Experimental investigation of quantum key distribution protocols with twisted photons

Bouchard, Frédéric; Heshami, Khabat; England, Duncan; Fickler, Robert; Boyd, Robert W.; Englert, Berthold-Georg; Sánchez-Soto, Luis L.; Karimi, Ebrahim

Publisher's version / Version de l'éditeur:

Quantum Physics, 2018-02-15

Experimental investigation of quantum key distribution protocols with twisted photons

Frédéric Bouchard,[1,*] Khabat Heshami,[2] Duncan England,[2] Robert Fickler,[1] Robert W. Boyd,[1,3,4]
Berthold-Georg Englert,[5,6,7] Luis L. Sánchez-Soto,[3,8] and Ebrahim Karimi[1,3,9,†]

[1]*Physics Department, Centre for Research in Photonics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa ON Canada, K1N 6N5*
[2]*National Research Council of Canada, 100 Sussex Drive, Ottawa ON Canada, K1A 0R6*
[3]*Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany*
[4]*Institute of Optics, University of Rochester, Rochester, NY 14627, USA*
[5]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*
[6]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore.*
[7]*MajuLab, CNRS-UNS-NUS-NTU International Joint Unit, UMI 3654, Singapore.*
[8]*Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain*
[9]*Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.*

Quantum key distribution is on the verge of real world applications, where perfectly secure information can be distributed among multiple parties. Several quantum cryptographic protocols have been theoretically proposed and independently realized in different experimental conditions. Here, we develop an experimental platform based on high-dimensional orbital angular momentum states of single photons that enables implementation of multiple quantum key distribution protocols with a single experimental apparatus. Our versatile approach allows us to experimentally survey different classes of quantum key distribution techniques, such as the 1984 Bennett & Brassard (BB84), tomographic protocols including the six-state and the Singapore protocol, and a recently introduced differential phase shift (Chau15) protocol. This enables us to experimentally compare the performance of these techniques and discuss their benefits and deficiencies in terms of noise tolerance in different dimensions. Our analysis gives an overview of the available quantum key distribution protocols for photonic orbital angular momentum and highlights the benefits of the presented schemes for different implementations and channel conditions.

INTRODUCTION

Quantum cryptography allows for the broadcasting of information between multiple parties in a perfectly secure manner under the sole assumption that the laws of quantum physics are valid [1]. Quantum Key Distribution (QKD) [2, 3] is arguably the most well-known and studied quantum cryptographic protocol to date. Other examples are quantum money [4] and quantum secret sharing [5]. In QKD schemes, two parties, conventionally referred to as *Alice* and *Bob*, exchange carriers of quantum information, typically photons, in an untrusted quantum channel. An adversary, known as *Eve*, is granted full access to the quantum channel in order to eavesdrop on Alice and Bob's shared information. It is also assumed that Eve is only limited by the laws of physics and has access to all potential future technologies to her advantage, including optimal cloning machines [6], quantum memories [7], quantum non-demolition measurement apparatus [8], and full control over the shared photons. In particular, the presence of Eve is revealed to Alice and Bob in the form of noises in the channel. It is the goal of QKD to design protocols for which secure information may be transmitted even in the presence of noises [9]. For quantum channels with high-level of noises, it has been recognized that high-dimensional states of photons constitute a promising avenue for QKD schemes, due to their potential increase in noise tolerance with larger encrypting alphabet [10, 11]. However, this improvement comes at the cost of generating and detecting complex high-dimensional superpositions of states, which may be a difficult task [12].

Orbital angular momentum (OAM) states are associated with helical phase fronts for which a quantized angular momentum value of $\ell\hbar$ along the photons propagation direction can be ascribed, where ℓ is an integer and $\hbar$ is the reduced Planck constant [13]. Any arbitrary superposition of OAM states can be straightforwardly realized by imprinting the appropriate transverse phase and intensity profile on an optical beam, which is typically done by displaying a hologram onto a spatial light modulator (SLM) [14–16]. OAM-carrying photons, also known as twisted photons, have been recognized to constitute useful carriers of high-dimensional quantum states for quantum cryptography [17–19], quantum communication [20–23] and quantum information processing [24–28]. The flexibility in preparation and measurement of twisted-photon states enables us to create and use a single experimental setup for implementing several QKD protocols that offer different advantages, such as efficiency in secure bit rate per photon or noise tolerance for operation over noisy quantum channels. Here, we use OAM states of photons to perform and compare high-dimensional QKD protocols such as the 2-, 4- and 8-dimensional BB84 [2], tomographic protocols [29–31] using mutually unbiased bases (MUB) [32] and Symmetric Informationally Complete (SIC) Positive Operator-Valued Measures (POVMs) [33], and the 4- and 8-dimensional *Chau15* protocols. We finally demonstrate applications in full characterization of the quantum channel through quantum process tomography [34].

