# Spatially Structured Light for High-Dimensional Quantum Information

by

Felix Hufnagel

Thesis submitted to the University of Ottawa
in partial fulfillment of the requirements for the
Doctor of Philosophy degree in Physics

Department of Physics
University of Ottawa
Ottawa, Canada

# Abstract

Encoding information on single photons of light is an important part of many quantum information applications. There are many photonic degrees of freedom which can be used for encoding quantum information, and we refer to these diverse states as structured light. Structured light is used for many quantum information such as quantum key distribution, entanglement distribution, sensing, and quantum walks. One advantage of structured light is that we can encode more than 1 bit of information on a single photon. This has obvious benefits for quantum communication in allowing one to increase the information density of the communication channel. However another benefit which comes out of the security proofs of quantum communication protocols is an increased tolerance to errors. This can be useful if one want to communicate in a noisy environment. In this thesis we focus on the transverse spatial modes of light, in particular the Laguerre-Gaussian modes and how these can be used for high-dimensional quantum protocols. This culminates in three works detailing new quantum protocols and the implementation of an adaptive optics system to improve key rates in free-space channels. We present a new protocol for quantum key distribution which is a high-dimensional extension of the round-robin differential-phase-shift protocol and experimentally demonstrate the protocol using Laguerre-Gaussian modes with an azimuthal index up to $\ell = 15$. We also describe a high-dimensional extension to quantum certified deletion. First however, we discuss the liquid crystal devices that are used to generate these states and show the kinds of interesting light that can be produced. We detail an experimental demonstration of magic windows using liquid crystal devices, and show a new and optimal method for diffractive focussing which is confirmed experimentally

with liquid crystal devices. We also present 2 works on photon pair sources which are a fundamental piece of quantum communication systems. We describe a method for tailoring the symmetry of momentum entangled states and show the full Laguerre-Gaussian mode correlations from an SPDC source. Many different technological steps are required for the implementation of quantum information protocols, and here we demonstrate advances across many of these steps from states preparation to source characterization to protocol implementation.

# Acknowledgements

First I am happy to thank my supervisor Ebrahim Karimi, who has been an incredible advisor and friend throughout our years of our scientific pursuits together. I am very grateful for all of the late nights spent enjoying science and enjoying life together. I am so appreciative of all the opportunities and support both academic and otherwise.

I acknowledge the financial support of the Natural Sciences and Engineering Research Council of Canada (NSERC).

I was lucky to be mentored by great experimentalists during my time in Ottawa. To Fred, Hugo, and Alicia, thank you for all of the fun times we had in and out of the lab. From the river to the roof to conferences, I could not ask for better people to work with. I would also like to thank Alessio and Lukas for all of the time spent together on experiments. Their efforts were so important to many of the projects in this thesis. I'd also like to thank the rest of the SQO group for all of the fun we have shared, and particularly for stimulating discussions with Dilip, Nazanin, Manuel, and Yingwen. I would also like to thank Khabat for all of the insightful discussions and collaboration. I would also like to thank Nick for his incredible friendship as we went through our degrees together.

I would like to thank all of my collaborators Maxim Efremov, Wolfgang Schleich, Anne Broadbent, Mikka Stasiuk, Xiaoqin Gao, Aaron Goldberg, Filippo Miatto, Mohammadreza Rezaee, Fatimah Alsaiari, and Jeremy Upham.

Finally, I would like to thank my parents, John and Rhonda, and my sister Aisha, for all of their love and support throughout my life, and for continuing to be excited about

the things I do.

I would like to thank Sophie, my loving wife and best friend for everything. Thank you for bringing so much joy to my life and for always being willing to adventure with me.

To my lovely Sophie,
and to Ross.

# Table of Contents

# List of Publications

## PhD

1. M. A. Efremov, **F. Hufnagel**, H. Larocque, W. P. Schleich, and E. Karimi, "Optimal Diffractive Focusing of Quantum Waves," *arXiv* 2406.13545 (2024).

2. L. Scarfe, **F. Hufnagel**, M.F. Ferrer-Garcia, A. D'Errico, K. Heshami, and E. Karimi, "Fast Adaptive Optics for High-Dimensional Quantum Communications in Turbulent Channels" *arXiv* 2311.13041 (2023).

3. **F. Hufnagel**, A. Broadbent, and E. Karimi, "High-Dimensional Quantum Certified Deletion" *arXiv* 2304.03397 (2023).

4. M. Stasiuk, **F. Hufnagel**, X. Gao, A.Z. Goldberg, F. Bouchard, E. Karimi, and K. Heshami, "High-dimensional Encoding in the Round-Robin Differential-Phase-Shift Protocol" *Quantum* **7**, 1207 (2023).

5. J. Bégin, A. Jain, A. Parks, **F. Hufnagel**, P. Corkum, E. Karimi, T. Brabec, and R. Bhardwaj, "Nonlinear helical dichroism in chiral and achiral molecules" *Nature Photonics* **17**, 82 (2023).

6. X. Gao, Y. Zhang, A. D'Errico, **F. Hufnagel**, K. Heshami, and E. Karimi, "Manipulating the symmetry of transverse momentum entangled biphoton states" *Optics Express* **30**, 21276 (2022).

7. **F. Hufnagel**, Alessio D'Errico, Hugo Larocque, Fatimah Alsaiari, Jeremy Upham, and Ebrahim Karimi. "Flat magic window" *Optica* **9**, 479 (2022).

8. A. D'Errico, **F. Hufnagel**, F. Miatto, M. Rezaee, and E. Karimi, "Full-mode characterization of correlated photon pairs generated in spontaneous downconversion" *Optics Letters* **46**, 2388 (2021).

9. A. Sit, **F. Hufnagel**, E. Karimi, "Chapter 6: Quantum cryptography with structured photons," in *Nanophotonics*, Structured Light for Optical Communication, Elsevier, 139–176 (2021).

10. S. Sederberg, F. Kong., **F. Hufnagel**, F., C. Zhang, E. Karimi, and P.B. Corkum, "Vectorized optoelectronic control and metrology in a semiconductor" *Nature Photonics* **14**, 680 (2020).

## MSc

11. **F. Hufnagel**, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, E. Karimi, "Investigation of underwater quantum channel in a 30-meter flume tank using structured photons," *New Journal of Physics* **22**, 093074 (2020).

12. **F. Hufnagel**, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. Englang, 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).

13. D. Ahn, Y. S. Teo, H. Jeong, F. Bouchard, **F. Hufnagel**, E. Karimi, D. Koutny, J. Rehacek, Z. Hradil, G. Leuchs, and L. L. Sanchez-Soto, "Adaptive Compressive Tomography with No a priori Information" Physical Review Letters (2019).

14. F. Bouchard, D. Koutny, **F. Hufnagel**, Z. Hradil, J. Rehacek, Y. S. Teo, D. Ahn, H. Jeong, L. L. Sanchez-Soto, G. Leuchs, and E. Karimi, "Compressed sensing of twisted photons", *Optics Express* **27**, 17426 (2019).

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

16. 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", *Optics Express* **26**, 22563 (2018).

17. G. S. Thekkadath, **F. Hufnagel**, and J. S. Lundeen, "Determining complementary properties using weak-measurement: uncertainty, predictability, and disturbance", *New Journal of Physics* **20**(11), 113034 (2018).

