


**Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons**

Michael de Oliveira, Isaac Nape, Jonathan Pinnell, Najmeh TabeBordbar , and Andrew Forbes\*  
*School of Physics, University of the Witwatersrand, Johannesburg 2000, South Africa*

 (Received 21 January 2020; accepted 9 March 2020; published 1 April 2020)

Secret sharing allows three or more parties to share secret information which can only be decrypted through collaboration. It complements quantum key distribution as a valuable resource for securely distributing information. Here we take advantage of hybrid spin and orbital angular momentum states to access a high-dimensional encoding space, demonstrating a protocol that is easily scalable in both dimension and participants. To illustrate the versatility of our approach, we first demonstrate the protocol in two dimensions, extending the number of participants to ten, and then demonstrate the protocol in three dimensions with three participants. We reconstruct secrets depicted as images with a fidelity of up to 0.979. Moreover, our scheme exploits the use of conventional linear optics to emulate the quantum gates needed for transitions between basis modes on a high-dimensional Hilbert space, allowing us to exceed the 1 bit per photon limit of two-dimensional protocols. Our work offers a practical approach for sharing information across multiple parties, a crucial element of any quantum network.

DOI: [10.1103/PhysRevA.101.042303](https://doi.org/10.1103/PhysRevA.101.042303)

**I. INTRODUCTION**

In a world where cloud computing environments dominate our personal and corporate lives, secure communication and key distribution between multiple parties is a growing concern. This includes the secure sharing of encryption keys, missile launch codes, bank account information, and social media profiles. In popular cryptography methods either a single copy of the encryption key is kept in one location for maximum secrecy or multiple copies of the same key are kept in different locations for greater reliability, but at an increased security risk. Secret sharing is a multiparty communication technique where a secret is divided and shared among  $N$  parties and then securely reconstructed through collaboration, making it ideal for storing and sharing information that is highly sensitive, achieving both high levels of privacy and reliability [1,2].

The first quantum secret sharing (QSS) scheme proposed the use of particle entangled states [3]. In this protocol, three parties (Alice, Bob, and Charlie) randomly choose between two measurement bases and independently measure their particle. If their measurement results are correlated, Bob and Charlie can use their measurement bases and outcome information to determine the result of Alice's measurement; otherwise, the round is discarded. Since approximately half the instances will be discarded the intrinsic efficiency is about 50%. This protocol was improved to accommodate an arbitrary number of parties based on multiparticle qubit entanglement states [4], and later to multiparticle  $d$  dimensional entanglement states [5].

Although much theoretical, in both the discrete-variable [6–14] and continuous-variable regime [15,16], and (to a lesser extent) experimental [17–19] attention has focused

on QSS using multiparticle entangled states, progress has been limited by the intrinsic hurdle that the number of parties involved is bound by the number of entangled particles: this makes particle entanglement-based QSS inefficient and unscalable (multiphoton entanglement is notoriously inefficient).

As a result of these limitations, two-dimensional QSS schemes using single photon states have been proposed [20,21] and implemented [22,23] for a scalable number of parties. The advantage arises in its circular structure, where each party performs sequential unitary operations on the same single photon, instead of several entangled photons which require convoluted setups. The security was found to be less robust as compared to quantum key distribution (QKD) and susceptible to cheating strategies in that dishonest parties could infer some information about the choice of bases of another party [24,25]. To address this deficiency, multiparty high-dimensional single photon QSS protocols were theoretically proposed [26–29] but with few suggestions as to how they might be (practically) implemented in the laboratory [30–32]. Challenges in high-dimensional state preparation, transformation, and detection, the key steps of any QSS protocol, have so far presented barriers to experimental realization [33].

Here we realize an experimental high-dimensional single photon QSS protocol using photons that are vectorially structured in their orbital angular momentum (OAM) and polarization. Our approach requires only simple linear optical elements: spin-orbit coupling optics to prepare the initial state, waveplates with dove prisms to encode the secret in the sequential phase transformation of each party, and a deterministic detector for all basis elements in the high-dimensional vector space. We successfully implement this protocol in two-dimensions for ten parties and three dimensions with three parties. Our approach is scalable in the number of participants, highly efficient, and provably secure.

