Quantum Communication through the Elements: Earth, Air, Water

by

Alicia Sit

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the degree of
Master of Science in Physics

Ottawa-Carleton Institute of Physics
Department of Physics
University of Ottawa

Abstract

This thesis encompasses a body of experimental work on the use of structured light in quantum cryptographic protocols. In particular, we investigate the ability to perform quantum key distribution through various quantum channels (fibre, free-space, underwater) in laboratory and realistic conditions. We first demonstrate that a special type of optical fibre (vortex fibre) capable of coherently transmitting vector vortex modes is a viable quantum channel. Next, we describe the first demonstration of high-dimensional quantum cryptography using structured photons in an urban setting. In particular, the prevalence of atmospheric turbulence can introduce many errors to a transmitted key; however, we are still able to transmit more information per carrier using a 4-dimensional scheme in comparison to a 2-dimensional one. Lastly, we investigate the possibility of performing secure quantum communication with twisted photons in an uncontrolled underwater channel. We find that though it is possible for low-dimensional schemes, high-dimensional schemes suffer from underwater turbulence without the use of corrective wavefront techniques.

Acknowledgements

I wish to thank my supervisor, Prof. Ebrahim Karimi, for his continous support, indispensable advice and for giving me countless opportunities throughout the course of my Master's degree. I acknowledge the financial support of the Canada Research Chairs (CRC) program, and of the Natural Sciences and Engineering Research Council of Canada (NSERC).

I would also like to thank the entire Structured Quantum Optics (SQO) group, current and past members, for creating such a fun and exciting environment to do great science. The projects undertaken for this thesis would quite literally have been impossible to complete without their help and participation. In particular, I would like to thank Robert Fickler (the best post-doc) and Frédéric Bouchard (the Alice to my Bob) for spending many many cold, sleepless nights on the roof together—the beginning of our QKD adventures—as well as teaching and mentoring me on all things lab, physics and life as a researcher. In addition, I would like to thank Frédéric Bouchard, Hugo Larocque and Felix Hufnagel—three awesome friends and students—for innumerable hours passed together laughing and learning. Of course, many, if not all of my projects, have had the great opportunity of being a collaboration, local and international; therefore, I thank all of my collaborators and fellow co-authors from NRC (Khabat Heshami, Duncan England), the Max-Planck Institute for the Science of Light (Gerd Leuchs, Christoph Marquardt, and their teams), and Boston University (Siddharth Ramachandran's team).

Last but not least, I would like to thank my parents and family for their generosity and support from the beginning. And finally, to Morgan Robinson, my partner in life, for his perpetual support when I stayed late at the lab, and being my rock when things got tough.

Table of Contents

CV

Publications

1. **A. Sit**, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günther, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica* **4**, 1006 (2017).

2. M. T. Runyon, C. H. Nacke, **A. Sit**, M. Granados-Baez, L. Giner, and J. S. Lundeen, "Implementation of nearly arbitrary spatially varying polarization transformations: an in-principle lossless approach using spatial light modulators," *Applied Optics* **57**, 5769 (2018).

3. F. Bouchard, **A. Sit**, K. Heshami, R. Fickler, and E. Karimi, "Round-Robin Differential Phase-Shift Quantum Key Distribution with Twisted Photons," *Physical Review A* **98**, 010301(R) (2018).

4. F. Bouchard, **A. Sit**, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics Express* **26**, 22563 (2018).

5. **A. Sit**, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi, "Quantum cryptography with structured photons through a vortex fiber," *Optics Letters* **43**, 4108 (2018).

6. Y. Zhang, **A. Sit**, F. Bouchard, H. Larocque, F. Grenapin, E. Cohen, A. C. Elitzur, J. L. Harden, R. W. Boyd, and E. Karimi, "Interaction-Free Ghost-Imaging of Structured Objects," *Optics Express* **27**, 2212 (2019).

7. F. Nejadsattari, Y. Zhang, F. Bouchard, H. Larocque, **A. Sit**, E. Cohen, R. Fickler, and E. Karimi, "Experimental realization of wave-packet dynamics in cyclic quantum walks," *Optica* **6**, 174 (2019).

8. F. Bouchard, F. Hufnagel, D. Koutný, A. Abbas, **A. Sit**, K. Heshami, R. Fickler, and E. Karimi, "Quantum process tomography of a high-dimensional quantum communication channel," *Quantum* **3**, 138 (2019).

9. F. Hufnagel, **A. Sit**, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, and E. Karimi, "Characterization of an underwater channel for quantum communcation in the Ottawa River," arXiv preprint arXiv:1905.09437 (2019).

Statement of originality and collaborative contributions

To the best of her knowledge, the author states that the work described in this Master's thesis constitute original research in the field of physics. Below, we provide the collaborative contributions of each participant for every chapter.

Ebrahim Karimi initiated the work of Chapter 2. P. Gregg, L. Yan and S. Ramachandran designed and fabricated the vortex fiber. H. Larocque fabricated the q-plates. A. Sit designed and performed the experiment, as well as analyzed the data. R. Fickler, F. Alsaiari and F. Bouchard helped with the experiment. R.W. Boyd and E. Karimi supervised all aspects of the projects. All authors contributed to the text of the manuscript.

Ebrahim Karimi initiated the work of Chapter 3. A. Sit, F. Bouchard and R. Fickler designed, built and performed the experiment, as well as analyzed the data. J. Gagnon-Bischoff helped with the construction of the experiment. H. Larocque fabricated the q-plates. K. Heshami helped with the theoretical model. D. Elser, C. Peuntinger, K. Gunthner, B. Heim, C. Marquardt and G. Leuchs supervised the first iteration of this project that took place in Erlangan, Germany. R.W. Boyd and E. Karimi supervised all aspects of the project. All authors contributed to the text of the manuscript.

Ebrahim Karimi initiated the work of Chapter 4. A. Sit, F. Bouchard and F. Hufnagel designed and performed the experiment. A. Abbas helped with building the experiment. F. Bouchard, F. Hufnagel and A. Sit analyzed the data. K. Heshami helped with the theoretical model. Y. Zhang, R. Fickler, C. Marquardt, G. Leuchs, R.W. Boyd and E. Karimi supervised all aspects of the project. All authors contributed to the text of the manuscript.

List of Figures

Chapter 1

Introduction

1.1 Overview

Communication is one of our fundamental means of exchanging information. The human race over the centuries has devised a remarkable number of ways to communicate faster and farther, reducing the task of sending messages across the world to a click of a button. Nonetheless, in our small world where billions of people have access to this technology, the need for secure encryption is paramount so that only the designated recipient has access to potentially sensitive information. Classical encryption techniques, for example Rivest-Shamir-Adleman (RSA) encryption, rely on mathematically "hard" problems which are computationally expensive to break, such as factoring large numbers. However, perhaps alarmingly so, it has been mathematically proven that RSA encryption can, and will, be broken in polynomial time using quantum computers with Shor's algorithm [1]. Despite this very real threat, scientists and engineers around the world are researching and creating solutions to keep our information secure. One of the more advanced and promising avenues is quantum cryptography, which takes advantage of quantum mechanical properties to maintain security. Quantum Key Distribution (QKD) is one quantum cryptographic task which makes use of these properties – such as Heisenberg's uncertainty principle, the superposition principle, and the no-cloning theorem [2] – to construct information-theoretic secure protocols to establish a secure random key between two separated parties, colloquially named Alice and Bob [3]. These quantum properties ensure that an eavesdropper, Eve, cannot gain access to the transmitted information as she would introduce detectable errors in the key when Alice and Bob sacrifice and compare a

small portion of their keys after transmission. Indeed, each QKD protocol has a unique threshold which dictates the amount of errors the transmitted information can tolerate before running the risk that an eavesdropper has compromised the key; several QKD schemes include the BB84 [3], Ekert [4], and tomographic [5] protocols.

Unlike classical encryption protocols which use classical bits — 0 and 1 — as information carriers, QKD protocols use quantum particles to encode information. The easiest quantum particles to use for this are photons – the quanta of light – as they travel very fast and are easy to manipulate in terms of quantum state generation and detection, since they won't interact with the environment. The main quantum channels are optical fiber and free-space (ground-to-ground, satellite-to-ground, ground-to-satellite) links. Amazingly, the real-world implementation of these systems has greatly matured within the last few decades. Optical fiber links with a "plug-and-play" QKD protocol are already commercially available (Switzerland) [6], and entanglement distribution has been shown to be feasible on existing fiber networks (China, Canada) [7, 8]. In the free-space case, several ground-to-ground links around the world have been constructed to test QKD protocols – their scales range from several hundred metres (USA, Italy, Canada) to several kilometers (intra-city) (Germany, Austria, Canada) [9, 10, 11], to the largest of 143 km between two Canary Islands (Austria, Germany) [12]. Taking it even further, within the last couple of years, successful connections between satellites and ground stations for QKD (China, Germany, Italy) [13, 14, 15, 16] have paved the way for establishing a global quantum network. Beyond fibre and free-space channels, recent interest has arisen for utilizing water as a quantum communication channel between underwater submersibles [17], and potentially from submersibles to satellites.

With photons, information can be encoded using one of the various photonic degrees of freedom (DOF): wavelength, polarization, time-bin, spatial modes, etc – each with their own advantages and disadvantages. The decision of which manner to encode information is coupled in some sense to the quantum channel used for communication and the amount of tolerable errors, which in turn can limit the QKD protocol implemented and the number of bits transmitted. This thesis will study the implementations of so-called *structured photons* in each of the three quantum channels (fibre, free-space, underwater) for the use in QKD. We define a photon (or more generally light) to be structured if information is encoded using more than one degree of freedom. For example, light possessing both spin and orbital angular momentum — particularly when in an arbitrary superposition of these two DOFs — will dis-

play a complex (structured) transverse polarization distribution; indeed, this type of structured light will hereafter be the main focus of this thesis. In general, structured photons reside in a high-dimensional Hilbert space, which has several implications and motivations for their use in quantum cryptography [18, 19]. The first is that we are no longer limited to an encryption alphabet of '0' and '1' (i.e. qubits): we now have access to a theoretically unbounded alphabet, and thus increasing the information capacity of the quantum channel to send potentially more than one bit per carrier. The second advantage is that the characteristic error threshold for a given QKD protocol increases, which means that it is more noise and error tolerant, as will be shown in a Sec. 1.3.

Since there are many common aspects to the works discussed in this thesis, the remaining sections of this chapter will briefly cover the relevant photonic degrees of freedom in Sec. 1.2 and the relevant QKD protocols in Sec. 1.3. These sections will provide the fundamentals for the next three chapters, though more details will be given as needed. A big challenge, as we will encounter, is the ability to actually implement structured photons in realistic quantum channels that are subject to uncontrolled environmental factors. We will thus start off in the laboratory setting for Chap. 2 where we explore a unique type of optical fibre that supports specific structured modes of light, and show its feasibility for QKD. In Chap. 3, however, we trade the conventional (stable) lab for a home-built (unstable) one on the roof. Here, we get our first taste of the true challenge of implementing QKD with structured photons in a real free-space environment: atmospheric turbulence. This perturbing and ever changing environmental factor can introduce excess noise into the channel; nonetheless, we show that it is still possible to gain an advantage with high-dimensional schemes. For our last quantum channel in Chap. 4, we navigate the relatively unexplored realm of underwater QKD with structured light, where again we have turbulence, but in quite a different regime to that of free-space. We then close this thesis with concluding remarks in Chap. 5.

1.2 Photonic degrees of freedom

Photons — the quanta of light — are extremely versatile objects. Particularly in the study of quantum communication, photons make for excellent information carriers. Below, we define the two main photonic degrees of freedom (DOFs) pertinent to the works discussed in this thesis: polarization and orbital angular momentum.

1.2.1 Polarization

As an electromagnetic wave propagating through free-space — and not subject to any strong focusing — light consists of an electric (and magnetic) field oscillating in the transverse plane. Here, the transverse plane (x-y plane) is that which is perpendicular to the direction of propagation (z). The manner in which the electric field oscillates, i.e. its vectorial nature, describes the *polarization* of the light. If the field oscillates along the x-axis, it is said to be *horizontally* polarized; likewise, it is *vertically* polarized if it oscillates along the y-axis. In bra-ket notation for a quantum state, horizontal and vertical polarization will be written as $|H\rangle$ and $|V\rangle$, respectively. Polarization behaves as a spin-1/2 system, i.e. a qubit; we can thus form various two-dimensional bases to describe an arbitrary polarization state. For example, we could express any arbitrary polarization state as a superposition of $|H\rangle$ and $|V\rangle$:

$$|\Pi\rangle = a_H |H\rangle + a_V e^{i\theta} |V\rangle , \tag{1.1}$$

where the amplitudes a_H, a_V are normalized such that $a_H^2 + a_V^2 = 1$, and θ is the phase difference between the components. With $\theta = 0$, we can create any linear polarization state by varying the amplitude weights; in particular, we define *diagonal* ($|D\rangle$) and *anti-diagonal* ($|A\rangle$) polarizations, respectively, as,

$$|D\rangle = \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle) , \tag{1.2}$$

$$|A\rangle = \frac{1}{\sqrt{2}} (|H\rangle - |V\rangle) . \tag{1.3}$$

If $|\theta| = \pi/2$ with $a_H = a_V$, we find that the electric field vector rotates in a circle about the direction of propagation; the light is thus *circularly* polarized. The sign of θ dictates the "handedness" of the polarization, i.e. whether it rotates clockwise or counterclockwise when looking down the propagation axis ($+\hat{z}$). The convention that we will use throughout this thesis is such that *left-handed circular* polarization $|L\rangle$ corresponds to clockwise rotation, and *right-handed circular* polarization $|R\rangle$ corresponds to counterclockwise rotation. Explicitly, we have that,

$$|L\rangle = \frac{1}{\sqrt{2}} (|H\rangle + i |V\rangle) , \tag{1.4}$$

$$|R\rangle = \frac{1}{\sqrt{2}} (|H\rangle - i |V\rangle) . \tag{1.5}$$

Since the electric field for circular polarization is physically rotating, we can ascribe to the photons a spin angular momentum (SAM). With the convention here, $|L\rangle$ ($|R\rangle$)

carries a SAM of $+(-)\hbar$ along the direction of propagation, where $\hbar$ is the reduced Planck constant. Indeed, if a small (birefringent) particle were to be illuminated by circularly polarized light, it will begin to spin about itself as the light transfers its SAM to the particle.

1.2.2 Orbital angular momentum

In addition to carrying SAM, light may also carry orbital angular momentum (OAM) [20]. Whereas SAM dealt with the vectorial nature of light (polarization), OAM deals with the wavefront of the light — they are thus two independent degrees of freedom. Since the majority of experiments include circular apertures, it is natural to work with Laguerre-Gaussian (LG) modes which also exhibit cylindrical symmetry and best describe OAM-carrying beams for the purpose of this thesis.

Recall that a collimated beam of light, with wavelength λ, propagating in a homogeneous medium (the scenario for most laboratory experiments) is described by the paraxial wave equation:

$$\left(\nabla_\perp^2 + 2ik\frac{\partial}{\partial z}\right)\Psi(x,y,z) = 0, \tag{1.6}$$

where $\Psi(x,y,z)$ is the mode/wavefunction of the beam in the transverse plane, $k = 2\pi/\lambda$ is the wavenumber, and $\nabla_\perp^2$ is the transverse Laplacian operator. Solving Eq. (1.6) in cylindrical coordinates (r,φ,z), and imposing cylindrical symmetry, yields the LG modes, which carry OAM, as solutions:

$$\begin{aligned}\mathrm{LG}_{\ell,p}(r,\varphi,z) = \frac{C_{\ell,p}}{w(z)}\left(\frac{r\sqrt{2}}{w(z)}\right)^{|\ell|}\exp\left(-\frac{r^2}{w(z)^2}\right)L_p^{|\ell|}\left(\frac{2r^2}{w(z)^2}\right)\times \\ \times\exp\left(ik\frac{r^2}{2R(z)}\right)\exp\left(ikz\right)\exp\left(i\ell\varphi\right)\exp\left(-i\Phi(z)\right).\end{aligned} \tag{1.7}$$

Here, ℓ is an integer for the azimuthal index, and p is a positive integer for the radial index; $C_{\ell,p} = (2p!/(\pi(p+|\ell|)!))^{1/2}$ are the normalization constants; $w(z) = w_0(1+(z/z_R)^2)^{1/2}$ is the beam radius with beam waist w_0 at $z=0$, and Rayleigh range $z_R = \pi w_0^2/\lambda$; $L_p^{|\ell|}(\cdot)$ are the generalized Laguerre polynomials; $R(z) = z(1+(z_R/z)^2)$ is the radius of curvature; and $\Phi(z) = (2p+|\ell|+1)\arctan(z/z_R)$ is the so-called Gouy phase.

