Experimental Realization of Quantum Tomography of Photonic Qudits via Symmetric Informationally Complete Positive Operator-Valued Measures

N. Bent,[1] H. Qassim,[1] A. A. Tahir,[1] D. Sych,[2] G. Leuchs,[1,2] L. L. Sánchez-Soto,[2,3] E. Karimi,[1,*] and R. W. Boyd[1,4]

[1]*Department of Physics, University of Ottawa, 150 Louis Pasteur, Ottawa, Ontario, K1N 6N5 Canada*
[2]*Max-Planck-Institut für die Physik des Lichts, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany*
[3]*Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain*
[4]*Institute of Optics, University of Rochester, Rochester, New York 14627, USA*

(Received 3 May 2015; published 12 October 2015)

Symmetric informationally complete positive operator-valued measures provide efficient quantum state tomography in any finite dimension. In this work, we implement state tomography using symmetric informationally complete positive operator-valued measures for both pure and mixed photonic qudit states in Hilbert spaces of orbital angular momentum, including spaces whose dimension is not power of a prime. Fidelities of reconstruction within the range of 0.81–0.96 are obtained for both pure and mixed states. These results are relevant to high-dimensional quantum information and computation experiments, especially to those where a complete set of mutually unbiased bases is unknown.

DOI: 10.1103/PhysRevX.5.041006

Subject Areas: Optics, Quantum Physics, Quantum Information

I. INTRODUCTION

Quantum state tomography (QST) is an experimental procedure that allows the reconstruction of a quantum state via direct measurements on identical copies of the state. An important issue in QST is optimality, a term that has been defined in a variety of ways [1–5]. In general, optimality refers to maximizing the amount of information extracted per single measurement, or equivalently to maximizing the accuracy of the estimation of the quantum state while simultaneously minimizing the sample size. It has been shown that QST using mutually unbiased bases (MUBs) achieves optimality in the class of projective measurements [1], in which a state is projected onto elements of sets of orthogonal bases. They have also been shown to minimize the amount of measurements required. However, the *complete* set of MUBs cannot in general be constructed for a Hilbert space of arbitrary dimension, even for a dimension as low as six [6,7]. This can make QST more complicated for higher dimensions, although recently a QST method using MUBs has been examined for dimensions ranging from two to five [8].

The widely believed impossibility of finding complete set of MUBs for Hilbert spaces whose dimension is not power of a prime [9] calls for the use of positive operator-valued measures (POVMs), a mathematical construction that generalizes the concept of a quantum measurement [10,11]. In the class of POVMs, symmetric informationally complete (SIC) POVMs are optimal [12]. These POVMs have the significant advantage that they have been conjectured to exist in arbitrary dimensions [4,12,13]. Furthermore, they have been calculated numerically for dimensions up to 67 [14], which facilitates their use in configurations that utilize higher-dimensional spaces, such as the orbital angular momentum (OAM) degree of freedom of light. In addition, their optimality means that minimum information is sacrificed in the QST process, which is of paramount importance in applications such as quantum key distribution (QKD), where the two parties need to minimize the informational loss that comes with verifying the security of the source, as well as that which comes from the actual key generation [15]. For instance, the Singapore protocol for performing QKD relies on QST using SIC POVMs [4,15]. Although, this SIC-POVM-based QST has been experimentally realized for qubits [16,17] and qutrits [18], the most interesting cases, i.e., higher-dimensional spaces, are yet to be demonstrated.

OAM of optical beams provides an unbounded Hilbert space in the single-photon regime [19], as they carry a well-defined quantized OAM per photon along the direction of propagation. There has been great interest in innovating and verifying quantum protocols using this variable [20–23]. In this work, we experimentally demonstrate SIC POVMs for photonic qudit spaces with dimensions up to ten. We then implement this concept to perform *optimal* QST of both pure and mixed states in dimensions of 6 and 10, where complete sets of MUBs are unknown. The results show that this technique can yield QST with high fidelities of estimation, and can therefore be utilized in quantum cryptography and

*ekarimi@uottawa.ca

quantum communication in all dimensions, including those for which the complete set of MUBs are unknown.

II. THEORETICAL BACKGROUND

A d-dimensional quantum system is represented by a positive semidefinite $d \times d$ density matrix that requires $d^2 - 1$ independent real numbers for its specification. A von Neumann measurement fixes at most $d - 1$ real parameters, so $d + 1$ tests have to be performed to reconstruct the state. This means that $d(d + 1)$ histograms have to be recorded: the approach is, thus, suboptimal because this number is higher than the number of parameters in the density matrix. The von Neumann strategy can be further optimized regarding this redundancy when the bases in which the measurements are performed are MUBs: two orthonormal bases are MUBs if whenever we choose one state in the first basis, and a second state in the second basis, the modulus squared of their overlap is equal to $1/d$ [24]. When the dimension of the Hilbert space is a prime power, it is known that there exists a maximal set of $d + 1$ MUBs [25].

Put in a more formal way, let us denote by $|\Psi_{\alpha k}\rangle$ the kth element ($0 \le k \le d - 1$) of the αth orthonormal basis of a maximal set of MUBs ($0 \le \alpha \le d$). Then we have

$$\hat{E}_{\alpha k} = \frac{1}{d+1}|\Psi_{\alpha k}\rangle\langle\Psi_{\alpha k}|,$$
$$|\langle\Psi_{\alpha k}|\Psi_{\alpha' \ell}\rangle|^2 = \frac{1}{d}, \qquad \alpha \neq \beta, \tag{1}$$

where the orthogonal projectors $\hat{E}_{\alpha k}$ are normalized so $\sum_{\alpha k}\hat{E}_{\alpha k} = \mathbb{1}$. The probability $p_{\alpha k}$ of obtaining an outcome $|\Psi_{\alpha k}\rangle$ is given by Born's rule $p_{\alpha k} = \mathrm{Tr}(\hat{E}_{\alpha k}\hat{\rho})$, where $\hat{\rho}$ stands for density operator of the system.

Of course, more general classes of measurements exist that generalize the von Neumann measurements. This class is represented by the POVM measurements. To gain physical insights, we recall [10] that the most general POVM can always be obtained by coupling a system A to an *ancilla* B and performing a von Neumann measurement on the complete system. When both the system and its ancilla are qudits, the full system lives in a d^2-dimensional Hilbert space, which makes it possible to measure d^2 probabilities during a von Neumann measurement, and so, this fixes $d^2 - 1$ parameters. When the coupling to the ancilla and the von Neumann measurement are judiciously chosen, we are able in principle to infer the value of the density matrix of the initial qudit system from the knowledge of those $d^2 - 1$ parameters, in which case the POVM is said to be informationally complete (IC).

Moreover, IC POVMs can be further optimized as for the independence of the data in different detectors. The so-called covariant SIC POVMs [26] constitute an elegant solution to this optimization constraint. Actually, in this case the Heisenberg-Weyl displacement operators allow one to construct a set of d^2 minimally overlapping projectors onto pure qudit states [compare with the $d(d+1)$ projectors for the case of MUBs].

