optica

High-dimensional intracity quantum cryptography with structured photons

ALICIA SIT,[1] FRÉDÉRIC BOUCHARD,[1] ROBERT FICKLER,[1] JÉRÉMIE GAGNON-BISCHOFF,[1] HUGO LAROCQUE,[1] KHABAT HESHAMI,[2] DOMINIQUE ELSER,[3,4] CHRISTIAN PEUNTINGER,[3,4] KEVIN GÜNTHNER,[3,4] BETTINA HEIM,[3,4] CHRISTOPH MARQUARDT,[3,4] GERD LEUCHS,[1,3,4] ROBERT W. BOYD,[1,5] AND EBRAHIM KARIMI[1,6,*]

[1]Physics Department, Centre for Research in Photonics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa, Ontario K1N 6N5, Canada
[2]National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada
[3]Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany
[4]Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany
[5]Institute of Optics, University of Rochester, Rochester, New York 14627, USA
[6]Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran
*Corresponding author: ekarimi@uottawa.ca

Received 5 June 2017; revised 20 July 2017; accepted 25 July 2017 (Doc. ID 297325); published 24 August 2017

Quantum key distribution (QKD) promises information-theoretically secure communication and is already on the verge of commercialization. The next step will be to implement high-dimensional protocols in order to improve noise resistance and increase the data rate. Hitherto, no experimental verification of high-dimensional QKD in the single-photon regime has been conducted outside of the laboratory. Here, we report the realization of such a single-photon QKD system in a turbulent free-space link of 0.3 km over the city of Ottawa, taking advantage of both the spin and orbital angular momentum photonic degrees of freedom. This combination of optical angular momenta allows us to create a 4-dimensional quantum state; wherein, using a high-dimensional BB84 protocol, a quantum bit error rate of 11% was attained with a corresponding secret key rate of 0.65 bits per sifted photon. In comparison, an error rate of 5% with a secret key rate of 0.43 bits per sifted photon is achieved for the case of 2-dimensional structured photons. We thus demonstrate that, even through moderate turbulence without active wavefront correction, high-dimensional photon states are advantageous for securely transmitting more information. This opens the way for intracity high-dimensional quantum communications under realistic conditions.

OCIS codes: (270.5568) Quantum cryptography; (060.2605) Free-space optical communication; (050.4865) Optical vortices.

https://doi.org/10.1364/OPTICA.4.001006

1. INTRODUCTION

Secure quantum communication, i.e., quantum key distribution (QKD), is on the forefront of the commercialization of future quantum technologies. Since its first theoretical proposal [1], it has been one of the major driving forces to investigate and apply quantum features for future information processing schemes [2,3]. While this process of developing commercial quantum cryptography devices has already started, possible next-generation QKD schemes, such as high-dimensional encoding, have come under scrutiny in quantum information research. Although different proof-of-principle experiments have shown the superiority of such schemes in terms of noise resistance and data capacity [4–8], their applicability still has to be demonstrated under real-world conditions. Here, another key question that needs to be addressed is the most suited photonic degree of freedom that allows encoding of high-dimensional quantum states.

In addition to polarization and wavelength, a light wave may carry orbital angular momentum (OAM) [9], corresponding to helical wavefronts. Polarization is naturally bidimensional, i.e., $\{|L\rangle, |R\rangle\}$, and the associated angular momentum can take the values of $\pm\hbar$ per photon, where $\hbar$ is the reduced Planck constant, and $|L\rangle$ and $|R\rangle$ are left- and right-handed circular polarizations, respectively. In contrast, OAM is inherently unbounded, such that a photon with ℓ intertwined helical wavefronts, $|\ell\rangle$, carries $\ell\hbar$ units of OAM, where ℓ is an integer [10]. Quantum states of light resulting from an arbitrary coherent superposition of different polarizations and spatial modes, e.g., OAM, are referred to as *structured photons*; these photons can be used to realize higher-dimensional states of light [11]. Aside from their fundamental significance in quantum physics [12,13], single photons encoded in higher dimensions provide an advantage in terms of security tolerance and encrypting alphabets for quantum cryptography [4,5,8] and classical communications [14]. The behavior of light-carrying OAM through turbulent conditions has been studied theoretically and simulated in the laboratory scale [15–18]. Experimentally, OAM states have been tested in classical communications across intracity links in Los Angeles (120 m) [19], Venice (420 m) [20], Erlangen (1.6 km) [21], Vienna (3 km) [22], and between two Canary Islands (143 km) [23], which is the longest link thus far. With attenuated lasers, OAM states and vector vortex beams have been respectively implemented in high-dimensional and 2-dimensional BB84 protocols, where the former was performed in a laboratory [8] and the latter in a hall in Padua (210 m) [24]. Though not QKD, the entanglement distribution of bidimensional twisted photons has been recently studied across the Vienna link [25]. Note that no true single-photon high-dimensional QKD experiment has been performed outside of the laboratory thus far.

In this paper, we combine polarization $\{|H\rangle, |V\rangle\}$ and an OAM subspace of $\{|\ell\rangle, |-\ell\rangle\}$ to form 4-dimensional quantum states $|k\rangle$, for $k = 1, 2, 3, 4$, belonging to the set $\{|H,\ell\rangle, |V,\ell\rangle, |H,-\ell\rangle, |V,-\ell\rangle\}$, where $|H\rangle = (|L\rangle + |R\rangle)/\sqrt{2}$ and $|V\rangle = -i(|L\rangle - |R\rangle)/\sqrt{2}$ are horizontal and vertical polarization states, respectively. We can create two sets of mutually unbiased bases (MUBs) from $|k\rangle$, defined as $|\psi\rangle^i = \mathcal{M}_0^{ik}|k\rangle$ and $|\varphi\rangle^j = \mathcal{M}_1^{jk}|k\rangle$, where $|{}^i\langle\psi|\psi\rangle^j|^2 = |{}^i\langle\varphi|\varphi\rangle^j|^2 = \delta_{ij}$, and $|{}^i\langle\psi|\varphi\rangle^j|^2 = 1/4$ for $i, j = 1, 2, 3, 4$ (see Supplement 1 for $\mathcal{M}_0$ and $\mathcal{M}_1$). Figure 1 illustrates the spatial structure of these MUBs for the case of $\ell = 2$. The information encoded within these modes lies in the transverse polarization and phase distributions; however, all of these modes possess a “doughnut”-shaped intensity distribution. The polarization distributions contain only linearly polarized states, and such beams are commonly called vector vortex beams [26]; in the case of $\{|\varphi\rangle^j\}$, the linear polarizations vary across the transverse plane. $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ are conjugate quantities, and based on quantum complementarity they cannot be measured simultaneously; this forms the backbone of security in quantum cryptography. Specifically, in the BB84 protocol [1], the bases of preparation and measurement are randomly chosen between two MUBs by a sender and receiver, traditionally called Alice and Bob, respectively. We used the two MUBs of structured modes, $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$, to perform a high-dimensional BB84 protocol [4,5].