# Statement of Originality and Contributions

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

E. Karimi initiated the work of Chapter 2 on magic windows. F. Hufnagel and H. Larocque performed the theoretical calculations and simulations. F.Hufnagel and A.D'Errico fabricated the device. J. Upham spin-coated the device. F.Hufnagel and A.D'Errico and F. Alsaiari perfomed the experiment. F. Hufnagel performed the data analysis. F. Hufnagel and E. Karimi and H. Larocque wrote the manuscript.

W. P. Schleich and E. Karimi initiated the work of Chapter 2 on optimal focusing. M. Efremov performed the theoretical calculations. F. Hufnagel and H. Larocque performed the simulations. F. Hufnagel performed the experiment and fabricated the device. F. Hufnagel analysed the experimental data. All authors wrote the manuscript.

E. Karimi initiated the work of Chapter 3 on momentum entanglement. F. Hufangel and X. Gao, and Y. Zhang and A. D'Errico performed the experiment. E. Karimi and K. Heshami and X. Gao developed the theory. X. Gao and Y. Zhang analysed the data. X. Gao and Y. Zhang and E. Karimi wrote the manuscript.

E. Karimi initiated the work of Chapter 3 on full mode characterization of SPDC. F. Hufnagel and A. D'Errico and M Rezaee performed the experiment. A. D'Errico and F.

Miatto and E. Karimi developed the theory. A. D'Errico performed the simulations. A. D'Errico analysed the data. All authors wrote the manuscript.

E. Karimi and A. Broadbent initiated the work of Chapter 4. F. Hufangel developed the theory. F. Hufnagel performed the experiment and the data analysis. All authors wrote the manuscript.

K. Heshami and E. Karimi initiated the work of Chapter 4 on round robin QKD. F. Bouchard and M. Stasiuk and X. Gao and A. Goldberg and K. Heshami developed the theory. F. Bouchard and M. Stasiuk performed the simulations. F. Hufnagel performed the experiment and analysed the data. F. Hufnagel and F. Bouchard and M. Stasiuk wrote the manuscript.

E. Karimi initiated the work of Chapter 4 on adaptive optics. F. Hufangel and L. Scarfe and M. Ferrer-Garcia performed the experiment. F. Hufangel and L. Scarfe and M. Ferrer-Garcia performed the data analysis. All authors wrote the manuscript.

# List of Figures

# Chapter 1

# Introduction

Quantum theory developed throughout the 20th century and provided the solution to many fundamental problems in physics including black-body radiation, Compton scattering, and the photoelectric effect. It also enabled forward thinking ideas from physicists and mathematicians such as Richard Feynmann about how the properties of quantum systems could be used in the future for technological applications in computing. Furthermore, in combining ideas from quantum theory with the 20th century development of classical information theory by Claude Shannon, the field of quantum information was developed. Quantum information makes use of the properties of quantum systems to develop new technologies for applications in computing, communication, and sensing. These technologies may use single, photons, atoms, or larger systems which obey some quantum properties, and will take advantage of the inherently quantum properties of these systems to overcome some challenge which we can not solve with classical tools. An important example of this is the computing challenge of finding the prime factors of a large number. It remains an open problem in computer science and mathematics to find an efficient classical algorithm for prime factorization. This algorithmic difficulty has been used as a critical piece of modern secure communication with public key encryption protocols such as RSA. However, it was shown in 1994 by Peter Shore that a quantum computer would be capable of solving the

factoring problem in polynomial time [1]. The eventual realization of Shore's algorithm on a quantum computer will introduce a security vulnerability for much of our modern communication and thus the field of quantum key distribution (QKD) has received significant attention as a potential solution to this problem.

There are some distinctly quantum phenomena we should identify which we will try to exploit to create interesting quantum technologies. First we may consider the notion of uncertainty. In macroscopic systems we may have some experimental situation where we have some uncertainty about the state of a classical system due to precision limits in our measurement devices. However, in the classical case we would not consider this a fundamental property of the system, but rather a need for improved equipment and a reason for a new funding proposal. For example, our ability to identify details in a picture taken with an old camera may be overcome by increasing the size of the sensor or the lens systems being used in an upgraded device. In contrast, with quantum systems we have a fundamental limit on the information that we are able to access about some quantum state. This is famously described by the Heisenberg uncertainty principle with respect to the position and momentum of a particle by,

$$\Delta x \Delta p \geq \hbar/2 \tag{1.1}$$

where $\Delta x$ and $\Delta p$ are the individual uncertainties for the position and momentum. Here $x$ and $p$ are conjugate variables, and we can see that in the limit as we reduce the uncertainty $\Delta x$, i.e., as we have more precise information about $x$, we reduce the information that can be obtained about $p$. This inequality can also be applied to any conjugate variables such as energy and time, or angular momentum and angular position.

Second we have the phenomenon of entanglement, which describes non-classical correlations between quantum particles. These correlations are specifically defined as being non-classical as there does not exist a classical description which can replicate the correlations we find in the case of entangled particles. The defining property of a pair of entangled particles is that they have correlations which violate the Bell inequality. Before going into depth on the formalism of the Bell inequality and how this can be used to provide evi-

dence of entanglement, we will introduce some of the mathematical concepts necessary for studying quantum mechanics.

In the quantum information topics discussed here, we will rely heavily on the "bra-ket" notation introduced by Paul Dirac in 1939 [2]. We start by introducing a quantum state, which we will represent using the "ket" symbol, $|\cdot\rangle$, which represents a vector. This ket has a hermitian conjugate denoted by the "bra", $\langle\cdot|$ which acts as a linear functional on the kets. We define this hermitian conjugate using the *dagger* notation, i.e., $\langle\cdot| = |\cdot\rangle^\dagger$. We have an inner product between the bras and kets, $\langle\phi|\psi\rangle$, which gives a complex number that represents the overlap or the similarity between two quantum states. In another way, we can think of $\langle\phi|\psi\rangle$ representing the probability amplitude of finding the quantum state $|\psi\rangle$ to transition to the state $|\phi\rangle$. To get a measurable, real-valued probability we multiply the amplitude by its complex conjugate giving $P = \langle\phi|\psi\rangle\langle\psi|\phi\rangle = |\langle\phi|\psi\rangle|^2$, giving the square modulus. In a finite Hilbert space these bra and ket vectors will represent row and column vectors and the overlap $\langle\phi|\psi\rangle$ is the inner product given by matrix multiplication. As an explicit example lets consider a 2 dimensional Hilbert space given by the polarization of a photon. We can choose the horizontal and vertical polarization states as an orthogonal basis, where we write the states as $|H\rangle = (1, 0)$ and $|V\rangle = (0, 1)$. Now the inner product, or projection, gives us the orthogonality condition for these 2 states: $\langle H|V\rangle = \langle V|H\rangle = 0$ and $\langle H|H\rangle = \langle V|V\rangle = 1$. We can also have quantum states which are some arbitrary superposition of these orthogonal basis vectors. Continuing with the polarization states, we can have a superposition state given by $|\psi\rangle = c_0|H\rangle + c_1|V\rangle$ where $c_0$ and $c_1$ are complex numbers such that $|c_0|^2$ and $|c_1|^2$ are the probabilities of measuring the state $|\psi\rangle$ in the states $|H\rangle$ and $|V\rangle$. Specifically can write the diagonal and anti-diagonal polarization states as $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$, and the right and left circular polarizations are given by $|R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and $|L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$. The diagonal/anti-diagonal and right/left polarizations provide two additional orthogonal bases for the photonic polarization.

