

High-Dimensional Quantum Information: From Sensing to Underwater Quantum Communication

by

Felix Hufnagel

Thesis submitted to the University of Ottawa

In partial fulfillment of the requirements

For the degree of

Master of Science in Physics

Department of Physics

University of Ottawa

© Felix Hufnagel, Ottawa, Canada, 2020

Abstract

Quantum information has become an exciting field of research in the last 20 years, as experimental advancements allow us to control, manipulate, and detect states of quantum systems. A subset of this field studies the application of high-dimensional quantum states in communication, computing, and metrology. Specifically, this thesis explores the use of the high-dimensional Laguerre-Gaussian (LG) and vector vortex optical modes in underwater quantum communication channels. Making use of these high-dimensional states in quantum communication provides certain advantages including increased security and increased information capacity. We investigate underwater channels characterized by large optical turbulence and signal attenuation. These two challenges are of significant interest underwater communication channels. The detection of high-dimensional states also provides a great challenge for efficiently performing quantum information tasks as the dimensionality of the system increases. Here we study three different sensing sensing protocols, demonstrating how compressed sensing techniques can be very useful for high-dimensional quantum systems. In particular we perform high dimensional quantum process tomography, develop a compressed sensing protocol for LG modes which requires only intensity measurements, and a generalized adaptive compressed sensing protocol which can be used in any high-dimensional quantum systems.

Acknowledgements

I would like to first thank Ebrahim Karimi for providing me the opportunity to pursue science, and for encouraging me to explore the things I find exciting. I could not ask for more from a supervisor and have enjoyed our discussions, scientific and otherwise.

It brings me incredible joy to be able to thank Frédéric Bouchard, Alicia Sit, and Hugo Larocque for being entertaining friends and exceptional scientists. I have fond memories of staying up all night performing an experiment with each of you, and of having fun at conferences together. Frédéric has been a great mentor, showing me how to be a scientist through his persistence in solving problems and his excitement for science. Hugo's attention to quality work and precision has been an inspiration. I admire the encouragement and kindness shown by Alicia to all of her peers. Her knowledge and dedication as an experimentalist has taught me much.

I would also like to thank Yingwen Zhang, Khabat Heshami, and Duncan England for stimulating discussions and exciting collaborations. I wish to thank Luis Lorenzo Sánchez-Soto who shows great passion for discovering new science. I want to thank Florence Grenapin and Noah Staudte for their enthusiasm in attacking scientific problems. I must also thank Dominic Mortimer and Nicolas Couture for their friendship as we studied physics together. I would also like thank all the members of the SQO group, past and present, who have made such a great environment for research.

Lastly I thank my parents, John and Rhonda, and my papa, Ross, for their continuous love and support. I thank my sister, Aisha, for laughing with me and for making me smile.

Table of Contents

Abstract	ii
Acknowledgements	iii
List of publications	vi
Statement of originality and collaborative contributions	viii
1 Introduction	1
2 Quantum Sensing in High-Dimensional Hilbert Spaces	4
2.1 Quantum measurement	5
2.2 Spatial Modes	7
2.3 Compressed Sensing	10
2.4 Publication: Quantum process tomography of a high-dimensional quantum communication channel	11
2.5 Publication: Compressed sensing of twisted photons	24
2.6 Publication: Adaptive Compressive Tomography with No a priori Information	33
3 Underwater Quantum Communication	38
3.1 Quantum Key Distribution	39
3.2 Optical Turbulence	41
3.3 Publication: Quantum cryptography with twisted photons through an outdoor underwater channel	43

3.4	Publication: Characterization of an underwater channel for quantum communications in the Ottawa River	54
3.5	Publication: Underwater quantum communication over a 30-meter flume tank	63
4	Conclusions	70
	Bibliography	72

List of publications

1. **F. Hufnagel**, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, & E. Karimi, “Underwater quantum communication over a 30-meter flume tank”, *arXiv:2004.04821* (2020)
2. **F. Hufnagel**, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, & E. Karimi, “Characterization of an underwater channel for quantum communications in the Ottawa River”, *Optics Express* **27**, 26346-26354 (2019).
3. F. Bouchard, **F. Hufnagel**, D. Koutný, A. Abbas, A. Sit, K. Heshami, R. Fickler, & E. Karimi, “Quantum process tomography of a high-dimensional quantum communication channel”, *Quantum* **3**, 138 (2019).
4. F. Bouchard, D. Koutný, **F. Hufnagel**, Z. Hradil, J. Řeháček, Y. S. Teo, D. Ahn, H. Jeong, L. L. Sánchez-Soto, G. Leuchs, & E. Karimi, “Compressed sensing of twisted photons”, *Optics Express* **27**, 17426-17434 (2019).
5. D. Ahn, Y. S. Teo, H. Jeong, F. Bouchard, **F. Hufnagel**, E. Karimi, D. Koutný, J. Řeháček, Z. Hradil, G. Leuchs, & L. L. Sánchez-Soto, “Adaptive Compressive Tomography with No a priori Information” *Physical Review Letters* **122**, 100404 (2019).
6. F. Bouchard, A. Sit, **F. Hufnagel**, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, & E. Karimi, “Quantum cryptography with twisted photons through an outdoor underwater channel”, *Optics Express*

26, 22563-22573 (2018).

7. G. S. Thekkadath, **F. Hufnagel**, & J. S. Lundeen, “Determining complementary properties using weak-measurement: uncertainty, predictability, and disturbance”, *New Journal of Physics* **20**, 113034 (2018).

Statement of originality and collaborative contributions

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

F. Bouchard, K. Heshami, and E. Karimi initiated the work in chapter 2 on process tomography. F. Hufnagel, A. Abbas, and F. Bouchard performed the experiment. F. Bouchard and D. Koutný analysed the data. F. Bouchard wrote the manuscript with help from all authors. All authors contributed to the discussion of the results.

L. L. Sánchez-Soto, G. Leuchs, & E. Karimi initiated the work in chapter 2 on compressed sensing of twisted photons. F. Hufnagel and F. Bouchard performed the experiment. The theory was developpe by Y. S. Teo, D. Ahn, and H. Jeong. The data was analysed by D. Koutný, Z. Hradil, and J. Řeháček. L. L. Sánchez-Soto wrote the manuscript with help from all authors. All authors contributed to the discussion of the results.

L. L. Sánchez-Soto, G. Leuchs, & E. Karimi initiated the work in chapter 2 on adaptive compressed sensing. F. Hufnagel and F. Bouchard performed the experiment. The theory was developpe by Y. S. Teo, D. Ahn, and H. Jeong. The data was analysed by D. Koutný, Z. Hradil, and J. Řeháček. L. L. Sánchez-Soto wrote the manuscript with help from all authors. All authors contributed to the discussion of the results.

F. Hufnagel, F. Bouchard, A. Sit, A. Abbas, and E. Karimi initiated the work in chapter 3 on quantum cryptography with twisted photons. F. Hufnagel, F. Bouchard, A. Sit, and A. Abbas performed the experiment. F. Hufnagel, F. Bouchard, A. Sit, and K. Heshami analysed the data. F. Hufnagel, F. Bouchard, A. Sit, and E. Karimi wrote the manuscript with help from all authors. All authors contributed to the

discussion of the results.

F. Hufnagel, A. Sit, and E. Karimi initiated the work in chapter 3 on quantum communication in the Ottawa River. F. Hufnagel, A. Sit, and F. Grenapin performed the experiment. F. Hufnagel, A. Sit, and F. Bouchard analysed the data. F. Hufnagel wrote the manuscript with help from all authors. All authors contributed to the discussion of the results.

F. Hufnagel, A. Sit, F. Bouchard, B. J. Sussman, and E. Karimi initiated the work in chapter 3 on quantum communication through a flume tank. F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, and D. England performed the experiment. F. Hufnagel, F. Bouchard, and K. Heshami analysed the data. F. Hufnagel wrote the manuscript with help from all authors. All authors contributed to the discussion of the results.

Chapter 1

Introduction

Quantum mechanics was born in the early years of the twentieth century out of a desire to explain the experimentally observed phenomena in black-body radiation, the atomic emission spectrum, the photoelectric effect, and later the Compton effect. In 1905 Einstein's proposal that light is carried in discrete energy packets, explained the problem of electron emission observed in the photoelectric effect [1]. Indeed, Einstein extended Planck's ideas from 5 years earlier which discretized the emission spectrum in blackbody radiation, though Planck did not realize that it was in fact the electromagnetic field that was inherently discrete as opposed to just the radiator. Though not giving it this name, Einstein had recognized the discretization of electromagnetic radiation in packets which would later be called photons. Einstein was present at the birth of quantum theory, though later he would come to fight against the strange predictions that would arise upon carrying the postulates of the theory to its conclusion. Two of the strange predictions of quantum theory come from the work of Heisenberg, in 1927, and are closely related [2]. Those being the uncertainty principle and the property that measurement of a system introduces a disturbance on the system. These properties, along with the superposition principle, provide the necessary instruments for the field of quantum information.

In 1935 the famous Einstein, Podolsky, Rosen (EPR) paper introduced the concept of entanglement which shows the strangeness of quantum theory, and allows for some of the powerful applications of quantum information [3]. The EPR paper was written in opposition to quantum theory, suggesting that the conclusions which could be reached by extending the wave function description were ridiculous and could not correspond to reality. I will briefly dive into the arguments made in this paper just to show the strange properties displayed by quantum mechanics to the reader who

has not had the pleasure of learning about quantum mechanics. They began by considering 2 quantum systems which were made to interact for some time. If we assume that we know the initial states of each system before the interaction then we are able to calculate the wave function of the combined system. However, we are unable to find the exact state of either particle without performing a measurement. Let us now consider that we would like to make a measurement of the position of particle 1. In the position basis, we can write the wave function as a product of orthogonal function

$$\Psi(x_1, x_2) = \sum_{n=0}^{\infty} u_n(x_1) \psi_n(x_2), \quad (1.1)$$

where the $u_n(x_1)$ are the position eigenfunctions of particle 1 with eigenvalues α_n . If a measurement now yields the result α_k , then the total wave function "reduces" to $\Psi(x_1, x_2) = u_k(x_1) \psi_k(x_2)$, thus giving the wave function of $\psi_k(x_2)$ for particle 2. We could instead have chosen to make a measurement on the momentum of particle 1. Now, we are not in the basis of functions $u_n(x_1)$, so the general wave function is given by

$$\Psi(x_1, x_2) = \sum_{n=0}^{\infty} \nu_n(x_1) \phi_n(x_2). \quad (1.2)$$

Now if particle 1 is measured to be in the state $\nu_j(x_1)$, then the state of the total system reduces to $\Psi(x_1, x_2) = \nu_j(x_1) \phi_j(x_2)$, thus giving the wave function of $\phi_j(x_2)$ for particle 2. What Einstein and his colleagues found so distressing was that the choice of measurement on particle 1 changes the wave function of particle 2, bringing into question our idea on the existence of reality. EPR concluded that quantum mechanics in its form at that time was incomplete, and thus requires additional information, such as hidden variables, in addition to the wave function. This property of quantum mechanics is now referred to as entanglement. Thirty years later, John Bell developed a theorem which proved that this is in fact how quantum systems behave, and that there are no local additional parameters, local hidden variables, that can reproduce the quantum mechanical behaviour of an entangled system. [4]. The weirdness of quantum mechanics allowed the physicists of the early 20th century to understand and describe the physical systems around them such as radiation and the atom. Toward the turn of the 21st century however, physicist began to focus on how to use quantum mechanics to accomplish previously impossible tasks. This harnessing of quantum mechanics is the field of quantum information, which can be broadly divided into quantum computation, quantum communication, quantum simulation, and quantum metrology.

In chapter 2 the problem of measuring high dimensional quantum states and processes is presented through 3 separate papers. The first is an experimental demonstration of quantum process tomography for various hacking attacks on a quantum communication channel. The second paper outlines a new compressed sensing protocol for low rank spatial modes of light. The third paper introduces a new adaptive compressed sensing protocol, which is experimentally demonstrated using spatial modes of light. In chapter 3 underwater quantum communication is explored through 3 separate papers. These papers are the progression of our work in underwater channels including: a 3 meter channel in an outdoor swimming pool, a 5 meter channel in the Ottawa River, a 30 meter channel in a flume tank.

The articles included are self-sufficient in terms of describing the methods used, and also in providing a comprehensive literature review of the current research. Thus, I have chosen to not restate all of this in the chapter introductions, but rather would like to briefly introduce a few of the fundamental concepts such that the reader who has not studied the subjects gains some insight as to where these ideas come from.

Chapter 2

Quantum Sensing in High-Dimensional Hilbert Spaces

This chapter is based on the following papers:

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

DOI: <https://doi.org/10.22331/q-2019-05-06-138>

© 2019 Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften

2. F. Bouchard, D. Koutný, **F. Hufnagel**, Z. Hradil, J. Řeháček, Y. S. Teo, D. Ahn, H. Jeong, L. L. Sánchez-Soto, G. Leuchs, & E. Karimi, “Compressed sensing of twisted photons”, *Optics Express* **27**, 17426-17434 (2019).

DOI: <https://doi.org/10.1364/OE.27.017426>

© 2019 Optical Society of America

3. D. Ahn, Y. S. Teo, H. Jeong, F. Bouchard, **F. Hufnagel**, E. Karimi, D. Koutný, J. Řeháček, Z. Hradil, G. Leuchs, & L. L. Sánchez-Soto, “Adaptive Compressive Tomography with No a priori Information” *Physical Review Letters* **122**, 100404 (2019).

DOI: <https://doi.org/10.1103/PhysRevLett.122.100404>

© 2019 American Physical Society

2.1 Quantum measurement

As shown in the introduction, the task of measuring a quantum system is not trivial. Heisenberg's uncertainty principle restricts us from learning the total state of a quantum system through multiple measurements on a quantum system. The action of making a measurement and how it will affect the system being measured must be carefully considered. The Born rule forms the basis for the theory of quantum measurement stating how we can relate a measured result to the wave function of a quantum system [5]. Generally, the Born rule states that the probability of finding a quantum system in a particular state is given by the square of the wave function at that point. For discrete variables, the probability of finding a quantum state $|\psi\rangle$ in an eigenstate $|a_i\rangle$ is given by $p(a_i) = |\langle a_i|\psi\rangle|^2$. This is generalized to continuous quantum systems by formulating the probability density function as $p(x, y, z) = |\psi(x, y, z)|^2$. In the mid 1920's, many of the early researchers of quantum theory were developing mathematical frameworks hoping to adequately and satisfyingly describe all of the observations of quantum mechanics [6]. The approach outlined by John Von Neumann in 1927 succeeded in this, and is now the most commonly used approach to quantum mechanics. With 2 papers in 1927, Neumann introduced the use of the Hilbert space, spectral theorem, and density operator; all of which are fundamental to our current understanding of quantum theory [7, 8]. These tools are fundamental to the quantum measurement theory, and in particular the density operator formalism provides the groundwork for compressed sensing.

The Hilbert space is a complete vector space having an inner product. For its application to quantum mechanics it is an infinite dimensional space in which the quantum states are represented by points in this abstract space. A quantum state is uniquely determined in this space by a density matrix which allows us to describe both pure states, and mixed states which consist of an incoherent superposition of pure states. Mathematically the density matrix is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|, \quad (2.1)$$

where $|\psi_i\rangle = \sum_n c_n |a_i\rangle$ are the pure states and p_i are the probabilities of the respective state. Here we have generalized to show that the pure states $|\psi_i\rangle$ can be made up of a coherent superposition of the eigenvectors. This is not the same as having a probabilistic mixture of states as in ρ . The unit vectors of the Hilbert space are the pure states, i.e., the eigenvectors of an observable. We can measure the probability amplitude of a quantum system being in a certain eigenstate by projecting onto these unit vectors. We are able to change the basis that we make a measurement in by changing the coordinate system, thus the observables which we measure such as position, momentum, polarization, etc. are represented by linear operators acting on the Hilbert space. Taking some observable A , we define its operator as

$$\hat{A} = \sum_i a_i |a_i\rangle \langle a_i|, \quad (2.2)$$

where a_i are the eigenvalues for the eigenvectors $|a_i\rangle$ of our observable. The expectation value of this observable is given by the trace over the product of the operator with the density matrix $\mathcal{E}(A) = \text{Tr}(\rho \hat{A})$. If we consider the special case where we have a pure state then $\rho = |\psi\rangle \langle \psi|$. Putting this into our trace formula we get

$$\mathcal{E}(\hat{A}) = \text{Tr}(|\psi\rangle \langle \psi| \hat{A}) = \langle \psi | \hat{A} | \psi \rangle, \quad (2.3)$$

which is equivalent to the Born rule.

Our goal in deriving strategies for quantum measurement is to come up with a set of measurement operators whose probabilities will give us enough information to determine the quantum state ρ . When we want to observe photons, the result of us making a measurement is usually that we destroy the quantum system – the photon – during the measurement process. However, we require more than a single measurement setting to learn the total state of a quantum system, i.e., ρ . Thus, what we will do is prepare an ensemble of identical photons, and make the different measurements on different photons. This method of measuring the quantum state is called quantum state tomography. The precise mathematical framework of quantum state tomography was introduced by Fano in 1957 [9]. We will usually be interested in a particular property of a quantum system. Taking the photon for example, we may be interested in determining the polarization of the photon while ignoring the frequency, spatial mode, momentum, etc. The number of orthogonal pure states will determine the number of rows and columns making up our density matrix. For polarization we have two orthogonal pure states, $\{|L\rangle, |R\rangle\}$, the left and right circular polarizations. The linear polarization states are given by the linear combination of the circular polarizations: $|H\rangle, |V\rangle = (|L\rangle \pm |R\rangle)/\sqrt{2}$ and $|A\rangle, |D\rangle = (|L\rangle \pm i|R\rangle)/\sqrt{2}$. Since there

are two orthogonal pure states, the polarization state can be uniquely defined by a 2 by 2 density matrix. The density matrix is required to be Hermitian and have unit trace which leaves us with $N^2 - 1$ independent matrix elements for a system with N orthogonal pure states. Therefore we require at least this many measurements in order to uniquely determine a quantum state. This is not an issue when determining the polarization of a photon, however, as we move to quantum systems with higher dimensions, N^2 can become very large making characterizing these high dimensional quantum states difficult. In quantum information, there are many applications where the use of a high dimensional quantum systems is advantages. For these high dimensional quantum states to be practical we must be able to characterize them effectively.

Instead of measuring the quantum state, we can also be interested in characterizing a quantum process. We call this quantum process tomography[10]. It is very similar to state tomography in that we must come up with measurement operators which allow us to completely characterize a matrix; however, now we must fully cover the possible inputs and possible outputs of the quantum system. The quantum process can be given by

$$\mathcal{E}(\rho) = \sum_{m,n} \chi_{mn} \sigma_m \rho \sigma_n, \quad (2.4)$$

where the set of σ_i form a complete and orthogonal set of operators. In 2 dimensions these are the Pauli matrices and in higher dimensions they are the Gell-Mann matrices. Here χ is the called the process matrix. In the first paper of this chapter we perform process tomography on quantum communication channels in up to 5 dimensions.

2.2 Spatial Modes

The high dimensional quantum system that we will focus on is the spatial modes of light. As we have discussed, one property of photons is polarization, which is a 2 dimensional system. There are other photonic degrees of freedom that can be used in quantum information. Usually we think of light being in a Gaussian transverse spatial distribution. This is the mode that is most naturally produced in a laser cavity. When we consider monochromatic light, we can reduce the Maxwell's equation to the Helmholtz equation. Furthermore we will use the paraxial approximation for the case in which the transverse amplitude of the electromagnetic field is slowly varying with respect to z , the direction of propagation. The Laguerre-Gaussian modes are

one orthogonal set of solutions to the paraxial wave equation. These modes form a discrete orthogonal set of states in two variables, ℓ and p . In cylindrical coordinates, (r, ϕ, z) these modes are given by

$$\begin{aligned} \text{LG}_{\ell,p}(r, \phi, z) &= \sqrt{\frac{2p!}{\pi (p + |\ell|)!}} \frac{1}{w(z)} \left(\frac{\sqrt{2}r}{w(z)} \right)^{|\ell|} L_p^{|\ell|} \left(\frac{2r^2}{w(z)^2} \right) \\ &\times \exp \left(-r^2 \left[\frac{1}{w(z)^2} - i \frac{k}{2R(z)} \right] + i\ell\phi + i\zeta_{\ell,p}(z) \right), \end{aligned} \quad (2.5)$$

where ℓ and p are the azimuthal and radial mode indices respectively. $L_p^{|\ell|}$ are the generalized Laguerre polynomials. $w(z)$ and $R(z)$ are the beam waist and radius of curvature at z . $\zeta_{\ell,p}(z) = (2p + |\ell| + 1) \arctan(z/z_R)$ is the Gouy phase shift.

One interesting aspect of the Laguerre-Gauss modes is that they can carry orbital angular momentum (OAM) determined by the azimuthal phase term $\exp(i\ell\phi)$. These OAM modes have a phase variation about the axis of propagation which results in a phase singularity, and thus an intensity null, at their centre. The magnitude of the OAM is given by $\ell\hbar$ per photon, and it has been shown that this momentum can be transferred to particles. What we are interested in is the relative ease with which we are able to create these OAM modes, which we can use as a high dimensional Hilbert space for quantum information tasks. We can create superposition modes out of these OAM states giving us access to multiple orthogonal bases which are important for quantum key distribution, the subject of chapter 3. Another interesting term in the LG modes is the Gouy phase. This term describes the phase shift experienced by an LG mode as it propagates. The Gouy phase has a linear dependence on $|\ell|$, which means that different OAM modes will experience a different Gouy phase. We are able to take advantage of this in some measurement techniques as the intensity profile of different modes will behave differently depending on the ℓ values that they hold.

The most common method for measuring spatial modes is the phase flattening technique [11]. To understand this method, we must realize first that we can add a phase to any light beam. A focussing lens is the most common way that we add phase to an incoming beam of light. In this case the phase which we add is dependent on radial distance from the centre of the lens. A lens with a focal length f adds a phase term of $\exp(ikr^2/2f)$ where r is the radial coordinate and k is the beam's wavevector. After the lens, the beam has this added phase which results in the focussing or diverging in accordance with f . For the LG modes, we have both an azimuthal and radial phase dependence. The phase flattening technique involves the addition of the

phase one has chosen to measure on the incoming light. When the imprinted phase is the inverse of that of the incoming light, the transverse phase profile is flattened, which results in a Gaussian-like beam in the far-field. This beam can then couple to a single mode fibre because it does not possess azimuthal phase. An incoming beam with any other azimuthal phase will not be able to couple to the fibre. In this way we are able to perform projective measurements in orthogonal basis states to reconstruct the quantum state topographically. Spatial light modulators (SLM) are one of the most common and versatile equipment for adding arbitrary transverse phases to optical beams. SLMs have liquid crystal pixels which give control of the phase at each pixel. For example, the SLMs used in most of these works have displays of 600 by 800 pixels. Liquid crystal has birefringent properties which can be controlled by applying heat or an electric voltage. In the SLMs the voltage of each pixel is tuned to determine the birefringence, resulting in a desired phase delay at that pixel. Though less versatile, another method of generating and measuring spatial modes is q-plates. These are tunable liquid crystal plates in which the orientation of the liquid crystals has been aligned with transverse dependence. For generating an OAM mode this would be an azimuthal dependence. In these devices, the birefringence is dependent on the angle between the incident polarization, and the orientation of the liquid crystal. Thus, we again achieve spatial control of the polarization states. The voltage can be used to tune the q-plate for operation at different wavelengths. This is given by,

$$\begin{bmatrix} \mathbf{e}_L \\ \mathbf{e}_R \end{bmatrix} \xrightarrow{\text{QP}} \cos\left(\frac{\delta}{2}\right) \begin{bmatrix} \mathbf{e}_L \\ \mathbf{e}_R \end{bmatrix} + \sin\left(\frac{\delta}{2}\right) \begin{bmatrix} \mathbf{e}_R e^{2i\alpha(x_1, x_2)} \\ \mathbf{e}_L e^{-2i\alpha(x_1, x_2)} \end{bmatrix}, \quad (2.6)$$

where $\alpha(x_1, x_2)$ is the spatial distribution of the phase being added to the beam, $\mathbf{e}_L$ and $\mathbf{e}_R$ stand for the left and right polarization states, and δ is the tuning parameter controlled by the applied electric field. Here the q-plate is perfectly tuned, resulting in the total conversion of the incoming beam, when the $\cos(\frac{\delta}{2})$ term is equal to zero. It can be seen by the above equation that one can produce beams with a spatially dependent phase using these q-plates. One can also produce beams with spatially varying polarization by sending a linear or elliptical polarization state onto the q-plate. This produces modes which combine the spatial degree of freedom with the polarization degree of freedom. These modes described more in the paper *Underwater quantum communication over a 30-meter flume tank*, in chapter 3.

2.3 Compressed Sensing

High-dimensional quantum states have applications for many fields of quantum information; however, as the dimension grows it becomes increasingly difficult to characterize quantum states with practical efficiency. To determine the density matrix of any arbitrary quantum state, it is necessary to make at least $N^2 - 1$ measurements as previously stated. Consider briefly a pure state. This can be given by just one of the indices of the density matrix, with zeros everywhere else. In the same way we can have nearly pure, or low rank, states whose density matrices have only a small number of non-zero elements. These low rank density matrices tempt us to try to find a more efficient set of measurements which would yield all the information necessary to determine the quantum state ρ . In the most broad sense, the attempt to reduce the number of measurements needed to characterize high-dimensional states is called compressed sensing and was realized in 2006 for image processing [12]. These ideas were first applied to quantum states in 2010 [13]. Here they consider a many qubit system with dimension $d = 2^n$ where n is the number of qubits. They show that for systems with low rank $r \ll d$ they are able to uniquely determine the quantum state with $O(r d \log_2(d))$ measurement settings as opposed to $O(d^2)$. The n -qubit measurement operators $w = \otimes_{i=1}^n w_i$ are constructed with the tensor product of 2 dimensional Pauli matrices $w_i \in \{\mathbb{1}, \sigma_1, \sigma_2, \sigma_3\}$. At random $m = c r d \log_2(d)$ different measurement operators w are chosen. Using the probabilities attained from the randomly selected measurement settings, a convex optimization can be performed to determine ρ with a probability of failure exponentially decreasing with c . These results have been pushed forward over the last ten years, leading to the works presented here. The second paper, *Compressed sensing of twisted photons*, incorporates the main ideas of compressed sensing for low rank states, with the Gouy phase property of LG modes to create a measurement technique which requires only making intensity measurements of the LG modes at a few different propagation distances. This compressed sensing protocol is applicable only to spatial modes of light. On the other hand the third paper, *Adaptive Compressive Tomography with No a priori Information*, presents a compressed sensing protocol which can be applied to any quantum system. Here, the measurement process is separated into different steps. Between steps, information from the previous measurement results is used to restrict the space that is explored in the next steps.

Quantum process tomography of a high-dimensional quantum communication channel

Frédéric Bouchard¹, Felix Hufnagel¹, Dominik Koutný², Aazad Abbas¹, Alicia Sit¹, Khabat Heshami³, Robert Fickler^{1 4 5}, and Ebrahim Karimi^{1 6}

¹Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, ON, K1N 6N5, Canada.

²Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic.

³National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada

⁴Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria.

⁵Current address: Photonics Laboratory, Physics Unit, Tampere University, Tampere, FI-33720, Finland.

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

April 30, 2019

The characterization of quantum processes, e.g. communication channels, is an essential ingredient for establishing quantum information systems. For quantum key distribution protocols, the amount of overall noise in the channel determines the rate at which secret bits are distributed between authorized partners. In particular, tomographic protocols allow for the full reconstruction, and thus characterization, of the channel. Here, we perform quantum process tomography of high-dimensional quantum communication channels with dimensions ranging from 2 to 5. We can thus explicitly demonstrate the effect of an eavesdropper performing an optimal cloning attack or an intercept-resend attack during a quantum cryptographic protocol. Moreover, our study shows that quantum process tomography enables a more detailed understanding of the channel conditions compared to a coarse-grained measure, such as quantum bit error rates. This full characterization technique allows us to optimize the performance of quantum key distribution under asymmetric experimental conditions, which is particularly useful when considering high-dimensional encoding schemes.