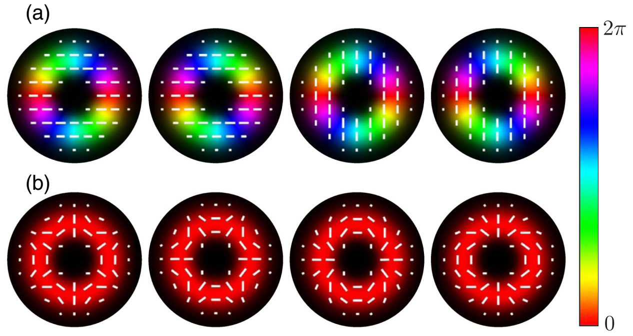

Fig. 1. Mode structure of mutually unbiased bases for $\ell = 2$. (a) $\{|\psi\rangle^i\}$ and (b) $\{|\varphi\rangle^j\}$ are examples of two bases of structured states of light, encoding in both polarization and OAM of $\ell = 2$. Each basis is orthonormal, and the two bases are mutually unbiased with respect to each other such that $|{}^i\langle\psi|\varphi\rangle^j|^2 = 1/4$. These MUBs have the advantage of possessing identical intensity profiles—“doughnut” shaped—and are shape-invariant upon free-space propagation. The information, therefore, is encoded in the transverse polarization and phase distributions, denoted by the white lines and the hue, respectively.

There are different approaches used to generate and sort these structured modes of light. We utilize liquid crystal devices known as q-plates [27], which coherently couple optical spin angular momentum to OAM. Q-plates are advantageous as they are placed in-line, are efficient in comparison to diffractive elements, and can be used to create arbitrary complex modal structures [28]. These q-plates used in conjunction with a carefully chosen sequence of wave plates can generate $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ (see Supplement 1 for details). Furthermore, it is possible to rapidly switch between the states in $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$, of the order of 1 MHz, by replacing the wave plates with Pockels cells. Since q-plates are coherent and linear devices, they also work in the single-photon regime [29].

2. EXPERIMENT

We built a free-space link between the rooftops of two buildings, 0.3 km apart and 40 m above the ground, on the University of Ottawa campus; see Fig. 2. Two enclosures were constructed to contain and protect all of the optics and equipment at the sender and receiver. The sender unit is comprised of both the heralded single-photon source and the setup where Alice can prepare states. The receiver unit contains Bob’s state measurement setup and the single-photon detection system. No active adaptive optics or vibration isolation systems were implemented.

In the heralded single-photon source, photon pairs are generated via the spontaneous parametric downconversion process in a 5 mm long ppKTP crystal pumped by a 405 nm laser diode (200 mW). Nondegenerate wavelengths for the signal ($\lambda_s = 850$ nm) and idler ($\lambda_i = 775$ nm) photons are chosen in order to efficiently separate the two; only the signal photon is encoded with information. The signal and idler are each coupled into a separate single-mode fiber (SMF) to spatially filter the photons into the fundamental mode. Bandpass filters, 850 ± 5 nm and 775 ± 20 nm, are placed in front of the fiber couplers to select the correct photon pairs. The singles count rates at the source after the SMFs, detected with avalanche photodiodes (APDs), are 4 MHz and 10 MHz for the signal and idler, respectively. The idler photon heralds the presence of the signal photon, as determined by a coincidence logic box. This procedure gives a coincidence rate of around 1 MHz for a coincidence window of 5 ns with $\lesssim 0.2$ MHz of accidental coincidence detections.

Alice takes the signal photon and prepares it in one of the states of the different MUBs through the use of an appropriate sequence of wave plates and q-plates. She then recombines the signal and idler photons on a dichroic mirror and enlarges the spatial structure of both beams such that they can be sent in the same beam across the link to Bob and to minimize divergence upon propagation, respectively. At the last lens (f_2) of the sending unit, the beam waist is approximately 12 mm. After propagation over the 0.3 km distance, we find the beam waist to be enlarged to approximately 20 mm as a consequence of atmospheric influences and imperfect optics. In order to measure the received quantum states, Bob demagnifies the photon’s structure with another set of lenses and separates the information-carrying signal photon from the heralding idler photon with another dichroic mirror. The idler photon is directly coupled into a SMF to act as a herald for the signal photon. With a sequence of wave plates, q-plates, PBSs, and SMFs, mirrored to that of Alice’s, Bob can make a measurement on the signal photon by projecting it onto one of the states from one of the MUBs. In such a way, Bob has a spatial

