High-dimensional quantum key distribution based on mutually partially unbiased bases

Fumin Wang,[1,2] Pei Zeng,[3] Jiapeng Zhao,[2] Boris Braverman,[4,*] Yiyu Zhou,[2] Mohammad Mirhosseini,[5] Xiaoli Wang,[1]
Hong Gao,[1] Fuli Li,[1] Robert W. Boyd,[2,4,†] and Pei Zhang[1,6,‡]

[1] *MOE Key Laboratory for Nonequilibrium Synthesis and Modulation of Condensed Matter, School of Science, Xi'an Jiaotong University, Xi'an 710049, China*
[2] *The Institute of Optics, University of Rochester, Rochester, New York 14627, USA*
[3] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[4] *Department of Physics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5*
[5] *California Institute of Technology, Pasadena, California 91125, USA*
[6] *Shaanxi Key Laboratory of Quantum Information and Quantum Optoelectronic Devices, School of Science, Xi'an Jiaotong University, Xi'an 710049, China*

(Received 22 March 2019; accepted 25 February 2020; published 23 March 2020)

We propose a practical high-dimensional quantum key distribution protocol based on mutually partially unbiased bases utilizing transverse modes of light. In contrast to conventional protocols using mutually unbiased bases, our protocol uses Laguerre-Gaussian and Hermite-Gaussian modes of the same mode order as two mutually partially unbiased bases for encoding, which leads to a scheme free from mode-dependent diffraction in long-distance channels. Since only linear and passive optical elements are needed, our experimental implementation significantly simplifies qudit generation and state measurement. Since this protocol differs from conventional protocols using mutually unbiased bases, we provide a security analysis of our protocol.

DOI: 10.1103/PhysRevA.101.032340

I. INTRODUCTION

Quantum key distribution (QKD) is one of the well-known applications of quantum information, which promises secure communication—the "holy grail" of communication security—based only on the laws of physics [1–5]. A typical QKD protocol involves two parties who aim to generate a secret key by exchanging quantum signals over an insecure communication channel [6–15]. Security is assessed against the most powerful attack on the channel, where an eavesdropper perturbs the quantum systems using the most general strategies allowed by physical laws [16–20]. Traditionally, QKD protocols are performed with qubits, where the information is encoded in an ensemble of two-level quantum systems. In these binary QKD systems, the information capacity is limited to 1 bit per photon. To improve the information capacity of QKD systems, high-dimensional QKD has experienced rapid developments in recent years [21–31]. However, due to limited performance of generation and measurement techniques, the potential of high-dimensional QKD has not yet been fully exploited [32].

The orbital-angular-momentum states of photons form a promising state space that can be used to realize high-dimensional quantum systems [33–35]. The orbital-angular-momentum states of quantum number ℓ span an infinite-dimensional Hilbert space and thus more than 1 bit information can be encoded onto each photon [36]. Due to the severe mode mixing in multimode fibers, the orbital-angular-momentum modes have been commonly applied in free-space communications. Free-space communication can be advantageous in various circumstances, such as satellite-to-ground and intersatellite communication or connecting end users to network nodes where installing optical fibers is time consuming and expensive. A number of studies have investigated the benefits of employing orbital-angular-momentum modes in free-space quantum cryptography [37–43]. However, the existing realization of high-dimensional QKD protocols with orbital-angular-momentum encoding is still impractical in a realistic free-space link, and one important reason is the low efficiency in measuring single photons in two bases—the orbital-angular-momentum basis and its complementary Fourier conjugate angular basis [38]. The problem comes from the fact that the states in these two bases with different quantum number ℓ have ℓ-dependent diffraction. This mode-dependent diffraction will lead to a mode-dependent propagation phase (analogous to the Gouy phase for Laguerre-Gaussian states) as well as mode-dependent loss in the case of finite-sized apertures and long-distance propagation [31]. In this realistic scenario, current techniques for measuring the photons have a low efficiency and relatively high crosstalk, which lead to a system more vulnerable to quantum attacks.

Here, we propose a practical high-dimensional QKD protocol that overcomes the above challenges. Conventional QKD protocols are based on the mutual unbiased bases (MUBs). In a set of MUBs $\{B_0, B_1, B_2, \ldots, B_n\}$, a state in the B_k basis can be written as an equal superposition of all states in the B_j basis for any $j \neq k$. It can be shown that a Laguerre-Gaussian mode can be expressed as a coherent superposition of Hermite-Gaussian modes of the same mode order and vice versa [44],

[*] bbraverm@uottawa.ca
[†] robert.boyd@rochester.edu
[‡] zhangpei@mail.ustc.edu.cn

suggesting that the Laguerre-Gaussian and Hermite-Gaussian bases can be used in a QKD protocol. Since the Laguerre-Gaussian and Hermite-Gaussian bases are not fully mutually unbiased, we name this choice of bases as a set of mutually partially unbiased bases (MPUBs). For a practical realization of high-dimensional QKD, using the proposed MPUBs leads to a stable propagation by overcoming the mode-dependent diffraction. By using a passive $\pi/2$ mode converter [44], both Laguerre-Gaussian and Hermite-Gaussian modes can be easily generated and measured [45]. A security proof based on an asymptotic scenario is given in this work to confirm the security of the MPUB-based QKD protocol.