1 Introduction

Quantum information science has witnessed the emergence of a wide range of new technologies and applications [1]. Quantum cryptography [2], quantum computation [3] and quantum sensing [4] are examples of promising venues for a possible next technological revolution. In order to construct complex quantum machines or quantum networks, a full characterization of its building blocks is critical. A method for reconstructing the action of a component in a quantum system is known as *quantum process tomography* (QPT) [5, 6]. Previously, QPT has been performed to characterize several quantum physical systems, such as liquid-state NMR [7, 8], photonic qubits [9], atoms in optical lattices [10], trapped ions [11], solid-state qubits [12], continuous-variable quantum states [13], semiconductor quantum dot qubits [14] and, recently, nonlinear optical systems [15]. Another class of important quantum systems that can benefit from full characterization are quantum channels and components for quantum key distribution (QKD) and quantum communications [16, 17], where, so far, quantum channels may be categorized as optical fibre [18], line-of-sight free-space [19] and ground-to-satellite (satellite-to-ground) [20] links.

The benefits of fully characterizing quantum communication channels lie at a better understanding of possible error sources and, more importantly, on the detection of the potential presence of an eavesdropper, namely *Eve*, tapping

Frédéric Bouchard: 

into the quantum channel. Her presence is revealed in the form of noise introduced in the channel. The authorized partners, typically referred to as *Alice* and *Bob*, may estimate noise levels in the channel to assess the amount of leaked information to Eve. After this error assessment, Alice and Bob may perform classical post-processing protocols, such as *privacy amplification* [21], in order to remove Eve's leaked information. Conventional methods for secure key rate analysis rely on symmetry assumptions to associate an average (coarse-grained over all preparation and measurement settings) bit error rate parameter to a reduction in secure key rates. However, experimental errors often tend to break these symmetry assumptions, motivating the use of numerical techniques in QKD [22].

While usual QKD schemes rely on encoding quantum information in two-level systems, i.e. qubits, there exists a particular class of QKD schemes known as *high-dimensional* QKD protocols [23, 24]. High-dimensional schemes have the potential advantage of tolerating larger noise levels in the channel and carrying more than one bit of information per carrier. So far, a full characterization of high-dimensional processes based on QPT has not been achieved experimentally. With the emergence of high-dimensional quantum information, QPT will become an essential tool for the characterization of complex experiments dealing with high-dimensional quantum states. As a physical implementation, the orbital angular momentum (OAM) of photons represents a promising route for high-dimensional encoding due to the maturity of its generation and detection schemes [25, 26]. OAM states, corresponding to helical wavefronts of the form $\exp(i\ell\varphi)$, where the OAM value ℓ is an integer and φ is the azimuthal coordinate, may be realized using single phase elements. Computer-generated holograms displayed on a spatial light modulator (SLM) provide a simple and versatile method for generating and manipulating these modes [27]. High-dimensional QKD has been demonstrated experimentally using OAM in the laboratory [28, 29, 30], in intra-city free-space links [31, 32, 33] and, recently, in other types of quantum links [34].

Here, we demonstrate the benefits of a full characterization of a quantum channel through quantum process tomography. This full charac-

terization will allow us to complement the numerical approach in [22] to optimize secure key rates under specific experimental conditions and to develop new protocols lacking symmetry that may outperform existing approaches.

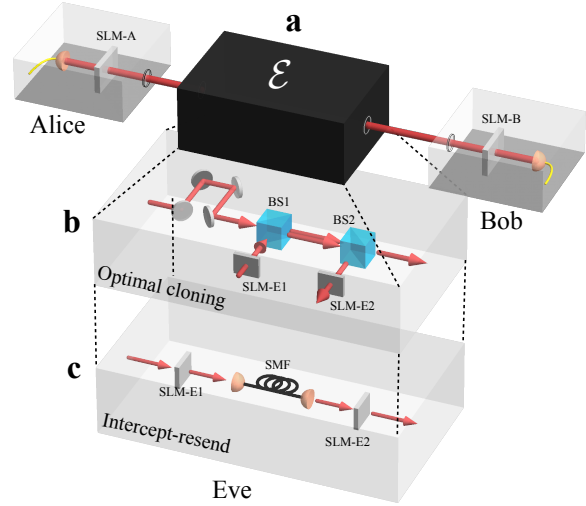


Figure 1: Simplified experimental setup. **a** Alice's preparation stage consists of a single photon source (not shown) that feeds the heralded photons to a generation apparatus consisting of a spatial light modulator (SLM-A). Alice's photon is subsequently sent into the quantum channel which is considered as a black box with quantum process $\mathcal{E}$. The output of the black box is fed to Bob's detection stage consisting of a spatial light modulator (SLM-B) and a single-mode optical fibre (SMF), via performing phase-flattening. We experimentally consider three different types of processes for our quantum channel: an ideal channel with no attack, the case of an optimal cloning attack (**b**), and the case of an intercept-resend attack (**c**). In particular, the configuration of the optimal cloning scheme consists of an SLM (SLM-E1) which generates a completely mixed state that is fed to the Hong-Ou-Mandel type interferometer at a balanced beam splitter (BS1). The *cloned* photons are then sent into a second beam splitter (BS2) in order to spatially separate them. Eve can use a second SLM (SLM-E2) to measure the state of her cloned photon while sending the other cloned photon to Bob. The experimental configuration of the intercept resend consists of two SLMs (SLM-E1 and SLM-E2) sandwiching a SMF.

2 Theory of quantum process tomography

Let us set the stage by introducing the basic concepts of QPT. The goal of QPT is to determine

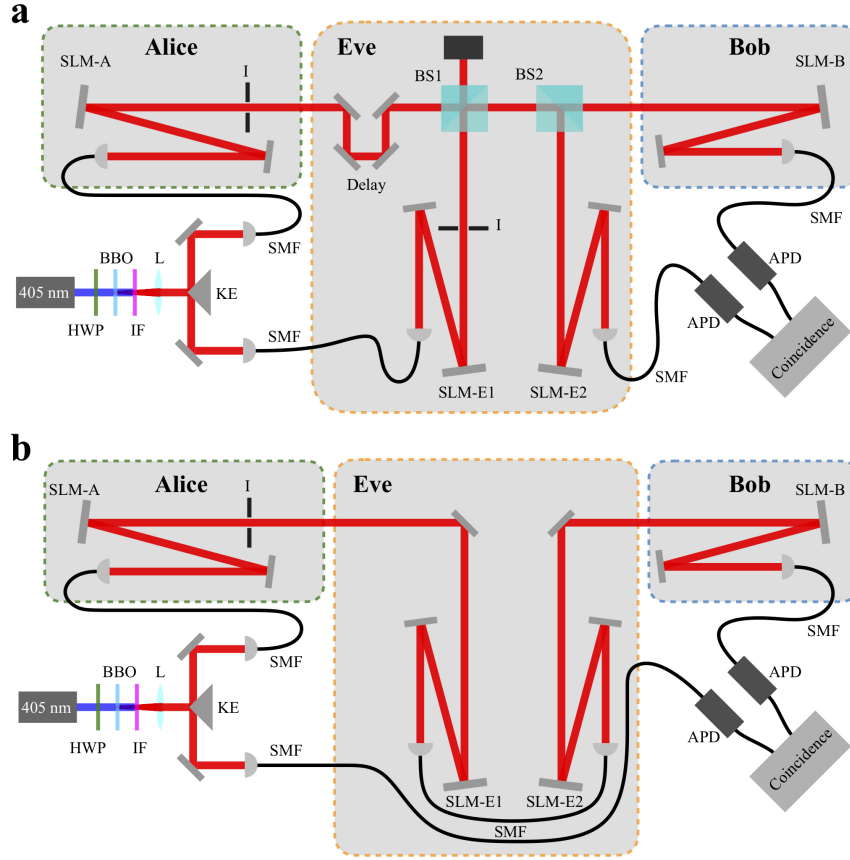


Figure 2: **Detailed experimental setup for (a) the optimal cloning attack and (b) the intercept-resend attack.** Single photons are generated, via spontaneous parametric downconversion (SPDC), by pumping a BBO crystal with a 355 nm quasi-continuous laser. The polarization of the laser is chosen in such a way to satisfy the phase-matching condition of the crystal. Subsequent to SPDC, the 355 nm laser is filtered out using an interference filter (IF). By using a lens (L), the photon pairs are split at the knife-edge (KE) mirror. The photons are then made to couple to single mode fibres (SMF) to filter their spatial modes to the fundamental Gaussian mode. Alice encodes the photon by using the spatial light modulator (SLM-A), and sends it to the quantum channel. Eve may perform an attack by using a delay line, beam splitters (BS1 and BS2), spatial light modulators (SLM-E1 and SLM-E2), and SMF. Bob measures the photon coming from the quantum channel by using his spatial light modulator (SLM-B). Photons counts are recorded at the avalanche photodiodes (APD) detects and coincidence measurements are recorded using a coincidence box.

the completely positive map $\mathcal{E}$ representing the action of the system on any d -dimensional input state ρ_{in} . The output state is then given by $\rho_{\text{out}} = \mathcal{E}(\rho_{\text{in}})$. The process is typically represented as,

$$\mathcal{E}(\rho) = \sum_{m,n} \chi_{mn} \hat{A}_m \rho \hat{A}_n^\dagger, \quad (1)$$

where the $\hat{A}_m$ operators form a complete basis typically given by the Pauli operators or the Gell-Mann operators in higher dimensions. The trace-preserving positive Hermitian $d^2 \times d^2$ matrix χ_{mn} , defined as the *process matrix*, completely and

uniquely characterizes the action of the process $\mathcal{E}$. We may note that QPT may also be performed for non-trace-preserving maps [35].

A convenient alternative description of processes is given by the *Choi-Jamiołkowski* isomorphism (CJI), which states that every completely positive map can be represented as an operator living in a d^2 -dimensional Hilbert space. Such an operator, known as the Choi matrix $\rho_{\mathcal{E}}$, can be defined as the result of the channel acting upon one part of a maximally entangled state, $|\Phi\rangle$,

$$\rho_{\mathcal{E}} = (\hat{I} \otimes \mathcal{E}) |\Phi\rangle\langle\Phi|. \quad (2)$$

The output state is thus given accordingly by,

$$\rho_{\text{out}} = \text{Tr}_{\text{in}} \left[\left(\rho_{\text{in}}^T \otimes \hat{I} \right) \rho_{\mathcal{E}} \right], \quad (3)$$

where T denotes the transposition, $\hat{I}$ is the d -dimensional-identity operator and $\text{Tr}_{\text{in}}[\cdot]$ represents the partial trace over the input state's Hilbert space. In order to perform QPT, a set of tomographically complete states are sent into the channel and state tomography is performed on the output states. In our case, we consider states belonging to mutually unbiased bases (MUBs) in dimension d , which are known for dimensions that are powers of prime numbers [36]. A MUB projector is given by $\Pi_m^{(\alpha)}$, where $\alpha \in \{1, \dots, d+1\}$ labels one of the MUBs and $m \in \{1, \dots, d\}$ labels one of the states in this MUB. The completeness and orthogonality relations are respectively given by, $\sum_{\alpha, m} \Pi_m^{(\alpha)} / (d+1) = \hat{I}$ and $\text{Tr}(\Pi_m^{(\alpha)} \Pi_n^{(\beta)}) = \delta_{\alpha\beta} \delta_{mn} + (1 - \delta_{\alpha\beta})/d$, where δ_{ij} is the Kronecker delta. With the help of the CJI, one can derive Born rule-like expressions for probabilities,

$$\begin{aligned} p_{m,n}^{(\alpha,\beta)} &= \text{Tr} \left[\Pi_n^{(\beta)} \mathcal{E} \left(\Pi_m^{(\alpha)} \right) \right] \\ &= \text{Tr} \left[\left(\left(\Pi_m^{(\alpha)} \right)^T \otimes \Pi_n^{(\beta)} \right) \rho_{\mathcal{E}} \right]. \end{aligned} \quad (4)$$

This equation underlies the relation between quantum process tomography and quantum state tomography. The Choi matrix, $\rho_{\mathcal{E}}$, is experimentally reconstructed using the maximum-likelihood estimation. Better algorithms have also been recently proposed for QPT [37]. Finally, the process matrix is directly obtained from the Choi matrix.

In order to recover the Choi matrix, $\rho_{\mathcal{E}}$, defined in Eq. 2, for various attack scenarios, we follow maximum likelihood algorithms. The positive operator-valued measure (POVM) used to describe the process matrix consists of MUB measurements, i.e. $\Pi_j = (\Pi_m^{(\alpha)})^T \otimes \Pi_n^{(\beta)}$, where the index j runs over all the MUBs measurements performed by Alice and Bob. Theoretical probabilities given by the Born rule, $p_j = \text{Tr}[\Pi_j \rho_{\mathcal{E}}]$, observed with relative frequencies f_j , can be inverted by maximizing the log-likelihood functional

$$\log \mathcal{L} = \sum_j f_j \log \{p_j(\hat{\rho}_{\mathcal{E}})\}, \quad (5)$$

yielding the Choi matrices. Any density operator maximizing the likelihood functional satisfies the

extremal equation $\hat{R} \hat{\rho}_{\mathcal{E}} = \hat{\rho}_{\mathcal{E}}$, which leads to the well known iterative solutions [38] that takes a symmetric form,

$$\hat{\rho}_{\mathcal{E}}^{(k+1)} = \mu \hat{R} \hat{\rho}_{\mathcal{E}}^{(k)} \hat{R}, \quad (6)$$

where $\mu = \text{Tr}[\hat{R} \hat{\rho}_{\mathcal{E}}^{(k)} \hat{R}]^{-1}$ is a proper normalization constant and the operator $\hat{R}$ is defined as follows,

$$\hat{R} = \sum_j \frac{f_j}{p_j(\hat{\rho}_{\mathcal{E}})} \hat{\Pi}_j. \quad (7)$$

Typically, a few thousands of iterations are needed to observe the stationary point of the map in Eq. 6 with the maximally mixed state as a suitable choice of a starting point.

3 Experimental results

Our experiment consists of three components: the generation stage, the quantum channel and the detection stage, which are owned by Alice, Eve and Bob, respectively. We implement the prepare-and-measure QKD scheme with heralded single-photons using the OAM degree of freedom, see Fig. 1-a. The single photon pairs, consisting of the *signal* and *idler*, are generated by spontaneous parametric downconversion (SPDC) at a type I β -barium borate (BBO) crystal. The nonlinear crystal is pumped by a quasi-continuous wave laser operating at a wavelength of 355 nm. The generated photon pairs are coupled to single-mode optical fibres (SMF) in order to filter their spatial modes to the fundamental Gaussian mode. A coincidence rate of 30 kHz is measured, directly at the source, within a coincidence time window of 2 ns. We use the detection of the idler photon as the heralding trigger for the signal photon, thereby realizing a heralded single photon source with a measured second-order coherence of $g^{(2)}(0) = 0.015 \pm 0.004$. The heralded signal photon is sent to SLM-A corresponding to Alice's generation stage. The OAM states are produced using a phase-only holography technique [27]. Alice's heralded photon is subsequently sent over the quantum channel, considered here as a black box between Alice and Bob. At Bob's receiver, we perform a state-projection over the required states, which we realize by a mode filter implemented through a phase-flattening hologram and coupling into a SMF [39, 40]. In order to minimize Poissonian

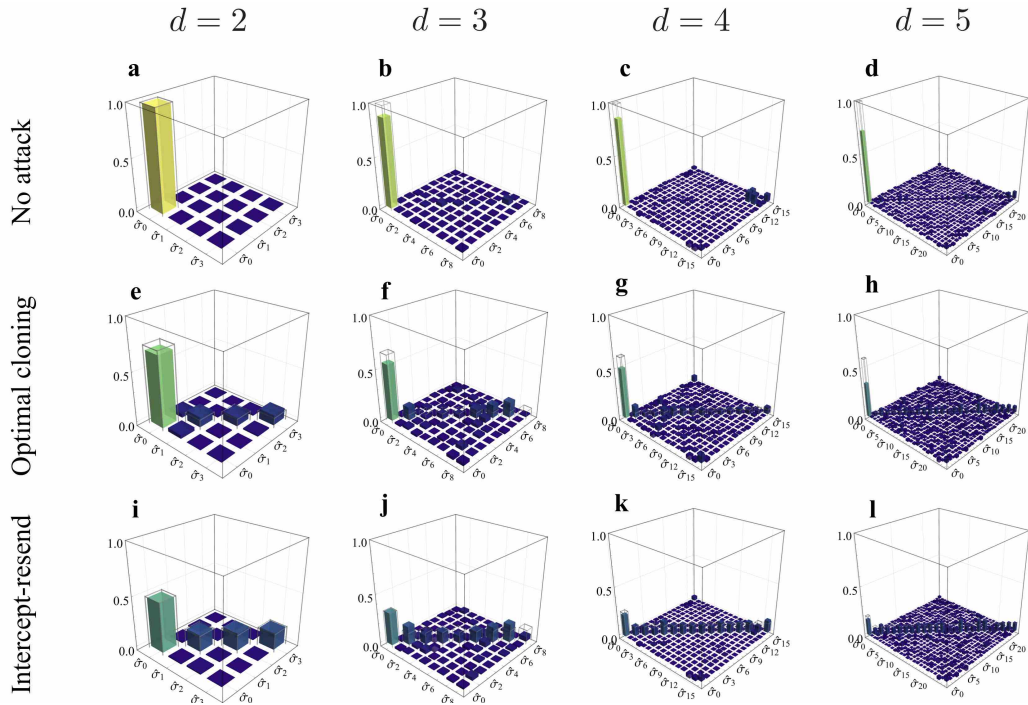


Figure 3: **Process matrix of high-dimensional quantum channels.** The real part of the experimentally reconstructed process matrices are presented for dimensions ranging from 2 to 5 in the case of (a-d) an ideal quantum channel, (e-h) a universal symmetric optimal quantum cloning attack, and (i-l) a universal intercept-resend attack. The theoretical results are represented by the wire-grid bars.

noise, the counts are accumulated over an integration time of 60 seconds per measurement setting. A detailed experimental setup is shown in Fig. 2. In particular, Alice and Bob perform QPT using MUBs [41], which are experimentally realized using OAM states. The computational bases ($\alpha = 1$) are given by $\{|\ell\rangle; \ell = -d/2, \dots, d/2; \ell \neq 0\}$ and $\{|\ell\rangle; \ell = -(d-1)/2, \dots, (d-1)/2\}$ for even and odd dimensions, respectively, for symmetry considerations. The second basis is given by the discrete Fourier transform, i.e. $\{|\phi_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{kj} |j\rangle; k = 0, \dots, d-1\}$, where $\omega_d = \exp(i2\pi/d)$. The explicit form of the other MUB elements can be found elsewhere [42].

3.1 Ideal quantum communication channel

In the case of an ideal quantum channel, i.e. no eavesdropper, the real parts of the experimentally reconstructed process matrices are shown in Fig. 3(a-d) for dimensions ranging from $d = 2$ to 5. Ideal processes, where $\mathcal{E}(\rho) = \rho$, are described by process matrices given by $\tilde{\chi}_{ij} = \delta_{0i}\delta_{0j}$. Deviations of our reconstructed ideal process matrices

from the theory are attributed to imperfections in generation and detection of the distributed quantum states, i.e. the OAM modes. As higher dimensions are considered, larger crosstalk among the OAM modes is observed, which further deteriorates the experimentally reconstructed process matrix. Recently, we have introduced a new technique to measure spatial modes, which should improve detection fidelities [43]. In order to describe the quality or performance of the quantum channel, several figures of merit are available to describe our process [44]. One such figure is the *process fidelity* which is defined as $F_P = \text{Tr}(\chi_{\text{exp}} \tilde{\chi})$. For the ideal quantum channel, F_P can be directly obtained from the process matrix χ_{exp} , i.e. $F_P = \chi_{i=0,j=0}$. Moreover, the *average fidelity*, $\bar{F}$, of the process can be defined as the state fidelity between the output and the input averaged over all possible states with the convenient relation $\bar{F} = (dF_P + 1)/(d + 1)$. Similarly, the *average purity* is defined as the purity of the outgoing states averaged over all possible states and describes the level of mixture introduced by the process. It can be related to the average fidelity

Attack	Dimension - d	Process fidelity - F_p	Average state fidelity - $\bar{F}$	Process purity - $\bar{P}$
No attack	2	0.990 ± 0.001	0.993 ± 0.001	0.987 ± 0.001
	3	0.907 ± 0.003	0.930 ± 0.002	0.868 ± 0.004
	4	0.888 ± 0.003	0.911 ± 0.002	0.832 ± 0.004
	5	0.821 ± 0.002	0.851 ± 0.002	0.729 ± 0.003
Optimal cloning	2	0.71 ± 0.01	0.806 ± 0.006	0.687 ± 0.007
	3	0.604 ± 0.005	0.703 ± 0.003	0.538 ± 0.004
	4	0.524 ± 0.007	0.619 ± 0.006	0.432 ± 0.006
	5	0.419 ± 0.003	0.511 ± 0.003	0.321 ± 0.002
Intercept-resend	2	0.488 ± 0.006	0.659 ± 0.004	0.550 ± 0.003
	3	0.334 ± 0.002	0.500 ± 0.001	0.375 ± 0.001
	4	0.226 ± 0.002	0.381 ± 0.002	0.273 ± 0.001
	5	0.171 ± 0.001	0.309 ± 0.001	0.215 ± 0.001

Table 1: **Quality of the quantum channel processes.** Process fidelity, average fidelity and average purity of the quantum channel under different eavesdropping strategies, i.e. optimal cloning attack and intercept-resend attack, for dimensions ranging from 2 to 5.

according to $\bar{P} = (1 - 2\bar{F} + d\bar{F}^2)/(d - 1)$, respectively. The experimentally obtained process fidelities, average fidelities and average purities for the ideal channel are shown in Table 1 for dimensions ranging from $d = 2$ to 5.

3.2 Optimal quantum cloning attack

A special case of such a process is the so-called universal optimal cloning attack. In this scenario, Eve sends the incoming photon to an optimal cloning machine which produces two imperfect copies of the incoming photon, out of which she keeps one and sends the other to Bob, see Fig. 1-b. Later on, Eve may decide to perform a measurement on her copy in order to obtain information from Alice and Bob's shared photon. For the case of universal optimal cloning, Eve's copying machine has the effect of symmetrically introducing errors on the outgoing state. The cloning fidelity is defined as $F_{cl} = 1/2 + 1/(1 + d)$. Universal optimal cloning machines have been realized experimentally using the symmetrization method [45, 46, 47, 48, 49], where both cloned photons possess the same cloning fidelity. At the heart of the symmetrization technique for optimal cloning is the Hong-Ou-Mandel interference effect [52]. For indistinguishable photons incident at the input port of a balanced beam splitter, a two-photon interference effect occurs which forbids the photons to exit the beam splitter from different output ports. Surprisingly, a slight

modification of the Hong-Ou-Mandel experiment leads to a universal optimal symmetric cloning machine. In this case, the second photon needs to be in a d -dimensional completely mixed state and is fed into the second input port of the beam splitter at exactly the same time. As the representation of the mixed state is the same in any basis, this scheme is universal, i.e. works for any state of the Hilbert space. When the two photons exit the beam splitter from the same output port, optimal cloning has been successful. A second beam splitter is then used to separate the two photons, e.g. one photon goes to Bob and the other one stays at Eve. We then experimentally perform the universal optimal cloning machine in the quantum channel for dimensions up to 5 and perform, again, a full characterization of the attack on the channel through QPT, see Fig. 3-(e-h) and Table 1. Leaving attacks on QKD systems aside, a full characterization of optimal quantum cloning machines is interesting in itself for applications to quantum state estimation [50, 51]. Indeed, there is an equivalence between a universal optimal cloning machine taking N input replicas and outputting an infinite number of clones and a quantum state estimation setup. A full characterization of the cloning machine would then enable a higher mode purity in the state estimation task.

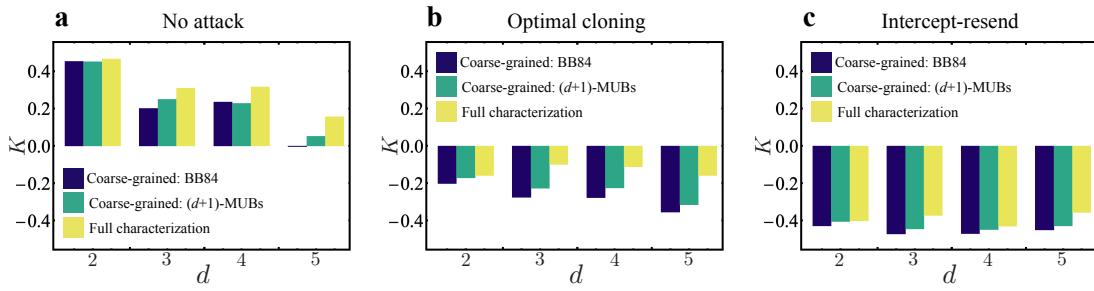


Figure 4: **Secret key rates.** Experimentally obtained secret key rates for the cases of no attack, optimal cloning and intercept-resend. The dark blue bars correspond to the BB84 protocol where the secret key rate is obtained by estimating a coarse-grained error rate. The green bars correspond to the $(d+1)$ -MUBs protocol where the secret key rate is obtained also by estimating a coarse-grained error rate. The yellow bars correspond to a secret key rate calculated from the full characterization of the quantum channel. In all cases, a filter type measurement is considered yielding an overall efficiency of $1/d$.

3.3 Intercept-resend attack

Another eavesdropping scheme that achieves processes with lower average fidelities is the so-called intercept-resend attack, see Fig 3-(i-1). In contrast to the above described optimal cloning attack, Eve directly measures the received photon information, where she randomly performs her measurement in bases uniformly chosen at random (intercept). She then prepares a photon in the observed state and transmits it to Bob (resend). When considering the intercept-resend over all MUBs, the fidelity of the states at the output of the channel is given by $F_{ir} = 2/(1+d)$. We experimentally perform the intercept-resend attack in our quantum channel by means of two SLMs, i.e. SLM-E1 and SLM-E2, with a SMF in between, see Fig. 1-c. The first SLM (SLM-E1) along with the SMF acts as the intercept section, while the second SLM (SLM-E2) acts as the resend. In the universal case, Eve randomly chooses $\alpha = 1, \dots, d+1$ and $m = 1, \dots, d$ and simultaneously displays phase elements equivalent to $\langle \psi_m^{(\alpha)} |$ and $|\psi_m^{(\alpha)}\rangle$ on the SLM-E1 and SLM-E2, respectively.

4 Secret key rates

So far, we have shown the feasibility of performing high-dimensional QPT on several quantum communication channels with our experimental implementation and provided a qualitative illustration of the effect of different eavesdropping strategies. In this section, we use the experimen-

tal outcomes obtained when performing QPT as our raw key from which we carry a formal security analysis. In particular, we show that the full characterization enables an enhanced estimation of the information leakage to an adversary eavesdropper. This results in a more accurate and favourable estimation of the achievable secret key rate, K , of the channel for a given QKD protocol. Furthermore, we demonstrate that the full characterization of the channel becomes even more advantageous when considering larger dimensions.