While polarization is one example of a photonic quantum state, we can write the quantum state for any degree of freedom such as the frequency, position, momentum, or number

of photons. We can also use the bra-ket notation for a continuous variable to represent the wave function $\psi(x)$ which is the probability amplitude of finding the quantum state $|\psi\rangle$ in the position $|x\rangle$. This is again written as the inner product $\psi(x) = \langle x|\psi\rangle$. Again in the lab what we are often going to measure the real-valued probability density, $P(x)$ which is the more familiar concept of the probability of finding a quantum particle at position $x$. The probability density is again given by multiplying the amplitude by its complex conjugate, i.e., $P(x) = \psi^*(x) \cdot \psi(x) = |\psi(x)|^2$. We can then find the normalization of the wave function by requiring that the probability of finding the quantum particle anywhere in space is equal to 1, thus integrating over all space we have $\int \psi^*(x) \cdot \psi(x) dx = 1$. We also have linear operators which act on the quantum states and transform them to another state. In the discreet, $d$-dimensional Hilbert space, an operator $\hat{A}$ is an $d \times d$ matrix and thus the matrix multiplication $\hat{A}\,|\psi\rangle$ results in another ket, $|\psi'\rangle$. Finally, we do not always have so called *pure states* which are easily represented by a single wave function. We can also have *mixed states* which are statistical ensembles of pure states. These are constructed from a ket-bra pair to give an $d \times d$ matrix and are typically denoted as $\hat{\rho} = \sum_{i,j=1}^{d} p_{ij}\,|\psi_i\rangle\,\langle\psi_j|$, where $p_{ij}$ are the statistical weights of each state. These will provide us with much more versatility in talking about quantum states for the purpose of quantum information.

Returning now to the topic of entanglement, we can describe these entangled states by considering a pair of anti-correlated particles $A$ and $B$ in a state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle_A\,|\downarrow\rangle_B - |\downarrow\rangle_A\,|\uparrow\rangle_B\right) \tag{1.2}$$

where $|\uparrow\rangle$ and $|\downarrow\rangle$ represent the spin up and spin down state of the particle. We can see that a measurement of particle $A$, revealing its state to be in either state $|\uparrow\rangle$ or $|\downarrow\rangle$, tells us which state particle $B$ is in. We can then rewrite this state in another basis, which can be achieved by applying the $\hat{\sigma}_x$ rotation resulting in the orthogonal basis states $|\pm\rangle = \left(|\uparrow\rangle \pm |\downarrow\rangle\right)/\sqrt{2}$. The original state in the rotated basis now becomes

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|+\rangle_A\,|-\rangle_B - |-\rangle_A\,|+\rangle_B\right). \tag{1.3}$$

Now a measurement of particle $A$ in state $|+\rangle$ results in particle $B$ being in state $|-\rangle =$

$(|\uparrow\rangle - |\downarrow\rangle)/\sqrt{2}$. This is very strange, because we are changing the state of particle $B$ simply by changing the choice of measurement on particle $A$ [3]. This apparent paradox was outlined by Einstein, Podolsky, and Rosen in 1935 and is referred to as the EPR paradox [4]. When considering that these particles could be separated by some vast amount of space, we can understand why Albert Einstein referred to these strange predictions of quantum theory as a "spooky action at a distance."

We can change the formulation to more accurately represent the 2-particle state by introducing density matrices to describe the state instead of the state vector *ket*. The two particle entangled state is then given by $\hat{\rho}_{AB} = |\psi\rangle\langle\psi|$ which in the spin up/down state is written as

$$\hat{\rho}_{AB} = \frac{1}{2}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right)\left(\langle\uparrow|_A\langle\downarrow|_B - \langle\downarrow|_A\langle\uparrow|_B\right) \tag{1.4}$$

We can then just look at the state of particle $B$ by the partial trace over particle $A$, i.e., $\hat{\rho}_B = Tr_A(|\psi\rangle\langle\psi|)$ which gives

$$\hat{\rho}_B = \frac{1}{2}\left(|\uparrow\rangle_B\langle\uparrow| + |\downarrow\rangle_B\langle\downarrow|\right) = \frac{1}{2}\hat{I}_B, \tag{1.5}$$

where $\hat{I}_B$ is the 2-dimensional identity operator in the state space of particle $B$. Similarly, the trace over particle $A$ in the plus/minus basis gives $\hat{\rho}_B = 1/2\hat{I}_B$. This form of density matrix for particle $B$ is referred to as the maximally mixed state, and we must reiterate that this is when we do not consider the measurement outcome for particle $A$ as those have been traced over. So now particle $B$ is in a completely mixed state, even though it started in a pure state in combination with particle $A$. Thus the state of particle $B$ is fundamentally altered by erasing the information of particle $A$ which we do when we perform the trace.

This apparent inconsistency motivated physicists to introduce the idea of "hidden variables" as a physical mechanism to describe this behaviour. The idea being that these unknown physical parameters are responsible for the quantum correlations that one measures experimentally. One such class of these theories considers local hidden variables which are not affected by spatially separated actions such as a measurement on the other

particle. These theories are related to the idea of local realism, i.e., the assumption that a physical property must be able to be predicted with certainty and is not dependent on the choice of measurement settings. In 1964 John Bell showed that there is an upper bound on measurement outcomes coming from any theory satisfying the properties of local realism [5]. To show this, consider again the correlated particles $A$ and $B$ now with some hidden variable $\lambda$ and measurement settings $a$ and $b$. The outcomes for measurement on $A$ and $B$ are independent of each other and we have $A = A(\lambda, a)$ and $B = (\lambda, b)$. The correlations between the two measurements can then be defined as

$$P(a,b) = \sum_{\lambda} \rho(\lambda) A(\lambda, a) B(\lambda, b) \tag{1.6}$$

where $\rho(\lambda)$ is the probability distribution of the hidden variable. Bell's theorem shows that a local realism interpretation is not possible beyond a certain bound which is broken by the expected results of a quantum experiment, thus verifying that the quantum correlations we observe cannot be produced by a classical system. Again this shows that these quantum phenomena are not a matter of our lack of understanding about these systems, but rather a fundamental behaviour of quantum systems which runs counter to our intuition. This can be demonstrated using photon pairs generated with perfect polarization correlations, and three polarization measurements at angles $0, +2\pi/3$ and $-2\pi/3$. If the outcomes of these measurements are pre-determined by local hidden variables, it can be shown that the probability of measuring the same result is at least $1/3$. However, when we consider the quantum scenario with the entangled state $|\psi\rangle = (|H\rangle_A |H\rangle_B + |V\rangle_A |V_B\rangle)/\sqrt{2}$, we find that the probability of getting the same measurement result is 0.125 in the case of the $2\pi/3$ measurement setting, thus breaking the $P \geq 1/3$ bound given by the local hidden variables.

Following the development of quantum mechanics, our understanding atoms and light-matter interaction allowed for great technological leaps in the 20th century. These include the transistor and the laser which have been fundamental to our rapid progress in nearly every field of industry and technology. These devices, who's discovery stemmed from a new understanding of the physical systems, are often referred to as the first quantum revolu-

tion. While the transistor and the laser rely on the laws of quantum mechanics, we do not actually make use of quantum effects such as superposition, uncertainty, and entanglement. The quantum 2.0 revolution describes our current effort to actively control single quantum states such as atoms or photons to create new technologies whose applications are dependent on these uniquely quantum phenomena. Quantum 2.0 has become realistic in recent years as various technologies have improved such as single photon detectors, atomic traps, milliKelvin refrigeration, ultra-stable lasers, nano-fabrication, and many others. Along with technological improvements, theoretical work into entanglement sources, communication protocols, computing architectures, error correcting codes, and sensing protocols has expanded as the feasibility of new quantum technologies has increased [6, 7]. Today both academic and industrial parties are pushing the boundaries of quantum communication, computing, and sensing. As the ecosystem grows, the progress is able to accelerate as different groups become more focussed on unique problems with more and more of the necessary tools such as sensors and control systems being industrially produced specifically for quantum tasks.

