Tutorial Vol. 37, No. 11 / November 2020 / Journal of the Optical Society of America B A309

Journal of the Optical Society of America B

OPTICAL PHYSICS

High-dimensional cryptography with spatial modes of light: tutorial

Eileen Otte,[1] Isaac Nape,[2] Carmelo Rosales-Guzmán,[3,4] Cornelia Denz,[1] Andrew Forbes,[2] and Bienvenu Ndagano[5,*]

[1]Institute of Applied Physics, University of Muenster, Corrensstr. 2/4, D-48149 Muenster, Germany
[2]School of Physics, University of the Witwatersrand, Private Bag 3, Wits 2050, South Africa
[3]Centro de Investigaciones en Óptica, A. C., Loma del Bosque 115, Col. Lomas del Campestre, 37150 León, Gto., Mexico
[4]Wang Da-Heng Collaborative Innovation Center for Quantum Manipulation and Control, Harbin University of Science and Technology, Harbin 150080, China
[5]School of Physics and Astronomy, University of Glasgow, Glasgow G12 8QQ, UK
*Corresponding author: Bienvenu.Ndagano@glasgow.ac.uk

Received 2 June 2020; revised 14 August 2020; accepted 16 August 2020; posted 17 August 2020 (Doc. ID 399290); published 15 September 2020

Fast and secure sharing of information is among the prime concerns of almost any communication system. While commonly used cryptographic algorithms cannot provide unconditional security, high-dimensional (HD) quantum key distribution (QKD) offers an exceptional means to this end. Here, we provide a tutorial to demonstrate that HD QKD protocols can be implemented in an effective way using optical elements that are known to most optics labs. We use spatial modes of light as our HD basis and show how to simulate QKD experiments with bright classical light, fostering its easy implementation for a more general audience including industry laboratories or laboratory classes in university teaching and in advanced laboratories for validation purposes. In particular, we use orbital angular momentum Bessel–Gaussian modes for our HD QKD demonstration to illustrate and highlight the benefits of using spatial modes as their natural Schmidt basis and self-healing feature.

https://doi.org/10.1364/JOSAB.399290

1. INTRODUCTION

Data encryption enables secure communication between a sender and an intended receiver. This includes a secure communication channel and a powerful encryption algorithm. To guarantee that the encrypted information can only be retrieved by the legitimate parties, an important step is the secure distribution of a cryptographic key. While classical cryptographic methods are highly computationally secure even with unlimited computational power, quantum mechanics provides an information theoretically unconditional secure solution to the key exchange problem [1]. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e., non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (no-cloning theorem) [2,3]. This could be used to detect eavesdropping during key distribution. Note however that quantum cryptography does not prevent eavesdropping by this principle. Rather, it alerts the presence of an eavesdropper through security tests built on the fundamental laws of quantum mechanics that include Heisenberg's uncertainty principle and the non-cloning theorem [2,3]. Among the different algorithms of quantum cryptography, quantum key distribution (QKD) is the best-known and most developed one.

Quantum communication involves encoding information in quantum states called qubits, which are known to be more powerful than their classical counterparts bits. Photons are used as carriers for these qubits, with information encoded in a certain degree of freedom of the photons; polarization is one example. Perhaps the best-known QKD scheme is the BB84 protocol [4], proposed by Bennett and Brassard in 1984 and demonstrated in 1989 [5]. The BB84 protocol uses pairs of orthogonal states that belong to two bases that are not mutually orthonormal. In this cryptography protocol, a measurement of the photon state leads to so-called quantum indeterminacy, which is exactly the precondition of the no-cloning theorem; no single measurement can fully determine the quantum state if the encoding basis is unknown. Since its conception, the BB84 protocol has paved the way for other QKD protocols [5–8]. Nowadays, polarization and time-bin encoding have become

the workhorse of QKD protocols (see Refs. [9,10] for a comprehensive review), allowing them to reach into the commercial realm.

Recently, there have been many efforts to increase the performance of QKD protocols, with higher information capacity and longer transmission distances foremost amongst them [11–16]. High-dimensional (HD) QKD protocols with dimensions $d > 2$ have gained considerable attention of late, ranging from time-energy encoding in single mode fibers [17,18] to the additional use of the spatial degree of freedom by employing space-division multiplexing in multi-core fibers [19], linear momentum states [20,21], or, in particular, spatial modes of light [22–29]. This is because as the dimension increases, so does the information capacity per photon and the error threshold [30–32]. Particularly, Ecker *et al.* have shown experimentally that, in the case of entangled states, the increase in dimension can translate into an increased robustness to noise [33], supporting the view that HD QKD would be more tolerant to noise. To date, there have been many seminal advances in using spatial modes of light, including orbital angular momentum (OAM) and hybrid polarization-OAM modes, to perform HD QKD in free-space [34–41], in optical fibers [42], and underwater [43,44]. The spatial mode basis not only gives access to a larger dimension, but also allows us to exploit the inherent properties of the modes. For example, Bessel modes have been used in the study of self-healing entanglement and HD QKD through obstacles [41,45–47].

While many excellent reviews exist on the topic of HD spatial mode entanglement and HD QKD, there is little in the way of tutorial style approaches to edit this exploding research field for a more general audience including industry laboratories or laboratory classes in university teaching. In contrast, there are excellent educational treatise for demonstrating two-dimensional (2D) quantum systems and protocols, mostly based on polarization [48–55] but also with spatial modes as an encryption base [56]. The purpose of this tutorial is precisely to fill this gap. To this end, we take the reader through the process of understanding HD QKD, from fundamental concepts through to practical implementation. Especially, we show how to easily implement a proof-of-principle HD QKD using standard equipment of optics, exploiting the ability to simulate many quantum processes with bright classical light [56–59]. This supports bringing a more general audience closer to HD QKD, while allowing a route for researchers outside quantum information to test concepts prior to a full quantum implementation. We begin our explanation with 2D QKD, followed by a right-from-the-start description of the concepts involved in HD QKD. We reinforce concepts by taking the reader step-by-step through the process of an experimental implementation of a HD QKD protocol. By way of example, we use Bessel beams as our spatial mode basis and use the example to illustrate the benefits of a given mode set, e.g., the ability to self-heal behind obstacles and to propagate in an almost non-diffracting way over a certain distance [60].

2. QUANTUM KEY DISTRIBUTION: FROM TWO TO MANY DIMENSIONS

In this section, we present the original idea of QKD using polarization states, together with the key parameters one would compute to determine the viability of a QKD transmission. This will allow us to understand the appeal of extending QKD to higher dimensions, before discussing the means to realizing it.

A. QKD with Polarization

The original idea of QKD proposed by Bennett and Brassard [4] is illustrated in Fig. 1. Let us consider a communication protocol between two parties, Alice and Bob. As shown in Fig. 1(a), bits of information (0 or 1) are encoded in the polarization degree of freedom of photons. The sender, Alice, chooses to encode her bits in the orthonormal basis ψ, with elements $\{|H\rangle, |V\rangle\}$, where $|H\rangle$ and $|V\rangle$ are horizontal and vertical polarization states, respectively. Alice assigns a bit value to each of the states, say $|H\rangle \equiv 0$ and $|V\rangle \equiv 1$. The receiver, Bob, can decode the message by measuring the photons in the same basis as Alice. This communication protocol is, however, vulnerable to an attack by Eve, an eavesdropper. Provided Eve knows of Alice's basis, she can intercept the photons sent by Alice, measure them, and resend identically prepared photons to Bob without raising any suspicion.

To reveal the presence of the eavesdropper, Alice uses an additional basis ϕ with elements $\{|A\rangle, |D\rangle\}$, where $|A\rangle$ and $|D\rangle$ are anti-diagonal and diagonal polarization states, respectively, such that $|A\rangle \equiv 0$ and $|D\rangle \equiv 1$. The polarization states in the two bases are related as follows: $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ and $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. In this new protocol illustrated in

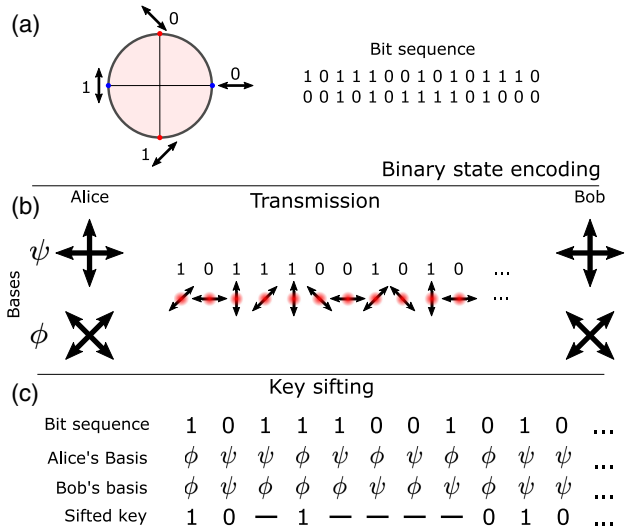

Fig. 1. Concept of QKD. (a) Classical bits are encoded in eigenstates of two polarization bases that are mutually unbiased. A classical bit sequence is sent in the process of generating the secret key. (b) A sender, Alice, randomly chooses a basis in which to encode the classical bits and sends them to Bob, the receiver. Bob randomly measures the photon states in either of the two bases. (c) At the end of the transmission, Alice and Bob publicly disclose their encoding and measurement bases and discard outcomes for which their bases do not match. The sifted key will further be checked to estimate the error rate in the transmission.

Fig. 1(b), Alice encodes bit values in either one of the ψ or ϕ bases, chosen *randomly*, unbeknownst to Bob and Eve, and sends a series of N bits to Bob. Similarly, Bob measures the photons in either of the two bases, chosen *at random*. When encoding and measurement bases match, Bob detects the correct state with unit probability. In the instances that the encoding and measurement bases do not match, Bob makes an ambiguous detection; for a given state encoded in the ψ basis, measurement in the ϕ basis leads to a 50% detection probability for the states $|A\rangle$ and $|D\rangle$. Thus, Bob cannot deduce the encoded state when measuring in the wrong basis. Crucially, this is also true for Eve and is ultimately what reveals her presence, as shown in the following.