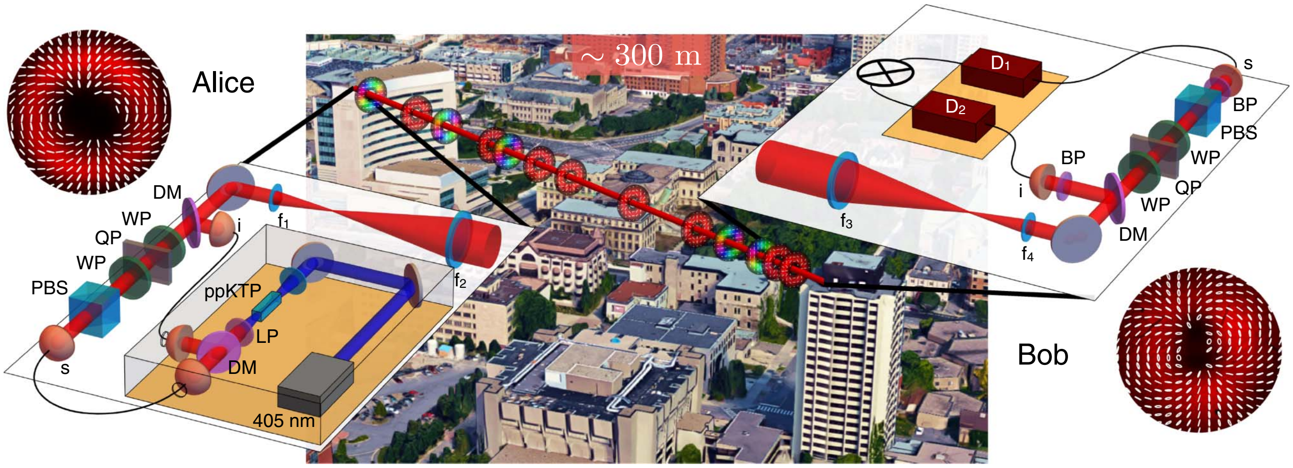

Fig. 2. Ottawa intracity quantum communication link. Schematic of the sender (left) with a heralded single-photon source (signal, *s*, and idler, *i*) and Alice's state preparation setup. Alice prepares a state from $\{|\psi\rangle^i\}$ or $\{|\varphi\rangle^j\}$ using a polarizing beam splitter (PBS), wave plates (WP), and a *q*-plate (QP). The signal and idler photons are recombined on a dichroic mirror (DM) before being sent to Bob. Two telescopes comprised of lenses with focal lengths of $f_1 = 75$ mm, $f_2 = f_3 = 400$ mm (diameter of 75 mm), and $f_4 = 50$ mm are used to enlarge and collect the beam, minimizing its divergence through the 0.3 km link. Bob, receiver (right), can then perform measurements on the sent states and record the coincidences between the signal and idler photons with detectors D_1 and D_2 at a coincidence logic box. Enclosures are built around the sender and receiver to shelter them from the wind and weather, as well as to shield them from background light. Examples of experimentally reconstructed polarization distributions for a structured mode from $\{|\varphi\rangle^j\}$ using a continuous wave laser that Alice prepared (top left) and Bob measured (bottom right) are shown in the insets. ppKTP, periodically poled KTP crystal; LP, long-pass filter; BP, bandpass filter. Map data: Google Maps, 2016.

mode filter such that, if he projects onto the same state that Alice sent, the signal photon will be phase-flattened and optimally detected. By using APDs and a coincidence logic box (5 ns coincidence window), the received idler photon acts as a trigger for the arrival of the signal photon and the coincidence rates are recorded. The best performance of our free-space link after coupling to the SMFs on Bob's side gave count rates for the signal and idler photons of 0.75 MHz and 2.5 MHz, respectively, with an optimal coincidence rate of approximately 50 kHz. However, due to large temperature and turbulence differences from night to night, the numbers varied throughout the various experimental runs. Overall, from sender to receiver, there are approximately 20% and 25% coupling efficiencies (equivalently 7 dB and 6 dB of losses) for the signal and idler photons, respectively, which gives an approximately 5% success rate for recording coincidences.

Since no adaptive optics were utilized, a portion of the raw data points sampled are greatly perturbed by the turbulence. The most dominant effect of the atmospheric turbulence given the range of our measured atmospheric structure constant, C_n^2, between 2.5×10^{-15} m$^{-2/3}$ and 6.4×10^{-16} m$^{-2/3}$ (see Section 3) is beam wandering [30]. Under stable conditions, the idler photon remains in the fundamental mode and always couples to the SMF; however, when there is turbulence, it does not optimally couple. Since the signal photon is coaxially propagating with the idler photon, it experiences the same atmospheric turbulence; we can thus use the idler photon as not only a herald for the signal photon but also as a "target" to gauge the beam wandering in Bob's setup. This helps to correct our measurements for turbulence in postprocessing. During a BB84 protocol, Alice is preparing each signal photon into a state from a randomly chosen MUB and then sends it with its heralding idler photon to Bob. Once each pair reaches Bob, turbulence may have caused them to wander from the optical axis. Each measurement consists of coincidence counts acquired for 200 ms, repeated 50 times, and then averaged. If there is excessive turbulence, the accumulated idler counts will have dropped. Therefore, Bob only keeps the coincidence measurements whose corresponding idler counts are near the optimal value, i.e., when there is little to no turbulence. Otherwise, he discards his measurement. As a target beam, the idler photon helps to sift out turbulence-affected pairs, decreasing the quantum bit error rate and thereby increasing the amount of securely transmitted information per sifted photon.

It is important to note that despite sending two photons across the link simultaneously, our scheme is still immune to photon-number-splitting attacks since the idler photon *does not* contain any of the polarization or OAM information of the signal photon. Apart from being able to monitor the turbulence, the only other information that the idler photon contains is timing information for heralding purposes, which could alternatively be communicated over a classical channel. Therefore, even if an eavesdropper had full access to the idler photon, she would not be able to access the signal information. A full security proof would be able to take into account the signal and idler photons, including bounds on possible side information of this particular setup. However, this is beyond the scope of this work and will be further investigated in the future.

3. TURBULENCE CHARACTERIZATION

To characterize the Ottawa intracity free-space link, we investigate the turbulence by evaluating its characteristic properties, such as the atmospheric structure constant C_n^2 and the Fried parameter r_0 [30–32]. We do so by sending a Gaussian-shaped laser beam (850 nm) over the 0.3 km long link and record its arrival position with a CCD camera. Because atmospheric turbulence changes on a millisecond time scale, short-term exposure images can reveal beam wandering, which is caused by fast-moving air cells, each having slightly different pressures, and thus small differences in