This thesis is primarily focussed on using spatial modes of light to establish secure, high-dimensional quantum communication channels. In achieving this goal we will cover a breadth of topics that are necessary to complete this task including liquid crystal device design for generating the spatial modes, characterization of quantum sources photon pairs, and developing unique high-dimensional quantum communication protocols which we implement experimentally. Finally, we also realize the implementation of a fast adaptive optics system for overcoming atmospheric turbulence with spatial modes of light for quantum communication. Chapter 2 details the design of liquid crystal devices through 2 separate works in which novel optical fields are created. Chapter 3 discusses the characterization of single photon sources, specifically two works investigating spontaneous parametric down conversion sources with position/momentum entanglement and full-mode Laguerre-Gaussian states. Chapter 4 includes 2 new protocols for high-dimensional quantum communication as well as my work on adaptive optics for quantum channels.

# Chapter 2

# Liquid Crystal Devices

## 2.1 Spatial Modes of Light

Light is the most effective physical system for communication, as demonstrated through all the 20th century development from radio communication(m), to cellular (mm) and fibre optic telecom (1.5 $\mu m$). We will use light in the infrared and visible (400-800 nm) spectrum for single photon quantum communication. It is important that we understand how the light behaves and thus beginning with the Maxwell's equations is a rather obvious place to start. For the electric field, $\mathbf{E}$, and magnetic field $\mathbf{B}$ in vacuum, we have the following four equations completely describing their dynamics:

$$\boldsymbol{\nabla} \cdot \mathbf{E} = \frac{\rho}{\epsilon_0}, \tag{2.1}$$

$$\boldsymbol{\nabla} \cdot \mathbf{B} = 0, \tag{2.2}$$

$$\boldsymbol{\nabla} \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}, \tag{2.3}$$

$$\boldsymbol{\nabla} \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t}, \tag{2.4}$$

where $\epsilon_0$ and $\mu_0$ are the permittivity and permeability of vacuum, and $\mathbf{J}$ and $\rho$ are the current and charge densities, respectively. In a vacuum when we set $\rho = 0$, $\mathbf{J} = 0$;

Maxwell's equations can be solved to give the Helmholtz's wave equations for $\mathbf{E}$ and $\mathbf{B}$,

$$\left(\nabla^2 - \mu_0\epsilon_0\frac{\partial^2}{\partial t^2}\right)\begin{Bmatrix}\mathbf{E}\\ \mathbf{B}\end{Bmatrix} = 0, \tag{2.5}$$

where $\nabla^2$ is the Laplacian operator. We typically use light at optical wavelengths in the $400-800$ nm range which we generate using a laser. At these wavelengths, we are able to *collimate* the light, which means that it is propagating primarily in a one direction as opposed to radiating outwards in every direction as one expects from an RF antenna. This means that the deviation of the wave vector away from the optical axis is very small and thus we can make use of the paraxial approximation, i.e., the slowly varying amplitude approximation, to arrive at the paraxial wave equation,

$$\left(\nabla_\perp^2 + 2ik\frac{\partial}{\partial z}\right)\mathbf{E}(\mathbf{r}) = 0, \tag{2.6}$$

where $\nabla_\perp^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$ is the transverse Laplacian operator and $\mathbf{E}(\mathbf{r})$ is the electric field vector. We now have a wave-equation which describes the evolution of an optical field in the z-direction, and we can consider what are the solutions to the transverse, x-y, modes of this field. This will give different sets of orthogonal mode solutions depending on the coordinates that we choose. We will mostly look at the cylindrical coordinates giving us the Laguerre-Gaussian modes which are written as,

$$\begin{aligned}\mathrm{LG}_{\ell,p}(r,\varphi,z) = \frac{C_{\ell,p}}{w(z)}\left(\frac{r\sqrt{2}}{w(z)}\right)^{|\ell|}\exp\left(-ik\frac{r^2}{2R(z)}\right)\exp\left(-\frac{r^2}{w(z)^2}\right)\times\\ \times L_p^{|\ell|}\left(\frac{2r^2}{w(z)^2}\right)\exp\left(i\Phi_{\ell p}(z)\right)\exp\left(i\ell\varphi\right).\end{aligned} \tag{2.7}$$

where $C_{\ell,p} = (2p!/(\pi(p+|\ell|)!))^{1/2}$, $L_p^{|\ell|}(\cdot)$ is the generalized Laguerre polynomial, and $\Phi_{\ell p}(z) = (2p+|\ell|+1)\mathrm{arctan}(z/z_R)$ is the mode-dependent Gouy phase. $R(z) = z(1+(z/z_r)^2)$ is the radius of curvature where $z_r = \pi\omega_0^2/\lambda$ and $\omega(z) = \omega_0(1+(z/z_r)^2)^{1/2}$ is the beam radius at a propagation distance $z$ for the beam waist $\omega_0$. The $\exp\left(-\frac{r^2}{w(z)^2}\right)$ term is a Gaussian which scales on propagation. The $e^{i\ell\phi}$ term defines the azimuthally varying

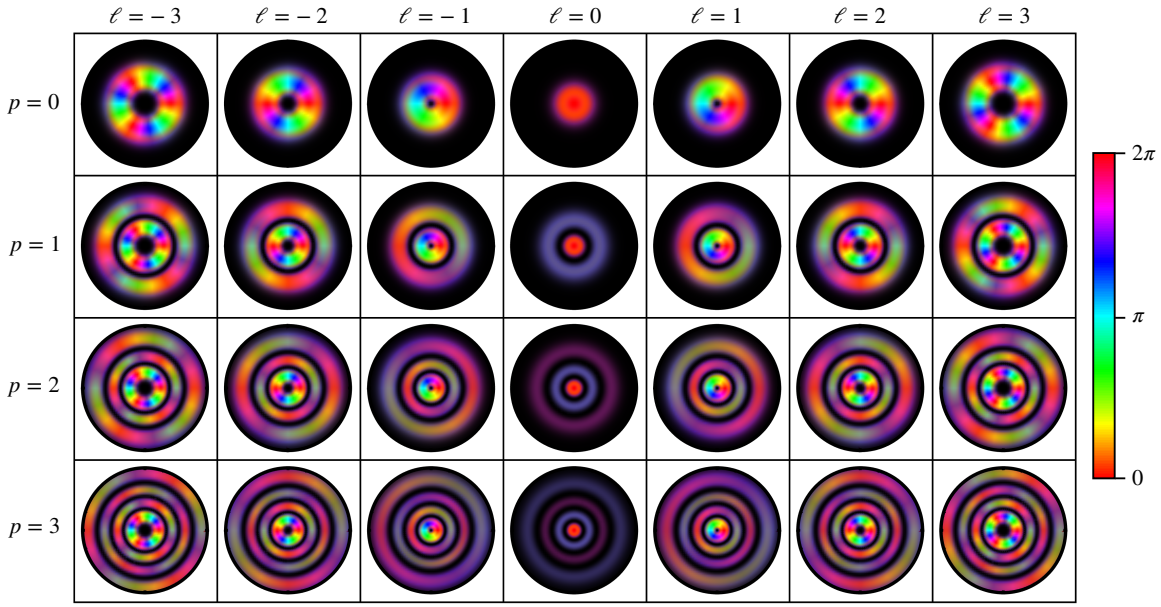


Figure 2.1: **Laguerre-Gaussian modes**. Intensity and phase of the lowest order $\ell$ and $p$ modes are plotted with their intensity and phase. As the order increases the modes become larger, taking up more of the cylindrical aperture.

phase which gives rise to $\ell\hbar$ units of orbital angular momentum (OAM) and is of particular interest for the works in this thesis.