THEORETICAL BACKGROUND

Let us first start by briefly reviewing the BB84 protocol, which was introduced in 1984 by Bennett and Brassard [2]. In this protocol, Alice uses qubits to share a bit of information (0 or 1) with Bob, while using two different MUB [32]. This QKD protocol relies on the *uncertainty principle*, since a measurement by Eve in the wrong basis will not yield any useful information for herself. However, this also means that half of the time, Alice and Bob will perform their generation/detection in the wrong basis. This is known as sifting: Alice and Bob will publicly declare their choices of bases for every photon sent and only when their bases match will they keep their shared key. On average, Alice and Bob will only use half of their bits in their shared *sifted key*. In addition to sifting, Alice and Bob's shared key will be further reduced in size at the final stage of the protocol when performing error correction (EC) and privacy amplification (PA) [9]. In the case of BB84 in dimension 2, the number of bits of secret key established per sifted photon, defined here as the secret key rate R, is given by the following expression,

$$R = 1 - 2h(e_b), \tag{1}$$

where e_b is the quantum bit error rate (QBER) and $h(x) := -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon entropy. From this equation, we find that the secret key rate becomes negative for $e_b > 0.11$. Hence, if Alice and Bob only have access to a quantum channel with a QBER larger than 0.11 to perform the BB84 protocol, they will not be able to establish a secure key regardless of sifting and losses. Due to this limitation, it has been the goal of many research efforts to come up with QKD protocols that are more error tolerant. One of the first proposed QKD protocols that was aimed at extending the 0.11-QBER threshold, is the so-called *six-state* protocol [29]. The six-state protocol is an extension of the BB84 in dimension 2, where all three MUB are used. Indeed, it is known that in dimension 2, there exists precisely 3 MUB. In the general case of a d-dimensional state space, the number of MUB is $(d+1)$, given that d is a power of a prime number [32]. Moreover, it is known that there exist at least three MUB for any dimension [32] such that these 3 MUB can be used to increase error thresholds in dimensions which are not a power of a prime number [35]. Of course, this has the drawback of decreasing the efficiency of obtaining sifted data from $1/2$ to $1/3$. Nevertheless, by simply adding another basis to the encoding measurement scheme, the QBER threshold now increases to 0.126, as can be deduced from the secret key rate of the six-state protocol [29]

$$R = 1 - h\left(\frac{3}{2}e_b\right) - \frac{3}{2}e_b\log_2(3). \tag{2}$$

Another avenue to increase error tolerability in QKD is to use high-dimensional quantum states, also known as *qudits*. This may be intuitively understood from the fact that the presence of an optimal cloning attack leads to larger signal disturbance in higher-dimensional QKD schemes [11, 36]. The BB84 protocol may be extended here by using qudits. The adoption of high-dimensional quantum systems has two distinct benefits: (i) an increase of the error-free key rate per sifted photons to a value of $R = \log_2(d)$; (ii) an increase in the maximum tolerable QBER, i.e. the error threshold for $R = 0$. For the simple case of a d-dimensional BB84 protocol, the secret key rate is given by [37],

$$R = \log_2(d) - 2h^{(d)}(e_b), \tag{3}$$

where $h^{(d)}(x) := -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the d-dimensional Shannon entropy. Furthermore, it is also possible to extend the *six-state* protocol to higher dimensions by employing all $(d+1)$ MUB, assuming that d is a power of a prime number, where the secret key rate is given by,

$$R = \log_2(d) - h^{(d)}\left(\frac{d+1}{d}e_b\right) - \frac{d+1}{d}e_b\log_2(d+1). \tag{4}$$

This type of QKD scheme is also known as tomographic QKD [30, 31], where all measurements, including the sifted ones, are used to perform quantum state tomography (QST). In particular, MUB are closely related to the problem of quantum state tomography, where projections over all the states of every MUB, although redundant, yields a full reconstruction of the state's density matrix [38]. Following similar ideas, the *Singapore* protocol has been proposed using SIC-POVMs [31], as they are known to be the most efficient measurements to perform QST. The Singapore protocol may be equivalently performed in a prepare-and-measure or an entanglement-based scheme, similar to the analogy between BB84 and Ekert [39], respectively. Moreover, this QKD protocol may also be extended to higher dimensions [40] with the major advantage that the SIC-POVMs are believed to exist for all dimensions, including those that are not powers of prime numbers, contrary to MUB.

Another class of QKD protocols using qudits has recently been introduced, in which qudits are used to encode a single bit of information. Although, such protocols primarily benefits from one of the advantages mentioned earlier, i.e. an increase in the QBER threshold, they have proven to be interesting and advantageous due to a simplified generation and measurement of the states. Their main drawback is the fact that at a null QBER, the key rate per sifted photons is never larger than $R = 1$. An example of such a protocol is the *Differential Phase Shift* (DPS) QKD protocol [41]. The information is encoded by Alice in the relative phase of a superposition of all states then sent over the quantum channel. Bob may then measure the relative phase by detection of the different phases using an interferometric apparatus. In particular, the advantage of the 3-dimensional DPS scheme is in the higher sifting efficiency in comparison to BB84. An extension of the DPS protocol is the *Round-Robin Differential Phase Shift* (RRDPS) protocol [42] where Bob's interferometric apparatus is slightly modified. This modification results in a bound