Traditionally, the secret key rate of a channel is calculated by evaluating the error rate, Q , from the raw key shared by Alice and Bob. Analytical formulae are derived to obtain the secret key rate as a function of the error rate. For instance, the BB84 protocol [2] in dimension d has the following simple analytical formula,

$$K^{(d)}(Q) = \log_2(d) - 2h^{(d)}(Q), \quad (8)$$

where $h^{(d)}(x) := -x \log_2(x/(d-1)) - (1-x) \log_2(1-x)$ is the d -dimensional Shannon entropy. This protocol does not require a full characterization of the quantum channel and has a sifting efficiency of $1/2$. An extension of the d -dimensional BB84 protocol to tomographically complete measurements, yielding a full characterization of the channel, is known as the *six-state* protocol for the specific case of $d=2$. For dimensions that are powers of prime numbers, all $d+1$ MUBs are adopted. The sifting efficiency of this protocol is given by $1/(d+1)$. Nevertheless, in the infinite key limit, the sifting efficiency

of the BB84 and the six-state protocol can approach 1, by making the basis choice extremely asymmetric [53]. This argument also holds for higher dimensions. The secret key rate of this $(d+1)$ -MUB protocol as a function of the error rate is given by,

$$K^{(d)}(Q) = \log_2(d) - h^{(d)}\left(\frac{d+1}{d}Q\right) - \frac{d+1}{d}Q \log_2(d+1). \quad (9)$$

Nonetheless, using such analytical formulae has a number of drawbacks. First, it only considers sifted data and assumes perfect unbiasedness among different MUBs. This assumption may increase the resulting secret key rate, but does not consist of an adequate representation of the channel and may lead to an underestimation of Eve's leaked information. Moreover, the secret key rate is obtained from a coarse-graining of the individual error rates per measurement settings. Thus, given this single parameter, a pessimistic estimation of the secret key rate is obtained due to the limited knowledge of the channel. Instead, we propose a protocol based on QPT where all the measurement outcomes, both from matching and non-matching bases, are considered in the secret key rate analysis. This protocol based on full characterization of the channel outperforms the counterpart coarse-grained protocols particularly for the case of asymmetric errors, which is often the case in experiments.

In our analysis, the secret key rate of a channel is estimated by considering the Devetak-Winter formula [54]. To do so, we recast our prepare-and-measure QKD protocol into an entanglement-based scheme using the source-replacement scheme [55], where Alice and Bob share pairs of entangled photons represented by the density matrix ρ_{AB} . In general, the secret-key rate is obtained according to,

$$K = \min_{\rho_{AB} \in \mathcal{C}} [H(Z_A|E) - H(Z_A|Z_B)], \quad (10)$$

where $\mathcal{C}$ is the set of physical density matrices that is consistent with the experimental constraints, e.g. error rates or measurement outcomes; $H(X|Y) := H(\rho_{XY}) - H(\rho_Y)$ is the conditional von Neumann entropy, with $H(\rho) := -\text{Tr}[\rho \log_2 \rho]$; Z_A and Z_B are the sets of positive operator valued measures (POVM) associated with Alice's and Bob's measurement settings, respectively. Finally, $\rho_{Z_A Z_B}$ and $\rho_{Z_A E}$ are

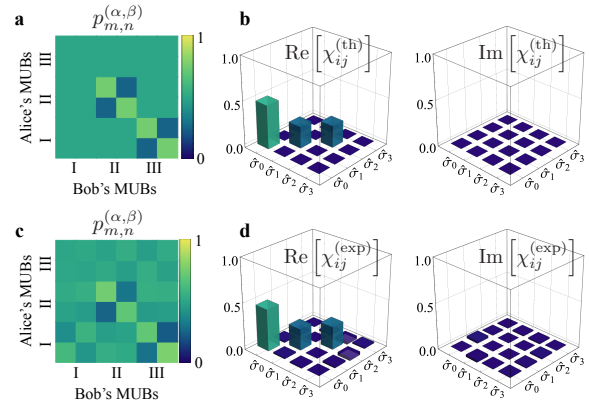


Figure 5: **Asymmetric intercept-resend.** **a** Theoretical and **c** experimental probability of detection matrices, as given in Eq. 4, corresponding to the asymmetric process of an intercept-resend eavesdropping strategy over MUB II and III in dimension 2. **b** Theoretical and **d** experimental real and imaginary part of the process matrix.

given by,

$$\rho_{Z_A Z_B} = \sum_{j,k} \text{Tr} \left[\left(Z_A^j \otimes Z_B^k \right) \rho_{AB} \right] |j\rangle\langle j| \otimes |k\rangle\langle k|, \quad (11)$$

$$\rho_{Z_A E} = \sum_j |j\rangle\langle j| \otimes \text{Tr}_A \left[\left(Z_A^j \otimes \hat{I} \right) \rho_{AE} \right], \quad (12)$$

where ρ_{ABE} is the tripartite density matrix shared by Alice, Bob and Eve, respectively. Hence, every additional experimental measurement is included in the minimization, which results in a greater, or equal, secret key rate. In the limiting case where we have a full characterization of the channel, ρ_{AB} is fully reconstructed and is given by the Choi matrix, $\rho_{\mathcal{E}}$, mentioned earlier. Thus the secret key rate may be directly calculated from ρ_{AB} ,

$$K = H(Z_A|E) - H(Z_A|Z_B), \quad (13)$$

where all experimental measurements are taken into consideration, even for the case of mismatching MUBs.

In the prepare-and-measure scheme, we can now determine the set of POVMs corresponding to Alice and Bob's generation and measurement apparatuses. At Alice's preparation stage, we have $Z_A = \{|0\rangle\langle 0|, \dots, |d-1\rangle\langle d-1|\}$, since Alice has the freedom to generate any state at random. However, at Bob's measuring stage, we consider two different sets of POVMs, i.e. $Z_B^{\text{sort}} =$

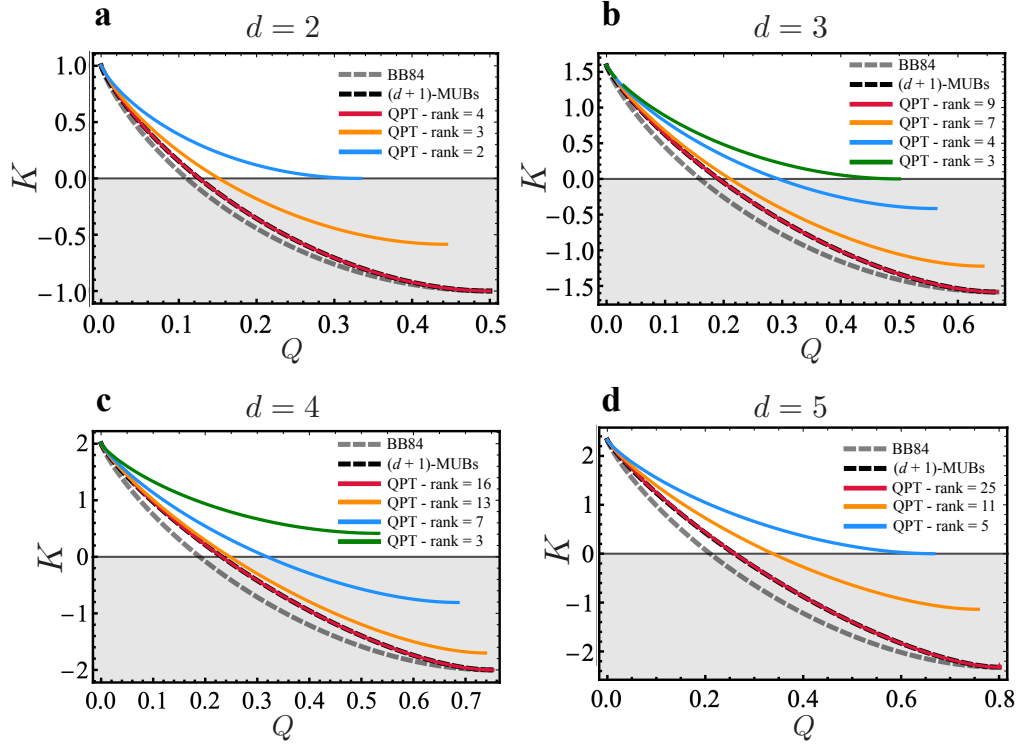


Figure 6: **Security analysis for noise models with varying levels of symmetry.** **a-d** The secret key rate is calculated for different scenarios in dimensions ranging from 2 to 5. The secret key rate for the BB84 and the $(d+1)$ -MUBs protocols are directly calculated from Eq. 8 and Eq. 9, respectively, where the level of noise is characterized using the error rate. Using the process matrix representation, we then consider noisy channels corresponding to diagonal trace-preserving process matrices of different ranks. The secret key rate is directly calculated using Eq. 13, and an error rate is determined for comparison with the coarse-grained protocols. For the case of a process matrix of rank $r = d^2$ with constant diagonal elements, i.e. Eq. 14, we retrieve the case of completely symmetric noise, i.e. Eq. 9. Asymmetric noise is then simulated by considering process matrices of lower ranks.

$\{|0\rangle\langle 0|, \dots, |d-1\rangle\langle d-1|\}$ and $Z_B^{\text{filter}} = \{|i\rangle\langle i|\}$, where the former corresponds to a sorting-type measurement and the latter corresponds to a filter-type measurement, and Alice and Bob post-select on the event where Bob successfully obtains a measurement of the state $|i\rangle\langle i|$ with $i \in \{0, \dots, d-1\}$. When carrying out the security analysis, one can see that the secret key rate, K , for the cases of Z_B^{sort} and Z_B^{filt} only differs from an overall efficiency of $1/d$. Thus, we carry out the high-dimensional QKD protocols based on QPT with a filter-type measurement scheme at Bob's stage using an SLM. There exists efficient sorters for the OAM computational and discrete Fourier transform basis [56]; however, the establishment of arbitrary multi-outcome measurement devices remains an open challenge for quantum applications [57].

For the full characterization of our high-

dimensional quantum channel via QPT with no explicit eavesdropping strategy applied, we calculate the corresponding secret key rate and compare it to a coarse-grained estimation of the channel, see Fig. 4 a. In the case of explicit eavesdropping strategies, such as optimal cloning and intercept-resend, the secret key rate will obviously be negative, see Fig. 4 b-c, and no secret key can be exchanged between Alice and Bob. We observe that for larger dimensions, the full characterization secret key rate performs better compared to the achievable secret key rate obtained from a coarse-graining of the channel. This may be due to the fact that, as one considers higher-dimensional states, the symmetry assumption involved in coarse-graining is increasingly not fulfilled. Therefore, full characterization of quantum channels may offer a means by which the full potential of high-dimensional protocols is exploited.

In highly asymmetric scenarios, which is often the case due to systematic errors such as misalignments, full characterization may even surpass the performance of coarse-grained protocols, such as the BB84 protocol, when considering the lower sifting efficiency of the full characterization protocol in the finite-key scenario.

Finally, in order to better understand the advantage of full characterization protocols compared to their coarse-grained counterparts, we carry out a security analysis for different noise models. In particular, we take advantage of the process matrix representation of the quantum channel to simulate different levels of symmetry in noise. In the limit, where the noise is completely symmetric over all states of all bases, the process matrix of the channel can be described as following,

$$\chi_{ij}^{r=d^2} = \frac{F(d+1)-1}{d} \delta_{0i} \delta_{0j} + \frac{(1-F)}{2(d-1)} (\delta_{ij} - \delta_{0i} \delta_{0j}), \quad (14)$$

where $\chi_{ij}^{r=d^2}$ is a $d^2 \times d^2$ diagonal matrix with a rank of $r = d^2$, and F determines the level of noise in the channel. For instance, the result of such a process on an input state, say $\rho_{\text{in}} = |0\rangle\langle 0|$, is given by the output state $\rho_{\text{out}} = F|0\rangle\langle 0| + (1-F)/(d-1) \sum_{i=1}^{d-1} |i\rangle\langle i|$. The processes of universal optimal cloning and universal intercept-resend fall under this category of process matrices, as can be seen in Fig. 3, with fidelities $F_{\text{cl}} = 1/2 + 1/(1+d)$ and $F_{\text{ir}} = 2/(1+d)$, respectively. Here, we consider another type of eavesdropping strategy that is not considered universal. We experimentally perform QPT of an intercept-resend attack where the eavesdropper only consider 2 out of the 3 MUBs available to Alice and Bob in dimension 2, see Fig. 5. This would be an appropriate attack in the case of BB84, where only two MUBs are utilized by Alice and Bob. However, in this case the noise added by the process to the output state is no longer symmetric. We observe state- and basis-dependent state fidelities which can be understood as asymmetric noise. Interestingly, the process matrix of the 2-MUB intercept-resend attack, see Fig. 5, has only 3 non-zero diagonal elements compared to 4 non-zero diagonal elements for the case of universal attacks, see Fig. 3, in dimension 2. Inspired, by the shape of the process matrix in this

simple case, we investigate different asymmetric noise models by varying the rank of the process matrix

For a process matrix of rank $r = d^2$, we retrieve the secret key rate formula for the coarse-grained $(d+1)$ -MUBs protocol, i.e. Eq. 9, as can be seen in Fig. 6. In dimension 2, we may then consider channels with process matrices of other ranks, corresponding to different degrees of noise symmetry. In particular, we consider trace-preserving process matrices of rank 3, i.e. $\chi_{ij}^{d=2,r=3} = F\delta_{0i}\delta_{0j} + (1-F)/2(\delta_{1i}\delta_{1j} + \delta_{2i}\delta_{2j})$, and rank 2, i.e. $\chi_{ij}^{d=2,r=2} = F\delta_{0i}\delta_{0j} + (1-F)(\delta_{1i}\delta_{1j})$. As can be seen in Fig. 6-a, noise corresponding to a process matrix of rank 2 or 3, leads to a significant improvement in secret key rate compared to a coarse-grained characterization of the channel using the error rate. Interestingly, for the case of the rank 2 process matrix of the form given above, i.e. $\chi_{ij}^{r=2}$, although the resulting error rate is well above the traditional error threshold, the secret key rate remains positive all the way up to $Q = 0.33$. We consider trace-preserving process matrices of rank 7, 4, and 3, in dimension 3, rank 13, 7, and 3, in dimension 4, and rank 11 and 5, in dimension 5, i.e.

$$\begin{aligned} \chi_{ij}^{d=3,r=7} &= F\delta_{0i}\delta_{0j} + \frac{1}{4}(1-F) \sum_{k=1}^6 \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=3,r=4} &= F\delta_{0i}\delta_{0j} + \frac{1}{2}(1-F) \sum_{k=1}^3 \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=3,r=3} &= F\delta_{0i}\delta_{0j} + \frac{3}{4}(1-F) (\delta_{1i}\delta_{1j} + \delta_{8i}\delta_{8j}) \\ \chi_{ij}^{d=4,r=13} &= F\delta_{0i}\delta_{0j} + \frac{1}{16}(1-F) \sum_{k=1}^{12} \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=4,r=7} &= F\delta_{0i}\delta_{0j} + \frac{1}{3}(1-F) \sum_{k=1}^6 \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=4,r=3} &= F\delta_{0i}\delta_{0j} + (1-F)(\delta_{1i}\delta_{1j} + \delta_{12i}\delta_{12j}) \\ \chi_{ij}^{d=5,r=11} &= F\delta_{0i}\delta_{0j} + \frac{1}{4}(1-F) \sum_{k=1}^{10} \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=5,r=5} &= F\delta_{0i}\delta_{0j} + \frac{1}{4}(1-F) \sum_{k=21}^{24} \delta_{ki}\delta_{kj}, \quad (15) \end{aligned}$$

respectively. In all cases, we can observe a clear advantage of using a full characterization

scheme compared to the error rate channel assessment. Interestingly, for all dimensions we find cases where after the transmission, the coarse-grained errors would label the channel as insecure, while our more detailed analysis still enables a secure communication. This advantage is possible because our analysis allows to distinguish between cases where an eavesdropper has not gained enough information about the state although they have transformed it such that Alice and Bob will have large error rates.

5 Conclusion

In summary, full characterization of quantum processes via QPT is an invaluable tool for high-dimensional quantum information processing. In particular, the complexity resulting from the generation and detection of the high-dimensional states involved may be fully characterized. In the study of quantum channels for quantum communications, full characterization via QPT turns out to be a beneficial resource that allows one to take full advantage of the potential high-dimensional nature of the protocols at play to increase the overall secret key rate.

Acknowledgments This work was supported by Canada Research Chair (CRC); 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). D.K. would like to acknowledge the project no IGA-PrF-2018-003.

References

- [1] Dowling, J. P. & Milburn, G. J. Quantum technology: the second quantum revolution, *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **361**, 1655–1674 (2003).
- [2] Bennett, C. H. & Brassard, G., Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE international conference on computers, systems, and signal processing, bangalore, india, 1984 (1984).
- [3] Nielsen, M. A. & Chuang, I. Quantum computation and quantum information. Cambridge: Cambridge University Press (2002).
- [4] Degen, C., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
- [5] Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455–2467 (1997).
- [6] Poyatos, J., Cirac, J. I. & Zoller, P. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.* **78**, 390 (1997).
- [7] Nielsen, M. A., Knill, E. & Laflamme, R. Complete quantum teleportation using nuclear magnetic resonance. *Nature* **396**, 52 (1998).
- [8] Childs, A. M., Chuang, I. L. & Leung, D. W. Realization of quantum process tomography in NMR. *Phys. Rev. A* **64**, 012314 (2001).
- [9] O’Brien, J. L. *et al.* Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.* **93**, 080502 (2004).
- [10] Myrskog, S. H., Fox, J. K., Mitchell, M. W. & Steinberg, A. M. Quantum process tomography on vibrational states of atoms in an optical lattice. *Phys. Rev. A* **72**, 013615 (2005).
- [11] Riebe, M., Kim, K., Schindler, P., Monz, T., Schmidt, P. O., Korber, T. K., Hansel, W., Haffner, H., Roos, C. F. & Blatt, R. Process tomography of ion trap quantum gates. *Phys. Rev. Lett.* **97**, 220407 (2006).
- [12] Howard, M. *et al.* Quantum process tomography and linblad estimation of a solid-state qubit. *New Journal of Physics* **8**, 33 (2006).
- [13] Lobino, M. *et al.* Complete characterization of quantum-optical processes. *Science* **322**, 563–566 (2008).
- [14] Kim, D. *et al.* Quantum control and process tomography of a semiconductor quantum dot hybrid qubit. *Nature* **511**, 70 (2014).

- [15] Jacob, K. V., Mirasola, A. E., Adhikari, S. & Dowling, J. P. Direct characterization of linear and quadratically nonlinear optical systems. *Phys. Rev. A* **98**, 052327 (2018).
- [16] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
- [17] Bienvenu, N., Perez-Garcia, B., Roux, F. S., McLaren, M., Rosales-Guzman, C., Zhang, Y., Mouane, O., Hernandez-Aranda, R. I., Konrad, T. & Forbes, A. Characterizing quantum channels with non-separable states of classical light. *Nat. Phys.* **13**, 397 (2017).
- [18] Muller, A., Zbinden, H. & Gisin, N. Underwater quantum coding. *Nature* **378**, 449 (1995).
- [19] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G. & Simmons, C. M. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.* **81**, 3283 (1998).
- [20] Yin, J., Cao, Y., Li, Y. H., Ren, J. G., Liao, S. K., Zhang, L., Cai, W. Q., Liu, W. Y., Li, B., Dai, H., Li, M., Huang, Y. M., Deng, L., Li, L., Zhang, Q., Liu, N. L., Chen, Y. A., Lu, C. Y., Shu, R., Peng, C. Z., Wang, J. Y. & Pan, J. W. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **119**, 200501 (2017).
- [21] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE T. Inform. Theory* **41**, 1915–1923 (1995).
- [22] Coles, P. J., Metodiev, E. M. & Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nature Commun.* **7**, 11712 (2016).
- [23] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
- [24] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
- [25] Molina-Terriza, G., Torres, J. P. & Torner, L. Twisted photons. *Nature Physics* **3**, 305 (2007).
- [26] Erhard, M., Fickler, R., Krenn, M. & Zeilinger, A. Twisted photons: New quantum perspectives in high dimensions. *Light: Sci. & Appl.* **7**, 17146 (2018).
- [27] Forbes, A., Dudley, A. & McLaren, M. Creation and detection of optical modes with spatial light modulators. *Advances in Optics and Photonics* **8**, 200–227 (2016).
- [28] Mafu, M., Dudley, A., Goyal, S., Giovannini, D., McLaren, M., Padgett, M. J., Konrad, T., Petruccione, F., Lutkenhaus, N. & Forbes, A. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).
- [29] Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
- [30] Bouchard, F. *et al.* Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018).
- [31] Vallone, G., D'Ambrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F. & Villoresi, P. Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.* **113**, 060503 (2014).
- [32] Krenn, M., Handsteiner, J., Fink, M., Fickler, R. & Zeilinger, A. Twisted photon entanglement through turbulent air across Vienna. *PNAS* **112**, 14197–14201 (2015).
- [33] Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
- [34] Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Opt. Exp.* **26**, 22563–22573 (2018).
- [35] Bongioanni, I., Sansoni, L., Sciarrino, F., Vallone, G. & Mataloni, P. Experimental quantum process tomography of non-trace-preserving maps. *Phys. Rev. A* **82**, 042307 (2010).
- [36] Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Annals of Physics* **191**, 363–381 (1989).

- [37] Knee, G. C., Bolduc, E., Leach, J. & Gauger, E. M. Quantum process tomography via completely positive and trace-preserving projection. *Phys. Rev. A* **98**, 062336 (2018).
- [38] Ježek, M., Fiurášek, J. & Hradil, Z. Quantum inference of states and processes. *Phys. Rev. A* **68**, 012305 (2003).
- [39] Mair, A., Vaziri, A., Weihs, G. & Zeilinger, A. Entanglement of the orbital angular momentum states of photons. *Nature* **412**, 313–316 (2001).
- [40] Qassim, H. *et al.* Limitations to the determination of a Laguerre–Gauss spectrum via projective, phase-flattening measurement. *J. Opt. Soc. Am. B* **31**, A20–A23 (2014).
- [41] Fernández-Pérez, A., Klimov, A. B. & Saavedra, C. Quantum process reconstruction based on mutually unbiased basis. *Phys. Rev. A* **83**, 052332 (2011).
- [42] Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535–640 (2010).
- [43] Bouchard, F., Valencia, N. H., Brandt, F., Fickler, R., Huber, M., & Malik, M., Measuring azimuthal and radial modes of photons. *Optics Express* **26**, 31925 (2018).
- [44] Gilchrist, A., Langford, N. K. & Nielsen, M. A. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A* **71**, 062310 (2005).
- [45] Irvine, W. T. M., Linares, A. L., deDood, M. J. A. & Bouwmeester, D. Optimal quantum cloning on a beam splitter. *Phys. Rev. Lett.* **92**, 047902 (2004).
- [46] Ricci, M., Sciarrino, F., Sias, C. & DeMartini, F. Teleportation scheme implementing the universal optimal quantum cloning machine and the universal not gate. *Phys. Rev. Lett.* **92**, 047901 (2004).
- [47] Nagali, E. *et al.* Optimal quantum cloning of orbital angular momentum photon qubits through Hong–Ou–Mandel coalescence. *Nature Photonics* **3**, 720 (2009).
- [48] Nagali, E., Giovannini, D., Marrucci, L., Slussarenko, S., Santamato, E. & Sciarrino, F. Experimental optimal cloning of four-dimensional quantum states of photons. *Phys. Rev. Lett.* **105**, 073602 (2010).
- [49] Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E. High-dimensional quantum cloning and applications to quantum hacking. *Science Adv.* **3**, e1601915 (2017).
- [50] Bruß, D. & Macchiavello, C. Optimal state estimation for d-dimensional quantum systems. *Phys. Lett. A* **253**, 249–251 (1999).
- [51] Thekkadath, G. S., Saaltink, R. Y., Giner, L. & Lundeen, J. S. Determining complementary properties with quantum clones. *Phys. Rev. Lett.* **119**, 050405 (2017).
- [52] Hong, C.-K., Ou, Z.-Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).
- [53] Lo, H.-K., Chau, H. F., & Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *Journal of Cryptology* **18**, 133–165 (2005).
- [54] Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, 207–235 (The Royal Society, 2005).
- [55] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
- [56] Berkhout, C. G. *et al.* Efficient sorting of orbital angular momentum states of light. *Phys. Rev. Lett.* **105**, 153601 (2010).
- [57] Fontaine, N. K. *et al.* Laguerre-Gaussian mode sorter. *arXiv preprint arXiv:1803.04126v2* (2018).



Compressed sensing of twisted photons

FRÉDÉRIC BOUCHARD,¹ DOMINIK KOUTNÝ,² FELIX HUFNAGEL,¹
ZDENĚK HRADIL,² JAROSLAV ŘEHÁČEK,² YONG-SIAH TEO,³
DAEKUN AHN,³ HYUNSEOK JEONG,³ LUIS L. SÁNCHEZ-SOTO,^{4,5,*}
GERD LEUCHS,^{1,5} AND EBRAHIM KARIMI^{1,5}

¹Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, Ontario, K1N 6N5, Canada

²Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic

³Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea

⁴Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain

⁵Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

*lsanchez@fis.ucm.es

Abstract: The ability to completely characterize the state of a system is an essential element for the emerging quantum technologies. Here, we present a compressed-sensing-inspired method to ascertain any rank-deficient qudit state, which we experimentally encode in photonic orbital angular momentum. We efficiently reconstruct these qudit states from a few scans with an intensified CCD camera. Since it only requires a small number of intensity measurements, our technique provides an easy and accurate way to identify quantum sources, channels, and systems.

© 2019 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

1. Introduction

The orbital angular momentum (OAM) of single photons, which provides an unbounded vector space, has been recognized as a preeminent platform for encoding both quantum [1–3] and classical [4,5] information. Although the generation of photons with OAM is relatively simple, the full characterization of a state in the OAM Hilbert space stands as a challenging task. Several methods have demonstrated accurate projective measurements to determine OAM states [6–11]. However, these projective measurements work adequately only for pure states. The case of mixed states requires full state tomography, and this involves projective measurements on arbitrary superpositions of two or more OAM eigenstates [12], a task which remains challenging.

To circumvent these problems, we propose and experimentally demonstrate a method inspired by compressed sensing. Originating from the context of classical signal processing [13, 14], this technique harnesses prior assumptions about the state to reconstruct it from an undersampled set of measurements. It is routinely used to estimate vectors or matrices from incomplete information, with applications in many diverse fields of research [15, 16]. Compressed sensing has also been adapted as a tool for state tomography of discrete systems in quantum theory [17–24].

The primary goal of our scheme for reconstructing OAM states is to significantly reduce the number of z -axis scans (Z) given an *a priori* value of the mode rank s . We shall demonstrate that intensity measurement with only a small Z (thus giving n_Z number of linearly independent detection outcomes) is sufficient to unambiguously reconstruct OAM states of low rank s , which constitutes our main result. Actually, the compressed sensing algorithms, supplemented with the positivity constraint [25], which operates as a kind of regularization, enables us to construct informationally complete measurements that are robust to noise and modeling errors. In other words, one can use a very simple setup for the characterization of a state with *a priori* information about its nature.

2. Setting the scenario

We begin our analysis by recalling a few basic concepts that we will need to understand the technique. We are dealing with single photons carrying OAM, which has made this degree of freedom an ideal candidate for the investigation of complex quantum phenomena and their applications. For this reason, we describe the OAM modes in a quantum parlance, although everything can be immediately translated into a classical framework.

In any tomographic protocol, one infers the state, represented by the density matrix ϱ , from the distinct outcomes of a collection of measurements performed on identical copies of the system. The outcomes of these measurements are given by the Born rule $p_\alpha = \text{Tr}(\varrho \Pi_\alpha)$, where $\{\Pi_\alpha\}$ is the positive operator-valued measure (POVM) describing the setup [26]. We denote the action of the POVM by $\mathcal{A} : \varrho \mapsto \mathbf{p}$, that maps ϱ onto the vector containing all the probabilities $\{p_\alpha\}$.

A POVM is informationally complete (IC) when the corresponding outcome probabilities are sufficient to determine an arbitrary state [27, 28]. Obviously, the number of outcomes of any IC measurement is at least d^2 , where d is the dimension of the system, which makes traditional methods infeasible as d increases. However, if we know *a priori* that the rank of the system fulfills $\text{rank}(\varrho) \leq s$, with $s \ll d$, then we can substantially reduce the number of measurement samples required to uniquely reconstruct the unknown signal matrix. It has been shown that for any map $\mathcal{A}$, the so-called restricted isometry property [29] (which characterizes matrices that are nearly orthonormal, at least when operating on sparse vectors is sufficient to yield a unique rank- s reconstruction: the true state ϱ_0 is then the only density matrix within the set of positive Hermitian matrices of any rank that yields the measurement probabilities $\mathbf{p}$ [25]. The corresponding estimator $\hat{\varrho}$ for ϱ_0 , based on collected statistical data, is given by

$$\hat{\varrho} = \min_{\varrho} \|\mathcal{A}[\varrho] - \mathbf{p}\| \quad \text{subject to} \quad \varrho \geq 0, \quad (1)$$

whose solution can be efficiently found by convex programming [30].