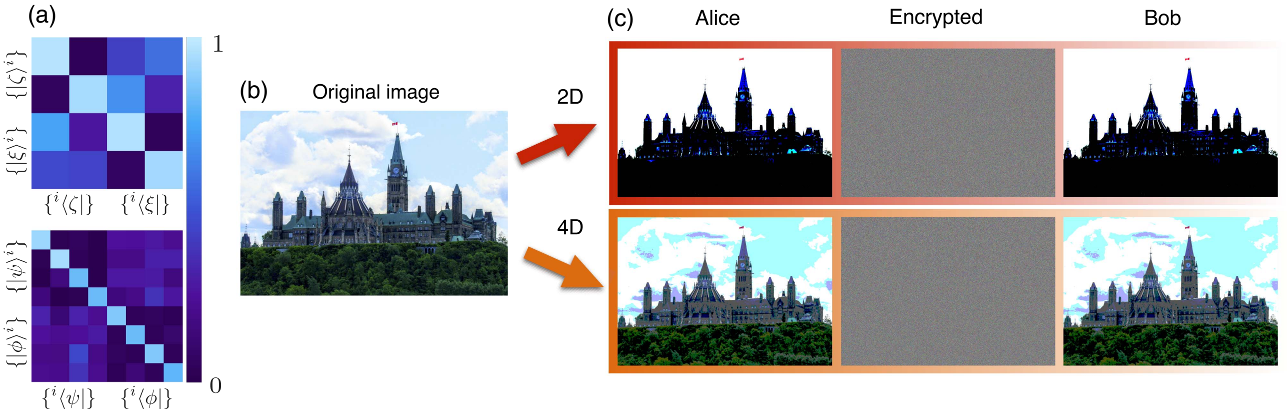

Fig. 3. Simulated encryption of an image with structured photons. (a) Experimentally measured probability-of-detection matrices, $P^{i,j} = |^i\langle\alpha|\beta\rangle^j|^2$, where $\alpha, \beta = \{\psi, \varphi\}$, for 2D (top row) and 4D (bottom row) structured photons with turbulence. These matrices have the corresponding bit error rates of $Q^{2\text{D}} = 5\%$ and $Q^{4\text{D}} = 11\%$, respectively. (b) Image of the Parliament of Canada that Alice encrypts and sends to Bob through a classical channel using their shared secret key. (c) Alice discretizes her intended image (left column) with d levels, where d is the encryption dimension, such that each pixel corresponds to three single photons (RGB values, leading to d^3 colors per pixel) that she sends to Bob. Using the experimentally measured probability-of-detection matrices (a), Alice then adds the shared secret key, generated from a BB84 protocol, on top of her discretized image to encrypt it (middle column). Bob decrypts Alice's sent image with his shared key to recover the image (right column). Implementing a 4-dimensional state clearly allows the ability to send more information per photon, where, in the ideal case, Alice can send twice the amount of information with respect to 2-dimensional states. However, due to noise present in the channel, we experimentally obtain an increase of 1.51 in the amount of information sent by Alice with respect to the case of 2-dimensional states. Image credit: Norman Bouchard.

refractive indices. The stronger the turbulence and the larger the distance of the link, the larger are the deflections from the optical axis. The latter can be deduced by taking an average over many short-term exposure images, which effectively leads to an atmospherically broadened Gaussian beam profile. During different measurement nights, we record 500 short exposure images (0.07 ms each), from which we calculate a Fried parameter between 18 cm and 41 cm, which corresponds to an atmospheric structure constant C_n^2 ranging from around 2.5×10^{-15} m$^{-2/3}$ to 6.4×10^{-16} m$^{-2/3}$, assuming Kolmogorov theory for atmospheric turbulence. Hence, the link shows moderate turbulence effects on the transmitted light fields.

4. RESULTS AND DISCUSSION

In QKD, a secret key may be established between Alice and Bob with a secret key rate, defined as the number of bits of secret key established divided by the number of sifted photons, given by $R(Q) = \log_2(d) - 2h(Q)$, where Q is the quantum bit error rate and $h(\cdot)$ is the Shannon entropy in dimension d. Hence, there is a threshold value of Q_0 above which a nonzero shared secure key cannot be generated. In dimension 2, this threshold value is the well-known $Q_0^{2\text{D}} = 11.0\%$, while it almost doubles to $Q_0^{4\text{D}} = 18.9\%$, in dimension 4 [5]. This clearly exhibits the robustness of high-dimensional quantum cryptography.

We perform a 4-dimensional BB84 protocol under different atmospheric conditions. Probability-of-detection matrices for the 4-dimensional structured photonic states, $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ with $\ell = 2$, of the BB84 protocol are shown in Fig. 3(a) (bottom row). In dimension 4, from the *raw* probability-of-detection matrix, the quantum bit error rate is $Q = 14\%$, and is below the threshold value of $Q_0^{4\text{D}}$, resulting in a positive corresponding secret key rate of $R = 0.39$ bits per sifted photon. Thus, without any corrections, a securely transmitted high-dimensional key can be established. By considering the idler as a target beam, which accounts for turbulence, the quantum bit error rate is reduced to $Q^{4\text{D}} = 11\%$ with a secret key rate of $R^{4\text{D}} = 0.65$ bits per sifted photon. The secret key rate is lower than the maximum theoretical value of 2 bits per sifted photon, which is due to imperfections in transmission.

For a comparison, we perform a BB84 protocol with two-dimensional structured photons in the MUBs of $|\zeta\rangle = \{(|L,-1\rangle \pm |R,1\rangle)/\sqrt{2}\}$ and $|\xi\rangle = \{(|L,-1\rangle \pm i|R,1\rangle)/\sqrt{2}\}$; see Fig. 3(a) (top row). A quantum bit error rate and secret key rate of $Q^{2\text{D}} = 5\%$ and $R^{2\text{D}} = 0.43$ bits per sifted photon were obtained, respectively, using the target as compensation. Indeed, $R^{4\text{D}}$ is larger than $R^{2\text{D}}$, showing the potential for transmitting more secure information per sifted photon in higher dimensions. This is visually shown in Fig. 3(c) (top and bottom rows): the image that Alice sends Bob [Fig. 3(b)] can be discretized with more steps in dimension 4 (bottom row) as compared to dimension 2 (top row). Due to turbulence, the quantum bit error rate for dimension 4 on many nights was above $Q_0^{4\text{D}}$. An example of one of these nights is shown in the Supplement 1 with a calculated quantum bit error rate of $Q_{\text{noisy}}^{4\text{D}} = 27\%$ calculated from the probability-of-detection matrix. However, allowing for two-way classical communications, the tolerable error bit rate increases to $31.5\% > Q_{\text{noisy}}^{4\text{D}}$ in dimension 4 [33] (see Supplement 1).

5. CONCLUSION

We have shown the feasibility of increasing the secure data transmission rate using high-dimensional quantum states compared to bidimensional states despite a noisy channel. Indeed, protocols based on higher-dimensional states are more advantageous in noisier channels because the security threshold can tolerate more errors. This paves the road toward high-dimensional intracity quantum cryptography via quantum key distribution.

In addition, our results lay the groundwork for intracity quantum teleportation with structured photons, which is an essential component of a free-space quantum network. We anticipate that these demonstrations can be extended over longer distances provided with adequate active turbulence monitoring and compensation.

Funding. Canada Research Chairs; Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF).

Acknowledgment. All authors would like to thank Peter Banzer and Thomas Bauer for insightful discussions and acknowledge the support of the Max Planck—University of Ottawa Centre for Extreme and Quantum Photonics. E.K. would like to thank Guy LeBlanc, Donald Hopkins, David Needham, and Sean Kirkwood for their help on establishing the free-space link over the city of Ottawa. A.S. thanks Harold and Thérèse Sit for their continuous support and encouragement. The authors thank Norman Bouchard for providing the photo of the parliament of Canada. A.S. and H.L. acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC). F.B. acknowledges the support of the Vanier Canada Graduate Scholarships Program of the NSERC. R.F. acknowledges the support of the Banting postdoctoral fellowship of the NSERC.