At the end of the transmission, Alice and Bob *publicly* reveal the encoding and measurement bases for every transmitted state via a classical channel. They subsequently discard bit values measured in the instances where the encoding and measurement bases do not match, as shown in Fig. 1(c). In the absence of an eavesdropper, Alice and Bob should be left with, on average, a set of $N/2$ bits. However, in the presence of an eavesdropper, the remaining $N/2$ bits would be plagued with errors resulting from Eve's measurements. Importantly, while it is assumed that an eavesdropper has full knowledge about Alice's and Bob's systems, the security is not compromised, since the bases and key bits are chosen at random and privately. Recall that Eve would have guessed the wrong basis 50% of the time. Provided Eve intercepted all of the photons sent by Alice, she would resend to Bob a state in the wrong basis 50% of the time. Bob is thus left with, on average, $N/4$ correct bits and $N/4$ wrong bits. To reveal the presence of the eavesdropper, Alice and Bob *publicly* compare a subset of their sifted $N/2$ bits and estimate the error. Finally, the publicly disclosed subset is naturally discarded from the final key. Note that, evidently, this procedure is inefficient. Alternatively, they can assign different probabilities to the two polarization bases and then use one basis for generating the key while reserving the other for eavesdropping detection [61].

Depending on the estimated error, Alice and Bob will decide whether to discard the transmission or proceed with further privacy amplification and then encryption using the sifted key.

B. Security Analysis

The decision of whether or not to utilize a key obtained from a QKD protocol depends on the ability to securely exchange information in the presence of an eavesdropper. The extent to which this is possible is dictated by the error rate, Q, introduced in the sifted key. Physically, the error rate is the probability of Bob detecting the wrong state, given that he measured the photon in the correct basis. A standard procedure to determine Q is by building a transfer matrix for the system, as shown in Fig. 2. Alice prepares a given state, and Bob measures it in one of the bases that will be used for the protocol, chosen as ψ and ϕ. Bob's measurements result in detection probabilities is graphically depicted in Fig. 2 for polarization-based QKD (i, $j = \{1, 2\}$) and can be summarized as

$$T = \begin{pmatrix} |\langle\psi_i^{\text{Bob}}|\hat{U}|\psi_j^{\text{Alice}}\rangle|^2 & |\langle\psi_i^{\text{Bob}}|\hat{U}|\phi_j^{\text{Alice}}\rangle|^2 \\ |\langle\phi_i^{\text{Bob}}|\hat{U}|\psi_j^{\text{Alice}}\rangle|^2 & |\langle\phi_i^{\text{Bob}}|\hat{U}|\phi_j^{\text{Alice}}\rangle|^2 \end{pmatrix}, \quad \textbf{(1)}$$

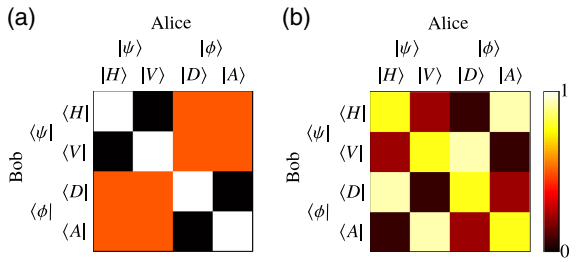

Fig. 2. Transfer matrices analysis of QKD with polarization states for a perfect system (a) $Q = 0\%$ and (b) $Q = 23\%$.

from which one then computes the error rate in the different bases:

$$Q_\psi = 1 - \frac{1}{2}\sum_{i=1}^{2} |\langle\psi_i^{\text{Bob}}|\hat{U}|\psi_i^{\text{Alice}}\rangle|^2, \quad \textbf{(2)}$$

$$Q_\phi = 1 - \frac{1}{2}\sum_{i=1}^{2} |\langle\phi_i^{\text{Bob}}|\hat{U}|\phi_i^{\text{Alice}}\rangle|^2. \quad \textbf{(3)}$$

The second term in Eqs. (2) and (3) is the probability that Bob measures the state $|\psi_i^{\text{Bob}}\rangle$ ($|\phi_i^{\text{Bob}}\rangle$), given that Alice sent the state $|\psi_i^{\text{Alice}}\rangle$ ($|\phi_i^{\text{Alice}}\rangle$) through a communication channel represented by the operator $\hat{U}$. This term is also known as the measurement fidelity (F). In the ideal case that $\hat{U}$ does not perturb the state, i.e., the channel is the identity operator, then F becomes equal to one and $Q = 0$. Note that it is not unusual to have $Q_\psi \neq Q_\phi$. The error rate for the QKD protocol as a whole is considered here as $Q = \text{mean}\{Q_\psi, Q_\phi\}$. Figure 2(a) graphically depicts the outcomes of a simulated transfer matrix T for $Q = 0$. When measuring in the correct basis, Bob unambiguously detects the state encoded by Alice. When using the wrong basis, Bob is unable to distinguish the encoded state, as all outcomes are equally likely. Comparatively, Fig. 2(b) shows a simulated instance where the communication channel ($\hat{U}$) introduces errors in the transmission, leading to an error rate Q of 23%.

Having estimated the error rate of the system, Alice and Bob can now quantitatively analyze the performance of their system by computing important quantum information parameters. The first of these is the amount of information that Alice and Bob share, and it is computed from [31]

$$I_{AB}(Q) = 1 + Q\log_2(Q) + (1 - Q)\log_2(1 - Q). \quad \textbf{(4)}$$

In the ideal case of $Q = 0$, the maximum amount of information that Alice and Bob can share, for every photon sent, is 1 bit. Assuming the presence of an eavesdropper (Eve), some information can be extracted during the transmission. One way to model this scenario is by assuming that Eve has at her disposal a cloning machine. However, from the no-cloning theorem [62], we know that Eve cannot copy an *arbitrary* quantum state. Hence, her action will inevitably introduce errors in the transmission between Alice and Bob; the more information Eve tries to extract, the more error she introduces. This becomes evident when looking at Eve's cloning fidelity, i.e., the ability to copy the state sent, given by Ref. [63]:

Table 1. Security Analysis of Simulated QKD Transfer Matrices in Fig. 2

Q	F	I_{AB}	F_E	I_{AE}	R_Δ
0	1	1	0.5	0	1
0.23	0.77	0.22	0.92	0.63	–0.56

$$F_E(Q) = \frac{1}{2}\left(1 + 2\sqrt{Q(1-Q)}\right). \tag{5}$$

This equation perhaps embodies appeal regarding the security of QKD: Eve can achieve a maximal cloning fidelity of one at the cost of introducing a 50% error in the transmission between Alice and Bob. The amount of information Eve shares with Alice can be computed by Ref. [63]:

$$I_{AE}(F_E,\, Q) = 1 + (F_E - Q)\log_2\left(\frac{F_E - Q}{1-Q}\right) + (1-F_E)\log_2\left(\frac{1-F_E}{1-Q}\right). \tag{6}$$

By maximizing her cloning fidelity, Eve can share one bit of information per photon with Alice, but introduces 50% error in the transmission between Alice and Bob. However, Eve can also choose to maintain her stealth by introducing a lower amount of error. This however will come at the cost of a reduced cloning fidelity and shared mutual information with Alice.

Assuming the presence of an eavesdropper that can potentially compromise the transmission and introduce error, a parameter of interest to Alice and Bob is the amount of secure information that they can exchange. This is called the secret key rate and is expressed as a function of the error rate with [64]

$$R_\Delta(Q) = 1 + 2(1-Q)\log_2(1-Q) + 2Q\log_2(Q). \tag{7}$$

To keep exchanging secret information, the secret key rate must be positive. This is ensured for $Q < 11\%$, reaching a maximum of 1 bit of secret information per photon for $Q = 0$. In Table 1 is a summary of the important information parameters, obtained for the simulated transfer matrices shown in Fig. 2.

C. Extending QKD to Many Dimensions

It is worth noting that in practice, all errors in the sifted key are attributed to the eavesdropper; this includes errors introduced by an eavesdropper when measuring the photons, imperfect preparation and detection of the quantum states, and importantly, the noisy nature of the communication channel. While the latter can be mitigated to some extent depending on the type of noise introduced in the channel, it is one of the limiting factors to long distance QKD protocols. Furthermore, losses incurred during propagation in the communication channel reduces the key transmission rate with increasing distance [65]. There is, therefore, an interest in increasing the robustness of QKD protocols, while packing as much secret information in every photon. One way to realize this is by increasing the dimension of the quantum states employed.

To this end, the different security parameters discussed above have been extended to higher dimensions [63]. The mutual information between Alice and Bob now takes the form

$$I_{AB}(d,\, Q) = \log_2(d) + (1-Q)\log_2(1-Q) + (Q)\log_2\left(\frac{Q}{d-1}\right). \tag{8}$$

Observe that now, the amount of secure information scales logarithmically with the dimension d; the more dimensions that are employed in the QKD protocol, the more information can be packed into every single photon. Interestingly, the increase in dimensions also has an impact on the eavesdropper cloning fidelity, which now reads

$$F_E(d,\, Q) = \frac{1}{d}\left(1 + (d-2)\,Q + 2\sqrt{(d-1)\,Q(1-Q)}\right). \tag{9}$$

The unfavorable $1/d$ scaling factor indicates that, compared to a 2D case, Eve has to introduce much more error to reach the maximum cloning fidelity of $(d-1)/d$. The associated mutual information shared between Alice and Eve,

$$I_{AE}(d,\, Q) = \log_2(d) + (F_E - Q)\log_2\left(\frac{F_E - Q}{1-Q}\right) + (1-F_E)\log_2\left(\frac{1-F_E}{(d-1)(1-Q)}\right), \tag{10}$$

scales favorably with dimension, allowing Eve to extract more information compared to the 2D case. Crucially, the fraction of secret information shared between Alice and Bob also scales favorably with dimension and, at the same time, encompasses all the benefits of HD QKD. In higher dimensions, the secret key rate for a two-basis protocol is given by Ref. [66]:

$$R_\Delta(d,\, Q) = \log_2(d) + 2(1-Q)\log_2(1-Q) + 2Q\log_2\left(\frac{Q}{d-1}\right). \tag{11}$$

Figure 3 graphically portrays the relation summarized in Eq. (11) between secret key rate R_Δ, error rate Q, and dimension d of the quantum state. There are two striking features to notice: (i) higher-dimensional states carry more information, and (ii) HD QKD protocols are more robust to errors. The high information capacity is enticing, as it allows us to counter

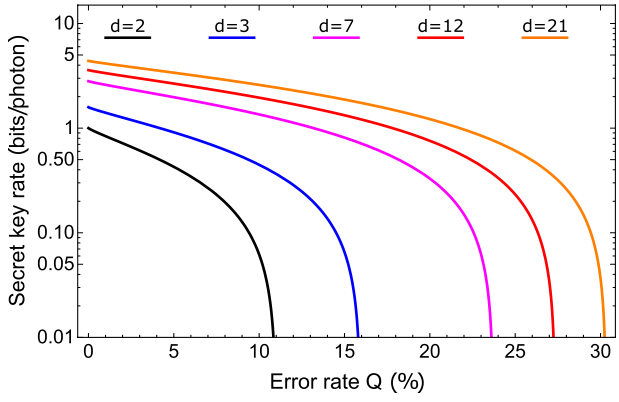

Fig. 3. Variation of the secret key rate R_Δ as a function of the error rate Q for dimensions $d = 2, 3, 7, 12$, and 21.

the effects of losses; in a communication channel with a given attenuation (optical fibers, for example), packing more information in every single photon increases the key transmission rate. Additionally, the higher error rate threshold means HD QKD protocols would be more secure in noisy channels compared to a 2D protocol.