The insights into the regularizing effect of the positivity constraint permit us to tackle reconstructing OAM quantum states. To represent the structure of the transverse field we will be using the well-known Laguerre-Gauss (LG) modes that can be written as [31],

$$\begin{aligned} \text{LG}_{p\ell}(r, \phi, z) &= \langle r, \phi, z | \ell, p \rangle = \sqrt{\frac{2p!}{\pi(p+|\ell|)!}} \frac{1}{w(z)} \left(\frac{\sqrt{2}r}{w(z)} \right)^{|\ell|} \\ &\times L_p^{|\ell|} \left(\frac{2r^2}{w(z)^2} \right) \exp \left(-r^2 \left[\frac{1}{w(z)^2} - i \frac{k}{2R(z)} \right] - i\ell\phi - i\psi_{p\ell}(z) \right), \end{aligned} \quad (2)$$

where (r, ϕ, z) denote cylindrical coordinates, k is the wave number, $L_p^{|\ell|}(\cdot)$ is the generalized Laguerre polynomial, $\ell \in \{0, \pm 1, \pm 2, \dots\}$ is the azimuthal mode index, and $p \in \{0, 1, 2, \dots\}$ is the radial mode index, which is related to the number of radial nodes. The parameters $R(z)$, $w(z)$, and $\psi_{p\ell}(z)$ denote the radius curvature of the wave fronts, the beam radius, and the Gouy phase at the propagation distance z , respectively:

$$\begin{aligned} w^2(z) &= w_0^2 \left[1 + (z/z_R)^2 \right], \\ R(z) &= z \left[1 + (z_R/z)^2 \right], \\ \psi_{p\ell}(z) &= (2p + |\ell| + 1) \arctan(z/z_R), \end{aligned} \quad (3)$$

with the Rayleigh range $z_R = kw_0^2/2$ and w_0 the beam waist, which we assume located at $z = 0$. In what follows, we will set $p = 0$ and denote $\psi_\ell(z) = \psi_{p=0\ell}(z)$.

We propose to reconstruct the signal in the LG basis from Z intensity scans registered by a CCD camera positioned at distances $z_1, z_2, \dots$, with respect to the beam waist, which is in the

spirit of the Gerchberg-Saxton algorithm [32]. This amounts to projecting the density matrix on free-space position eigenstates; viz,

$$p(r, \phi, z) = \langle r, \phi, z | \rho | r, \phi, z \rangle = \sum_{\ell, \ell'} \text{LG}_{\ell,0}(r, \phi, z) \varrho_{\ell\ell'} \text{LG}_{\ell',0}^*(r, \phi, z) \propto e^{-2r^2} \sum_{\ell\ell'} \varrho_{\ell\ell'} C_{\ell\ell'}, \quad (4)$$

where

$$C_{\ell\ell'} = r^{|\ell|+|\ell'|} \exp[i(\ell - \ell')\phi] \exp\{i[\psi_\ell(z) - \psi_{\ell'}(z)]\}, \quad r(z) = r/w(z). \quad (5)$$

Each combination of r , ϕ , and z coordinates, which corresponds to the associated pixel readings, gives us one particular linear combination of density matrix elements. Evidently by varying r , ϕ , and z , the more linearly independent these generated combinations are, the more IC the POVM is.

3. Informational completeness of intensity scans

The aim of compressed sensing is to perform a set of IC POVM measurement outcomes to uniquely reconstruct the unknown state ρ . In our context of twisted-photon state reconstruction, the POVM refers to the set of CCD intensity scans along the propagation axis. In this section, we shall analytically demonstrate that a few CCD scans shall be needed to unambiguously, and thus compressively, reconstruct an arbitrary d -dimensional state under various conditions on the angular momentum quantum number ℓ . To simplify the details as much as possible, we will ignore statistical noise and take $p(r, \phi, z)$ to represent the raw data. We also assume there are no limits on sampling in r and ϕ coordinates.

First, we consider d -dimensional signals represented by LG beams with nonnegative azimuthal indexes only $\ell \in \{0, 1, \dots, d-1\}$. We will show that a single CCD scan provides complete information about the signal. In this case (for a fixed z) one can ignore the Gouy's phase. Obviously, incompleteness arises whenever two different pairs (ℓ', ℓ'') generate the same $C_{\ell'\ell''}$ for all r and ϕ . Since for $\ell', \ell'' \geq 0$, we have $|\ell'| - |\ell''| = \ell' - \ell''$, there just cannot be two such pairs both satisfying $\ell' - \ell'' = N$ and $\ell' - \ell'' = M$ with the same N and M and incompleteness does not arise. Hence, all density matrix elements can be uniquely determined from a single CCD scan for any dimension d of our system.

When the sign of the topological charge is not constrained, the space dimension is $d = 2\ell_{\max} + 1$, so that $\ell \in \{-\ell_{\max}, \dots, 0, \dots, \ell_{\max}\}$. Now, the CCD scans are no longer IC no matter how many planes Z are sampled. Indeed, incompleteness arises when two or more elements $C_{\ell'\ell''}$ coincide for all r , ϕ and z . This requires

$$|\ell'| - |\ell''| = N, \quad \ell' - \ell'' = M, \quad |\ell'| - |\ell''| = S, \quad (6)$$

to hold for two or more distinct pairs (ℓ', ℓ'') . For every $0 < n \leq \ell_{\max}$ one finds two such realizations: $\ell', \ell'' = n$ and $\ell', \ell'' = -n$ and as a result states $|\ell\rangle$ and $|- \ell\rangle$ cannot be discriminated by intensity measurements alone. As there are $\ell_{\max}$ such cases, the maximum number of linearly independent measurements generated by CCD scans in dimension d is

$$n_{Z \rightarrow \infty} = 4\ell_{\max}^2 + 4\ell_{\max} + 1 = d^2 - \frac{1}{2}(d-1). \quad (7)$$

For large dimensions $d^2 \gg d$ and the measurement setup becomes nearly complete.

Let us explore how the set of independent detections builds up. For a single plane, the Gouy's phase and hence relation (6) are of no consequence. The number of independent detections equals the number of distinct couples (N, M) that can be generated by $-\ell_{\max} \leq \ell', \ell'' \leq \ell_{\max}$. It can be checked that for a given N , each pair of nonnegative indexes $\ell', \ell'' \geq 0$, $|\ell'| + |\ell''| = N$ generates a unique (N, M) . Negative $\ell', \ell'' < 0$ do not add new entries to this set. Finally, there are only two possible M s for all pairs with opposite signs $M = \ell' - \ell'' = \ell' + (-\ell'') = \pm N$. When $N \leq \ell_{\max}$ these are already accounted for by $\ell' = 0, \ell'' = N$ and $\ell' = N, \ell'' = 0$ appearing

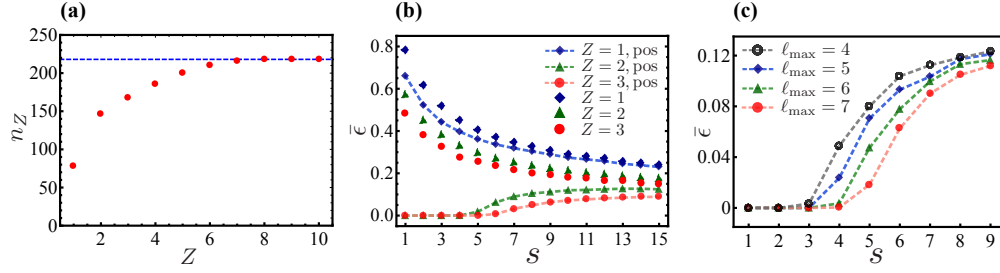


Fig. 1. Simulation of our compressed sensing protocol with twisted photons. (a) Number of independent detections n_Z generated by Z intensity scans along the propagation axis performed on a signal with $\ell_{\max} = 7$ ($d = 15$). The maximum of $n_Z = 218$ detections is obtained for $Z \geq 8$ scans. (b) Reconstructions errors, $\bar{\epsilon}$, from the compressed sensing protocol of the twisted photons as a function of the rank of the state for a fixed dimension ($\ell_{\max} = 7$) and for $Z = 1, 2$, and 3 CCD scans, with and without positivity constraint. (c) The reconstructions errors for two CCD scans and different dimensions. In all the cases, we take a 19×19 pixels screen.

in the set of nonnegative pairs. When $N > \ell_{\max}$, the values $M = \pm N$ make new entries. This gives $\sum_{\ell'=0}^N \sum_{\ell''=0}^{\ell_{\max}} \delta_{\ell'', N-\ell'} = N + 1$ entries for $N \leq \ell_{\max}$ and $2 + \sum_{\ell'=N-\ell_{\max}}^{\ell_{\max}} \sum_{\ell''=0}^{\ell_{\max}} \delta_{\ell'', N-\ell'} = 2\ell_{\max} - N + 3$ entries for $N > \ell_{\max}$. Taking sum over $N = 0 \dots 2\ell_{\max}$ this makes a total of

$$n_{Z=1} = \ell_{\max}^2 + 4\ell_{\max} + 1 = \frac{1}{4}(d^2 + 6d - 3) \quad (8)$$

independent detections generated by a single intensity scan—about a quarter of the maximum number of independent detections (7).

Going further, we realize that each couple (N, M) is degenerate; i.e., can be generated by at least two distinct pairs (ℓ', ℓ'') , except for $(N = 0, M = 0)$, and $(N = \ell_{\max}, M = \pm\ell_{\max})$. In addition, degenerate $(N > 0, M = 0)$ cannot be resolved by additional scans, as we have already discussed. Hence, the second scan adds $\Delta n_{Z=2} = \ell_{\max}^2 + 4\ell_{\max} + 1 - (3 + \ell_{\max}) = \ell_{\max}^2 + 3\ell_{\max} - 2$ additional independent detections, bringing the total for two scans to

$$n_{Z=2} = 2\ell_{\max}^2 + 7\ell_{\max} - 1 = \frac{1}{2}(d^2 + 5d - 8). \quad (9)$$

For higher Z , the new independent detections grow linearly with $\ell_{\max}$. A typical behaviour is shown in Fig. 1(a) for $\ell_{\max} = 7$: the maximum $n_{Z \rightarrow \infty}$ is approximately attained with 8 scans. Actually, the minimum scans required to approximately attain the maximum number of independent detections in the signal space is $Z_{\min} = \ell_{\max} + 1$.

The compressive tomography is done by solving (1), where now $\alpha = \{r, \phi, z\}$, and Π_α is defined by $\text{Tr}(\varrho \Pi_\alpha) = p(r, \phi, z)$. We first perform numerical simulations to explore the method. A set of random states of a given rank in the $\ell_{\max} = 7$ space is chosen and scanning measurements are simulated for $Z = 1, 2$, and 3 CCD planes with a 19×19 pixel geometry.

The data is subject to state reconstruction with and without the positivity constraints, where the latter is implemented with the help of the Moore-Penrose pseudoinverse [33]. Finally, for each true state, the corresponding Hilbert-Schmidt distances between the true and reconstructed states are calculated and the mean is taken over the set of true states of the same rank [34]. We take this as the error $\bar{\epsilon} = \mathbb{E}[\text{Tr}(\varrho_{\text{true}} - \hat{\varrho})^2]$.

In Fig. 1(b), we have plotted the errors $\bar{\epsilon}$ as a function of the rank of the state, for $\ell_{\max} = 7$. We observe a strong regularizing effect of the positivity constraint, especially on low-rank signals. First, positivity always makes the reconstruction errors smaller. Second, it cures the informational incompleteness of the tomography, provided the complexity of the measured signal stays below a

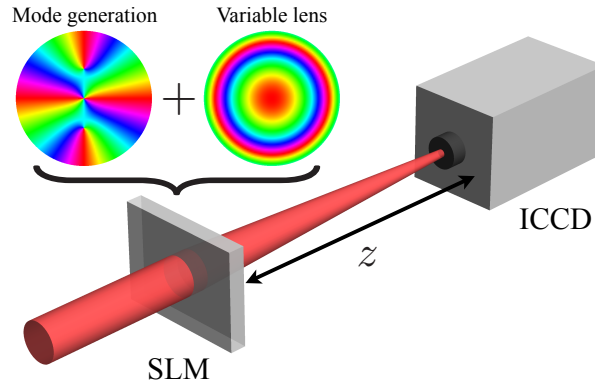


Fig. 2. Sketch of the experimental setup. A photonic state is generated by manipulating the phase and intensity of an incoming beam via the spatial light modulator (SLM). The beam is then focused using a variable holographic lens imprinted on the SLM together with the state generation hologram. The ICCD camera has a fixed position and records intensity scans. Inset shows the state and lens phase patterns, $[0, 2\pi)$, in a hue color.

certain threshold. Last, this threshold gets increased as we collect more scans. Notice though that protocols with positivity perform worse on more complex signals because the regularizing effect of positivity weakens. Loosely speaking, in comparing neighbourhoods of low- and high-rank states, one finds more nonphysical matrices in the former. Those objects get filtered by the positivity constraints leading to improved performance. The opposite is true of the protocols without positivity. Here, the more mixed states are less biased in the space of density matrices, so their average distance to the reconstructed matrix is smaller. Notice that this discussion does not apply to mutually compatible observations, for which positivity constraints are of no consequence. This can be observed in Fig. 1(c) for a single scan, where the regularizing effect of positivity disappears. Stronger incompatibilities introduced by detections from different planes $[\Pi_\alpha, \Pi_{\alpha'}] \neq 0$ are required to promote signal sparsity. The influence of the signal dimension with a fixed measurement is also illustrated in Fig. 1(c), for the particular case of two scans. The quality of the compressive OAM tomography improves with the signal dimension. At first glance, this might seem counterintuitive; however, note that the sparsity of a signal of a given rank grows with dimension and so do the regularizing effects of positivity constraints.

4. Experiment

To verify our scheme, we construct an experimental setup that allows us to generate and detect vortex beams at the single photon level using a spatial light modulator (SLM) and an intensified CCD (ICCD camera), respectively. A simplified sketch is shown in Fig. 2. A quasi-continuous UV laser, at a wavelength of 355 nm, is used to pump a type-I β -barium borate (BBO) crystal in order to generate single photons via spontaneous parametric downconversion. The spatial modes of the generated photons are filtered to the fundamental Gaussian mode by coupling them to a single mode fibre (SMF). A coincidence rate of 30 kHz and singles rate of 200 kHz is measured after the SMF. The photons are then coupled out of the SMF and are made incident on an SLM, (X10468-07, Hamamatsu) consisting of an electronically controlled nematic liquid crystal device with 792×600 pixels. The phase and the intensity of the generated photons are controlled via a holographic intensity masking technique [35], with a diffraction efficiency greater than 70 %. To achieve a higher mode quality, a 10 $\times$ microscope objective with a numerical aperture of 0.25 is employed to obtain a relatively large collimated beam at the SLM. The mode waist of the amplitude-modulated hologram at the SLM is determined to have an effectively flat phase and

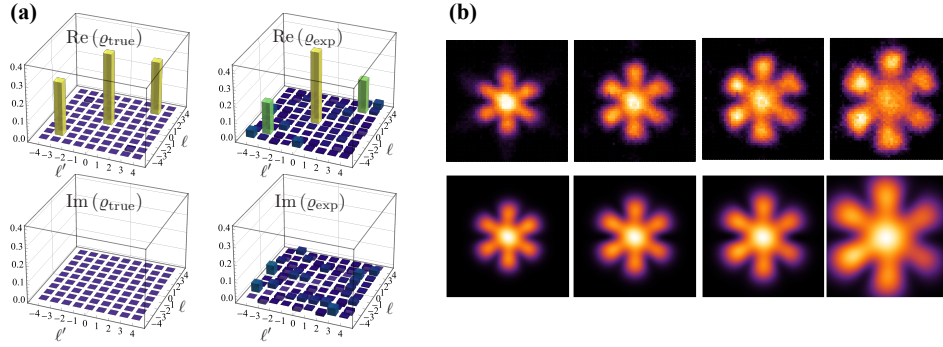


Fig. 3. Experimental reconstruction from compressed sensing. (a) Density matrix of the true state and (b) Reconstructed density matrix after two intensity scans with a signal space spanned by $\ell \in \{-4, \dots, 4\}$. The upper row shows four experimental ICCD scans at the planes $z/z_R = 0, 1/3, 1/2$, and 1, respectively. The lower row shows the predictions from the reconstructed state of the same ICCD scans.

intensity for the incoming beam over the region of interest of the hologram. By doing so, we may generate any arbitrary spatial mode with a high-level of accuracy. In the case of pure states, a single hologram is used for shaping the transverse modes of all photons in the ensemble. For mixed states, the appropriate holograms are randomly varied to generate incoherent statistical mixtures of the desired modes. A single intensity scan is then recorded over the whole ensemble of generated photons.

To observe the intensity variation of LG modes upon propagation, due to the differences in Gouy phases, the beam must propagate for distances that are on the order of the Rayleigh range z_R . This is achieved by simply focusing the beam. In the scheme described above, the ICCD camera is moved along the path of the beam in the z -direction. However, this is equivalent to varying the focal length of the lens and considering a fixed position of the ICCD camera. This is accomplished by imprinting a phase profile of the form $\exp(-i k r^2/2f)$, where f is the focal length of the flat lens. By doing so, our experimental reconstruction does not require any mechanical displacement of the components in the setup. Intensity scans are recorded for different focal lengths corresponding to positions of $z/z_R = 0, 1/3, 1/2$ and 1. Finally, both coincidence

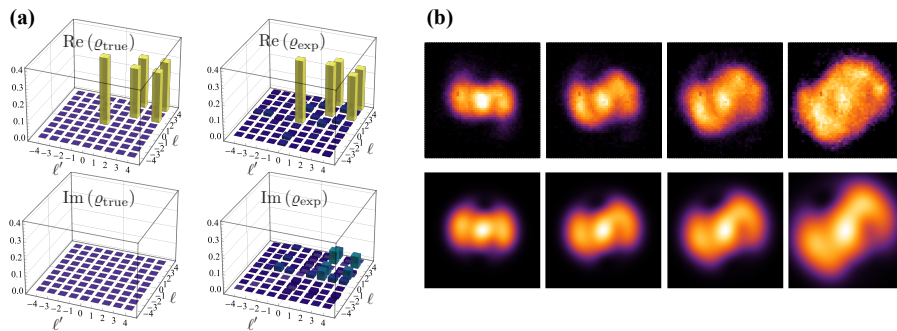


Fig. 4. Experimental reconstruction from compressed sensing. (a) Density matrix of the true state and (b) Reconstructed density matrix after one intensity scan. The upper row shows four experimental ICCD scans at the planes $z/z_R = 0, 1/3, 1/2$, and 1, respectively. The lower row shows the predictions from the reconstructed state of the same ICCD scans.

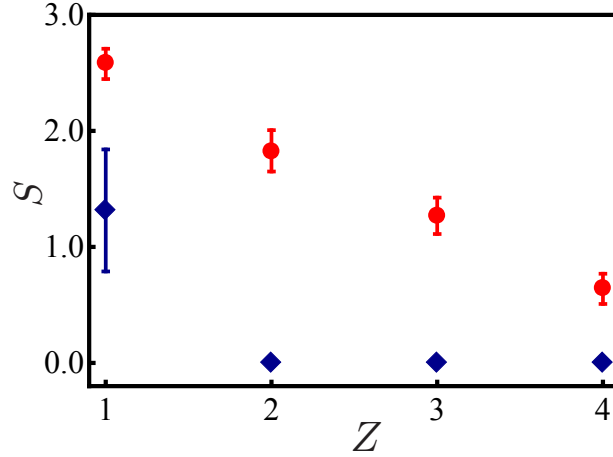


Fig. 5. Entropy S as a function of the number of intensity scans Z , for a signal space spanned by $\ell \in \{-4, \dots, 4\}$ and for true states of the form in (10). The circles are obtained by averaging over 20 random states and the error bars indicate the corresponding variance. Blue refers to protocol with positivity, while red is without positivity.

and singles counts measurements can be recorded with the ICCD camera. However, since we do not make use of the spatial correlation resulting from spontaneous parametric downconversion, the ICCD camera is used without triggering, where shorter integration time may be considered.

The true states are chosen to be following rank-2 states,

$$\varrho = p |0\rangle \langle 0| + (1 - p) |\Psi\rangle \langle \Psi|, \quad (10)$$

with $|\Psi\rangle = \cos \theta | -3\rangle + \sin \theta | 3\rangle$. In the experiment, we randomly generate 20 states for values of p and θ chosen. The OAM mixed states are generated by randomly varying the holograms displayed on the SLM. The holograms corresponding to the states $|0\rangle$ and $|\Psi\rangle$ are displayed for a fraction of the total integration time corresponding to p and $(1 - p)$, respectively. In Fig. 3, we present the results for a typical state ϱ with two ICCD scans. The corresponding reconstructed density matrix is plotted in the left column. Even though we are dealing with informationally incomplete measurements, the protocol with positivity using two intensity scans fits the theoretical data quite well. Without the positivity constraint, the reconstructed states are very different from the true ones. We have also experimentally checked that when the signal space is constrained to only positive topological charges ℓ , one intensity scan is enough to accurately predict the intensity scans in other planes, as anticipated by our theory.

We have also considered another set of rank-2 states, similar to Eq. (10), but now with $|\Psi\rangle = \cos \theta | 2\rangle + \sin \theta | 4\rangle$. The results are presented in Fig. 4. The reconstructed density matrix is plotted in the left column. We have also experimentally checked that when the signal space is constrained to only positive topological charges ℓ , one intensity scan is enough to accurately predict the intensity scans in other planes, as anticipated by our theory.

To assess the degree of IC for the intensity scans, we first consider a matrix of reconstructed states $\{\hat{\varrho}_j\}$ with its j th column defined as a flattened $\hat{\varrho}_j$. A unique solution for the extremal problem Eq.(1) then implies that the entropy of normalized singular values for this matrix is zero. To compute the entropy, we reconstructed 20 true states for every ICCD scan, and average over all of them. As can be seen in Fig. 5, the protocol with positivity constraints is enough to characterize the input state with solely two scans. We corroborate once again that if we restrict our space to be spanned only with nonnegative azimuthal indices, the measurement is IC for both strategies (with and without positivity) with only one intensity scan.

5. Concluding remarks

In summary, we have developed a compressed sensing scheme able to uniquely reconstruct any rank-deficient qudit state encoded in the OAM degree of freedom. The positivity constraint has played a substantial role as a powerful regularization to perform a tomographic reconstruction in the regime of informationally incomplete data for intermediately sized quantum systems. This establishes a novel and efficient tomographic paradigm for OAM systems that could trigger interesting experimental research on complex quantum states, which otherwise might have been infeasible with currently known detection schemes in such experiments.

Funding

European Union's Horizon 2020 Research and Innovation Programme (766970); Canada Research Chairs; Ontario's Early Researcher Award; BK21 Plus Program (21A2013111123); National Research Foundation of Korea (2010-0018295); Korea Institute of Science and Technology Institutional Program (2E27800-18-P043); Ministerio de Economía y Competitividad (FIS2015-67963-P); Grant Agency of the Czech Republic (18-04291S); Internal Grant Agency of the Faculty of Sciences of Palacký University (PrF 2018-003)

References

1. 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).
2. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New J. Phys.* **17**, 033033 (2015).
3. 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**, 1006–1010 (2017).
4. G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, "Free-space information transfer using light beams carrying orbital angular momentum," *Opt. Express* **12**, 5448–5456 (2004).
5. 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 (2012).
6. A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons," *Nature* **412**, 313 (2001).
7. J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, "Measuring the orbital angular momentum of a single photon," *Phys. Rev. Lett.* **88**, 257901 (2002).
8. J. Leach, J. Courtial, K. Skeldon, S. M. Barnett, S. Franke-Arnold, and M. J. Padgett, "Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon," *Phys. Rev. Lett.* **92**, 013601 (2004).
9. E. Karimi, B. Piccirillo, E. Nagali, L. Marrucci, and E. Santamato, "Efficient generation and sorting of orbital angular momentum eigenmodes of light by thermally tuned q-plates," *Appl. Phys. Lett.* **94**, 231124 (2009).
10. G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. Beijersbergen, and M. J. Padgett, "Efficient sorting of orbital angular momentum states of light," *Phys. Rev. Lett.* **105**, 153601 (2010).
11. M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, "Efficient separation of the orbital angular momentum eigenstates of light," *Nat. Commun.* **4**, 2781 (2013).
12. N. Bent, H. Qassim, A. A. Tahir, D. Sych, G. Leuchs, L. L. Sánchez-Soto, E. Karimi, and R. W. Boyd, "Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures," *Phys. Rev. X* **5**, 041006 (2015).
13. E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inform. Theory* **52**, 489–509 (2006).
14. E. J. Candes and T. Tao, "The power of convex relaxation: Near-optimal matrix completion," *IEEE Trans. Inf. Theory* **56**, 2053–2080 (2010).
15. Y. C. Eldar and G. Kutyniok, *Compressed Sensing: Theory and Applications* (Cambridge University, 2012).
16. A. Stern, *Optical Compressive Imaging* (CRC, 2016).
17. D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," *Phys. Rev. Lett.* **105**, 150401 (2010).
18. A. Shabani, R. L. Kosut, M. Mohseni, H. Rabitz, M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White, "Efficient measurement of quantum dynamics via compressive sensing," *Phys. Rev. Lett.* **106**, 100401 (2011).
19. W.-T. Liu, T. Zhang, J.-Y. Liu, P.-X. Chen, and J.-M. Yuan, "Experimental quantum state tomography via compressed sampling," *Phys. Rev. Lett.* **108**, 170403 (2012).

20. C. Schwemmer, G. Tóth, A. Niggebaum, T. Moroder, D. Gross, O. Gühne, and H. Weinfurter, "Experimental comparison of efficient tomography schemes for a six-qubit state," *Phys. Rev. Lett.* **113**, 040503 (2014).
21. A. V. Rodionov, A. Veitia, R. Barends, J. Kelly, D. Sank, J. Wenner, J. M. Martinis, R. L. Kosut, and A. N. Korotkov, "Compressed sensing quantum process tomography for superconducting quantum gates," *Phys. Rev. B* **90**, 144504 (2014).
22. F. Tonolini, S. Chan, M. Agnew, A. Lindsay, and J. Leach, "Reconstructing high-dimensional two-photon entangled states via compressive sensing," *Sci. Rep.* **4**, 6542 (2014).
23. A. Steffens, C. A. Riofrío, W. McCutcheon, I. Roth, B. A. Bell, A. McMillan, M. S. Tame, J. G. Rarity, and J. Eisert, "Experimentally exploring compressed sensing quantum tomography," *Quantum Sci. Technol.* **2**, 025005 (2017).
24. C. A. Riofrío, D. Gross, S. T. Flammia, T. Monz, D. Nigg, R. Blatt, and J. Eisert, "Experimental quantum compressed sensing for a seven-qubit system," *Nat. Commun.* **8**, 15305 (2017).
25. A. Kalev, R. L. Kosut, and I. H. Deutsch, "Quantum tomography protocols with positivity are compressed sensing protocols," *npj quantum inf.* **1**, 15018 (2015).
26. A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, 2002).
27. E. Prugovečki, "Information-theoretical aspects of quantum measurement," *Int. J. Theor. Phys.* **16**, 321–331 (1977).
28. P. Busch and P. J. Lahti, "The determination of the past and the future of a physical system in quantum mechanics," *Found. Phys.* **19**, 633–678 (1989).
29. E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *C. R. Math.* **346**, 589–592 (2008).
30. S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University, 2004).
31. A. Siegman, *Lasers* (Oxford University, 1986).
32. R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of the phase from image and diffraction plane pictures," *Optik* **35**, 237–246 (1972).
33. A. Ben-Israel and T. N. E. Greville, *Generalized Inverses: Theory and Applications* (Wiley, 1977).
34. A. Luis, "Degree of coherence for vectorial electromagnetic fields as the distance between correlation matrices," *J. Opt. Soc. Am. A* **24**, 1063–1068 (2007).
35. E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, "Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram," *Opt. Lett.* **38**, 3546–3549 (2013).