\*andrew.forbes@wits.ac.za

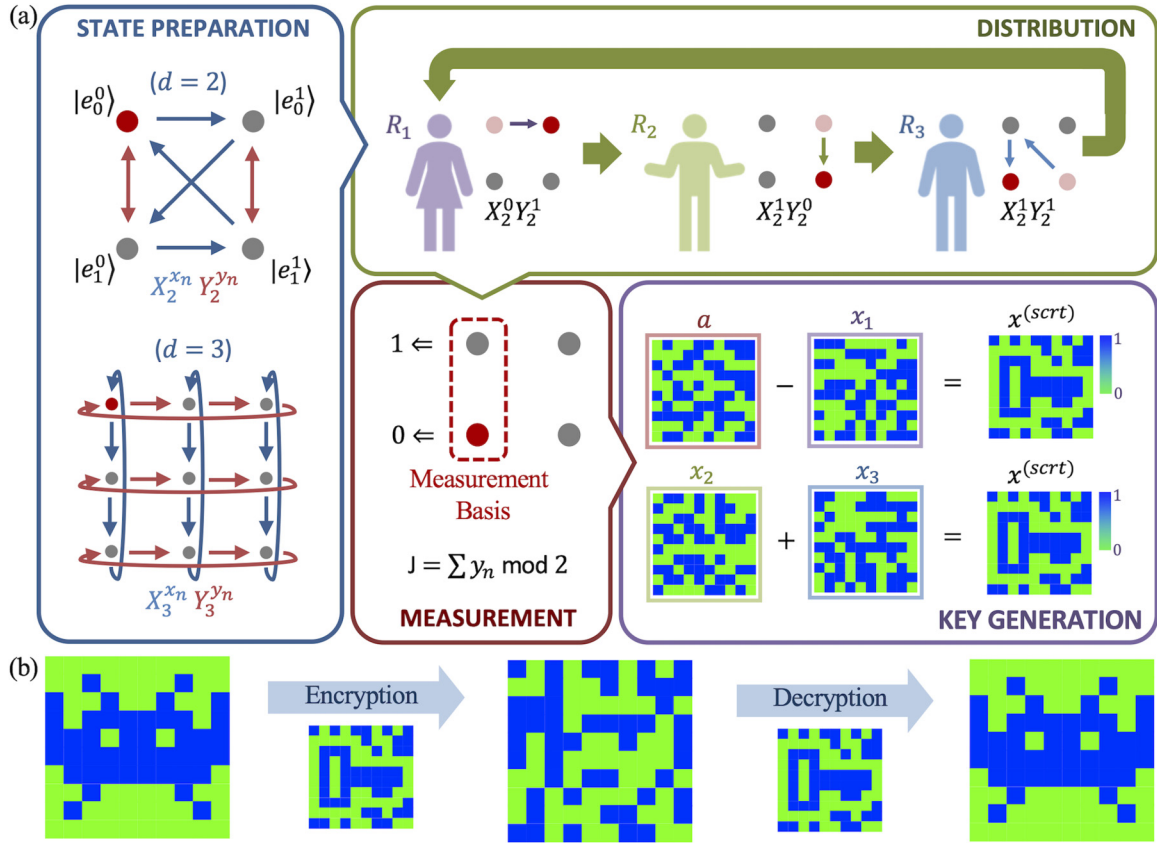


FIG. 1. General scheme for a four party single qubit QSS scheme. (a) The distributor,  $R_1$ , prepares an initial state from a set of  $d = 2$  MUBs. The qubit is then sequentially distributed to each party, who in turn performs a unitary phase operation given by  $X_d^{x_n} Y_d^{y_n}$ . The choice of  $X^{x_n}$  is analogous to a change in local states within the basis and a choice of  $Y^{y_n}$  corresponds to a change of basis. The last participant sends the qubit back to the distributor. The distributor requests that parties  $R_2, R_3, R_4$  broadcast their choice of  $y_n$  and performs a measurement in a basis that leads to a deterministic result. The distributor can generate a secret key  $x^{(\text{s crt})}$  by using the measurement result to reset their choice of  $x_n$ . The other parties, upon collaborating and broadcasting their choice of  $x_n$ , can also generate the same secret key  $x^{(\text{s crt})}$ . We also show the state preparation for  $d = 3$  dimensions. Note that the operators are cyclic in three dimensions because of the cyclic property of MUBs in odd prime dimensions. (b) The distributor can securely encrypt a message by applying a simple XOR encryption operation using their generated secret key. The encrypted message, after being distributed, can be decrypted by each participant using their own secret key. At no point is the secret key shared among any participants.

## II. SINGLE PHOTON QUANTUM SECRET SHARING PROTOCOL

We begin by extending the single photon QSS protocol [26] to prime dimensions and then we outline the general structure of an  $N$ -party QSS scheme using a single photon state. In this protocol multiple participants perform local operations on a single photon encoded in prime  $d$  dimensions. Suppose a participant  $R_1$ , also known as the distributor, wants to share a secret key amongst multiple parties,  $R_2, \dots, R_N$ ; then the QSS protocol can be summarized in four steps (see Fig. 1).

(1) *State preparation.* The distributor,  $R_1$ , prepares an initial single photon state  $|e_0^{(0)}\rangle$  from a set of mutual unbiased bases (MUB) in the desired prime dimension  $d$ . In our protocol, the MUBs are formulated from the logical basis,  $|\ell\rangle$ , as

$$|e_k^{(j)}\rangle = \frac{1}{\sqrt{2}} \sum_{\ell=0}^1 \omega^{\frac{1}{2}\ell(j+2k)} |\ell\rangle \quad (1)$$

in two dimensions and in odd prime dimensions ( $d'$ ) they are generalized as [26]

$$|e_k^{(j)}\rangle = \frac{1}{\sqrt{d'}} \sum_{\ell=0}^{d'-1} \omega^{\ell(k+j\ell)} |\ell\rangle, \quad (2)$$

where  $k$  maps onto a mode from the  $j$ th MUB and  $\omega = \exp(\frac{i2\pi}{d})$ . Note that  $\ell, j, k \in \{0, \dots, d-1\}$ .

(2) *Distribution.* The distributor modulates the photon initially in the state  $|e_0^{(0)}\rangle$  with the operators  $X_d^{x_1} Y_d^{y_1}$ , where  $x_1, y_1 \in \{0, \dots, d-1\}$  are chosen randomly and indicate how many times the operators should be applied. The photon is then sent sequentially to each participant  $R_2, \dots, R_N$ , who, upon receiving the single photon, randomly chooses  $x_n, y_n \in \{0, \dots, d-1\}$ , such that they apply the corresponding unitary operations  $X_d^{x_n} Y_d^{y_n}$ .

To map between the MUB basis states, each party has access to two operators:  $X_d$  and  $Y_d$ . The operator  $X_d$  is defined

as

$$X_d = \sum_{\ell=0}^{d-1} \omega^\ell |\ell\rangle \langle \ell| \quad (3)$$

for prime dimensions. We adapted the protocol [26] for two dimensions such that the operator  $Y_d$  is defined as

$$Y_2 = \sum_{\ell=0}^1 \omega^{\frac{1}{2}\ell} |\ell\rangle \langle \ell| \quad (4)$$

in two dimensions and in odd prime dimensions ( $d'$ ) as

$$Y_{d'} = \sum_{\ell=0}^{d'-1} \omega^{\ell^2} |\ell\rangle \langle \ell|. \quad (5)$$

The operator  $X_d^{x_n}$  cycles through  $x_n$  modes in the same basis, while the operator  $Y_d^{y_n}$  cycles through  $y_n$  MUBs, as shown in Fig. 1(a). Using both operators in sequence results in the mapping between all MUB states, which is crucial in the implementation of the single photon secret sharing protocol.

(3) *Measurement.* After receiving the single photon from the last participant, the distributor requests that parties  $R_2, \dots, R_N$  broadcast their choice of  $y_n$  in a random order, keeping their value of  $x_n$  a secret. By considering the sum of all  $y_n$ , the distributor chooses a measurement basis from the MUB set in such a way that the measurement leads to a deterministic result. In prime dimensions this is equivalent to applying the local unitary operator  $Y_d^J$  and measuring the photon in the basis  $|e_k^{(J)}\rangle$ , where

$$J = \sum_{n=1}^N y_n \text{ mod } d. \quad (6)$$

The final measurement result obtained by the distributor is labeled  $a \in \{0, \dots, d-1\}$ . Since the measurement is performed in a basis that yields a correlated result, the efficiency of the protocol is 100% [29]. If Eq. (6) holds, the participants have a strongly correlated selection of  $x_n$ , satisfying

$$\sum_{n=1}^N x_n + C = a \text{ mod } d, \quad (7)$$

where we define  $C = \lfloor \frac{1}{2} \sum_{n=1}^{N+1} y_n \rfloor$  for two dimensions, which accounts for the additional  $X_2$  operator imparted by every odd number of  $Y_2$  operators, and  $C = 0$  in odd prime dimensions, due to the cyclic property of the operators in  $d'$  dimensions.

(4) *Key generation.* The distributor resets his value of  $x_1^{(\text{scrt})} = (a - x_1 + C) \text{ mod } d$  according to the measurement result  $a$ . Consequently, if participants  $R_2, \dots, R_N$  collaborate and reveal among themselves their choice of  $x_n$ , they can reconstruct the distributor's secret value  $x_1^{(\text{scrt})} = \sum_{n=2}^N x_n \text{ mod } d$ , which was previously only known to the distributor  $R_1$ . By repeating this procedure, the distributor can share a secret key among the remaining  $N-1$  participants. Using the secret key, the distributor can securely encrypt a message and distribute it to the participants, who in turn can use their own secret key to decrypt the message, as in Fig. 1(b).

Participant  $R_1$  checks the security, such that he randomly selects a subset of rounds. The degree of security specifications determines the size of the subset. In order to increase the

security, as justified in [29],  $R_1$  must make sure that the subset of valid rounds includes a round in which each participant broadcasts his choice of  $y_n$  last. Each participant reveals their inferred value  $x^{(\text{scrt})}$  for the subset of rounds, which is compared to the value determined by the distributor. If there is a discrepancy any dishonest eavesdropping or cheating strategy is exposed.