One approach is to use the spatial degree of freedom of photons. In classical communication, spatial modes of bright classical light have been successfully used to encode information [67] and increase the information capacity in communication over free-space [68] and in fiber channels [68]. Tools to prepare and measure spatial modes of bright classical light have since been translated to the quantum regime to implement HD QKD with spatial modes in many dimensions [69–72]. While the choice of spatial modes is arbitrary, modes carrying discrete (quantized) OAM have taken center stage, and tools to measure them have been developed extensively [73–77].

3. FROM TWO- TO HIGH-DIMENSIONAL QKD WITH SPATIAL MODES

Although we have indicated that we will be using Bessel–Gaussian (BG) modes for this tutorial, it is pertinent to ask which modes could and/or should be used. The simple answer is that all modes sets are equivalent, in that they offer, in principle, unlimited dimensions. But there are other characteristics that may make you lean towards one over another. For example, OAM forms a natural Schmidt basis and is easy to measure with low loss devices, so, for these reasons, this is a very popular basis to select.

The family of transverse spatial modes that carry OAM are generally associated with complex fields $\Psi_\ell(r,\varphi) = A(r)\exp(i\ell\varphi)$ having radially (r) dependent amplitudes $A(r)$ and characteristic azimuthally (φ) dependent factors, $\exp(\mathrm{i}\ell\varphi)$. The discrete quantity $\ell \in \mathbb{Z}$, commonly referred to as the azimuthal index or topological charge, corresponds to an angular momentum of $\ell\hbar$ per photon. The discrete and unbounded nature of these modes with respect to the azimuthal index ℓ makes them attractive for HD encoding, since they form a complete basis on the Hilbert space of spatial modes. For this reason, an information basis beyond $d = 2$ dimensions can be constructed using the OAM basis modes.

Before we can construct such a basis, we first have to select a mode set that represents physical modes of free-space. Examples of applicable transverse OAM modes include Laguerre–Gaussian (LG) and propagation-invariant BG modes. These mode sets have identical azimuthal features, while their radial parts have distinctive attributes. For example, LG basis modes are discrete and complete in the radial degree of freedom, while, in contrast, the higher-order BG modes are continuous.

Some of the reasons to choose BG modes are (i) they carry OAM, (ii) the radial degree of freedom can be controlled by phase-only axicons, and (iii) they additionally offer some intriguing benefits such as the ability to reconstruct upon encountering obstructions. In fact, we will illustrate how to exploit this as part of the tutorial.

A. Constructing the Bases for QKD

The implementation of QKD with spatial modes follows the same approach described earlier for polarization states. First, recall the 2D encoding with the bases $\psi = \{|H\rangle, |V\rangle\}$ and $\phi = \{|D\rangle, |A\rangle\}$. Though the choice of these two bases may have seemed arbitrary, this was not the case. They were chosen because they are part of a set of mutually unbiased bases (MUBs). The key feature of MUBs is that one cannot, with a *single measurement*, distinguish a state prepared in one basis through a projection in another basis that is mutually unbiased. For example, projecting the state $|H\rangle$ in the ϕ basis leads to the following probability outcome: $|\langle D|H\rangle|^2 = |\langle A|H\rangle|^2 = 1/2$. As such, given a single photon prepared by Alice as $|H\rangle$, Bob (or Eve) cannot with a *single shot measurement* in the ϕ basis unambiguously identify Alice's state.

One may be interested to know how many such MUBs exist in a given number of dimensions. This is unfortunately not a trivial problem, and the answer is currently not known—their existence has only been proven for prime dimensions [78]. Nevertheless, for QKD, we do not need to know all MUBs, a minimum of two will suffice. In two dimensions, we have previously given the relation between the elements of two polarization MUBs: $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ and $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. One may have already deduced that elements of a third MUB can also be constructed in a similar manner, by varying the phase factor between $|H\rangle$ and $|V\rangle$ states. By this, we obtain right-circular and left-circular polarization states $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ and $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, respectively. It then follows that, given that a basis for a degree of freedom is known, states of a second, MUB can be constructed through a linear superposition of eigenstates of the first basis, with appropriate phase factors. In the following, we explore this approach for constructing 2D MUBs with spatial BG modes and their implementation in a QKD scheme. Further down, expanding to higher dimensions, we provide a recipe to construct this MUB in arbitrary dimensions.

B. Two-dimensional QKD with BG Modes

The transverse field of higher-order BG modes that carry OAM of azimuthal charge ℓ are expressed as [60]

$$\Psi^{\ell}_{\mathrm{OAM}}(r,\varphi) = \sqrt{\frac{2}{\pi}} J_\ell(k_r r)\exp\left(\frac{-r^2}{w_0^2}\right)\exp(i\ell\varphi). \tag{12}$$

Here, (r,φ) represent polar coordinates, k_r is the radial wave number, $J_\ell(\cdot)$ is the ℓ th-order Bessel function of the first kind, modulated by a Gaussian envelope with beam waist w_0. Crucially, BG modes of a given radial wave number obey the orthonormality relation

$$\int r\,\mathrm{d}r \int \mathrm{d}\varphi\; \Psi^{\ell}_{\mathrm{OAM}}\Psi^{m}_{\mathrm{OAM}} = \delta_{\ell,m}. \tag{13}$$

The BG basis thus provides an infinitely large set of orthonormal states that can be used for QKD. From this infinitely large set, we first restrict ourselves to a 2D state space to form the first basis consisting of the elements $|\Psi\pm\rangle = \Psi^{\pm1}_{\mathrm{OAM}}$. The intensity and phase maps of these modes are shown in Fig. 4(a).

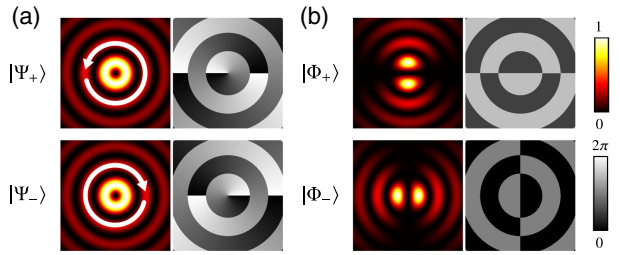

Fig. 4. MUB states for 2D QKD based on BG modes (transverse normalized intensity and phase distributions). (a) States $|\Psi_\pm\rangle$ carry an azimuthally varying phase structure, i.e., OAM of topological charge $\ell = \pm 1$ (white arrow: OAM handedness). (b) States $|\Phi_\pm\rangle$ represent the superposition of OAM modes, i.e., $(|\Psi_+\rangle \pm |\Psi_-\rangle)/\sqrt{2}$.

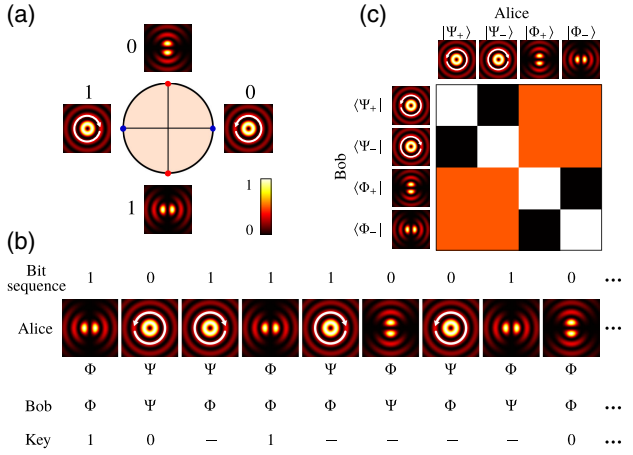

Fig. 5. Concept of 2D QKD with spatial modes of light. (a) Classical bits are encoded in eigenstates of OAM basis Ψ and basis Φ, which are mutually unbiased. (b) Key generation process (cf. Fig. 1, QKD with polarization). Alice randomly chooses a basis in which she sends bits of a classical bit sequence to Bob. The respective states represent spatial modes of light as indicated by transverse intensity distributions. Bob randomly selects a basis to measure the received modes. By comparison of selected bases, Alice and Bob create the shared key. (c) Transfer matrix for two-dimensional QKD-based (BG) spatial modes.

Following the approach for polarization-based QKD, we can construct a second MUB with elements that are given by $|\Phi_\pm\rangle = 1/\sqrt{2}(|\Psi_+\rangle \pm |\Psi_-\rangle)$. The transverse intensity and phase distributions of these modes are shown in Fig. 4(b).

With the MUBs chosen, Alice and Bob can perform QKD using spatial patterns in the very same way as using a polarization base. The procedure is illustrated in Fig. 5. Just as with polarization encoding, bits of information (0 or 1) are encoded in the OAM degree of freedom of photons, as depicted in Fig. 5(a). As illustrated in Fig. 5(b), the sender, Alice, chooses to encode her bits in the orthonormal spatial basis Ψ, with elements $\{|\Psi_+\rangle, |\Psi_-\rangle\}$, and the MUB $\Phi = \{|\Phi_+\rangle, |\Phi_-\rangle\}$. Subsequently, Bob measures the photons in either one of the two bases chosen *at random*. Similar to the approach based on polarization, the detection probabilities can also be represented using a transfer matrix, depicted in Fig. 5(c). Using this matrix, Alice and Bob perform a security analysis, similar to that shown with the polarization states in Section 2.B, to determine the security parameters.