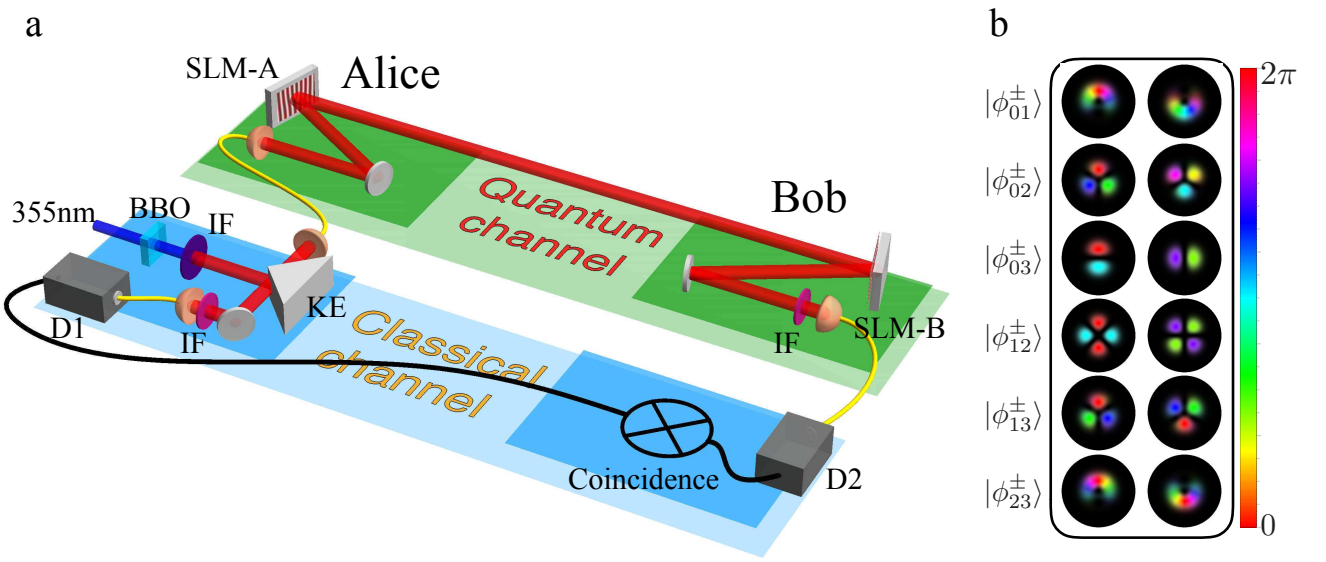

FIG. 1. (a) Simplified experimental setup. Alice generates pairs of single photons using spontaneous parametric downconversion in a type-I β-barium borate (BBO) crystal. The pump wavelength (355 nm) is filtered using an interference filter (IF) and the photons are separated using a knife edge (KE) in the far-field of the crystal. The spatial modes of the photon pairs are filtered using single mode optical fibres making the photons completely separable. Alice imprints a state onto her signal photon using a holographic technique by means of a spatial light modulator (SLM-A). The photon is then sent to Bob through the quantum channel. Bob measures the photon's state using a phase flattening technique with his SLM-B followed by a single mode optical fibre. Moreover, Alice locally measures the idler photon and sends timing information to Bob via an electric signal over the classical channel. Our experimental configuration allows us to test different protocols by changing the holograms displayed on the SLMs using the same experimental apparatus without intermediate adjustments. Thus, we are able to compare the different strategies in a systematic manner. (b) States employed in the Chau15 ($N = 4$) protocol. The phase (Hue colour) is shown modulated by the intensity profile of the beam.

.

on Eve's leaked information removing the need to monitor signal disturbance (QBER) for performing privacy amplification. Nevertheless, the qudits employed in the RRDPS QKD protocol consist of a superposition of d states, which may pose some practical limitations in experimental implementations as d becomes larger. The recently introduced *Chau15* protocol [43, 44] addresses this problem as it uses "qubit-like" superpositions where only two states of the d-dimensional space are employed. More specifically, the information is encoded in the relative phase of a qubit-like state of the form $|\varphi_{ij}^{\pm}\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$ with states in a 2^n-dimensional Hilbert space with $n \geq 2$. This protocol will be explained in more details in the discussion section.

EXPERIMENTAL SETUP

We implement a prepare-and-measure QKD scheme at the single-photon level using the OAM degree of freedom of photons, see Fig. 1 (a). The single photon pairs, namely *signal* and *idler*, are generated by spontaneous parametric downconversion (SPDC) at a type I β-barium borate (BBO) crystal. The nonlinear crystal is pumped by a quasi-continuous wave ultraviolet laser operating at a wavelength of 355 nm. The generated photon pairs are coupled to single-mode optical fibres (SMF) in order to filter their spatial modes to the fundamental mode; i.e., Gaussian. Following the SMF, a coincidence rate of 30 kHz is measured within a coincidence time window of 2 ns. The heralded signal photon is sent onto SLM-A corresponding to Alice's generation stage. The OAM states are produced using a phase-only holography technique [15]. Due to the versatility of SLMs, any OAM superposition states of single photons may be produced, hence covering a large possibility of QKD schemes. Alice's heralded photon is subsequently sent over the untrusted quantum channel. Upon reception of the photon, Bob uses his SLM-B followed by a SMF to perform a projection over the appropriate states for a given protocol. In order to do so, Bob uses the phase-flattening technique to measure OAM states of light [45, 46]. If the incoming photon carried the OAM mode corresponding to Bob's projection, the phase of the mode is flattened and the photon will couple to the SMF. This verification-type measurements can further reduce the sifting rate, unless the protocols requires only a binary measurement and "no-click" events are included.