In more general terms, a POVM can be defined as a set of positive operators $\{\hat{E}_i\}$ that achieve a decomposition of the identity: $\sum_i \hat{E}_i = \mathbb{1}$. In order for those operators to reveal full information about the state, they must be IC. Furthermore, in analogy to MUBs, the set of rank-1 projectors that minimizes the informational overlap is called symmetric [9] and is defined as

$$\hat{E}_i = \frac{1}{d}|\Phi_i\rangle\langle\Phi_i|, \qquad |\langle\Phi_i|\Phi_j\rangle|^2 = \frac{1}{d+1}, \qquad i \neq j. \tag{2}$$

The structure of a general SIC POVM is quite complex [12]. However, the particular case of group-covariant SIC POVMs has been investigated thoroughly and it has been conjectured that they exist in arbitrary dimensions [12,14]. In particular, Weyl-Heisenberg covariant SIC POVM elements can be generated by applying the d^2 displacement operators

$$\hat{D}_{jk} = \omega_d^{jk/2}\sum_{m=0}^{d-1}\omega_d^{jm}|k \oplus m\rangle\langle m| \tag{3}$$

on some reference (or fiducial) vector $|f\rangle$. Here, $\{|i\rangle\}$ is an orthonormal basis of the space in question, $\omega_d = \exp(2\pi i/d)$ is the dth root of the identity, and $\oplus$ represents addition modulo d [12]. The SIC POVM elements are then obtained as the subnormalized rank-1 projectors onto the resulting states. In this manner, an entire set of SIC POVM elements can be generated if a single fiducial vector is determined. Numerical solutions for fiducial vectors for dimensions up to 67 can be found in Ref. [12]. Once a set of SIC POVM elements is identified, the probability p_i of obtaining an outcome $|\Phi_i\rangle$ is also given by Born's rule, $p_i = \mathrm{Tr}(\hat{E}_i\hat{\rho})$.

To gain more insights into these matters, let us look at the simple yet relevant example of a single qubit (e.g., a spin 1/2). Now, MUBs measurements correspond to three successive Stern-Gerlach measurements performed along orthogonal directions. This allows one to directly infer the three Bloch parameters, $s_x = \langle\hat{\sigma}_x\rangle$, $s_y = \langle\hat{\sigma}_y\rangle$, and $s_z = \langle\hat{\sigma}_z\rangle$ (where σ's denote Pauli matrices), and hence to determine unambiguously the density matrix of the system via

$$\hat{\rho} = \frac{1}{2}(\mathbb{1} + s_x\hat{\sigma}_x + s_y\hat{\sigma}_y + s_z\hat{\sigma}_z). \tag{4}$$

The three MUBs determine six points, which are the vertices of an octahedron, as sketched in Fig. 1(a).

On the other hand, in the standard measurement of a SIC POVM for a single qubit, four probabilities of firing $P_{00}, P_{01}, P_{10}, P_{11}$ are measured: they are in one-to-one correspondence with the Bloch parameters (s_x, s_y, s_z), namely,

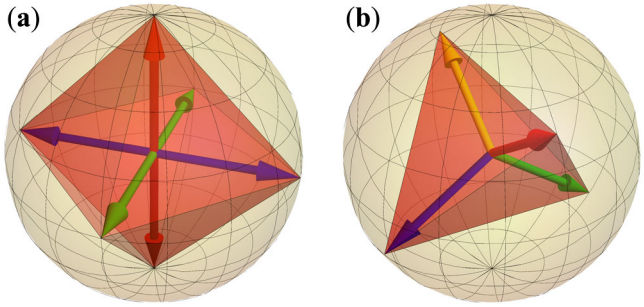

FIG. 1. Bloch sphere representation of two different informationally complete measurements of a qubit. (a) MUB measurement has six measurement outcomes that correspond to vertices of an octahedron. (b) SIC POVM measurement has four measurement outcomes that correspond to vertices of a tetrahedron.

$$P_{00} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(s_x + s_y + s_z)\right],$$
$$P_{01} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(-s_x - s_y + s_z)\right],$$
$$P_{10} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(s_x - s_y - s_z)\right],$$
$$P_{11} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(-s_x + s_y - s_z)\right]. \quad (5)$$

One can check that $2P_{00}$ can be understood as the average of the projector $|\phi\rangle\langle\phi|$, where $|\phi\rangle$ is the pure state $|\phi\rangle = \alpha|0\rangle + \beta^*|1\rangle$, with $|0\rangle$ and $|1\rangle$ being the basis of the qubit and $\alpha = \sqrt{1 + (1/\sqrt{3})}$ and $\beta^* = e^{i\pi/4}\sqrt{1 - (1/\sqrt{3})}$. Then, the four parameters P_{ij} are the average values of projectors onto four pure states that are "Pauli displaced" of each other; explicitly, they read [16]

$$\hat{D}_{ij}|\phi\rangle\langle\phi|\hat{D}_{ij} = \frac{1}{2}\left[\left(1 - \frac{1}{\sqrt{3}}\right)\hat{D}_{00} + \frac{1}{\sqrt{3}}\sum_{k,\ell=0}^{1}(-1)^{i\ell - jk}\hat{D}_{k\ell}\right], \quad (6)$$

where, according to the general definition [Eq. (3)], the displacements are now $\hat{D}_{00} = \mathbb{1}$, $\hat{D}_{01} = \hat{\sigma}_z$, $\hat{D}_{10} = \hat{\sigma}_x$, and $\hat{D}_{11} = \hat{\sigma}_y$. The overlapping between them is equal, in modulus, to $1/\sqrt{3} = 1/\sqrt{d+1}$.

It is easy to realize that these states correspond to vertices of a tetrahedron whose corners lie on the Bloch sphere, which is illustrated in Fig. 1(b). Interestingly, these states provide a maximal violation of the so-called crypto-local hidden-variables theories for a bipartite quantum system [27,28]. They minimize the informational redundancy between the four collected histograms due to the fact that their angular opening is maximal. This SIC POVM approach is at the realm of the Singapore protocol [15], which we discuss in Sec. V.

With these measured statistics, a linear reconstruction can in theory be performed to obtain the density matrix [29]. Since all experiments suffer from some sort of errors, linear reconstruction often constructs nonpositive or mock matrices. There are several different algorithms to obtain a bona fide matrix from the given counts [30–32], but we use the "forced purity" method since it is much less computationally exhausting than methods like maximum likelihood and gives similar fidelities [32].

III. EXPERIMENT

To encode and decode information in the photonic transverse degrees of freedom, we use a spatial light modulator (SLM), which permits pixel-by-pixel control of the phase of the reflected (transmitted) light. Recently, Bolduc *et al.* have shown [33] an exact solution to the problem of finding the hologram pattern that gives any transverse field profile in the first order of diffraction, limited only by the resolution and quality of controlling the phase delay of the SLM's pixels.