In the next step, we investigate the necessary tools to implement a high-dimensional single photon QSS scheme. We explore vector modes and how we can implement unitary phase operators using simple linear optics.

### III. EXPERIMENTAL REALIZATION

Here, we introduce the tools (operations) needed for single photon QSS in prime dimensions. Lastly, we show how the protocol can be implemented in both  $d=2$  and  $d=3$  dimensions using polarization and OAM control.

#### A. Two-dimensional realization

If we consider the polarization subspace coupled with the OAM subspace, spanned only by  $|\ell\rangle$ , we can construct a two-dimensional mode set, i.e.,  $\mathcal{H}_2 = \text{span}(|R\rangle|\ell\rangle, |L\rangle|-\ell\rangle)$  as illustrated in Fig. 2(a). The basis states can be mapped as orthogonal column vectors,

$$|R\rangle|\ell\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |L\rangle|-\ell\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (8)$$

This allows us to map the MUBs [see Fig. 2(b)] as row vectors in matrix form as follows:

$$M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad M_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}. \quad (9)$$

The first step in implementing the protocol is preparing the photon in the initial state within our MUB set. We generated the initial state,  $|e_0^{(0)}\rangle = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle)$  denoted by  $|\Psi_0\rangle$ , from a horizontally polarized photon incident on a spin-orbit coupling  $q$ -plate [34,35].

The next step is to find a way to independently move between each MUB state by applying the required operators. This is easily implemented by a half waveplate (HWP). It is straightforward to see that a HWP acting on the initial state  $|e_0^{(0)}\rangle$  induces a relative phase difference,  $e^{i4\theta}$ , between the circular polarization states. This can be summarized as

$$\hat{U}(\theta) \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i4\theta} \end{pmatrix}, \quad (10)$$

where  $\theta \in \{0, \pi/8, \pi/4, 3\pi/8\}$  is the rotation angle of the HWP, corresponding to the transformations  $\hat{U}(\theta) = \{X_2^0 Y_2^0, X_2^0 Y_2^1, X_2^1 Y_2^0, X_2^1 Y_2^1\}$ . In this way, Fig. 2(b) shows that we can move independently between all MUBs.

Once the initial state is sent through a set of even  $N$  consecutive HWPs, allowing each party to apply their unitary operator, the final state of the photon will be

$$|\Psi_N\rangle = \frac{e^{i\Omega}}{\sqrt{2}} [ |R\rangle|\ell\rangle + e^{i\Phi} |L\rangle|-\ell\rangle ], \quad (11)$$

where  $\Omega = (-i)^N e^{-2i[\sum_{n=1}^N (-1)^{n+1}\theta_n]}$  and  $\Phi = 4\sum_{n=1}^N (-1)^{n+1}\theta_n$ . The distributor then applies the

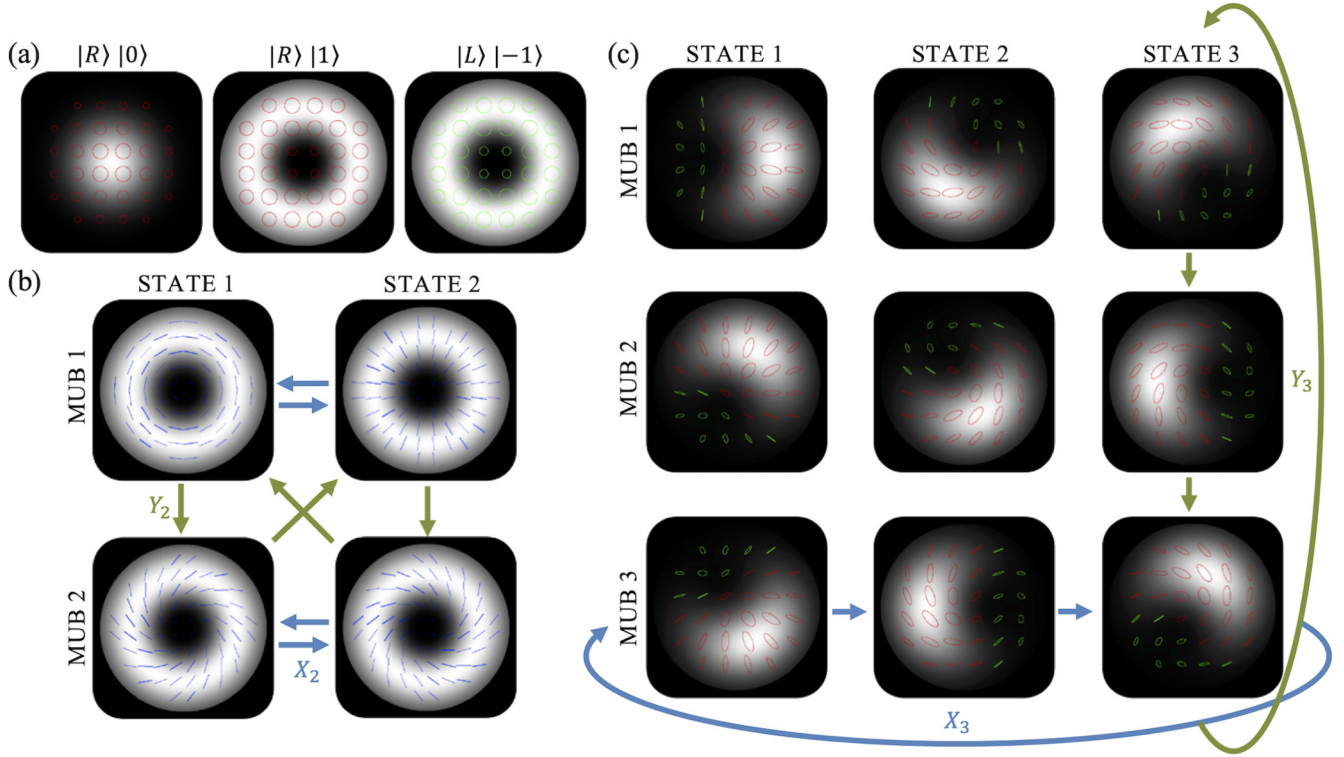


FIG. 2. Illustration of the spin-orbit coupled modes that form our computational basis, from which we construct our MUBs. (a) Right circularly polarized light is shown in red, left circularly polarized light is shown in green, and linear polarization in blue. (b) We realize the operators in  $d = 2$  using a half waveplate (HWP). A HWP at  $\theta = \pi/4$  realizes the  $X_2$  operator, cycling between the states within the same basis; at  $\theta = \pi/8$  we realize the  $Y_2$  operator, moving between MUBs. Note that the  $Y_2$  operator is not cyclic, due to the extra  $X_2$  operator that is imparted by every odd number of  $Y_2$ . (c) Here we show the cyclic nature of the operators in  $d = 3$ . A dove prism (DP) allows us to realize the  $X_3$  gate, cycling between the states within the same basis, and a half waveplate (HWP) allows us to realize the  $Y_3$  gate, cycling between the MUBs.

corresponding operator for  $\phi_j \in \{0, \pi/2\}$  using a HWP, such that performing the measurement in the basis  $\frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + e^{i\phi_j}|L\rangle|-\ell\rangle)$  leads to the deterministic result.