Though this looks a bit complicated, the main factor that we are interested in is the $\exp(i\ell\varphi)$. This is an azimuthally varying phase factor to which we attribute

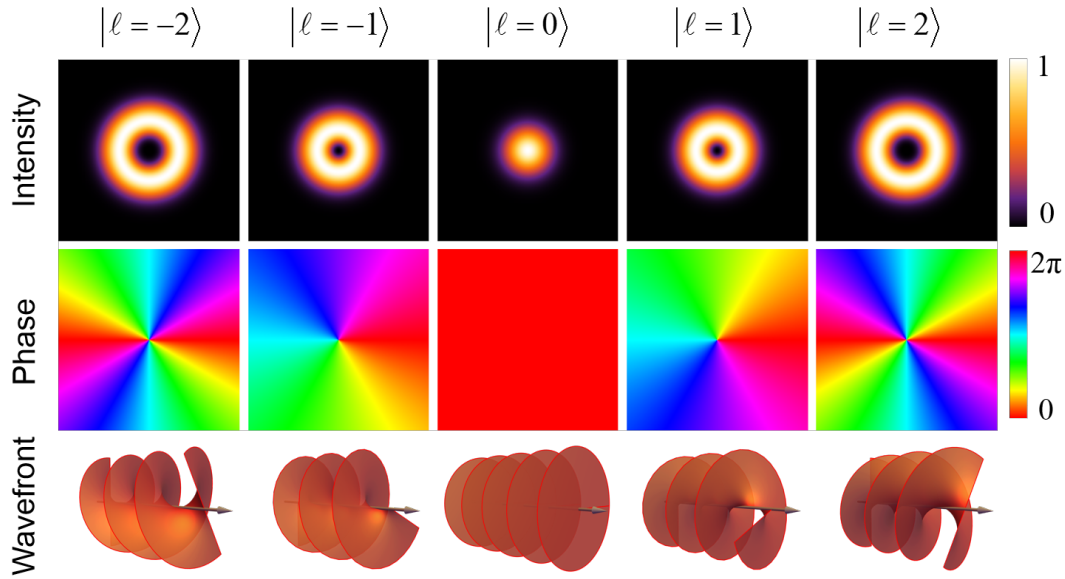

Figure 1.1: **Orbital angular momentum states of light**. The intensity profile (top row) of OAM ($p = 0$) states possess a null on the axis of propagation for nonzero ℓ, resulting from a phase singularity in an azimuthally varying phase profile (middle row). The wavefront (bottom row) of such modes has $|\ell|$ intertwined helices twisting with a handedness according to the sign of ℓ.

$\ell\hbar$ units of OAM. Figure 1.1 shows what various LG beams physically look like. In particular, due to the $\exp(i\ell\varphi)$ factor, the wavefront (contour of constant phase) of the mode exhibits $|\ell|$ intertwined helices, whose handedness is given by the sign of ℓ; photons purely carrying OAM are thus commonly referred to as "twisted". Another feature of note is that the phase is undefined on the axis of propagation—hence, it has a phase singularity. This phase singularity causes a null in intensity resulting in the amplitude taking on a "doughnut"-like form, whose hole grows with $|\ell|$. Additionally, the modes gain p extra rings that are π out of phase with each other; however, for simplicity, we only deal with the case of $p = 0$. For notation, a quantum state carrying $\ell\hbar$ units of OAM will be written as $|\ell\rangle$.

Since ℓ is a theoretically unbounded index, the LG modes/OAM states reside in an infinite-dimensional Hilbert space. However in practice, we are limited to a high-dimensional subset of OAM states due to truncation from a finite numerical aperture. To date, the largest generated ℓ is 10010, which was used for a quantum entanglement experiment [21]. Nonetheless, a d-dimensional OAM subspace provides an advantage in quantum information to bi-dimensional systems (like polarization) as we can create

a larger encoding alphabet and thus send more information per carrier, which scales as $\log_2(d)$ bits. Other applications of OAM, beyond high-dimensional entanglement and quantum communication, include, to name a few, stimulated emission depletion (STED) microscopy which uses OAM to greatly improve imaging resolution [22, 23], as well as coronography to better image exoplanets [24].

1.3 Quantum key distribution

It is important to note that QKD protocols securely distribute a random secret key over a quantum channel between users, not the message itself. Indeed, once the protocol is completed, Alice and Bob can contact each other over any unsecured, classical channel of their choice—phone, email, etc—to exchange their message, encrypted using their random shared secret key in a one-time pad protocol (unbreakable when the key is the length of the message) [25]. For the practical realization of QKD, there is a final step before Alice or Bob can encrypt their message, known as *error correction* and *privacy amplification* [26], which removes any remaining errors in the secret key and eliminating any partial information that an eavesdropper Eve might have. The technical implementations of error correction and privacy amplification are beyond the scope of this thesis, which focuses on the proof-of-principle experimental demonstrations of various QKD protocols in different quantum channels.

1.3.1 BB84 protocol

Created in 1984 by Charles Bennett and Gilles Brassard, the BB84 protocol is the first QKD protocol to be proposed [3]. The underlying simplicity of BB84 has made it an ideal candidate for lab and field tests as a prepare-and-measure protocol, wherein Alice prepares quantum states and then Bob measures them. As per the original proposal, we will use polarization to encode information, and then extend to higher dimensions. Assuming that Alice and Bob wish to establish a random secret key, the BB84 protocol goes as follows:

1. Alice and Bob decide on a pair of *mutually unbiased bases* (MUB) with which to encode information. For example, using polarization, they may choose $\mathcal{M}_0 = \{|H\rangle, |V\rangle\}$ and $\mathcal{M}_1 = \{|A\rangle, |D\rangle\}$.

These two polarization bases are mutually unbiased as the projection of a state from $\mathcal{M}_0$ onto a state from $\mathcal{M}_1$ yields the probability of 1/2, and vice versa. In general, for a set of j states $|\alpha_i\rangle_j$ in a basis $\mathcal{M}_i$, this condition is written as,

$$|_j\langle\alpha_i|\alpha_{i'}\rangle_{j'}|^2 = \begin{cases} \delta_{jj'}, & \forall i = i' \\ 1/d, & \forall i \neq i' \end{cases}. \tag{1.8}$$

Here, d is the dimension of encoding Hilbert space ($d = 2$ for polarization). It is to be noted that there are $d + 1$ MUB in a d-dimensional space, where d is a power of a prime number; however, two MUB can always be formed for an arbitrary dimension [27]. For example with OAM states in dimension d, beyond the logical basis of $|\psi_k\rangle \in \{0, 1, 2...d\}$, one can construct a second MUB by taking the discrete Fourier transform, $|\phi_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i2\pi jk/d} |\psi_k\rangle$. Continuing on,

2. Alice and Bob agree on the encoding alphabet for each state in each MUB. For example, they might choose that $|H\rangle$ and $|A\rangle$ correspond to "0", whereas $|V\rangle$ and $|D\rangle$ correspond to "1". Here, "0" and "1" are classical bits.

3. Alice randomly chooses a classical bit ("0" or "1"), then randomly chooses a MUB ($\mathcal{M}_0$ or $\mathcal{M}_1$) to accordingly prepare a photon with the correct polarization.

4. Alice sends her prepared photon over an untrusted quantum channel to Bob.

5. Bob randomly chooses a MUB ($\mathcal{M}_0$ or $\mathcal{M}_1$) to measure the photon sent to him in and records the result ("0" or "1" depending on which state the photon ended up being projected onto).

After Alice and Bob have exchanged N photons, they are finished using the quantum channel, and call each other on an authenticated classical channel. In order to distill their shared random secret key, they need to sift out the "wrong" photons: if Bob measured in a different basis than what Alice prepared in, then his results are completely random since the different bases are mutually unbiased (equally probable to get "0" or "1"). However, if Bob measured in the same MUB as Alice prepared in, then his results yields with 100% certainty the same classical bit as Alice. Thus, in an ideal world, the final step to the BB84 protocol is,

6. For each photon sent, Alice and Bob *only* tell each other which MUB they respectively prepared and measured in, sifting out the rest of the photons. For an infinitely long key, 1/2 of the photons are sifted out. The remaining string of classical bits now corresponds to a shared secret key between Alice and Bob.

As mentioned, if this was an ideal world, then Alice and Bob would have exactly the same shared secret key. Unfortunately, there is always the possibility of an eavesdropper, Eve, trying to gain information about Alice and Bob's shared secret key. More often than not the quantum channel is just noisy; however, all factors that contribute to a non-ideal channel are attributed to Eve, who has complete access and power over the quantum channel. The consequence of this is that the final key may contain errors due to perturbations caused by interactions from an eavesdropper. For example, Eve could try and perform a cloning-attack to copy the photons being sent, or an intercept-resend attack to directly read the information [28]. However, by the no-cloning theorem, it is impossible for Eve to perfectly clone an arbitrary quantum state and thus she introduces errors to the sent states. Additionally, if she tries to directly read the information by projecting it onto one of the MUB, she has a 50% chance of correctly guessing which MUB Alice prepared in since Alice's MUB were randomly chosen. Thus, the other half of the time, Eve is projecting the sent photon into the wrong basis and Bob will register a random outcome, aka an error. An additional step is therefore required,

7. By using the classical channel, Alice and Bob sacrifice a portion of their shared secret key to compare the key values and analyze what the quantum bit error rate (QBER), i.e. how different are their respective keys. If the QBER is above $Q^{(2)}_{\text{threshold}} = 11\%$, their key is compromised and they must abort the protocol and try again.

This $Q^{(2)}_{\text{threshold}} = 11\%$ is the characteristic error threshold for a 2-dimensional BB84 protocol in which no positive secret key rate, K, can be produced (in the infinite key limit) as a result of too many errors from information leakage to Eve. For a general dimension d, the secret key rate as a function of error rate Q is given analytically as [29],

$$K^{(d)}(Q) = \log_2(d) - 2h^{(d)}(Q), \tag{1.9}$$

where,

$$h^{(d)}(Q) = -Q\log_2\left(\frac{Q}{d-1}\right) - (1-Q)\log_2(1-Q), \tag{1.10}$$

is the d-dimensional Shannon entropy [3]. In particular, $K^{(2)}(Q^{(2)}_{\text{threshold}} = 0.11) = 0$; therefore, it is impossible for Alice and Bob to produce a secure key.

For a high-dimensional BB84 protocol in dimension d, the base structure of the protocol remains the same. The only aspects that differ is that the MUB $\mathcal{M}_0$ and $\mathcal{M}_1$ now have d states in them instead of 2, and the error threshold increases according to when $K^{(d)}(Q^{(d)}_{\text{threshold}}) = 0$. In particular, $Q^{(3)}_{\text{threshold}} = 15.95\%$ and $Q^{(4)}_{\text{threshold}} = 18.93\%$, which will be relevant for the following chapters.

1.3.2 Other protocols

An extension to the BB84 protocol is when all $d+1$ MUB are utilized, known as the *six-state protocol* for $d = 2$ or (d+1)-MUB protocol in arbitrary d [30]. The sifting efficiency for this type of protocol is now $1/(d+1)$ instead of $1/d$. The (d+1)-MUB protocol is essentially the same as the original BB84 protocol, except now Alice and Bob randomly choose between the $d+1$ MUB. For the case of polarization, the third MUB is $\mathcal{M}_2 = \{|L\rangle, |R\rangle\}$. The error threshold hold increases slightly (e.g. 12.6% for $d = 2$) when using this protocol.

Chapter 2

Structured light and vortex fibres

This chapter is based on the following paper:

1. **A. Sit**, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi, "Quantum cryptography with structured photons through a vortex fiber," *Optics Letters* **43**, 4108 (2018).

DOI: https://doi.org/10.1364/OL.43.004108

2.1 Structured light

Defined here as the combination of two different photonic degrees of freedom, here taken to be polarization and OAM, *structured light* and *structured photons* can be used to realize high-dimensional states of light [31]. They thus have the advantage of increased information capacity and error tolerance in quantum communication. These states of light often possess a complex polarization distribution with a certain topology or symmetry. A first notation to write structured photons is $|\Pi, \ell\rangle$, where the first index in the ket is the polarization ($\Pi = H, V, A, D, L, R$) and the second is the OAM value. For example, a radially polarized beam—part of the vector vortex beam class whose spatial polarization distribution only posseses linear states—can be written as,

$$|\text{radial}\rangle = \frac{1}{\sqrt{2}} \left(|R, 1\rangle + |L, -1\rangle \right), \tag{2.1}$$

A second notation that can be used to describe these structured beams is to use the SAM instead of polarization as $|\ell\rangle_\pi$, where now the index in the ket is the OAM value and the subscript is the SAM value (either $\pi = -1, 1$). A radially polarized beam can thus also be written as,

$$|\text{radial}\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_{-1} + |-1\rangle_1\right). \tag{2.2}$$

This second notation is used in the work of this chapter, whereas the first notation is used in Ch. 3.

2.1.1 Generation

Polarization states can be prepared with a polarizer and a sequence of half- and quarter-wave plates [32]. OAM states can be generated in a variety of manners, including spiral phase plates, cylindrical lenses, and holographic methods [33, 34, 20]. A state of light possessing both polarization and OAM can be created by cascading the appropriate polarization and OAM generation optics. To structure arbitrary superpositions of these states of light, the brute force approach method of superposing them in an interferometric manner is effective, though not necessarily compact or stable.

For certain classes of structured states—such as a radially polarized beam and states relevant for this chapter—patterned liquid crystal devices are an efficient solution [35]. These home-fabricated devices consist of two glass plates coated with a polymer which is aligned to have a specific topology q (half-integer); liquid crystals are injected between the plates, which naturally align to the orientation of the polymer [36]. A voltage can be run across the plate in order to change the effective retardance of the liquid crystals, which can thus tune the device for different wavelengths. These types of patterned birefringent elements are called q-plates and have the ability to couple spin to orbital angular momentum under the following transformations:

$$|L, \ell\rangle \xrightarrow{q-plate} |R, \ell + 2q\rangle, \tag{2.3}$$

$$|R, \ell\rangle \xrightarrow{q-plate} |L, \ell - 2q\rangle. \tag{2.4}$$

Additionally, since q-plates are linear devices, if a superposition of left- and right-hand circlular polarizations are incident on it, an inseparable state of polarization and OAM is created. For example, we can create a radially polarized beam by passing a

horizontally polarized Gaussian beam through a $q = 1/2$ plate. A typical generation setup consists of a Gaussian beam passing through a sequence of waveplates (to control the polarization incident on the q-plate) and then the q-plate itself.

2.1.2 Detection and characterization

In order to detect a structured state of light which was generated using a q-plate, it is simply passed through the reverse sequence of q-plate and waveplates to "remove" the OAM component—also known as phase-flattening—such that $\ell = 0$ for all polarization components. This phase-flattened mode can now be coupled to a single-mode fiber (SMF) and the result recorded at a power metre or single photon detector. This is essentially projecting the incoming state onto itself and recording the overlap, or simply a click if at the single photon level.

Polarization tomography can also be performed to measure the quality of the structured mode. This method consists of analyzing the six main polarization components (H, V, A, D, L, R), i.e. the three polarization MUB. Note, this is an overcomplete set of measurements—four measurements are sufficient to determine an arbitrary polarization state. Since we are dealing with spatially structured polarization distributions, a camera is used to record intensity images for each polarization state. Point-by-point, the Stokes parameters can be calculated and a spatial polarization distribution can be reconstructed [37]. The overlap between this reconstructed polarization distribution and the theoretical one can be calculated to give a form of fidelity of the structured mode. If the exact polarization and OAM content of a general structured beam is desired to be known, a combination of polarization and OAM tomography should be performed.

2.2 Optical vortex fibres

Conventional optical fibres that are most commonly used for coupling light, e.g. single- or multi-mode fibres, have a step-index profile where the core has a higher refractive index than the cladding material. This forms a dielectric waveguide that guides modes via total internal reflection. This section follows the arguments from [38, 39]. In the scalar approximation, these guided modes are known as the "linearly polarized" (LP_{lm}) modes, where the intensity profile of a given mode has $2l$ field maxima in the azimuthal direction and m field maxima in the radial direction. For example,

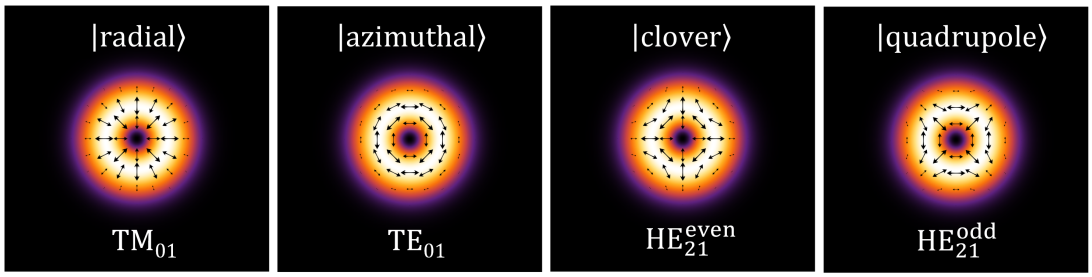

Figure 2.1: **Vector vortex modes**. The polarization distributions for the vector solutions of the LP_{11} mode group of an optical fibre. These are a class of structured modes that are superpositions of $|\ell = \pm 1\rangle$ and different circular polarizations.

the fundamental LP_{01} mode resembles a Gaussian. Each mode has a particular effective refractive index n_{eff}, i.e. how the mode propagates through the fibre. Each scalar LP mode corresponds to a group of vector vortex mode solutions; for example, the full vector solutions of LP_{01} are the HE^{x}_{11} and HE^{y}_{11} modes, which are orthogonally polarized Gaussian-like modes with the same n_{eff}.