The Laguerre-Gauss modes provide an orthogonal basis in $\ell$ and $p$ and thus we can use them in the same way as we use polarization to encode quantum information. The advantage the spatial modes have over polarization is that we are not limited to a 2-dimensional space but in fact have a theoretically infinite Hilbert space to work with. Some of the lowest order LG modes are plotted with intensity and phase in Fig 2.1 We describe a quantum state in the Laguerre-Gauss basis by $|\ell, p\rangle$ where

$$\langle r, \phi, z|\ell, p\rangle = \mathrm{LG}_{\ell,p}(r, \phi, z) \tag{2.8}$$

gives the probability amplitude of finding the state $|\ell, p\rangle$ in the coordinate space state $|r, \phi, z\rangle$. The quantum states $|\ell\rangle$ are defined as the eigenstates of the OAM operator $\hat{\ell} = -i\hbar\partial_\phi$. This operator is conjugate to the azimuthal position operator, $\hat{\phi}$, just as transverse position and momentum are conjugate variables.

## 2.2 Generation and Characterization Methods

LG modes of different $\ell$ and $p$ values do typically posses a different intensity pattern, however they are not orthogonal in their intensity patterns, and thus a camera can not be used to completely distinguish different modes and we must gain some phase information about the beam. The dominant approach to LG mode characterization is using the phase-flattening technique. However, there do exist compressed sensing protocols and phase retrieval approaches that are able to determine the LG mode in certain scenarios where some information is already known about the state being measured. Generally we want to make a full-field measurement of the intensity and phase. The phase-flattening technique is a projective measurement in which the conjugate phase of the mode profile which we want to detect is applied to the incoming beam resulting in the phase being removed if the input beam matches the applied conjugate phase. A spatial light modulator (SLM) is often used to apply this phase as the pattern can easily be changed, however one can also use q-plates, metasurfaces, or other devices to impart the desired phase. This now flattened transverse phase results in a Gaussian-like profile in the far field which allows the light to be coupled to a single mode optical fibre (SMF). If the incoming light still has some azimuthal phase component then it will not couple to the single mode fibre. Thus we are able to project onto desired modes and through changing the projected phase we can build up a complete set of measurements. One of the difficulties with phase-flattening is that it crucially depends on the use of a single mode optical fibre which means that the efficiency is bounded by the coupling efficiency. Another difficulty is that the efficiency is typically mode dependent. This can be particularly bothersome in suboptimal environments such

as a free-space quantum communication channel where beam deviations will impact the ability to couple all of the incoming light to the SMF. This will be addressed in more detail in the final chapter where we use adaptive optics to overcome atmospheric turbulence in an OAM based QKD channel.

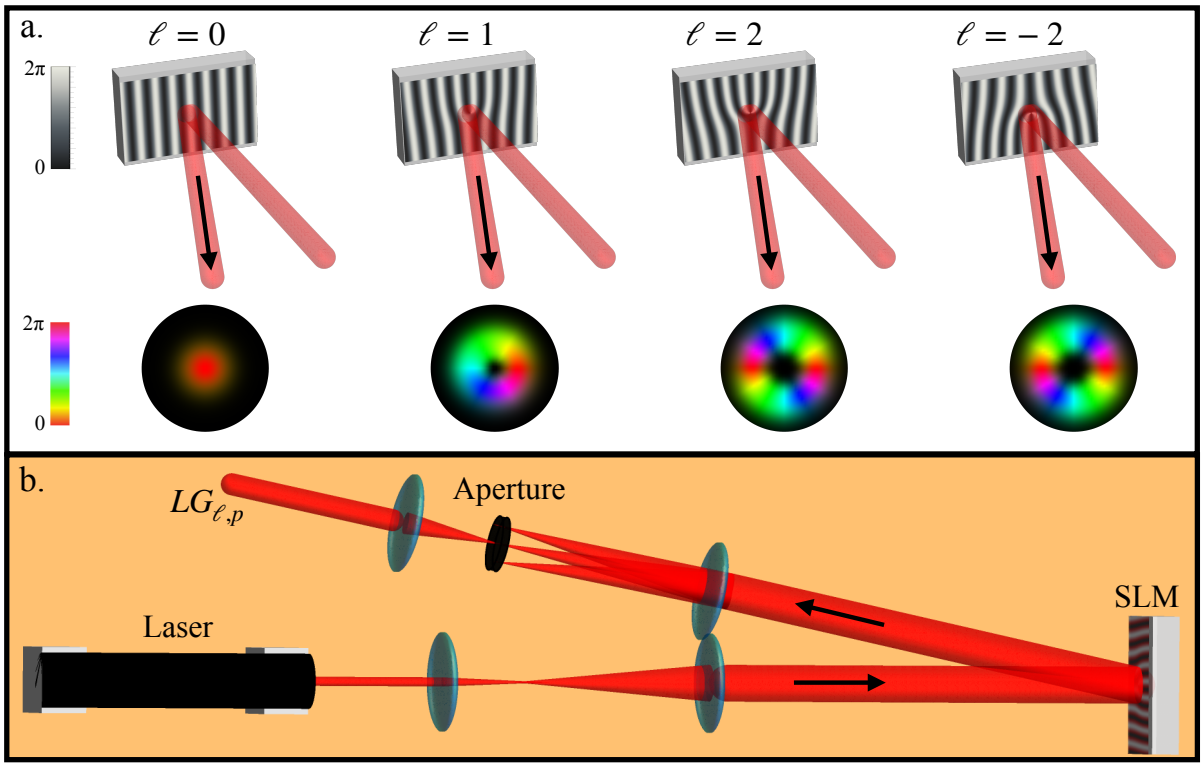


Figure 2.2: **SLM for LG generation**. A diffraction pattern is used on the SLM such that the desired mode is produced in the first order of diffraction. In this way, any inefficiency in the SLM does not result in unconverted light getting in the desired $\mathrm{LG}_{\ell,p}$ mode.

The single measurement setting of the phase-flattening approach provides many limitations in practical applications as many of the measurement results will give no information when the photon is not coupled to the fibre, except that the photon is not the mode displayed on the SLM. Thus there have been various developments toward "sorting" mea-

surements for OAM and spatial modes in general. These sorting techniques are analogous to a polarising beam splitter which give an output in the H and V polarisation mode as opposed to a polariser which only transmitted a single polarisation. One method which has seen many implementations makes use of multiple unitary optical transformations from the azimuthal OAM modes to distinct spatial positions. The device consists of a phase "unwrapper" and a phase correction component, which in combination translate the azimuthal phase gradient to a linear phase gradient. Then a Fourier lens is applied which sends the linear phase to distinct spatial positions in the far field [8]. Recently the approach of *mulit-plane light conversion* as these devices can be tailored to arbitrary specifications not limited to just sorting OAM modes but also more complex modes or OAM superposition states [9, 10]. As the name implies, this approach involves applying different phases to the incoming beam at multiple planes. The phases here are numerically determined using iterative methods such as the genetic algorithm to come up with a unitary operation between some input set of modes and some spatial output bins. One advantage of this approach is that one can tailor the output modes such that they be optimally coupled to a fibre or directly to some detector.