Next, we discuss the detection system used to distinguish between all MUB states. The different states can be deterministically detected using a combination of geometric phase control and multipath interference, as seen in Fig. 3(a). The photon was mapped onto two polarization dependent paths ( $a$  and  $b$ ) using a combination of quarter waveplates (QWP) and a polarizing beam splitter (PBS), such that the state of the qubit becomes

$$|\Psi_N\rangle = \frac{e^{i\Omega}}{\sqrt{2}}[|R\rangle_a|1\rangle_a + e^{i\Phi}|L\rangle_b|-\ell\rangle_b], \quad (12)$$

where the subscripts  $a$  and  $b$  refer to the polarization dependent paths. The photon paths were interfered at a 50:50 beam splitter (BS), setting the dynamic phase difference between the two paths to  $\pi/2$ . An extra reflection was added to one path so that the number of reflections, and thus the polarization of the two output paths, was automatically reconciled. Henceforth, we will drop the polarization kets in the expression as the polarization information is path dependent. The resulting state after the BS is

$$|\Psi'_N\rangle = \frac{e^{i\Omega}}{2}[(1 - e^{i\Phi})|1\rangle_c + i(1 + e^{i\Phi})|-\ell\rangle_d], \quad (13)$$

where the subscript  $c$  and  $d$  refer to the output paths of the beam splitter. From this equation we see that the detection scheme is in fact deterministic for given values of  $\Phi$ , such that all the light will be in either path  $c$  or  $d$ .

Next, we extend the two-dimensional implementation to three dimensions, using a similar linear optics setup.

### B. Three-dimensional realization

We now consider a mode set that spans a three-dimensional (qutrit) space of spin-orbit coupled modes, i.e.,  $\mathcal{H}_3 = \text{span}(\{|R\rangle|0\rangle, |R\rangle|\ell\rangle, |L\rangle|-\ell\rangle\})$  as depicted in Fig. 2(a). If we map the basis states as orthogonal column vectors, i.e.,

$$|R\rangle|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |R\rangle|\ell\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |L\rangle|-\ell\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad (14)$$

the MUBs can be mapped as row vectors in matrix form as

$$\begin{aligned} M_1 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, & M_2 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \omega \\ 1 & \omega & 1 \\ \omega & 1 & 1 \end{pmatrix}, \\ M_3 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 \\ \omega^2 & 1 & 1 \end{pmatrix}, \end{aligned} \quad (15)$$

where  $\omega = \exp(i\frac{2\pi}{3})$ .

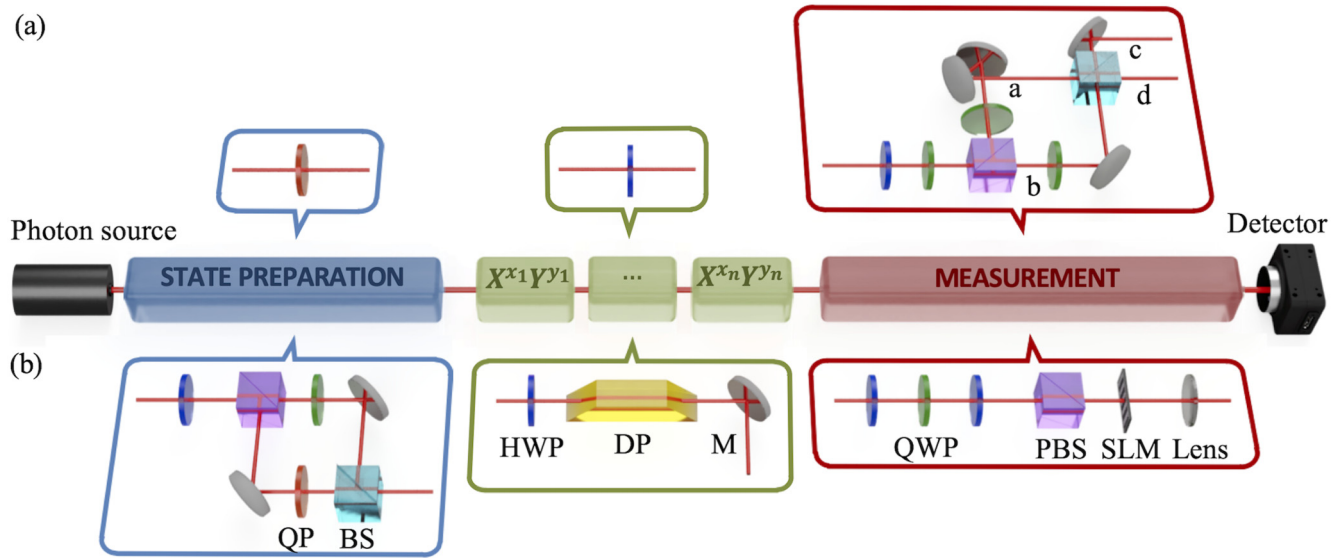


FIG. 3. Generalized experimental setup of a single photon quantum secret sharing scheme, showing the state preparation, distribution, and measurement steps for (a)  $d = 2$  and (b)  $d = 3$  dimensions. The initial states are generated using a combination of geometric phase optics [i.e., a  $q$ -plate (QP)]. The initial state is then sequentially communicated to each participant, who performs a unitary phase operator employed using simple linear optics such as a half waveplate (HWP) and a dove prism (DP). A HWP in the measurement step was used to perform the measurement in the same basis each time. The different states can be deterministically detected (a) using a combination of geometric phase control and multipath interference using beam splitters (BM) and polarizing beam splitter (PBS), or (b) via modal decomposition using a spatial light modulator (SLM). M are mirrors.

The initial state was prepared using an interferometric combination of a  $q$ -plate, HWP, and beam splitter, as in Fig. 3(b). We further engineer the required operators by using a half waveplate in combination with a dove prism (DP) as illustrated. As before, the HWP induces a relative phase difference,  $e^{4i\theta}$ , between the circular polarization DOF and the DP imparts a phase which is proportional to the OAM state. A mirror after the dove prism is needed to invert the final OAM state. The unitary transformation, in the basis from Eq. (14), can be summarized as

$$\hat{U}(\theta, \gamma) \propto \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{-2i\gamma\ell_2} & 0 \\ 0 & 0 & e^{2i\gamma\ell_3+4i\theta} \end{pmatrix}, \quad (16)$$

where  $\theta \in \{0, \pi/6, 2\pi/6\}$  is the rotation angle of the HWP and  $\gamma \in \{0, \pi/3, 2\pi/3\}$  is the rotation angle of the DP. The DP allows us to realize the  $X_3$  gate, cycling between the states within the same basis, and the HWP allows us to realize the  $Y_3$  gate, cycling between the MUBs [see Fig. 2(c)].