A suitable choice for a basis is the photonic OAM eigenstates, which correspond to a beam that possesses a helical phase front $\langle \mathbf{r}|\ell\rangle = \exp(i\ell\phi)$, where ℓ is an integer and ϕ is the azimuthal angle of cylindrical coordinates [19]. Such a beam carries a well-defined, quantized OAM value

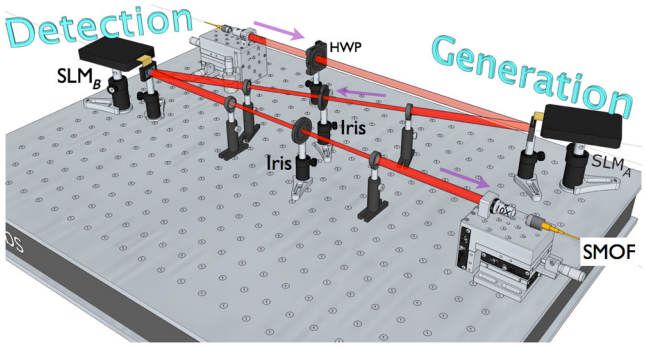

FIG. 2. Experimental setup for generating and detecting OAM photonic qudit states. The signal photon generated via spontaneous parametric down-conversion (not shown) is spatially cleaned and sent into the main setup via a single-mode optical fiber (SMOF). Photonic qudit states (SIC POVMs) are generated by a holographic approach in which the desired kinoform is displayed on the spatial light modulator A (SLM$_A$). A half-wave plate (HWP) optimizes the first order of diffraction on SLM$_A$, since SLMs are polarization dependent. The mode $|\Psi\rangle$ produced by SLM$_A$ is then projected onto a SIC POVM element $\hat{E}_i$ on SLM$_B$. The resulting far field is coupled into a SMOF, which selects the TEM$_{00}$-like component. We implement two $4f$ systems with unit magnification to image SLM$_A$ onto SLM$_B$ and SLM$_B$ onto the microscope objective. Irises are used to select the first order of diffraction at the far-field plane of SLMs, where higher diffraction orders are well separated.

of $\ell\hbar$ per photon along its direction of propagation, where $\hbar$ is the reduced Planck's constant. The Hilbert space associated with OAM eigenstates is unbounded, thus allowing quantum protocols based on qudits to be implemented practically. Moreover, OAM state discrimination can be easily achieved by using the so-called phase flattening technique [34], wherein the azimuthal phase dependence of a Laguerre-Gauss mode is removed by projecting the mode onto a SLM that displays the complex conjugate field, and the diffracted beam is then coupled into a single-mode optical fiber (SMOF). For instance, the intensity and phase distribution of light beams associated to SIC POVM elements of OAM photonic qusixt are shown in Appendix B. Mutual projection between these SIC POVM elements results in an unbiased value of $|\langle\Phi_i|\Phi_j\rangle|^2 = 1/7$ for $i \neq j$.

Next, we give a brief description of the experimental setup depicted in Fig. 2. A frequency-tripled quasi-cw mode-locked Nd-YAG laser (repetition rate of 100 MHz and average output power of 150 mW at 355 nm) is used to pump a nonlinear β-barium borate (BBO) crystal cut for type-I degenerate phase matching. The photon pairs (signal and idler) generated via spontaneous parametric down-conversion are split out by means of a knife-edge prism and coupled into SMOFs, where only TEM_{00}-like spatial modes are supported (see Ref. [35] for details of the single-photon source). Idler photons are detected by a silicon avalanche photodiode after being spectrally filtered by an interference filter with a bandwidth of $\Delta\lambda = 10$ nm and then used as trigger. To optimize the diffraction efficiency, polarization of signal photons is rotated to horizontal after compensating for polarization rotation induced by SMOF and is sent to the main apparatus: an OAM generation stage followed by a detection stage.

The generation stage is composed of a SLM, which converts the photons to either a pure (localized or superposition) or a mixed state of Laguerre-Gauss modes. The detection stage includes a SLM followed by a microscope objective coupling to a SMOF. The coupled photons are detected by a silicon avalanche photodiode, and finally a National Instruments data acquisition card records photon counts and coincidences between the signal and idler detectors. The planes of the generation SLM, the detection SLM, and the microscope objective are imaged onto each other via $4f$-lens systems with unit magnification.

Holograms displayed on both the generating and detecting SLMs are calculated using the aforementioned technique [33]. Numerical solutions for fiducial vectors in dimensions 2–10, as reported in Ref. [14], are utilized to obtain the coefficients of expansion of SIC POVMs in the OAM basis. In order to remove the bias that comes from any spatial mismatch between the transverse modes of the two SLMs, as well as the bias that originates from different coupling efficiencies for different OAM eigenmodes [36], the entire set of SIC POVMs elements for each dimension are generated and then detected. Hence, a matrix of projections of SIC POVM elements, $P_{ij} = |\langle\Phi_i|\Phi_j\rangle|^2$, is

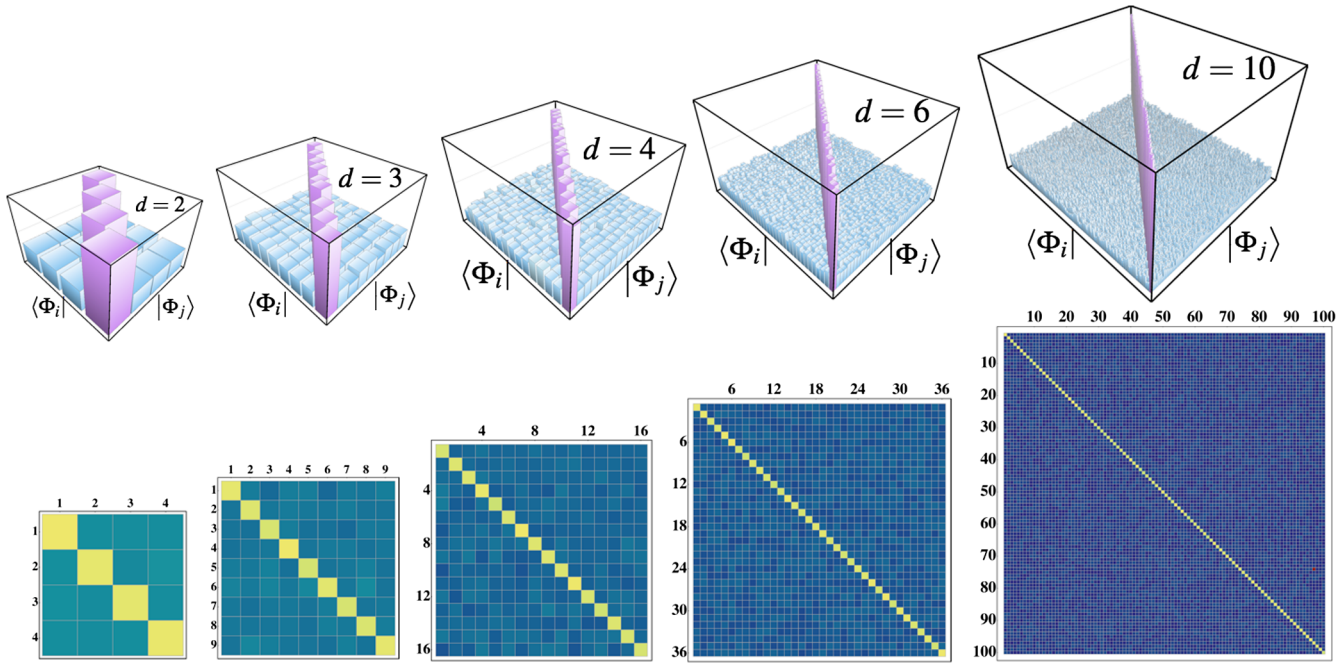

FIG. 3. Experimentally measured characterization of the generation and detection of SIC POVMs elements for different photonic qudit subspaces. Each block corresponds to $P_{ij} = |\langle\Phi_i|\Phi_j\rangle|^2$, where $|\Phi_i\rangle$ correspond to the ith SIC POVM element, i.e., $\hat{E}_i = (1/d)|\Phi_i\rangle\langle\Phi_i|$. Lower figures are the density plots of the upper histograms. Projecting SIC POVMs for each dimension d acquires d^2 set of measurements.