See Supplement 1 for supporting content.

REFERENCES

1. C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in *International Conference on Computer System and Signal Processing* (IEEE, 1984), pp. 175–179.
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys. **81**, 1301–1350 (2009).
3. H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” Nat. Photonics **8**, 595–604 (2014).
4. H. Bechmann-Pasquinucci and W. Tittel, “Quantum cryptography using larger alphabets,” Phys. Rev. A **61**, 062308 (2000).
5. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, “Security of quantum key distribution using d-level systems,” Phys. Rev. Lett. **88**, 127902 (2002).
6. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, “Experimental quantum cryptography with qutrits,” New J. Phys. **8**(5), 75 (2006).
7. 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).
8. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O’sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, “High-dimensional quantum cryptography with twisted light,” New J. Phys. **17**, 033033 (2015).
9. L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, “Orbital angular momentum of light and the transformation of Laguerre–Gaussian laser modes,” Phys. Rev. A **45**, 8185–8189 (1992).
10. A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, “Entanglement of the orbital angular momentum states of photons,” Nature **412**, 313–316 (2001).
11. E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, and F. Sciarrino, “Experimental generation and characterization of single-photon hybrid ququarts based on polarization and orbital angular momentum encoding,” Phys. Rev. A **81**, 052317 (2010).
12. G. Molina-Terriza, J. P. Torres, and L. Torner, “Twisted photons,” Nat. Phys. **3**, 305–310 (2007).
13. F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, and L. Marrucci, “Quantum walks and wavepacket dynamics on a lattice with twisted photons,” Sci. Adv. **1**, e1500087 (2015).
14. A. E. Willner, H. Huang, Y. Yan, Y. Ren, N. Ahmed, G. Xie, C. Bao, L. Li, Y. Cao, Z. Zhao, J. Wang, M. P. J. Lavery, M. Tur, S. Ramachandran, A. F. Molisch, N. Ashrafi, and S. Ashrafi, “Optical communications using orbital angular momentum beams,” Adv. Opt. Photon. **7**, 66–106 (2015).
15. C. Paterson, “Atmospheric turbulence and orbital angular momentum of single photons for optical communication,” Phys. Rev. Lett. **94**, 153901 (2005).
16. M. Malik, M. O’Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. Lavery, M. J. Padgett, and R. W. Boyd, “Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding,” Opt. Express **20**, 13195–13200 (2012).
17. O. J. Faras, V. D’Ambrosio, C. Taballione, F. Bisesto, S. Slussarenko, L. Aolita, L. Marrucci, S. P. Walborn, and F. Sciarrino, “Resilience of hybrid optical angular momentum qubits to turbulence,” Sci. Rep. **5**, 8424 (2015).
18. S. K. Goyal, A. H. Ibrahim, F. S. Roux, T. Konrad, and A. Forbes, “The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum,” J. Opt. **18**, 064002 (2016).
19. J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, “Terabit free-space data transmission employing orbital angular momentum multiplexing,” Nat. Photonics **6**, 488–496 (2012).
20. F. Tamburini, E. Mari, A. Sponselli, B. Thidé, A. Bianchini, and F. Romanato, “Encoding many channels on the same frequency through radio vorticity: first experimental test,” New J. Phys. **14**, 033001 (2012).
21. M. P. Lavery, B. Heim, C. Peuntinger, E. Karimi, O. S. Magaña-Loaiza, T. Bauer, C. Marquardt, R. W. Boyd, M. Padgett, and G. Leuchs, “Study of turbulence induced orbital angular momentum channel crosstalk in a 1.6 km free-space optical link,” in *CLEO: Science and Innovations* (Optical Society of America, 2015), paper STu1L–4.
22. M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, “Communication with spatially modulated light through turbulent air across Vienna,” New J. Phys. **16**, 113028 (2014).
23. M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, “Twisted light transmission over 143 km,” Proc. Natl. Acad. Sci. USA **113**, 13648–13653 (2016).
24. G. Vallone, V. D’Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, “Free-space quantum key distribution by rotation-invariant twisted photons,” Phys. Rev. Lett. **113**, 060503 (2014).
25. M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, “Twisted photon entanglement through turbulent air across Vienna,” Proc. Natl. Acad. Sci. USA **112**, 14197–14201 (2015).
26. Q. Zhan, “Cylindrical vector beams: from mathematical concepts to applications,” Adv. Opt. Photon. **1**, 1–57 (2009).
27. L. Marrucci, C. Manzo, and D. Paparo, “Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media,” Phys. Rev. Lett. **96**, 163905 (2006).
28. H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R. W. Boyd, and E. Karimi, “Arbitrary optical wavefront shaping via spin-to-orbit coupling,” J. Opt. **18**, 124002 (2016).
29. E. Nagali, F. Sciarrino, F. De Martini, L. Marrucci, B. Piccirillo, E. Karimi, and E. Santamato, “Quantum information transfer from spin to orbital angular momentum of photons,” Phys. Rev. Lett. **103**, 013601 (2009).
30. N. Ageorges and C. Dainty, *Laser Guide Star Adaptive Optics for Astronomy* (Springer, 2013), Vol. **551**.
31. A. N. Kolmogorov, “The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers,” Dokl. Akad. Nauk SSSR **30**, 301–305 1941.
32. D. L. Fried, “Optical resolution through a randomly inhomogeneous medium for very long and very short exposures,” J. Opt. Soc. Am. **56**, 1372–1379 (1966).
33. G. M. Nikolopoulos, K. S. Ranade, and G. Alber, “Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication,” Phys. Rev. A **73**, 032325 (2006).

optica

High-dimensional intracity quantum cryptography with structured photons: supplementary material

Alicia Sit[1], Frédéric Bouchard[1], Robert Fickler[1], Jérémie Gagnon-Bischoff[1], Hugo Larocque[1], Khabat Heshami[2], Dominique Elser[3,4], Christian Peuntinger[3,4], Kevin Günthner[3,4], Bettina Heim[3,4], Christoph Marquardt[3,4], Gerd Leuchs[1,3,4], Robert W. Boyd[1,5], and Ebrahim Karimi[1,6,*]

[1]Physics Department, Centre for Research in Photonics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa ON K1N 6N5, Canada

[2]National Research Council of Canada, 100 Sussex Drive, Ottawa ON K1A 0R6, Canada