The vector vortex solutions of higher order LP mode groups begin to resemble structured states of light. In particular relevant to the experiment in this chapter, LP_{11} contains the TM_{01} (radial polarization), $HE^{\text{even, odd}}_{2,1}$ (clover and quadrupole polarization), and TE_{01} (azimuthal polarization) modes, as shown in Fig. 2.1. We can reformulate these modes in terms of SAM and OAM using the second notation from Sec. 2.1,

$$\text{HE}^{\text{even}}_{2,1} \pm i\text{HE}^{\text{odd}}_{2,1} = |\ell = \pm 1\rangle_{\pm 1}\,, \tag{2.5}$$

$$\text{TM}_{01} = |\text{radial}\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_{-1} + |-1\rangle_{1}\right), \tag{2.6}$$

$$\text{TE}_{01} = |\text{azimuthal}\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_{-1} - |-1\rangle_{1}\right). \tag{2.7}$$

Whereas $HE^{\text{even}}_{2,1}$ and $HE^{\text{odd}}_{2,1}$ are degenerate in n_{eff}, TM_{01} and TE_{01} are not. However, in conventional fibres, the difference Δn_{eff} between $HE^{\text{even, odd}}_{2,1}$, TM_{01}, and TE_{01} is so negligible that there is intermodal mixing over a long fibre. A conventional fibre is thus not suitable as a quantum channel for the stable propagation of OAM states of light. Much like in polarization-maintaining fibres (PMF), if a strong birefringence between the LP_{01} modes is present ($\Delta n_{\text{eff}} > 10^{-4}$), then the orthogonal polarizations will not couple and remain stable over long fibre distances. This concept can be applied to designing a fibre that stably propagates OAM states of light. In particular, if the refractive index profile of the fibre core is structured to have a ring of higher index

around the core instead of just a step, then the near-degeneracy of the three vector solutions in the LP_{11} mode group is lifted ($\Delta n_{\text{eff}} > 10^{-4}$). Thus, the $HE_{2,1}^{\text{even, odd}}$ modes won't couple to the TM_{01}, and TE_{01} modes, and we can stably propagate arbitrary superpositions of $|\ell = \pm 1\rangle_{\pm 1}$. These types of fibre are known as vortex or ring fibres. Similar principles apply to vortex fibres that support more OAM modes.

2.3 Heralded single-photon source

In quantum cryptography, it is ideal to use a single-photon source, i.e. one that predictably creates a $n = 1$ Fock state on demand. Unfortunately, these do not quite exist yet. However, it is not secure to simply use a strongly attenuated laser beam (weak coherent state), since the photon statistics still have $n > 1$ components by Poissonian statistics, which Eve could possibly use to gain information through a photon number splitting attack [40]. Therefore, an additional protocol, known as the *decoy state protocol*, is run on top of the chosen QKD protocol, which randomly varies the average photon number of each state sent, to counteract this [41].

For our proof-of-principle experiments, we opt to use a *heralded* single-photon source instead. This type of photon source generates pairs of photons via a process known as spontaneous parametric down-conversion (SPDC) [42]. Here, a blue pump photon (λ_p) is incident on a $\chi^{(2)}$ nonlinear crystal, e.g. periodically poled potassium titanyl phosphate (ppKTP), which splits the blue photon into two red photons (a signal λ_s and idler λ_i photon). The energy and momentum must be conserved in this process such that $1/\lambda_p = 1/\lambda_s + 1/\lambda_i$ and $\vec{k}_p = \vec{k}_s + \vec{k}_i$. Depending on the phase-matching conditions—controlled by the tilt or the temperature of the crystal—the wavelengths of the signal and idler can be made to be degenerate or non-degenerate. The signal and idler photons are correlated in all degrees of freedom. However, for our experiments, we wish to encode information on the signal and simply use the idler for timing purposes, i.e. to trigger a single-photon detector thus heralding the presence of the signal. Of note, the idler photon is kept in a Gaussian state throughout all experiments; it thus contains no information of the signal photon. Detecting coincidence events in this manner (the near simultaneous detection of two events from two separate detectors) eliminates the problem of multi-photon statistics, and is therefore secure against a photon number splitting attack.

Optics Letters

Quantum cryptography with structured photons through a vortex fiber

Alicia Sit,[1,*] Robert Fickler,[1] Fatimah Alsaiari,[1] Frédéric Bouchard,[1] Hugo Larocque,[1] Patrick Gregg,[2] Lu Yan,[2] Robert W. Boyd,[1] Siddharth Ramachandran,[2] and Ebrahim Karimi[1]

[1]Department of Physics, University of Ottawa, Advanced Research Complex, 25 Templeton Street, Ottawa, Ontario K1N 6N5, Canada

[2]Department of Electrical and Computer Engineering, 8 St. Mary's St., Boston University, Boston, Massachusetts 02215, USA

*Corresponding author: asit089@uottawa.ca

Received 13 June 2018; revised 20 July 2018; accepted 26 July 2018; posted 27 July 2018 (Doc. ID 335026); published 17 August 2018

Optical fiber links and networks are integral components within and between cities' communication infrastructures. Implementing quantum cryptographic protocols on either existing or new fiber links will provide information-theoretical security to fiber data transmissions. However, there is a need for ways to increase the channel bandwidth. Using the transverse spatial degree of freedom is one way to transmit more information and increase tolerable error thresholds by extending the common qubit protocols to high-dimensional quantum key distribution (QKD) schemes. Here we use one type of vortex fiber where the transverse spatial modes serves as an additional channel to encode quantum information by structuring the spin and orbital angular momentum of light. In this proof-of-principle experiment, we show that two-dimensional structured photons can be used in such vortex fibers in addition to the common two-dimensional polarization encryption, thereby paving the path to QKD multiplexing schemes.

OCIS codes: (060.2330) Fiber optics communications; (060.5565) Quantum communications; (270.5568) Quantum cryptography.

https://doi.org/10.1364/OL.43.004108

Implementing quantum cryptography is necessary for improving the security of sensitive information. Following the development of the first quantum key distribution (QKD) protocol by Bennett and Brassard in 1984 (BB84) [1], much progress has been made in transmitting information farther and faster. Experimentally, it is important to investigate realizations of different quantum channels for various real-world scenarios that require the security of quantum cryptography. Free-space channels, in particular between ground stations and satellites, satisfy the need for long distance, global connections where optical fibers are not an option [2–5]. On a shorter length scale, optical fiber quantum channels become favorable as they do not have problems with line-of-sight, weather, or time of day [6]. Indeed, intra-city optical fiber networks have been retrofitted to transmit quantum signals [7], and commercially available fiber systems are now readily available for secure data encryption [8].

In general, a challenge that quantum channels face is the capacity to send more information. One solution is to encode information using multiple photonic degrees of freedom, for example, spin angular momentum (SAM) and orbital angular momentum (OAM). Light carrying OAM possesses a phase term of $e^{i\ell\varphi}$, where ℓ is an integer and φ is the transverse azimuthal coordinate, leading to ℓ helical wavefronts and doughnut-like intensity distributions. The OAM Hilbert space is unbounded, corresponding to a theoretically infinite encoding alphabet [9,10]. In practice, the number of spatial modes that can be transmitted through a quantum channel is constrained by the numerical aperture of the system but, nonetheless, are useful for high-dimensional protocols [11,12]. We refer to photons encoded using multiple photonic degrees of freedom as *structured*, since the coherent combination of SAM and OAM creates spatially varying transverse polarization distributions [13]. Thus, the amount of transmitted information can be doubled for a fixed ℓ. QKD with OAM and structured photons has so far been successfully demonstrated in free space [14–16].

Several varieties of specialty fibers exist that can transmit OAM modes, including vortex or rings [17], twisted photonic crystals [18], inverse-parabolic graded indices [19], and air-core fibers [20,21]. The vortex fibers, characterized by rings of higher refractive indices in their transverse profiles, have been shown to preserve entanglement [22], as well as terabit per second transmission rates through OAM multiplexing in classical communication schemes [23]. Recently, an air-core fiber which supports multiple OAM modes was used to implement a real-time high-dimensional decoy state protocol [24]. Such types of OAM supporting fibers provide an in-line alternative for high-dimensional protocols compared to fibers with multiple cores [25–27].

In QKD, it is important for the transmitted states to be indistinguishable in time, or not to decohere with propagation. Such effects would lead to errors in the obtained measurement outcomes, which cannot be distinguished from the effect of an eavesdropper (Eve) on the quantum link. Thus, the two parties, colloquially named Alice and Bob, would not be able to establish a secure key. On their own, different OAM states of light are distinguishable after propogation through ordinary fibers. One way that these OAM supporting fibers maintain the required

indistinguishability is by using a particular set of structured modes of light combining OAM and SAM, the advantage being that these modes could be spatial-division multiplexed with the fundamental mode, which could be encoded with polarization. In this Letter, we present a characterization of one such vortex fiber, and show that it could be used for QKD in a two-dimensional BB84 protocol encoding quantum information on heralded single photons with spatially structured polarization distributions, in addition to encoding in polarization of the fundamental mode. This opens up the possibility to use structured photon fiber networks to increase the classical bandwidth during quantum secure transmission of information.

The vortex fiber used in this Letter is a solid core vortex fiber which supports photons with $\pm\hbar$ units of OAM [17,28], where $\hbar$ is the reduced Planck constant. The operating principle of this type of vortex fiber is that its transverse profile contains a ring of higher refractive index, which resembles the OAM mode shape and acts as a guide for OAM-encoded photons. In additon to having two orthogonal OAM states, photons can simultaneously be either left- or right-handed circularly polarized with $\pm\hbar$ units of SAM. We will write structured photons with the notation $|\ell\rangle_\pi$, where π is the SAM value and ℓ is the OAM value. We will further use the convention that $\pi = +1$ and $\pi = -1$ correspond to left- and right-handed circular polarizations, respectively. In the case of this vortex fiber, the states with the same handedness, $\{|1\rangle_1, |-1\rangle_{-1}\}$, are degenerate in time with each other, i.e., possess identical group velocities in the fiber, but non-degenerate with states of opposite handedness $|1\rangle_{-1}$, $|-1\rangle_1$, and the other fundamental modes of the fiber [29]. Therefore, we take advantage of the states with the same handedness for QKD protocols with this vortex fiber. In particular, for the BB84 protocol, we form two mutually unbiased bases (MUBs), i.e., no information is gained about the states in one basis by making measurements in the other basis, using the aforementioned states, $\mathcal{M}_0 = \{|1\rangle_1, |-1\rangle_{-1}\}$, and $\mathcal{M}_1 = \{(|1\rangle_1 + |-1\rangle_{-1})/\sqrt{2}, (|1\rangle_1 - |-1\rangle_{-1})/\sqrt{2}\}$. This Letter provides a proof-of-concept test that it is feasible to use structured photons, as qubits, through vortex fiber quantum channels which, in principle, can be extended to higher dimensions.

In our experiment (see Fig. 1), we generate heralded single photons via spontaneous parametric downconversion using a 5 mm long periodically poled potassium titanyl phosphate (ppKTP) crystal pumped with a 405 nm diode laser (200 mW). The photon pairs (signal $\lambda_s = 775$ nm and idler $\lambda_i = 850$ nm) are separated via a dichroic mirror (DM), coupled to different single-mode fibers (SMFs). We herald our single photons by detecting the partner photon at an avalanche photodiode (APD) with a dark count rate of less than 50 Hz, which triggers a coincidence counter. The single photon, on which we will imprint information, is first sent to a pair of diffraction gratings and a slit that acts as a narrow bandpass filter, not shown in Fig. 1. A first diffraction grating and lens perform a Fourier transform so that the spectrum is given at the focus. A moveable slit with an adjustable slit width can thus be placed at the focus to precisely choose the desired wavelength and bandwidth. A wavelength of approximately 775 ± 0.75 nm is chosen for the signal photon, since the fiber was designed to operate at this wavelength. A second lens and diffraction grating perform the inverse transformation to recombine the frequencies, subsequently coupled back into SMFs. This adjustable filter is approximately 10% efficient. With a 5 ns coincidence window, our heralded single-photon source has a rate of approximately 4500 coincidences per second after the filter. However, we note that this is not a fundamental constraint, rather a technical deficiency of our setup.

In the preparation stage, Alice prepares the signal photon into a state from either $\mathcal{M}_0$ or $\mathcal{M}_1$ using a sequence of wave plates and a patterned liquid crystal device known as a q-plate, where $q = \ell/2$ is the topological charge of the liquid crystals. Such a device coherently couples SAM to OAM [30,31]. To generate structured photons with $|\ell| = 1$, a $q = 1/2$ plate is utilized, which naturally produces states with the opposite handedness; a half-wave plate is placed after the q-plate to create states with the same handedness, such as in $\mathcal{M}_0$ and $\mathcal{M}_1$. The theoretical phase and polarization distributions of each state are displayed in Fig. 2(a). We note that the modes in MUB $\mathcal{M}_0$ possess uniformly circular polarization distributions, whereas the superposition MUB $\mathcal{M}_1$ consists of spatially varying polarization distributions of only linear polarizations, i.e., structured modes of light. In order to compensate for birefringent coupling induced by the fiber, a set of compensation wave plates [29,32] (not shown in Fig. 1), consisting of two

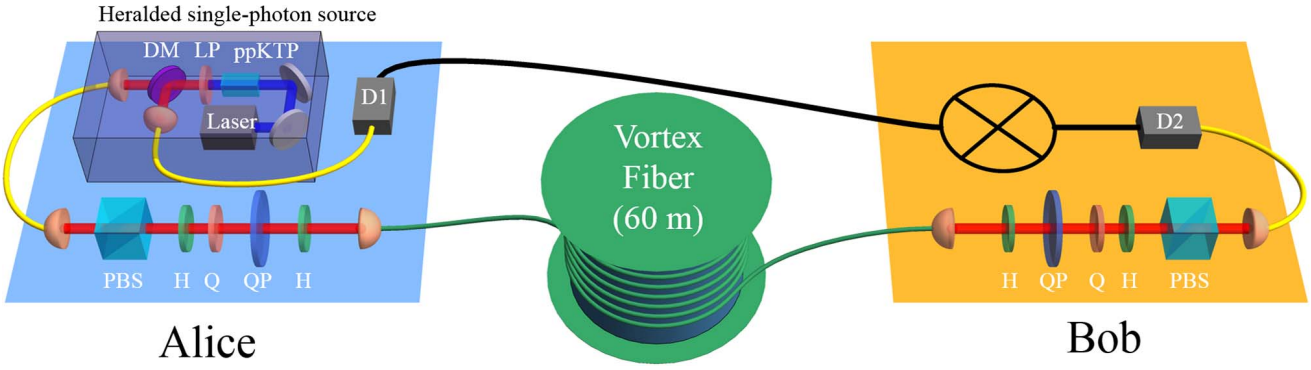

Fig. 1. Sketch of the experimental setup. Non-degenerate photon pairs (signal $\lambda_s = 775$ nm, idler $\lambda_i = 850$ nm) are produced by spontaneous parametric downconversion from a 5 mm long ppKTP crystal pumped by a 200 mW 405 nm pump diode laser; they are then split on a dichroic mirror (DM). Alice prepares the heralded single photon in a particular quantum state with a sequence of wave plates and a $q = 1/2$ plate (QP), and then sends it to Bob through the vortex fiber (quantum channel). Bob performs a particular measurement with a reverse sequence of wave plates and $q = 1/2$ plate, recording a coincidence event between the result (D2) and the heralding trigger photon (D1). H, half-wave plate; Q, quarter-wave plate; LP, long-pass filter; PBS, polarizing beam splitter.

half-wave and two quarter-wave plates, is placed before Alice's q-plate in order to have control of the relative phases between the states in $\mathcal{M}_0$ and $\mathcal{M}_1$.

The structured photons that Alice creates are then coupled into a 60 m long vortex fiber, acting as the untrusted quantum channel, and sent to Bob. There are approximately 50% losses after coupling to the vortex fiber. Bob's setup is similar to Alice's with a mirror sequence of wave plates and $q = 1/2$ plate. A subsequent coupling into an SMF and a detection by an APD enables Bob to project the single photons onto one of the four possible states from the two MUBs, because his system acts as a mode filter: if Bob projected onto the same state as the one Alice sent, then his wave plates and q-plate phase-flatten the mode back to the fundamental, which exclusively couples to the SMF. Bob records the coincidence events between the measured results and the heralding trigger photon at the coincidence logic box. Overall, the system is approximately 9% efficient, with several hundred heralded single photons per second detected after passing through the experimental setup.