## 2.3 Liquid Crystal Devices

Liquid crystal devices are used in many technologies for manipulating the polarization and phase of light. This includes the ubiquitous liquid crystal display screens which have a layer of liquid crystals placed between two polarisers. For our applications, the liquid crystal can be oriented on a certain axis and then imparts a geometric phase, also called the Pancharatnam-Berry phase, onto incoming circularly polarized light. In the case of the Pancharatnam-Berry optical element (PBOE) devices that we produce for the generation of structured light, this geometric phase results in a space-varying phase dependence imparted on the outgoing optical beam. This can be used to produce OAM beams, vector vortex beams, or arbitrary optical states of light as in the magic window and optimal diffractive

focusing papers below [11–14]. The so called *q-plates* have an azimuthally symmetric liquid crystal orientation with topological charge of "q". A $q = 1/2$ plate has liquid crystals which go from an orientation of 0 degrees, to 90 degrees upon a half turn azimuthally, and then back to 0 degrees (or equivalently 180 degrees). We can describe the action of a general PBOE with liquid crystal orientation $\alpha(x, y)$ by

$$\begin{bmatrix} \mathbf{e}_L \\ \mathbf{e}_R \end{bmatrix} \underset{\longrightarrow}{\text{QP}} \cos\left(\frac{\delta}{2}\right) \begin{bmatrix} \mathbf{e}_\text{L} \\ \mathbf{e}_\text{R} \end{bmatrix} + \text{i}\sin\left(\frac{\delta}{2}\right) \begin{bmatrix} \mathbf{e}_\text{R}\, e^{+2i\alpha(x,y)} \\ \mathbf{e}_\text{L}\, e^{-2i\alpha(x,y)} \end{bmatrix}, \tag{2.9}$$

where $\delta$ is the tuning parameter which is modulated by applying an AC voltage across the plate, and $\mathbf{e}_\text{R}$ and $\mathbf{e}_\text{L}$ are the right and left circularly polarized components of the electric field. This allows for control over the phase and or the polarization of the output beam depending on the polarization sent incident on the q-plate. If we go with a left polarized Gaussian input, and tune the voltage of the q-plate such that $\delta = \pi$, then the action of the q-plate becomes $\mathbf{e}_L \underset{\longrightarrow}{\text{QP}} \mathbf{e}_R e^{+2i\alpha(x,y)}$. Now if the device is fabricated such that the orientation of the liquid crystals is azimuthally symmetric, $\alpha(x, y) = \ell\phi/2$ then we will generate an output which has the opposite handed circular polarization and an $i\ell\phi$ phase dependence, corresponding to an OAM carrying beam with angular momentum of $\ell\hbar$ per photon. If instead of a circular polarization input we have some linear polarization, which is a combination of $\mathbf{e}_L$ and $\mathbf{e}_R$, an interesting polarization pattern will be produced which is determined by the phase relationship of the output left and right-circular component. In the case of a $q = 1/2$ plate, these output modes are called the azimuthally and radially polarized states and the star and lemon states, and are generated by an incident horizontal, vertical, diagonal, and anti-diagonal polarization. These polarization *vector-vortex* modes are orthogonal and can be used for information encoding instead of the OAM as we have demonstrated in underwater and free-space channels [15,16]. These structured polarization states are also interesting for various applications in light-matter interaction for microscopy, optical tweezers, and coherent control [17–19].

For the optimal focusing paper below, we want to produce a uniformly polarized output with amplitude modulation. Because of the ability to tailor the output polarization using

the q-plate, we can consider using these devices to modulate the amplitude of a beam by placing a polariser after the output. Writing the action of the PBOE in a different form for a horizontal or vertical polarised input, we can see the following effect

$$\begin{aligned}\hat{\mathcal{U}}_q \quad \cdot \quad & \begin{pmatrix}\mathbf{e}_{\mathrm{H}}\\ \mathbf{e}_{\mathrm{V}}\end{pmatrix} = \cos\left(\frac{\delta}{2}\right)\begin{pmatrix}\mathbf{e}_{\mathrm{H}}\\ \mathbf{e}_{\mathrm{V}}\end{pmatrix} \\ + \quad & \mathrm{i}\sin\left(\frac{\delta}{2}\right)\begin{pmatrix}\cos\left(2\alpha(x,y)\right) & \sin\left(2\alpha(x,y)\right)\\ \sin\left(2\alpha(x,y)\right) & -\cos\left(2\alpha(x,y)\right)\end{pmatrix}\begin{pmatrix}\mathbf{e}_{\mathrm{H}}\\ \mathbf{e}_{\mathrm{V}}\end{pmatrix}. \end{aligned} \tag{2.10}$$

Again as a particular example consider sending a single input polarisation such as $\mathbf{e}_H$ with a horizontal polariser placed after the plate, and tuning the voltage to give $\delta = \pi$ we see that the action becomes $\mathbf{e}_H \xrightarrow{\mathrm{QP}} \mathbf{e}_H \cos(2\alpha(x,y))$. Thus we can determine the liquid crystal orientation needed to give some normalized amplitude field $A(x,y)$ for a horizontally polarised beam by $\alpha(x,y) = 1/2 \arccos(A(x,y))$.

## 2.4 Device fabrication and characterization

The liquid crystal devices that we fabricate consist of a 4.8 $\mu$m thick liquid crystal cell contained by 2 indium tin oxide (ITO) coated glass plates, which are spin-coated with a thin photoalignment layer. This layer is used in the fabrication process to determine the orientation of the liquid crystals in the device. The first step is to spin-coat the ITO glasses with the photoalignment material PAAD-22 from BEAM Co. This substrate has peak absorption at 366 nm which allows for use of the device at wavelengths above 500 nm without affecting the alignment of the substrate. Next the two glasses are glued together, with care being taken to ensure that they are glued parallel to each other such that the liquid crystal cell has a uniform thickness around the entire area of operation. The plate now has the photoalignment coating but the liquid crystal has not yet been added. We now illuminate the plate with a 405 nm laser source which first reflects off a digital micro-mirror device (DMD), and then passes through a half-wave plate. The 600 by 600 pixel DMD allows us to illuminate the plate with single pixel precision and the HWP lets us

control the polarization of the incoming light. The substrate aligns with the input UV light and thus we are able to control the orientation of the molecules and consequently the liquid crystal with single pixel precision. The face of the DMD is imaged onto the plate and with either magnification or demagnification we can adjust the size or precision of the device's effective area. The substrate is exposed to the polarized UV radiation for 30 or more minutes at each polarization / pixel setting, and then the liquid crystal can be added to the cell and the cell is sealed with epoxy [11].