Having introduced the principles of QKD in two dimensions with spatial modes, we are now in a position to extend these principles to higher dimensions. To do so, we will first present the construction of two MUBs in arbitrary dimensions. This construction procedure will be used in the next section to demonstrate an experimental QKD simulation with classical light.

C. HD QKD with BG Modes

In order to demonstrate the full capacity of spatial mode encoding in QKD, we expand the dimension of our MUBs. Employing BG modes, this simply implies selecting more modes in which we will encode information. Practically, this means that we will no longer just encode

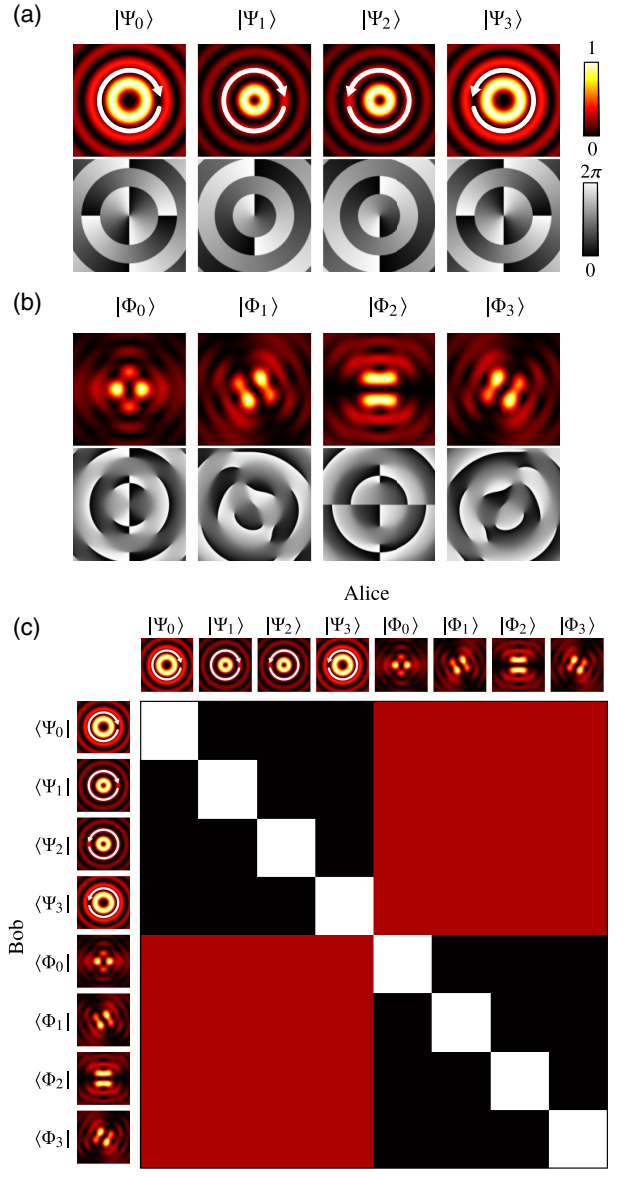

Fig. 6. HD QKD based on BG beams. (a), (b) Transverse normalized intensity (top) and phase (bottom) distribution of MUB states Ψ_j and Φ_j ($j \in [0, d-1]$), respectively, and (c) transfer matrix for $d = 4$.

0 and 1; instead, our alphabet becomes much richer with 0, 1, 2, 3, …, d. Our first HD encoding basis will thus consist of d orthonormal BG modes $\Psi^{\ell}_{\mathrm{OAM}}$. Let us label this basis as $\Psi = \{|\Psi_0\rangle, |\Psi_1\rangle, \ldots, |\Psi_{d-1}\rangle\}$. There *always exists* a basis $\Phi = \{|\Phi_0\rangle, |\Phi_1\rangle, \ldots, |\Phi_{d-1}\rangle\}$, mutually unbiased to Ψ, whose elements are obtained through the following construction [78]:

$$|\Phi_n\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp(i2\pi nk/d)|\Psi_k\rangle. \tag{14}$$

One can then obtain the mathematical relation between MUBs in arbitrary dimensions: $|\langle\Phi_n|\Psi_k\rangle|^2 = 1/d$. As an example, Figure 6(a) shows the intensity and phase maps basis state of a four-dimensional BG basis, carrying OAM $\ell = \{\pm 1, \pm 2\}$. The set of state from a MUB, constructed as per Eq. (14) is shown Fig. 6(b). A simulation of the ideal transfer matrix of these modes through a non-perturbing channel is shown in Fig. 6(c).

In the following, with the aim of highlighting the beneficial effects of high dimensions on security values, we will exemplarily illustrate a 21-dimensional QKD protocol using BG modes.

4. EXPERIMENTAL REALIZATION

To experimentally exploit the spatial degree of freedom of photons for HD QKD, one would first need to generate and measure individual photons. A now ubiquitous way of generating single photons is through spontaneous parametric down-conversion. In this process, a high-frequency photon from a pump laser is, with a certain probability, converted inside a non-linear crystal into a pair of lower frequency photons. These photons are spatially and temporally correlated; the two photons are born at the same place and at the same time. As shown Fig. 7(a) the down-converted pair of photons, due to conservation of momentum, exit the crystal with a certain angle—this angle is controlled by the crystal properties. Of the two photons, one is sent to Alice and the other to Bob. Alice performs a measurement using her spatial light modulator (SLM)—she prepares a state—while Bob does the same on his photon—he measures a state. Owing to the temporal correlation between the photons, a click on Alice's and Bob's detectors at the same time (coincidence detection) implies the detection of photons from the same pair. Counting the outcomes in coincidence ensures that only single photon states were used. We will use this experiment as the point of comparison for the tutorial. This quantum scheme can be mimicked with bright classical light in an easy-to-implement manner, using the set-up visualized in Fig. 7(b) [79].

In this classical experiment, Alice uses a laser and an SLM to prepare (encode) her state, which is then sent to Bob. Bob in turn performs the measurement step using his SLM, following the steps exactly as detailed earlier. In our demonstration, we used liquid crystal on silicon SLMs (Holoeye Pluto), but this can be replaced with digital micromirror devices (DMDs) to make the set-up cheap and fast. What makes the classical approach feasible is so-called back-projection and exploits Klyschko's advanced wave model [59]. The idea is that it is possible to treat the detection of the quantum entangled pair, in the retrodictive picture, as though one of the detected photon pairs is propagated backward (time reversed) through the system, reaching the crystal plane, then following the path of its twin photon to

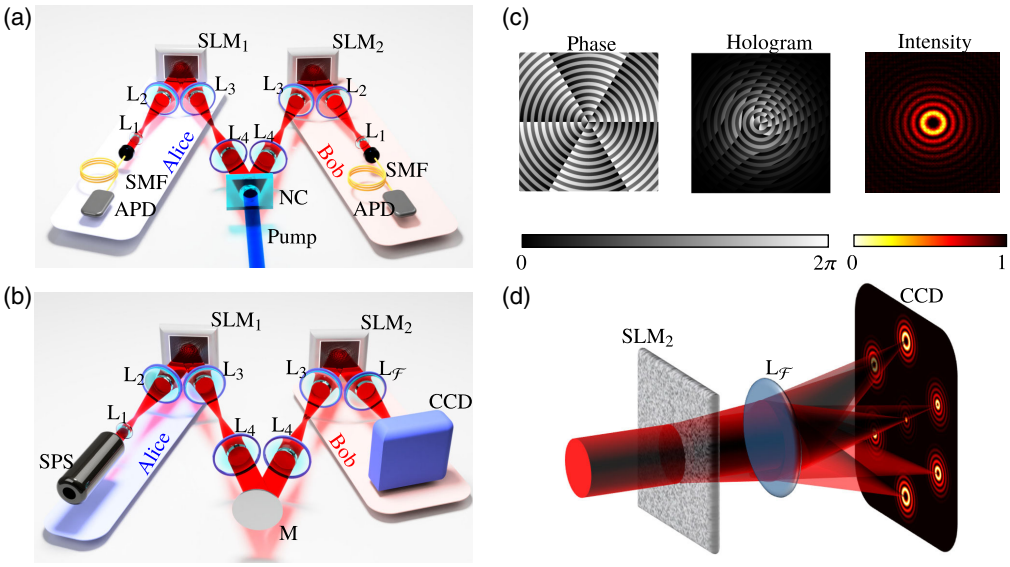

Fig. 7. (a) Sketch of experimental set-up using a single photon source (SPS). Two photons are generated from a nonlinear crystal (NC). Alice keeps one of the photons in her lab while transmitting the other to Bob. Alice encodes a Ψ or Φ basis mode using SLM_1 and sends the other to Bob where he also encodes a Ψ or Φ basis mode on SLM_2. The photons are detected in coincidence using single mode fibers (SMFs) and avalanche photo diodes (APDs). (b) In the classical back-projection analogue, Alice modulates a laser beam with mode chosen from the Ψ or Φ basis, where the resulting field is imaged to the mirror (M) plane, representing the NC plane, by lenses L_3 and L_4. The photon is then reflected from the mirror to SLM_2 and subsequently mapped to the far-field with a lens $\mathrm{L}_{\mathcal{F}}$ to a CCD camera. SLM_2, $\mathrm{L}_{\mathcal{F}}$, and the camera constitute Bob's measurement system. (c) Example of a binary phase function and respective hologram creating a BG mode $\ell = 6$ (right: normalized intensity). (d) Operating principle of Bob's decoding holograms in the simulation experiment.

the second detector. To achieve this, one needs only to replace Alice's detector with a laser source, producing the backward propagating photon, and the crystal with a simple mirror [79]. The physics requires that the SLM, mirror, source, and detector are all in the image plane of one another, easily achieved with imaging telescopes. This technique is routinely used in real quantum experiments for alignment. Now we suggest it as a simple tool to make the tutorial practical.