The detection system included mapping our vector basis to a scalar basis using a set of half waveplate and quarter waveplates. We measured the detection probabilities of each MUB state by performing optical inner-product measurements using match filters encoded on the SLM via modal decomposition, which is used extensively in both classical and quantum studies [36], as well as vector mode detection [37].

First, to perform the modal overlap between the normalized spatial modes  $\psi(\mathbf{r})$  and  $\phi(\mathbf{r})$ , we simply compute the inner product

$$c = \langle \phi | \psi \rangle = \iint \phi^*(\mathbf{r})\psi(\mathbf{r}) d^2r, \quad (17)$$

where  $r = (x, y)$  and  $|c|^2$  is the overlap probability determining the correlation between the two modes. Accordingly, any arbitrary input field,  $\psi(\mathbf{r})$ , can be correlated with a second mode  $\phi(\mathbf{r})$ , where  $|c|^2 = 1$  for a high correlation, meaning the modes are equivalent, and  $|c|^2 = 0$  for no correlation meaning that the modes are orthogonal. Optically,  $\phi(\mathbf{r})$  can be a match filter in the form of a hologram encoded on an SLM. Therefore, the detection modes were encoded as phase and amplitude holograms on a Holoeye Pluto spatial light modulator (SLM)—a well established technique for spatial mode detection [36]. As such the overlap probability  $|c|^2$  can be obtained by taking the Fourier transform of the product  $\phi^*(\mathbf{r})\psi(\mathbf{r})$ , which is the output mode after the match filter, and hence yielding the state

$$A(k_x, k_y) = \iint \phi^*(x, y)\psi(x, y) e^{-i(k_x x + k_y y)} dx dy, \quad (18)$$

where  $k_x, k_y$  are transverse wave vectors in Cartesian coordinates. Evaluating the on-axis point  $(k_x, k_y) = (0, 0)$  results in Eq. (17). Therefore,

$$A(0, 0) = \iint \phi^*(\mathbf{r})\psi(\mathbf{r}) d^2r = c \quad (19)$$

results in the intensity at the field center,  $I(0, 0) = |A(0, 0)|^2$ , being the modal overlap weighting (equivalently detection probability)  $|c|^2$ .

Alternatively, using a quantum Fourier transform (QFT) to map between the MUB superpositions of OAM modes to the OAM standard basis, one can deterministically sort the MUBs and thereafter sort the OAM modes. In three dimensions, a QFT for OAM has been proposed [38]. The technique exploits the tritter [39], by using path and phase control. Once the mapping between the MUB and OAM basis is achieved, mode

sorters can be used deterministically to measure the OAM modes [40]. Mode sorting has been extensively used for both scalar [41] and vector modes [42].

#### IV. RESULTS

Here we present the results for our implementation of the quantum secret sharing protocol with single photon states in  $d = 2$  and  $d = 3$  dimensions. For practical purposes, the experiment was first performed with a classical light source and a CCD camera. Later, the light source was attenuated to an average photon number of  $\mu = 0.02$  per pulse. Although weak coherent states cannot be used without photon splitting strategies this could, in principle, be overcome by preparing and testing the transmission properties of some decoy states. In the single photon regime, the measurement system includes coupling the photons through fibers to avalanche photon detectors (APD).

##### A. Two-dimensional results

The two-dimensional detection results of our vector basis are shown in Fig. 4. This was performed by rotating the angle  $\theta$  of the HWP and measuring the intensity of each output port using a CCD camera at each port [see Fig. 4(a)] and in the single photon regime, using single photon detectors [see Fig. 4(b)].

There is an excellent agreement between the experimental results (data points) and the theory (dashed curves). The visibility,  $V$ , of the detection scheme in each output port was calculated using the equation

$$V = \frac{|\mathcal{I}_{\max} - \mathcal{I}_{\min}|}{\mathcal{I}_{\max} + \mathcal{I}_{\min}}, \quad (20)$$

where  $\mathcal{I}$  is the intensity in each arm. Spatial filtering was applied to the data obtained using the CCD camera to remove unwanted noise, resulting in  $V = 0.958 \pm 0.005$ . In our system, the errors are introduced by the additive imperfections in the half waveplates causing slight misalignment in the setup. The visibility for the single photon regime was measured to be  $V = 0.924 \pm 0.003$ , which can be accounted for by the photon loss in fiber coupling and detector dark counts. Nonetheless, such values imply the use of a well-aligned and stable interferometer.

For phase-coding setups, the fidelity of the detection system is related to the interference visibility by [43]

$$F = \frac{1 + V}{2}. \quad (21)$$

Hence the fidelity of the system was calculated to be  $F = 0.979 \pm 0.005$  for the classical implementation and  $F = 0.962 \pm 0.003$  for the single photon regime. Using this deterministic detector, we can detect any arbitrary superposition of our vector basis with high fidelity.

##### B. Three-dimensional results

To demonstrate the feasibility of our secret sharing scheme in three dimensions, we verify that the  $d + 1$  MUBs are each orthogonal with respect to each other by measuring the scattering probabilities. The crosstalk matrix is shown

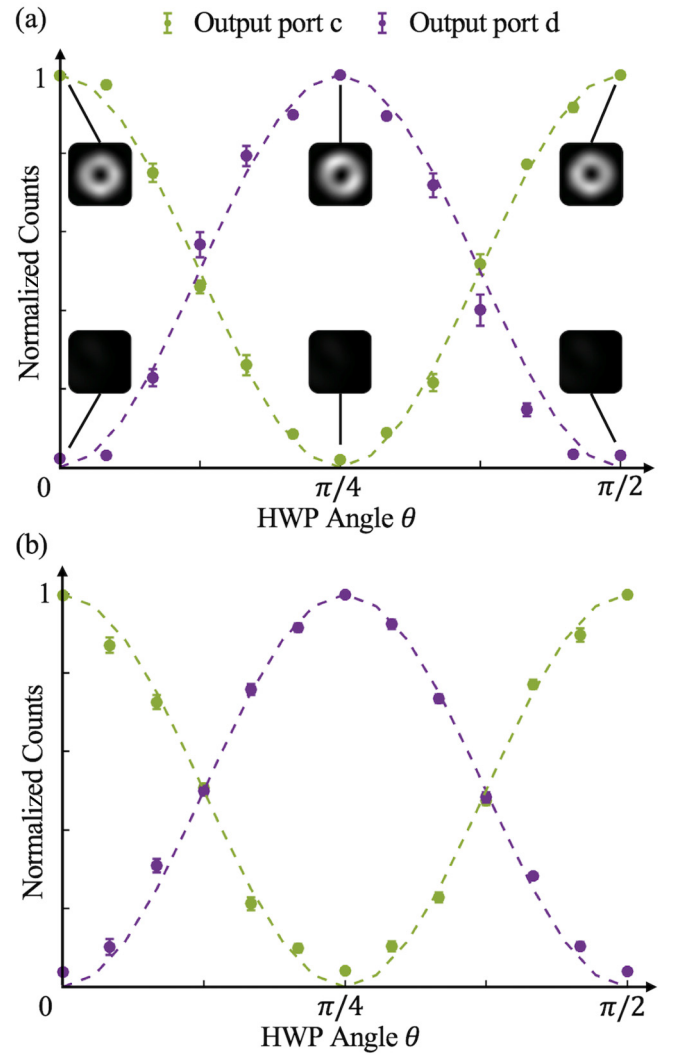


FIG. 4. Detection of superposition of vector states. Each graph shows the detection (normalized counts) of the photons in a superposition of the vector states  $|\Psi_N\rangle$ , generated by rotating the HWP angle  $\theta$ , using (a) CCD camera and (b) photo diodes in the single photon regime. Each data point was generated by averaging over 35 measurements. The dashed lines show the theoretical curve.

theoretically in Fig. 5(a) and experimentally in Fig. 5(b) and Fig. 5(c), for the classical and single photon regime, respectively. To obtain the results we first prepared the initial superposition state  $|e_0^{(0)}\rangle$  and applied the  $X_3$  and  $Y_3$  gates to iterate through the various basis modes and MUB mode sets. Using a set of waveplates, we mapped the circular polarization photon states to the horizontal polarization state and performed projective measurements via modal decomposition.