II. MUTUALLY PARTIALLY UNBIASED BASES

By using the relation between Hermite and Laguerre polynomials, a Laguerre-Gaussian state $|l_{n,m}\rangle$ of order (n, m) can be decomposed into a set of Hermite-Gaussian states $|h_{N-k,k}\rangle$ with the same mode order as [44]

$$|l_{n,m}\rangle = \sum_{k=0}^{N=m+n} i^k b(n, m, k)\, |h_{N-k,k}\rangle\,, \tag{1}$$

with real coefficients

$$b(n, m, k) = \left(\frac{(N-k)!k!}{2^N n!m!}\right)^{1/2} \times \frac{1}{k!}\frac{d^k}{dt^k}[(1-t)^n(1+t)^m]_{t=0}, \tag{2}$$

where the integer number $k \in [0, N]$, and $N = n + m$ is the mode order. The factor i^k in Eq. (1) corresponds to a $\pi/2$ relative phase difference between successive components. Similarly, a Hermite-Gaussian state rotated by 45°, $|h^{\urcorner}_{n,m}\rangle$ can be decomposed into exactly the same constituent basis set

$$|h^{\urcorner}_{n,m}\rangle = \sum_{k=0}^{N} b(n, m, k)\, |h_{N-k,k}\rangle\,, \tag{3}$$

with the same real coefficients $b(n, m, k)$ as above.

With the relations shown above, we can construct two MPUBs $\{l_{n,m}\}$ (the Laguerre-Gaussian basis) and $\{h^{\urcorner}_{n,m}\}$ (the Hermite-Gaussian basis), which are given by two sets of basis vectors:

$$\vec{L} = \{|l_{0,N}\rangle\,, |l_{1,N-1}\rangle\,, |l_{2,N-2}\rangle\,, \ldots, |l_{N,0}\rangle\}^T, \tag{4a}$$

$$\vec{H} = \{|h^{\urcorner}_{0,N}\rangle\,, |h^{\urcorner}_{1,N-1}\rangle\,, |h^{\urcorner}_{2,N-2}\rangle\,, \ldots, |h^{\urcorner}_{N,0}\rangle\}^T, \tag{4b}$$

with $\vec{L} = U_{LH}\vec{H}$. U_{LH} is the transformation matrix relating these two bases. The elements of U_{LH} are given by

$$u_{\mu,j} = \sum_{k=0}^{N} i^k b(\mu, N-\mu, k) b(j, N-j, k), \quad 0 \leqslant \mu, j \leqslant N, \tag{5}$$

where N is a positive integer. The $(N+1)$-dimensional QKD protocol is given as follows:

(i) Alice generates $\log_2(N+1)$ random bits (all the random bits we mentioned are generated with equal probability) as information to be encoded and one extra random bit P_A to decide the encoding basis: $\{|l_{n,m}\rangle\}$ or $\{|h^{\urcorner}_{n,m}\rangle\}$. Then Alice sends the corresponding $(N+1)$-dimensional qudit state to Bob.

(ii) Bob generates one random bit P_B to determine the measurement basis. Upon receiving the state, Bob measures the qudit state in $\{|l_{n,m}\rangle\}$ or $\{|h^{\urcorner}_{n,m}\rangle\}$ basis. From the measurement result, Bob receives $\log_2(N+1)$ bits of information.

(iii) Alice and Bob repeat steps (i) and (ii) for many rounds and keep their bits as raw data for later use.

(iv) Sifting process: Alice and Bob announce and compare all the P_A, P_B data. They compare P_A and P_B, discard raw data where $P_A \neq P_B$, and keep their bits with $P_A = P_B$ as the raw key.

(v) Alice randomly chooses half of the remaining events as test bits in order to estimate the bit error rate on the code bits and announces her selection to Bob. They compare the values of their test bits, aborting the protocol if the error rate is too high.

(vi) By public discussion, they run classical error correction and privacy amplification protocols to share a secret key.

According to Ref. [46], a fully random choice of basis is not necessary. An important advantage of $\{l_{n,m}\}$ and $\{h^{\urcorner}_{n,m}\}$ bases is that they have the same mode order so that the mode-order-dependent diffraction can be avoided. In addition, since the Laguerre-Gaussian and Hermite-Gaussian states in the same mode order can be directly expressed as states with certain azimuthal quantum number ℓ and radial quantum number p, the generation and detection of Laguerre-Gaussian modes and Hermite-Gaussian modes is much simpler compared to that of the orbital-angular-momentum state and its Fourier conjugate angular state.

III. PRACTICAL PERFORMANCE

A. Analysis of mode-dependent diffraction

MPUBs are free from mode-dependent diffraction because all modes used in the protocol have the same mode order, which leads to considerate transmission robustness. Compared with the MPUB-based QKD, the traditional orbital-angular-momentum encoding protocol suffers severe information loss due to mode-dependent diffraction. In the traditional protocol, one basis consists of orbital-angular-momentum states while the complementary basis is the Fourier conjugate angular basis [47]. The commonly used Fourier conjugate angular state of index j prepared by Alice is defined as

$$|j\rangle = \frac{1}{\sqrt{d}} \sum_{l=-L}^{L} |l\rangle \exp\left(\frac{-i2\pi jl}{d}\right), \tag{6}$$

where $d = 2L + 1$ is the dimension of the encoding space and L is the maximum orbital-angular-momentum quantum number used in the protocol. The Fourier conjugate angular basis $B_0 = \{|j\rangle\}$ and angular momentum quantum basis $B_1 = \{|l\rangle\}$ are mutually unbiased to each other. However, as we mentioned above, different orbital-angular-momentum modes diffract differently according to the quantum number. Hence, if a Fourier conjugate angular mode is prepared as an equal superposition of all orbital-angular-momentum modes, the received Fourier conjugate angular mode will be different from the transmitted state due to different propagation phases. In other words, the received state becomes a superposition