[3]Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

[4]Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

[5]Institute of Optics, University of Rochester, Rochester, New York, 14627, USA

[6]Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran

[*]Corresponding author: ekarimi@uottawa.ca

Published 24 August 2017

This document provides supplementary information to "High-dimensional intracity quantum cryptography with structured photons," https://doi.org/10.1364/optica.4.001006.

https://doi.org/10.6084/m9.figshare.5248189

1. MUTUALLY UNBIASED BASIS

Given a set of bases $\alpha_0, \ldots, \alpha_n$ of dimension d, they are said to be mutually unbiased with respect to one another if they satisfy the following condition,

$$|^{j}\langle\alpha_i|\alpha_{i'}\rangle^{j'}|^2 = \begin{cases} \delta_{j,j'} & \forall\, i = i' \\ \frac{1}{d} & \forall\, i \neq i' \end{cases} ; \quad i \in \{0, 1, ...n\}, \;\; j \in \{1, 2, .., d\}. \tag{S1}$$

For dimensions where d is a power of a prime, $d+1$ mutually unbiased bases (MUBs) can be found. For 2-dimensional quantum key distribution (QKD) protocols, photons can be encoded using polarization and orbital angular momentum (OAM). We represent states of light that have a particular polarization and OAM value using a compound ket notation. In this way, if a photon has a certain polarization Π and carries ℓ units of OAM, it is written as $|\Pi, \ell\rangle$.

The two MUBs of dimension 2 are given by,

$$\begin{aligned} \{|\zeta\rangle^i\} &= \left\{\frac{1}{\sqrt{2}}\left(|L,-\ell\rangle + |R,+\ell\rangle\right), \frac{1}{\sqrt{2}}\left(|L,-\ell\rangle - |R,+\ell\rangle\right)\right\}, \\ \{|\xi\rangle^j\} &= \left\{\frac{1}{\sqrt{2}}\left(|L,-\ell\rangle + i\,|R,+\ell\rangle\right), \frac{1}{\sqrt{2}}\left(|L,-\ell\rangle - i\,|R,+\ell\rangle\right)\right\}. \end{aligned} \tag{S2}$$

In dimension 4, the natural basis is $|k\rangle \in \{|H,\ell\rangle, |H,-\ell\rangle, |V,\ell\rangle, |V,-\ell\rangle\}$, and the two sets of MUBs $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ were generated by the following matrices,

$$\begin{aligned} \mathcal{M}_0^{ik} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ \mathcal{M}_1^{jk} &= \frac{1}{2}\begin{pmatrix} 1 & i & 1 & -i \\ 1 & i & -1 & i \\ 1 & -i & 1 & i \\ -1 & i & 1 & i \end{pmatrix}, \end{aligned} \tag{S3}$$

such that $|\psi\rangle^i = \mathcal{M}_0^{ik}|k\rangle$ and $|\varphi\rangle^j = \mathcal{M}_1^{jk}|k\rangle$. This results in the following states:

$$\{|\psi\rangle^i\} = \{|H,+\ell\rangle, |H,-\ell\rangle, |V,+\ell\rangle, |V,-\ell\rangle\}, \tag{S4}$$

$$\begin{aligned} \{|\varphi\rangle^j\} = \Big\{ &\frac{1}{\sqrt{2}}(|L,\ell\rangle + |R,-\ell\rangle), \frac{1}{\sqrt{2}}(|L,\ell\rangle - |R,-\ell\rangle), \\ &\frac{1}{\sqrt{2}}(|L,-\ell\rangle + |R,\ell\rangle), \frac{1}{\sqrt{2}}(|L,-\ell\rangle - |R,\ell\rangle)\Big\}. \end{aligned} \tag{S5}$$

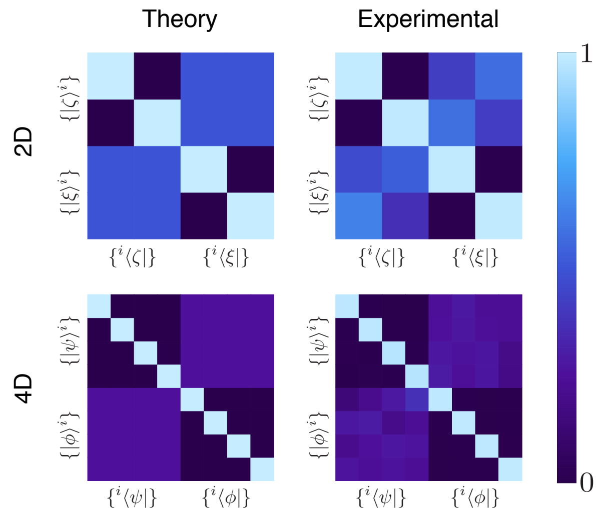

Fig. S1. Visualization of MUBs in d=2 and d=4 Theoretical probability-of-detection matrices (left column) for dimensions 2 and 4 using Eq. (S2) and Eqs. (S4–S5) by applying Eq. (S1). The probability-of-detection matrices as measured in the laboratory (right column) give bit error rates of 0.83% and 1.83% in dimensions 2 ($\ell = 2$) and 4 ($\ell = 2$), respectively.

Figure S1 shows a visual representation of the 2D (top row) and 4D (bottom row) MUBs using Eq. (S1), comparing the theoretical probability-of-detection matrix to the experimental one as measured in the laboratory, i.e. without the intra-city link. The quantum bit error rate is calculated as one minus the average of the on-diagonal elements. The calculated quantum bit error rates from the experimentally measured matrices are 0.83% and 1.83% in dimensions 2 ($\ell = 2$) and 4 ($\ell = 2$), respectively.

2. GENERATION OF IMPLEMENTED MUBS IN $D = 2$ AND 4

In order to create structured photons possessing both polarization and OAM, we utilize patterned liquid crystal devices known as q-plates. Q-plates coherently couple spin (i.e. polarization) to orbital angular momentum such that $\ell = \pm 2q$, where q is the topological charge of the liquid crystal distribution. The action of a q-plate is as follows:

$$|L,0\rangle \xrightarrow{q-plate} |R,+2q\rangle\,, \tag{S6}$$

$$|R,0\rangle \xrightarrow{q-plate} |L,-2q\rangle\,. \tag{S7}$$

Since q-plates are linear devices, a photon in a superposition of $|L,0\rangle$ and $|R,0\rangle$ will be mapped to a state in a superposition of $|R,+2q\rangle$ and $|L,-2q\rangle$. Thus, just as waveplates are used to transform polarization states on the Poincaré sphere, waveplates in combination with a q-plate perform the same transformations on a hybrid OAM-Poincaré sphere.