From the crosstalk matrices, we measured an average fidelity of  $F = 0.946 \pm 0.003$  when using classical light and similarly we measured  $F = 0.938 \pm 0.001$  in the single photon regime. In our system, the errors are introduced by imperfections, including the rotation of the dove prism and half waveplates causing slight misalignment in the setup.

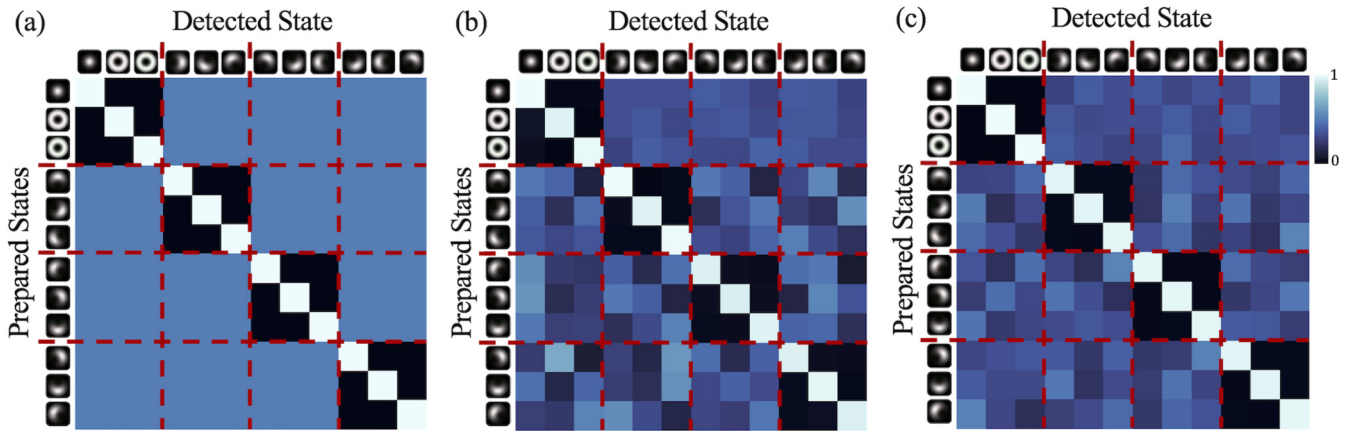


FIG. 5. Crosstalk matrices shown theoretically in (a) and experimentally in (b) and (c), for classical light and the single photon regime, respectively. This shows the scattering probabilities for modes prepared and detected in identical bases (diagonal) and the overlap between modes from mutually unbiased bases (off diagonal).

### C. Security analysis

From the measured detection fidelities, we performed a security analysis on our QSS scheme for  $d = 2$  and  $d = 3$  dimensions. The results of the analysis are summarized in Table I.

The quantum bit error rate (QBER), reflecting the probability of making detection errors, is related to the fidelity by

$$\text{QBER} = 1 - F, \quad (22)$$

which is zero for a perfect system. The detection fidelities translated into an optical QBER between 0.021 and 0.062, well below the 0.110 and 0.156 bounds for unconditional security against coherent attacks in two and three dimensions, respectively [44]. Systematic errors can be attributed to detector dark counts and the interferometric phase drift, which influences the prepared relative phases. This forced a phase recalibration before each run.

From the fidelity we can calculate the mutual information,  $I$ . This places a bound on the amount of information that can be shared between the distributor and participants. This bound is only due to the generation and detection fidelities, and is not intrinsic to the protocol itself. This is given by

$$I = \log_2(d) + F \log_2(F) + (1 - F) \log_2\left(\frac{1 - F}{d - 1}\right). \quad (23)$$

TABLE I. Summary of the  $d = 2$  and  $d = 3$  experimental results for our secret sharing protocol, for both the classical regime using the CCD camera as a detector and for the single photon regime using APDs. We show the experimental values of the detection fidelity ( $F$ ), the quantum bit error rate (QBER) in bits per photon, and mutual information ( $I$ ) between distributor and participants.

Measures	$d = 2$		$d = 3$	
	Classical	Quantum	Classical	Quantum
$F$	0.979	0.962	0.946	0.938
QBER	0.021	0.038	0.054	0.062
$I$	0.853	0.767	1.225	1.187

For a perfect system we would expect a value of 1 bit per photon in a  $d = 2$  qubit system and 1.58 bits per photon in a  $d = 3$  qutrit system. For  $d = 3$  this was measured to be nearly  $1.5 \times$  the maximum achievable in  $d = 2$  dimensions. We note that increasing the dimension of the quantum secret sharing protocol did result in higher mutual information capacity.

### D. Secret key generation

To corroborate the advantage of our protocol utilizing a higher-dimensional encoding space, we experimentally shared a secret in both  $d = 2$  and  $d = 3$  dimensions using the experimental setups described.

In two dimensions, the protocol was performed by  $N = 10$  participants, each equipped with a  $X_2$  and  $Y_2$  gate (half waveplate). We ran the protocol for 100 valid runs, resulting in a generated secret key of 100 bits. The results are shown in Fig. 6(a), for the identical secret key retrieved by the distributor and shared between the participants. The distributor's secret key was determined by resetting his choice of  $x_1$  using the measurement results and the participants choice of  $y_n$ . The participants shared secret key was calculated by summing the keys of the participants  $R_2, \dots, R_{10}$ , modulus two.

Next, exploiting the higher-dimensional ( $d = 3$ ) encoding space, we shared a secret key between  $N = 3$  participants, each equipped with the  $X_3$  gate (dove prism) and  $Y_3$  gate (half waveplate). The results are shown in Fig. 6(b) for the secret code retrieved by the distributor and shared between the participants. The keys are identical as desired. Using the high-dimensional protocol for 100 valid runs we generated a secure key that was 158 bits.