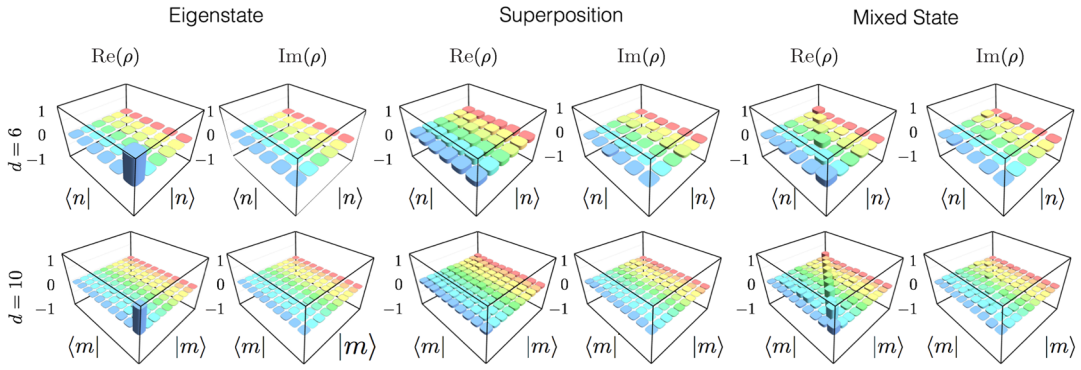

FIG. 4. Examples of the reconstructed density matrices of pure and mixed states. Left and right columns of each measurement show real and imaginary parts of the density matrix. Different rows correspond to different photonic qudit dimensions of 6 and 10. The state $|n\rangle$ ranges from $\{|-3\rangle,\ldots,|+3\rangle\}$ and $|m\rangle$ ranges from $\{|-5\rangle,\ldots,|+5\rangle\}-\mathrm{TEM}_{00}$, i.e., $|0\rangle$ is excluded. Pure eigenstates, superpositions, and mixed states are defined as $|+3\rangle$, $1/6\sum_{n=-3}^{+3}|n\rangle$, and $\hat{\rho}=1/6\sum_{n=-3}^{+3}|n\rangle\langle n|$, for dimension 6, and $|+5\rangle$, $1/10\sum_{m=-5}^{+5}|m\rangle$ and $\hat{\rho}=1/10\sum_{m=-5}^{+5}|m\rangle\langle m|$, for dimension 10, where $\{n,m\}\neq 0$.

created, as shown in Fig. 3, which is then used to normalize the data. For a comparative parameter we use the similarity parameter $S=(\sum_{i,j}\sqrt{P_{ij}P'_{ij}})^2/(\sum_{i,j}P_{ij}\sum P'_{ij})$, where P_{ij} and P'_{ij} stand for experimental and theoretical projections of SIC POVM elements, respectively. We observe an average similarity of 97% for projection of SIC POVMs in dimensions $d=\{2,3,4,5,6,7,8,9,10\}$.

To carry out QST, the state of photons is converted to a state characterized by a density matrix $\hat{\rho}$. Mixed states are generated by cycling through the display of random kinoforms from a suitable set with predetermined weight, which is achieved by a random-number algorithm. The state of the photon is then projected onto each of the SIC POVM elements and coupled to a SMOF leading to the coincidence counter. Histograms are recorded for each SIC POVM element and reconstructed density matrices are then postprocessed.

IV. RESULTS AND DISCUSSION

We perform QST in the first two "problematic" dimensions of 6 and 10 for pure eigenstates, superpositions, and mixed states. These two Hilbert spaces are chosen because complete sets of MUBs are unknown for them. Thus, one should implement an overcomplete QST by projecting the state onto sub-Hilbert spaces. Figure 4 shows the real and imaginary parts of experimentally reconstructed density matrices of a pure eigenstate, a superposition, and a mixed state in dimensions 6 and 10. Fidelity of the reconstructed density matrices with respect to the generated ones is shown in Table I for pure and mixed states in dimensions 6 and 10 [37]. The fidelity is lower on mixed states than on pure states because the position of the vector in the Bloch sphere is not on the surface, and as such it takes more counts to be able to distinguish its coordinates. As the dimension grows, the more coordinates a point has in the Bloch ball, the larger the number of counts needed to resolve its position [38].

It is important to compare our results with other forms of QST. Probably, the comparison that is most easily made would be one using MUBs. SIC POVMs provide d fewer states on which one has to project in comparison with MUBs, when the complete set of MUBs is known. For dimensions where a complete set of MUBs is unknown, we have to factor d into all of its prime-power factors. From there we can build a POVM that is the tensor product of the MUBs of the Hilbert spaces of factors of d. For instance, Hilbert space of dimension 6 can be factored into Hilbert spaces of 2 and 3, which have 3 and 4 MUBs, respectively. This means that the total number of states for performing overcomplete QST is $(4\times 3)(3\times 2)=72$, which is twice that of the SIC POVM for dimension 6; i.e., $6^2=36$. For dimension 10, using the same method we would have $(6\times 5)(3\times 2)=180$ states, in comparison to the $10^2=100$ needed for SIC POVM.

In addition, we calculate the fidelity for a given noisy matrix in dimensions from 4 to 10 using SIC POVMs and MUBs. We use the method in Ref. [32] to generate pseudoexperimental data. We keep the total amount of counts constant for the whole experiment and then distribute the counts equally per measurement. The total

TABLE I. Experimental fidelities of pure and mixed reconstructed states in dimensions 6 and 10. The coincidence counts are 5 and 3 kHz for dimension 6 and dimension 10, respectively.

	Pure		Mixed
Dimension	Eigenstate	Superposition	Maximally mixed
6	0.960 ± 0.003	0.931 ± 0.003	0.905 ± 0.05
10	0.887 ± 0.003	0.859 ± 0.003	0.818 ± 0.07

TABLE II. Counts per QST method necessary to obtain a 90% fidelity. This is obtained based on Monte Carlo simulations; see the main text for details.

Dimension		% average fidelity	Total counts
4	MUB	95	2500
	SIC POVM	93	2500
5	MUB	94	13 000
	SIC POVM	93	13 000
6	MUB	90	35 000
	SIC POVM	92	35 000
7	MUB	94	89 000
	SIC POVM	92	89 000
8	MUB	94	216 000
	SIC POVM	91	216 000
9	MUB	93	511 000
	SIC POVM	91	511 000
10	MUB	88	1 120 000
	SIC POVM	91	1 120 000

amount of counts are scaled exponentially. These results are displayed in Table II. For dimensions where the complete set of MUBs is known, MUBs are known to minimize the number of measurements required, thus outperforming SIC POVMs [39]. In dimensions 6 and 10, SIC POVMs surpass the overcomplete measurement.

V. APPLICATION TO QKD: SINGAPORE PROTOCOL WITH OAM

An important application of SIC POVMs can be found in QKD, wherein two parties, Alice and Bob, exchange a key, using a quantum channel, which they can use to encode and decode information transmitted over a public classical channel. There have been various different protocols that have been proposed and implemented [40,41]. Interestingly, SIC-POVM-based QKD turns out to be better than the MUB-based one [42]. The Singapore protocol relies on SIC POVMs in two distinct ways: (i) as a method of measuring the qubits and (ii) as a method of testing the source by performing optimal QST on a number of qubits, which are sacrificed in order to check the integrity of the source. In this protocol, Alice and Bob share anticorrelated qubits, and each sends their qubit into a four-detector apparatus, with each detector corresponding to a SIC POVM element. Following Ref. [15], we label the four detectors A, B, C, and D. Two different methods are then combined to generate the key: Renes pairing [43] and iterative Singapore pairing. The starting point for each method is a sequence of measurement outcomes for both Alice and Bob, say,

$$\text{Alice} \quad A, B, D, C, B, A, \ldots$$

$$\text{Bob} \quad C, A, C, B, A, B, \ldots,$$

where, because of anticorrelations, the same detector never fires off for both Alice and Bob, but the remaining three detectors have equal probabilities of firing off due to the symmetric nature of SIC POVMs. In Renes pairing, for each pair of outcomes, Alice chooses the outcome of her measurement, say, A for the first qubit and another random letter, say, B. She assigns 0 and 1 to each letter, say, $A \to 0$ and $B \to 1$, and then instructs Bob publicly to assign the opposite numbers to each of the letters A and B, i.e., for Bob $A \to 1$ and $B \to 0$. Bob, of course, will never obtain Alice's letter, but will report success if Alice has succeeded in guessing his letter, i.e., if his letter is B in this example. In case of a failure, that pair of qubits is discarded. This method of key generation clearly has an efficiency of $1/3$, since Alice will succeed in guessing Bob's letter one-third of the time.