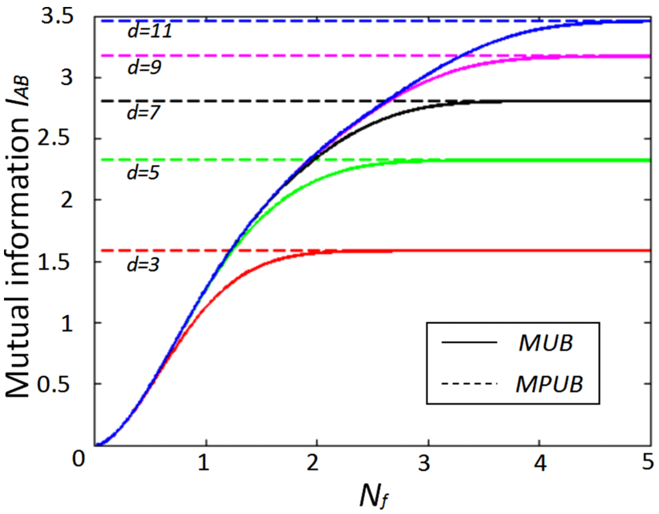

FIG. 1. The mutual information per detected photon, I_{AB}, as a function of N_f, where d is the dimension of the encoding space. The solid lines show I_{AB} in the MUB case, while the dashed lines give I_{AB} in the MPUB case. Since the states in MPUBs have the same mode order, the mutual information is independent of N_f, which means the influence of mode-dependent diffraction is fully eliminated in this case.

of Fourier conjugate angular states in the prepared basis [31]. Therefore, the error rate will increase when the mode-dependent diffraction is taken into consideration.

In order to show the performance of MUB and MPUB under the influence of mode-dependent diffraction, we assume a free-space link with distance z. In the case of a pair of circular apertures, the mode transmission efficiency is a function of the Fresnel number product N_f, which is given by

$$N_f = \frac{\pi D_1 D_2}{4\lambda z}, \tag{7}$$

where D_1 and D_2 are the diameters of the transmitting and receiving apertures, respectively, and λ is the wavelength [48].

The mutual information between Alice and Bob, I_{AB}, in the MUB and MPUB cases is shown in Fig. 1. In the MUB case, there are huge differences between small N_f and larger N_f. In this case, the detection probability distribution of orbital-angular-momentum states is nonuniform. Therefore, it is difficult to use these modes (with different mode orders) in long-distance QKD systems. The error induced by mode-dependent diffraction can be reduced by a sophisticated mode sorter, which increases experimental complexity. In the MPUB case, since the states have the same mode order, the mutual information is independent of N_f, which means the influence of mode-dependent diffraction can be fully eliminated.

B. Resistance to turbulence

For practical applications, the main problem of the transverse mode encoding QKD is the atmospheric turbulence. In this section, we simulate the practical performance of our MPUB-based protocol in a turbulence model [49] and compare it with the traditional MUB-based protocol with orbital-angular-momentum encoding in the same condition.

According to the method of Ref. [49], the cumulative effect of the turbulence over the propagation path can be modeled as a pure phase perturbation $\exp[i\phi(r,\theta)]$ on the beam at the output plane. So after going through the turbulence, the conditional probability of measuring a photon initially with Laguerre-Gaussian mode number l_0 to be l is given by

$$p(l) = \int_0^\infty |R(r,z)|^2 r \Theta(r, l - l_0)\, dr, \tag{8}$$

where $\Theta(r, l - l_0)$ is the circular harmonic transform of the rotational coherence function, which is given by

$$\Theta(r, l - l_0) = \frac{1}{2\pi} \int_0^{2\pi} C_\phi(r,\beta) \exp[-i\beta(l - l_0)]\, d\beta, \tag{9}$$

where $C_\phi(r,\beta)$ is the rotational coherence function of the phase perturbations at radius r. For the Kolmogorov turbulence model, the rotational coherence function at radius r is

$$C_\phi(r,\beta) = \exp\left[-6.88 \times 2^{2/3} \left(\frac{r}{r_0}\right)^{5/3} \left|\sin\left(\frac{\beta}{2}\right)\right|^{5/3}\right], \tag{10}$$

where r_0 is the Fried parameter [50]. The orbital-angular-momentum quantum number probability distribution for various Laguerre-Gaussian states propagating through Kolmogorov turbulence can be evaluated using Eqs. (8)–(10). For different mode orders, the effect of the phase perturbations depends on the radial power distribution of the beam, which for the LG_l^p is

$$\langle r^2 \rangle = \int_{r=0}^\infty R_{l,p}(r) r^2\, dr = (2p + |l| + 1)b^2, \tag{11}$$

where the azimuthal index $l = n - m$ and the radial index $p = \min(n, m)$. Equation (11) gives a characteristic relative mean-squared beam radius $r_{p,l} = b\sqrt{2p + |l| + 1}$.

The simulation results of the practical secure key rates (per detected photon) for the two protocols of different dimensions and in different turbulence levels are shown in Fig. 2. Apertures with a sufficiently large size are used for these simulations. The Fried parameter r_0 corresponds approximately to the spatial coherence length of the aberrations. For $b \ll r_0$, the reduction in the secure key rate caused by phase aberrations is small due to limited intermode crosstalk, but it increases rapidly as b becomes comparable to r_0. The simulation shows that when the encoding dimension $d \leqslant 4$, the behaviors of the two protocols are similar and the traditional MUB-based protocol has slightly better performance. When the dimension increases, the difference between the two protocols' behaviors becomes larger and the MPUB-based protocol has a higher key rate when $d > 4$.