Adaptive Compressive Tomography with No *a priori* Information

D. Ahn, Y. S. Teo,^{*} and H. Jeong

Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea

F. Bouchard, F. Hufnagel, and E. Karimi

Physics Department, University of Ottawa, 25 Templeton Street, Ottawa, Ontario, K1N 6N5 Canada

D. Koutný, J. Řeháček, and Z. Hradil

Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic

G. Leuchs and L. L. Sánchez-Soto

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



(Received 17 December 2018; published 15 March 2019)

Quantum state tomography is both a crucial component in the field of quantum information and computation and a formidable task that requires an incalculable number of measurement configurations as the system dimension grows. We propose and experimentally carry out an intuitive adaptive compressive tomography scheme, inspired by the traditional compressed-sensing protocol in signal recovery, that tremendously reduces the number of configurations needed to uniquely reconstruct any given quantum state without any additional *a priori* assumption whatsoever (such as rank information, purity, etc.) about the state, apart from its dimension.

DOI: [10.1103/PhysRevLett.122.100404](https://doi.org/10.1103/PhysRevLett.122.100404)

Introduction.—The characterization of an unknown (true) quantum state $\rho_t \geq 0$ of Hilbert-space dimension d is a subject of immense study in quantum information [1–3]. To fully reconstruct an *arbitrary* ρ_t , one may perform a set of measurements that is enough to characterize all $d^2 - 1$ independent parameters that define ρ_t . Unfortunately, the number of such measurements generally grows polynomially with d , or exponentially with the number of subsystems that determine the quantum-source complexity. This poses a technical limitation on how far conventional quantum tomography can go in practical experiments [4,5].

If we know *a priori* that rank $\{\rho_t = \rho_r\} \leq r$ is extremely small, $r \ll d$, then the concept of compressed sensing (CS), whose foundation was first mathematically laid in the context of imaging [6–8], facilitates the search for a unique estimator by measuring much fewer configurations [9–12]. We say that the corresponding data are *informationally complete (IC)* for ρ_r . The state-of-the-art CS measurements to be performed given such prior information have been constructed in Ref. [13].

The standard CS procedure, nevertheless, has two important issues that need to be addressed. First, an *a priori* knowledge about r is necessary to establish a preliminary order-of-magnitude estimate for the number of configurations needed to fully characterize ρ_r of rank no larger than r . Accuracy of the final estimator is hence highly dependent on the validity of this *a priori* guess. Second, one has no means of verifying whether the measurement

data at hand are truly IC for ρ_r in the standard scheme. Typically, accuracy surveys with target states are employed [10–12] and the value of such a survey relies on the precision of these target states. Therefore, the decision of *a priori* rank information and presumed choices of target states are ultimately debatable in the presence of experimental errors, rendering the reliability of any related tomography scheme questionable.

In this Letter, we establish a new adaptive tomography paradigm that completely removes the need for any sort of *a priori* information about ρ_r (except for its dimension d). Our proposed *adaptive compressive tomography* (ACT) also includes an efficient recipe to determine informational completeness of the collected data. No target states are ever required to validate the resulting state estimator. The convex boundary of the quantum state space and the positivity constraint plays the principal role in checking whether the accumulated data are IC and adaptively choosing measurements efficiently to uniquely reconstruct ρ_r , the two of which completely define the purpose of ACT.

To demonstrate ACT, we perform an experiment with the orbital angular momentum (OAM) of single photons and apply ACT to states of various ranks engineered in these degrees of freedom. Both experimental and simulated results show that ACT requires a smaller number of measurements to reconstruct rank-deficient quantum states as compared to conventional CS tomography with known types of CS measurements.

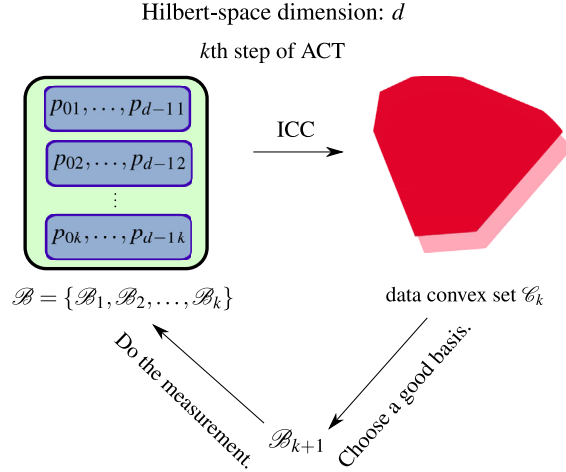


FIG. 1. Schematic diagram of a particular adaptive step in ACT tomography. In a clockwise flow, ACT first performs ICC to check whether data (blue) collected from measuring $\mathcal{B}$ are IC or not. If not, it proceeds to choose a good basis to measure in the next step.

The quantum state space and ACT.—In the absence of statistical fluctuations, we measure a randomly chosen computational basis $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ on ρ_r of Hilbert-space dimension d . The corresponding Born probabilities $p_j = \langle j | \rho_r | j \rangle$ ($0 \leq j \leq d-1$) specify only the diagonal elements of ρ_r , and there is in principle a *data convex set* $\mathcal{C} = \{\rho | \rho \leftrightarrow p_j \ \forall \ j\}$ comprising infinitely many estimators $\hat{\rho}$ that are consistent with p_j . Evidently, $\rho_r \in \mathcal{C}$, and so the only fundamental objective of ACT is to shrink $\mathcal{C}$ to a single point with only $k_{\text{IC}} \ll d+1$ IC measurement bases for $r \ll d$. For noiseless situations, this point must be ρ_r .

To gain insights into how quantum positivity constraint plays a major role in shrinking $\mathcal{C}$, we argue in the Supplemental Material (Sec. I [14]) that if one methodically measures $k_0 = \lceil (r^2 - r)/(d-1) \rceil + 1$ orthonormal bases, one of which being the eigenbasis $\mathcal{B}_{\rho_r}$ of ρ_r , then $\hat{\rho} = \rho_r$ is the *unique positive estimator* consistent with all measured probabilities. For $r \ll d$, the regime of our interest, $k_0 = 2$. It is however clear that $k_{\text{IC}} > 2$ in real-world settings where ρ_r is completely unknown (apart from its dimension d), so the famous no-go answer to Pauli’s phase-retrieval problem [15,16] still stands. Regardless, the positivity constraint can still ensure an efficient compression of the IC tomography procedure solely by data analysis.

The goal of ACT is to uniquely reconstruct any given unknown ρ_r through adaptively measuring one orthonormal basis at a time according to collected data, as sketched in Fig. 1. In the k th step of the adaptive scheme, ACT performs two main procedures. (1) First, ACT checks whether the probabilities $p_{j'k'} = \text{tr}\{\rho_r \Pi_{j'k'}\}$ obtained from outcomes $\Pi_{j'k'} > 0$ ($\Pi_{j'k'} \Pi_{j''k''} = \delta_{j',j''} \delta_{k',k''}$) of all the measured orthonormal bases $\mathcal{B} = \{\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k\} = \{\Pi_{01}, \dots, \Pi_{d-11}, \dots, \Pi_{0k}, \dots, \Pi_{d-1k}\}$ so far are IC. Since the *accumulated* data define a

data convex set $\mathcal{C}_k$ of size s_k that contains all quantum states ρ consistent with $p_{j'k'}$, this procedure is tantamount to finding out whether s_k is zero or not. If $s_{k=k_{\text{IC}}} = 0$, then the estimator $\hat{\rho}_{k=k_{\text{IC}}} \geq 0$ consistent with the IC data is unique by definition, and equal to ρ_r when statistical fluctuation is absent. (2) If $s_k \neq 0$, the accumulated data collected are not IC and ACT shall choose the next basis by analyzing $\mathcal{C}_k$. Beginning with $k = 1$, a “good” adaptive bases sequence should lead to a quick convergence of $\mathcal{C} \rightarrow \rho_r$ as ACT progresses.

Informational completeness certification (ICC).—To certify whether all collected data are IC or not in the k th adaptive step, it suffices to note that since $\mathcal{C}_k$ is convex, maximizing and minimizing the linear function $f_Z(\rho) = \text{tr}\{\rho Z\}$ for some operator Z over $\rho \in \mathcal{C}_k$, respectively, give unique solutions ρ_{max} and ρ_{min} to the corresponding maximum $f_{\text{max},k}$ and minimum $f_{\text{min},k}$. Without loss of generality, Z is taken to be a random full-rank state. We may define the quantity $s_{\text{CVX},k} = (f_{\text{max},k} - f_{\text{min},k}) / (f_{\text{max},1} - f_{\text{min},1})$ that is a *size monotone* (see Sec. II of Supplemental Material [14]) for $\mathcal{C}_k$ in the sense that $s_k < s_{k-1}$ if $s_{\text{CVX},k} < s_{\text{CVX},k-1}$ —it is a witness for the shrinkage of $\mathcal{C}_k$. As more linearly independent bases are measured, $s_{\text{CVX},k} \geq s_{\text{CVX},k+1}$ and $s_{\text{CVX},k_{\text{IC}}} = 0$ implies that $s_{k_{\text{IC}}} = 0$ and that all data collected are IC for a unique reconstruction of ρ_r . Therefore, at every adaptive step in ACT, we run: ICC in the k th step. (1) Maximize and minimize $f_Z(\rho) = \text{tr}\{\rho Z\}$ for a fixed, randomly chosen full-rank state $Z \neq 1/d$ to obtain $f_{\text{max},k}$ and $f_{\text{min},k}$ subject to the following: (i) $\rho \geq 0$, $\text{tr}\{\rho\} = 1$, (ii) $\text{tr}\{\rho \Pi_{j'k'}\} = p_{j'k'}^{(\text{ML})}$ for $0 \leq j' \leq d-1$ and $1 \leq k' \leq k$. (2) Compute $0 \leq s_{\text{CVX},k} \leq 1$ and check if it is smaller than some threshold ε . (3) If $s_{\text{CVX},k} < \varepsilon$, terminate ACT. Continue otherwise.

The aforementioned strategy is, as a matter of fact, a semidefinite program (SDP) [17] that can be efficiently solved by a variety of numerical methods. We should clarify here that while determining whether a set of measurement bases $\mathcal{B}$ possesses the conventional CS property for the entire class of rank- r states is an NP-hard problem [18], ascertaining whether $\mathcal{B}$ gives a unique estimator for one unknown ρ_r with the measurement data is, on the other hand, only as computationally difficult as carrying out the semidefinite program in ICC with a worst-case polynomial complexity [17].

For experimental data $\sum_j \nu_{j'k'} = 1$ ($1 \leq k' \leq k$) with statistical noise, $\mathcal{C}_k$ is defined as the *maximum-likelihood (ML) convex set* in which all $\rho \in \mathcal{C}_k$ satisfy the physical constraints $p_{j'k'}^{(\text{ML})} = \text{tr}\{\rho \Pi_{j'k'}\}$ imposed by the ML principle for quantum states $[p_{j'k'}^{(\text{ML})} \rightarrow p_{j'k'} \text{ for } N \rightarrow \infty]$ [2,3,19,20]. All arguments for noiseless data hold exactly for the ML probabilities, so that the working principle of ICC is *perfectly robust against arbitrary noise* in the sense that $s_{\text{CVX},k_{\text{IC}}} = 0$ still implies $s_{k_{\text{IC}}} = 0$ for noisy data owing to the preserved convexity of the newly defined $\mathcal{C}_k$. Noise only affects the reconstruction accuracy of the final unique

estimator relative to ρ_r , which is a different subject matter for discussion.

Adaptive selection of measurement bases.—The optimal orthonormal basis to pick in the k th step and measure in the $(k + 1)$ th step is the one that minimizes $s_{\text{CVX},k+1}$. Since ρ_r is unknown, we can treat some *a posteriori* estimator $\hat{\rho}_k$ from $\mathcal{C}_k$ as a guess for ρ_r to generate simulated data during the minimization of $s_{\text{CVX},k+1}$ over all future basis choices. The complicated dependence of $s_{\text{CVX},k+1}$ on the future basis however makes its brute-force optimization computationally exhaustive for large d .

For a more tractable approach to adaptively measure good bases, we first note that $\mathcal{C}_{k < k_{\text{IC}}}$ essentially contains states with eigenbases that are distinct from $\{\mathcal{B}_1, \dots, \mathcal{B}_k\}$ (see Sec. III of the Supplemental Material [14]). So even if we know nothing about ρ_r , if it is rank-deficient, then taking $\mathcal{B}_{k+1}$ to be the diagonal basis of a rank-deficient $\hat{\rho}_k \in \mathcal{C}_k$ ensures a distinct measurement basis in each step that generates a reasonably fast converging sequence $\mathcal{B}_k \rightarrow \mathcal{B}_{\rho_r}$ as k increases since $\mathcal{C}_k \rightarrow \rho_r$ at the same time. There is more than one approach to pick eigenbases of rank-deficient states from $\mathcal{C}_k$, and as an example we shall consider the minimization of von Neumann entropy function $S(\rho) = -\text{tr}\{\rho \log \rho\}$. A superfast algorithm suitable for minimizing S over $\mathcal{C}_k$ exists [20,21]. Incidentally, it was reported in Refs. [22,23] that entropy minimization also offers high compressive efficiencies in both sparse-signal and low-rank matrix recovery.

Complete ACT protocol.—All aforementioned arguments can accommodate real experimental situations, where the relative frequency data do not typically correspond to physical quantum states for $k > 1$. The data convex sets contain states that are now consistent with the corresponding physical ML probabilities derived from data, which are statistically consistent with the true probabilities. The final unique estimator $\hat{\rho}_{k_{\text{IC}}}$ would then incur a statistical bias from ρ_r that drops as N increases. For many-body quantum sources, the bases generated by ACT are entangled. In practice, product bases are typically much more practical to implement for such sources. While verifying if a rank-deficient $\hat{\rho}_k \in \mathcal{C}_k$ can possess a product eigenbasis is computationally difficult, ACT can still be adjusted to feasibly generate near-optimal product bases (PACT) by defining $\mathcal{B}_{k+1}$ to be the product basis that is nearest to the eigenbasis of $\hat{\rho}_k$ with respect to some given norm using a nonlinear optimization routine. Both ACT and PACT for any experimental setting are summarized as follows: Beginning with $k = 1$ and a random computational basis $\mathcal{B}_1$: (1) measure $\mathcal{B}_k$ and collect the relative frequency data $\sum_{j'=0}^{d-1} \nu_{j'k} = 1$. (2) From $\{\nu_{0k'}, \dots, \nu_{d-1k'}\}_{k'=1}^k$, obtain kd physical ML probabilities. (3) Perform ICC with the ML probabilities and compute $s_{\text{CVX},k}$: (i) If $s_{\text{CVX},k} < \epsilon$, terminate ACT and take $\rho_{\text{max}} \approx \rho_{\text{min}}$ as the estimator and report $s_{\text{CVX},k}$. (ii) Else Proceed. (4) Choose a rank deficient $\hat{\rho}_k \in \mathcal{C}_k$ [for instance by minimizing the von Neumann entropy $S(\rho)$

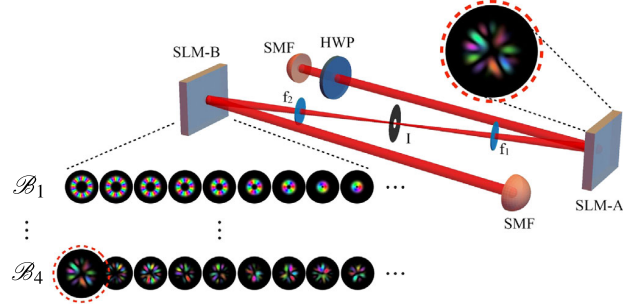


FIG. 2. Schematic of the OAM-based experimental setup. A 16-dimensional OAM state is generated at SLM-A using a holographic technique that allows the tailoring of the intensity and phase profile of the incoming beam. The modulated first-order of diffraction is filtered out using an iris (I) and a pair of lenses (f_1 and f_2). A similar holographic technique is used at the second SLM-B to measure the state in a given basis. The first measurement basis, $\mathcal{B}_1$, is given by the OAM computational basis. In the case of the rank 1 state shown on SLM-A, the corresponding eigenbasis is achieved after the fourth iteration.

in $\mathcal{C}_k$]. (5) Define $\mathcal{B}_{k+1}$ to be the eigenbasis of $\hat{\rho}_k$ for ACT, or a basis close to it for PACT via some prechosen distance minimization technique. (6) Set $k = k + 1$ and repeat.

Analysis and experiments.—We put both ACT and PACT tomography schemes to the experimental test by comparing their results with those from measuring random Pauli (RP) bases considered in Refs. [10–12], the Baldwin-Goyeneche (BG) bases in Ref. [13] that generalizes a known five-bases construction for $r = 1$ to an IC set of $k_{\text{IC}} = 4r + 1$ bases for rank- r quantum states, and the set of random orthonormal bases of $k_{\text{IC}} \approx [4r(d - r)/(d - 1)]$ studied in Ref. [24]. This exact scaling shall be used to benchmark the experimental k_{IC} s.

To demonstrate all three schemes (see Fig. 2), we experimentally emulate a four-qubit ($d = 16$) quantum system and both entangled and product measurement bases using an OAM-based setup. In particular, we consider the Laguerre-Gauss (LG) modes with azimuthal and radial mode indices ℓ and $p = 0$, respectively. Hence, OAM states correspond to a subspace of the LG modes and are characterized by a helical wave front given by $e^{i\ell\phi}$, where ℓ is the azimuthal index that corresponds to the OAM value, and ϕ is the azimuthal coordinate. The appropriate phase and intensity patterns are realized using a holographic technique called *intensity masking*, which is readily achieved by a programmable spatial light modulator (SLM) [25]. By doing so, we can prepare *any* many-body state and measurement basis. The generated photons are detected using the projective technique of *intensity flattening* [26], where any arbitrary spatial mode can be measured using an SLM followed by a single mode fiber (SMF).

A heralded single photon source is achieved by pumping a 3 mm β -barium borate type I nonlinear crystal with a quasicontinuous wave laser at a wavelength of 355 nm,

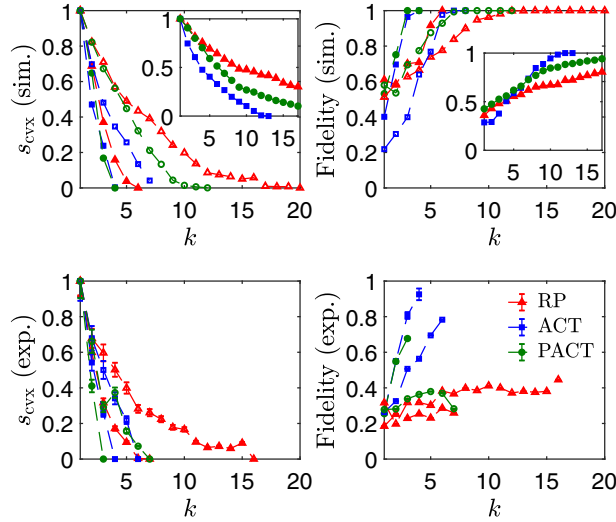


FIG. 3. Plots of simulation (noiseless) and experimental values of s_{cvx} and $\hat{\rho}_k$ fidelity against the measured basis number k for $d = 16$, where $\hat{\rho}_k := \rho_{\min}$ for the RP scheme. Estimated experimental error bars reflect the propagated Poissonian-source standard deviations. All plot markers are averaged over five ρ_r s. The filled markers represent results for rank-1 ρ_r s whereas the unfilled ones represent those for rank-3 ρ_r s. The insets showcase simulation performances of rank-6 states as a demonstration of high-rank ($r \approx D/2$) compressive tomography, with $1 \leq k \leq (D+1) = 17$ restricted to the minimal bases number for arbitrary-state tomography. The lower experimental fidelities for RP and PACT are due to a technical bias of the OAM setup for finite N , where bases close to the eigenbasis of ρ_r tend to give estimated Born probabilities that are relatively more accurate than those that are not. So for OAM sources, ACT is the most favorable option, as both PACT and RP correspond to measurement bases that are never close to the eigenbasis of ρ_r . Even with noisy data, ICC can still validate whether the resulting ML probabilities obtained from data are IC (left panels), which is the point of ACT.

producing photon pairs at 710 nm via spontaneous parametric down-conversion. A coincidence rate of 40 kHz, within a coincidence time window of 5 ns, is measured after filtering the photons to the fundamental Gaussian modes using SMF. Subsequent to the generation and detection of the photonic states, explained above, coincidence measurements are recorded using single photon detectors and a coincidence logic.

All results are summarized in Figs. 3 and 4, and the messages conveyed are succinctly stated here: for noiseless simulated data, in terms of *average* k_{IC} over uniformly (Hilbert-Schmidt) distributed rank- r true states, ACT is the most efficient, since it guides the measurement basis to the eigenbasis of ρ_r . The more many-body-suited PACT that adaptively generates product bases requires a larger k_{IC} to yield IC data, but the average performance margin with ACT is narrow for low- r states and is on par with the scaling of entangled Goyeneche-type bases ($k_{\text{IC}} = 4r + 1$)

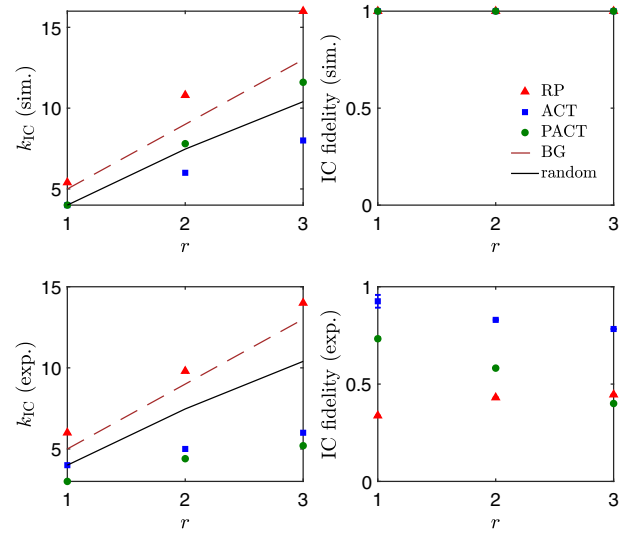


FIG. 4. Plots of simulation (noiseless) and experimental values of k_{IC} and the $\hat{\rho}_{k=k_{\text{IC}}}$ fidelity against the rank $1 \leq r \leq 3$ of ρ_r . All k_{IC} values ascertained using ICC are averaged over five ρ_r s per rank. Otherwise all specifications are the same as Fig. 3. Although, for real data, positivity modifies the k_{IC} performances with ML, and PACT achieves informational completeness much quicker than RP as far as local bases are concerned. A comparison with random IC orthonormal bases shows that ACT gives a much lower value owing to the additional assessment of and optimization over $\mathcal{C}$.

for larger r . RP turns out to be least efficient amongst all tested schemes. Even in the presence of real data noise, both ACT and PACT remain the more favorable candidates for tomography on general complex systems.

Concluding remarks.—The feasible concept of adaptive compressive tomography developed here provides a powerful method to reconstruct any unknown rank-deficient quantum state with optimally chosen entangled or product orthonormal measurement bases, especially for quantum sources of complex degrees of freedom, which includes many-body systems. More importantly, the adaptive scheme requires no *a priori* knowledge or assumptions about the state or near-proximity target states because it can self-sufficiently validate whether the measured data are informationally complete or not using semidefinite programming, so that reliable compressive tomography can now be carried out in real experimental situations with noisy data. The superior compressive efficiencies of both entangled and product versions of our adaptive schemes are confirmed experimentally and demonstrated with respect to other established protocols.

We acknowledge financial support from the BK21 Plus Program (21A2013111123) funded by the Ministry of Education (MOE, Korea) and National Research Foundation of Korea (NRF), the NRF grant funded by the Korea government (MSIP) (Grant No. 2010-0018295), the European Unions Horizon 2020 Research and

Innovation Programme under Grant Agreement No. 766970, Canada Research Chairs (CRC), the Spanish MINECO (Grant No. FIS2015-67963-P), the Grant Agency of the Czech Republic (Grant No. 18-04291S), and the IGA Project of the Palacký University (Grant No. IGA PrF 2018-003).

*ys_teo@snu.ac.kr

- [1] I. Chuang and M. Nielsen, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
- [2] *Quantum State Estimation*, edited by M. G. A. Paris and J. Řeháček, Lecture Notes in Physics, Vol. 649 (Springer, Berlin, 2004).
- [3] Y. S. Teo, *Introduction to Quantum-State Estimation* (World Scientific Publishing Co., Singapore, 2015).
- [4] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, Scalable multiparticle entanglement of trapped ions, *Nature (London)* **438**, 643 (2005).
- [5] J. G. Titchener, M. Gräfe, R. Heilmann, A. S. Solntsev, A. Szameit, and A. A. Sukhorukov, Scalable on-chip quantum state tomography, *NJP Quantum Inf.* **4**, 19 (2018).
- [6] D. Donoho, Compressed sensing, *IEEE Trans. Inf. Theory* **52**, 1289 (2006).
- [7] E. J. Candès and T. Tao, Near-optimal signal recovery from random projections: Universal encoding strategies? *IEEE Trans. Inf. Theory* **52**, 5406 (2006).
- [8] E. J. Candès and B. Recht, Exact matrix completion via convex optimization, *Found. Comput. Math.* **9**, 717 (2009).
- [9] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Quantum State Tomography via Compressed Sensing, *Phys. Rev. Lett.* **105**, 150401 (2010).
- [10] A. Kalev, R. L. Kosut, and I. H. Deutsch, Quantum tomography protocols with positivity are compressed sensing protocols, *NJP Quantum Inf.* **1**, 15018 (2015).
- [11] A. Steffens, C. A. Riofro, W. McCutcheon, I. Roth, B. A. Bell, A. McMillan, M. S. Tame, J. G. Rarity, and J. Eisert, Experimentally exploring compressed sensing quantum tomography, *Quantum Sci. Technol.* **2**, 025005 (2017).
- [12] C. A. Riofro, D. Gross, S. T. Flammia, T. Monz, D. Nigg, R. Blatt, and J. Eisert, Experimental quantum compressed sensing for a seven-qubit system, *Nat. Commun.* **8**, 15305 (2017).
- [13] C. H. Baldwin, I. H. Deutsch, and A. Kalev, Strictly-complete measurements for bounded-rank quantum-state tomography, *Phys. Rev. A* **93**, 052105 (2016).
- [14] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.122.100404> for details concerning properties of the size monotone and data convex set.
- [15] W. Pauli, *Die allgemeinen Prinzipien der Wellenmechanik, Handbuch der Physik*, edited by H. Geiger and K. Scheel (Springer-Verlag, Berlin, 1933), Vol. 24.
- [16] C. Carmeli, T. Heinosaari, J. Schultz, and A. Toigo, How many orthonormal bases are needed to distinguish all pure quantum states?, *Eur. Phys. J. D* **69**, 179 (2015).
- [17] L. Vandenberghe and S. Boyd, Semidefinite programming, *SIAM Rev.* **38**, 49 (1996).
- [18] A. S. Bandeira, E. Dobriban, D. G. Mixon, and W. F. Sawin, Certifying the restricted isometry property is hard, *IEEE Trans. Inf. Theory* **59**, 3448 (2013).
- [19] J. Řeháček, Z. Hradil, E. Knill, and A. I. Lvovsky, Diluted maximum-likelihood algorithm for quantum tomography, *Phys. Rev. A* **75**, 042108 (2007).
- [20] J. Shang, Z. Zhang, and H. K. Ng, Superfast maximum-likelihood reconstruction for quantum tomography, *Phys. Rev. A* **95**, 062336 (2017).
- [21] Y. S. Teo, H. Zhu, B.-G. Englert, J. Řeháček, and Z. Hradil, Quantum-State Reconstruction by Maximizing Likelihood and Entropy, *Phys. Rev. Lett.* **107**, 020404 (2011).
- [22] S. Huang, D. N. Tran, and T. D. Tran, Sparse signal recovery based on nonconvex entropy minimization, in *2016 IEEE International Conference on Image Processing (ICIP)*, Phoenix, AZ, USA, 2016 (IEEE, Phoenix, 2016), p. 3867.
- [23] D. N. Tran, S. Huang, S. P. Chin, and T. D. Tran, Low-rank matrices recovery via entropy function, in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, China, 2016 (IEEE, Shanghai, 2016), p. 4064.
- [24] M. Kech and M. M. Wolf, Constrained quantum tomography of semi-algebraic sets with applications to low-rank matrix recovery, *Inf. Inference* **6**, 171 (2016).
- [25] E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram, *Opt. Lett.* **38**, 3546 (2013).
- [26] F. Bouchard, N. H. Valencia, F. Brandt, R. Fickler, M. Huber, and M. Malik, Measuring azimuthal and radial modes of photons, *Opt. Express* **26**, 31925 (2018).