The main ingredient of the Singapore protocol, however, is iterative Singapore pairing, in which Alice chooses a random letter, for instance, the letter A, and reports publicly to Bob two positions where that letter occurs in her sequence, i.e., positions 1 and 6, but not the actual letter itself. If Bob has distinct letters in those positions of his sequence, he forms two sets: one of those two letters, i.e., $\{C, B\}$, and another of the remaining two letters, $\{A, D\}$. Thanks to anticorrelations, he knows that Alice's letter is in the second set. He then flips a coin to randomly assign the numbers 0 and 1 to the two sets and informs Alice accordingly in a public message, e.g., $\{C, B\} \to 0$, and $\{A, D\} \to 1$. They both then record that key bit associated with the set to which Alice's letter belongs, which, in our example, is the key bit 1. If, on the other hand, Bob had identical letters in the positions that Alice sent him, he reports to her that he does so, and both discard their respective qubits but write down the outcomes in a secondary sequence. For example, if Alice had chosen the letter B, which occurs at positions 2 and 5 of her sequence, Bob would have had the letter A in both of these locations, and thus they would have discarded those qubits and written their letters in the secondary sequences:

$$\text{Alice} \quad B$$

$$\text{Bob} \quad A$$

A secondary sequence generated in this manner preserves the anticorrelation statistics of Alice's and Bob's measurements. This process then continues until all identical pairs of Alice's main sequence are exhausted, at which point they switch to the secondary sequence, and generate more key bits from it, together with yet a third sequence. The process is iterated until Alice exhausts all identical letter pairs in her last sequence. It can be shown that each round of Singapore pairing has an efficiency of $2/5$, which is higher than that of Renes pairing. To maximize the bit generation efficiency of the protocol even further, Alice and Bob perform a Renes pairing at the end of each Singapore pairing round.

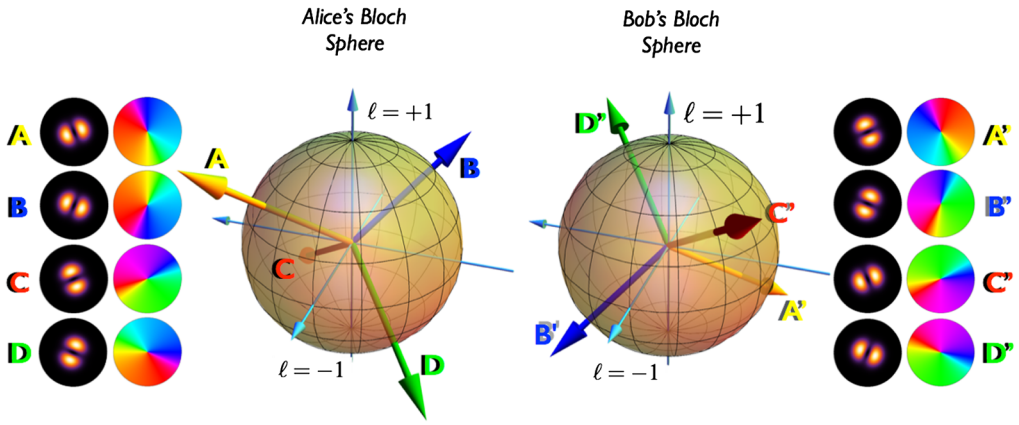

FIG. 5. State representation of SIC POVMs for OAM qubit on Alice's and Bob's Bloch (Poincaré) spheres. The two sets of vectors $\{A, B, C, D\}$ and $\{A', B', C', D'\}$ represent Alice's and Bob's SIC POVM elements, respectively. Any pair of conjugate vectors, e.g., A and A', are orthogonal, and hence a qubit generated by Alice in one of these states has zero probability of being detected as the conjugate state, and equal probabilities of the remaining three. We intently draw the vectors to be outside of the Bloch spheres. Indeed, the implemented states are on the surface of the Bloch spheres, since they are pure states.

The anticorrelated source can be replaced by a single-qubit source prepared by Alice in one of the states associated with SIC POVM, given that Bob arranges to have his respective SIC POVM rotated by an angle π on the Bloch sphere with respect to Alice's (see Fig. 5). In this case, both letter sequences will still be anticorrelated in the exact same way as in the entanglement-based version, and will produce the same statistics.

Finally, an essential step in the Singapore protocol is verifying the integrity of the source of anticorrelated qubits. To this end, Alice and Bob perform full state tomography on a number of the anticorrelated qubits in their possession prior to the actual key generation. Any attack by Eve is detected as a deterioration in the quality of entanglement, and upon exceeding a certain threshold, Alice and Bob will deem the qubits unfit and abort the protocol. It is therefore preferable that they perform highly accurate QST while sacrificing the minimum number of qubits, and SIC POVM QST is indeed the optimal way to do so. It is worth mentioning that the induced experimental noises for $d = 2$, shown in Fig. 3, is about 0.006 ± 0.005, which is well below the Singapore protocol threshold noise 0.3893 [44].

VI. CONCLUSION

In summary, we experimentally demonstrate optimal QST with SIC POVMs in Hilbert spaces associated with photon OAM. In order to achieve this, we generate and project photonic SIC POVMs in the OAM degree of freedom of dimensions 2–10 by means of spatial light modulators. Fidelities of reconstruction in the range of 0.859–0.960 are achieved for pure states and 0.818–0.905 for mixed states in dimensions 6 and 10. We hope that this work will pave the way for more robust and accurate implementations of analyzing photonic OAM states, especially OAM-based quantum computing and cryptography.

ACKNOWLEDGMENTS

The authors thank Markus Grassl and Joseph M. Renes for fruitful discussions. The authors acknowledge the support of the Canada Excellence Research Chairs (CERC) Program. R. W. B. was supported by the DARPA InPho program. L. L. S.-S. acknowledges support from the Spanish MINECO (Grant No. FIS2011-26786) and the Program UCM-BSCH (Grant No. GR3/14).

APPENDIX A: LINEAR ESTIMATION

A d-dimensional quantum system can be described most generally by a density matrix:

$$\hat{\rho} = \sum_{i,j=1}^{d} p_{ij} |\psi_i\rangle\langle\psi_j|, \qquad \mathrm{Tr}(\hat{\rho}) = 1, \tag{A1}$$

where $\mathrm{Tr}(\hat{A})$ is the trace of the operator $\hat{A}$ and $\{|\psi_i\rangle\}$ is an orthonormal basis. Since $\hat{\rho}$ must be Hermitian with positive diagonal elements that sum to one, it is completely determined by $d^2 - 1$ independent real parameters. The problem of tomography is thus the determination of these parameters via a suitable set of measurements. There are two different ways one can go about determining those parameters experimentally: (i) employing projective (von Neumann) measurements or (ii) seeking generalized quantum measurements, i.e., POVMs, of which the former are a subcategory.