We are now ready to perform HD QKD. To begin, Alice randomly chooses a sequence of modes from two MUBs, which are generated with phase-only holograms on SLM_1 [cf. Fig. 7(c)], placed in the image plane of the crystal/mirror. Let us start with BG modes carrying OAM (Ψ_k modes from the first MUB); these are generated with binary holograms (comprising only values of 0 and π) defined by the transmission function

$$T(r,\varphi) = \text{sign}\{J_\ell(k_r r)\}\exp(i\ell\varphi), \tag{15}$$

with the sign function sign{·} [80,81]. To create a BG mode of chosen order ℓ, we encode the phase function with $k_r = 18\ \text{rad mm}^{-1}$ on a blazed grating (linear spatial phase ramp) and multiply the resulting hologram by a Gaussian aperture function ($w_0 = 0.89$ mm; wavelength $\lambda = 633$ nm), as shown in Fig. 7(c). The blazed grating allows the separation of modulated from un-modulated light from the SLM; the generated modes are formed in the first diffraction order, which we filter with an aperture. Modes Φ_n from the second MUB are engineered following Eq. (14) with Ψ_k experimentally coded using the transmission function $T(r,\varphi)$ in Eq. (15). Again, the respective phase functions are encoded on a blazed grating and multiplied by the Gaussian aperture function. For this tutorial, we chose to perform a QKD protocol with $d = 21$ dimensions. For this purpose, we used BG modes carrying OAM $\ell \in [-10, 10]$.

Bob measures the transmitted modes by decoding phase functions [Eqs. (15) and (14)] on SLM_2, in combination with a Fourier lens ($L_{\mathcal{F}}$) and a CCD camera. In the classical experiment, we record the on-axis intensity on the camera; this is proportional to the detection probability [73]. For quantum implementations, single mode fibers combined with single photon detectors would be used, counting the coincidences of the signal photon in Alice's arm and idler photon in Bob's arm [43]. To measure more than one mode at a time, we multiplex seven decoding holograms by assigning different granting angles to each encoded mode. Hence, each basis requires three decoding holograms, each containing seven phase functions. With this approach, different spatial positions in the detection plane correspond to different modes Ψ_k or Φ_n.

A. HD QKD Security Analysis

We sequentially prepared and measured photons encoded in the Ψ and Φ bases to build the transfer matrix. The intensity profiles of the modes are shown in Fig. 8(a): the OAM basis modes were chosen in the range, as shown in the top panel, while modes from the second MUB are shown in the lower panel. The ideal and experimental transfer matrices are shown in Figs. 8(b) and 8(c), respectively. Using the obtained transfer matrices, we proceeded to measure the key performance indicators, i.e., error rates and information quantifiers, as outlined in Section 2.C.

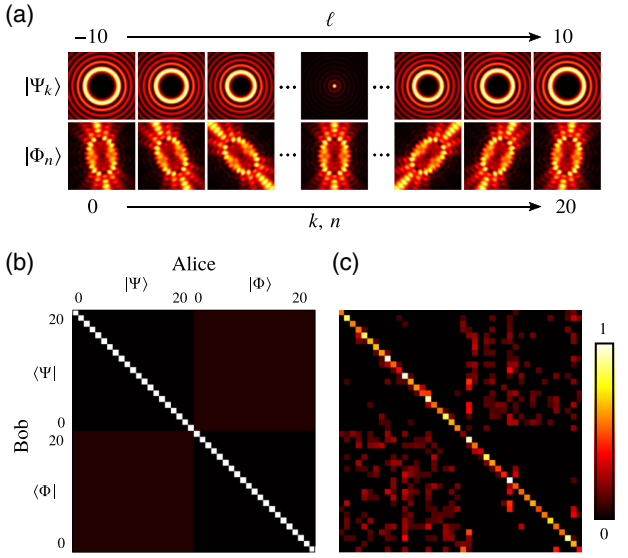

Fig. 8. (a) Transverse normalized intensity distributions of BG modes Ψ_k carrying OAM $\ell = [-10, 10]$ and states from an MUB, Φ_n, with $n, k = [0, 20]$. (b) and (c) show, respectively, the ideal and experimentally measured transfer matrix. The experimentally measured transfer matrix carries an error rate of 24%.

To extract the error rates, we used Eqs. (2) and (3) for each basis. We measured an average error rate of $Q = 24\%$, due to modal cross-talk from scattered light arising from diffraction orders. For a perfect system, the error rate would be $Q = 0$. Importantly, the error threshold for a 21-dimensional system is $Q = 32\%$, which is above our measured result, as desired. While the reduced performance is attributed to the detection method, the information capacity of the system can be boosted by employing refractive mode sorting [82], which can yield error rates as low as $Q = 8\%$ (equivalently a high fidelity of $F = 0.92$ was shown for $d = 25$). Now that we have confirmed that our system is below the error threshold, we can quantify the amount of secure information that can be shared over the channel using the previously discussed parameters.

We used Eq. (8) to compute the mutual information and obtained $I_{AB} = 2.56$ bits per photon (ideal value is 4.39 bits per photon). Note that this is beyond the 1 bit per photon limit for 2D QKD, highlighting the gain in information capacity from the increase in dimension. Furthermore, we measured the amount of information an eavesdropper can obtain from photons that she could successfully clone following Eq. (10), resulting in $I_{AE} = 1.36$ with a corresponding fidelity of $F_E = 0.456$. When compared to the 2D case for similar error rate in Table 1 ($Q = 23\%$, $F_E = 0.92$, and $I_{AE} = 0.63$), we note that although Eve's cloning fidelity is reduced due to the higher dimension, she shares more information with Alice, as discussed in Section 2.C. Finally, we estimated the secure key rate using Eq. (11) and obtained $R_\Delta = 0.73$ per photon. This level of secret information is well below the 2D limit of 1 bit per photon; this is due to the high error rate. However, it is worth realizing that the 24% error rate in this HD protocol is more than double what can be tolerated in the 2D case (11%), demonstrating the robustness of HD QKD protocols.

B. Generating a Key

Now that we have characterized the system and have obtained all key performance parameters for HD QKD, it is instructive to demonstrate the actual key generation and message encryption and decryption procedure, as illustrated in Fig. 9. We numerically simulated the key generation process by using the experimental transfer matrix in Fig. 8(c). In principle, the key generation procedure follows the same steps that are outlined in Section 2.A. The only difference is that the encoding basis now has $d = 21$ symbols (i.e., $0,\ 1,\ 2 \ldots, d-1$) as apposed to only two. As such, the discreet OAM modes (or Ψ basis), i.e., with charges $\ell \in [-10, 10]$, correspond to discrete numbers [0,20] constituting the encoding alphabet. The same holds for the MUB Φ.

In the numerical simulation of the key generation, we assumed Alice encoded photons with randomly selected modes from the Ψ or Φ basis, while Bob measured in a random basis that is also chosen between Ψ or Φ. Physically, Alice and Bob both possess a collection of values that are randomly selected numbers that either came from the Ψ or Φ basis. In the simulation, we represented them in the form of two matrices, one having the basis selections and the other having the chosen states. Following this, Alice announces her basis selections over a classical public channel, while Bob signals whether his detectors measured in the same basis or not. All instances where the basis selections were not correlated were discarded. In the simulation, this was achieved by comparing the entries of the matrices containing the basis selections and keeping only those that match. The remaining key bits constitute the sifted raw key. A graphical depiction of the procedure is illustrated in Fig. 9(a), while the simulated key for encrypting a gray-scale image with dimensions of 800×2200 pixels is shown in Fig. 9(b) (left). Ideally, once the sifted bits are obtained, Alice and Bob can exchange a fragment of the key to determine the error rate in order to obtain a lower bound on the key rate according to Eq. (11) and proceed with error correction to reduce the correlations between their key and any key bits obtained by an eavesdropper. While this step is essential, for brevity, we only used the sifted key. From our simulation, we obtained an error rate of 26%.

In Figs. 9(b) and 9(c), we depict the encryption and decryption procedure. A 800×2200 pixel image [X^{Message}, (c) "Encoded"] and Alice's sifted key [A^{Key}, (b) "Sifted key"] were mapped to 8 bit integers ranging from 0 to 255. From this, the image encryption was achieved via a bit wise XOR mapping between the key and the image, i.e., $EM = \text{bitwise XOR}(X^{\text{Message}}, A^{\text{Key}})$. The subsequent encryption message [EM, (b)] was then decrypted by performing a similar bitwise XOR mapping between the encrypted message and the key that Bob possesses (B^{Key}), i.e., $IM = \text{bitwise XOR}(EM^{\text{Message}}, B^{\text{Key}})$. The quality of the final decrypted image [(c) "Decoded"] depends on the bit error rate in their keys. The fidelity of the keys can be further improved with error correction and privacy amplification.

C. Bessel Advantage

As indicated earlier, we have chosen BG modes as exemplary modes for QKD since they do not only carry OAM, but also include a controllable radial degree of freedom, which assigns some intriguing properties to these basis states: propagation

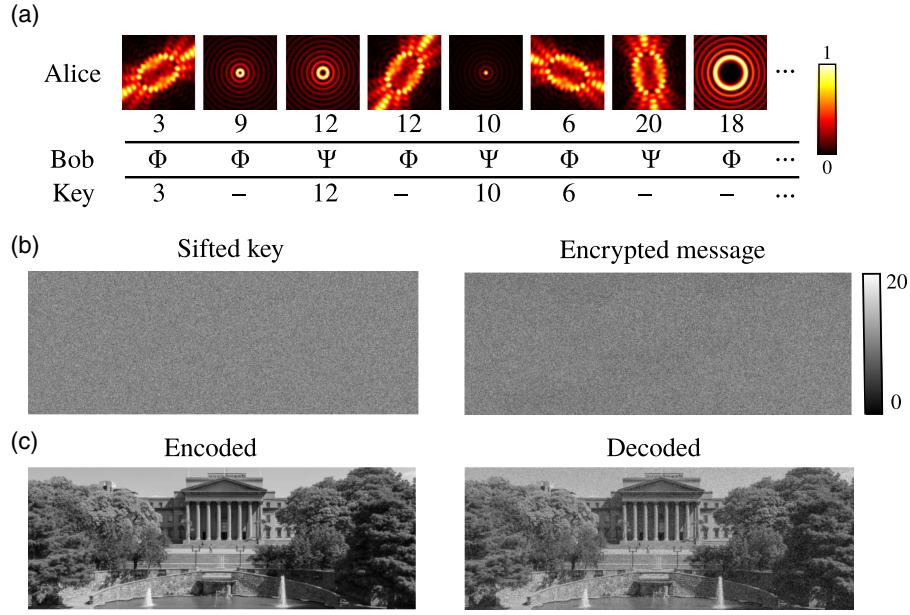

Fig. 9. Twenty-one-dimensional QKD with spatial modes. (a) Shared key generation process by prepare-and-measure procedure. Alice randomly chooses states of arbitrary basis, measured by Bob with a random choice of basis (Ψ or Φ). By comparison of basis choice, the shared key is filtered. (b), (c) The discrete levels [0,20] can be used to encode the gray-scale levels of a message in the form of an image. The applied sifted raw key resulting from a single QKD session with an error rate of $Q = 0.24$ [experimental data, cf. matrix in Fig. 8(c)], and the encryption and decryption procedure are illustrated. Alice encodes (c) an image with a (b) key generated from the QKD session. The image is then encrypted using bitwise XOR mapping between the image and key [encrypted message in (b)]. Bob subsequently decrypts the received image with his key by following the same procedure. The quality of the final decrypted image [(c) "Decoded"] depends on the bit error rate in their keys.