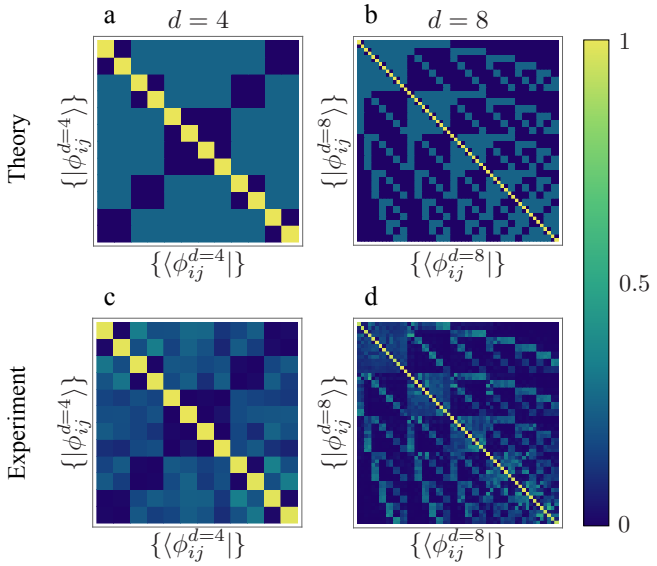

FIG. 2. Results for the Chau15 protocol. (a)-(b) Theoretical probability-of-detection matrices for the Chau15 protocol in dimension $d = 4$ and $d = 8$, respectively. Rows are given by states $|\varphi_{ij}^{\pm}\rangle \in \{|\varphi_{1,2}^{+}\rangle, |\varphi_{1,2}^{-}\rangle, |\varphi_{1,3}^{+}\rangle, ..., |\varphi_{3,4}^{-}\rangle\}$ sent by Alice, whereas columns corresponds to sate projections, $\langle\varphi_{ij}^{\pm}|$, by Bob. (c)-(d) Experimentally measured probability-of-detection matrices for the Chau15 protocol in dimension $d = 4$ and $d = 8$. The sifted data corresponds to the on-diagonal 2×2 blocks. The remaining of the probability-of-detection matrix may be used to evaluate the dit error rate.

RESULTS AND DISCUSSION

Chau15 protocol

At first, we perform the recently introduced Chau15 protocol, which is a qudit-based prepare-and-measure QKD scheme, where information is encoded in a qubit-like state of the form $|\varphi_{ij}^{\pm}\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$ with states in a 2^n-dimensional Hilbert space with $n \geq 2$; see [43, 44, 47]. The protocol starts with Alice randomly selecting i, j, and s, where $\{i,\ j\} \in \mathrm{GF}(d = 2^n)$, $\mathrm{GF}(d)$ being the Galois field, and $s = \pm 1$. Then, Alice prepares and sends the state $(|i\rangle + (-1)^s|j\rangle)/\sqrt{2}$ over an untrusted channel to Bob. Upon reception, Bob randomly selects i', $j' \neq i' \in \mathrm{GF}(d)$ and measures the state along $(|i'\rangle \pm |j'\rangle)/\sqrt{2}$. By announcing (i, j) and (i', j') through a classical channel, Alice and Bob can establish a raw bit sequence (key) from those events where $(i, j) = (i', j')$ and by keeping a record of s.

As discussed in [44], the performance of the scheme can be assessed through two sets of parameters. The first is the bit error rate of the sifted raw key (e_{raw}). The second is the average bit error rate and the average dit error rate associated with mismatch between preparation and measurement basis states. The average bit and dit error rates are estimated by averaging probabilities of the qudit states undergoing operations of $X_u Z_v$ in the insecure quantum channel, where $X_u|i\rangle = |i + u\rangle$, $Z_v|i\rangle = (-1)^{\mathrm{Tr}(vi)}|i\rangle$, and $\mathrm{Tr}(i) = i + i^2 + i^4 + ... + i^{d/2}$; see [44] for more details. These parameters can be extracted from the experimental joint probability measurements. Alice and Bob respectively prepare and measure $|\varphi_{ij}^{\pm}\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$, where $|i\rangle$ and $|j\rangle$ $(i \neq j)$ are pure OAM states in a Hilbert space of dimension $d = 4,\ 8$, see Fig. 1 (b). Using the OAM, Alice and Bob choose $i, j \in \{\ell = -2, -1, 1, 2\}$ for $d = 4$ and $i, j \in \{\ell = -4, -3, -2, -1, 1, 2, 3, 4\}$ for $d = 8$, where the $\ell = 0$ state has been omitted to make the states symmetric. In Fig. 2, we show theoretical and experimental probability-of-detection matrices obtained from a Chau15 QKD protocol for the cases of $d = 4$ and $d = 8$. After sifting, Alice and Bob are left with the on-diagonal 2×2 blocks of the presented probability-of-detection matrices.

In the case of $d = 4$, we obtained an average bit error rate of $e_b^{(d=4)} = 0.778$ %, and average dit error rate $e_d^{(d=4)} = 3.79$ %. This results in an asymptotic secure key rate of $R^{(d=4)} = 0.8170$ bit per sifted photon. For the case of $d = 8$, we obtained experimental values for the average bit error rate, average dit error rate and asymptotic secure key rate of $e_b^{(d=8)} = 3.11$ %, $e_d^{(d=8)} = 0.82$ % and $R^{(d=8)} = 0.8172$, respectively. Note that the probability of obtaining sifted data in the Chau15 protocol is given by $2/(d^2 - d)$ compared to the fixed sifting rate of 1/2 for the BB84 protocols in all dimensions. As we will see in the following sections, the Chau15 protocol does not perform well in the low-error case compared with other QKD protocols. Moreover, the unfavourable scaling of the sifting with dimensionality greatly affects the overall secure key rate (sifting included). Hence, the advantage of the Chau15 scheme is in the high-error case. In particular, given a small enough dit error rate, bit error rates of up to $e_b^{\max} = 50$ % may be tolerated. In the case of OAM states of light, this does not represent a clear advantage since bit and dit error rates will, in general, be the result of similar error sources, e.g. misalignment, turbulence or optical aberration. However, for other kinds of high-dimensional states of light, such as time-bins, the distinction between bit and dit error rates is less ambiguous and the Chau15 may then be used to its full potential.