A projective measurement [10] is represented by a set of orthogonal projectors: $\hat{P}_i := |\psi_i\rangle\langle\psi_i|$, with $\hat{P}_i \hat{P}_j = \delta_{ij} \hat{P}_i$ and

$\sum_i \hat{P}_i = \mathbb{1}$, where $\mathbb{1}$ is the identity operator. Such a measurement can yield only $d-1$ independent real parameters of the total density matrix $\hat{\rho}$, and as such one needs $d+1$ measurements to determine the state. Since each measurement has d outcomes, one in total obtains d^2+d different measurement outcomes [9]. Moreover, it has been shown [1] that the optimal choice of such measurements is that corresponding to MUBs, since their mutual unbiasedness means that the informational overlap between those measurements is minimized. The drawback is that a complete set of $d+1$ MUBs is not easy to deduce. In fact, the complete sets of MUBs (i.e., $d+1$) have only been found analytically for Hilbert spaces of composite dimension, i.e., power of a prime [9].

To simplify the analysis, it is useful to express the density matrix and SIC POVM elements using the standard parametrizations:

$$\hat{\rho} = \frac{1}{d}(\mathbb{1} + \mathbf{b}\cdot\boldsymbol{\sigma}), \tag{A2}$$

$$\hat{E}_i = \alpha_i(\mathbb{1} + \beta_i\cdot\boldsymbol{\sigma}), \tag{A3}$$

where $\boldsymbol{\sigma}$ is a traceless Hermitian operator basis, which coincide with the generators of the group $\mathrm{SU}(d)$ and constitutes the generalization of the Pauli matrices. The vector $\mathbf{b}$ is a generalized Bloch vector in R^{d^2-1}, whereas α_i are real numbers that satisfy $\alpha_i \geq 0$, and $\beta_i \in R^{d^2-1}$ are vectors satisfying $\mathbb{1} + \beta_i\cdot\boldsymbol{\sigma} \geq 0$.

The last two conditions follow from the fact that the operators $\hat{E}_i$ are positive. Since the POVM elements must satisfy $\sum_i \hat{E}_i = \mathbb{1}$, we see that they are not independent; i.e., after determining d^2-1 elements, the last one gets fixed by the normalization. Hence, it is sufficient to work with d^2-1 elements. Combining Eq. (A2) and Born's rule, we can express the probabilities for these elements as

$$\begin{pmatrix} p_1 \\ \vdots \\ p_{d^2-1} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{d^2-1} \end{pmatrix} + \mathcal{T}\begin{pmatrix} b_1 \\ \vdots \\ b_{d^2-1} \end{pmatrix}, \tag{A4}$$

where $\mathcal{T} = (\alpha_1, \alpha_2, \ldots, \alpha_{d^2-1})^T(\beta_1, \beta_2, \ldots, \beta_{d^2-1})$, and T denotes the transpose. In the above equation, components of the Bloch vector are related to the probabilities of outcomes of the SIC POVM elements via the parameters α_i and β_i, which are determined from the parametrization of $\hat{E}_i$, i.e., Eq. (A2). The problem of tomography is reduced to inverting the matrix $\mathcal{T}$ to obtain the Bloch vector, whose d^2-1 components completely determine the density matrix. Experimentally, we estimate the probabilities p_i by projecting onto each element $\hat{E}_i$, obtaining relative frequencies of occurrence $\nu_1, \ldots, \nu_{d^2-1}$, upon which the estimator of the Bloch vector is derived from Eq. (A4) as

$$\begin{pmatrix} b_1 \\ \vdots \\ b_{d^2-1} \end{pmatrix} = \mathcal{T}^{-1}\begin{pmatrix} \nu_1 - \alpha_1 \\ \vdots \\ \nu_{d^2-1} - \alpha_{d^2-1} \end{pmatrix}. \tag{A5}$$

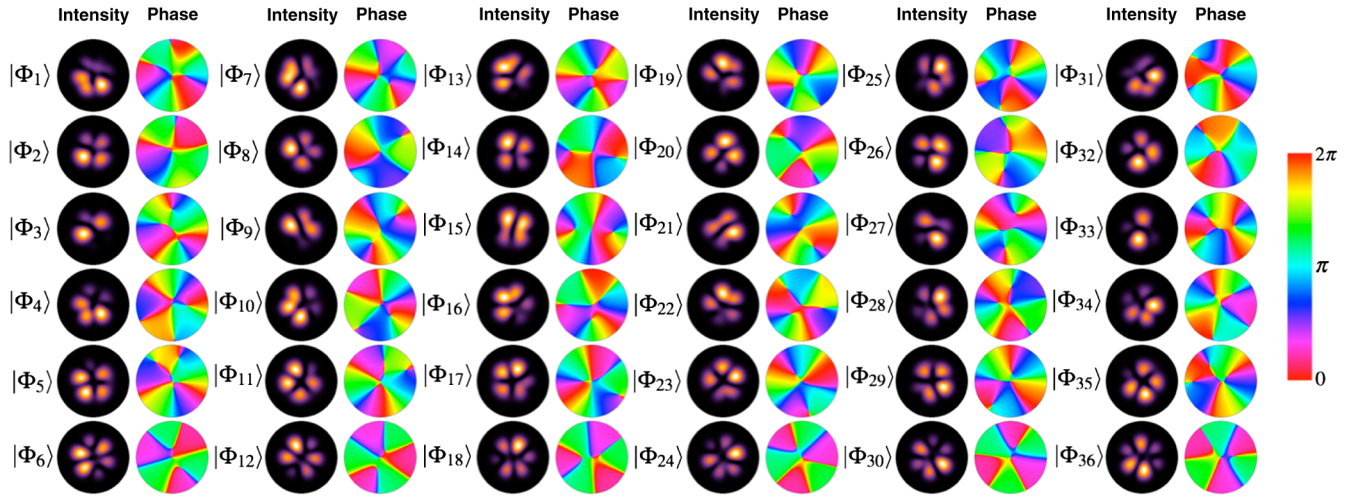

FIG. 6. Intensity and phase of SIC POVM elements for photonic qudit state of dimension six. The states are calculated by acting 36 Weyl-Heisenberg operators represented in Eq. (3) on the fiducial state of $|f_6\rangle$. The implemented OAM Hilbert space spans on $\{|+3\rangle, |+2\rangle, |+1\rangle, |-1\rangle, |-2\rangle, |-3\rangle\}$ OAM eigenstates.