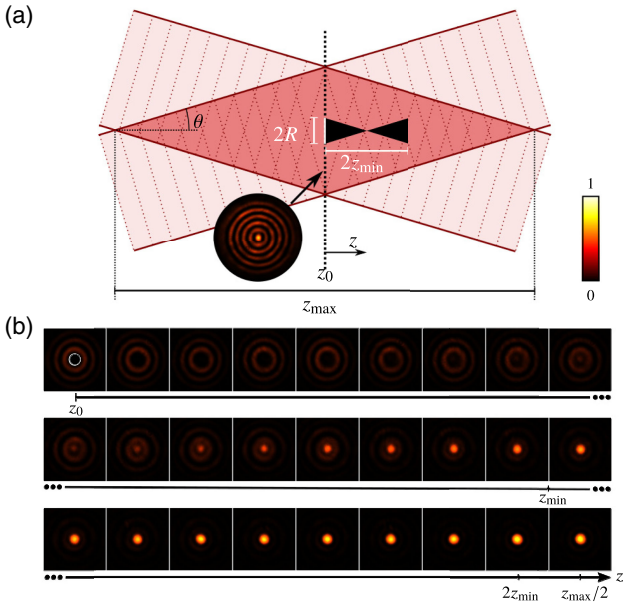

Fig. 10. Concept of self-healing BG mode. (a) Plane wave interference (red) for BG mode realization of non-diffracting distance $z_{\max}$. If an obstruction of radius R is included (white line at z_0), a shadow region (black) is formed. After $2z_{\min}$, the BG mode is fully self-healed. The inset shows the transverse intensity profile at z_0 of fundamental BG mode. (b) Experimental demonstration of self-healing behavior of fundamental BG beam. Transverse intensity images for different propagation distances z are shown (white circle: obstacle of radius $R = 150$ m).

invariance (or non-diffraction) as well as the ability to reconstruct upon encountering obstructions (self-healing). As visualized in Fig. 10(a), BG modes can be seen as a superposition of plane waves with wave vectors lying on a cone described by the angle $\theta = k_r/k$ (wave number $k = 2\pi/\lambda$) [60]. Hence, the respective intensity/amplitude and phase distribution stays transversely invariant for a defined propagation distance $z_{\max} = 2\pi\, w_0/\lambda k_r$ ("non-diffracting distance") [83]. If an obstacle of radius R is placed in the central z_0 plane within the non-diffracting rhombus-shaped region, the light field properties reconstruct after a certain distance due to coherent superposition of plane waves passing the obstruction. A BG mode is considered as fully self-healed after $2z_{\min}$ (see black shadow/self-healing region), i.e., two times the self-healing distance $z_{\min} \approx R/\theta \approx \frac{2\pi R}{k_r \lambda}$ [84]. At this distance, the obstructed transverse field distribution in the circular area of radius R at z_0 is fully reconstructed to its original distribution. This self-healing feature is exemplified in Fig. 10(b), presenting the transverse intensity distribution at different propagation distances of a fundamental BG mode obstructed by an absorbing obstacle of radius $R = 150$ m (white circle). The fundamental BG modes were experimentally shaped by a SLM applying Eq. (15); the obstacle was created digitally by circularly cutting a central area of chosen radius R in the respective hologram, representing the inclusion of an absorbing obstacle [47].

In performing HD QKD, one may now benefit from these special characteristics of BG modes [41,45]. Note that not only states from the BG basis Ψ_k show non-diffraction and self-healing, the MUB states Φ_n inherit these properties, as they represent a linear combination of BG modes. For chosen experimental settings ($k_r = 18\ \text{rad mm}^{-1}$, $w_0 = 0.89$ mm, $\lambda = 633$ nm), both mode sets have a non-diffracting distance of $z_{\max} = 49.16$ cm. We study the effect of self-healing on the security values of the above presented Bessel-based HD QKD protocol with $d = 21$ by determining transfer matrices for differently sized obstacles. For this purpose, we digitally generate artificial obstacles at z_0 within the modes sent by Alice by cutting a central area of chosen radius R in the respective SLM_1 hologram in our classical back-projection system [see Fig. 7(a)]. The digital generation of the obstacle allows for a dynamic change of obstruction characteristics. Now, we want to facilitate Bob's measurement within the non-diffracting distance of Alice's modes while investigating the influence of the obstacle on the system. Therefore, as illustrated in Fig. 11(a), we utilize a lens system (f, focal distance) imaging the encoding SLM_1 plane (z_0 plane) in front of SLM_2, so that Bob's detection plane is positioned at $z = \Delta z = 23$ cm $> z_0$. By this, we are able to adjust the level of self-healing at which Bob is performing his measurement. By changing the obstacles size within the z_0 plane, Bob is detecting a fully self-healed (black region) or obstructed (partially self-healed; green/yellow dashed lines) state [47].

We determine the transfer matrices for obstacles of sizes $R = \{150, 200, 500, 600\}$ m. Matrices are presented in Figs. 11(b)–11(e). For $R = \{150, 200\}$ m, modes sent by Alice fully self-heal before being detected by Bob, since $\Delta z \geq 2z_{\min}$ with $z_{\min} = 8.27$ cm and $z_{\min} = 11.03$ cm, respectively. In contrast, for $R = \{500, 600\}$ m, modes cannot fully reconstruct before being detected, as $\Delta z < 2z_{\min}$ with $z_{\min} = 27.57$ cm and $z_{\min} = 33.03$ cm, respectively. Note that, especially for larger R, applied superposition states Φ_n are more sensitive to on-axis absorbing obstacles than pure OAM states Ψ_k. Due to their structural complexity close to the optical axis [see Fig. 8(a)], which is not self-healed at the detection plane (for $R = \{500, 60\}$ m), the inner product of superposition states $\langle \Phi_{n_1} | \Phi_{n_2} \rangle$ gives lower matrix values than $\langle \Psi_{k_1} | \Psi_{k_2} \rangle$.

Security analysis results are summarized in Table 2 in comparison to ideal values as well as to experimental values if no obstacle is included ($R = 0$ m). The fidelity F reveals values of about 73–76% for fully self-healed modes [Figs. 11(b) and 11(c)], with equal fidelity for no obstacle (76%, see Section 4.A) and $R = 150$ m. In contrast, F decreases exponentially for larger obstacles ($2z_{\min} > \Delta z$), i.e., if non-reconstructed modes are considered. Hence, we observe a positive effect of self-healing on the fidelity: as modes self-reconstruct, the fidelity recovers as well. For the mutual information between Alice and Bob I_{AB} (in bits per photon), we determined values of about 2.43–2.56 for the undisturbed and self-healing case. Again, the value drops significantly with a decreasing level of self-healing (see I_{AB} values for $R = \{500, 600\}$ m) highlighting the advantage of self-reconstruction within the system. Note that, even though I_{AB} does not reach its full ideal potential (see ideal values in Table 1) due to experimental complexity, all values, even for partial self-healing, are significantly larger than the maximum achievable with only qubit states (=1). For fully reconstructed modes, we almost triple ($\times 2.43 - 2.56$) this value, while for non-self-healed modes we approximately double it ($\times 2.13$) or enhance it by a factor of 1.43.

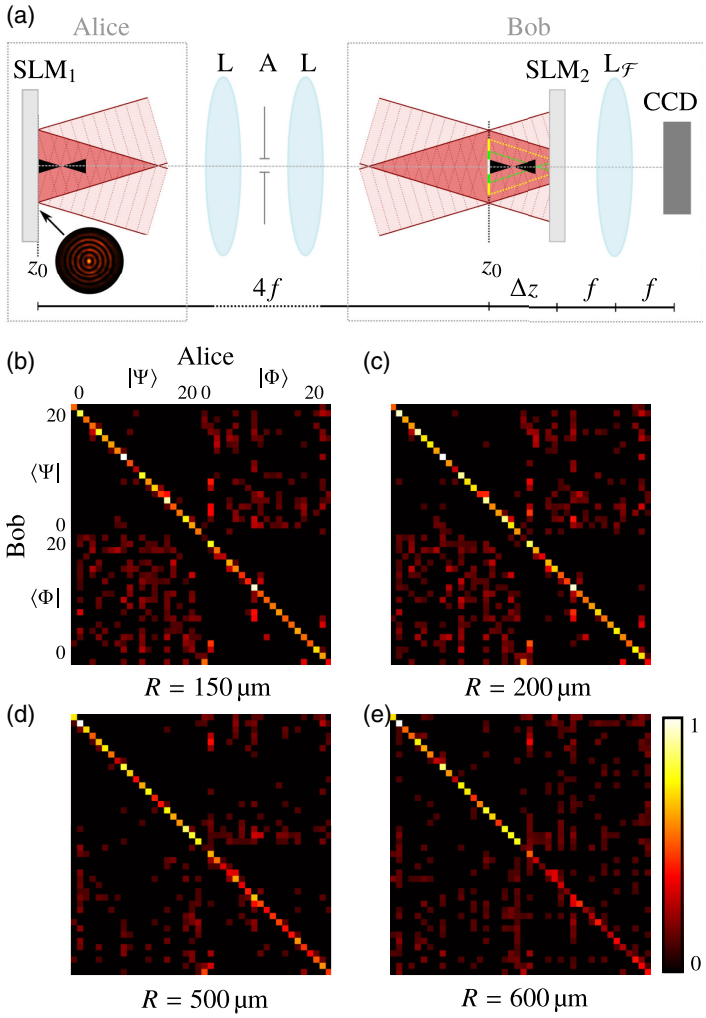

Fig. 11. Security analysis of Bessel-based HD protocol for included obstructions of radius R. (a) Experimental prepare-and-measure concept with adjustable self-healing level before detection by Bob [SLM, spatial light modulator, $L_{(\mathcal{F})}$; (Fourier) lens of focal distance f; A, aperture; CCD, camera]. By adapting the size of the digital obstructions on SLM_1, Bob measures modes sent by Alice when they are fully self-healed (black self-healing region) and when they are partially/not yet self-healed (green/yellow dashed line). (b)–(e) Transfer matrices for different obstruction sizes R, thus, self-healing levels. Alice's modes (b)–(c) can ($R = \{150, 200\}$ m) or (d)–(e) cannot ($R = \{500, 600\}$ m) fully self-heal before being measured by Bob.