Chapter 3

Underwater Quantum Communication

This chapter is based on the following papers:

1. F. Bouchard, A. Sit, **F. Hufnagel**, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, & E. Karimi, “Quantum cryptography with twisted photons through an outdoor underwater channel”, *Optics Express* **26**, 22563-22573 (2018).

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

© 2018 Optical Society of America

2. **F. Hufnagel**, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, & E. Karimi, “Characterization of an underwater channel for quantum communications in the Ottawa River”, *Optics Express* **27**, 26346-26354 (2019).

DOI: <https://doi.org/10.1364/OE.27.026346>

© 2019 Optical Society of America

3. **F. Hufnagel**, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, & E. Karimi, “Underwater quantum communication over a 30-meter

flume tank”, *arXiv*:2004.04821 (2020)

3.1 Quantum Key Distribution

Quantum communication was first proposed in 1984 by Charles Bennett and Gilles Brassard with their quantum key distribution (QKD) protocol, now referred to as BB84 [14]. The goal of quantum communication is to utilize the potential of the quantum mechanical properties of light. In the case of QKD, this is done to attain absolute secure communication. There are other application especially when considering entanglement distribution which open the door to quantum teleportation and remote quantum computation applications [15]. In the BB84 key distribution protocol two parties, namely Alice and Bob, want to share a secret key which they will use as a one time pad for classical encryption. It is important to note that this one time pad is used on a classical channel unrelated to the quantum channel. The task of QKD is to generate this key without allowing an eavesdropper to gain any information by hacking the channel. The first step in the BB84 protocol is that Alice and Bob decide on a set of mutually unbiased bases (MUB) which will be used in encoding information on the photon. The important property of these MUB is that a measurement in the same basis as the photon was encoded will give an exact knowledge of the state which was sent. While measurement in a different basis than the photon was sent will give zero information about the state. This can be clearly demonstrated with mathematics by taking as our two bases $|\psi_n\rangle$ and $|\phi_n\rangle$ where the number of states $n \in \{1, \dots, d\}$ is dependent on the dimensionality of the states being used. In the original protocol using polarization we have $d = 2$. The mutually unbiased property requires the measurement probabilities, i.e., the projection onto a given state, to follow

$$\begin{aligned} |\langle\psi_i|\psi_j\rangle|^2 &= \delta_{ij} \\ |\langle\psi_i|\phi_j\rangle|^2 &= \frac{1}{d}, \end{aligned} \tag{3.1}$$

where $\delta_{ij} = 0$ for $i \neq j$ and $\delta_{ij} = 1$ for $i = j$. Let us show this explicitly for the example of polarization. We can use the orthogonal linear polarization bases. One of these being the horizontal and vertical polarization, and the other being the diagonal and anti-diagonal. Defining these in terms of the first basis, we have:

$$|\psi_n\rangle = \{|H\rangle, |V\rangle\},$$

$$|\phi_n\rangle = \{|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}\}, \quad (3.2)$$

as our two MUB. It can be seen that these satisfy equation (3.1). To encode information in these bases, one of the states in each basis is assigned “1” and the other assigned “0”. Alice now prepares her photons to send to Bob, randomly selecting the basis and the state. At the receiving end, Bob randomly selects the basis he will make the measurement in and records the result. Note that Bob will randomly select the “wrong” basis 50% of the time since Alice’s choice of basis is random and unknown to Bob. At this point the quantum channel has served its purpose. Alice and Bob now communicate classically telling each other which basis they sent and measured the photons in. They throw away the bits corresponding to measurements made in the wrong basis. It is important to note that this classical communication is done after the photons have been sent so this information is not available to an eavesdropper at the time that the quantum states are being sent. Finally, Alice and Bob will take some of the bits and share the values with each other to check for errors. This is where the properties of quantum mechanics come into play. If an eavesdropper made measurements on the photons when they were transmitted, then she would alter the quantum state. This alteration of the quantum state will present itself in errors when Alice and Bob check. Thus they are able to find out if someone has hacked their channel. If this is the case, Alice and Bob will throw away the entire key and not use it as a one time pad for encryption. There is a certain error threshold, below which it can be guaranteed that an eavesdropper does not gain any information. For the BB84 protocol in 2 dimensions this error threshold is 11%, however it increases as higher dimensional states are used.

High-dimensional QKD protocols can give advantages in security and in the amount of information that can be sent per photon. The extension of these results has shown that high-dimensional states could be useful in applications with high background noise such as in daytime conditions, or high loss channels. The BB84 protocol can be extended to higher dimensions by identifying MUB, which has been shown to be possible in dimensions that are a power of prime numbers. The MUB for dimension d can then be given in terms of a basis $|j\rangle$ by

$$|\psi_m^{(\alpha)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (\omega_d^m)^{d-j} (\omega_d^{-(\alpha-1)})^{s_j} |j\rangle. \quad (3.3)$$

Here α is the index for the different bases, m denotes the states in each basis, $\omega_d = \exp(2\pi i/d)$ and $s_j = j + \dots + (d-1)$ [16].

3.2 Optical Turbulence

In the following 3 papers we study open water quantum channels. This is strongly related to the more developed field of free-space QKD, which entails sending photons through open air from Alice to Bob. The number one difficulty with these types of channels is atmospheric turbulence, or in our case, underwater turbulence. As photons propagate through the atmosphere or underwater, they come across slight variations in the index of refraction [17]. These variations can be due to pressure, temperature, or in the case of water different salinity. When considering spatial modes, these fluctuations can result in the optical beam wandering, being stretched in different directions, or in extreme cases the break up of the beam into small spots through a process called scintillation. The result is that measurements of the phase profile can give large errors which restricts the ability to perform QKD. One approach to correct these errors is the implementation of an adaptive optics system. These system make measurements of the phase distortions being introduced by the channel, and correct these distortions using a phase deformable mirror. The frequency of the distortions is very high in the atmospheric case, on the order of kilohertz. In the underwater environment the frequency is significantly lower, usually being visible to the eye. This open the possibility to study adaptive optics technologies in underwater channels before moving to the more difficult problem of the atmosphere.

The turbulence we observed in the underwater channel is studied in detail in all of the papers in this section. In the first paper we use single photon pairs generated through spontaneous parametric down conversion to establish a quantum channel across 3 meters of water in an outdoor swimming pool. The OAM space of $\ell = \{-1, 0, 1\}$ is used to achieve the first high-dimensional underwater quantum channel. As the OAM modes have a spatial dependence, turbulence can have particularly destructive effects on the beams profile. In highly turbulence regimes a phenomena called singularity splitting can be observed. This occurs when OAM states of $|\ell| > 1$ break up into multiple $\ell = \pm 1$ beams, giving rise to multiple intensity singularities. This is observed in the first paper, and the movement of the singularities is tracked over time. The second paper reports the achievable error rates of a polarization protocol across a 5 meter channel in the Ottawa river. Here the turbulence is again studied with OAM states ranging from $\ell = 1 - 9$, as well as the superposition petal modes. Distortions in the intensity profile is shown changing over time. A Shack-Hartmann wavefront sensor is also used to measure the phase distortions on a Gaussian beam. It should be noted that due to the massive scattering losses in the Ottawa river channel,

the optical beam is practically not very directional since much of the optical power is scattered out of the propagation path. Thus in such a heavy scattering environment, we might expect the attenuation to be similar to that seen by radio waves which have a very large absorption coefficient in water. In the third paper, an underwater channel is established for polarization states and structured vector vortex modes which combine the polarization and spatial degree of freedom. Here we reach a channel length of 30 meters.



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,*}

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

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

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

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

⁵Institute 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.

© 2018 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

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

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

2. Experimental results

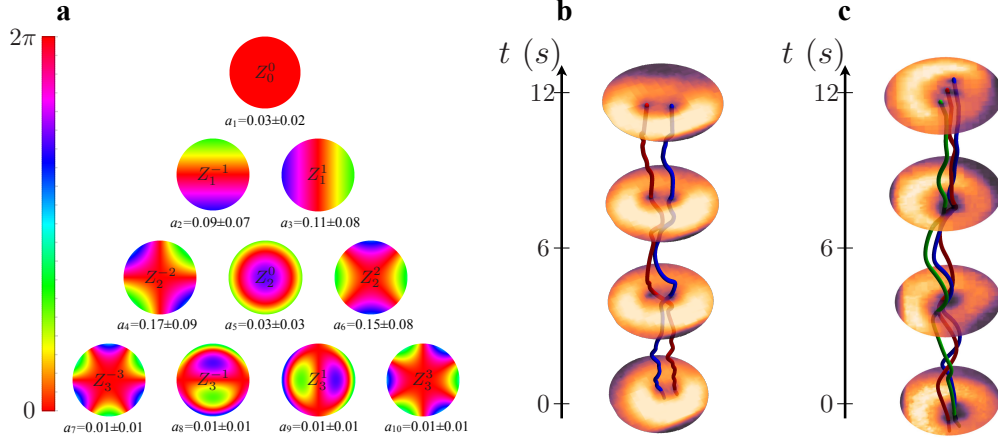


Fig. 1. Experimental characterization of underwater turbulence. (a) Calculated coefficients for the lowest ten Zernike polynomials from intensity images of a Gaussian beam after propagation through 3 m of water to characterize the turbulence in one particular set of conditions at the time of measurement. 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 quantum 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

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.

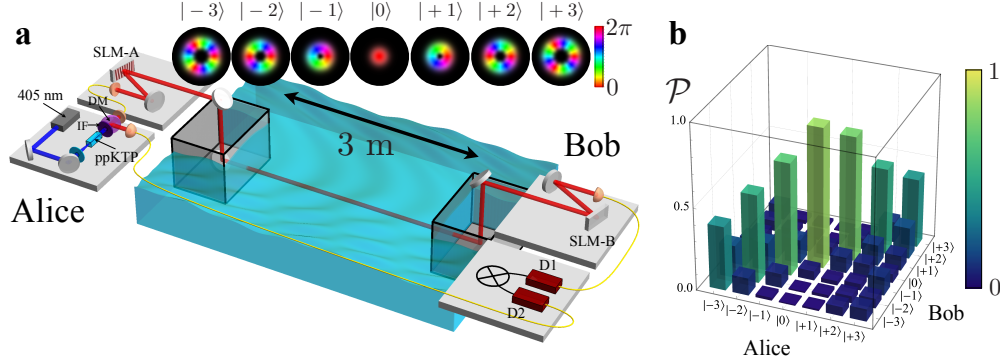


Fig. 2. Experimental setup and state cross-talk measurements. (a) Photon pairs (signal $\lambda_s = 710 \text{ nm}$, idler $\lambda_i = 943 \text{ nm}$) are generated via spontaneous parametric downconversion pumped from a periodically poled KTP (ppKTP) crystal by a 405 nm diode laser. A long pass filter (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 patterns (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],

$$\Phi(r, \varphi) = \sum_j a_j Z_j(r, \varphi), \quad (1)$$

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, $n = 1$ ($j = 2, 3$),

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 ($\lambda_s = 710$ nm) and idler ($\lambda_i = 940$ nm) photons are generated by spontaneous parametric downconversion, 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 received 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

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.

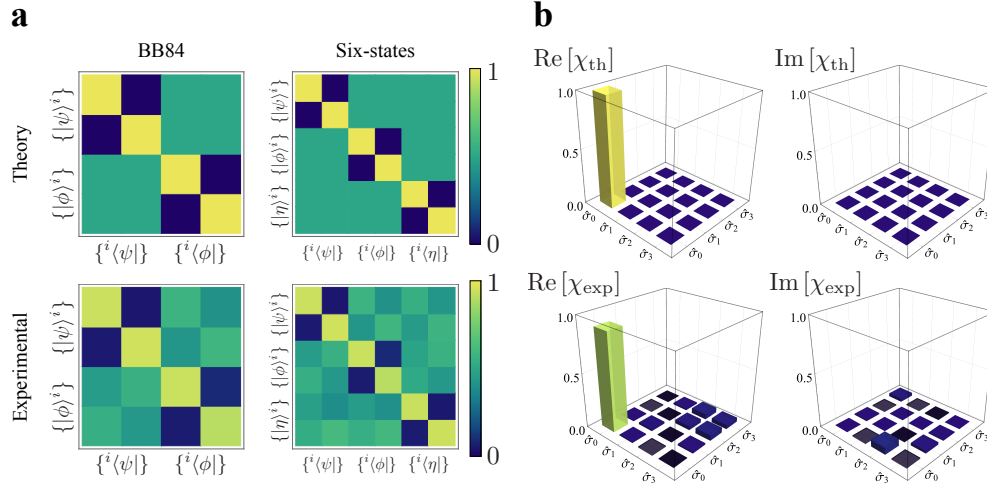


Fig. 3. Probability-of-detection matrices for $d=2$ BB84 and Six-states protocols, and the channel process matrix. (a) Theoretical and experimentally measured probability-of-detection matrices for BB84 (left column) and Six-states (right column) protocols in $d = 2$. We measured QBERs of $Q = 6.57\%$ 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 $|\phi\rangle^i \in \{|+\rangle, |-\rangle\}$, 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 $Q_{\text{threshold}}^{2D} = 11\%$ 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.

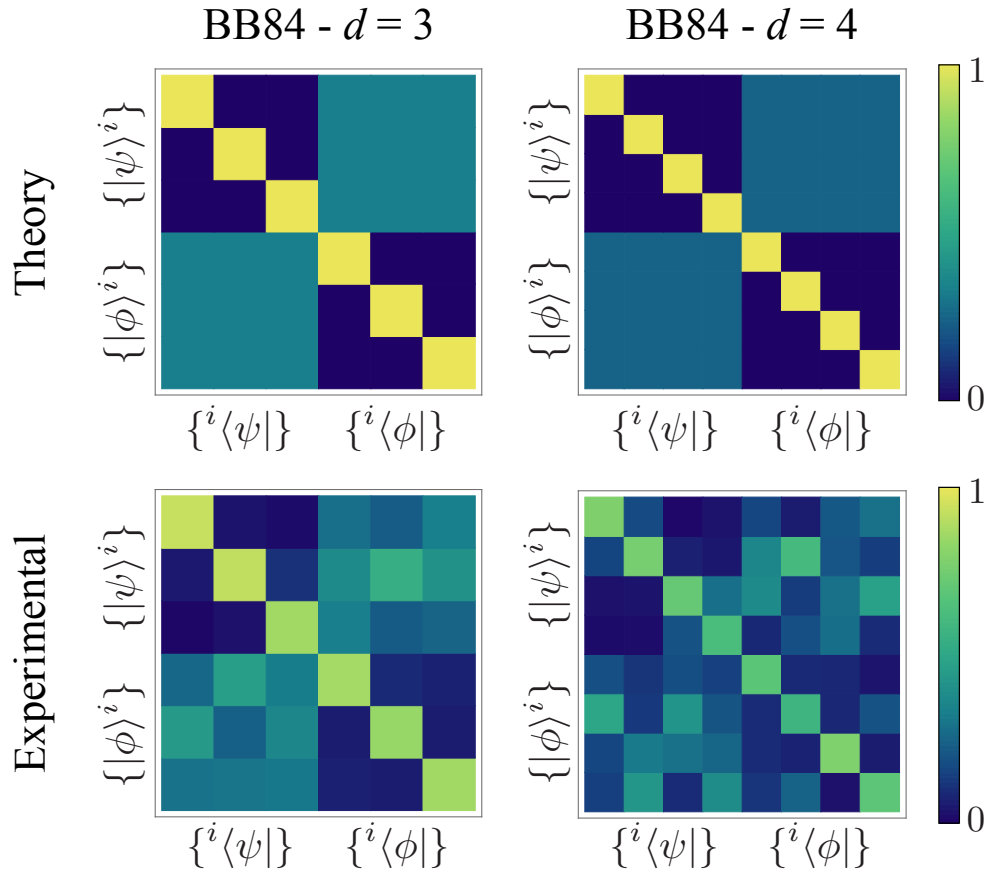


Fig. 4. High-dimensional probability-of-detection matrices. Theoretical (top row) and experimentally measured (bottom row) probability-of-detection matrices for BB84 protocols in $d = 3$ and $d = 4$. We measured QBER of $Q^{3D} = 11.73\%$ and $Q^{4D} = 29.77\%$, respectively. The QBER in $d = 3$ is below 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 $Q_{\text{threshold}}^{4D} = 18.9\%$.

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 $\mathcal{F} = \text{Tr}[\chi_{\text{exp}} \cdot \chi_{\text{th}}] / \text{Tr}[\chi_{\text{th}} \cdot \chi_{\text{th}}]$.

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, $|\psi\rangle^i \in \{|i\rangle; i = 1, 2, \dots, d\}$, 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 $Q^{3D} = 11.73\%$ and $Q^{4D} = 29.77\%$ were measured for the case of $d = 3$ and $d = 4$, respectively. For the 3-dimensional BB84 ($Q_{\text{threshold}}^{3D} = 15.95\%$), a secret key rate of $R^{3D} = 0.307$ 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. $Q_{\text{threshold}}^{4D} = 18.93\%$, meaning no secret key can be 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.

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

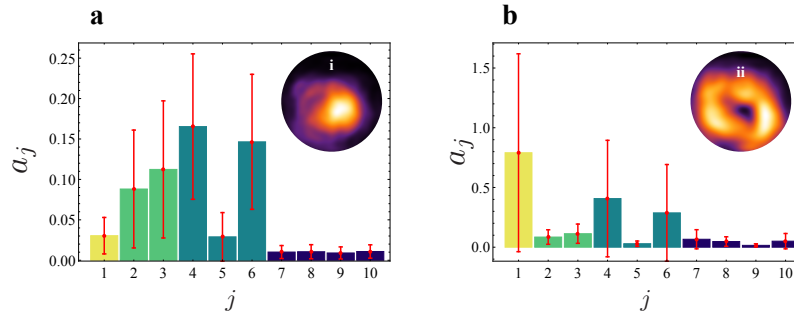


Fig. 6. Characterization of underwater turbulence. (a) Experimentally obtained coefficients for an input gaussian ($\ell = 0$) mode. Inset i, shows an example of a distorted gaussian beam profile at the output of the channel. The Zernike decomposition was carried over a disk with a radius of 2.1 mm,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

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

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

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

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

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

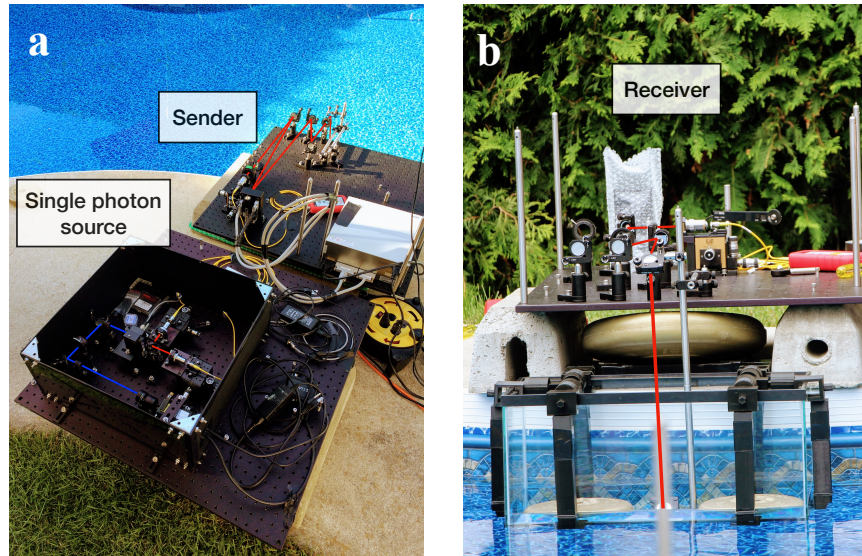


Fig. 7. Sender and receiver setup of the outdoor underwater link. (a) Close-up of the single photon source and the sender's setup. The blue line represents the pump beam and the red lines represent the signal and idler beams. (b) Close up of the receiver's aquarium, periscope and setup.

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).

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 Akademii 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).



Characterization of an underwater channel for quantum communications in the Ottawa River

FELIX HUFNAGEL,¹ ALICIA SIT,^{1,*} FLORENCE GRENA PIN,¹
FRÉDÉRIC BOUCHARD,¹ KHABAT HESHAMI,^{1,2} DUNCAN ENGLAND,²
YINGWEN ZHANG,¹ BENJAMIN J. SUSSMAN,^{1,2} ROBERT W.
BOYD,^{1,3}  GERD LEUCHS,^{1,3}  AND EBRAHIM KARIMI^{1,2,3} 

¹Department of Physics, University of Ottawa, 25 Templeton, Ottawa, Ontario, K1N 6N5, Canada

²National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada

³Max Planck Institute for the Science of Light, Staudtstr. 2, D-91058 Erlangen, Germany

Abstract: We examine the propagation of optical beams possessing different polarization states and spatial modes through the Ottawa River in Canada. A Shack-Hartmann wavefront sensor is used to record the distorted beam's wavefront. The turbulence in the underwater channel is analysed, and associated Zernike coefficients are obtained in real-time. Finally, we explore the feasibility of transmitting polarization states as well as spatial modes through the underwater channel for applications in quantum cryptography.

© 2019 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

1. Introduction

There are several different methods employed today for communicating underwater. The most widely used method is acoustic, capable of transmitting information over many kilometres [1]; however, the transmission rate is on the order of kilobits per second, limited by the speed of sound in water as well as the modulation rate of acoustic signals [2]. A second method is to use radio-frequency (RF) signals, which can be easily incorporated into current communication networks. This technique is limited to communication distances on the order of several meters due to high absorption in water at radio frequencies. Both the acoustic and RF implementations suffer from the necessity of bulky and expensive equipment for both transmitting and receiving signals. Over the last decade, using the optical domain for underwater communication has gained increasing interest [3,4]. With an optimal transmission window between blue and green (400-550 nm) wavelengths, a propagation distance between 50-200 m in clear water can be reached [5]. Higher data rates should additionally be achievable - up to gigabits per second depending on the scheme - allowing for larger data transfers and real-time communication. In [6], a data rate of 20 Mbps, at a distance of 200 m, has been experimentally achieved.

In a realistic aquatic environment, there are several other factors beyond absorption which can limit the distance and quality of a marine optical communication link, i.e. scattering and turbulence. Scattering in water is dependent on the density and the size of particles in the channel and will contribute significantly to attenuation and therefore to the maximum achievable distance. Scattering is separated into two types: Mie scattering for particles on the order of the wavelength of the light, and Rayleigh scattering for particles much smaller than the wavelength [7]. Especially in water where there are relatively large plankton and mineral particles floating in the water, Mie scattering will have to be considered, along with Rayleigh scattering, due to the water molecules [8]. Another limiting factor when it comes to an actual implementation of an optical link is turbulence [9,10]. A spatially varying index of refraction from temperature and salinity differences through the optical link can result in beam wander as well as higher order distortion effects on the propagating beam. This can contribute both to loss and errors in the transmitted

signal. In optical communication, security—affected by factors such as errors in the channel—is an important feature for successful information transfer. Typically, a line-of-sight approach is implemented, making eavesdropping much more difficult, as opposed to the broadcasting method for acoustic and RF communication where the signal is sent in all directions. By considering quantum cryptographic schemes, the security can be further enhanced [11]; for instance, quantum key distribution (QKD) allows authorized partners to communicate with unconditional security [12–14].

There are several different optical degrees of freedom which can be used to encode information in these QKD protocols. A popular option for direct line-of-sight channels is the polarization of photons, with successful experiments in free-space [15,16]. One limitation with polarization, however, is its inherently limited 2-dimensional Hilbert space, allowing for the maximum transmission of one bit per photon. The orbital angular momentum (OAM) degree of freedom of light, on the other hand, provides the potential of an unbounded state space, and thus unbounded encryption alphabet. Light beams carrying OAM possess a helical wavefront with ℓ intertwined helices, i.e. $\exp(i\ell\phi)$ where ℓ is an integer number and ϕ is the transverse azimuthal angle in polar coordinates [17]. These beams possess a doughnut-shaped intensity profile due to the presence of a phase singularity at their centre (ϕ is undefined at the origin in cylindrical polar coordinates). The unbounded state space of these spatial modes allow us to implement high-dimensional quantum communication channels [18–21], but they do come with unique challenges. One key challenge that has been observed with free-space communication is that turbulence in the channel can introduce errors in the transmitted information [22]. The measurement of OAM states is heavily dependent on the position of the incoming beam and thus these states are much more prone to errors from turbulence than polarization states which must just maintain their orientation.

Underwater quantum communications have been numerically investigated [23] and experimentally demonstrated in laboratory conditions using polarization [24,25], in outdoor conditions using the OAM degree of freedom [26], and over a 55 m water channel using polarization [27] and spatial modes [28]. These experimental investigations have lead to several numerical investigations of QKD in underwater channels [29–31]. In this Letter, we investigate the propagation of light through the Ottawa River in Canada's capital. In particular, we analyze the underwater turbulence by looking at the distorted wavefront and associated Zernike coefficients both obtained from a Shack-Hartmann wavefront sensor. Furthermore, we explore the transmission of polarization states of light and spatial modes of light through the underwater channel for quantum cryptography applications.

2. Experiment

The experiments presented here were conducted through the Ottawa River (latitude = 45.541048, longitude = -76.565719) during late August 2018. The water temperature was on average 20° C for the duration of the experiment. However, the ambient temperature varied significantly from the middle of the day to the middle of the night. This contributed to turbulent conditions with water at the surface being heated or cooled more than the water below. Of course since it is a river, there were already naturally varying currents, which moved the water through the beams propagation path resulting in a changing index of refraction.