APPENDIX B: WEYL-HEISENBERG MATRICES FOR DIMENSION 6

For completeness, we give here the $6^2 = 36$ elements of the Weyl-Heisenberg matrices for SIC POVMs in dimension $d = 6$, calculated according to Eq. (3):

$$\mathcal{D}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{D}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathcal{D}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad \mathcal{D}_5 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \mathcal{D}_6 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega_6 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega_6^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\omega_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega_6^2 \end{pmatrix}, \quad \mathcal{D}_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -\omega_6^{5/2} \\ \omega_6^{1/2} & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega_6^5 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\omega_6^{1/2} & 0 & 0 \\ 0 & 0 & 0 & 0 & -i & 0 \end{pmatrix},$$

$$\mathcal{D}_9 = \begin{pmatrix} 0 & 0 & 0 & 0 & -\omega_6^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \omega_6 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega_6^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\omega_6 & 0 & 0 \end{pmatrix}, \quad \mathcal{D}_{10} = \begin{pmatrix} 0 & 0 & 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & -\omega_6^{5/2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega_6^{1/2} \\ i & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega_6^{5/2} & 0 & 0 & 0 & 0 \\ 0 & 0 & -\omega_6^{1/2} & 0 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_{11} = \begin{pmatrix} 0 & 0 & -\omega_6 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\omega_6^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega_6 \\ \omega_6^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \mathcal{D}_{12} = \begin{pmatrix} 0 & -\omega_6^{1/2} & 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & -\omega_6^{5/2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega_6^{1/2} & 0 \\ 0 & 0 & 0 & 0 & 0 & i \\ \omega_6^{5/2} & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_{13} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega_6^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\omega_6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega_6^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\omega_6 \end{pmatrix}, \quad \mathcal{D}_{14} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -\omega_6^2 \\ \omega_6 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\omega_6^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_6 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix},$$

$$\mathcal{D}_{15} = \begin{pmatrix} 0 & 0 & 0 & 0 & -\omega_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \omega_6^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\omega_6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_6^2 & 0 & 0 \end{pmatrix}, \quad \mathcal{D}_{16} = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\omega_6^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega_6 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\omega_6^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega_6 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_{17}=\begin{pmatrix}0&0&\omega_6^2&0&0&0\\0&0&0&-\omega_6&0&0\\0&0&0&0&1&0\\0&0&0&0&0&\omega_6^2\\-\omega_6&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\quad \mathcal{D}_{18}=\begin{pmatrix}0&\omega_6&0&0&0&0\\0&0&-1&0&0&0\\0&0&0&-\omega_6^2&0&0\\0&0&0&0&\omega_6&0\\0&0&0&0&0&-1\\-\omega_6^2&0&0&0&0&0\end{pmatrix},\quad \mathcal{D}_{19}=\begin{pmatrix}1&0&0&0&0&0\\0&-1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&-1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&-1\end{pmatrix},$$

$$\mathcal{D}_{20}=\begin{pmatrix}0&0&0&0&0&-i\\i&0&0&0&0&0\\0&-i&0&0&0&0\\0&0&i&0&0&0\\0&0&0&-i&0&0\\0&0&0&0&i&0\end{pmatrix},\quad \mathcal{D}_{21}=\begin{pmatrix}0&0&0&0&-1&0\\0&0&0&0&0&1\\-1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&-1&0&0&0\\0&0&0&1&0&0\end{pmatrix},\quad \mathcal{D}_{22}=\begin{pmatrix}0&0&0&i&0&0\\0&0&0&0&-i&0\\0&0&0&0&0&i\\-i&0&0&0&0&0\\0&i&0&0&0&0\\0&0&-i&0&0&0\end{pmatrix},$$

$$\mathcal{D}_{23}=\begin{pmatrix}0&0&1&0&0&0\\0&0&0&-1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&-1\\1&0&0&0&0&0\\0&-1&0&0&0&0\end{pmatrix},\quad \mathcal{D}_{24}=\begin{pmatrix}0&-i&0&0&0&0\\0&0&i&0&0&0\\0&0&0&-i&0&0\\0&0&0&0&i&0\\0&0&0&0&0&-i\\i&0&0&0&0&0\end{pmatrix},\quad \mathcal{D}_{25}=\begin{pmatrix}1&0&0&0&0&0\\0&-\omega_6&0&0&0&0\\0&0&\omega_6^2&0&0&0\\0&0&0&1&0&0\\0&0&0&0&-\omega_6&0\\0&0&0&0&0&\omega_6^2\end{pmatrix},$$

$$\mathcal{D}_{26}=\begin{pmatrix}0&0&0&0&0&-\omega_6\\\omega_6^2&0&0&0&0&0\\0&1&0&0&0&0\\0&0&-\omega_6&0&0&0\\0&0&0&\omega_6^2&0&0\\0&0&0&0&1&0\end{pmatrix},\quad \mathcal{D}_{27}=\begin{pmatrix}0&0&0&0&\omega_6^2&0\\0&0&0&0&0&1\\-\omega_6&0&0&0&0&0\\0&\omega_6^2&0&0&0&0\\0&0&1&0&0&0\\0&0&0&-\omega_6&0&0\end{pmatrix},\quad \mathcal{D}_{28}=\begin{pmatrix}0&0&0&1&0&0\\0&0&0&0&-\omega_6&0\\0&0&0&0&0&\omega_6^2\\1&0&0&0&0&0\\0&-\omega_6&0&0&0&0\\0&0&\omega_6^2&0&0&0\end{pmatrix},$$

$$\mathcal{D}_{29}=\begin{pmatrix}0&0&-\omega_6&0&0&0\\0&0&0&\omega_6^2&0&0\\0&0&0&0&1&0\\0&0&0&0&0&-\omega_6\\\omega_6^2&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\quad \mathcal{D}_{30}=\begin{pmatrix}0&\omega_6^2&0&0&0&0\\0&0&1&0&0&0\\0&0&0&-\omega_6&0&0\\0&0&0&0&\omega_6^2&0\\0&0&0&0&0&1\\-\omega_6&0&0&0&0&0\end{pmatrix},\quad \mathcal{D}_{31}=\begin{pmatrix}1&0&0&0&0&0\\0&-\omega_6^2&0&0&0&0\\0&0&-\omega_6^{1/3}&0&0&0\\0&0&0&-1&0&0\\0&0&0&0&\omega_6^2&0\\0&0&0&0&0&\omega_6\end{pmatrix},$$

$$\mathcal{D}_{32}=\begin{pmatrix}0&0&0&0&0&-\omega_6^{1/2}\\\omega_6^{5/2}&0&0&0&0&0\\0&i&0&0&0&0\\0&0&\omega_6^{1/2}&0&0&0\\0&0&0&-\omega_6^{5/2}&0&0\\0&0&0&0&-i&0\end{pmatrix},\quad \mathcal{D}_{33}=\begin{pmatrix}0&0&0&0&\omega_6&0\\0&0&0&0&0&1\\-\omega_6^2&0&0&0&0&0\\0&-\omega_6&0&0&0&0\\0&0&-1&0&0&0\\0&0&0&\omega_6^2&0&0\end{pmatrix},$$

$$\mathcal{D}_{34} = \begin{pmatrix} 0 & 0 & 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & -\omega_6^{1/2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega_6^{5/2} \\ i & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega_6^{1/2} & 0 & 0 & 0 & 0 \\ 0 & 0 & -\omega_6^{5/2} & 0 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_{35} = \begin{pmatrix} 0 & 0 & \omega_6^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\omega_6^2 \\ -\omega_6 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathcal{D}_{36} = \begin{pmatrix} 0 & -\omega_6^{5/2} & 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & -\omega_6^{1/2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega_6^{5/2} & 0 \\ 0 & 0 & 0 & 0 & 0 & i \\ \omega_6^{1/2} & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

A set of SIC POVM elements can be calculated by acting with the above matrices on the fiducial vector: $|f_6\rangle = (0.524, 0.025 - 0.618i, -0.128 - 0.107i, -0.360 - 0.335i, 0.089 - 0.002i, 0.180 - 0.177i)$.

[1] W. K. Wootters and B. D. Fields, *Optimal State-Determination by Mutually Unbiased Measurements*, Ann. Phys. (N.Y.) **191**, 363 (1989).