The MUBs in dimension 2, $\{|\zeta\rangle^i\}$ and $\{|\xi\rangle^j\}$ are generated using the sequence of a half-wave plate (HWP) followed by a q-plate. The waveplate angles are given in (S8).

state	HWP
$\lvert\zeta\rangle^1$	0°
$\lvert\zeta\rangle^2$	+45°
$\lvert\xi\rangle^1$	+22.5°
$\lvert\xi\rangle^2$	−22.5°

(S8)

The MUBs in dimension 4, $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ are generated by sandwiching a q-plate between either HWPs or QWPs. If photons pass left to right through the following optical elements, the waveplate angles that Alice uses to generate $\{|\psi\rangle^i\}$ are given in the (S9), and $\{|\varphi\rangle^j\}$ in (S10).

state	QWP before QP	QWP after QP
$\lvert\psi\rangle^1$	−45°	−45°
$\lvert\psi\rangle^2$	+45°	+45°
$\lvert\psi\rangle^3$	−45°	+45°
$\lvert\psi\rangle^4$	+45°	−45°

(S9)

state	HWP before QP	HWP after QP
$\lvert\varphi\rangle^1$	0°	0°
$\lvert\varphi\rangle^2$	+45°	0°
$\lvert\varphi\rangle^3$	0°	–
$\lvert\varphi\rangle^4$	+45°	–

(S10)

Bob uses the same waveplate angles, but mirrors the sequence of waveplates as Alice has in order to project his received photons onto a particular state.

3. EXPERIMENTAL DATA

Coincidence counts are accumulated per 200 ms. For each of Bob's measurements, he records fifty data points. Bob obtains a probability-of-detection matrix by averaging the data points for each measurement and then normalizing over each state that Alice sends. The states that Alice sends and the states that Bob projects onto are labelled on the left and top, respectively, of each matrix below.

Normalized raw data for probability-of-detection matrix in dimension 2 as measured across the intra-city link using a q=1/2-plate, as shown in Fig. 3a of the main text (top row):

$$\begin{array}{c|cc|cc|} & {}^1\langle\zeta| & {}^2\langle\zeta| & {}^1\langle\xi| & {}^2\langle\xi| \\ |\zeta\rangle^1 & 0.971 & 0.029 & 0.421 & 0.579 \\ |\zeta\rangle^2 & 0.062 & 0.938 & 0.677 & 0.323 \\ \hline |\xi\rangle^1 & 0.731 & 0.269 & 0.959 & 0.041 \\ |\xi\rangle^2 & 0.459 & 0.541 & 0.068 & 0.932 \end{array} \tag{S11}$$

Target corrected data from (S11):

$$\begin{array}{c|cc|cc|} & {}^1\langle\zeta| & {}^2\langle\zeta| & {}^1\langle\xi| & {}^2\langle\xi| \\ |\zeta\rangle^1 & 0.972 & 0.028 & 0.351 & 0.649 \\ |\zeta\rangle^2 & 0.050 & 0.950 & 0.653 & 0.347 \\ \hline |\xi\rangle^1 & 0.725 & 0.275 & 0.961 & 0.039 \\ |\xi\rangle^2 & 0.463 & 0.537 & 0.069 & 0.931 \end{array} \tag{S12}$$

Normalized raw data for probability-of-detection matrix in dimension 4 as measured across the intra-city link:

$$\begin{array}{c|cccc|cccc}
 & {}^{1}\langle\psi| & {}^{3}\langle\psi| & {}^{2}\langle\psi| & {}^{4}\langle\psi| & {}^{1}\langle\varphi| & {}^{2}\langle\varphi| & {}^{3}\langle\varphi|^{3} & {}^{4}\langle\varphi| \\
|\psi\rangle^{1} & 0.918 & 0.019 & 0.051 & 0.012 & 0.252 & 0.245 & 0.275 & 0.228 \\
|\psi\rangle^{3} & 0.020 & 0.937 & 0.038 & 0.005 & 0.190 & 0.192 & 0.312 & 0.306 \\
|\psi\rangle^{2} & 0.012 & 0.156 & 0.816 & 0.012 & 0.279 & 0.277 & 0.289 & 0.155 \\
|\psi\rangle^{4} & 0.149 & 0.009 & 0.018 & 0.824 & 0.152 & 0.195 & 0.384 & 0.269 \\
\hline
|\varphi\rangle^{1} & 0.319 & 0.125 & 0.325 & 0.231 & 0.869 & 0.039 & 0.064 & 0.029 \\
|\varphi\rangle^{2} & 0.252 & 0.217 & 0.239 & 0.292 & 0.038 & 0.822 & 0.042 & 0.098 \\
|\varphi\rangle^{3} & 0.185 & 0.177 & 0.447 & 0.191 & 0.065 & 0.027 & 0.872 & 0.037 \\
|\varphi\rangle^{4} & 0.207 & 0.205 & 0.381 & 0.208 & 0.030 & 0.134 & 0.036 & 0.800
\end{array} \qquad \textbf{(S13)}$$

Target corrected data from (S13), as shown in Fig. 3a of the main text (bottom row):

$$\begin{array}{c|cccc|cccc}
 & {}^{1}\langle\psi| & {}^{3}\langle\psi| & {}^{2}\langle\psi| & {}^{4}\langle\psi| & {}^{1}\langle\varphi| & {}^{2}\langle\varphi| & {}^{3}\langle\varphi|^{3} & {}^{4}\langle\varphi| \\
|\psi\rangle^{1} & 0.924 & 0.035 & 0.011 & 0.031 & 0.272 & 0.232 & 0.254 & 0.243 \\
|\psi\rangle^{3} & 0.024 & 0.960 & 0.012 & 0.004 & 0.197 & 0.213 & 0.260 & 0.330 \\
|\psi\rangle^{2} & 0.005 & 0.052 & 0.930 & 0.013 & 0.239 & 0.301 & 0.301 & 0.159 \\
|\psi\rangle^{4} & 0.049 & 0.004 & 0.029 & 0.918 & 0.094 & 0.242 & 0.433 & 0.232 \\
\hline
|\varphi\rangle^{1} & 0.376 & 0.108 & 0.321 & 0.195 & 0.874 & 0.033 & 0.065 & 0.028 \\
|\varphi\rangle^{2} & 0.273 & 0.197 & 0.255 & 0.275 & 0.035 & 0.825 & 0.045 & 0.096 \\
|\varphi\rangle^{3} & 0.200 & 0.132 & 0.511 & 0.157 & 0.060 & 0.016 & 0.889 & 0.035 \\
|\varphi\rangle^{4} & 0.186 & 0.163 & 0.365 & 0.287 & 0.026 & 0.129 & 0.043 & 0.803
\end{array}$$