We first test the OAM mode propagation through the vortex fiber using a simulator laser diode at 808 ± 0.5 nm by comparing the modes before and after the vortex fiber. Though slightly above the operating wavelength of the fiber, the difference in results should be negligible. The experimentally measured spatial polarization distributions, shown in Figs. 2(b) and 2(c), respectively, were reconstructed using polarization tomography [33]. This is achieved by projecting the transmitted modes onto horizontal, vertical, diagonal, anti-diagonal, left-hand circular, and right-hand circular polarizations using a quarter-wave plate, half-wave plate, and polarizing beam splitter. The six resulting intensity distributions, recorded with a CCD, are used to calculate the Stokes parameters at each point in the mode, thus reconstructing the experimental spatial polarization distribution. A first visual inspection shows that modes after the vortex fiber still resemble the modes that were sent in. By calculating the overlap between the theoretical and experimental polarization distributions, average fidelities of the modes before and after the vortex fiber are $98.8\% \pm 0.3\%$ and $93\% \pm 2\%$, respectively.

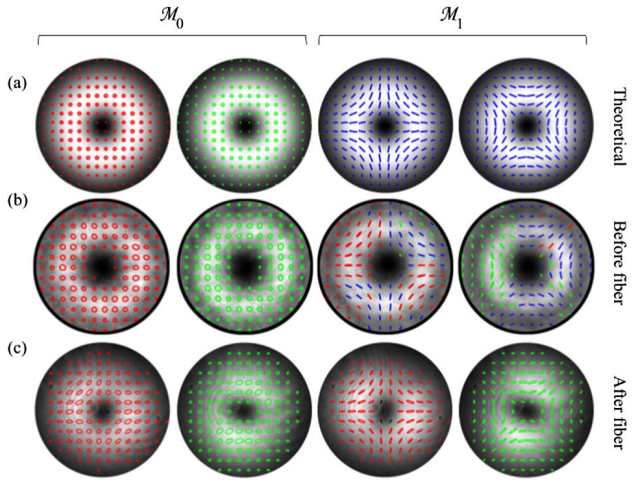

Fig. 2. Intensity (grayscale image) and polarization (overlaid colored pattern) distributions of the vortex fiber modes: (a) theoretical representation, experimentally reconstructed distributions (b) before and (c) after the vortex fiber. The states in MUBs $\mathcal{M}_0$ and $\mathcal{M}_1$ are shown in the first two and last two columns, respectively. The ellipses are colored according to handedness (left-handed = green; right-handed = red); linear states are colored blue, with a tolerance of being 10% elliptically polarized for the experimental plots.

Next, we characterize our vortex fiber more quantitatively as a quantum channel for QKD by methodically generating each state from $\mathcal{M}_0$, $\mathcal{M}_1$, and projecting them onto each state from $\mathcal{M}_0$, $\mathcal{M}_1$. The resulting normalized heralded single-photon counts form a probability-of-detection matrix. The experimental probability-of-detection matrices for the two MUBs, $\mathcal{M}_0$ and $\mathcal{M}_1$, in dimension 2 are shown in Fig. 3(a). In the BB84 protocol with qubits, such as here, the maximum tolerable quantum bit error rate (QBER) threshold, below which a positive secret key rate is produced, is $Q^{\text{th}} = 11\%$. We measured the QBER, calculated as the average of the errors after sifting, to be $Q^{|\ell|=1} = 8.6\%$, which is below the threshold. The secret key rate per sifted photon can be calculated from the QBER as $R(Q) = 1 - 2h(Q)$, where $h(\cdot)$ is the Shannon entropy in dimension 2. Our corresponding secret key rate is 0.15 bits per sifted photon.

We can see from the measurements that when Alice and Bob choose different bases there is crosstalk between the different modes. This is reflected in the mode profiles after propagation through the fiber, giving rise to asymmetric intensity profiles and elliptical polarization distributions in Fig. 2. These errors in the mode structure caused by intermodal coupling in the fiber correspond to a higher QBER, thus requiring more post-processing, such as error correction and privacy amplification [34], leading to lower key rates. However, as stated earlier the vortex fiber also allows for simultaneous performing of polarization-only encoding using a BB84 protocol via spatial-division multiplexing and by encoding the fundamental mode of the fiber, i.e., $\ell = 0$. The MUBs in this case are defined to be $\mathcal{M}_0' = \{|0\rangle_1, |0\rangle_{-1}\}$ and $\mathcal{M}_1' = \{(|0\rangle_1 + |0\rangle_{-1})/\sqrt{2}, (|0\rangle_1 - |0\rangle_{-1})/\sqrt{2}\}$. The measured probability-of-detection matrix is shown in Fig. 3(b). The corresponding QBER of this polarization BB84 scheme is $Q^{\ell=0} = 1.2\%$, with a secret key rate of 0.81 bits per sifted photon. This possibility for multiplexing enables the parallel transmission of more information. An interferometer which sorts based on the total angular momentum of the state [35], or a generalized angular momentum sorter [36], could be used to demultiplex the modes efficiently.

In conclusion, in this Letter, we have explored how structured photons could be used to implement QKD within an

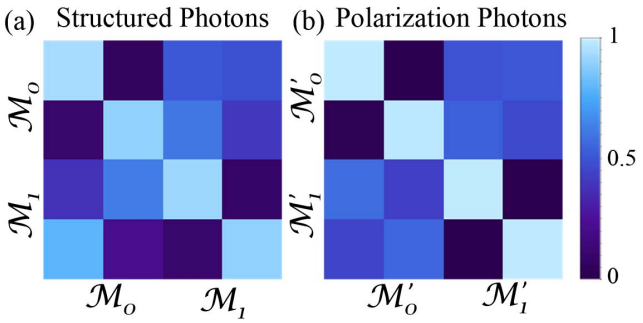

Fig. 3. Experimental probability-of-detection matrices for BB84 schemes using (a) structured photons and (b) polarization. The labels on the left and bottom of the matrix represent the states sent by Alice and projected on by Bob, respectively. QBERs of $Q^{|\ell|=1} = 8.6\%$ and $Q^{\ell=0} = 1.2\%$ are measured for the cases of structured and polarization photons, respectively.

OAM-conserving vortex fiber in a proof-of-concept experiment. The vortex fiber used conserves OAM of $|\ell| = 1$, and modes with the same handedness for both OAM and SAM are indistinguishable with propogation in the fiber; thus, they can serve as additional quantum channels. The obtained QBER rates for the encoding using structured photons, as well as polarization-only encoded photons, are below the theoretical threshold in two dimensions for BB84 and, as such, can be used for establishing a secure key between two parties that are 60 m apart. Although this distance might seem rather short at first sight, network structures within buildings or server infrastrcutures could benefit already from these shorter distances. Future investigations would include studying how errors scale with fiber length and new fibers that support more values of ℓ so that high-dimensional QKD protocols could be employed [12,37]. These types of fibers could create high-dimensional quantum fiber networks, in conjunction with other modes of the fiber, such as the fundamental, which could increase the transmission bandwidth and tolerable error thresholds for more robust and secure quantum communications.

Funding. Natural Sciences and Engineering Research Council of Canada (NSERC); Canada Research Chairs; Canada Excellence Research Chairs, Government of Canada (CERC); Canada Foundation for Innovation (CFI); National Science Foundation (NSF) (ECCS-1610190); Office of Naval Research (ONR) (N00014-13-1-0627).

REFERENCES

1. C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Bangalore, India (1984), Vol. **175**, p. 8.
2. J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Science **356**, 1140 (2017).
3. J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Phys. Rev. Lett. **119**, 200501 (2017).
4. J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Nature **549**, 70 (2017).
5. S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, Phys. Rev. Lett. **120**, 030501 (2018).
6. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
7. R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, Nat. Photonics **10**, 676 (2016).
8. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
9. G. Molina-Terriza, J. P. Torres, and L. Torner, Nat. Phys. **3**, 305 (2007).
10. M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, Light Sci. Appl. **7**, 17146 (2018).
11. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
12. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
13. H. Rubinsztein-Dunlop, A. Forbes, M. V. Berry, M. R. Dennis, D. L. Andrews, M. Mansuripur, C. Denz, C. Alpmann, P. Banzer, T. Bauer, E. Karimi, L. Marrucci, M. Padgett, M. Ritsch-Marte, N. M. Litchinitser, N. P. Bigelow, C. Rosales-Guzmán, A. Belmonte, J. P. Torres, T. W. Neely, M. Baker, R. Gordon, A. B. Stilgoe, J. Romero, A. G. White, R. Fickler, A. E. Willner, G. Xie, B. McMorran, and A. M. Weiner, J. Opt. **19**, 013001 (2017).
14. 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, New J. Phys. **17**, 033033 (2015).
15. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Phys. Rev. Lett. **113**, 060503 (2014).
16. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, Optica **4**, 1006 (2017).
17. S. Ramachandran, P. Kristensen, and M. F. Yan, Opt. Lett. **34**, 2525 (2009).
18. G. K. L. Wong, M. S. Kang, H. W. Lee, F. Biancalana, C. Conti, T. Weiss, and P. St.J. Russell, Science **337**, 446 (2012).
19. B. Ung, P. Vaity, L. Wang, Y. Messaddeq, L. A. Rusch, and S. LaRochelle, Opt. Express **22**, 18044 (2014).
20. C. Brunet, P. Vaity, Y. Messaddeq, S. LaRochelle, and L. A. Rusch, Opt. Express **22**, 26117 (2014).
21. P. Gregg, P. Kristensen, and S. Ramachandran, Optica **2**, 267 (2015).
22. N. Bozinovic, S. Ramachandran, M. Brodsky, and P. Kristensen, *Frontiers in Optics 2011/Laser Science XXVII* (Optical Society of America, 2011), paper PDPB1.
23. N. Bozinovic, Y. Yue, Y. Ren, M. Tur, P. Kristensen, H. Huang, A. E. Willner, and S. Ramachandran, Science **340**, 1545 (2013).
24. D. Cozzolino, D. Bacco, B. D. Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenlowe, "Fiber based high-dimensional quantum communication with twisted photons," preprint arXiv:1803.10138 (2018).
25. J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. W. Sharpe, M. Lucamarini, B. Frölich, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **24**, 8081 (2016).
26. G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, Phys. Rev. A **96**, 022317 (2017).
27. Y. Ding, D. Bacco, D. Kjeld, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, npj Quantum Inf. **3**, 1 (2017).
28. L. Yan, P. Kristensen, and S. Ramachandran, *Conference on Lasers and Electro-Optics*, OSA Technical Digest 2016 (Optical Society of America, 2016), paper SM4P.3.
29. P. Gregg, M. Mirhosseini, A. Rubano, L. Marrucci, E. Karimi, R. W. Boyd, and S. Ramachandran, Opt. Lett. **40**, 1729 (2015).
30. L. Marrucci, C. Manzo, and D. Paparo, Phys. Rev. Lett. **96**, 163905 (2006).
31. H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R. W. Boyd, and E. Karimi, J. Opt. **18**, 124002 (2016).
32. R. Bhandari, Phys. Lett. A **138**, 469 (1989).
33. F. Cardano, E. Karimi, S. Slussarenko, L. Marrucci, C. de Lissio, and E. Santamato, Appl. Opt. **51**, C1 (2012).
34. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
35. J. Leach, J. Courtial, K. Skeldon, S. M. Barnett, S. Franke-Arnold, and M. J. Padgett, Phys. Rev. Lett. **92**, 013601 (2004).
36. H. Larocque, J. Gagnon-Bischoff, D. Mortimer, Y. Zhang, F. Bouchard, J. Upham, V. Grillo, R. W. Boyd, and E. Karimi, Opt. Express **25**, 19832 (2017).
37. F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, "Experimental investigation of quantum key distribution protocols with twisted photons," preprint arXiv:1802.05773 (2018).

Chapter 3

High-dimensional free-space QKD in an urban environment

This chapter is based on the following paper:

1. **A. Sit**, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günther, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica* **4**, 1006 (2017).

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

3.1 Constructing a free-space link across campus

In order to eventually distribute information globally, QKD protocols will be operated over satellite-to-ground (and vice versa) free-space links. However, not everyone has access to a satellite link; thus, it is more economical to build shorter point-to-point horizontal free-space links on the ground for testing purposes. For the work described in this chapter, we chose to construct a sender (Alice) and receiver (Bob) unit between the rooftops of Desmarais Hall and Thompson Residence, 300 m apart, on the University of Ottawa campus.

When creating a suitable outdoor work-space to host lasers, a plethora of optics, and sensitive single photon detectors, many non-scientific problems crop up. For

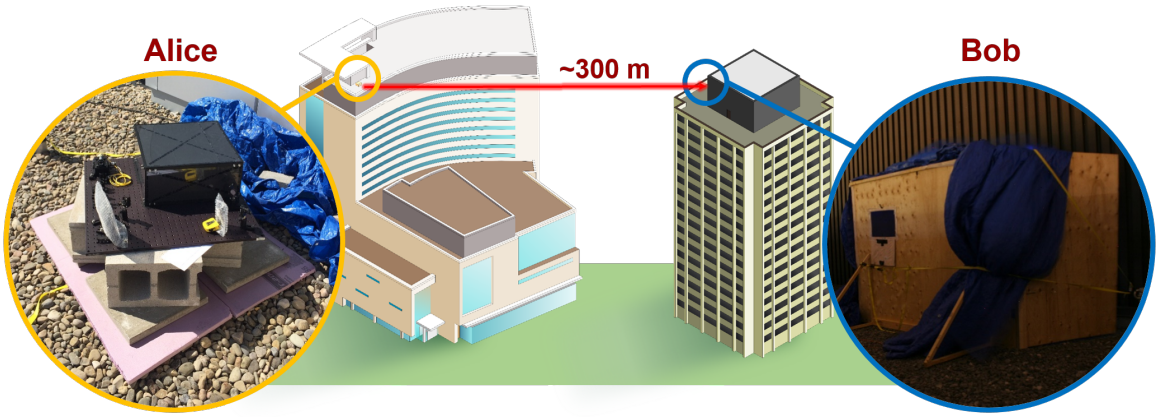

Figure 3.1: **Urban free-space link**. The sender (Alice) and receiver (Bob) units constructed on the rooftops of Desmarais Hall and Thompson Residence, respectively.

example, sheltering everything from the elements (rain, excess background light), and building a stable platform is required. For the latter problem, heavy cinder blocks, with a layer of stiff foam to cushion the aluminum breadboard, was chosen for the sender side on Desmarais. On the receiver side on Thompson, a tall (non-optical) table was chosen as there was a four-foot-high guard wall at the edge of the roof. For shelter, we built ply wood boxes around each unit, 4'×4'×2' and 8'×4'×6' for the sender and receiver, respectively (length × width × height), shown in Fig. 3.1. These boxes provided enough shelter from the rain and wind (though not bugs) to make working all night feasible (to eliminate excess background light).

3.2 Atmospheric turbulence

3.2.1 Fried parameter and structure constant

Perhaps the most readily observed consequence of atmospheric turbulence is the twinkling of the stars in the night sky, which are speckled and blurred upon a closer look through a telescope. This naturally occurring phenomenon is brought about by rapidly moving air cells with slightly different refractive indices, caused by small temperature variations; this is enough to cause slight deviations across a beam of light. The average size of these air cells (cell of constant refractive index) is described by the Fried parameter, r_0 [43]. Experimentally, r_0 can be measured by taking short exposure snapshots of a Gaussian laser beam: on the millisecond time scale, the laser

beam jitters (deflects) about. In a long exposure shot, the beam appears broadened. The average deflection angle $\bar{\beta}$ of the short exposure images is determined from the average beam displacement, $\bar{s}$, from the centre of the broadened beam,

$$\bar{\beta} = \tan\left(\frac{\bar{s}}{L}\right) \approx \frac{\bar{s}}{L}, \tag{3.1}$$

where L is the length of the free-space channel. Note that $\bar{\beta}$ is linear in $\bar{s}$, to first approximation, since $L \gg \bar{s}$ (metres vs millimetres). The corresponding Fried parameter of the free-space channel is then calculated as,

$$r_0 = 0.98\frac{\lambda}{\bar{\beta}}. \tag{3.2}$$

The larger the deflection angle, the smaller the Fried cell, which corresponds to a larger turbulence strength. On the other hand, the smaller the deflection angle, the larger the Fried cell, which means a smaller turbulence strength. This observation is consistent with physical intuition as a beam is more perturbed if there are more variations in the refractive index across its wavefront.

The strength of the turbulence is described by the atmospheric structure constant C_n^2 which is related to the fluctuations, both spatially and temporally, in the refractive index n. It can be defined as [44, 45],

$$C_n^2 = \langle [n(r_1 + r) - n(r_1)]^2 \rangle = D_n(r)\, r^{-2/3}, \tag{3.3}$$

where we take r to be the distance from a point r_1 in space, $D_n(r)$ is the structure function of the refractive index, and $\langle \cdot \rangle$ is the statistical average. We can also relate C_n^2 to experimental parameters such as the Fried parameter:

$$C_n^2 = \frac{r_0^{-5/3}}{0.432k^2L}, \tag{3.4}$$

where k is the wavenumber of the light. Another observation is that smaller wavelengths experience worse turbulence than longer wavelengths. Typical C_n^2 values are on the order of 10^{-18} $\mathrm{m}^{-2/3}$ for small turbulence effects to 10^{-14} $\mathrm{m}^{-2/3}$ for strong turbulence effects.