Table 2. Security Analysis on Bessel-Based HD Protocol Summarizing the Detection Fidelity F, Mutual Information I_{AB} between Alice and Bob, Eve's Cloning Fidelity F_E and Mutual Information I_{AE} with Alice, Quantum Error Rate Q and Lower Bound of the Secret Key Rate R_Δ (in bits/photon) for Obstacles of Different Radii R as well as the Ideal Case Without Obstacle

R in μm	0	150	200	500	600	Ideal
F	0.76	0.76	0.74	0.69	0.54	1
I_{AB}	2.56	2.56	2.43	2.13	1.44	4.39
F_E	0.45	0.45	0.47	0.53	0.67	0.048
I_{AE}	1.36	1.36	1.48	1.75	2.44	0
Q	0.24	0.24	0.26	0.31	0.45	0
R_Δ	0.73	0.73	0.46	–0.12	–1.51	4.39

Similar to Eve's cloning fidelity for the non-obstructed case ($F_E = 0.45$), we determine values of $F_E = \{0.45, 0.47\}$ for the self-healed cases ($R = \{150, 200\}$ m), indicating the robustness to cloning-based attacks. A similar or slightly higher cloning fidelity is measured for the partially self-healed case ($R = \{500, 600\}$ m) with $F_E = \{0.53, 0.67\}$. A slight increase in F_E for $R = 600$ m can be explained by the lower level of self-healing. Matching these results, for the mutual information shared between Alice and Eve, we observe that I_{AE} exponentially decreases for a decreasing level of self-healing.

For self-healing modes, the error rate has the same value (24% for $R = 150$ m) as in the undisturbed case or is at about 26% ($R = 200$ m). As expected, Q increases for lower levels of self-healing. In contrast to the ideal situation, modal cross-talk from scattered light arising from higher diffraction orders lowers the key rate R_Δ below the Shannon limit. For full reconstruction of sent modes, the key rate shows an equivalent value for $R = 150$ m, as detected without obstacle (0.73); for $R = 200$ m, a value of 0.46 bits per photon is determined. If Alice's modes cannot fully self-heal before Bob detects them, the

key rate falls far below the Shannon limit, even becoming negative, i.e., no secret information can be shared. Thus, although the experimental key rate is relatively low for the detection of fully self-healed as well as partially self-healed modes, the beneficial effect of self-healing within the Bessel-based HD cryptography is visible.

5. SOME CHALLENGES ASSOCIATED WITH HD QKD

We have presented a tutorial on HD QKD where spatial modes of photons are used as basis states to encode information. Employing multi-dimensional (more than two) states for QKD increases the information capacity of every photon and, potentially, leads to higher secure information transfer rate in a more robust manner when compared to 2D QKD. This tutorial serves as a starting point for graduate students or interested researchers from other disciplines who wish to immerse themselves in this field. It is however important to note that there are technological and scientific challenges that continue to drive research in the field and that must be addressed before we see widespread deployment of HD QKD systems that use spatial modes. We find it useful to provide the reader with an overview of these challenges. While many of these would apply to any communication system (transmission losses or inefficiency of the optics and the detectors for example), we focus on those that are particular to HD QKD with spatial modes.

The first challenge is the speed at which spatial modes are imprinted onto a photon. In our demonstration, we used liquid crystal SLMs to encode the different spatial modes; that is because the SLM is a versatile, re-programmable tool that can spatially modulate light (photons) in a dynamic manner using digital holograms. However, most SLMs available on the market have modulation speeds on the order of tens of hertz (Hz), with select ones approaching the kilohertz (kHz) range through custom solutions (see Meadowlark, model HSP1920, for example). Alternatively, one could use a DMD that is cheaper and faster, though the loss penalty tends to be higher compared to SLMs. For example, Mirhosseini *et al.* have used a DMD to encode spatial information at 4 kHz to realize a seven-dimensional QKD transmission in a laboratory environment. While they achieved a final transmission rate of 6.8 secret bits per second, it should be noted that the efficiency of the system was only around 0.2%, highlighting the need technological improvement to sustain the question for practical HD QKD. Rather than achieving mode switching by refreshing pixels on a modulating device, one could employ a combination of high-speed optical switches and static modulating elements. In this scenario, an array of static elements that encode specific spatial modes are sequentially fed with pulses of light. The choice of modes sent is determined by an optical switch that is essentially an interferometer with a phase modulator inside. By varying the phase difference in the interferometer, one determines which output sees constructive or destructive interference, thus controlling the path of the photons [42]. This approach allows for faster modulation speeds given that these optical switches can operate at hundreds of megahertz (MHz). Alternatively, each static mode modulator can be coupled to a single photon emitter and controlled by a digital switch. In this way, the generation rate is no longer limited by the element that imprints the spatial profile on the photons, but by the modulation rate of the optical/electronic switch.

The second challenge is the efficiency of the measurement strategy. In the current approach, we used a SLM to measure the different basis states in which we encode information. To do so, we display a hologram on the SLM and observe the product of the input field and the SLM phase function in the far-field. By measuring the on-axis intensity in the far-field, we effectively evaluate the inner product between the incident field and the phase function encoded on the SLM; this is referred to as a projection measurement. Classically, one can evaluate multiple inner products at the same time by displaying multiple outputs at different spatial positions on a CCD camera, as shown in Fig. 7(d). This is possible given that we have many photons; the intensity is distributed over multiple modes. However, at the single photon level, this is not possible, since we cannot split a photon. The same measurement at the single photon level would require the acquisition of statistics from multiple measurements on identically prepared photons; to probe a photon encoded in one of d spatial modes, one would need at least $d-1$ projection measurements. In the context of QKD, this means two things: either Alice sends multiple copies of the same state for every bit of the message to allow Bob to have sufficient statistics, or Alice sends a single copy, and Bob has a probability $1/d$ of measuring the right state. Even when his measurement basis matches that of Alice, this means a loss of fraction of $(d-1)/d$ that grows with the dimension. The first scenario compromises the security of the QKD transmission, while the second carries a significant loss penalty. There is therefore a need for measurement techniques that do not rely on projection measurements. One such solution involves mapping spatial modes to spatial positions (or spatial frequencies) using refractive mode sorters [37,75,82,85,86], complex phase masks [87,88], or combinations of linear optical elements [89,90]. These approaches are particularly interesting, as they only require, in principle, a single shot measurement to identify the spatial mode with unit efficiency.

6. CONCLUSION

QKD is the most technologically advanced form of quantum communication, with real-world demonstrations already showing promise for more secure information transfer [91–96]. As we inch closer to a widespread deployment of the technology, it is important to note that the field of QKD is still a vibrant and exciting one. One of the areas of research that has exploded in recent years has been increasing the information capacity of photons to realize HD QKD. In this introductory tutorial to QKD with spatial modes of light, we have conveyed the attractiveness in employing HD states as a resource. While there is more than one way to realize HD QKD, we have focused on spatial modes of light. Exploiting the spatial degree of freedom of photons for HD encoding leads to an increase in information capacity per photon and a more robust QKD protocol. While the implementation of QKD requires specialized single photon sources and detectors, we aimed to provide through this tutorial a framework to classically emulate, with tools ubiquitous to many industry and university optics laboratories, the different

steps involved in realizing HD QKD. Even though we chose to focus on spatial modes of the BG type for their interesting non-diffractive and self-healing property, we reiterate that it was simply by means of example.

Funding. Deutsche Forschungsgemeinschaft (DE 486/23-1); Horizon 2020 Framework Programme (ColOpt ITN 721465); Department of Science and Technology, Republic of South Africa.

Disclosures. The authors declare no conflicts of interest.