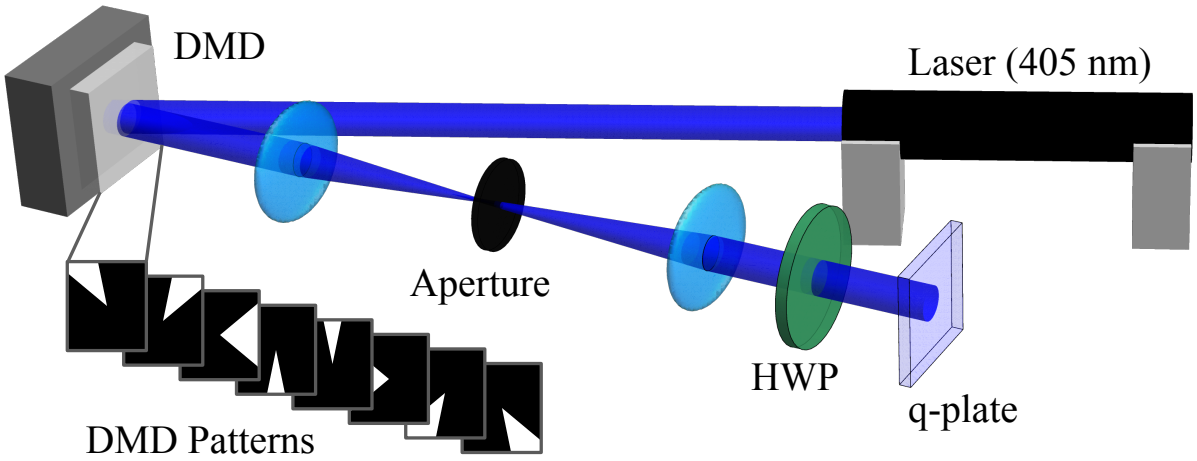


Figure 2.3: **Generation of liquid crystal devices**. A 405 nm laser is used along with a digital micromirror device (DMD) and a half-wave plate to give pixel-by-pixel precision in determining the liquid crystal orientation.

The challenges in fabricating the liquid crystal devices is primarily in achieving perfect imaging of the DMD onto the device, glueing the plates together with uniform thickness, and in choosing the patterns for the fabrication process. In principle we are limited only by the precision of our wave-plate rotation and the number of pixels. However, we also need to consider the effect of having patterns with regions of single pixels which may lead to an overlapping effect if there is imperfection in imaging the DMD. In both the magic window and focusing papers we go with a pattern set consisting of around 20 different polarization

settings and thus 20 phase/amplitude steps.

Once the device has been created, we must determine the desired tuning voltage to give $\delta = \pi$ resulting in the device being "perfectly tuned" giving full conversion from left- to right-circular polarization and thus imparting the entire beam with the desired phase. The tuning voltage is wavelength dependent, as it alters the total birefringence of the liquid crystal cell. This allows a single device to be useful at different optical wavelengths. To find the optimal tuning voltage we can place the device between cross polarisers along with quarter-wave plates to measure circular polarisation and maximize the transmission, i.e., maximizing the conversion from left- to right-circular polarization. Then depending on the application we can either characterize the intensity of the output beam using a camera, or we can make phase measurements by interfering the output beam with a Gaussian beam and observing the interference pattern. For an OAM beam if we interfere with a Gaussian beam at some non-zero angle this will result in the pitchfork hologram which we are familiar with as they are used to generate these OAM modes on an SLM. If the interfering beam is co-linear then we will see a spiral pattern with opposite handedness depending on the OAM having a positive or negative charge.

The rest of this chapter presents 2 articles on liquid crystal device fabrication. The first paper shows the implementation of liquid crystal devices to produce magic windows which can form arbitrary intensity images which remain visible upon propagation. The second work outlines a new formulation for optimal diffractive focusing, and includes an experimental demonstration using liquid crystal devices. The diffractive focusing abilities of an aperture or the Fresnel zone plate have been studied extensively including investigations into continuous zone plates with a variable amplitude following a sine or cosine function instead of discreet amplitude jumps between opaque and transparent zones [20–22]. The result presented below improves on these classic diffractive focusing methods.

Research Article Vol. 9, No. 5 / May 2022 / Optica 479


# Flat magic window

Felix Hufnagel,[1,*] Alessio D'Errico,[1,3] Hugo Larocque,[2] Fatimah Alsaiari,[1] Jeremy Upham,[1] and Ebrahim Karimi[1]

[1]Department of Physics, University of Ottawa, 25 Templeton street, Ottawa, Ontario K1N 6N5, Canada
[2]Research Laboratory of Electronics, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
[3]e-mail: [redacted]
*Corresponding author: [redacted]

Received 19 January 2022; revised 14 March 2022; accepted 16 March 2022; published 5 May 2022

**Magic windows (or mirrors) consist of optical devices with a surface deformation or thickness distribution devised in such a way to form a desired image. The associated image intensity distribution has been shown in previous works to be related to the Laplacian of the height of the surface relief. Exploiting the Laplacian theory to calculate the needed phase pattern, we experimentally realize such devices with flat optics employing optical polarization-wavefront coupling, which represent a new paradigm for light manipulation. The desired pattern and experimental specifications for designing the flat optics was implemented with a reconfigurable spatial light modulator, which acted as the magic mirror. The flat plate, an optical polarization-wavefront coupler, is then fabricated by spatially structuring nematic liquid crystals. The plate is used to demonstrate the concept of a polarization-switchable magic window, where, depending on the input circular polarization handedness, one can display either the desired image or the image resulting from the negative of the window's phase.** 

https://doi.org/10.1364/OPTICA.454293

## 1. INTRODUCTION

The mechanism behind ancient magic mirrors from China and Japan was not understood until the 20th century, despite the earliest creations of these artistic pieces dating back to 2000 BC [1]. The cast bronze mirrors presented as normal mirrors while viewing one's reflection. However, when sunlight was shone directly on the mirror, it acted as a subtly parabolic mirror forming an image—corresponding to patterning on the back side of the mirror—presented on the floor or a screen [2]. A similar phenomenon can be observed in the reflection of the sun off large windows and onto a street below. Though the window appears flat and does not significantly distort an image while we look through it, the slight deformations from tension around the edges result in a nonuniform reflection onto the ground in the shape of an "$X$"-pattern. Despite deriving from a millennia old tradition, magic mirrors inspired a measurement technique (called Makyoh topography after the Japanese word for "wonder mirror") for detecting surface deformities in silicon wafers in the late 20th century [3,4]. This approach has the advantage of being very simple and practical for industry-based applications, in comparison with other measurement techniques such as interferometry or atomic force microscopy [5].

The magic mirror effect can be quantitatively explained through standard diffraction theory [3]. However, the final understanding of how images are formed from the magic mirrors was derived in 2005 by Sir Michael Berry [1]. Here, it was shown that the intensity of the image is given to the first-order approximation by the Laplacian of the height of surface reliefs on the mirror. The principle of the magic mirror can be applied to devices working in transmission, the so-called "magic windows," which can produce a similar effect forming the Laplacian image through very slight thickness deformations [6]. Specifically, the surface should be "smooth" enough, with gentle variations, such that caustics are not formed before the image appears. It is shown that the intensity of the Laplacian image is given in terms of the height of the surface relief, $h$, by $I_{\text{Laplacian Mirror}}(\mathbf{r}, Z) \simeq 1 + Z\nabla^2 h(\mathbf{r})$ [1]. Here, $Z = 2D/M$ and $\mathbf{r} = R/M$ are the rescaled distance along the propagation direction and transverse position from the center of the mirror, respectively, normalized to the magnification of the convex mirror $M$. $D$ and $R$ are the distances from the mirror and transverse position of the image, respectively. The Laplacian image produced from a magic window, however, depends on the relative refractive index of the window, $n$, in addition to the height of the surface relief, $h$, which is given by [6]

$$I_{\text{Laplacian Window}}(\mathbf{R}, z) \simeq 1 - z(n-1)\nabla^2 h(\mathbf{R}). \tag{1}$$

Here $z$ is the distance of the image plane from that of the window, and $R$ is the transverse distance from the center of the window. Given any image, we can, thus, find the necessary surface of the magic window or mirror by solving the Poisson equation in the transverse plane. A remarkable property of magic mirrors or windows is that, in contrast with conventional windows and lenses, the image can be observed in several observational planes without a substantial change in sharpness.