3.2.2 Data post-selection

As mentioned in Sec. 2.1.2, in order to measure structured states of light, Bob sends Alice's transmitted state through a set of waveplates and q-plate then couples the result to a SMF. This measurement scheme is sensitive to alignment as only a particular

k-vector will couple optimally. Inevitably, due to beam jitter and beam wandering caused by atmospheric turbulence, many results that Bob records are skewed and error-ridden. Of course, Bob does not know if the errors in his measurement are from atmospheric turbulence or Eve; thus, the QBER can be quite high. However, in our proof-of-principle experiment, a heralded photon scheme is used in which information is only encoded on the signal photon, and the idler photon is left as a Gaussian; the two photons co-propagate through the free-space link and thus experience the same turbulence effects. Bob can then not only record the coincidence events but also monitor the coupling efficiency of the idler photon. Since the idler photon is always a Gaussian, under ideal conditions, it should always optimally couple to the SMF; if its mode gets perturbed too much or moves off-axis (i.e. from atmospheric turbulence), then it will not couple as well to the SMF. The idler photon thus acts as a "target" to gauge beam wandering and jitter. This allows Bob to condition/post-select his coincidence measurements according to when the coupling efficiency of the idler photon is above a certain threshold.

Research Article Vol. 4, No. 9 / September 2017 / Optica 1006

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].

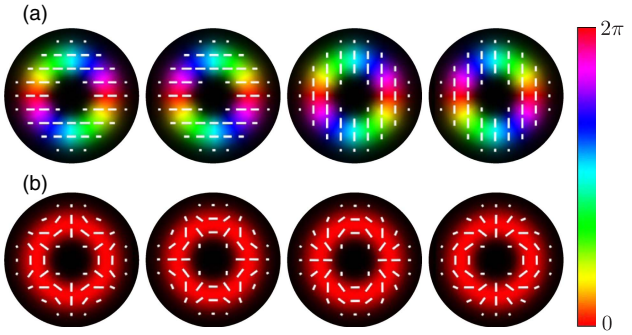

Fig. 1. Mode structure of mutually unbiased bases for $\ell = 2$. (a) $\{|\psi\rangle^i\}$ and (b) $\{|\varphi\rangle^j\}$ are examples of two bases of structured states of light, encoding in both polarization and OAM of $\ell = 2$. Each basis is orthonormal, and the two bases are mutually unbiased with 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

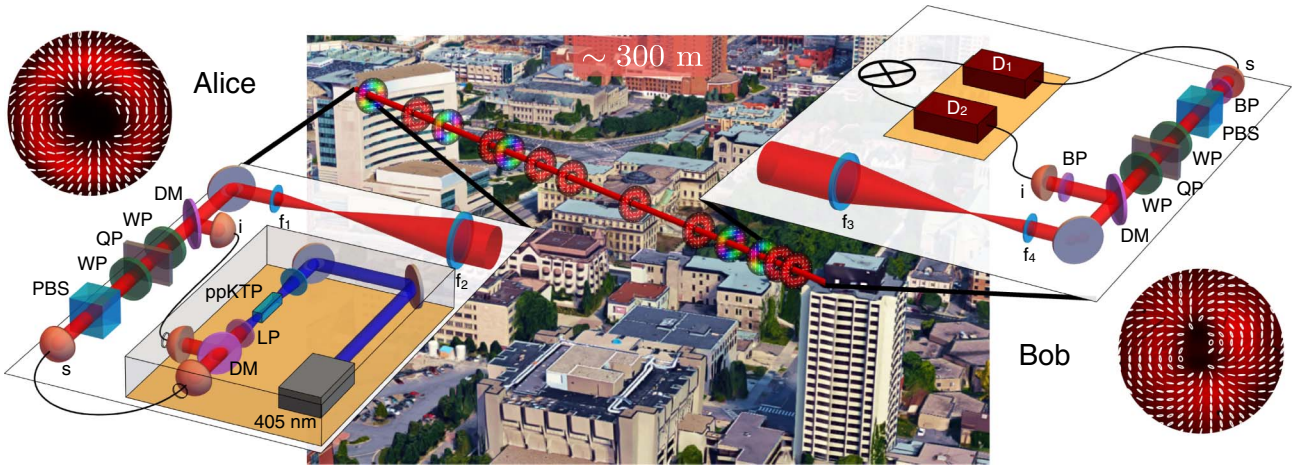

Fig. 2. Ottawa intracity quantum communication link. Schematic of the sender (left) with a heralded single-photon source (signal, *s*, and idler, *i*) and Alice's state preparation setup. Alice prepares a state from $\{|\psi\rangle^i\}$ or $\{|\varphi\rangle^j\}$ using a polarizing beam splitter (PBS), 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

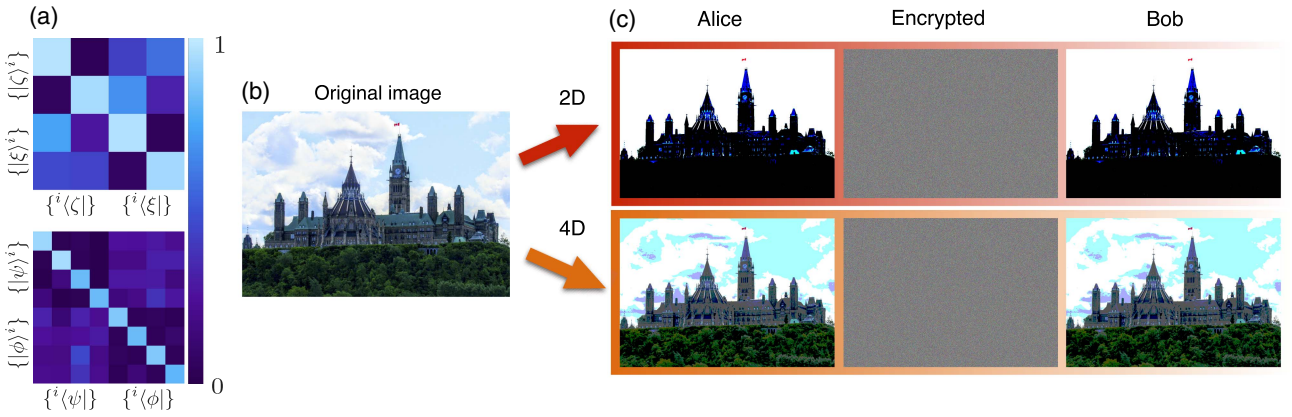

Fig. 3. Simulated encryption of an image with structured photons. (a) Experimentally measured probability-of-detection matrices, $P^{i,j} = |{}^i\langle\alpha|\beta\rangle^j|^2$, where $\alpha, \beta = \{\psi, \varphi\}$, for 2D (top row) and 4D (bottom row) structured photons with turbulence. These matrices have the corresponding bit error rates of $Q^{2D} = 5\%$ and $Q^{4D} = 11\%$, 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 $Q_0^{2D} = 11.0\%$, while it almost doubles to $Q_0^{4D} = 18.9\%$, 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^{4D}, 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 $Q^{4D} = 11\%$ with a secret key rate of $R^{4D} = 0.65$ 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 $Q^{2D} = 5\%$ and $R^{2D} = 0.43$ bits per sifted photon were obtained, respectively, using the target as compensation. Indeed, R^{4D} is larger than R^{2D}, 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^{4D}. An example of one of these nights is shown in the Supplement 1 with a calculated quantum bit error rate of $Q_{noisy}^{4D} = 27\%$ calculated from the probability-of-detection matrix. However, allowing for two-way classical communications, the tolerable error bit rate increases to $31.5\% > Q_{noisy}^{4D}$ 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).

Chapter 4

Quantum cryptography through water

This chapter is based on the following paper:

1. F. Bouchard, **A. Sit**, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics Express* **26**, 22563 (2018).

DOI: https://doi.org/10.1364/OE.26.022563

4.1 Optical properties of water

Unlike air which has a transmission window in the visible and infrared, the absorption spectrum of water is strongly absorbing in the infrared, with an optimal transmission window around 415-550 nm (blue-green wavelengths) [46]. Recall Beer-Lambert's law for a medium with absorption coefficient α (given in m^{-1}),

$$I = I_0 e^{-\alpha L}, \tag{4.1}$$

where I_0 and I are the intensities of light before and after propagating a distance L through the medium. A typical value for α in water at telecommunication wavelengths (1550 nm) is 17000 m^{-1}; this means that there will be 1% of the incident power

transmitted after only 300 μm! Wavelengths within the visible transmission window, on the other hand, can propagate 50-200 m.

4.2 Underwater turbulence

Much like in the free-space case where differences in temperature cause atmospheric turbulence (small variations in the refractive index rapidly moved about by the wind), a similar effect is observed underwater. However, underwater turbulence fluctuates much slower than air turbulence, making a transmitted laser beam dance, distort and slowly drift, as opposed to jitter and blur. We use several methods to characterize the underwater turbulence.

4.2.1 Zernike coefficients

The phasefront of a beam of light propagating through turbulence becomes distorted. This distorted phasefront can be decomposed in terms of the Zernike polynomials, $Z_j(r,\phi)$—a set of orthonormal polynomials on the unit disk [47],

$$Z_j(r,\phi) = \begin{cases} \sqrt{n+1}R_n^m(r)\sqrt{2}\cos(m\phi), & m \neq 0 \\ \sqrt{n+1}R_n^m(r)\sqrt{2}\sin(m\phi), & m \neq 0, \\ \sqrt{n+1}R_n^0(r), & m = 0 \end{cases} \tag{4.2}$$

where $j = 1 + (n(n+2)+m)/2$ is the Noll index with radial and azimuthal degree n and m, respectively. $R_n^m(r)$ are the radial polynomials,

$$R_n^m(r) = \begin{cases} \sum_{b=0}^{(n-m)/2} \frac{(-1)^b(n-b)!}{b!\left(\frac{n+m}{2}-b\right)!\left(\frac{n-m}{2}-b\right)!} r^{n-2b}, & (n-m) \text{ even}, \\ 0, & (n-m) \text{ odd}. \end{cases} \tag{4.3}$$

Each Zernike polynomial describes a specific type of distortion to the phasefront. For example, the first order aberrations (n=1) correspond to tip-tilt effects; second order aberrations (n=2) correspond to defocusing and astigmatism.

4.2.2 Gerchberg-Saxton algorithm

Given an intensity image of a beam distorted by turbulence, it is possible to retrieve the attributed phase profile by using the Gerchberg-Saxton algorithm (GSA), which

uses fast Fourier transforms [48]. Given the intensity profile before (Alice) and after (Bob) the turbulence, the GSA works as follows (in pseudo-code):

A = Alice's intensity image;

B = Bob's intensity image;

C = FT(A);

For N iterations,

  D = FT^{-1}(Abs(A)*Exp(i*Arg(C)));

  C = FT(Abs(B)*Exp(i*Arg(D)));

end

phase = Arg(C)

Here, FT and FT^{-1} are the Fourier and inverse Fourier transforms, respectively; Abs($\cdot$) calculates the magnitude of the input; Arg($\cdot$) calculates the argument of the input; and N is the number of iterations to perform the calculation. The retrieved phase profile is given by the argument of C after the last iteration. This retrieved phase profile can then be decomposed in term of the Zernike polynomials to determine the most dominant aberrations.

4.3 Underwater Channel

A large motivation behind testing optical-based QKD in an underwater environment is that the current technology of acoustic communication is limited in bandwidth and cannot be transmitted to above-water systems (e.g. satellites). Outdoor underwater quantum channels have much the same challenges as free-space channels, such as turbulence; however, new challenges present themselves in the operating wavelength window and the regime of turbulence.

The first underwater channel that this thesis explored was an outdoor, in-ground swimming pool. With a 10 m length, minimum width of 3 m, and volume of 60,000 L, this pool provided a great starting place to test proof-of-principle QKD experiments in water. Unlike the previous chapter where photon pairs produced around 800 nm propagate without problems over 300 m, this is no longer viable for long distance underwater communication. At the time of the experiment, we did not have access

to a heralded photon source that could produce photon pairs in the visible; we opted instead to produce very non-degenerate photon pairs—the signal at 710 nm and the idler at 940 nm. We could only then reasonably propagate the signal photon through 3 m of water. The idler photon, on the other hand, would stand no chance of propagating through any useful amount of water; therefore, it was coupled to a long SMF that connected directly from the photon source to Bob's detector. Since the idler photon did not travel underwater with the signal photon, it could not be used as a target beam like was done in the free-space case.

Research Article | Vol. 26, No. 17 | 20 Aug 2018 | OPTICS EXPRESS 22563
Optics EXPRESS

Quantum cryptography with twisted photons through an outdoor underwater channel

FRÉDÉRIC BOUCHARD,[1] ALICIA SIT,[1] FELIX HUFNAGEL,[1] AAZAD ABBAS,[1] YINGWEN ZHANG,[1] KHABAT HESHAMI,[2] ROBERT FICKLER,[1] CHRISTOPH MARQUARDT,[3,4] GERD LEUCHS,[1,3,4] ROBERT W. BOYD,[1,3,5] AND EBRAHIM KARIMI[1,3,*]

[1]*Department of Physics, University of Ottawa, Advanced Research Complex, 25 Templeton Street, 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*
[*]*ekarimi@uottawa.ca*

Abstract: Quantum communication has been successfully implemented in optical fibres and through free-space. Fibre systems, though capable of fast key and low error rates, are impractical in communicating with destinations without an established fibre link. Free-space quantum channels can overcome such limitations and reach long distances with the advent of satellite-to-ground links. However, turbulence, resulting from local fluctuations in refractive index, becomes a major challenge by adding errors and losses. Recently, an interest in investigating the possibility of underwater quantum channels has arisen. Here, we investigate the effect of turbulence on an underwater quantum channel using twisted photons in outdoor conditions. We study the effect of turbulence on transmitted error rates, and compare different quantum cryptographic protocols in an underwater quantum channel, showing the feasibility of high-dimensional encoding schemes. Our work may open the way for secure high-dimensional quantum communication between submersibles, and provides important input for potential submersibles-to-satellite quantum communication.

1. Introduction

Quantum key distribution (QKD) allows two individuals, conventionally referred to as *Alice* and *Bob*, to communicate information in a secure and secret manner [1]. Since the proposal of the first protocol by Bennett and Brassard in 1984 (BB84) [1], various protocols and methods, for example Ekert91 [2] and six-state [3], have been further proposed and experimentally investigated. Notably, one class of quantum cryptographic schemes, namely high-dimensional QKD protocols, makes use of *qudits* rather than qubits, wherein the encoded quantum states belong to a higher-dimensional Hilbert space [4, 5]. Such schemes have many potential advantages: in the case of an error-free channel, more than one bit of information can be distributed per carrier. Moreover, they tolerate larger error-thresholds due to the difficulties that an eavesdropper *Eve* has in getting information about the high-dimensional state [6]. This may allow for the implementation of QKD links in noisy environments with high quantum bit error rates (QBER). So far, various quantum channels have been studied in realistic conditions: free-space [7–9], including shorter line-of-sight intra-city links [8, 10], fibre networks [11] and ground-to-satellite links [12–15]. Recently, underwater quantum channels have been proposed and investigated theoretically [16, 17]. The first experimental demonstration of entanglement distribution through a 3 m-long water tube was recently achieved using polarization [18]. Insofar, secure communication through an

#332068 https://doi.org/10.1364/OE.26.022563
Journal © 2018 Received 17 May 2018; accepted 29 Jun 2018; published 17 Aug 2018

Optics EXPRESS

underwater quantum channel has yet to be demonstrated in an outdoor environment or in higher dimensions.

