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.

2. Experimental results

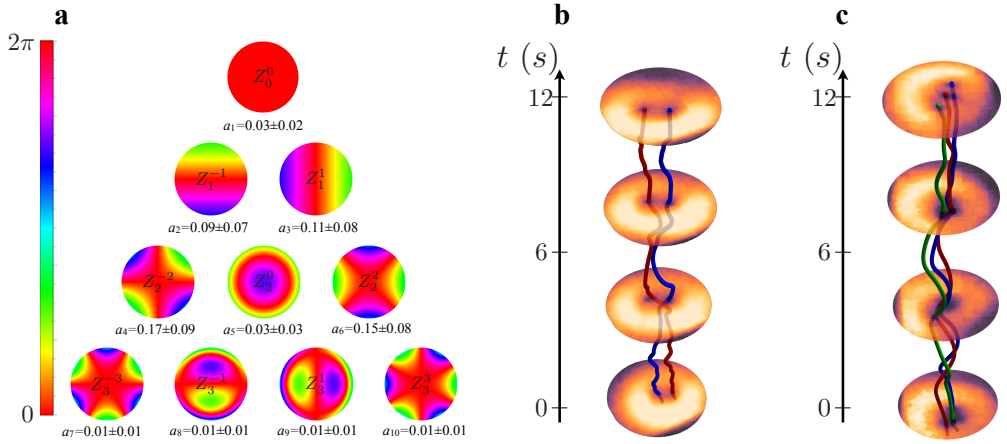

Fig. 1. Experimental characterization of underwater turbulence. (a) Calculated coefficients for the lowest ten Zernike polynomials from intensity images of a Gaussian beam after propagation through 3 m of water to characterize the turbulence in one particular set of conditions at the time of measurement. 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 jets. Further details of the experimental setup are presented in the appendix-B.

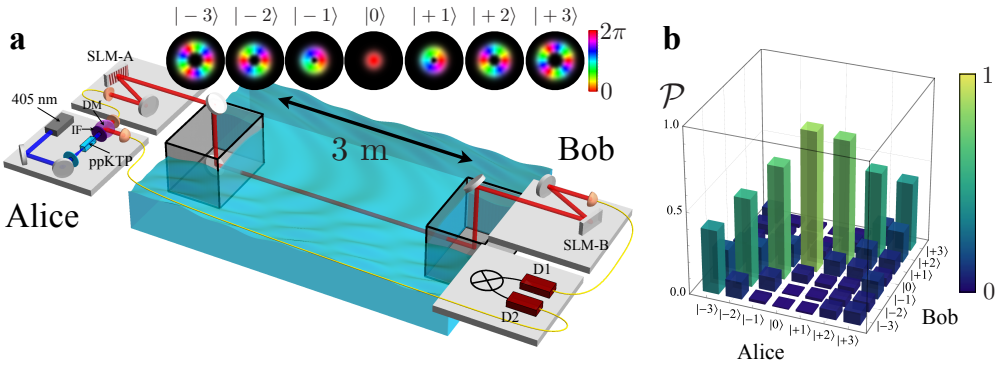

Fig. 2. Experimental setup and state cross-talk measurements. (a) Photon pairs (signal $\lambda_s = 710\ nm$, idler $\lambda_i = 943\ nm$) are generated via spontaneous parametric downconversion pumped from a periodically poled KTP (ppKTP) crystal by a 405 nm diode laser. A long pass filter (IF) blocks 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, the effect of errors is more critical since the protocol must be aborted if the error level exceeds a set threshold.