The results discussed in this work were taken using a 532 nm laser diode. The sender and receiver units were mounted on breadboards along the shoreline of the river. As shown in Fig. 1, the sender consisted of the laser, Spatial Light Modulator (SLM), and a half-wave plate. The wave-plates were used to prepare four linear polarization states, i.e. horizontal (H), vertical (V), anti-diagonal (A), and diagonal (D). The SLM is used for preparing the OAM states. This is done by displaying a phase hologram on the SLM and selecting the first diffracted mode from the hologram. The laser beam is then sent from Alice's breadboard on shore to the first periscope

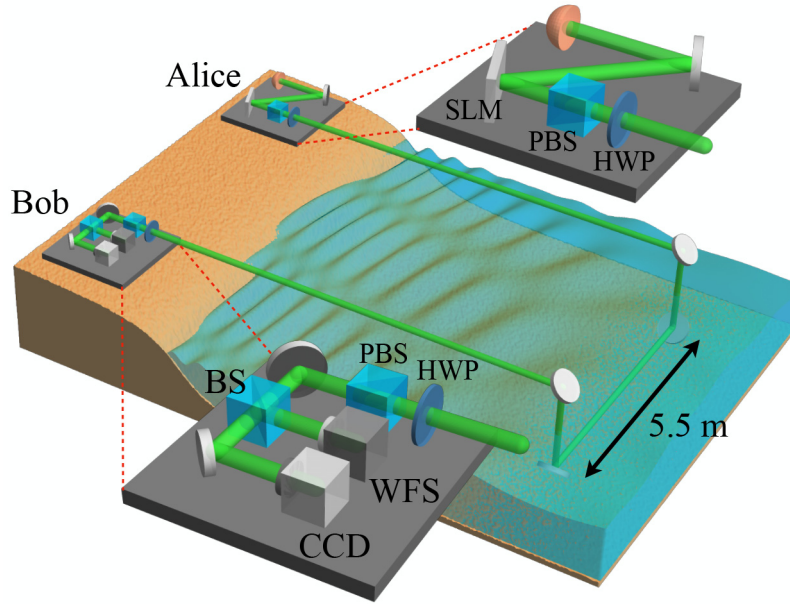


Fig. 1. Experimental setup. Two breadboards positioned on the beach are used for the sender and receiver, Alice and Bob respectively. A CW laser at $\lambda = 532$ nm is sent to an SLM, polarizing beamsplitter (PBS), and half-wave plate (HWP) for state preparation at Alice's side of the link. This is then sent to a first periscope (composed of two mirrors) which brings the beam underwater, where it propagates to the second periscope 5.5 m away. The receiver has a PBS and HWP for polarization measurements, and a beam splitter allows a CCD camera and Shack-Hartmann wavefront sensor (WFS) to take images.

system that brings the beam underwater. The beam then propagates underwater, parallel to the beach, to the second periscope system where it is brought out of the water and sent to the receiver unit, see Fig. 1. In order to eliminate air-water perturbations resulting from surface waves as the beam enters the water, a glass tube, closed at one end, is inserted within the periscope system to create an air-glass-water interface. At the receiver side, we captured the intensity of the beam for the polarization states of H, V, A, and D using a CCD camera. The camera only allows us to gain intensity information about the beam but not the phase. However in order to measure the phase of the beam, we place a Shack-Hartmann wavefront sensor (WFS) at the receiver. This device is made up of a micro-lens array placed in front of a CCD camera. The resulting effect is that the phase at each lens can be determined by the focus point of that lens on the CCD array. This allows one to determine the incidence angle of the given region of the beam and thus the phase relative to the rest of the beam. The accuracy of the wavefront sensor is limited by the number of micro-lenses in the array; the WFS that we use is the Thorlabs WFS20-7AR and has a 23×23 lenslet array with lenslet pitch of $150 \mu\text{m}$ and focal length of 5.2 mm.

Losses in the link due to scattering played a much larger roll in establishing a quantum channel than was expected. There has been analysis performed looking at the feasibility of quantum communication taking into account many factors including scattering [23]. These studies, however, consider at worst the Jerlov Type III ocean water with scattering loss of 1.3 dB/m. In our river channel, the total attenuation was significantly larger than these previously studied values. The channel losses from scattering varied over the course of many hours due to different magnitudes of waves in the river which brought sediment from the river bed into the beam path. During the polarization experiment, the total absorption was measured to be 5.4 dB/m,

significantly higher than even the worst water type considered in the previous calculations. This makes the absorption loss of 0.13 dB/m for pure water negligible for practical considerations of achievable distance [32]. Due to the large amount of scattering in the river, our experimental tests were limited to ~ 5 m. This high level of scattering was primarily due to large particles in the water ($d \gg \lambda$). The Mie scattering model is used when the particles' diameter is on the same order as the wavelength of the light. This is typically for particles such as pollen, dust, and water droplets which are approximately the same size as the wavelength of the light. In our channel, since we were near the shore of the river, there was even larger visible plant matter and dirt floating in the water. This resulted in a large amount of light being absorbed or back reflected as opposed to being primarily forward scattered as in the regular Mie scattering regime.

$ H\rangle$	0.93	0.06	0.40	0.59
$ V\rangle$	0.02	0.97	0.45	0.54
$ A\rangle$	0.49	0.50	0.97	0.03
$ D\rangle$	0.53	0.47	0.04	0.96
	$ H\rangle$	$ V\rangle$	$ A\rangle$	$ D\rangle$

Fig. 2. Polarization probability-of-detection matrix. The sender generates the linear polarization states of $\{|H\rangle, |V\rangle\}$ or $\{|A\rangle, |D\rangle\}$, chosen at random. The receiver randomly picks up one of the bases $\{|H\rangle, |V\rangle\}$ or $\{|A\rangle, |D\rangle\}$, and records the projection probability, whose numerical values are shown.

3. Results and discussion

The first goal of this project was to establish that polarization QKD could be achieved in this highly turbulent and highly scattering channel. For the original BB84 protocol [12], polarization states are chosen from a set of mutually unbiased bases (MUBs). We chose the bases to be $|\psi_i\rangle = \{|H\rangle, |V\rangle\}$ and $|\phi_i\rangle = \{|A\rangle, |D\rangle\}$.

The defining property of MUBs is that a measurement in the correct basis reveals with certainty the state that the photon was in, while measurement in the wrong basis gives no information about the state of the photon, i.e. $|\langle\psi_i|\phi_k\rangle|^2 = 1/2$. Herein lies the security of QKD: an eavesdropper making a measurement in the wrong basis will be successful only 50% of the time and will introduce errors when they are unsuccessful. The experimental probability-of-detection matrix for the polarization states is shown in Fig. 2. The discrepancy between the error rates of the $|H\rangle$ and $|V\rangle$ polarization are primarily due to imperfect polarization optics. This is not expected to be a property of the underwater channel. The resultant error rate is 4.01 %, which is below the threshold of 11.0 % necessary to perform QKD with a 2-dimensional BB84 protocol. The results here are obtained using classical light from a CW laser. However, on the assumption that the

background noise is small compared with the signal and thus the errors are introduced only by the channel, single photons will give the same error rate and we can calculate a bit rate of 0.52 bits per sifted photon.

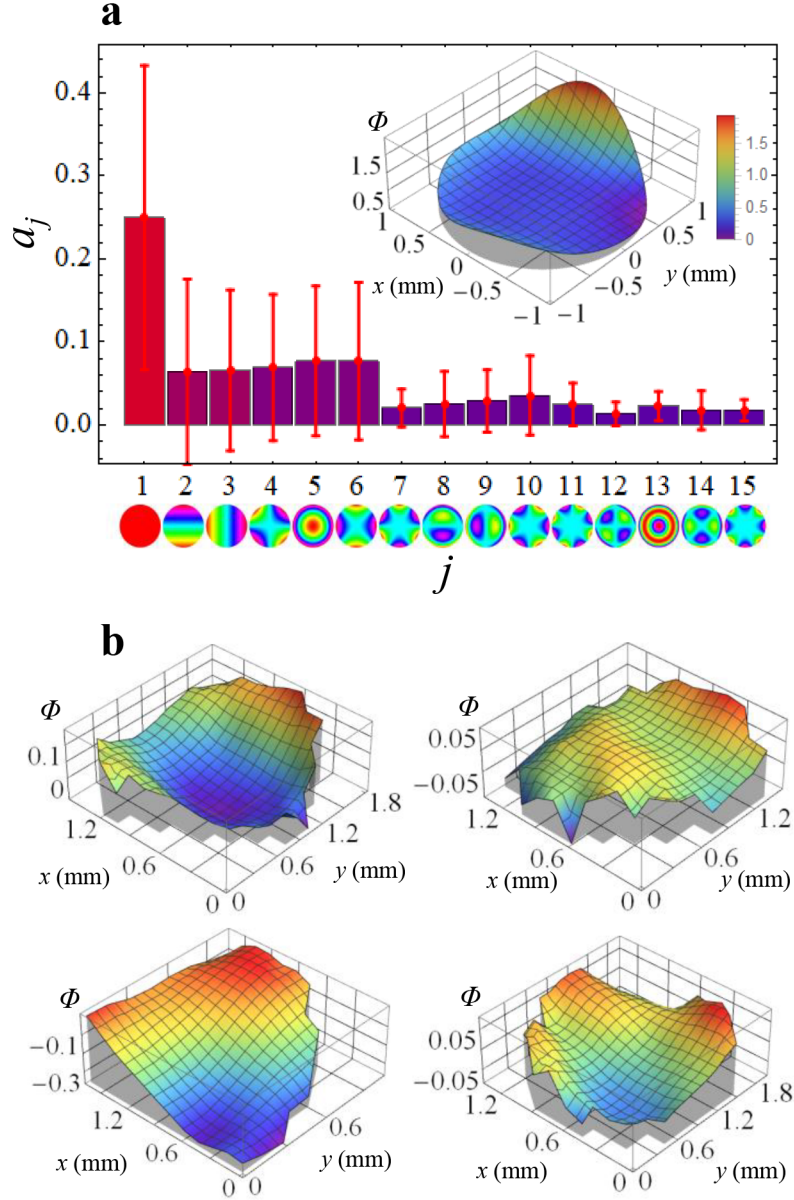


Fig. 3. Wavefront measurements. A Gaussian beam is sent through the underwater channel to measure the wavefront. Plot **a** shows the average value for the magnitude of the Zernike coefficients taken from the wavefront sensor. The coefficients are separated by their radial degree corresponding to the color bars. of The inset is a plot of the wavefront given by these values. The plots in **b** are wavefronts measured at different times of a gaussian beam through the 5 m underwater link. The wavefront measurements are taken using an array of $150\ \mu\text{m}$ diameter lenses.

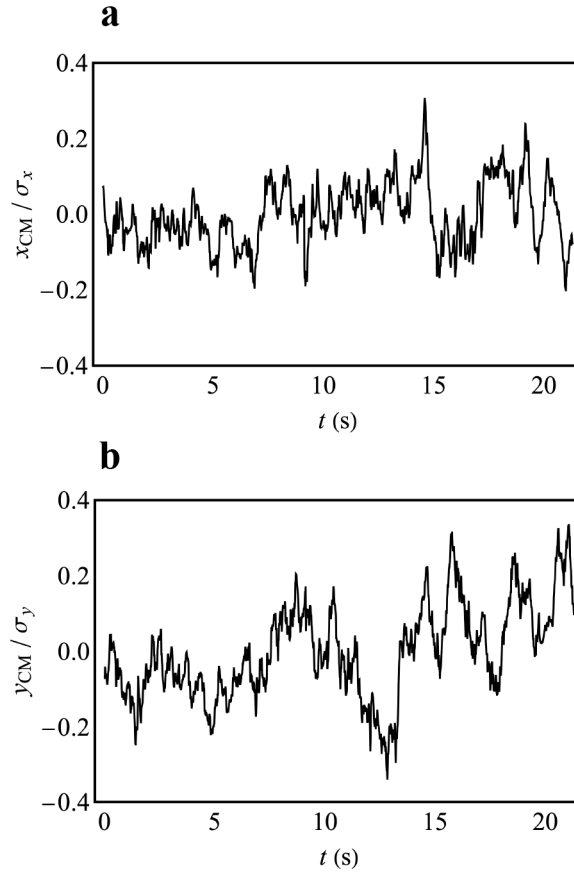


Fig. 4. Time dependence of tip-tilt aberrations. The intensity of a Gaussian beam was measured at the receiver using a CCD camera. The tip-tilt variations were then calculated by measuring the positional shift (x, y) of the Gaussian beam from the center. The x and y center of mass, relative to their respective beam waists σ_x and σ_y , are plotted as a function of time in **a** and **b**, respectively.

Although we achieved an error rate below the threshold, there are some residual errors in the system. In free space experiments, the errors are often attributed to optical turbulence, which comes from differences in the index of refraction along the path of propagation as described by the Kolmogorov theory of turbulence [33]. Tip-tilt effects can result in beam wandering, while higher order effects can be present in high turbulence situations, resulting in distortion of the beam's profile [26,34]. The aberrations in the beam are often visible in the intensity of the beam; however, more precise information lies in the phase of the received beam. In this experiment, we prepared a Gaussian beam at the sender, and measure the wavefront at the receiver. The Gaussian beam is the simplest for measuring the turbulence introduced by the channel, though OAM modes or any modes whose phase profile is known can be used. The Gaussian beam should have a spherical phase due to divergence; thus, any variations from this can be attributed to turbulence introduced by the water. From the wavefront measurements, the turbulence can be expanded in terms of the Zernike coefficients, i.e. $\Phi(r, \phi) = \sum_j a_j Z_j(r, \phi)$. Here, r and ϕ are the radial and azimuthal polar coordinates, respectively; a_j are the Zernike expansion coefficients; $Z_j(r, \phi) = Z_n^m(r, \phi)$ are the Zernike polynomials depicted underneath the x-axis of Fig. 3a; $j = 1 + (n(n+2) + m)/2$ is the Noll index; and n and m are the radial and azimuthal

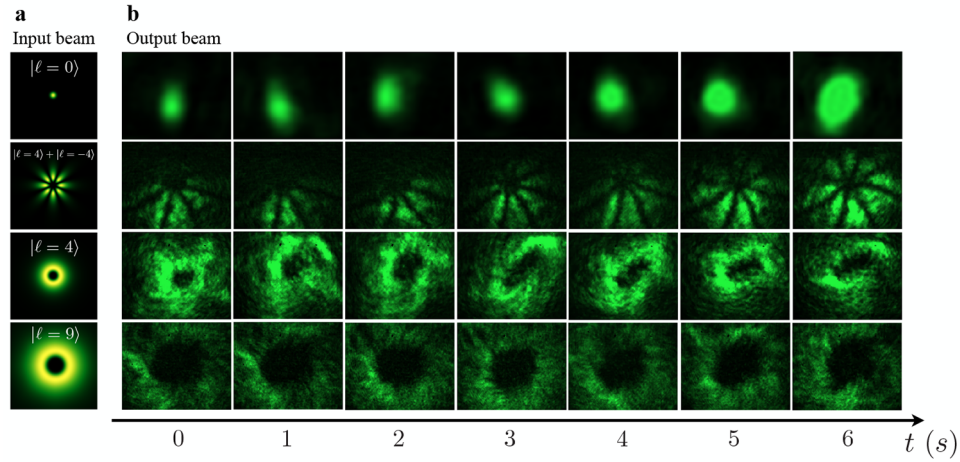


Fig. 5. Observed turbulence effects on spatial modes. The images in the first, second, third and fourth rows correspond to $LG_{0,0}$, $(LG_{4,0} + LG_{-4,0})/\sqrt{2}$, $LG_{4,0}$, and $LG_{9,0}$, respectively. The original beam profile is shown in **a**, and the images after propagation through the underwater channel are shown in **b**. The images are taken over a 6 second interval. The exposure time for the last three rows are set to 108 ms, while it is set to 20 ms for the Gaussian beam. The inhomogeneity in the beams' intensity profiles are due primarily to Mie scattering from floating objects in the underwater channel. Lower and higher-order aberrations are manifested in the beam wandering ($LG_{0,0}$) and singularity splitting.

indices, respectively. The values for the first 15 Zernike coefficients averaged from 30 wavefront measurements $\bar{a}_j$ are shown in Fig. 3-a along with the reconstructed wavefront Φ from these values. The wavefront measurements are taken with an average exposure time of 60 milliseconds and are separated by 10 seconds. The time separation of the wavefront measurements is large with respect to the fluctuation of the Zernike coefficients. Thus, each wavefront is essentially an independent measurement of the turbulence in the channel. In Fig. 3-b, a sample of four of these individual wavefront measurements is shown. These wavefront measurements show that the beam experienced significant variation upon propagation through the turbulent channel. It is also interesting to consider the time dependence of the turbulence in the channel. This is necessary if one plans to implement an adaptive optics system to correct for wavefront aberrations in the optical channel. The intensity profile of a Gaussian beam was recorded to analyze the tip tilt fluctuations as a function of time. This is shown in Fig. 4. The frequency of the fluctuations in the underwater channel is lower than one typically observes in free space channels. This could make underwater channels an interesting test bed for adaptive optics systems.

As stated before, the turbulence is also visible in the intensity profile of the beam at the receiver. It is easy to see tip-tilt aberrations from a Gaussian beam as it visibly drifts across the x and y axis of a camera. The higher order aberrations are often less visible. These aberrations do, however, show themselves very clearly in their effect on higher-order spatial modes. Specifically, the oblique and vertical astigmatism ($Z_2^{\pm 2}(r, \phi)$) stretch OAM modes, giving them an elliptical shape, as well as splitting the singularity into lower topological charges. Intensity profiles of OAM and superposition modes are shown in Fig. 5 with consecutive images taken over a time of 6 seconds. The turbulence from the channel is very apparent in the wandering of the $LG_{0,0}$ mode, and the higher-order aberrations are shown most clearly in the stretching of the $LG_{0,4}$ mode. In addition to turbulence, all of the modes experience significant intensity fluctuations from changing levels of scattering as well as from objects floating into the beam's path. The latter is displayed clearly in the images of the petal beam, i.e. $(LG_{0,4} + LG_{0,-4})/\sqrt{2}$. As the

correct measurement of spatial modes requires that the position and phase of the beam remain intact, it is clear that, even over a short propagation through water, active wavefront correction or the implementation of adaptive optics would be required to compensate for the aberrations.

4. Conclusion

We have shown that significant challenges present themselves in underwater communication. Despite low absorption from the water at blue-green wavelengths, the scattering from floating particles in the water can severely limit the achievable communication distance. Though scattering will impact the distance, we see that polarization states do maintain their integrity even after propagation through a very highly scattering channel. The second key challenge in an underwater optical channel is turbulence. This has the largest impact on communications using spatial modes. Through the 5.5 m channel, the OAM modes experience aberrations which will result in errors in a communication protocol. The magnitude of these errors will need to be investigated in future work. Adaptive optics techniques will also need to be investigated to compensate for these errors and allow for communication using spatial modes.

Funding

Canada Research Chairs; Canada Foundation for Innovation; Canada First Research Excellence Fund; Natural Sciences and Engineering Research Council of Canada.

Acknowledgments

This work was supported by Canada Research Chairs (CRC); Canada Foundation for Innovation (CFI); Canada First Research Excellence Fund (CFREF); Natural Sciences and Engineering Research Council of Canada (NSERC). We thank Denis Guay and the NRC for their help in designing and building the periscopes.

References

1. M. Stojanovic, *Acoustic (underwater) communications* Wiley Encyclopedia of Telecommunications, 2003.
2. J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, Research challenges and applications for underwater sensor networking, in *IEEE Wireless Communications and Networking Conference WCNC, 2006*, 1, 228–235, (2006).
3. T. Wiener and S. Karp, “The role of blue/green laser systems in strategic submarine communications,” *IEEE Trans. Commun.* **28**(9), 1602–1607 (1980).
4. J. C. Brock and S. J. Purkis, “The emerging role of lidar remote sensing in coastal research and resource management,” *J. Coastal Res.* **10053**, 1–5 (2009).
5. Z. Zeng, S. Fu, H. Zhang, Y. Dong, and J. Cheng, “A survey of underwater optical wireless communications,” *IEEE Commun. Surv. Tutorials* **19**(1), 204–238 (2017).
6. S. Fasham and S. Dunn, “Developments in subsea wireless communications,” in *IEEE Underwater Technology (UT)* (IEEE, 2015), pp. 1–5.
7. H. C. Hulst and H. C. van de Hulst, *Light scattering by small particles* (Courier Corporation, 1981).
8. C. D. Mobley, *Light and water: radiative transfer in natural waters* (Academic, 1994).
9. G. Nootz, E. Jarosz, F. R. Dalgleish, and W. Hou, “Quantification of optical turbulence in the ocean and its effects on beam propagation,” *Appl. Opt.* **55**(31), 8813–8820 (2016).
10. G. Nootz, S. Matt, A. Kanaev, K. P. Judd, and W. Hou, “Experimental and numerical study of underwater beam propagation in a Rayleigh–Bénard turbulence tank,” *Appl. Opt.* **56**(22), 6065–6072 (2017).
11. J. Uhlmann, M. Lanzagorta, and S. E. Venegas-Andraca, “Quantum communications in the maritime environment,” in *OCEANS 2015 - MTS/IEEE Washington* (IEEE, 2015) 1–10.
12. C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Int. Conf. on Comput. Syst. Signal Process.* (IEEE, 1984), pp. 175–179.
13. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.* **74**(1), 145–195 (2002).
14. 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**(3), 1301–1350 (2009).
15. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” *Phys. Rev. Lett.* **98**(1), 010504 (2007).

16. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature* **549**(7670), 43–47 (2017).
17. 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**(11), 8185–8189 (1992).
18. 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**(3), 032305 (2013).
19. 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**(3), 033033 (2015).
20. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Gunthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica* **4**(9), 1006–1010 (2017).
21. F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," *Quantum* **2**, 111 (2018).
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**(11), 113028 (2014).
23. P. Shi, S.-C. Zhao, Y.-J. Gu, and W.-D. Li, "Channel analysis for single photon underwater free space quantum key distribution," *J. Opt. Soc. Am. A* **32**(3), 349–356 (2015).
24. L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin, "Towards quantum communications in free-space seawater," *Opt. Express* **25**(17), 19795–19806 (2017).
25. S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over water channel," *Appl. Opt.* **58**(14), 3902–3907 (2019).
26. F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Opt. Express* **26**(17), 22563–22573 (2018).
27. C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, H. Tang, and X.-M. Jin, "Transmission of photonic polarization states through 55-meter water: Towards air-to-sea quantum communication," arXiv preprint arXiv:1811.11176 (2018).
28. Y. Chen, W.-G. Shen, Z.-M. Li, C.-Q. Hu, Z.-Q. Yan, Z.-Q. Jiao, J. Gao, M.-M. Cao, K. Sun, and X.-M. Jin, "Underwater transmission of high-dimensional twisted photons over 55 meters," arXiv preprint arXiv:1902.01392 (2019).
29. S. Tarantino, D. Cozzolino, K. Rottwitt, and D. Bacco, Feasibility of quantum communications in aquatic scenario, in *2018 IEEE Photonics Conference (IPC)*, (IEEE, 2018), pp. 1–2.
30. B. Guo, G. Yuan, J. Yu, H. Liu, W. Xu, and R. Hou, "Simulations and measurements of polarization states changing in underwater laser transmission," *Proc. SPIE* **10850**, 108500U (2018).
31. J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Opt. Express* **27**(3), 3055–3064 (2019).
32. R. C. Smith and K. S. Baker, "Optical properties of the clearest natural waters (200–800 nm)," *Appl. Opt.* **20**(2), 177–184 (1981).
33. A. N. Kolmogorov, "The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers," *Akademiia Nauk SSSR Doklady* **30**, 299–303 (1941).
34. 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. Rep.* **6**(1), 33306 (2016).

Underwater quantum communication over a 30-meter flume tank

Felix Hufnagel,¹ Alicia Sit,¹ Frédéric Bouchard,^{1,2,*} Yingwen Zhang,² Duncan England,² Khabat Heshami,^{1,2} Benjamin J. Sussman,^{1,2} and Ebrahim Karimi^{1,2}

¹*Department of physics, University of Ottawa, Advanced Research Complex,
25 Templeton Street, K1N 6N5, Ottawa, ON, Canada*

²*National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada*

Underwater quantum communication has recently been explored using polarization and orbital angular momentum. Here, we show that spatially structured modes, e.g., a coherent superposition of beams carrying both polarization and orbital angular momentum, can also be used for underwater quantum cryptography. We also use the polarization degree of freedom for quantum communication in an underwater channel having various lengths, up to 30 meters. The underwater channel proves to be a difficult environment for establishing quantum communication as underwater optical turbulence results in significant beam wandering and distortions. However, the errors associated to the turbulence do not result in error rates above the threshold for establishing a positive key in a quantum communication link with both the polarization and spatially structured photons. The impact of the underwater channel on the spatially structured modes is also investigated at different distances using polarization tomography.

I. INTRODUCTION

The development of quantum computers and their ability to factor large prime numbers through Shor's algorithm, poses a threat to modern communication security [1]. Since the realization of the first protocol by Bennett and Brassard in 1984 (BB84), quantum key distribution (QKD) has become the most actively researched solution for secure communication in a post-quantum world [2]. At present, quantum communication is a research field reaching maturity with commercial devices available for optical fibre QKD, experimental demonstrations of satellite-to-ground channels [3, 4], and new protocols being developed to improve key rates and security [5]. There are two primary quantum communication instances currently investigated: quantum communication channels and quantum communication protocols [6–8]. Channels must be experimentally investigated to demonstrate the transmission fidelity of quantum states, while new protocols bring advantages in terms of security, error tolerance, and key rates.

Many different protocols have been developed, some of which take advantage of high-dimensional quantum states [9]. Although quantum information is typically encoded using one of the different photonic degrees of freedom (such as polarization, time-bin, position and transverse momentum), multiple degrees of freedom can be used, forming structured states of light. The coherent combination of polarization and orbital angular momentum (OAM) is one example of structured light, with numerous applications in microscopy, optical tweezers, classical communication, and quantum information [10]. QKD protocols performed across free-space channels have been implemented, for example, with polarization [11], time-bin [12], OAM [13],

and structured photons [14, 15]. Likewise, there have been similar demonstrations in fibre channels [16–19]. Though two-dimensional qubit protocols are the most commonly implemented, there are advantages to high-dimensional communication in both noise tolerance [20] and bit-rate [21] which motivates the study of structured states [22].

Recently, there have been several studies demonstrating quantum communication tasks in underwater environments [23–26], motivated by the goal of secure communication between submersibles, research vessels, and surface vehicles. The absorption of water at radio frequencies has resulted in acoustic technology being the dominant form of communication for the last 100 years. There exists a transparency window between 400 nm and 500 nm, giving the possibility of optical and quantum communication at these wavelengths. Theoretical works predict a maximum practical quantum channel length of 300 m at 418 nm in clear conditions [27]. Though this is a short distance as compared to the current fibre and free-space links, it is enough for communication between submersibles and surface vehicles. Thus far, the feasibility tests of QKD with polarization encoding has been performed through a 3-m tube of water [24], and through an indoor testing channel of 55 m [26]. However much like in air, uncontrolled underwater channels are prone to the effects of turbulence—caused by local changes in the refractive index of water from temperature variations—which displaces and distorts a transmitted beam of light. Recent studies have explored the effects of underwater turbulence on QKD protocols and spatial modes of light in uncontrolled [23] and natural [25] water channels. However, the security analysis of different protocols is not considered in these previous studies. The high loss nature of underwater channels makes the optimization of the protocol necessary to achieve maximum distances and key rates. Here, we investigate an underwater channel at various lengths up to 30 m. The turbulence impact on the channel is observed through polarization tomography of

* frederic.bouchard@nrc-cnrc.gc.ca

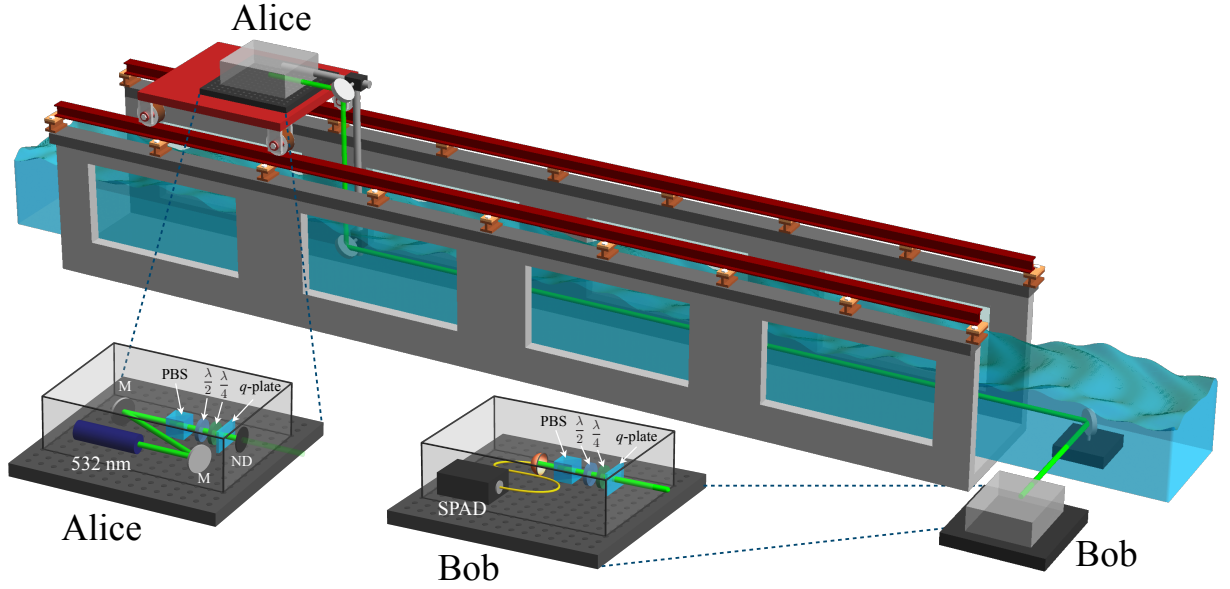


FIG. 1. **Experimental setup.** The underwater channel was created using a flume 1 m deep and wide, and 50 m long. The sender setup, Alice, was placed on a trolley which was able to run the length of the flume. Alice's setup consisted of a 532 nm diode laser as the source, and a $\lambda/2$ and $\lambda/4$ waveplate, as well as a $q = 1/2$ -plate for the case of the vector vortex modes experiment. The beam was sent from the sender, through a glass tube which entered the water thus avoiding the wavy air-water interface. The beam was directed, from a mirror placed in the tank, through a window on the side of the flume to Bob's setup. Bob's setup, which mirrors Alice's setup, consisted of a $q = 1/2$ -plate followed by a $\lambda/2$ and $\lambda/4$ waveplate and a polarizing beam splitter (PBS). Photons are then coupled to a single-mode optical fibre and detected by a single photon avalanche diode (SPAD). In order to perform polarization tomography, the reduced Stokes parameters were measured by means of a $\lambda/2$ and $\lambda/4$ waveplate, polarizing beam splitter (PBS) followed by a CCD camera.

the spatial modes, showing mode degradation upon propagation through the water. The BB84 protocol is tested using both polarization states and two-dimensional spatially structured modes. Key rate analysis is performed showing how optimization of the protocol's parameters is important in the high loss scenarios observed in underwater channels. Moreover the variable channel length gives us a real-world look into the scaling of such quantum protocols, and the impact on the key rates.