To explain this, we should notice intermode crosstalk is more severe in higher-dimensional state space at a high level of turbulence. Therefore, the influence of turbulence takes a central role and causes the key rates to decrease when $d \geqslant 10$ in the MUB case and $d \geqslant 12$ in the MPUB case. This result reveals that the MPUB-based protocol is more resistant to the effects of turbulence. This resistance comes from the fact that the same mode order states obtain same beam radius $r_{p,l}$ in the transmission process. The key rates are calculated from the average bit error rate, which is the average of the bit error rates in

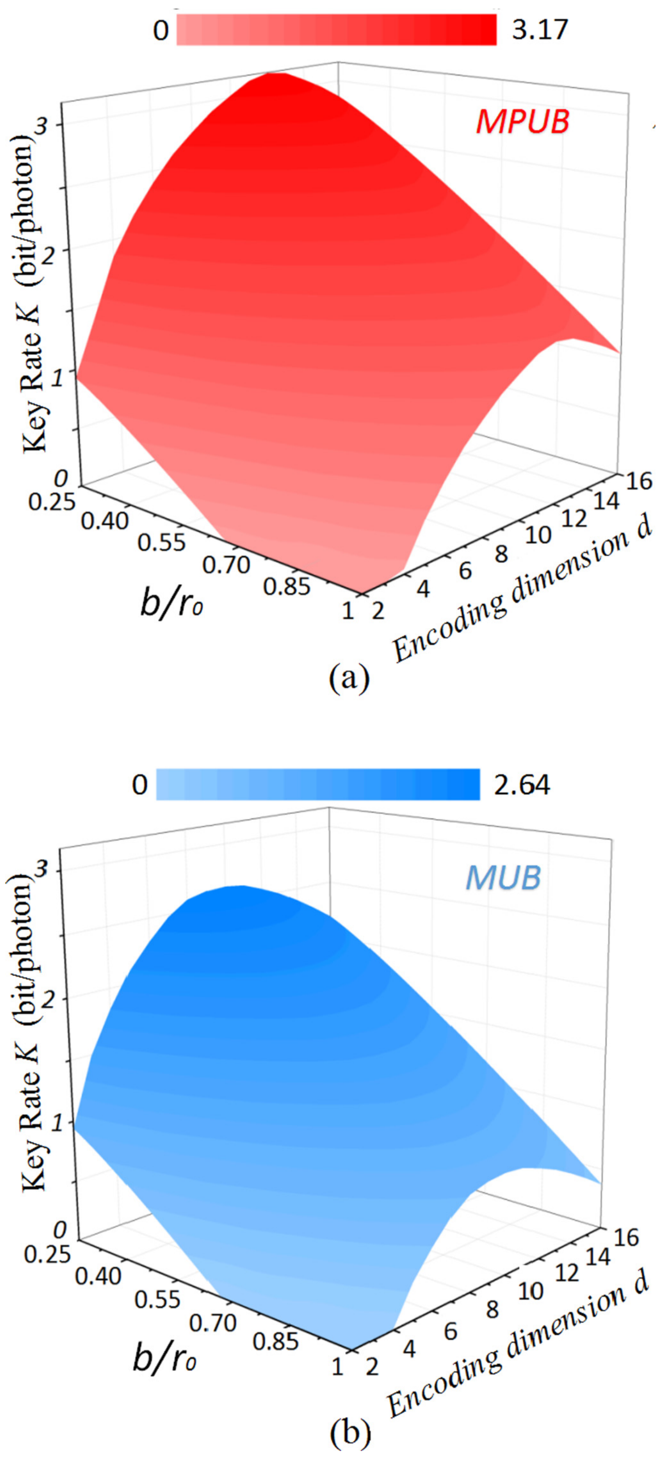

FIG. 2. Simulation of the key rates (per photon) as a function of the encoding dimension d and b/r_0. The Fried parameter r_0 corresponds approximately to the spatial coherence length of the aberrations and b is the width of the Laguerre-Gaussian mode. When $b \ll r_0$, the effects of the phase aberrations are weak and the intermode crosstalk is small, but they increase rapidly as b becomes comparable to r_0. For any encoding dimension $d \leqslant 4$, the behaviors of the two protocols are very similar. When the encoding dimension increases, the difference of the two protocols' behaviors becomes more obvious and the MPUB-based protocol has a greater key rate.

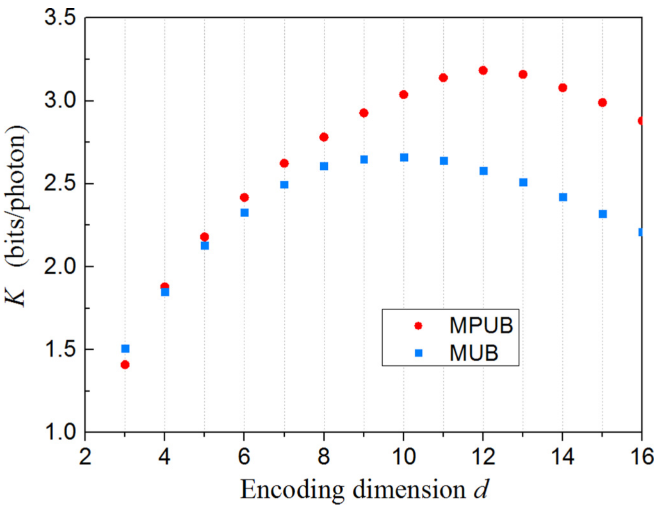

FIG. 3. Simulation of the key rate K as a function of dimension of the MPUB-based QKD (red circles) and MUB-based QKD (blue squares) at a fixed turbulence level. The parameters are set as $b = 0.01$ m and $r_0 = 0.08$ m, which corresponds to moderate ground-level turbulence strength $C_n^2 = 10^{-14}\,\mathrm{m}^{-2/3}$ and wavelength $\lambda = 1\,\mu\mathrm{m}$ [49].

two bases and can be directly calculated from the simulation data when $p(l = l_0)$ is known. In the MPUB protocol, during the measurement process, the Hermite-Gaussian states are converted to corresponding Laguerre-Gaussian states by using a $\pi/2$ converter. Therefore, the probabilities of measurement outcomes in the Hermite-Gaussian basis are calculated in the same way as above [Eqs. (8)–(11)].