Normalized raw data for probability-ofdetection matrix in dimension 4 on a turbulent night:

$$\begin{array}{c|cccc|cccc}
 & {}^{1}\langle\psi| & {}^{3}\langle\psi| & {}^{2}\langle\psi| & {}^{4}\langle\psi| & {}^{1}\langle\varphi| & {}^{2}\langle\varphi| & {}^{3}\langle\varphi|^{3} & {}^{4}\langle\varphi| \\
|\psi\rangle^{1} & 0.741 & 0.032 & 0.043 & 0.184 & 0.370 & 0.168 & 0.364 & 0.098 \\
|\psi\rangle^{3} & 0.096 & 0.722 & 0.138 & 0.044 & 0.120 & 0.432 & 0.221 & 0.228 \\
|\psi\rangle^{2} & 0.043 & 0.177 & 0.755 & 0.025 & 0.276 & 0.247 & 0.197 & 0.281 \\
|\psi\rangle^{4} & 0.101 & 0.041 & 0.047 & 0.811 & 0.122 & 0.433 & 0.332 & 0.113 \\
\hline
|\varphi\rangle^{1} & 0.126 & 0.471 & 0.197 & 0.206 & 0.707 & 0.051 & 0.144 & 0.098 \\
|\varphi\rangle^{2} & 0.211 & 0.234 & 0.352 & 0.203 & 0.110 & 0.694 & 0.079 & 0.117 \\
|\varphi\rangle^{3} & 0.265 & 0.285 & 0.259 & 0.191 & 0.195 & 0.056 & 0.632 & 0.117 \\
|\varphi\rangle^{4} & 0.478 & 0.146 & 0.185 & 0.191 & 0.048 & 0.103 & 0.075 & 0.775
\end{array} \qquad \textbf{(S14)}$$

4. NUMERICAL APPROACH FOR THE SECRET KEY RATE CALCULATION

Here we use a numerical approach to calculate the secret key rate for the MUBs in the current experiment that are shown in Eqs. (S3–S5). The secret key rate calculation below relies on the dual optimization problem that has recently been introduced as an efficient numerical approach for unstructured quantum key distribution [1]. The main result in [1] indicates that the achievable secure key rate is lower bounded by the following maximization problem,

$$K \geq \frac{\Theta}{\ln 2} - H(Z_A|Z_B), \qquad \textbf{(S15)}$$

where

$$\Theta := \max_{\vec{\lambda}} \left(- \left\| \sum_j Z_A^j R(\vec{\lambda}) Z_A^j \right\| - \vec{\lambda} \cdot \vec{\gamma} \right), \qquad \textbf{(S16)}$$

and

$$R(\vec{\lambda}) := \exp\left(-\mathbb{1} - \vec{\lambda} \cdot \vec{\Gamma} \right). \qquad \textbf{(S17)}$$

Here Z_A (Z_B) denotes the measurement performed by Alice (Bob) to derive the raw key, and $\vec{\gamma} = \{\gamma_i := \mathrm{Tr}(\rho_{AB}\Gamma_i)\}$ are determined through average value of experimental measurements.

For the generalized BB84 in dimension $d = 4$ with two MUBs, the experimental constraints can be summarized to

$$\text{Key-map POVM:} \quad Z_A = \left\{ |\psi\rangle^i \langle\psi|, \text{for} \quad i = 1 \cdots d = 4 \right\} \qquad \textbf{(S18)}$$

$$\text{Constraints:} \quad \langle \mathbb{1} \rangle = 1 \qquad \textbf{(S19)}$$

$$\langle \mathbf{E_X} \rangle = Q \qquad \textbf{(S20)}$$

$$\langle \mathbf{E_Z} \rangle = Q \qquad \textbf{(S21)}$$

where $\mathbf{E_{Z\,(X)}}$ are coarse-grained error operators in $\mathcal{M}_{0\,(1)}$ MUBs and defined as

$$\mathbf{E_X} = \mathbb{1} - \sum_i^{d=4} |\psi\rangle^i \langle\psi| \otimes |\psi\rangle^i \langle\psi| \qquad \textbf{(S22)}$$

$$\mathbf{E_Z} = \mathbb{1} - \sum_i^{d=4} |\varphi\rangle^i \langle\varphi| \otimes |\varphi\rangle^i \langle\varphi|. \qquad \textbf{(S23)}$$

Eqs. (S4) and (S5) show the definition for $|\psi\rangle^i$ and $|\varphi\rangle^i$ basis states.

Figure S2 shows the numerical result of the optimization problem in Eq. (S15) with MUBs in Eqs. (S4,S5) in comparison with the theoretical key rates in [2, 3]. This numerical approach may be extended to find secret key rate per signal with two-way classical communications to tolerate higher qubit error rates [4].

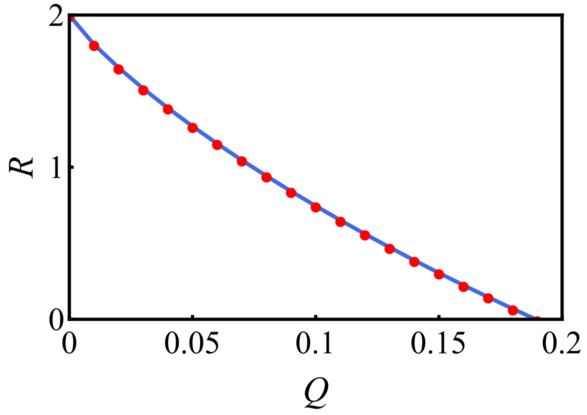

Fig. S2. Secret key rate per signal for BB84 in d=4 with 2 MUBs Solution to the numerical optimization problem in Eq. (S15) are shown for different values of average error rates (red dots). As it can be seen, the numerical optimization saturates the bound and shows a good agreement with the theory from [2, 3]. For more details on the numerical approach see [1].

REFERENCES

1. P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, “Numerical approach for unstructured quantum key distribution,” Nature Communications **7**, 11712 (2016).
2. A. Ferenczi, and N. Lütkenhaus, “Symmetries in quantum key distribution and the connection between optical attacks and optimal cloning,” Physical Review A **85**, 052310 (2012).
3. L. Sheridan, and V. Scarani, “Security proof for quantum key distribution using qudit systems,” Physical Review A **82**, 030301 (2010).

4. G. M. Nikolopoulos, K. S. Ranade, and G. Alber, “Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication,” Physical Review A **73**, 032325 (2006).