt. **18**, 064002 (2016).

[34] Y. Ren, G. Xie, H. Huang, C. Bao, Y. Yan, N. Ahmed, M. P. J. Lavery, B. I. Erkmen, S. Dolinar, M. Tur, M. A. Neifeld, M. J. Padgett, R. W. Boyd, J. H. Shapiro, and A. E. Willner, Opt. Lett. **39**, 2845 (2014).

[35] Y. Ren, G. Xie, H. Huang, N. Ahmed, Y. Yan, L. Li, C. Bao, M. P. J. Lavery, M. Tur, M. A. Neifeld, R. W. Boyd, J. H. Shapiro, and A. E. Willner, Optica **1**, 376 (2014).
[36] M. Li, M. Cvijetic, Y. Takashima, and Z. Yu, Opt. Express **22**, 31337 (2014).
[37] S. Li and J. Wang, Opt. Lett. **41**, 1482 (2016).
[38] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
[39] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[40] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[41] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012).
[42] 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, Nat. Phys. **13**, 397 (2017).
[43] C. Chen, H. Yang, S. Tong, and Y. Lou, Opt. Express **24**, 6959 (2016).
[44] R. Neo, M. Goodwin, J. Zheng, J. Lawrence, S. Leon-Saval, J. Bland-Hawthorn, and G. Molina-Terriza, Opt. Express **24**, 2919 (2016).
[45] B. Jack, J. Leach, H. Ritsch, S. M. Barnett, M. J. Padgett, and S. Franke-Arnold, New J. Phys. **11**, 103024 (2009).
[46] A. M. Yao and M. J. Padgett, Adv. Opt. Photon. **3**, 161 (2011).
[47] M. Agnew, J. Leach, M. McLaren, F. S. Roux, and R. W. Boyd, Phys. Rev. A **84**, 062101 (2011).
[48] J. C. Leader, J. Opt. Soc. Am. **68**, 175 (1978).
[49] L. C. Andrews and R. L. Phillips, *SPIE Press*, 2nd ed. (SPIE, Bellingham, WA, 2005), Vol. 1.
[50] W. Li, G. Feng, and S. Zhou, J. Mod. Opt. **60**, 704 (2013).
[51] E. Kovlakov, S. Straupe, and S. Kulik, Phys. Rev. A **98**, 060301(R) (2018).
[52] S.-L. Liu, Z.-Y. Zhou, S.-K. Liu, Y.-H. Li, Y. Li, Chen-Yang, Z.-h. Xu, Z.-d. Liu, G.-C. Guo, and B.-S. Shi, Phys. Rev. A **98**, 062316 (2018).
[53] M. Erhard, M. Malik, and A. Zeilinger, Quantum Sci. Technol. **2**, 014001 (2017).
[54] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[55] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[56] R. T. Thew and W. J. Munro, Phys. Rev. A **63**, 030302 (2001).
[57] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, Nature (London) **409**, 1014 (2001).
[58] N. A. Peters, J. B. Altepeter, D.A. Branning, E. R. Jeffrey, T.-C. Wei, and P. G. Kwiat, Phys. Rev. Lett. **92**, 133601 (2004).
[59] A. Vaziri, J.-W. Pan, T. Jennewein, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **91**, 227902 (2003).
[60] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, Nat. Phys. **7**, 677 (2011).