BB84 protocol

The same experimental setup is now used to perform the BB84 (2 MUB) protocol in dimension $d = 2, 4$ and 8. In the BB84 protocols, the first basis is given by the logical pure OAM basis, i.e. $|\psi_i\rangle \in \{-d/2, ...d/2\}$ and the second basis is given by the Fourier basis where the states are obtained from the discrete Fourier transform, $|\varphi_i\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{ij} |\psi_i\rangle$, with $\omega_d = \exp(i2\pi/d)$. The explicit form of the other MUB may be found elsewhere [32]. Although this works only for prime dimensions, it can be easily extended to composite dimensions. For the BB84 protocol, values of the QBER of $e_b^{d=2} = 0.628$ %, $e_b^{d=4} = 3.51$ % and $e_b^{d=8} = 10.9$ % were obtained in dimension 2, 4 and 8, respectively corresponding

to secure key rates of $R^{d=2} = 0.8901$, $R^{d=4} = 1.4500$ and $R^{d=8} = 1.3942$. In the low-error case, the BB84 scheme performs very well. This is partly due to the fact that the sifting, i.e. 1/2, is independent of dimensionality. Interestingly, the BB84 protocol performs better in dimension 4 than it does in dimension 8. Hence, although in the error-free case, larger dimensions result in larger secure key rates, this is not necessarily the case in experimental implementations, due to more complex generations and detections of the high-dimensional OAM states. The nature of the quantum channel may also dictate the optimal dimensionality of the protocol [48].

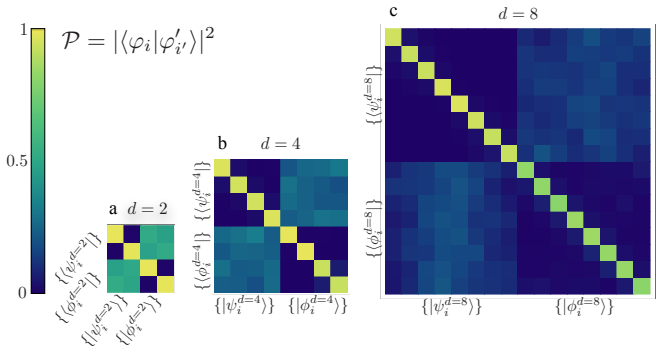

FIG. 3. BB84 protocol. (a)-(c) Experimentally measured probability-of-detection matrices for the BB84 protocol in dimension $d = 2, 4$ and 8, respectively. The rows and columns of the matrices correspond to the states sent and measured by Alice and Bob, respectively. The sifted data corresponds to the on-diagonal $d \times d$ blocks.

Tomographic protocols

MUB-based protocol

The six-state protocol in dimension $d = 2$ is an extension of the BB84 protocol where all existing MUB are considered. The protocol can be extended to higher dimensions (powers of prime numbers) where all $(d + 1)$ MUB are considered. In dimension 2 and 4, we obtained a QBER of $e_b^{d=2,m=3} = 0.923$ % and $e_b^{d=4,m=5} = 3.87$ % for the 3-MUB and the 5-MUB protocols, see Fig. 4 (a) and (c), corresponding to key rates of $R^{d=2,m=3} = 0.8727$ and $R^{d=4,m=5} = 1.5316$ bits per sifted photon. In comparison to the BB84 protocol, the $(d + 1)$-MUB protocol has a sifting efficiency of $1/(d + 1)$, which scales poorly with dimensions. Furthermore, this scheme only applies to dimensions that are powers of prime numbers. However, the $(d + 1)$-MUB approach consists of a tomographic protocol and in the case of large errors, it will outperform the BB84 scheme. In practical implementations, one could consider an intermediate scenario where the number of MUB considered is between 2 and $(d + 1)$ in order to optimize the secure key rate.

Singapore protocol

Finally, we perform another tomographic QKD protocol based on SIC-POVMs, known as the Singapore protocol. In particular, we use the Weyl-Heisenberg covariant SIC-POVMs elements. Reference vectors $|f\rangle$ have been conjectured to exist in arbitrary dimensions [33, 49] such that SIC-POVMs can be obtained by considering a displacement operator $\hat{D}_{jk}$ acting on the reference vector $|f\rangle$, where

$$\hat{D}_{jk} = \omega_d^{jk/2} \sum_{m=0}^{d-1} \omega_d^{jm} |k + m\rangle\langle m|, \tag{5}$$

and $\omega_d = e^{2\pi i/d}$. The fiducial vectors $|f\rangle$ have been derived numerically and analytically for different dimensions [33]. The fiducial vector is found such that $|\psi_{jk}\rangle = \{\hat{D}_{jk}|f\rangle,\ j, k = 0...d-1\}$ are normalized states satisfying $|\langle\psi_{jk}|\psi_{j'k'}\rangle|^2 = 1/(d+1)$ for $j \neq j'$ and $k \neq k'$. This set of d^2 states are then used by Alice and Bob in the prepare-and-measure Singapore protocol. Using the same experimental apparatus, we perform the Singapore protocol in dimension $d = 2$, where a QBER of $e_b = 1.23$ % was measured, see Fig. 4 (a).

Inspired by the Singapore protocol [31] an iterative key extraction method can be applied to extract a sifted secret key surpassing the 1/3 limit of the six-state protocol. The asymptotic efficiency of the iterative approach have been shown to reach 0.4 which is slightly smaller than the theoretical maximum of 0.415 under ideal conditions [31]. Here, we use the experimental joint probability matrix to find the experimental mutual information as an upper bound for the key extraction rate. For this purpose, we parametrize $|\psi_m^{A,B}(x)\rangle$ vectors (as Alice's and Bob's experimental preparation and measurement states). We then numerically minimize a maximum likelihood relation of the form $f(x) = \sum_{m,n=1}^{d^2} \left||\langle\psi_m^A(x)|\psi_n^B(x)\rangle|^2 - |\langle\psi_m|\psi_n\rangle|^2\right|^2$ to find deviations (errors) in the experimental SIC states of Alice and Bob. These deviations can also be interpreted as errors in the quantum channel.