## V. DISCUSSION

Transverse spatial modes of light carrying orbital angular momentum have become ubiquitous for encoding quantum information. Here, OAM modes have proven invaluable for secure and robust communication, and thus have the potential to increase the mutual information and security of quantum channels in QSS. However, despite its many potential advantages, the complete realization of high-dimensional quantum

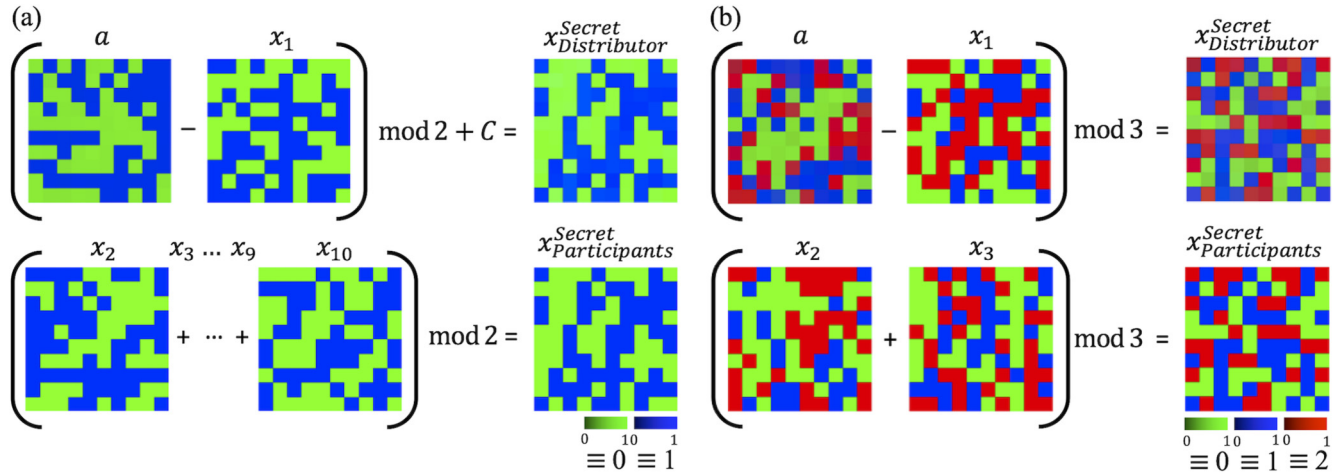


FIG. 6. Experimentally generated distributor's and participants' secret keys, in (a)  $d = 2$  and (b)  $d = 3$  dimensions, by implementing the protocol for 100 valid runs. The color bars indicate the measured probability of generating a 0, 1, or 2.

cryptography with OAM, so far, has been limited by technical difficulties arising in the full manipulation and transmission of this degree of freedom (DOF). To overcome these restraints, photon states encoded in different DOFs, called hybrid entangled states, have attracted a lot of attention [45]. Spin-orbit coupled states, e.g., vector modes, have been used to complete the entanglement purification in photon pairs for polarization Bell states [46,47]. Similarly, they have been used to overcome the limiting channel capacity of superdense coding [48] and to realize a high capacity QKD protocol [49].

We note that, although we used a weak coherent photon source, practical deployments require ideal single photon sources to ensure unconditional security. The engineering of such sources is an ongoing field of research [50] and as a result our scheme remains demonstrable. In principle, one could counter photon splitting attacks by preparing and testing the transmission properties of some decoy states, modulating several intensities of weak coherent photons and reserving one intensity as the signal state. Alternatively, state-of-the-art single photon emitters or sub-Poissonian sources like SPDC heralded photons can be used (see our previous QKD demonstration [51]). Nevertheless, even Fock states larger than  $n = 1$  have a nonzero detection probability and may pose a security risk, potentially requiring the use of decoy states. We stress that we used an attenuated laser source in which the photon statistics follow a Poisson distribution mainly for the high spatial coherence which is no different than that of a single photon source. Correspondingly, the superposition principle and mutually unbiased basis (the fundamental properties exploited in our scheme) are inherent properties in both sources, making both sources equivalent for state encoding and decoding protocols. In fact, a myriad of high-dimensional QKD schemes have been tested this way, using spatially structured photons in free space [52] and fiber [53].

The efficiency and secure key rate could be improved for practical deployments, by using commercially accessible detectors with low dark counts, short detector dead times, high resolution, and high detection efficiencies. Since our scheme is adaptable to any wavelength, detectors with up to 93% efficiency, a dead time of up to 40 ns, a dark count rate

of 1 count per s, and a timing resolution of up to 150 ns are available at telecom wavelengths—promising quantum communication speeds in the megahertz regime [54].

Here, we have reported a scheme for sharing secure keys between multiple parties by interfacing different DOF, namely spin and orbital angular momentum of single photons in high dimensions ( $d = 3$ ). Our scheme can be extended to multiple participants and requires conventional linear optical elements making it easily scalable. For a practical implementation waveplates and dove prisms can be rotated using electronically driven rotation mounts [55], whose rotation rate would be the only limiting factor with regards to the generation rates.

The spatial modes used here can be represented by LG modes and thus are the natural modes of quadratic media like free space and optical fiber making them ideal for practical implementations in long distance communication. So far, free-space quantum channels have been demonstrated with satellite-to-ground links [56], intracity free-space links [57], and in QKD using similar vector modes [58]. Moreover, our basis modes, if chosen carefully, lie within the first two mode groups, which may have low group delays and minimal crosstalk. Hence our scheme can also be exploited over long distances using few mode fibers, as demonstrated up to 1 km for QKD [59]. Applications can also be extended to underwater channels, previously shown for QKD [60]. The main application challenge would be overcoming deleterious effects, like turbulence resulting from local fluctuations in refractive index of refraction [61], which could reduce the QBER.

We iterate that QSS protocols involve the sharing of a random encryption key, as opposed to a predetermined secret message. Where the latter is necessary, quantum secure direct communication (QSDC) is a solution, where secret information is transmitted directly through a quantum channel without prior distribution of a secret key [62–66]. Appropriately, the technique presented here (i.e., using spin-orbit coupled modes as high-dimensional information carriers) has the potential to advance the likes of other quantum communication branches, such as QSDC.



## VI. CONCLUSION

In conclusion, we successfully implemented two-dimensional single photon QSS for 10 parties. We further extended our scheme to higher dimensions by interfacing independent degrees of freedom, providing a natural extension to high-dimensional QSS. Our approach shows that by using hybrid polarization and OAM encoding, it is possible to realize a  $d = 2$  and  $d = 3$  dimensional single photon QSS using conventional linear optical elements. Further, by exploiting the nonseparability of polarization and OAM in our choice of spatial modes, we were able to realize transitions on a high-dimensional Hilbert space, mapping between different MUB states, demonstrating the advantage

of interfacing independent DOFs. Our practical scheme is scalable to an unlimited number of participants and can be realized using current technologies, without generating complex multiparticle entangled states.

## ACKNOWLEDGMENTS

A.F. thanks the African Laser Centre for funding. The authors thank L. Marrucci for the  $q$ -plates.

M.d.O. performed the experiments with assistance from I.N. N.T., M.d.O., J.P., and I.N. developed the theory. All authors contributed to data analysis and writing of the manuscript. A.F. conceived of the idea and supervised the project.