Figure 3 shows the calculated key rates at a fixed turbulence level. The parameters here are set as $b = 0.01$ m and $r_0 = 0.08$ m, which corresponds to a moderate ground-level turbulence strength $C_n^2 = 10^{-14}\,\mathrm{m}^{-2/3}$ and wavelength $\lambda = 1\,\mu\mathrm{m}$ [49]. The results clearly show the difference between the two protocols analyzed above.

In this case, only the simulated turbulence influences the QKD system. The key rate K is given by [51,52]

$$K = \log_2 d + \frac{d+1}{d} Q \log_2\left(\frac{Q}{d(d-1)}\right) \times \left(1 - \frac{d+1}{d} Q\right) \log_2\left(1 - \frac{d+1}{d} Q\right), \qquad (12)$$

where Q is the average error rate calculated from $p(l = l_0)$.

C. Comparison with traditional QKD in free space

The first demonstration of free-space QKD over an atmospheric channel outside the laboratory was performed in 1996 [53]. Since then, several prepare-and-measure [13,54,55] and entanglement-based [56–58] systems have been implemented. A common feature of the above systems is the use of polarization encoding. The depolarizing property of the atmospheric channel is so weak that the states of polarization can be well maintained even after long-distance propagation. However, two-dimensional systems have a very limited information capacity, and such limitation cannot be resolved without involving other degrees of freedom.

Fortunately, the capacity limitation can be overcome in the MPUB-based system. By using the $\pi/2$ converter to transform Hermite-Gaussian states into Laguerre-Gaussian states, the system only needs to prepare and measure the Laguerre-Gaussian states, which simplify the implementation and can be easily extended to higher dimensions. Furthermore, Hermite-Gaussian states and Laguerre-Gaussian states both have symmetrical spatial constructions, because of which the encoded states are less influenced by rotation.

Above all, the development of traditional free-space QKD is approaching its upper limit. On the contrary, the orbital-angular-momentum-based free-space QKD systems are more promising in the near future to achieve higher-speed free-space communication. Moreover, the conventional QKD protocol with orbital-angular-momentum encoding suffers from turbulence distortion and diffraction loss, while these negative effects are minimized when using the MPUB protocol. Therefore, our work presents a step towards practical high-dimensional QKD.

IV. SECURITY ANALYSIS BASED ON UNCERTAINTY RELATIONSHIP

In this part, we prove the security analysis of the MPUB-based QKD system using the uncertainty relationship [59–62]. Suppose there are two bases $X \equiv \{|x_i\rangle\}$ and $Z \equiv \{|z_i\rangle\}$ $(i = 1, \dots, L)$ in an L-dimensional Hilbert space $\mathcal{H}$. The projection operators relative to these bases are $\{|x_i\rangle\,\langle x_i|\}$ and $\{|z_i\rangle\,\langle z_i|\}$. $H_X(\rho)$ and $H_Z(\rho)$ are the Shannon entropies of the probability distributions of the outcomes when measuring X and Z, respectively. From the previous works, the entropy uncertainty relationship is given by

$$H_X(\rho) + H_Z(\rho) \geqslant \log_2\left(\frac{1}{c}\right) := q_{MU} \quad \forall \rho \in \mathcal{H}, \tag{13}$$

where c is defined as the maximum overlap of any two states from the two bases,

$$c = \max_{i,j} c_{i,j}, \quad c_{i,j} := |\langle x_i|z_j\rangle|^2, \tag{14}$$

and $q_{MU} = -\log_2(c)$. For the two orthonormal but not fully unbiased bases $\{|l_i\rangle\}$ and $\{|h_i^{\urcorner}\rangle\}$ [these states are defined in Eqs. (1) and (3)], the maximum overlap $c = \max{(|u_{\mu,j}|^2)}$, where $u_{\mu,j}$ is defined in Eq. (5). Hence, the entropic uncertainty relationship for $\{|l_i\rangle\}$ and $\{|h_i^{\urcorner}\rangle\}$ is given by

$$H_{LG}(\rho) + H_{HG}(\rho) \geqslant -\log_2(\max |u_{\mu,j}|^2) \quad \forall \rho \in \mathcal{H}. \tag{15}$$

For the security analysis, a tripartite uncertainty relation is usually needed to constrain information available to an eavesdropper. In a tripartite scenario (as shown in Fig. 4), the initial state ρ_{ABE} is divided into three parts A, B, and E that are sent to Alice, Bob, and Eve, respectively. Suppose the subsystem held by Alice is ρ_A, and there are two complementary measurement bases (X and Z). The complementarity statement [23] says that the information Bob could obtain about one observable X_A by measuring his system B, plus the information Eve could obtain about the other observable Z_A by measuring E, cannot exceed a prescribed bound. So there is a certain unavoidable amount of uncertainty or entropy about the two observables conditioned on respective measurements of the two systems B and E. This uncertainty relationship [63] is given by