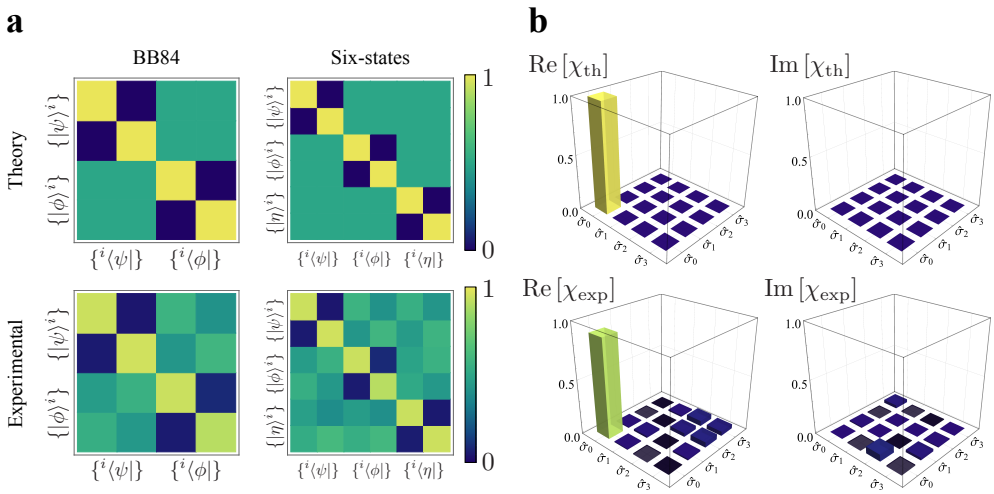

Fig. 3. Probability-of-detection matrices for d=2 BB84 and Six-states protocols, and the channel process matrix. (a) Theoretical and experimentally measured probability-of-detection matrices for BB84 (left column) and Six-states (right column) protocols in $d = 2$. We measured QBERs of $Q = 6.57\%$ and $Q = 6.35$ %, 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

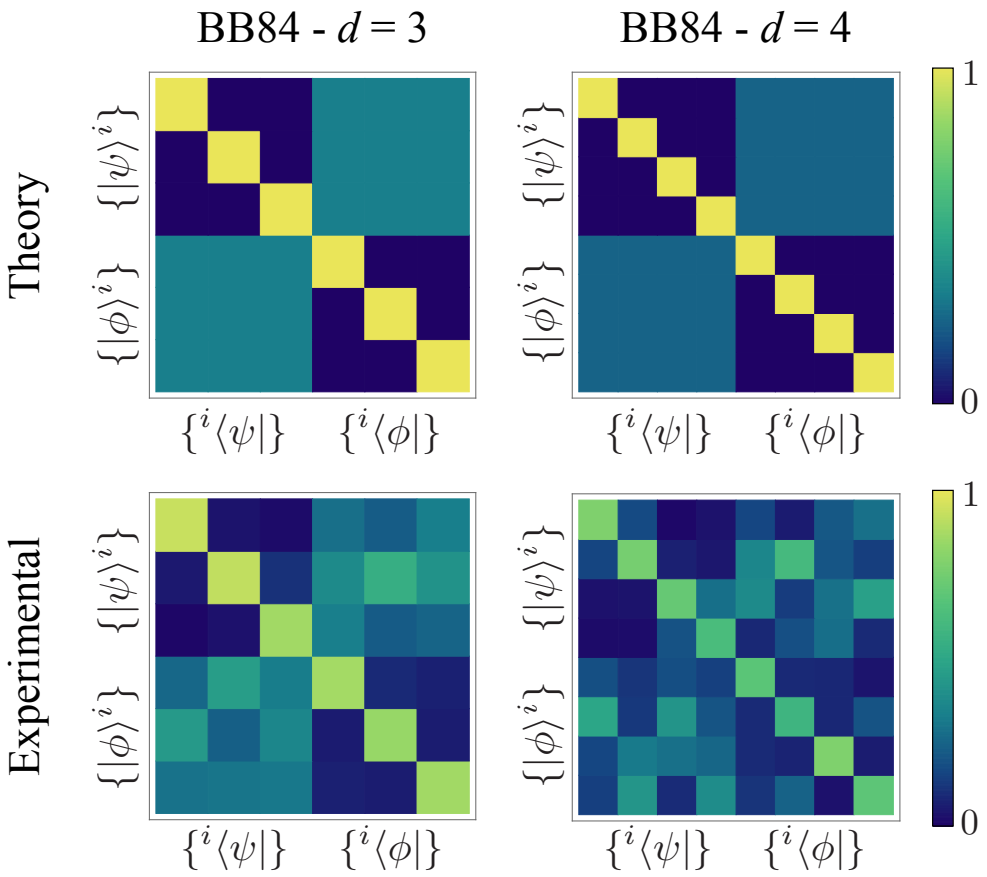

Fig. 4. High-dimensional probability-of-detection matrices. Theoretical (top row) and experimentally measured (bottom row) probability-of-detection matrices for BB84 protocols in $d = 3$ and $d = 4$. We measured QBER of $Q^{3D} = 11.73\%$ and $Q^{4D} = 29.77\%$, respectively. The QBER in $d = 3$ is below 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