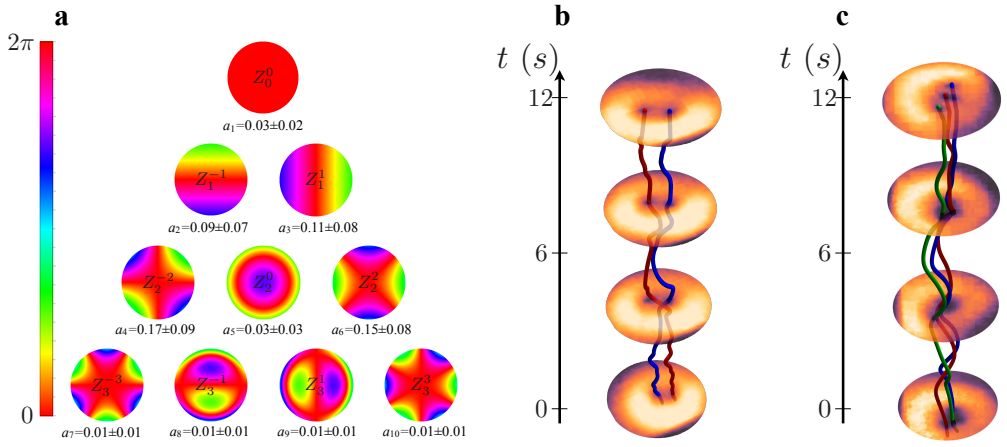

Fig. 1. Experimental characterization of underwater turbulence. (a) Calculated coefficients for the lowest ten Zernike polynomials from intensity images of a Gaussian beam after propagation through 3 m of water to characterize the turbulence in one particular set of conditions at the time of measurement. The dominant coefficients correspond to oblique and vertical astigmatism (a_4 and a_6), followed by tip and tilts effects (a_2 and a_3). The Zernike decomposition was carried out over a disk with a radius of 2.1 mm, which corresponds to $2w_0$, where $w_0 = 1.05$ mm is the beam radius at the input of the channel. (b) - (c) Evolution of vortex splitting over a 12 s period for a $\ell = 2$ and $\ell = 3$ modes, respectively, sent through 5 m of water. The red, blue, and green lines represent the trajectories of the individual singularities, highlighting their splitting and wandering that occurs due to the turbulence.

Photons are the carriers of choice for quantum communication, possessing multiple degrees of freedom with which information can be encoded. Polarization [1], time-bins [19], and spatial modes [20] are the most prevalent encryption methods, with the last two being common methods for achieving high-dimensional protocols. One family of spatial modes with mature preparation and measurement techniques is the OAM of light, also referred to as twisted photons [21, 22]. These modes possess a helical wavefront given by $\exp(i\ell\varphi)$, where ℓ is an integer and φ is the transverse azimuthal coordinate. The OAM states of photons is one realization of a Hilbert space with unbounded dimensionality. Since the modes form a complete orthonormal basis, these states can be used for high-dimensional QKD schemes [23–25]. In this Article, we report the effect of water turbulence on OAM modes of light in an outdoor swimming pool, and study its effect in quantum cryptographic schemes, performing a high-dimensional BB84 protocol with twisted photons.

Since the underwater quatum channel is an outdoor link, uncontrolled turbulent conditions can be expected, as in the case of free-space links, introducing additional errors and losses to the system [26]. Turbulence is observed in the form of beam distortions and beam wandering after propagating through a turbulent media. The effect of turbulence on the propagation of OAM modes through free-space air has been studied for various distances. In the Kolmogorov theory of turbulence in free-space, the turbulence is associated with a local variation in the refractive index due to temperature and pressure variations [27]. However, temperature gradients

Optics EXPRESS

in the atmosphere represent the main contribution to atmospheric turbulence. Water is an incompressible fluid and thus the main contribution to the optical turbulence is derived from local variations in temperatures. Recently, propagation of OAM modes through water has been reported in controlled laboratory conditions [28, 29]. Our experiments were performed in a 60,000 litres outdoor, in-ground pool, see the appendix-B for more details. The water was exposed to temperatures between 27°C during the day to 17°C at night. This creates a temperature gradient between the top and bottom of the pool, which was inhomogeneously mixed by built-in water

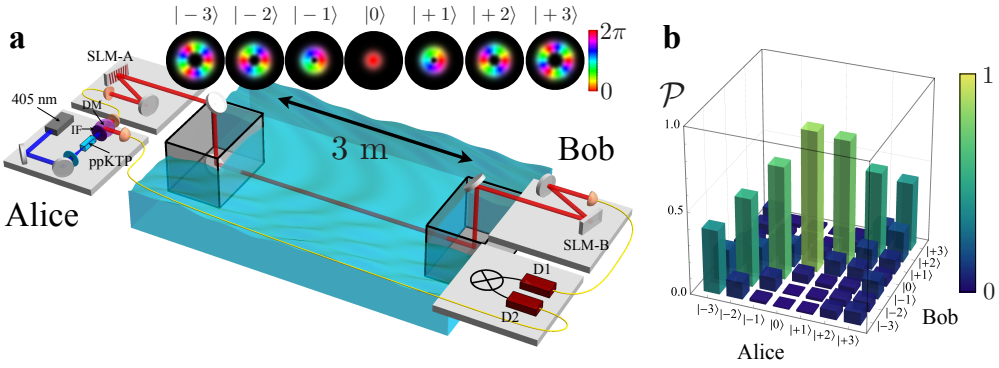

Fig. 2. Experimental setup and state cross-talk measurements. (a) Photon pairs (signal $\lambda_s = 710\ nm$, idler $\lambda_i = 943\ nm$) are generated via spontaneous parametric downconversion pumped from a periodically poled KTP (ppKTP) crystal by a 405 nm diode laser. A long pass filter (IF) blocks the UV and transmits the photon pairs, which are then split at a dichroic mirror (DM). The idler photon is directly detected by a single photon detector (D2) and acts as a heralding trigger for the information-carrying signal photon. Alice prepares the signal photon into a particular state, for example one from the insets, using SLM-A, then sends it to Bob through the 3 m underwater link. Bob performs a measurement on the received state using SLM-B and a single mode optical fibre connected to D1. Coincidence events between D1 and D2 are recorded. (b) Measured cross-talk matrix between the OAM states ($\ell = -3$ to 3) that Alice sends and Bob measures. Higher order states experience more cross-talk as compared to lower order states, seen as off-diagonal detection probabilities.

A characterization of the level of turbulence, assuming the single phase screen approximation, in our 3 m underwater channel is performed by sending a 635 nm Gaussian-shaped laser beam through the water and record the transmitted intensity patters (see Turbulence Characterization in Methods for more details). We employ the Gerchberg-Saxton algorithm (GSA), a phase retrieval algorithm using fast Fourier transforms [30], to reconstruct the phase of the beam after propagating through the water. The obtained phase profile, $\Phi(r, \varphi)$, is then decomposed in terms of Zernike polynomials, which forms a set of orthonormal polynomials on the unit disk [31],

$$\Phi(r, \varphi) = \sum_j a_j Z_j(r, \varphi), \tag{1}$$

where r and φ are the radial and azimuthal coordinates, respectively, a_j are the Zernike coefficients, $Z_j(r, \varphi) = Z_n^m(r, \varphi)$ are the Zernike polynomials (defined in the Methods), $j = 1 + (n(n+2)+m)/2$ is the Noll index, and n and m are the radial and azimuthal degree, respectively.

The average values of measured expansion coefficients a_j as well as their corresponding Zernike polynomials are shown in Fig. 1-a. In particular, low-order Zernike polynomials have specific meaning in terms of optical aberrations. First order aberrations, $n = 1$ ($j = 2, 3$),

Optics EXPRESS

correspond to a tip-tilt in the wavefront. In the weak atmospheric turbulence regime, tip-tilt is the major contribution and results in beam wandering. Second order optical aberrations, $n = 2$, are related to astigmatism ($j = 4, 6$) and defocusing ($j = 5$). It can be seen from Fig. 1-(a), that the contribution of astigmatism in our turbulent underwater link is the largest. Further analysis of the turbulence is presented in the appendix-A.

In particular, one effect of astigmatism on OAM modes is the singularity splitting for OAM values of $|\ell| > 1$; this splitting effect has also recently been studied in free-space [32]. The effect of vortex splitting in our underwater link is shown in Fig. 1-(b) and Fig. 1-(c), where an $\ell = 2$ and$\ell = 3$ mode respectively, each generated by a phase-only spatial light modulator (SLM), is sent through a slightly longer distance of 5 m. Hence, underwater channels may give rise to turbulent conditions that are fundamentally different from those present in a free-space channel. However, the turbulence was observed to change on a much slower time-scale as opposed to free-space, on the order of 10 Hz compared to 100 Hz. Thus, implementing a SLM in an adaptive optics type system might be fast enough to correct for the aberrations.

Our experimental setup, see Fig. 2-(a), for investigating QKD consists of a heralded single photon source (for more details see Experimental Setup in Methods), Alice's state preparation setup, Bob's measurement setup, and a 3 m-outdoor underwater link. In the near-infrared region, light is strongly absorbed by water; ideally, it is desirable to produce signal photons with a λ_s in the blue-green window (≈400-600 nm) which experiences the least amount of absorption. In the heralded single-photon source, the signal (λ_s = 710 nm) and idler (λ_i = 940 nm) photons are generated by spontaneous parametric downconvesion, and are coupled to single-mode optical fibres (SMOF) in order to filter their transverse spatial modes to the fundamental Gaussian mode. A coincidence rate of 432 kHz, within a coincidence time window of 5 ns, is measured after the SMOFs at the source. The idler photon is sent through a fibre delay line to Bob, acting as the heralding photon, and the signal photon is sent to Alice's generation apparatus. In order to eliminate the distortions that an air-water interface would introduce to the wavefront of the transmitted and recieved photons, we use periscopes to guide the photons into/out of glass tanks that are partially immersed in the water on either end of the link. The advantage of using such a configuration is that the photons pass through first a flat air-glass then a glass-water interface, and *vice versa*, without significant alterations to their wavefronts. For the quantum cryptographic tests, Alice prepares the signal photon into an OAM state using a SLM, then sends it across the underwater link. Bob uses a SLM and SMOF to project the received signal photons onto a given OAM state and records a coincidence event between the result and the heralding photon at a coincidence box [33].

We perform a cross-talk measurement of several OAM states ranging from −3 to 3, i.e. $\{|\ell\rangle\,; \ell = -3, -2, -1, 0, 1, 2, 3\}$, see Fig. 2-(b), where $|\ell\rangle$ represents the quantum state with helical wavefront of $\exp(i\ell\varphi)$. The cross-talk measurements are a good indicator of the level of errors (QBER) that one could expect in a QKD protocol. Practical implementations are seen to dictate the optimal dimensionality of the qudits used in a specific high-dimensional quantum cryptographic scheme. The OAM mode that experiences the least amount of cross-talk is the fundamental Gaussian mode ($\ell = 0$), with a cross-talk of $< 15\%$ with its neighbouring modes ($\ell = \pm 1$). This cross-talk could lead to sufficiently low QBER to securely transmit information, given a small OAM encryption subspace. As we go to larger OAM values, the modes suffer larger cross-talk, which makes the extension to higher-dimensions challenging. Explicitly, the effect of turbulence on a QKD protocol is twofold: it introduces errors and losses. Loss in the underwater channel can be attributed to absorption from the water, but also from the turbulence. An approximate absorption coefficient at 710 nm was measured in the lab to be 1.2 m^{-1}, which is on the same order of magnitude of tabulated values [34]. This corresponds to approximately 3% transmission after 3 m of underwater propagation. On the other hand, turbulence can also cause loss by beam wandering and distortion effects, characterized by the Zernike coefficients in

Optics EXPRESS

Fig. 1-(a), wherein the photons are shifted or stretched outside of the collection area of Bob's optics. Most QKD protocols are robust against losses at the cost of a reduced key rate. However,

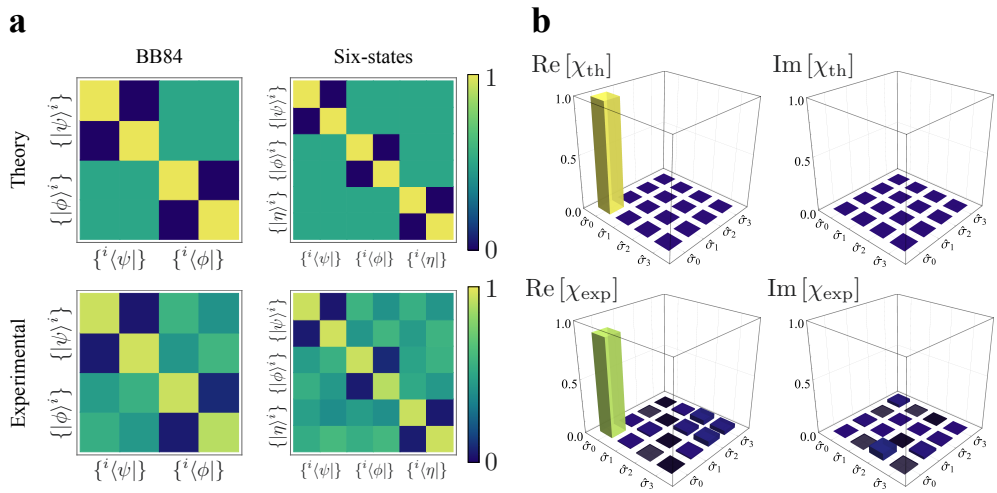

Fig. 3. Probability-of-detection matrices for d=2 BB84 and Six-states protocols, and the channel process matrix. (a) Theoretical and experimentally measured probability-of-detection matrices for BB84 (left column) and Six-states (right column) protocols in $d = 2$. We measured QBERs of $Q = 6.57\%$ and $Q = 6.35$ %, respectively, for these two protocols, corresponding to secret key rates of $R = 0.301$ and $R = 0.395$. (b) The six-state protocol is a tomographic protocol and can be used to reconstruct the process tomography matrix; the real and imaginary parts of the theoretical matrix are shown in the top row. The experimentally measured process matrix is shown in the bottom row with a process fidelity of $\mathcal{F} = 0.905$.

3. Discussion

As a first test of our underwater QKD link, we perform a 2-dimensional BB84 protocol. Alice uses the OAM subspace consisting of $\ell = \pm 1$ to encode the information. In the BB84 protocol, two mutually unbiased bases (MUBs) are required for Alice and Bob to encode and measure the states of the photons. The first MUB here is given by the logical basis, $|\psi\rangle^i \in \{|-1\rangle, |+1\rangle\}$, and the second MUB is given by $|\varphi\rangle^i \in \{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|-1\rangle \pm |+1\rangle)/\sqrt{2}$. The experimental probability-of-detection matrix is shown in Fig. 3-(a) (left column) along with its theoretical counterpart. The secret key rate per sifted photon, R, may be calculated using the following formula, $R(Q) = 1 - 2h(Q)$, where Q is the QBER and $h(\cdot)$ is the Shannon entropy. From the probability-of-detection matrix, a QBER of $Q = 6.57$ % is calculated, which is below the error threshold of $Q^{\text{2D}}_{\text{threshold}} = 11\%$ for the 2-dimensional BB84 protocol, corresponding to a positive secret key rate of $R = 0.301$ bits per sifted photon.

An extension of the BB84 protocol in dimension $d = 2$ is achieved by considering a third MUB, i.e. $|\eta\rangle^i \in \{|+i\rangle, |-i\rangle\}$, where $|\pm i\rangle = (|-1\rangle \pm i\,|+1\rangle)/\sqrt{2}$. This protocol, also known as the *Six-states* protocol [35], can tolerate slightly larger error thresholds of around $Q = 12.6$ %. The probability-of-detection matrix is shown in Fig. 3-(a) (right column), where a QBER of $Q = 6.35$ % is measured resulting in a secret key rate of $R = 0.395$ bits per sifted photon. However, when considering sifting, the *six-states* protocol suffers from a lower sifting rate, i.e.

Optics EXPRESS

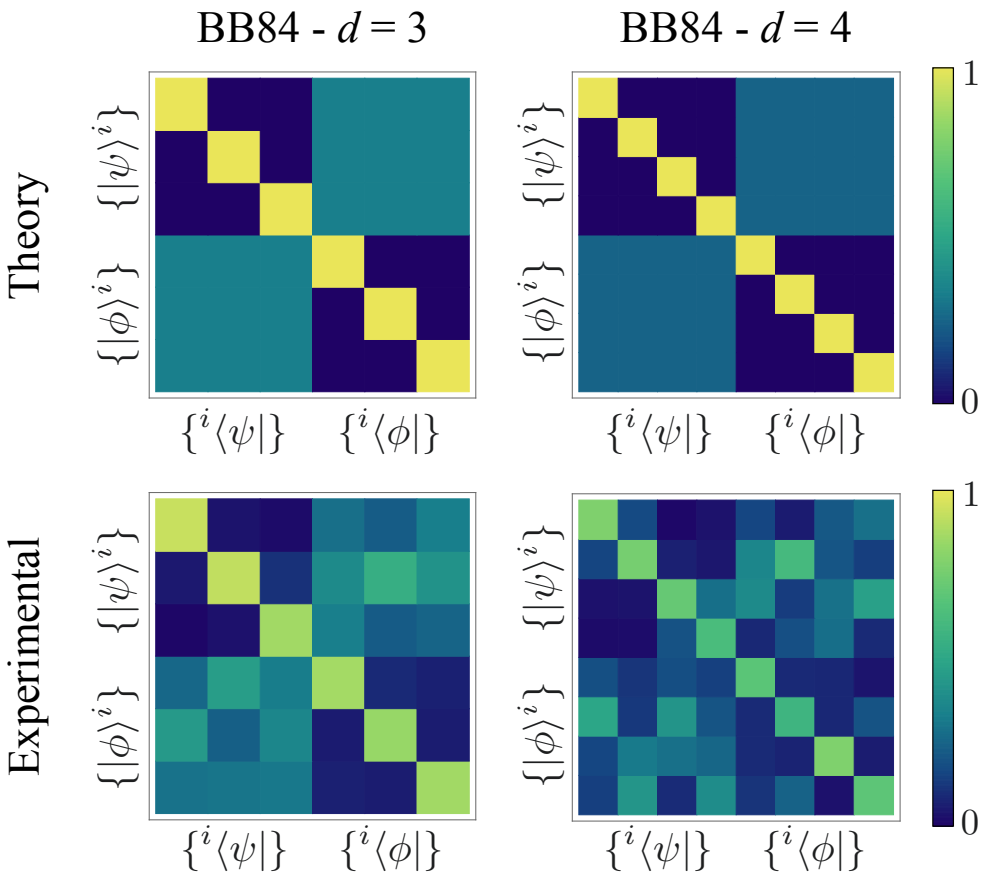

Fig. 4. High-dimensional probability-of-detection matrices. Theoretical (top row) and experimentally measured (bottom row) probability-of-detection matrices for BB84 protocols in $d = 3$ and $d = 4$. We measured QBER of $Q^{3D} = 11.73\%$ and $Q^{4D} = 29.77\%$, respectively. The QBER in $d = 3$ is below the tolerable error threshold, allowing for the establishment of a secret key rate of $R^{3D} = 0.307$ bits per sifted photon. However, the QBER in $d = 4$ exceeds the threshold of $Q^{4D}_{\text{threshold}} = 18.9\%$.