The Singapore protocol relies on an anti-correlation between Alice an Bob. In the entanglement-based version of this protocol, this can be achieved by sharing a singlet entangled state. Assuming a singlet state of $|\Psi^{(-)}\rangle_{AB} = \frac{1}{\sqrt{d}}\sum_{m=0}^{m=d-1}(-1)^{d-m}|m\rangle|d-m-1\rangle$, we can extract the joint anti-correlated prepare-and-measure probabilities. In dimension $d = 2$, this takes the form of $p_{kl} = \mathrm{Tr}[\hat{\rho}_{AB}(1+\vec{t}_k\cdot\vec{\sigma}_A)(1+\vec{t}_l\cdot\vec{\sigma}_B)]$, where $\vec{t}_k$s are unit vectors denoting SIC states and $\hat{\sigma}_i$s are Pauli matrices. This typically deviates from the ideal case with prepare-and-measure probabilities of $p_{kl} = (1 - \delta_{kl})/12$. Keep in mind that the Singapore protocol relies on completely symmetric prepare-and-measure probabilities. This symmetrization can be achieved by twirling the calculated probability matrix leading to

$$p_{kl}^{\mathrm{exp}} = \frac{4-\varepsilon}{48}(1 - \delta_{kl}) + \frac{\varepsilon}{16}\delta_{kl}, \tag{6}$$

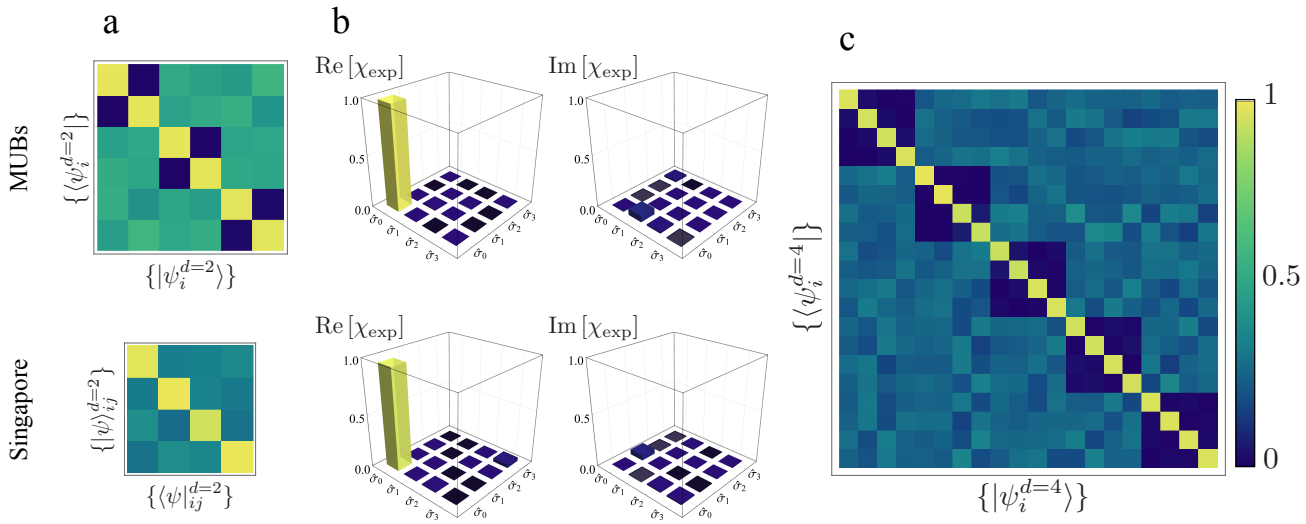

FIG. 4. Results for the $(d+1)$-MUB and Singapore protocols. (a) Experimentally measured probability-of-detection matrices for the $(d+1)$-MUB and Singapore protocols in dimension $d=2$. The rows and columns of the matrices correspond to the states sent and measured by Alice and Bob, respectively. For the case $(d+1)$-MUB protocols, the sifted data corresponds to the on-diagonal $d \times d$ blocks. (b) Reconstructed process matrix for the six-state (upper) and the Singapore (lower) protocols. (c) Experimentally measured probability-of-detection matrices for the $(d+1)$-MUB protocol in dimension $d=4$.

where $\varepsilon = 0.0137$. The mutual information between Alice and Bob is given by

$$I_{AB} = \sum_{k,l=1}^{d^2} p_{kl} \log_2 \left(\frac{p_{kl}}{p_k p_l} \right), \tag{7}$$

where $p_k = \sum_{l=1}^{d^2} p_{kl}$ and $p_l = \sum_{k=1}^{d^2} p_{kl}$. Our approach results in mutual information of $I_{AB}^{d=2} = 0.388$ compared to the theoretical maximum of 0.415; surpassing the maximum attainable rate in the six-state scheme. Moreover, protocols analogous to the Singapore protocol have a poor yield for higher-dimensional systems. The mutual information for qubit, qutrit and ququart pairs are respectively given by 0.415, 0.170 and 0.093 bits.

Quantum process tomography of the QKD channel

In this subsection we considered the two QKD protocols that offer full tomography capabilities [34, 50]. Quantum state preparation and measurements in all possible MUB states provide an overcomplete set of results that can be used to perform quantum process tomography on the channel. In the Singapore protocol, the SIC POVMs are optimal set of preparation and measurements for process tomography of the channel. Both of these protocols allow one to go beyond a coarse-grained qubit error rate estimation and fully characterize the quantum channel. We use the experimental results for the six-state and Singapore protocols to characterize the quantum channel.