- 
- [1] R. Ahlswede and I. Csiszár, *IEEE Trans. Inf. Theory* **39**, 1121 (1993).
- [2] B. Schneier, *Applied Cryptography*, 2nd ed. (Wiley, New York, 1996), Chap. 3, pp. 47–74.
- [3] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
- [4] A. Sen(De), U. Sen, and M. Żukowski, *Phys. Rev. A* **68**, 032309 (2003).
- [5] I.-C. Yu, F.-L. Lin, and C.-Y. Huang, *Phys. Rev. A* **78**, 012344 (2008).
- [6] S. Bandyopadhyay, *Phys. Rev. A* **62**, 012308 (2000).
- [7] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, *Phys. Rev. A* **64**, 042311 (2001).
- [8] T. Tyc and B. C. Sanders, *Phys. Rev. A* **65**, 042310 (2002).
- [9] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, *Phys. Rev. A* **65**, 042320 (2002).
- [10] S. Bagherinezhad and V. Karimipour, *Phys. Rev. A* **67**, 044302 (2003).
- [11] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, *Phys. Rev. A* **69**, 052307 (2004).
- [12] D. Fu-Guo, L. Gui-Lu, W. Yan, and X. Li, *Chin. Phys. Lett.* **21**, 2097 (2004).
- [13] Y. Li, K. Zhang, and K. Peng, *Phys. Lett. A* **324**, 420 (2004).
- [14] L.-F. Han, Y.-M. Liu, J. Liu, and Z.-J. Zhang, *Opt. Commun.* **281**, 2690 (2008).
- [15] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, *Phys. Rev. Lett.* **92**, 177903 (2004).
- [16] Y. Zhou, J. Yu, Z. Yan, X. Jia, J. Zhang, C. Xie, and K. Peng, *Phys. Rev. Lett.* **121**, 150502 (2018).
- [17] W. Tittel, H. Zbinden, and N. Gisin, *Phys. Rev. A* **63**, 042301 (2001).
- [18] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, *Phys. Rev. Lett.* **95**, 200502 (2005).
- [19] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, *Phys. Rev. Lett.* **98**, 020503 (2007).
- [20] G.-P. Guo and G.-C. Guo, *Phys. Lett. A* **310**, 247 (2003).
- [21] F.-G. Deng, H.-Y. Zhou, and G. L. Long, *J. Phys. A: Math. Gen.* **39**, 14089 (2006).
- [22] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 230505 (2005).
- [23] K.-J. Wei, H.-Q. Ma, and J.-H. Yang, *Opt. Exp.* **21**, 16663 (2013).
- [24] G. P. He, *Phys. Rev. Lett.* **98**, 028901 (2007).
- [25] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, *Opt. Commun.* **281**, 5472 (2008).
- [26] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, *Phys. Rev. A* **92**, 030302(R) (2015).
- [27] V. Karimipour and M. Asoudeh, *Phys. Rev. A* **92**, 030301(R) (2015).
- [28] S. Lin, G.-D. Guo, Y.-Z. Xu, Y. Sun, and X.-F. Liu, *Phys. Rev. A* **93**, 062343 (2016).
- [29] X.-B. Chen, X. Tang, G. Xu, Z. Dou, Y.-L. Chen, and Y.-X. Yang, *Quantum Inf. Process.* **17**, 225 (2018).
- [30] H. Qin and R. Tso, *J. Chin. Inst. Eng.* **42**, 143 (2019).
- [31] K.-h. Zhou, Y. Wang, T.-j. Wang, and C. Wang, *Int. J. Theor. Phys.* **53**, 3927 (2014).
- [32] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, *Npj Quantum Inf.* **2**, 16010 (2016).
- [33] A. Forbes and I. Nape, *AVS Quantum Sci.* **1**, 011701 (2019).
- [34] L. Marrucci, C. Manzo, and D. Paparo, *Phys. Rev. Lett.* **96**, 163905 (2006).
- [35] L. Marrucci, E. Karimi, S. Slussarenko, B. Piccirillo, E. Santamato, E. Nagali, and F. Sciarrino, *J. Opt.* **13**, 064001 (2011).
- [36] A. Forbes, A. Dudley, and M. McLaren, *Adv. Opt. Photon.* **8**, 200 (2016).
- [37] B. Ndagano, I. Nape, M. A. Cox, C. Rosales-Guzman, and A. Forbes, *J. Lightwave Technol.* **36**, 292 (2017).
- [38] Y. Jo, H. S. Park, S.-W. Lee, and W. Son, *Entropy* **21**, 80 (2019).
- [39] M. Żukowski, A. Zeilinger, and M. A. Horne, *Phys. Rev. A* **55**, 2564 (1997).
- [40] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, *Phys. Rev. Lett.* **105**, 153601 (2010).
- [41] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, *Nat. Commun.* **4**, 2781 (2013).
- [42] B. Ndagano, I. Nape, B. Perez-Garcia, S. Scholes, R. I. Hernandez-Aranda, T. Konrad, M. P. Lavery, and A. Forbes, *Sci. Rep.* **7**, 13882 (2017).
- [43] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [44] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).

- [45] E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, and F. Sciarrino, *Phys. Rev. A* **81**, 052317 (2010).
- [46] Y.-B. Sheng and F.-G. Deng, *Phys. Rev. A* **81**, 032307 (2010).
- [47] X.-H. Li, *Phys. Rev. A* **82**, 044304 (2010).
- [48] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, *Nat. Phys.* **4**, 282 (2008).
- [49] W.-Y. Wang, C. Wang, and G.-L. Long, *Int. J. Quantum Inf.* **7**, 529 (2009).
- [50] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, *Rev. Sci. Instrum.* **82**, 071101 (2011).
- [51] I. Nape, E. Otte, A. Vallés, C. Rosales-Guzmán, F. Cardano, C. Denz, and A. Forbes, *Opt. Exp.* **26**, 26946 (2018).
- [52] 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).
- [53] 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, *Phys. Rev. Appl.* **11**, 064058 (2019).
- [54] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin *et al.*, *Nat. Photon.* **7**, 210 (2013).
- [55] E. Toninelli, B. Ndagano, A. Vallés, B. Sephton, I. Nape, A. Ambrosio, F. Capasso, M. J. Padgett, and A. Forbes, *Adv. Opt. Photon.* **11**, 67 (2019).
- [56] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, *Phys. Rev. Lett.* **119**, 200501 (2017).
- [57] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin *et al.*, *Opt. Express* **13**, 202 (2005).
- [58] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim *et al.*, *Optica* **4**, 1006 (2017).
- [59] L. Cui, J. Su, X. Li, and Z. Ou, *Sci. Rep.* **7**, 14954 (2017).
- [60] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, E. Karimi *et al.*, *Opt. Express* **26**, 22563 (2018).
- [61] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, 2nd ed. (SPIE, Washington, 1998), pp. 57–80.
- [62] F.-G. Deng, G. L. Long, and X.-S. Liu, *Phys. Rev. A* **68**, 042317 (2003).
- [63] F.-G. Deng and G. L. Long, *Phys. Rev. A* **69**, 052319 (2004).
- [64] G.-L. Long and X.-S. Liu, *Phys. Rev. A* **65**, 032302 (2002).
- [65] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, *Sci. Bull.* **62**, 1519 (2017).
- [66] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, *Light: Sci. Appl.* **8**, 22 (2019).