Optics EXPRESS

1/3, in comparison to the BB84 protocol, which has a sifting rate of 1/2. Nevertheless, the *six-states* protocol is a tomographic protocol: the measurements by Alice and Bob can be used to fully characterize the quantum channel and reconstruct the process matrix of the link via quantum process tomography. Let the channel be characterized by a process ε, which relates the input and output states in the following manner, $\hat{\rho}_{\text{out}} = \varepsilon(\hat{\rho}_{\text{in}})$. The process may be described by the process matrix χ_{mn}, where $\varepsilon(\hat{\rho}) = \sum_{mn} \chi_{mn}\, \hat{\sigma}_m\, \hat{\rho}\, \hat{\sigma}_n^{\dagger}$, and $\hat{\sigma}_m$ are the Pauli matrices. The reconstructed process matrix, χ_{exp}, along with the theoretical ideal process matrix, χ_{th}, is shown in Fig. 3-(b). A process fidelity of $\mathcal{F} = 0.905$ is measured from the process matrix, where the process fidelity is defined as $\mathcal{F} = \text{Tr}\left[\chi_{\text{exp}} \cdot \chi_{\text{th}}\right] / \text{Tr}\left[\chi_{\text{th}} \cdot \chi_{\text{th}}\right]$.

The versatility of our experimental configuration allows us to test different types of QKD protocols in our underwater link. As a next step, we perform a high-dimensional quantum cryptographic scheme. The standard BB84 protocol is naturally extended using high-dimensional states, where two d-dimensional bases are employed. The first MUB is given by the logical basis, $|\psi\rangle^i \in \{|i\rangle\,; i = 1, 2, ..., d\}$, and the second MUB is given by the discrete Fourier transform $|\varphi\rangle^i \in \{\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{ij}\, |j\rangle\}$, where $\omega_d = \exp(i2\pi/d)$. We perform the 3- and 4-dimensional BB84 protocol using the OAM modes with $\ell = 0, \pm 1$ and $\ell = \pm 1, \pm 2$, respectively, in our underwater link. The results are shown in Fig. 4, where QBERs of $Q^{3\text{D}} = 11.73\%$ and $Q^{4\text{D}} = 29.77\%$ were measured for the case of $d = 3$ and $d = 4$, respectively. For the 3-dimensional BB84 ($Q^{3\text{D}}_{\text{threshold}} = 15.95\%$), a secret key rate of $R^{3\text{D}} = 0.307$ bits per sifted photon was obtained, which is slightly larger than the 2-dimensional BB84 secret key rate. For the 4-dimensional case, the QBER is above the error threshold, i.e. $Q^{4\text{D}}_{\text{threshold}} = 18.93\%$, meaning no secret key can distributed across the turbulent underwater link with a 4-dimensional BB84 protocol with twisted

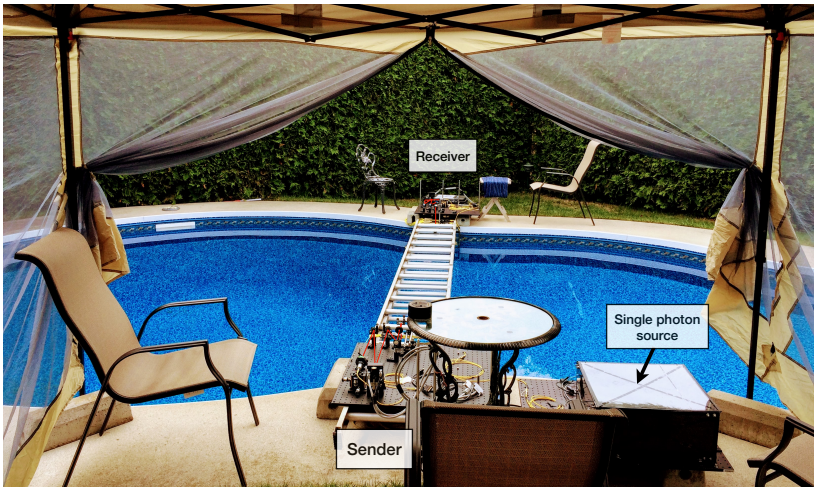

Fig. 5. Image of outdoor underwater link in an in-ground swimming pool. The single photon source, on the sender's side, is enclosed within a black box. The sender's setup is mounted on an optical breadboard and consists of a microscope objective stage, a spatial light modular, mirrors and a periscope which brings the beam in an air-filled aquarium that is half-way under the water. In order to stabilize the aquariums, they are secured to a ladder that is placed above the underwater link, but is not in direct contact with the optical breadboards. The idler photon is sent from the sender to the receiver through a single mode fiber that is mounted along the ladder. The receiver's setup is mounted on an optical breadboard and also consists of a periscope, mirrors, a spatial light modular and a microscope objective. Red lines were added to outline the beam's path.

Optics EXPRESS

photons. These errors originate from the aberrations induced by the underwater turbulence, introducing more cross-talk between higher OAM states. As mentioned previously, the frequency of the turbulence was on the order of tens of Hertz, which opens up the possibility to implement an adaptive optics system using the implemented SLMs on Alice's or Bob's side for correcting the aberrations. This procedure would provide a means for reducing the QBER below the error thresholds in higher-dimensions.

In summary, we have characterized the predominant turbulence effects in our underwater quantum channel to be astigmatism, outlining a notable difference between an air free-space and an underwater link. We have performed and compared different QKD protocols through this underwater link using twisted photons. For a short distance, i.e. 3 m, we were able to successfully achieve a positive secret key rate using a 2- and 3-dimensional BB84 protocol.

Appendix-A

Turbulence Characterization: A characterization of the level of turbulence in our underwater channel is done by sending a Gaussian laser beam, at a wavelength of 635 nm, over our 3 m underwater link, see Fig. 5. Short exposure images (0.07 ms) of the beam at the output of the link are recorded using a CCD camera. The water turbulence is characterized using a single phase screen approximation, i.e. we assumed the effect of turbulence can be described as a varying phase screen at the input of the link followed by uniform propagation. Assuming a Gaussian input beam, we use the intensity images recorded at the output of the link to reconstruct the phase of the input beam. The reconstructed input phase profile corresponds to the input single phase screen that models the turbulence of the channel. In order to obtain the phase of the output beam, we perform the Gerchberg-Saxton algorithm (GSA), a phase retrieval algorithm using fast Fourier transforms [30]. The obtained phase profile, $\Phi(r, \varphi)$, is then decomposed in terms of Zernike polynomials, which forms a set of orthonormal polynomials on the unit disk s are

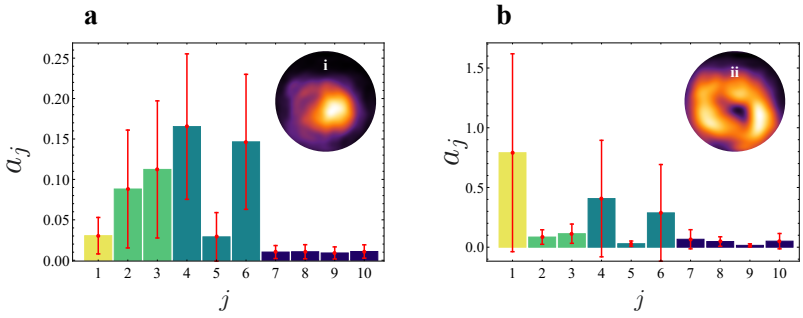

Fig. 6. Characterization of underwater turbulence. (a) Experimentally obtained coefficients for an input gaussian ($\ell = 0$) mode. Inset **i**, shows an example of a distorted gaussian beam profile at the output of the channel. The Zernike decomposition was carried over a disk with a radius of 2.1 mm, which corresponds to $2w_0$, where $w_0 = 1.05$ mm is the beam size at the input of the channel. (b) Experimentally obtained coefficients for an input orbital angular momentum beam ($\ell = 1$). Inset **ii**, shows an example of a distorted donut beam profile at the output of the channel. The Zernike decomposition was carried over a disk with a radius of 2.97 mm, which corresponds to $4w_0/\sqrt{2}$, where $w_0/\sqrt{2} = 0.74$ mm corresponds to the radius of maximum intensity of the donut beam at the input of the channel.

written in terms of the radial polynomial $R_n^m(r)$ [31],

$$Z_{\text{even}\,j}(r,\varphi) = \sqrt{n+1}\,R_n^m(r)\sqrt{2}\cos(m\varphi), \quad m \neq 0, \tag{2}$$

$$Z_{\text{odd}\,j}(r,\varphi) = \sqrt{n+1}\,R_n^m(r)\sqrt{2}\sin(m\varphi), \quad m \neq 0, \tag{3}$$

$$Z_j(r,\varphi) = \sqrt{n+1}R_n^0(r), \quad m = 0. \tag{4}$$

The GSA and Zernike polynomial decomposition is subsequently carried over all 143 images recorded at the output of the link. An example of experimentally obtained coefficients for $\ell = 0$ and $\ell = 1$ modes are shown in Fig. 6.

Appendix-B

In the heralded single photon source, a 405 nm diode laser (200 mW) pumps a periodically-poled potassium titanyl phosphate (ppKTP) crystal to produce single photon pairs via spontaneous parametric downconversion. A non-degenerate set of wavelengths is chosen to produce signal photons at $\lambda_s = 710$ nm, with corresponding idler photons at $\lambda_i = 943$ nm, see Fig.7. We note that the wavelength of the signal photon could be adjusted to lie in the desired blue-green window with a different crystal along with commercially available single photon detectors which work at the IR. The signal and idler photons are coupled to single-mode optical fibres (SMOF) in order to filter their transverse spatial modes to the fundamental Gaussian mode. A coincidence rate of 432 kHz, within a coincidence time window of 5 ns, is measured after the SMOFs at the source. The corresponding single photon count rates for the signal and idler photons are given by 5 MHz and 1.5 MHz, respectively. The idler photon is sent through a fibre delay line to Bob, acting as the heralding photon, and the signal photon is sent to Alice's generation apparatus. The

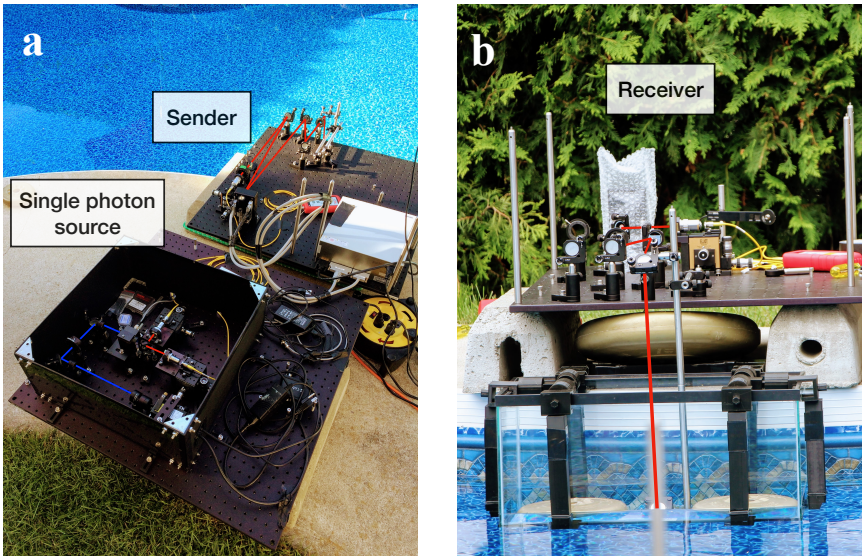

Fig. 7. Sender and receiver setup of the outdoor underwater link. (a) Close-up of the single photon source and the sender's setup. The blue line represents the pump beam and the red lines represent the signal and idler beams. (b) Close up of the receiver's aquarium, periscope and setup.

experiment was carried out during the night under the following weather conditions: temperature, relative humidity, wind speed and atmospheric pressure were measured as 17°C, 91%, 2 km/h and 100.79 kPa, respectively. The depth of the pool is 1.1 m and the beam was situated at 12 cm under the surface. The pH, Phosphate concentration, and water hardness were measured as 6.9, 318 ppb and 331 ppm, respectively.

Funding

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); Max Planck-University of Ottawa Centre for Extreme and Quantum Photonics.

Acknowledgments

All authors would like to thank Norman Bouchard and Marie-France Langlois for access to their in-ground pool.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proc. IEEE Int. Conf. on Comput. Syst. Signal Process. Bangalore, India **175**, 8 (1984).
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).
3. Y. C. Liang, D. Kaszlikowski, B.-G. Englert, L. C. Kwek, and C. H. Oh, "Tomographic quantum cryptography," Phys. Rev. A **68**, 022324 (2003).
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. F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, "High-dimensional quantum cloning and applications to quantum hacking," Sci. Adv. **3**, e1601915 (2017).
7. A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," EPL (Europhysics Lett. **23**, 383 (1993).
8. W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," Phys. Rev. Lett. **81**, 3283 (1998).
9. J. Rarity, P. Tapster, and P. Gorman, "Secure free-space key exchange to 1.9 km and beyond," J. Mod. Opt. **48**, 1887 (2001).
10. K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," Opt. Express **13**, 202 (2005).
11. R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, W. Tittel, "Quantum teleportation across a metropolitan fibre network," Nat. Photonics **10**, 676 (2016).
12. J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140 (2017).
13. J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Qi. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," Phys. Rev. Lett. **119**, 200501 (2017).
14. J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," Nature **549**, 70 (2017).
15. S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-Relayed Intercontinental Quantum Network," Phys. Rev. Lett. **120**, 030501 (2018).
16. P. Shi, S.-C. Zhao, W.-D. Li, and Y.-J. Gu, "Feasibility of underwater free space quantum key distribution," arXiv preprint arXiv:1402.4666 (2014).

Optics EXPRESS

17. Y.-Y. Zhou and X.-J. Zhou, "Performance analysis of quantum key distribution based on air-water channel," Optoelectronics Lett. **11**, 149 (2015).
18. L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin, "Performance analysis of quantum key distribution based on air-water channel," Opt. Express **25**, 19795 (2017).
19. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Sci. Adv. **3**, e1701491 (2017).
20. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. **8**, 75 (2006).
21. G. Molina-Terriza, J. P. Torres, and L. Torner, "Twisted photons," Nat. Phys. **3**, 305 (2007).
22. M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted Photons: New Quantum Perspectives in High Dimensions," Light. Sci. & Appl. **7**, 17146 (2018).
23. 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).
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. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," Optica **4**, 1006 (2017).
26. L. C. Andrews and R. L. Phillips, *Laser beam propagation through random media,* vol. 1 (SPIE Press, 2005).
27. A. N. Kolmogorov, "The local structure of turbulence in incompressible viscous fluid for very large reynolds numbers," Doklady Akademiia Nauk SSSR **30**, 299–303 (1941).
28. Y. Ren, L. Li, Z. Wang, S. M. Kamali, E. Arbabi, A. Arbabi, Z. Zhao, G. Xie, Y. Cao, N. Ahmed, Y. Yan, C. Liu, A. J. Willner, S. Ashrafi, M. Tur, A. Faraon, and A. E. Willner, "Orbital angular momentum-based space division multiplexing for high-capacity underwater optical communications," Sci. Reports **6**, 33306 (2016).
29. J. Baghdady, K. Miller, K. Morgan, M. Byrd, S. Osler, R. Ragusa, W. Li, B. M. Cochenour, and E. G. Johnson, "Multi-Gigabit/s underwater optical communication link using orbital angular momentum multiplexing," Opt. Express **24**, 9794 (2016).
30. J. R. Fienup, "Phase retrieval algorithms: a comparison," Appl. Opt. **21**, 2758 (1982).
31. R. J. Noll, "Zernike polynomials and atmospheric turbulence," J. Opt. Soc. Am. **66**, 207 (1976).
32. M. Lavery, C. Peuntinger, K. Günthner, P. Banzer, D. Elser, R. Boyd, M. Padgett, C. Marquardt, and G. Leuchs, "Free-space propagation of high-dimensional structured optical fields in an urban environment," Sci. Adv. **3**, e1700552 (2017).
33. 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).
34. S. A. Sullivan, "Experimental study of the absorption in distilled water, artificial sea water, and heavy water in the visible region of the spectrum," J. Opt. Soc. Am. **53**, 962-968 (1963).
35. D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett. **81**, 3018 (1998).