[2] R. Derka, V. Bužek, and A. Ekert, *Universal Algorithm for Optimal Estimation of Quantum States from Finite Ensembles via Realizable Generalized Measurement*, Phys. Rev. Lett. **80**, 1571 (1998).

[3] A. J. Scott, *Tight Informationally Complete Quantum Measurements*, J. Phys. A **39**, 13507 (2006).

[4] H. Zhu and B.-G. Englert, *Quantum State Tomography with Fully Symmetric Measurements and Product Measurements*, Phys. Rev. A **84**, 022327 (2011).

[5] J. Nunn, B. J. Smith, G. Puentes, I. A. Walmsley, and J. S. Lundeen, *Optimal Experiment Design for Quantum State Tomography: Fair, Precise, and Minimal Tomography*, Phys. Rev. A **81**, 042109 (2010).

[6] D. McNulty and S. Weigert, *On the Impossibility to Extend Triples of Mutually Unbiased Product Bases in Dimension Six*, Int. J. Quantum. Inform. **10**, 1250056 (2012).

[7] V. D'Ambrosio, F. Cardano, E. Karimi, E. Nagali, E. Santamato, L. Marrucci, and F. Sciarrino, *Test of Mutually Unbiased Bases for Six-Dimensional Photonic Quantum Systems*, Sci. Rep. **3**, 2726 (2013).

[8] D. Giovannini, J. Romero, J. Leach, A. Dudley, A. Forbes, and M. J. Padgett, *Characterization of High-Dimensional Entangled Systems via Mutually Unbiased Measurements*, Phys. Rev. Lett. **110**, 143601 (2013).

[9] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, *On Mutually Unbiased Bases*, Int. J. Quantum. Inform. **08**, 535 (2010).

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2010).

[11] D. Sych, J. Řeháček, Z. Hradil, G. Leuchs, and L. L. Sánchez-Soto, *Informational Completeness of Continuous-Variable Measurements*, Phys. Rev. A **86**, 052123 (2012).

[12] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric Informationally Complete Quantum Measurements*, J. Math. Phys. (N.Y.) **45**, 2171 (2004).

[13] G. Zauner, *Quantum Designs: Foundations of a Noncommutative Design Theory*, Int. J. Quantum. Inform. **09**, 445 (2011).

[14] A. J. Scott and M. Grassl, *Symmetric Informationally Complete Positive-Operator-Valued Measures: A New Computer Study*, J. Math. Phys. (N.Y.) **51**, 042203 (2010).

[15] B.-G. Englert, W. K. Chua, J. Anders, D. Kaszlikowski, and H. K. Ng, *Highly Efficient Quantum Key Distribution with Minimal State Tomography*, 2004.

[16] T. Durt, C. Kurtsiefer, A. Lamas-Linares, and A. Ling, *Wigner Tomography of Two-Qubit States and Quantum Cryptography*, Phys. Rev. A **78**, 042338 (2008).

[17] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Linear Optical Quantum Computing with Photonic Qubits*, Rev. Mod. Phys. **79**, 135 (2007).

[18] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs, and A. M. Steinberg, *Experimental Characterization of Qutrits Using Symmetric Informationally Complete Positive Operator-Valued Measurements*, Phys. Rev. A **83**, 051801 (2011).

[19] L. Allen, S. M. Barnett, and M. J. Padgett, *Optical Angular Momentum* (IOP Publishing, Bristol, England, 2003).

[20] G. Molina-Terriza, J. P. Torres, and L. Torner, *Twisted Photons*, Nat. Phys. **3**, 305 (2007).

[21] S. Franke-Arnold, L. Allen, and M. Padgett, *Advances in Optical Angular Momentum*, Laser Photonics Rev. **2**, 299 (2008).

[22] L. Marrucci, E. Karimi, S. Slussarenko, B. Piccirillo, E. Santamato, E. Nagali, and F. Sciarrino, *Spin-to-Orbital Conversion of the Angular Momentum of Light and Its*

Classical and Quantum Applications, J. Opt. **13**, 064001 (2011).

[23] 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).

[24] J. Schwinger, *Unitary Operator Basis*, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).

[25] I. D. Ivanovic, *Geometrical Description of Quantal State Determination*, J. Phys. A **14**, 3241 (1981).

[26] S. T. Flammia, A. Silberfarb, and C. M. Caves, *Minimal Informationally Complete Measurements*, Found. Phys. **35**, 1985 (2005).

[27] J. Romero, J. Leach, B. Jack, S. M. Barnett, M. J. Padgett, and S. Franke-Arnold, *Violation of Leggett Inequalities in Orbital Angular Momentum Subspaces*, New J. Phys. **12**, 123007 (2010).

[28] F. Cardano, E. Karimi, L. Marrucci, C. de Lisio, and E. Santamato, *Violation of Leggett-Type Inequalities in the Spin-Orbit Degrees of Freedom of a Single Photon*, Phys. Rev. A **88**, 032101 (2013).

[29] D. Petz and L. Ruppert, *Optimal Quantum-State Tomography with Known Parameters*, J. Phys. A **45**, 085306 (2012).

[30] B. Qi, Z. Hou, L. Li, D. Dong, G. Xiang, and G. Guo, *Quantum State Tomography via Linear Regression Estimation*, Sci. Rep. **3**, 03496 (2013).

[31] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, *Quantum State Estimation* (Springer, Berlin, 2004), pp. 113–145.

[32] M. S. Kaznady and D. F. V. James, *Numerical Strategies for Quantum Tomography: Alternatives to Full Optimization*, Phys. Rev. A **79**, 022109 (2009).

[33] E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, *Exact Solution to Simultaneous Intensity and Phase Encryption with a Single Phase-Only Hologram*, Opt. Lett. **38**, 3546 (2013).

[34] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, *Entanglement of the Orbital Angular Momentum States of Photons*, Nature (London) **412**, 313 (2001).

[35] E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd, *Exploring the Quantum Nature of the Radial Degree of Freedom of a Photon via Hong-Ou-Mandel Interference*, Phys. Rev. A **89**, 013829 (2014).

[36] H. Qassim, F. M. Miatto, J. P. Torres, M. J. Padgett, E. Karimi, and R. W. Boyd, *Limitations to the Determination of a Laguerre-Gauss Spectrum via Projective, Phase-Flattening Measurement*, J. Opt. Soc. Am. B **31**, A20 (2014).

[37] Fidelity is defined as $F = (\mathrm{Tr}\sqrt{\sqrt{\hat{\rho}}\hat{\rho}_r\sqrt{\hat{\rho}}})^2$, where ρ_r and ρ are the reconstructed and expected density matrices, respectively.

[38] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, *Maximum-Likelihood Estimation of the Density Matrix*, Phys. Rev. A **61**, 010304 (1999).

[39] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro, *Qudit Quantum-State Tomography*, Phys. Rev. A **66**, 012303 (2002).

[40] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, 1984* (IEEE, Bangalore, 1984), pp. 175–179.

[41] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[42] D. V. Sych, B. A. Grishanin, and V. N. Zadkov, *Analysis of Limiting Information Characteristics of Quantum-Cryptography Protocols*, Quantum Electron. **35**, 80 (2005).

[43] J. M. Renes, *Spherical-Code Key-Distribution Protocols for Qubits*, Phys. Rev. A **70**, 052314 (2004).

[44] B. G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, and J. Anders, *Efficient and Robust Quantum Key Distribution with Minimal State Tomography*, arXiv:quant-ph/0412075.