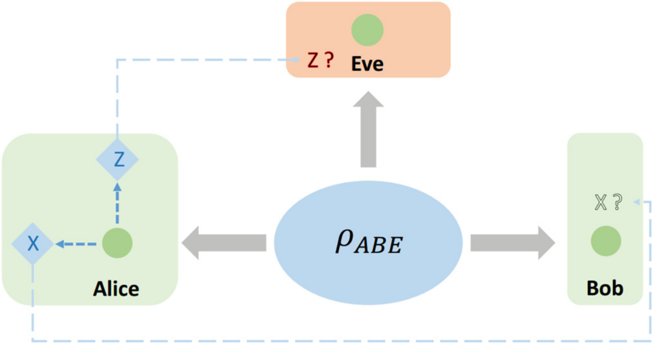

FIG. 4. Scenario of the tripartite uncertainty relationship.

$$H(X_A|B) + H(Z_A|E) \geqslant q_{MU}, \tag{16}$$

where $H(X|Y) = H(\rho_{XY}) - H(\rho_Y)$ is the conditional von Neumann entropy. $H(X_A|B)$ denotes Bob's uncertainty on the X measurement result and $H(Z_A|E)$ denotes Eve's uncertainty on the Z measurement.

We take Devetak and Winter's approach [64] for security analysis, which is based on the entanglement distillation of an entanglement-based QKD protocol. For our BB84-like protocol, an equivalent entanglement-based protocol can be easily defined. Two protocols are equivalent with respect to Eve if and only if

(i) The quantum state transmitted by Alice and all the classical signals revealed are the same.

(ii) All announced classical information is the same.

(iii) Alice and Bob perform the same measurement on the same quantum states to obtain the raw key bits.

(iv) Alice and Bob use the same postprocessing to extract secure secure key bits.

Suppose Alice prepares the state

$$\rho_0 := \frac{1}{\sqrt{N+1}} \sum_{i=0}^{N} |l_i\rangle_A\,|l_i\rangle = \frac{1}{\sqrt{N+1}} \sum_{i=0}^{N} |h_i^{\urcorner}\rangle_A\,|h_i^{\urcorner}\rangle\,, \tag{17}$$

which is defined on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}$. The qudit on space $\mathcal{H}_A$ is the ancillary state kept by Alice which is used to determine the encoded information. Bases $\{|l_i\rangle_A\}$ and $\{|h_i^{\urcorner}\rangle_A\}$ are two orthonormal bases on $\mathcal{H}_A$ which ensures Eq. (17) holds.

Alice then randomly chooses basis $\{|l_i\rangle_A\}$ or $\{|h_i^{\urcorner}\rangle_A\}$ to measure her ancillary qudit based on the random bit P_A she generates. She keeps her measurement result as raw data a and sends the qudit in space $\mathcal{H}$ to Bob. Bob performs step (ii) of the protocol described above. It is easy to show that, with respect to Eve, this entanglement-based protocol is equivalent to the proposed protocol without entanglement. Let $M_L(A)$ $[M_L(B)]$ denote the measurement that Alice (Bob) performs on system A (B) to derive the raw key. The asymptotic key rate K_a for the entanglement-based protocol is given by the

Devatak-Winter formula [64]

$$K_a = H(M_L(A)|E) - H(M_L(A)|M_L(B)), \tag{18}$$

and

$$\rho_{M_L(A)M_L(B)} = \sum_{j,k} \mathrm{Tr}\big[\big(M_L^j \otimes M_L^k\big)\rho_{AB}\big]\, |l'_j\rangle\,\langle l'_j| \otimes |l_k\rangle\,\langle l_k|\,, \tag{19}$$

$$\rho_{M_L(A)E} = \sum_{j} |l'_j\rangle\,\langle l'_j| \otimes \mathrm{Tr}_A\big[\big(M_L^j \otimes I\big)\rho_{AE}\big]. \tag{20}$$

$\{M_L^j\}$ and $\{M_L^k\}$ are the sets of positive operator-valued measure elements associated with Alice's and Bob's measurements. The $H(M_L(A)|M_L(B))$ term in Eq. (18) reflects the cost for classical error correction, which is equal to the classical conditional Shannon entropy of the measurement results $M_L(A)$, $M_L(B)$. Using the tripartite uncertainty relationship [Eq. (16)], we have

$$H(M_L(A)|E) + H(M_H(A)|B) \geqslant q_{MU}\,, \tag{21}$$

where q_{MU} defined in Eq. (13) can be calculated from the basis transform matrix U_{LH}. Combining Eqs. (18) and (21), we can obtain

$$\begin{aligned} K_a \geqslant & -\log_2(\max|u_{\mu,j}|^2) - H(M_H(A)|M_H(B)) \\ & - H(M_L(A)|M_L(B)). \end{aligned} \tag{22}$$

V. PROTOCOL DESCRIPTION WITH A DIMENSION $d = 4$

Based on the above analysis, our protocol can be realized based on two MPUBs $\{l_{n,m}\}$ and $\{h^{\urcorner}_{n,m}\}$ for any Hilbert space dimension $d \geqslant 2$. Under realistic atmospheric turbulence, our protocol beats the MUB-based protocol when the dimension $d \geqslant 4$. Therefore, we consider the case of a four-dimensional QKD with $N = 3$ as an explicit example of the protocol's operation. Figure 5 shows the states used in our protocol (Hermite-Gaussian and Laguerre-Gaussian modes of order 3).