The channel can be characterized as positive trace-preserving map $\mathcal{E}$ such that $\hat{\rho}_{\text{out}} = \mathcal{E}(\hat{\rho}_{\text{in}})$. This can then be described by the $d^2 \times d^2$ process matrix, χ, where $\mathcal{E}(\hat{\rho}) = \sum_{ij} \chi_{ij} \hat{\sigma}_i \hat{\rho} \hat{\sigma}_j^\dagger$. In $d=2$, $\hat{\sigma}_i$s are identity and Pauli matrices. This approach can be extended to higher dimensions using Gell-Mann matrices as they also offer an orthogonal basis, $\text{Tr}(\hat{\sigma}_i \hat{\sigma}_j) = 2\delta_{ij}$, spanning the vector space of complex matrices. Given the experimental preparation and measurement results, we parametrize the process matrix and minimize a maximum likelihood function of

$$f(\vec{t}) = \sum_{a,b} \frac{[N_{ab}/N - \langle\psi_b|(\sum_{i,j} \chi_{ij}(\vec{t}) \hat{\sigma}_i |\psi_a\rangle\langle\psi_a|\hat{\sigma}_j)|\psi_b\rangle]^2}{2\langle\psi_b|(\sum_{i,j} \chi_{ij}(\vec{t}) \hat{\sigma}_i |\psi_a\rangle\langle\psi_a|\hat{\sigma}_j)|\psi_b\rangle}, \tag{8}$$

to find the process matrix. Here N_{ab}/N are normalized prepare-and-measure results, and $|\psi_a\rangle$ ($|\psi_b\rangle$) are prepared states (measurement projection settings). Using numerical minimization, we find the process matrix for both the six-state and Singapore protocols that are depicted in Fig. 4b. This capability in tomographic protocols can potentially be used to identify attacks, and pre- or post-compensate for non-dynamical errors in the channel.

CONCLUSION

Application of quantum physics in public key cryptography first emerged in the seminal work of Bennet and Brassard in 1984; leading to several other protocols that benefit from different properties of quantum states for secure quantum communications. Many experimental efforts have been

Protocol	d	$e_b^{\max}$	$e_b^{\exp}$	$R(0)$	$R^{\exp}$	Sifting	$R^{\exp}\times$ Sifting
Chau15	4	50 %	0.778 %	1	0.8170	1/6	0.1362
	8	50 %	3.11 %	1	0.8172	1/28	0.0292
BB84	2	11.00 %	0.628 %	1	0.8901	1/2	0.4451
	4	18.93 %	3.51 %	2	1.4500	1/2	0.7250
	8	24.70 %	10.9 %	3	1.3942	1/2	0.6971
MUB	2	12.62 %	0.923 %	1	0.8727	1/3	0.2909
	4	23.17 %	3.87 %	2	1.5316	1/5	0.3063
Singapore	2	38.93 %	1.23 %	0.4	0.374*	1	0.374*

TABLE I. Quantum bit error rates and key rates are presented for various quantum key distribution protocols. Four protocols, in various dimensions d, were investigated. The theoretical values of the error-free secret key rate, i.e. $R(0)$, and the maximum QBER, i.e. $e_b^{\max}$ for which $R = 0$, are presented for the different protocols alongside the experimentally measured QBER, $e_b^{\exp}$, and secret key rates, $R^{\exp}$. Finally, the sifting rate, defined as the probability of obtaining sifted data, is also shown for each protocols. *Experimental rate for the Singapore protocol is deduced based on the point that a rate of 0.4 per 0.415 value of mutual information can be achieved.

dedicated to physical implementation of these protocols using mostly polarization and temporal degrees of freedom of photons. Despite significant progress in experimental realization of QKD protocols, each demonstration is practically limited to implement a single protocol in a specific dimension. Structured light, on the other hand, have been shown to offer flexibility in quantum state preparation and measurement in a theoretically unbounded Hilbert space. Here, we employed the versatility offered by the OAM states of photons to perform an experimental survey of four classes of QKD protocols in different dimensions. Table I summarizes the main results of the several QKD schemes. This included the Chau15 scheme (in $d = 4$, and 8) based on differential phases, the BB84 protocol in dimensions 2, 4, and 8, and tomographic protocols based on $(d + 1)$-MUB in $d = 2$ (six-state), and 4, and SIC-POVMs in $d = 2$. We observed experimental secure bit rates that ranges from 0.03 to 0.72 bit per sifted photon with schemes that have error tolerances from 11 % up to 50 %. Our experimental setup allows one to easily switch between protocols and dimensions to benefit from advantages of different protocols under varying channel conditions. This included using tomographic protocols for a more elaborate characterization of the errors in the quantum channel.