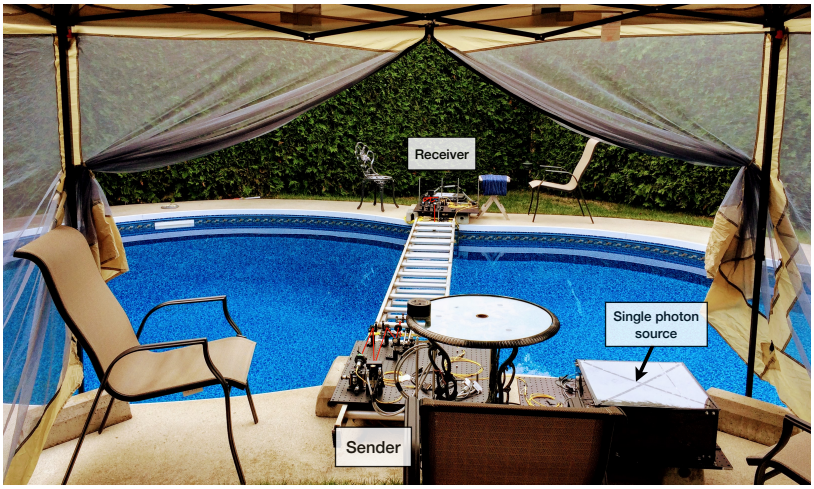

Fig. 5. Image of outdoor underwater link in an in-ground swimming pool. The single photon source, on the sender's side, is enclosed within a black box. The sender's setup is mounted on an optical breadboard and consists of a microscope objective stage, a spatial light modular, mirrors and a periscope 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, $\Phi(r, \varphi) = \sum_j a_j Z_j(r, \varphi)$ as defined in the main text. Explicitly, the Zernike polynomials are

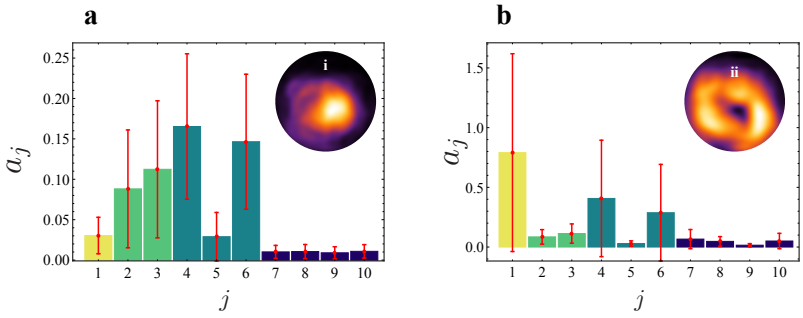

Fig. 6. Characterization of underwater turbulence. (a) Experimentally obtained coefficients for an input gaussian ($\ell = 0$) mode. Inset **i**, shows an example of a distorted gaussian beam profile at the output of the channel. The Zernike decomposition was carried over a disk with a radius of 2.1 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.

Optics EXPRESS

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

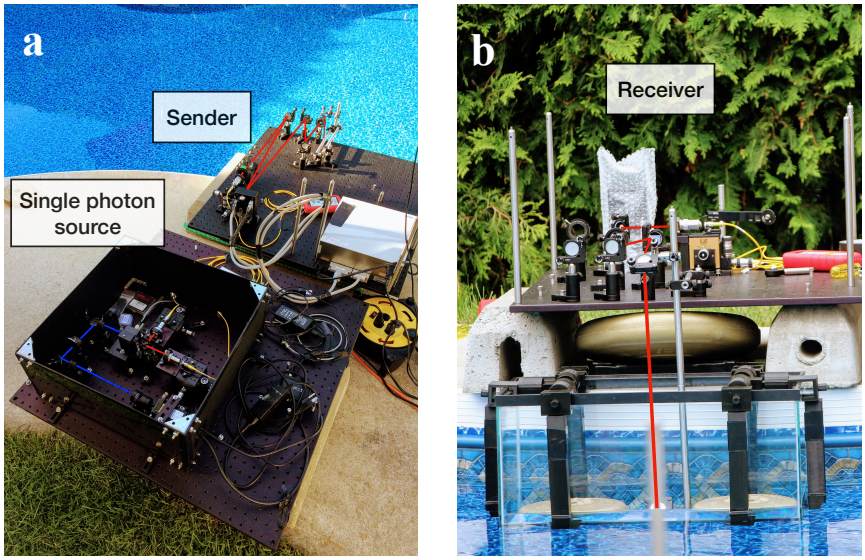

Fig. 7. Sender and receiver setup of the outdoor underwater link. (a) Close-up of the single photon source and the sender's setup. The blue line represents the pump beam and the red lines represent the signal and idler beams. (b) Close up of the receiver's aquarium, periscope and setup.

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).