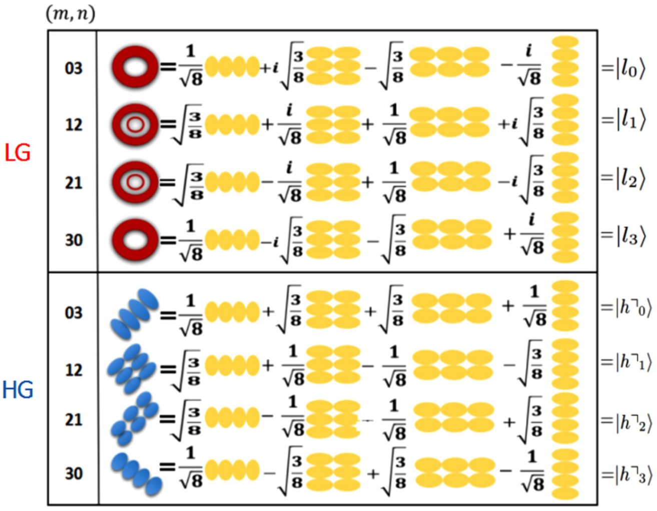
(m,n)
LG
HG
03
12
21
30
$= \frac{1}{\sqrt{8}} + i\sqrt{\frac{3}{8}} - \sqrt{\frac{3}{8}} - \frac{i}{\sqrt{8}} = |l_0\rangle$
$= \sqrt{\frac{3}{8}} + \frac{i}{\sqrt{8}} + \frac{1}{\sqrt{8}} + i\sqrt{\frac{3}{8}} = |l_1\rangle$
$= \sqrt{\frac{3}{8}} - \frac{i}{\sqrt{8}} + \frac{1}{\sqrt{8}} - i\sqrt{\frac{3}{8}} = |l_2\rangle$
$= \frac{1}{\sqrt{8}} - i\sqrt{\frac{3}{8}} - \sqrt{\frac{3}{8}} + \frac{i}{\sqrt{8}} = |l_3\rangle$
$= \frac{1}{\sqrt{8}} + \sqrt{\frac{3}{8}} + \sqrt{\frac{3}{8}} + \frac{1}{\sqrt{8}} = |h^{\urcorner}_0\rangle$
$= \sqrt{\frac{3}{8}} + \frac{1}{\sqrt{8}} - \frac{1}{\sqrt{8}} - \sqrt{\frac{3}{8}} = |h^{\urcorner}_1\rangle$
$= \sqrt{\frac{3}{8}} - \frac{1}{\sqrt{8}} - \frac{1}{\sqrt{8}} + \sqrt{\frac{3}{8}} = |h^{\urcorner}_2\rangle$
$= \frac{1}{\sqrt{8}} - \sqrt{\frac{3}{8}} + \sqrt{\frac{3}{8}} - \frac{1}{\sqrt{8}} = |h^{\urcorner}_3\rangle$

FIG. 5. Examples of the decomposition of Laguerre-Gaussian (red) and Hermite-Gaussian (blue) modes of order 3.

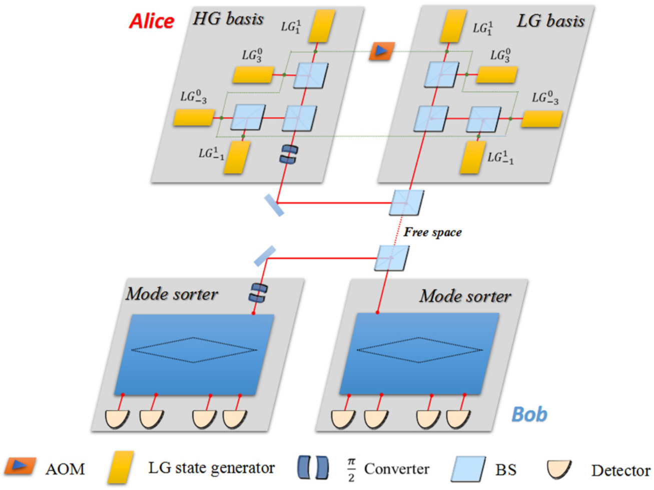

FIG. 6. Proposed experimental approach for four-dimensional QKD. Two $\pi/2$ converters are used for the transformation between LG and HG bases.

Each time, the state Alice chooses for information encoding is one of the eight states including $|l_i\rangle$ and $|h_i^{\urcorner}\rangle$ with $i = 0, 1, 2, 3$. The transformation matrix is given by

$$U_{LH} = \frac{1+i}{4}\begin{pmatrix} i & \sqrt{3} & -\sqrt{3}i & -1 \\ \sqrt{3} & -i & 1 & -\sqrt{3}i \\ -\sqrt{3}i & 1 & -i & \sqrt{3} \\ -1 & -\sqrt{3}i & \sqrt{3} & i \end{pmatrix}.$$

Figure 6 shows a sketch of a proof-of-principle experiment for the four-dimensional QKD protocol. The Laguerre-Gaussian state generators are used to prepare the original LG_l^p states including LG_3^0, LG_{-3}^0, LG_1^1, and LG_{-1}^1. All the generators are modulated by acousto-optical modulators. By using a digital radio frequency driver, acousto-optical modulators can quickly switch the generators, while a random number generator is used to control these acousto-optical modulators for choosing which state to be sent. In the state preparation and measurement part, the Laguerre-Gaussian mode states and the Hermite-Gaussian mode states can be transformed to each other with the help of a $\pi/2$ mode converter [44]. In our protocol, both the orbital-angular-momentum modes and radial modes are used, so at Bob's side a mode sorter is needed to detect the radial and azimuthal indices of LG_l^p states, which can be realized with recent advances in mode sorting [65–67]. Our protocol avoids generating and selecting grating patterns on active devices, which is the traditional method of MUB-based QKD for generating encoded states.

A promising potential of our protocol should be mentioned here. Due to the limitation of current optics technologies, there are no devices that can manipulate or switch the $\pi/2$ converter at a considerable speed. Once such set of devices is available, we can control the converter to switch between these two bases so that only one independent setup (generator or sorter) is needed for both Alice's and Bob's sides. Under such circumstances, the construction and operation of a MPUB-based high-dimensional QKD system could be as easy as the one of two-dimensional phase encoding QKD. However, it should be noted that our proposed protocol is still implementable in the absence of a switchable $\pi/2$ converter as shown in Fig. 6.