* fbouc052@uottawa.ca
† ekarimi@uottawa.ca

[1] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
[2] Bennett, C. H. & Brassard, G. Proceedings of the ieee international conference on computers, systems, and signal processing, bangalore, india, 1984 (1984).
[3] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
[4] Wiesner, S. Conjugate coding. *ACM Sigact News* **15**, 78–88 (1983).
[5] Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
[6] Scarani, V., Iblisdir, S., Gisin, N. & Acin, A. Quantum cloning. *Rev. Mod. Phys.* **77**, 1225 (2005).
[7] Simon, C. *et al.* Quantum memories. *Eur. Phys. J. D* **58**, 1–22 (2010).
[8] Werner, M. & Milburn, G. Eavesdropping using quantum-nondemolition measurements. *Phys. Rev. A* **47**, 639 (1993).
[9] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE T. Inform. Theory* **41**, 1915–1923 (1995).
[10] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
[11] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
[12] Krenn, M. *et al.* Generation and confirmation of a (100× 100)-dimensional entangled quantum system. *PNAS* **111**, 6243–6247 (2014).
[13] Allen, L., Beijersbergen, M. W., Spreeuw, R. & Woerdman, J. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Phys. Rev. A* **45**, 8185 (1992).
[14] Heckenberg, N., McDuff, R., Smith, C. & White, A. Generation of optical phase singularities by computer-generated holograms. *Opt. Lett.* **17**, 221–223 (1992).
[15] Bolduc, E., Bent, N., Santamato, E., Karimi, E. & Boyd, R. W. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Opt. Lett.* **38**, 3546–3549 (2013).
[16] Forbes, A., Dudley, A. & McLaren, M. Creation and detection of optical modes with spatial light modulators. *Advances in Optics and Photonics* **8**, 200–227 (2016).
[17] Gröblacher, S., Jennewein, T., Vaziri, A., Weihs, G. & Zeilinger, A. Experimental quantum cryptography with qutrits. *New J. Phys.* **8**, 75 (2006).
[18] Mafu, M. *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).
[19] Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
[20] D'ambrosio, V. *et al.* Complete experimental toolbox for alignment-free quantum communication. *Nat. Commun.* **3**, 961 (2012).
[21] Vallone, G. *et al.* Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.* **113**, 060503 (2014).

[22] Krenn, M., Handsteiner, J., Fink, M., Fickler, R. & Zeilinger, A. Twisted photon entanglement through turbulent air across vienna. *PNAS* **112**, 14197–14201 (2015).

[23] Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).

[24] Cardano, F. *et al.* Quantum walks and wavepacket dynamics on a lattice with twisted photons. *Science Adv.* **1**, e1500087 (2015).

[25] Cardano, F. *et al.* Statistical moments of quantum-walk dynamics reveal topological quantum transitions. *Nat. Commun.* **7**, 11439 (2016).

[26] Cardano, F. *et al.* Detection of zak phases and topological invariants in a chiral quantum walk of twisted photons. *Nature Commun.* **8**, 15516 (2017).

[27] Babazadeh, A. *et al.* High-dimensional single-photon quantum gates: concepts and experiments. *Phys. Rev. Lett.* **119**, 180510 (2017).

[28] Erhard, M., Fickler, R., Krenn, M. & Zeilinger, A. Twisted photons: New quantum perspectives in high dimensions. *Light Sci. Appl.* (2018).

[29] Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998).

[30] Liang, Y. C., Kaszlikowski, D., Englert, B.-G., Kwek, L. C. & Oh, C. H. Tomographic quantum cryptography. *Phys. Rev. A* **68**, 022324 (2003).

[31] Englert, B.-G. *et al.* Efficient and robust quantum key distribution with minimal state tomography. *arXiv preprint quant-ph/0412075* (2004).

[32] Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535–640 (2010).

[33] Renes, J. M., Blume-Kohout, R., Scott, A. J. & Caves, C. M. Symmetric informationally complete quantum measurements. *J. Math. Phys.* **45**, 2171–2180 (2004).

[34] Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455–2467 (1997).

[35] Brádler, K., Mirhosseini, M., Fickler, R., Broadbent, A. & Boyd, R. Finite-key security analysis for multilevel quantum key distribution. *New Journal of Physics* **18**, 073030 (2016).

[36] Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E. High-dimensional quantum cloning and applications to quantum hacking. *Science Adv.* **3**, e1601915 (2017).

[37] Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 030301 (2010).

[38] D'ambrosio, V. *et al.* Test of mutually unbiased bases for six-dimensional photonic quantum systems. *Sci. Rep.* **3**, 2726 (2013).

[39] Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).

[40] Bent, N. *et al.* Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures. *Phys. Rev. X* **5**, 041006 (2015).

[41] Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89**, 037902 (2002).

[42] Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475 (2014).

[43] Chau, H. Quantum key distribution using qudits that each encode one bit of raw key. *Phys. Rev. A* **92**, 062324 (2015).

[44] Chau, H., Wang, Q. & Wong, C. Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit-and qudit-based protocols. *Phys. Rev. A* **95**, 022311 (2017).

[45] Mair, A., Vaziri, A., Weihs, G. & Zeilinger, A. Entanglement of the orbital angular momentum states of photons. *Nature* **412**, 313–316 (2001).

[46] Qassim, H. *et al.* Limitations to the determination of a laguerre–gauss spectrum via projective, phase-flattening measurement. *J. Opt. Soc. Am. B* **31**, A20–A23 (2014).

[47] Wang, S. *et al.* Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme. *arXiv preprint arXiv:1707.00387* (2017).

[48] Bouchard, F. *et al.* Underwater quantum key distribution in outdoor conditions with twisted photons (2018). arXiv preprint arXiv:1801.10299.

[49] Scott, A. J. & Grassl, M. Symmetric informationally complete positive-operator-valued measures: A new computer study. *J. Math. Phys.* **51**, 042203 (2010).

[50] Ndagano, B. *et al.* Characterizing quantum channels with non-separable states of classical light. *Nat. Phys.* **13**, 397 (2017).

Acknowledgments All authors would like to thank Gerd Leuchs, Markus Grassl and Imran Khan for helpful discussions. F.B. acknowledges the financial support of the Vanier graduate scholarship of the NSERC. R.F. acknowledges the financial support of the Banting postdoctoral fellowship of the NSERC. This work was supported by Canada Research Chairs; Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF); Natural Sciences and Engineering Research Council of Canada (NSERC); Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and the National Research Foundation of Singapore; and Spanish Ministerio de Economia y Competitividad (MINECO).

Author Information Correspondence and requests for materials should be addressed to ekarimi@uottawa.ca.

Competing interests The authors declare no competing financial interests.