Chapter 5

Conclusion

In summary, we have explored three different types of channels (fibre, free-space, underwater) to test quantum cryptographic protocols with structured photons.

The first quantum channel that we explored was that of a vortex fibre. Unlike conventional optical fibres, a solid core vortex fibre has a ring of higher refractive index in its transverse cross section. For the vortex fibre of interest in this chapter, the ring lifts the near-degeneracy between the LP_{11} group modes, which allows for the coherent transmission of structured modes of light: OAM $|\ell = \pm 1\rangle$ with the corresponding aligned SAM. This provides a 2-dimensional Hilbert space with which we were able to successfully perform a proof-of-principle BB84 protocol. These types of vortex fibres, especially those which support multiple values of OAM, will provide a way to increase the bandwidth limit of conventional fibres.

As a first foray into free-space quantum communication, Chap. 3 described the construction of our first 300-m free-space link on the University of Ottawa campus. Through this link, we showed the first demonstration of high-dimensional quantum communication with structured photons in an urban environment. An omnipresent environmental factor that can greatly hurt a QKD protocol is that of atmospheric turbulence, which rapidly displaces and distorts a laser beam. These perturbations from atmospheric turbulence can introduce a large nuumber of errors on a transmitted secret key; as a first order correction, we used the idler photon as a "target" beam to post-select for the cases when the signal photon was least affected by turbulence. We were nonetheless able to show that more information per carrier could be transmitted with a 4-dimensional protocol in comparison to a 2-dimensional one. Short line-of-sight free-space links provide a good starting test bed for longer distance

implementations, such as ground-to-satellite links. Future avenues of research include studying if active wavefront correction techniques would benefit QKD protocols using structured photons.

The final potential quantum channel that was studied in this thesis is that of an underwater channel. Transmitting information in the optical domain, as opposed to the current acoustic technologies, provides a faster and more secure way of doing so, with the potential to create submarine-to-satellite links. Similar to free-space channels, underwater channels are also subject to turbulence, albeit on a timescale an order of magnitude slower. As a first attempt, we created a 3-m underwater quantum channel through an outdoor swimming pool. The predominant aberrations caused by turbulence were astigmatism and tip-tilt effects; as a result, we were limited to a 3-dimensional BB84 protocol with purely OAM modes as higher order modes became too distorted.

Regardless of the quantum channel, quantum cryptography will play an essential role in protecting our sensitive information in the future. The preliminary works discussed in this thesis will therefore hopefully provide a base for future studies for quantum key distribution with structured photons.

APPENDICES

Appendix A

Supplementary material: High-dimensional intra-city quantum quantum cryptography with structured photons

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,

$$\mathcal{M}_0^{ik} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},$$

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

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:

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

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

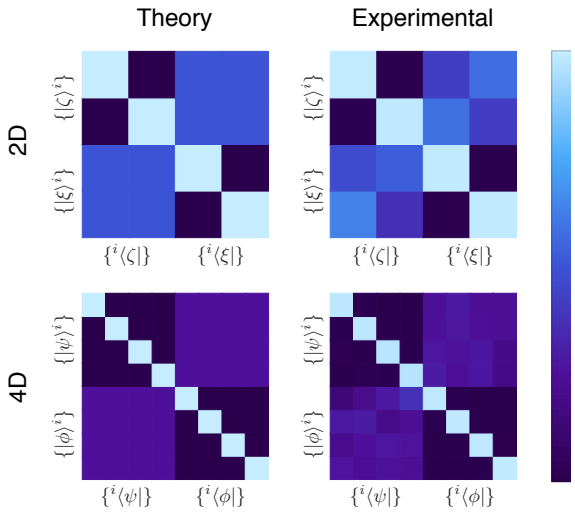

Fig. S1. Visualization of MUBs in d=2 and d=4 Theoretical probability-of-detection matrices (left column) for dimensions 2 and 4 using Eq. (S2) and Eqs. (S4–S5) by applying Eq. (S1). The probability-of-detection matrices as measured in the laboratory (right column) give bit error rates of 0.83% and 1.83% 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
$\|\zeta\rangle^1$	0°
$\|\zeta\rangle^2$	+45°
$\|\xi\rangle^1$	+22.5°
$\|\xi\rangle^2$	−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
$\|\psi\rangle^1$	−45°	−45°
$\|\psi\rangle^2$	+45°	+45°
$\|\psi\rangle^3$	−45°	+45°
$\|\psi\rangle^4$	+45°	−45°

(S9)

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

	$^1\langle\zeta\|$	$^2\langle\zeta\|$	$^1\langle\xi\|$	$^2\langle\xi\|$
$\|\zeta\rangle^1$	0.971	0.029	0.421	0.579
$\|\zeta\rangle^2$	0.062	0.938	0.677	0.323
$\|\xi\rangle^1$	0.731	0.269	0.959	0.041
$\|\xi\rangle^2$	0.459	0.541	0.068	0.932

(S11)

Target corrected data from (S11):

	$^1\langle\zeta\|$	$^2\langle\zeta\|$	$^1\langle\xi\|$	$^2\langle\xi\|$
$\|\zeta\rangle^1$	0.972	0.028	0.351	0.649
$\|\zeta\rangle^2$	0.050	0.950	0.653	0.347
$\|\xi\rangle^1$	0.725	0.275	0.961	0.039
$\|\xi\rangle^2$	0.463	0.537	0.069	0.931

(S12)

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

	${}^1\langle\psi\|$	${}^3\langle\psi\|$	${}^2\langle\psi\|$	${}^4\langle\psi\|$	${}^1\langle\varphi\|$	${}^2\langle\varphi\|$	${}^3\langle\varphi\|^3$	${}^4\langle\varphi\|$
$\|\psi\rangle^1$	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
$\|\varphi\rangle^1$	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

(S13)

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

	${}^1\langle\psi\|$	${}^3\langle\psi\|$	${}^2\langle\psi\|$	${}^4\langle\psi\|$	${}^1\langle\varphi\|$	${}^2\langle\varphi\|$	${}^3\langle\varphi\|^3$	${}^4\langle\varphi\|$
$\|\psi\rangle^1$	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		
$\|\psi\rangle^4$	0.049	0.004	0.029	0.918	0.094	0.242		
$\|\varphi\rangle^1$	0.376	0.108	0.321	0.195	0.874	0.033		
$\|\varphi\rangle^2$	0.273	0.197	0.255	0.275	0.035	0.825		
$\|\varphi\rangle^3$	0.200	0.132	0.511	0.157	0.060	0.016		
$\|\varphi\rangle^4$	0.186	0.163	0.365	0.287	0.026	0.129		

Normalized raw data for probability-ofdetection sion 4 on a turbulent night:

	${}^1\langle\psi\|$	${}^3\langle\psi\|$	${}^2\langle\psi\|$	${}^4\langle\psi\|$	${}^1\langle\varphi\|$	${}^2\langle\varphi\|$
$\|\psi\rangle^1$	0.741	0.032	0.043	0.184	0.370	0.168
$\|\psi\rangle^3$	0.096	0.722	0.138	0.044	0.120	0.432
$\|\psi\rangle^2$	0.043	0.177	0.755	0.025	0.276	0.247
$\|\psi\rangle^4$	0.101	0.041	0.047	0.811	0.122	0.433
$\|\varphi\rangle^1$	0.126	0.471	0.197	0.206	0.707	0.051
$\|\varphi\rangle^2$	0.211	0.234	0.352	0.203	0.110	0.694
$\|\varphi\rangle^3$	0.265	0.285	0.259	0.191	0.195	0.056
$\|\varphi\rangle^4$	0.478	0.146	0.185	0.191	0.048	0.103

4. NUMERICAL APPROACH FOR THE S RATE CALCULATION

Here we use a numerical approach to calculate the se the MUBs in the current experiment that are shown The secret key rate calculation below relies on the d problem that has recently been introduced as an eff approach for unstructured quantum key distributio result in [1] indicates that the achievable secure key rate is lower bounded by the following maximization problem,

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

where

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

and

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

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

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

$$\text{Constraints:} \quad \langle\mathbb{1}\rangle = 1 \tag{S19}$$

$$\langle \mathbf{E_X} \rangle = Q \tag{S20}$$

$$\langle \mathbf{E_Z} \rangle = Q \tag{S21}$$

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

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

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

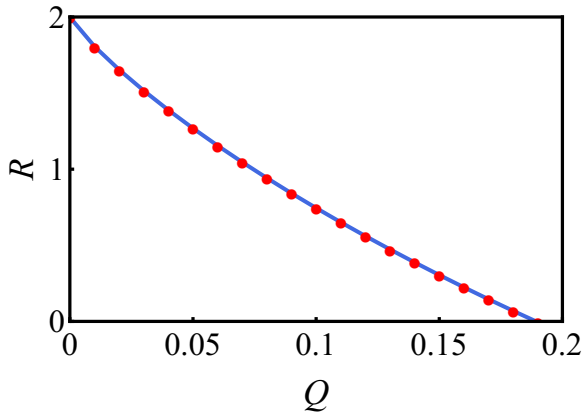

Fig. S2. Secret key rate per signal for BB84 in d=4 with 2 MUBs Solution to the numerical optimization problem in Eq. (S15) are shown for different values of average error rates (red dots). As it can be seen, the numerical optimization saturates the bound and shows a good agreement with the theory from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

Bibliography

[1] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[2] W. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[3] C.H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *in Procedings IEEE International Conference on Computer System Signal Processing*, 175:8, 1984.

[4] A.K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67:661, 1991.

[5] Y.C. Liang, D. Kaszlikowski, B.-G. Englert, L.C. Kwek, and C.H. Oh. Tomographic quantum cryptography. *Physical Review A*, 68:022324, 2003.

[6] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "plug and play" systems for quantum cryptography. *Applied Physics Letters*, 70:793, 1997.

[7] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and Pan J.-W. Quantum teleportation with independent sources and prior entanglement distribution over a network. *Nature Photonics*, 10:671, 2016.

[8] R. Valivarthi, M.G. Puigibert, Q. Zhou, G.H. Aguilar, V.B. Verma, F. Marsili, M.D. Shaw, S.W. Nam, D. Oblak, and W. Tittel. Quantum teleportation across a metropolitan fibre network. *Nature Photonics*, 10:676, 2016.

[9] M.P.J. Lavery. Vortex instability in turbulent free-space propagation. *New Journal of Physics*, 20:043023, 2018.

[10] 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 Journal of Physics*, 16:113028, 2014.

[11] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B Heim, C. Marquardt, G. Leuchs, R.W. Boyd, and E. Karimi. High-dimensional intra-city quantum cryptography with structured photons. *Optica*, 4:1006, 2017.

[12] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger. Twisted light transmission over 143 km. *Proceedings National Academy of Sciences*, 113:13648, 2016.

[13] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-to-ground entanglement-based quantum key distribution. *Physical Review Letters*, 119:200501, 2017.

[14] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356:1140, 2017.

[15] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan. Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120:030501, 2018.

[16] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi. Experimental satellite quantum communications. *Physical Review Letters*, 115:040502, 2015.

[17] P. Shi, S.-C. Zhao, Y.-J. Gu, and W.-D. Li. Channel analysis for single photon underwater free space quantum key distribution. *Journal of the Optical Society of America A*, 32(3):349–356, 2015.

[18] H. Bechmann-Pasquinucci and W. Tittle. Quantum cryptography using larger alphabets. *Physical Review A*, 61:062308, 2000.

[19] N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(12):127902, 2002.

[20] L. Allen, M.W. Beijersbergen, R.J.C. Spreeuw, and J.P. Woerdman. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Physical Review A*, 45(11):8185, 1992.

[21] R. Fickler, G. Campbell, B. Buchler, P.K. Lam, and A. Zeilinger. Quantum entanglement of angular momentum states with quantum numbers up to 10010. *Proceedings of the National Academy of Sciences*, 113(48):13642–13647, 2016.

[22] S.W. Hell and J. Wichmann. Breaking the diffraction resolution limit by stimulated emissioin: stimulated-depletion fluorescence microscopy. *Optics Letters*, 19(11):780–782, 1994.

[23] T.A. Klar and S.W. Hell. Subdiffraction resolution in far-field fluorescence microscopy. *Optics Letters*, 24(14):954–956, 1999.

[24] G. Foo, D.M. Palacios, and G.A. Swartzlander. Optical vortex coronagraph. *Optics Letters*, 30(24):3308–3310, 2005.

[25] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[26] C.H. Bennett, G. Brassard, C. Crépeau, and U.M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[27] T. Durt, B.-G. Englert, I. Bengtsson, and K. Zyczkowski. On mutually unbiased bases. *Internation Journal of Quantum Information*, 8(4):535–640, 2010.

[28] F. Bouchard, F. Hufnagel, Koutný D., A. Abbas, A. Sit, K. Heshami, R. Fickler, and E. Karimi. Quantum process tomography of a high-dimensional quantum communication channel. *Quantum*, 3:138, 2019.

[29] L. Sheridan and V. Scarani. Security proof for quantum key distribution using qudit systems. *Physical Review A*, 82:030301, 2010.

[30] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81:3018, 1998.

[31] H. Rubinsztein-Dunlop, A. Forbes, M.V. Berry, M.R. Dennis, D.L. Andrews, M. Mansuripur, C. Denz, C. Alpmann, P. Banzer, T. Bauer, E. Karimi, L. Marrucci, M. Padgett, M. Ritsch-Marte, N.M. Litchinitser, N.P. Bigelow, C. Rosales-Guzmán, A. Belmonte, J.P. Torres, T.W. Neely, M. Baker, R. Gordon, A.B. Stilgoe, J. Romero, A.G. White, R. Fickler, A.E. Willner, G. Xie, B. McMorran, and A.M. Weiner. Roadmap on structured light. *Journal of Optics*, 19(1):013001, 2016.

[32] R. Bhandari. Synthesis of general polarization transformations. a geometric phase approach. *Physics Letters A*, 138(9):469–473, 1989.

[33] N.R. Heckenberg, R. McDuff, C.P. Smith, and A.G. White. Generation of optical phase singularities by computer-generated holograms. *Optics letters*, 17(3):221–223, 1992.

[34] M.W. Beijersbergen, R.P.C. Coerwinkel, M. Kristensen, and J.P. Woerdman. Helical-wavefront laser beams produced with a spiral phaseplate. *Optics Communications*, 112(5):321–327, 1994.

[35] L. Marrucci, C. Manzo, and D. Paparo. Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media. *Physical Review Letters*, 96(16):163905, 2006.

[36] H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R.W. Boyd, and E. Karimi. Arbitrary optical wavefront shaping spin-to-orbit coupling. *Journal of Optics*, 18(12):124002, 2016.

[37] F. Cardano, E. Karimi, S. Slussarenko, L. Marrucci, C. de Lisio, and E. Santamato. Polarization pattern of vector vortex beams generated by q-plates with different topological charges. *Applied Optics*, 51(10):C1–C6, 2012.

[38] S. Ramachandran, P. Kristensen, and M.F. Yan. Generation and propagation of radially polarized beams in optical fibers. *Optics Letters*, 34(16):455–474, 2009.

[39] S. Ramachandran and P. Kristensen. Optical vortices in fiber. *Nanophotonics*, 2:455–474, 2013.

[40] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85:1330, 2000.

[41] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94:230504, 2005.

[42] C.K. Hong and L. Mandel. Experimental realization of a localized one-photon state. *Physical Review Letters*, 56:58, 1986.

[43] D.L. Fried. Optical resolution through a randomly inhomogeneous medium for very long and very short exposures. *Journal of the Optical Society of America*, 56:1372–1379, 1966.

[44] A.N. Kolmogrov. The local structure of turbulence in incompressible viscous fluids for very large reynolds numbers. *Turbulence: Classic Papers on Statistical Theory*, pages 151–155, 1961.

[45] S. Gang, W. Ning-Quan, X. Li-Ming, and W. Yi. Profile and character of atmospheric structure constant of refractive index c_n^2. *Atmospheric and Oceanic Science Letters*, 5(3):270–272, 2012.

[46] S.A. Sullivan. Experimental study of the absorption in distilled water, artificial sea water, and heavy water in the visible region of the spectrum. *Journal of the Optical Society of America*, 53:962–968, 1963.

[47] R.J. Noll. Zernike polynomials and atmospheric turbulence. *Journal of the Optical Society of America*, 66:207, 1976.

[48] J.R. Fienup. Phase retrieval algorithms: a comparison. *Applied Optics*, 21(15):2758–2769, 1982.