VI. CONCLUSION

In summary, we have proposed a practical high-dimensional QKD protocol. The MPUBs are used to avoid the mode-dependent diffraction and simplify the mode generation and detection so as to improve the secure key rate in practical application. For the experimental realization, a detailed approach based only on linear optical devices is presented, in which the speed of state generation mainly depends on acoustic-optical modulators which can reach gigahertz repetition rate. Moreover, it is straightforward to extend our protocol to higher-dimensional Hilbert spaces. Given its provable security and reasonable implementation, we believe that our protocol presents an important step towards realistic free-space quantum communication.

ACKNOWLEDGMENTS

We wish to thank Professor Xiongfeng Ma from Tsinghua University for helpful discussions. The authors acknowledge support from the Fundamental Research Funds for the Central Universities, the World-Class Universities (Disciplines) and the Characteristic Development Guidance Funds for the Central Universities, Joint Funds of the Ministry of Education of China (Grant No. 6141A02011604), Natural Science Foundation of Shaanxi Province (Grant No. 2017JM6011), National Natural Science Foundation of China (Grants No. 91736104, No. 11374008, and No. 11534008), and the U.S. Office of Naval Research. In addition, R.W.B. acknowledges support from the U.S. Office of Naval Research award ONR N00014-17-1-2443 and from the Natural Sciences and Engineering Research Council of Canada, the Canada Research Chairs program, and the Canada First Research Excellence Fund. B.B. acknowledges the support of the Banting Postdoctoral Fellowship.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

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

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

[6] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[8] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

[9] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).

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

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

[12] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82 (2002).

[13] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature (London) **419**, 450 (2002).

[14] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29**, 2797 (2004).

[15] M. Fujiwara, M. Toyoshima, M. Sasaki, K. Yoshino, Y. Nambu, and A. Tomita, Appl. Phys. Lett. **95**, 261103 (2009).

[16] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).

[17] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[18] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[19] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[20] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[21] J. S. Cotler and P. W. Shor, Quantum Inf. Comput. **14**, 1081 (2014).

[22] D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, Sci. Rep. **6**, 36756 (2016).

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

[24] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, Proc. Natl. Acad. Sci. USA **113**, 13648 (2016).

[25] S. Etcheverry, G. Cañas, E. S. Gòmez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Sci. Rep. **3**, 2316 (2013).

[26] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87**, 062322 (2013).

[27] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, and T. Gerrits, New J. Phys. **17**, 022002 (2015).

[28] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, Phys. Rev. Lett. **96**, 090501 (2006).

[29] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).

[30] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, npj Quantum Inf. **3**, 25 (2017).

[31] J. Zhao, M. Mirhosseini, B. Braverman, Y. Zhou, S. M. Hashemi Rafsanjani, Y. Ren, N. K. Steinhoff, G. A. Tyler, A. E. Willner, and R. W. Boyd, Phys. Rev. A **100**, 032319 (2019).

[32] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Inf. **2**, 16025 (2016).

[33] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Phys. Rev. A **45**, 8185 (1992).

[34] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 313 (2001).

[35] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, Opt. Express **12**, 5448 (2004).

[36] G. Molina-Terriza, J. P. Torres, and L. Torner, Phys. Rev. Lett. **88**, 013601 (2001).

[37] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, New J. Phys. **16**, 113028 (2004).

[38] 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).

[39] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).

[40] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, New J. Phys. **8**, 75 (2006).

[41] 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).

[42] M. P. J. Lavery, C. Peuntinger, K. Günthner, P. Banzer, D. Elser, R. W. Boyd, M. J. Padgett, C. Marquardt, and G. Leuchs, Sci. Adv. **3**, e1700552 (2017).

[43] 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).

[44] M. W. Beijersbergen, L. Allen, H. Van der Veen, and J. P. Woerdman, Opt. Commun. **96**, 123 (1993).

[45] J. Jia *et al.*, Appl. Opt. **57**, 6076 (2018).

[46] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).

[47] M. J. Padgett, F. M. Miatto, M. P. Lavery, A. Zeilinger, and R. W. Boyd, New J. Phys. **17**, 023011 (2015).

[48] G. A. Tyler, Opt. Lett. **36**, 4650 (2011).

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

[50] D. L. Fried, J. Opt. Soc. Am. **56**, 1372 (1966).

[51] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).

[52] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012).

[53] B. C. Jacob and J. D. Franson, Opt. Lett. **21**, 1854 (1996).

[54] J. G. Rarity, P. R. Tapster, and P. M. Gorman, J. Mod. Opt. **48**, 1887 (2001).

[55] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, Opt. Express **12**, 2011 (2004).

[56] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, Phys. Rev. Lett. **94**, 150501 (2005).

[57] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).

[58] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, Opt. Express **16**, 16840 (2008).

[59] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).

[60] K. Kraus, Phys. Rev. D **35**, 3070 (1987).

[61] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[62] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).

[63] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).

[64] I. Devetak and A. Winter, Proc. R. Soc. London A **461**, 207 (2005).

[65] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, Phys. Rev. Lett. **105**, 153601 (2010).

[66] Y. Zhou, M. Mirhosseini, D. Fu, J. Zhao, S. M. Hashemi Rafsanjani, A. E. Willner, and R. W. Boyd, Phys. Rev. Lett. **119**, 263602 (2017).

[67] X. Gu, M. Krenn, M. Erhard, and A. Zeilinger, Phys. Rev. Lett. **120**, 103601 (2018).