II. EXPERIMENT

The experimental setup consists of a sender (Alice) and receiver (Bob), as well as the flume tank which provides our underwater channel, see Fig. 1. The flume is 1-meter wide and 1-meter tall; its full length was 50 m. On the top of the flume was a track with a mounted trolley which can travel the length of the channel. Alice's setup was placed on the trolley such that the channel length could be adjusted from 1 m to the full 50 m. A periscope was hung from Alice's setup so that, with proper beam alignment, the trolley could be moved up and down the length of the flume while maintaining beam coupling to a single mode optical fibre at the receiver. The sender consisted of two configurations for changing between sending polarization states and sending the spatially structured

modes, e.g., vector vortex modes [28]. For sending polarization states, a 532 nm diode was sent to a polarizing beamsplitter (PBS), followed by a half-wave plate ($\lambda/2$) and a quarter-wave plate ($\lambda/4$) to allow any polarization state to be generated. Before being transmitted across the channel, the appropriate neutral density (ND) filters attenuated the beam to achieve a mean photon number of 0.1 photons per nanosecond. The vector vortex modes were generated by adding a q -plate with a topological charge of $q = 1/2$ after the polarization optics. At the receiver, the beam is initially collected by a 3-inch lens so that the whole beam is gathered even with slight beam wandering due to the underwater turbulence. The beam then passes through a $\lambda/2$ and $\lambda/4$ waveplate and then a PBS to project on a particular polarization state. The beam is then coupled to a single mode fibre connected to a single photon avalanche diode (SPAD) detector. To detect the vector vortex states, a q -plate with charge $q = 1/2$ is placed at the receiver before the polarization optics. In this way, the detection system mirrors the generation system. The setup is initially optimized with the trolley placed at 1 m from the receiver.

Linear polarization states are used to establish the polarization quantum communication channel. The two mutually unbiased bases (MUB) for encryption are $|\psi_i\rangle \in \{|H\rangle, |V\rangle\}$ and $|\phi_j\rangle \in \{|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |D\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$, re-

spectively. MUB possess the property that a projection made on the incorrect basis results in no information gained about the state of the photon, i.e. a probability of $1/2$ for each state $|\langle\psi_i|\phi_j\rangle|^2 = 1/2$. A full probability-of-detection matrix is determined by sending each of the four polarization states and subsequently performing projective measurements of the four states at the receiver setup. This probability-of-detection matrix gives us the quantum bit error rate (QBER) which is used to calculate the key rate that can be achieved with the underwater channel. The uniformly polarized photons, i.e. $|\psi_i\rangle$ and $|\phi_j\rangle$, should remain largely unaffected by the turbulence because water is not a birefringent medium. Thus, the introduced errors will be negligible for short distances. The length of the channel and level of turbulence will, however, introduce more losses as the photons are not able to be gathered at the receiver. This will have some effect on the measured error rate since the losses in the signal will give more weight to the dark counts and background noise as the distance increases.

TABLE I. **Quantum bit error rate and key rates for polarization BB84.** QBER and key rates per sifted photon for the polarization BB84 protocol are measured at different propagation distances. Note that in principle, the polarisation states can be modulated and detected at 100 MHz, and thus the actual key rate is *key rate per sifted photons $\times$ modulation rate $\times$ sifting efficiency*.

distance	0.5 m	10.5 m	20.5 m	30.5 m
QBER (%)	0.27	0.74	3.7	0.96
key rate	0.94	0.87	0.54	0.84

The QBER and key rates for the different distances are given in Table I. The results show the QBER increasing slightly as the channel length is increased. The primary source of these increased errors is the losses that result from the turbulence at the longer distances. The type of experiment we performed involves projecting on one of the polarization states and recording the number of counts during a set time period. The unpredictable nature of the turbulence in the channel results in some periods of time having larger losses due to beam wandering and spatial distortions. The beam wandering and spatial distortions, of course, increase with distance, but are effectively random and difficult to predict in our uncontrolled environment. This effect, which is random, results in the high error rate observed for the 20.5 m channel in comparison with the other channel lengths.

The structured photon states, here, vector vortex modes, are generated at the sender, and detected at the receiver by adding q -plates to the setup—details are given in the caption of Fig. 1. q -plates are patterned liquid crystal devices which introduce a polarization dependent geometric phase across the plate when it is illuminated with circularly polarized beams [29, 30]. The transformation of a perfectly tuned $q = 1/2$ -plate in the circular

polarization basis, left-circular $\mathbf{e}_L$ and right-circular $\mathbf{e}_R$ states, can be described as,

$$\begin{bmatrix} \mathbf{e}_L \\ \mathbf{e}_R \end{bmatrix} \xrightarrow{\text{QP}} \begin{bmatrix} \mathbf{e}_R e^{i\phi} \\ \mathbf{e}_L e^{-i\phi} \end{bmatrix}. \quad (1)$$

As we can see from the above equation, the $q = 1/2$ -plate will act on circular polarization states by converting left circularly polarized photons to right circularly polarized photons with OAM of $\ell = +1$. Similarly, incident photons with right circular polarization will be converted to left circular with OAM of the opposite sign, i.e. $\ell = -1$. The states used for our structured QKD protocol are created by sending linear polarization states, $\{|H\rangle, |V\rangle\}, \{|A\rangle, |D\rangle\}$, onto the $q = 1/2$ -plate. This results in a state that has a spatially dependent polarization in the form of radial, azimuthal, clockwise and counterclockwise sink topology, all possessing polarization topological charge of $+1$ [28]. This is opposed to the case when a circular polarization state is sent to the q -plate resulting in uniform conversion to the opposite circular polarization and the addition of an OAM of $\ell = \pm 1$. The protocol we implemented uses the structured modes as a 2-dimensional Hilbert space. The first MUB contained the radial and azimuthal states, i.e.,

$$|\Psi_i\rangle \in \left\{ \frac{(|L, -1\rangle + |R, +1\rangle)}{\sqrt{2}}, \frac{(|L, -1\rangle - |R, +1\rangle)}{\sqrt{2}} \right\}, \quad (2)$$

where $|\pi, \ell\rangle$ indicates the photons with polarisation and OAM states of $|\pi\rangle$ and $|\ell\rangle$, respectively. The states for the second MUB were the polarisation patterns in the form of clockwise and counterclockwise sinks (vortex) which were generated by sending the $|A\rangle$ and $|D\rangle$ polarization states onto the $q = 1/2$ -plate, i.e.,

$$|\Phi_i\rangle \in \left\{ \frac{(|L, -1\rangle + i|R, +1\rangle)}{\sqrt{2}}, \frac{(|L, -1\rangle - i|R, +1\rangle)}{\sqrt{2}} \right\}. \quad (3)$$

TABLE II. **Quantum bit error rate and key rates for a two-dimensional BB84 using vector vortex beam.** QBER and key rates per sifted photon for the vector vortex modes protocol are measured at different propagation distances. Note that in principle the mode generation and detection can be achieved by polarisation modulators at 100 MHz before (after) q -plates, and thus the actual key rate is *key rate per sifted photons $\times$ modulation rate $\times$ sifting efficiency*.

distance	1.5 m	5.5 m	10.5 m
QBER (%)	1.44	3.4	1.0
key rate	0.79	0.57	0.84

The combination of polarization, e.g., $\{|H\rangle, |V\rangle\}$ and OAM, e.g., $\{-1, +1\}$ can be used as a 4-dimensional Hilbert space for high-dimensional QKD [15]. To avoid errors assigned to high-dimensional generation and detection schemes [9, 31], we compare the 2-dimensional

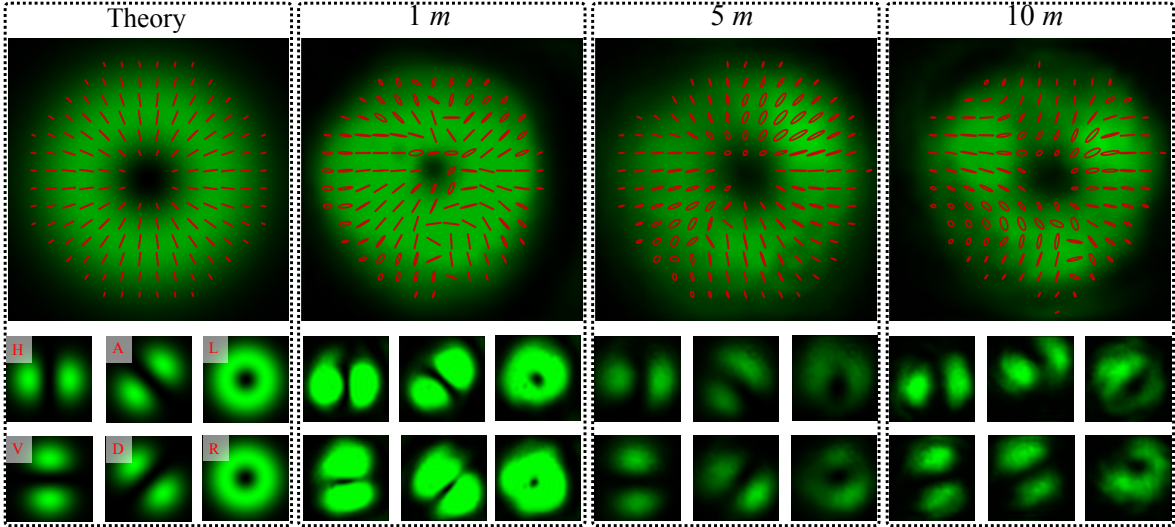


FIG. 2. **Polarization tomography of a radially polarized beam for different channel lengths.** The reconstructed spatial polarization profile of the radial polarization mode is shown (top) for the theoretical as well as experimentally reconstructed beams propagating through the channel length of 1 m, 5 m, and 10 m. The intensity profile is shown in green, while the orientation of the polarization is shown in the red ellipses. The reconstructed spatial polarization profile was found using polarization tomography. The reduced stokes parameters were calculated for each pixel using the polarization measurements, $\{H, V, D, A, L, R\}$, shown in the lower insets.

spatial modes with the polarization states. The vector vortex modes in Eqs. (2) and (3) were used to establish a quantum channel at 1, 5, and 10 meter distances. The difficulty with alignment of these spatial modes restricted us from coupling to single mode fiber for distances longer than 10 meters. The QBER and consequent key rates for these channels are given in Table II.

We also study the effect of underwater turbulence on the spatial profile of vector vortex modes propagating through different channel lengths. We perform polarization tomography by measuring the intensity of the structured beam, using a CCD camera, after passing a polarizer for $\{H, V, A, D, R, L\}$. From these measurements, the polarization is reconstructed pixel-by-pixel. The state sent across the channel is the radial polarization state. This is created by sending a vertical linearly polarized Gaussian beam onto the $q = 1/2$ plate. The resultant spin-orbit state is $(|L, -1\rangle + |R, +1\rangle)/\sqrt{2}$. The theoretical polarization profile as well as the measured profiles for 1, 5, and 10 meters is shown in Fig. 2. The spatial profile can be seen to degrade as the channel length increases. This is associated to turbulence in the water channel that increases by the length [23, 25]. The phase distortion associated to the turbulence includes not only tip-tilt aberrations, but also higher-order effects such as astigmatism to the spatial profile of the beam. The aberrations in the underwater scenario are slower than those observed in air free-space, and thus the astigmatism aberrations are more easily seen as opposed to the scintillation often observed in high turbulence cases in the air.

III. KEY RATE ANALYSIS

The initial BB84 proposal is an ideal protocol in which real single photons guarantee that there are not multiple photons in any given state which could open a door for an eavesdropping attack, i.e., photon number splitting attack [32]. For the BB84 protocol the number of bits that can be gained from each signal is,

$$G = \frac{1}{2}Q(1 - 2H(e)), \quad (4)$$

where Q is the gain and $H(e) = -e \log_2(e) - (1 - e) \log_2(1 - e)$ is the Shannon entropy for the error rate e . This ideal BB84 key rate requires some assumptions that are often not valid in practical QKD situations. The first of these assumption is the use of real single photons, i.e., heralded pairs, as opposed to an attenuated laser source. An attenuated laser source is a much more practical implementation, as photon pairs generated through spontaneous parametric down conversion (SPDC) are not deterministic. When using an attenuated source, the main point of weakness to consider is the possibility of more than one photon in a pulse. Other practical factors to consider are the effect of imperfect detectors and channel losses. These are brought into consideration in modern security proofs done for practical QKD protocols. We implement the decoy state protocol in our key rate analysis [33]. In any protocol using an attenuated laser source, one must choose the pulse mean photon number (μ). This μ is taken below 1 such that the Poisson distribution gives a low probability of a 2-photon state. The density matrix of this signal state is given as,

TABLE III. Experimental parameters of the underwater polarization channel.

Parameter	Dark Counts	Source Rep Rate	Detector Efficiency	Bob's Detection Efficiency	Channel Loss (α)
Flume Result	300 Hz	10^9 Hz	0.6	0.188	0.57 dB/m

$$\rho = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle \langle i|. \quad (5)$$

Here $|i\rangle$ is the Fock state, denoting i number of photons. In the decoy state protocol, we include another state, the decoy state, which has a different mean photon number (ν). The key rate for the decoy state protocol is given by,

$$K = \frac{1}{2} \{-Q_{\mu} f(E_{\mu}) H(E_{\mu}) + Q_1 (1 - H(e_1))\}, \quad (6)$$

where Q_{μ} is the gain of the total signal state sent by Alice, E_{μ} is the signal state QBER, Q_1 is the gain of the single photon state, e_1 is the error rate of the single photon state, and f is the error correction efficiency. Q_1 and e_1 are respectively lower and upper bounded by,

$$Q_1 \geq \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left(Q_{\nu} e^{\nu} - Q_{\mu} e^{\mu} \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right), \quad (7)$$

$$e_1 \leq \frac{E_{\nu} Q_{\nu} e^{\nu} - Y_0/2}{Q_1 \nu / (\mu e^{-\mu})}. \quad (8)$$

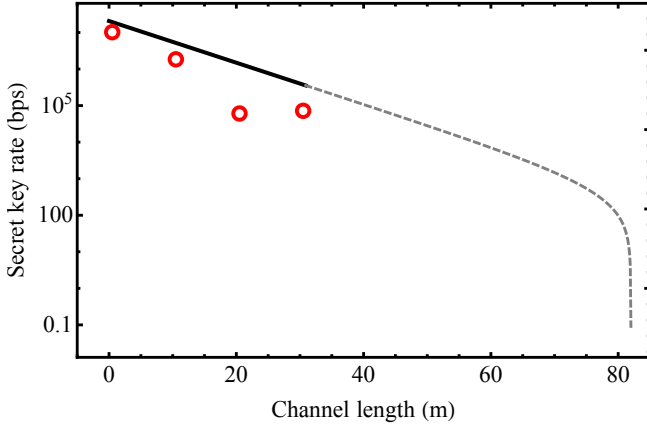


FIG. 3. **Secret key rate for the underwater polarization channel.** The optimal secret key rate for the underwater channel with the measured attenuation is shown by the black curve. The experimental points (red) show the key rates achieved with the quantum bit error rates measured for the 0.5 m, 10.5 m, 20.5 m, 30.5 m channels. The experimental points, though necessarily lower than the zero-QBER theory, does follow the theoretical line closely, giving support to the prediction that 80 meters can be achieved. The dashed line shows the expected optimal key rate for channel lengths longer than 30 m. The optimization calculation is performed using the values stated in Table III.

Here, Y_0 is the background rate per pulse, Q_{ν} is decoy state gain and E_{ν} is the decoy state QBER. We can optimize the values of μ and ν for different values of loss

(channel distance), given the parameters associated to our channel. The values for the detector efficiency, dark-counts, channel loss, and Bob's detection efficiency measured for our underwater polarization channels are given in Table III. These parameters can be used to calculate the values of μ and ν , which will yield the optimal key rate for different distances. This optimal key rate is plotted in Fig. 3 as the channel length, i.e., attenuation, is increased. The optimal key rate is shown in black accounting for errors resulting from dark counts only. The experimental data points which add the measured QBER to the background errors are shown in red for the channel lengths of 0.5, 10.5, 20.5, and 30.5 meters. The achievable key rates of the experimental points fall below the theoretical line as expected. However, the key rates do closely follow the trend depicted by the theory, suggesting that a channel length near 80 meters could be successfully established with these channel parameters. The key rate analysis for the vector vortex modes follows the exact method demonstrated for the polarization states. The only change is the experimentally observed QBER, which have similar values to those of the polarization channels of the similar length - on the order of 1% for 10 m - and thus results in similar key rates. For example, the key rate for the 10.5 meter channel of vector vortex modes is 72 Kbps.

IV. CONCLUSION AND OUTLOOK

We have studied a turbulent underwater channel for quantum communication using polarization and vector vortex modes, beams having spatially structured polarization states. Both the polarization and vector vortex modes maintained their fidelity upon propagation through the channel, resulting in sufficiently low error rates (QBER) to achieve a secure quantum channel. The turbulence - primarily beam wandering - introduces significant challenges with alignment and coupling to single mode fibre. In our channel, the beam path is near the surface of the water for the entire length which results in relatively high turbulence due to the temperature gradient at the air-water surface. Thus channels operating at greater depths may see less turbulence than observed here. Despite these challenges we have shown that both polarization states and spatially structured polarization states can be used in an underwater free-space setting, and for establishing a positive secret key rate for lengths up to 30 meters. The implementation of automated beam tracking equipment would allow one to achieve longer channels approaching the lengths that have been theoretically proposed. In fact, the slower turbulence ob-

served in an underwater channel makes this task of beam correction much easier than in a free-space air environment. We also performed key rate analysis taking into account the parameters measured in our channel. Given these parameters the maximum distance for secure communication would be 80 meters, though this is extremely dependent on the attenuation coefficient of the channel, and Bob's detection efficiency. Improvements in either of these areas would significantly extend the maximum achievable distance.

V. ACKNOWLEDGEMENTS

We would like to thank Nathalie Brunette, Michel Brassard, Yvan Brunet, and Tony Frade at the Ocean, Coastal and River Engineering Research Centre of National Research Council Canada for all of their efforts in helping us perform this research. This work was supported by Joint Centre for Extreme Photonics (JCEP), Canada Research Chairs (CRC), Canada First Excellence Research Fund (CFREF), and Ontario's Early Researcher Award. A.S. acknowledges the financial support of the Vanier graduate scholarship of the NSERC.

-
- [1] P. W. Shor, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.
 - [2] H. Bennett Ch and G. Brassard, *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, , 175 (1984).
 - [3] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, *Physical Review Letters* **115**, 040502 (2015).
 - [4] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, *Nature* **549**, 43 (2017).
 - [5] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaar, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, arXiv preprint arXiv:1906.01645 (2019).
 - [6] G. Leuchs, C. Marquardt, L. L. Sánchez-Soto, and D. V. Strekalov, in *Optical Fiber Telecommunications VII*, edited by A. E. Willner (Academic Press, 2020) pp. 495 – 563.
 - [7] A. K. Ekert, *Physical Review Letters* **67**, 661 (1991).
 - [8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Journal of cryptology* **5**, 3 (1992).
 - [9] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, *Quantum* **2**, 111 (2018).
 - [10] H. Rubinsztein-Dunlop, A. Forbes, M. Berry, M. Dennis, D. Andrews, M. Mansuripur, C. Denz, C. Alpmann, P. Banzer, T. Bauer, E. Karimi, L. Marrucci, M. Padgett, M. Ritsch-Marte, N. Litchinitser, N. Bigelow, C. Rosales-Guzmán, A. Belmonte, J. Torres, T. Neely, M. Baker, R. Gordon, A. Stilgoe, J. Romero, A. White, R. Fickler, A. Willner, G. Xie, B. McMorran, and A. Weiner, *Photonics Research* **19**, 013001 (2016).
 - [11] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, *Optics Express* **27**, 37214 (2019).
 - [12] J. Jin, J.-P. Bourgoin, R. Tannous, S. Agne, C. Pugh, K. Kuntz, B. Higgins, and T. Jennewein, *Optics Express* **27**, 37214 (2019).
 - [13] 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 Journal of Physics* **17**, 033033 (2015).
 - [14] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, *Physical Review Letters* **113**, 060503 (2014).
 - [15] 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).
 - [16] C. Marand and P. Townsend, *Europhysics Letters* **23**, 383 (1993).
 - [17] C. Marand and P. Townsend, *Optics Letters* **20**, 1695 (1995).
 - [18] A. Sit, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. Boyd, S. Ramachandran, and E. Karimi, *Optics Letters* **43**, 4108 (2018).
 - [19] G. Xavier and G. Lima, *Communications Physics* **3**, 1 (2020).
 - [20] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, *et al.*, *Physical Review X* **9**, 041042 (2019).
 - [21] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, *Science advances* **3**, e1701491 (2017).
 - [22] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, *Advanced Quantum Technologies* **2**, 1900038 (2019).
 - [23] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, and E. Karimi, *Optics Express* **26**, 22563 (2018).
 - [24] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, *Applied Optics* **58**, 3902 (2019).
 - [25] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. Sussman, R. Boyd, G. Leuchs, and E. Karimi, *Optics Express* **27**, 26346 (2019).
 - [26] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, H. Tang, and X.-M. Jin, *Photonics Research* **7**, A40 (2019).
 - [27] S. Sullivan, *Journal of the Optical Society of America* **53**, 962 (1963).
 - [28] F. Cardano, E. Karimi, S. Slussarenko, L. Marrucci, C. de Lisio, and E. Santamato, *Appl. Opt.* **51**, C1 (2012).
 - [29] L. Marrucci, C. Manzo, and D. Paparo, *Physical Review Letters* **96**, 163905 (2006).
 - [30] H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R. W. Boyd, and E. Karimi, *Journal of Optics* **18**, 124002 (2016).
 - [31] F. Zhu, M. Tyler, N. H. Valencia, M. Malik, and J. Leach, arXiv preprint arXiv:1908.08943 (2019).

- [32] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Physical Review Letters **85**, 1330 (2000).
- [33] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters **94**, 230504 (2005).

Chapter 4

Conclusions

We have looked at various aspects of high-dimensional quantum information. Various quantum sensing techniques will be necessary to continue making quantum technologies such as underwater communication more practical. In chapter 2, we presented 3 different quantum sensing protocols for high-dimensional systems, and then experimentally verified them. The quantum process tomography project showed the way in which one can characterize high dimensional quantum processes. In particular, we characterized two different eavesdropping attacks performed on a quantum communication channel. In the work on compressed sensing of twisted photons, we presented a protocol that allows one to measure low rank OAM states using only intensity measurements. This results in an experimental simplification as one does not have to measure the phase. The adaptive compressed sensing work introduces a new compressed sensing protocol which does not require any prior information about the rank of the quantum state. This allows one to use the protocol in any situation, gaining the compressed sensing benefits as long as the state does turn out to be low rank. This is exciting since often, one will not know the rank of the quantum state that they are trying to measure.

In chapter 3 we explored underwater quantum communication in three different settings. In the 3 meter outdoor swimming pool, we established a quantum communication channel using the three dimensional OAM states $\ell = \{-1, 0, 1\}$. This showed the possibility of using the OAM states as quantum carriers in an underwater environment. We were also able to observe the phenomena of singularity splitting brought on by turbulence in the channel. In the Ottawa River, we transmitted polarization states across 5 meters of highly scattering water. Here, we were able to measure the effect of turbulence on large OAM beams and also the phase distortions

on a Gaussian beam. Finally in the 30 meter flume channel, we established a quantum channel with polarization states. We also established a 10 meter channel with vector vortex modes, showing that these are also able to be used as quantum carriers in an underwater environment. The effect of turbulence can be seen here to distort the polarization structure of the vector vortex modes.

Though turbulence presents a difficulty in underwater quantum communication, we were able to see that the frequency of the distortions is much lower than in atmospheric channels. This allows us to consider adaptive optics techniques for future work. Some of the sensing techniques studied here could even be helpful in implementing these fast beam correction technologies. Further improvement of measurement techniques, and the development of more efficient sensing protocols may be instrumental in pushing quantum communications to the level of being used in real world applications. In particular we hope to establish a quantum communication channel between moving vessels in the underwater environment. And further, to establish a quantum channel between a submarine and a party above the surface of the water.

Bibliography

- [1] Albert Einstein. Über einen die erzeugung und verwandlung des liches betreffenden heuristischen gesichtspunkt. *Annalen der physik*, 322(6):132–148, 1905.
- [2] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43:172–198, 1927.
- [3] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.
- [4] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.
- [5] Max Born. Quantenmechanik der stoßvorgänge. *Zeitschrift für Physik*, 38(11-12):803–827, 1926.
- [6] Anthony Duncan and Michel Janssen. (never) mind your p’s and q’s: Von neumann versus jordan on the foundations of quantum theory. *The European Physical Journal H*, 38(2):175–259, 2013.
- [7] John Von Neumann. Mathematische begründung der quantenmechanik. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1927:1–57, 1927.
- [8] John Von Neumann. Wahrscheinlichkeitstheoretischer aufbau der quantenmechanik. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1927:245–272, 1927.
- [9] Ugo Fano. Description of states in quantum mechanics by density matrix and operator techniques. *Reviews of Modern Physics*, 29(1):74, 1957.

- [10] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.
- [11] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, 2001.
- [12] David L Donoho. Compressed sensing. *IEEE Transactions on information theory*, 52(4):1289–1306, 2006.
- [13] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. Quantum state tomography via compressed sensing. *Physical review letters*, 105(15):150401, 2010.
- [14] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, 1984.
- [15] A. K. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67(6):661, 1991.
- [16] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International journal of quantum information*, 8(04):535–640, 2010.
- [17] Andrey Nikolaevich Kolmogorov. The local structure of turbulence in incompressible viscous fluid for very large reynolds numbers. *Cr Acad. Sci. URSS*, 30:301–305, 1941.