REFERENCES

1. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).
2. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
3. P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
4. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
5. C. H. Bennett and G. Brassard, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working," SIGACT News **20**(4), 78–80 (1989).
6. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptol. **5**, 3–28 (1992).
7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
8. M. Dušek, N. Lütkenhaus, and M. Hendrych, "Quantum cryptography," Prog. Opt. **49**, 381–454 (2006).
9. 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**, 1301–1350 (2009).
10. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
11. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," New J. Phys. **11**, 075003 (2009).
12. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
13. C. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84**, 3762–3764 (2004).
14. 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, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
15. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**, 190501 (2016).
16. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).
17. T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, and S. W. Nam, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New J. Phys. **17**, 022002 (2015).
18. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Sci. Adv. **3**, e1701491 (2017).
19. G. B. Xavier and G. Lima, "Quantum information processing with space-division multiplexing optical fibres," Commun. Phys. **3**, 9 (2020).
20. S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," Phys. Rev. Lett. **96**, 090501 (2006).
21. S. Etcheverry, G. Cañas, E. Gómez, W. Nogueira, C. Saavedra, G. Xavier, and G. Lima, "Quantum key distribution session with 16-dimensional photonic states," Sci. Rep. **3**, 2316 (2013).
22. G. Molina-Terriza, J. P. Torres, and L. Torner, "Twisted photons," Nat. Phys. **3**, 305–310 (2007).
23. M. Krenn, M. Malik, M. Erhard, and A. Zeilinger, "Orbital angular momentum of photons and the entanglement of Laguerre–Gaussian modes," Philos. Trans. R. Soc. London, Ser. A **375**, 20150442 (2017).
24. M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted photons: new quantum perspectives in high dimensions," Light Sci. Appl. **7**, 17146 (2018).
25. M. J. Padgett, "Orbital angular momentum 25 years on," Opt. Express **25**, 11265–11274 (2017).
26. B. Ndagano, I. Nape, M. A. Cox, C. Rosales-Guzman, and A. Forbes, "Creation and detection of vector vortex modes for classical and quantum communication," J. Lightwave Technol. **36**, 292–301 (2018).
27. C. Rosales-Guzmán, B. Ndagano, and A. Forbes, "A review of complex vector light fields and their applications," J. Opt. **20**, 123001 (2018).
28. A. Forbes and I. Nape, "Quantum mechanics with patterns of light: progress in high dimensional and multidimensional entanglement with structured light," AVS Quantum Sci. **1**, 011701 (2019).
29. H. Rubinsztein-Dunlop, A. Forbes, M. V. Berry, M. R. Dennis, D. L. Andrews, M. Mansuripur, C. Denz, C. Alpmann, P. Banzer, T. Bauer, E. Karimi, L. Marrucci, M. Padgett, M. Ritsch-Marte, N. M. Litchinitser, N. P. Bigelow, C. Rosales-Guzmán, A. Belmonte, J. P. Torres, T. W. Neely, M. Baker, R. Gordon, A. B. Stilgoe, J. Romero, A. G. White, R. Fickler, A. E. Willner, G. Xie, B. McMorran, and A. M. Weiner, "Roadmap on structured light," J. Opt. **19**, 013001 (2017).
30. H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Phys. Rev. A **61**, 062308 (2000).
31. 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).
32. I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," Phys. Rev. Lett. **98**, 060503 (2007).
33. S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, "Overcoming noise in entanglement distribution," Phys. Rev. X **9**, 041042 (2019).
34. B. Ndagano and A. Forbes, "Characterization and mitigation of information loss in a six-state quantum-key-distribution protocol with spatial modes of light through turbulence," Phys. Rev. A **98**, 062330 (2018).
35. F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," Quantum **2**, 111 (2018).
36. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," Phys. Rev. A **88**, 032305 (2013).
37. 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).
38. F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, and E. Karimi, "Underwater quantum communication over a 30-meter flume tank," arXiv: 2004.04821 (2020).
39. F.-X. Wang, W. Chen, Z.-Q. Yin, S. Wang, G.-C. Guo, and Z.-F. Han, "Characterizing high-quality high-dimensional quantum key distribution by state mapping between different degrees of freedom," Phys. Rev. Appl. **11**, 024070 (2019).
40. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," Optica **4**, 1006–1010 (2017).
41. I. Nape, E. Otte, A. Vallés, C. Rosales-Guzmán, F. Cardano, C. Denz, and A. Forbes, "Self-healing high-dimensional quantum key distribution using hybrid spin-orbit Bessel states," Opt. Express **26**, 26946–26960 (2018).
42. D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenløwe, "Orbital angular momentum states enabling fiber-based high-dimensional quantum communication," Phys. Rev. Appl. **11**, 064058 (2019).
43. F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," Opt. Express **26**, 22563–22573 (2018).
44. Y. Chen, W.-G. Shen, Z.-M. Li, C.-Q. Hu, Z.-Q. Yan, Z.-Q. Jiao, J. Gao, M.-M. Cao, K. Sun, and X.-M. Jin, "Underwater transmission of high-dimensional twisted photons over 55 meters," PhotoniX **1**, 5 (2020).
45. M. McLaren, T. Mhlanga, M. J. Padgett, F. S. Roux, and A. Forbes, "Self-healing of quantum entanglement after an obstruction," Nat. Commun. **5**, 3248 (2014).
46. G. Sorelli, V. N. Shatokhin, F. S. Roux, and A. Buchleitner, "Diffraction-induced entanglement loss of orbital-angular-momentum states," Phys. Rev. A **97**, 013849 (2018).
47. E. Otte, I. Nape, C. Rosales-Guzmán, A. Vallés, C. Denz, and A. Forbes, "Recovery of nonseparability in self-healing vector Bessel beams," Phys. Rev. A **98**, 053818 (2018).
48. E. J. Galvez and M. Beck, "Quantum optics experiments with single photons for undergraduate laboratories," Edu. Training Opt. **2007**, 966513 (2007).
49. E. J. Galvez, "Resource letter spe-1: single-photon experiments in the undergraduate laboratory," Am. J. Phys. **82**, 1018–1028 (2014).
50. J. Brody and C. Selton, "Quantum entanglement with Freedman's inequality," Am. J. Phys. **86**, 412–416 (2018).
51. E. J. Galvez, "Qubit quantum mechanics with correlated-photon experiments," Am. J. Phys. **78**, 510–519 (2010).
52. R. Scholz, G. Friege, and K.-A. Weber, "Undergraduate quantum optics: experimental steps to quantum physics," Eur. J. Phys. **39**, 055301 (2018).
53. E. Dederick and M. Beck, "Exploring entanglement with the help of quantum state measurement," Am. J. Phys. **82**, 962–971 (2014).
54. M. N. Beck and M. Beck, "Witnessing entanglement in an undergraduate laboratory," Am. J. Phys. **84**, 87–94 (2016).
55. B. J. Pearson and D. P. Jackson, "A hands-on introduction to single photons and quantum mechanics for undergraduates," Am. J. Phys. **78**, 471–484 (2010).
56. E. Toninelli, B. Ndagano, A. Vallés, B. Sephton, I. Nape, A. Ambrosio, F. Capasso, M. J. Padgett, and A. Forbes, "Concepts in quantum state tomography and classical implementation with intense light: a tutorial," Adv. Opt. Photon. **11**, 67–134 (2019).
57. A. Forbes, A. Aiello, and B. Ndagano, "Classically entangled light," Prog. Opt. **64**, 99–153 (2019).
58. T. Konrad and A. Forbes, "Quantum mechanics and classical light," Contemp. Phys. **60**, 1–22 (2019).
59. D. Klyshko, "A simple method of preparing pure states of an optical field, of implementing the Einstein–Podolsky–Rosen experiment, and of demonstrating the complementarity principle," Sov. Phys. Usp. **31**, 74–85 (1988).
60. F. Gori, G. Guattari, and C. Padovani, "Bessel-Gauss beams," Opt. Commun. **64**, 491–495 (1987).
61. H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J. Cryptol. **18**, 133–165 (2005).
62. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
63. 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).
64. A. Ferenczi and N. Lütkenhaus, "Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning," Phys. Rev. A **85**, 052310 (2012).
65. M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," Nat. Commun. **5**, 5235 (2014).
66. L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," Phys. Rev. A **82**, 030301 (2010).
67. G. Gibson, J. Courtial, M. Padgett, M. Vasnetsov, V. Pas'ko, S. Barnett, and S. Franke-Arnold, "Free-space information transfer using light beams carrying orbital angular momentum," Opt. Express **12**, 5448–5456 (2004).
68. J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," Nat. Photonics **6**, 488–496 (2012).
69. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. **8**, 75 (2006).
70. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," Phys. Rev. A **88**, 032305 (2013).
71. 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).
72. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," New J. Phys. **17**, 033033 (2015).
73. A. Forbes, A. Dudley, and M. McLaren, "Creation and detection of optical modes with spatial light modulators," Adv. Opt. Photon. **8**, 200–227 (2016).
74. G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, "Efficient sorting of orbital angular momentum states of light," Phys. Rev. Lett. **105**, 153601 (2010).
75. M. P. J. Lavery, D. J. Robertson, A. Sponselli, J. Courtial, N. K. Steinhoff, G. A. Tyler, A. E. Wilner, and M. J. Padgett, "Efficient measurement of an optical orbital-angular-momentum spectrum comprising more than 50 states," New J. Phys. **15**, 013024 (2013).
76. G. F. Walsh, "Pancharatnam–Berry optical element sorter of full angular momentum eigenstate," Opt. Express **24**, 6689–6704 (2016).
77. G. Ruffato, M. Girardi, M. Massari, E. Mafakheri, B. Sephton, P. Capaldo, A. Forbes, and F. Romanato, "A compact diffractive sorter for high-resolution demultiplexing of orbital angular momentum beams," Sci. Rep. **8**, 10248 (2018).
78. T. Durt, B. G. Englert, I. Bengtsson, and K. Yczkowski, "On mutually unbiased bases," Int. J. Quantum Inform. **8**, 535–640 (2010).
79. Y. Zhang, M. Mclaren, F. S. Roux, and A. Forbes, "Simulating quantum state engineering in spontaneous parametric down-conversion using classical light," Opt. Express **22**, 17039–17049 (2014).
80. J. Turunen, A. Vasara, and A. T. Friberg, "Holographic generation of diffraction-free beams," Appl. Opt. **27**, 3959–3962 (1988).
81. D. M. Cottrell, J. M. Craven, and J. A. Davis, "Nondiffracting random intensity patterns," Opt. Lett. **32**, 298–300 (2007).
82. 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).
83. D. McGloin and K. Dholakia, "Bessel beams: diffraction in a new light," Contemp. Phys. **46**, 15–28 (2005).
84. Z. Bouchal, J. Wagner, and M. Chlup, "Self-reconstruction of a distorted nondiffracting beam," Opt. Commun. **151**, 207–211 (1998).

85. G. C. Berkhout, M. P. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, "Efficient sorting of orbital angular momentum states of light," Phys. Rev. Lett. **105**, 153601 (2010).
86. M. Malik, M. Mirhosseini, M. P. Lavery, J. Leach, M. J. Padgett, and R. W. Boyd, "Direct measurement of a 27-dimensional orbital-angular-momentum state vector," Nat. Commun. **5**, 3115 (2014).
87. R. Fickler, F. Bouchard, E. Giese, V. Grillo, G. Leuchs, and E. Karimi, "Full-field mode sorter using two optimized phase transformations for high-dimensional quantum cryptography," J. Opt. **22**, 024001 (2020).
88. N. K. Fontaine, R. Ryf, H. Chen, D. T. Neilson, K. Kim, and J. Carpenter, "Laguerre–Gaussian mode sorter," Nat. Commun. **10**, 1865 (2019).
89. Y. Zhou, M. Mirhosseini, D. Fu, J. Zhao, S. M. H. Rafsanjani, A. E. Willner, and R. W. Boyd, "Sorting photons by radial quantum number," Phys. Rev. Lett. **119**, 263602 (2017).
90. B. Ndagano, I. Nape, B. Perez-Garcia, S. Scholes, R. I. Hernandez-Aranda, T. Konrad, M. P. Lavery, and A. Forbes, "A deterministic detector for vector vortex states," Sci. Rep. **7**, 13882 (2017).
91. A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," J. Opt. Soc. Am. B **27**, A185 (2010).
92. D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New J. Phys. **13**, 123001 (2011).
93. 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, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**, 10387–10409 (2011).
94. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," Nat. Photonics **7**, 382–386 (2013).
95. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**, 21739–21756 (2014).
96. D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," Opt. Lett. **41**, 3511–3514 (2016).