There has been recent interest in the problem of shaping light intensity often referred to as freeform optics [7]. In this work, we

show how magic mirrors/windows can be implemented with flat optical devices. We use liquid crystal (LC) based devices, a reflective spatial light modulator (SLM), and a Pancharatnam–Berry optical phase element (PBOE) [8] to construct our magic mirror and magic window, respectively. We also exploit the Laplacian theory, which gives a simpler and more direct approach to calculate the desired phase patterns in contrast with more elaborate techniques, e.g., caustic design [9]. Figure 1(a) illustrates how these two types of LC devices can be programmed or fabricated to act as the reflective or transmissive surfaces shown in Fig. 1(b). Both types of devices rely on the uniaxial birefringence of its constituent nematic LCs to implement the magic mirror/window effect. On one hand, standard LC on silicon SLMs rely on a reflective back-plane that rotates LCs about an axis perpendicular to the direction of propagation of an incident optical beam. The resulting optical medium is, thus, defined by two linear polarization eigenstates. The first is along the rotation axis and is defined by a refractive index of $n_o$, the ordinary refractive index of the LCs. The second is orthogonal to the propagation direction of the beam and to the rotation axis, and it has a refractive index of $n(\chi) = ((\cos^2\chi)/n_o^2 + (\sin^2\chi)/n_e^2)^{-1/2}$, where $n_e$ and $\chi$ are the extraordinary index and the rotation angle of the LCs, respectively. Therefore, by exposing an SLM to an optical beam polarized along this second direction, we can impart a transverse phase profile onto the beam controlled by the relative angle of the LC in the display. An SLM can, thus, operate like a magic mirror if its programmed transverse phase profile replicates that attributed to the height profile of the mirror. On the other hand, LCs in PBOEs are rotated about an axis parallel to the direction of propagation of an optical beam. The resulting polarization eigenstates are, thus, either aligned or orthogonal to the orientation axis of the LCs and have indices of $n_e$ and $n_o$, respectively. When the thickness of this system imparts a $\pi$ phase shift between these two linear polarizations, then, as prescribed by Jones calculus, an incident circularly polarized beam experience a phase shift of $\pm 2\chi$ accompanied by a flip in handedness upon propagating such a LC

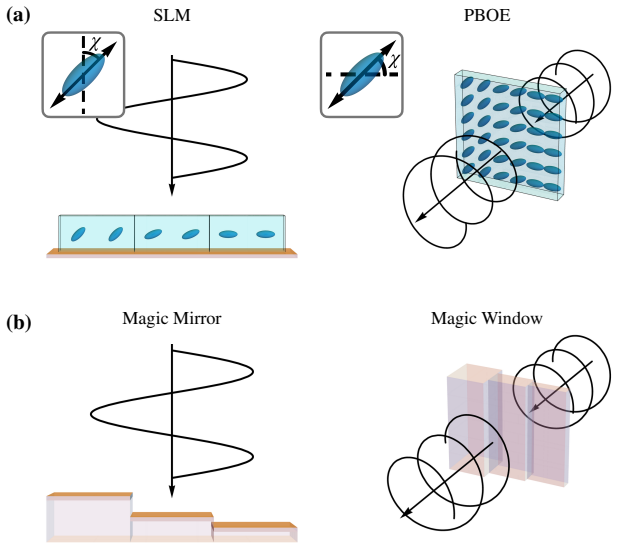


**Fig. 1.** Magic optics with liquid crystal displays. (a) Operation principle of SLMs and liquid crystal PBOEs. Both types of displays rely on rotated liquid crystals to impart a transverse phase profile onto an incident light beam. The SLM relies on out-of-plane rotations to impart a phase onto linearly polarized light whereas the PBOE relies on in-plane rotations to add a phase onto circularly polarization light at the expense of flipping its handedness. (b) Corresponding surfaces that are classically considered in magic optics.

cell, where $\chi$ is the rotation angle of the LCs. PBOEs leverage this phenomenon by rotating the orientation angle of the LCs across a transmissive optical display such as to impart a desired phase profile onto a circularly polarized beam. Thus, a LC PBOE acts like a magic window if it has a LC orientation pattern that produces the same phase profile as that induced by the thickness variations of the window. PBOEs, through an effect known as light's spin-to-orbital angular momentum coupling [10], also allow us to implement a polarization dependent phase distribution. Thus, one can observe the image resulting from the phase or its negative by switching the input polarization from left to right circular. In addition, the introduced topic of spin-to-orbit coupling allows one to explore the complex patterns of polarization singularities when the LC magic plate is illuminated with a linear superposition of left- and right-handed circular polarization. There have been many investigations into singular optics, arising from such polarization singularities, introduced in polarization system such as Stokes singularities, polarization knots, and links [11–14]. It is, thus, interesting to reconstruct the polarization topology of the images formed by a LC magic plate. In particular, we track the trajectory in the three-dimensional space of C-point singularities, i.e., loci of circular polarization. We show that C-points accumulate in points of the transverse plane where the image is forming.

## 2. LIQUID CRYSTAL MAGIC MIRROR

The magic mirror is realized using a Hamamatsu SLM with a screen resolution of 800 by 600 pixels. Figure 2(b) shows the detail of the experimental setup for both magic mirror and magic plate. Given the desired image, the required phase pattern for the mirror is computed. There is a freedom to increase the steepness of the pattern, i.e., increasing the number of times the phase pattern goes from 0 to $2\pi$. This can be seen as altering the concavity of the mirror, which results in changing how quickly the image is formed. In practical settings, care must be taken in choosing the window size and phase steepness. Due to beam divergence, an image that forms too slowly will lose its sharpness. At the same time, the pattern must be smooth enough such that caustics are not formed before the image plane [6]. The phase pattern was uploaded to the SLM with the addition of a vertical grating. The SLM is shined with a laser beam with an enlarged Gaussian beam shape to mimic an input, coherent, plane wave. The first order of diffraction is selected, filtering out the rest using an iris in the center of a $4-f$ lens system, to remove unconverted light resulting from inefficiencies in the SLM. In addition to selecting the first order of diffraction, the $4-f$ lens system is also used to image the SLM plane and probe the intensity at different propagation distances. The evolution of the intensity distribution is recorded on a CMOS camera from the plane of the SLM down to the image formation planes. Additional planes were also imaged beyond the latter to capture the formation of caustics. The implementation of three SLM magic mirrors is shown in Fig. 3, where the intensity distribution smoothly evolves from the input beam profile to the desired image pattern.

The goal of the experiment is to show a magic mirror and magic plate, encoded using the Laplacian theory, using LC technology in an SLM and PBOE. To achieve this, we must generate the phase pattern corresponding to the chosen intensity image. This phase pattern is then displayed on the SLM and PBOE. The image patterns that we use are converted to a bitmap form such that the pixels contain only a 1 or 0 for the intensity [see Fig. 2(a)]. Based on Eq. (1), the discretized intensity function $I(\mathbf{R}, z)$ is then used

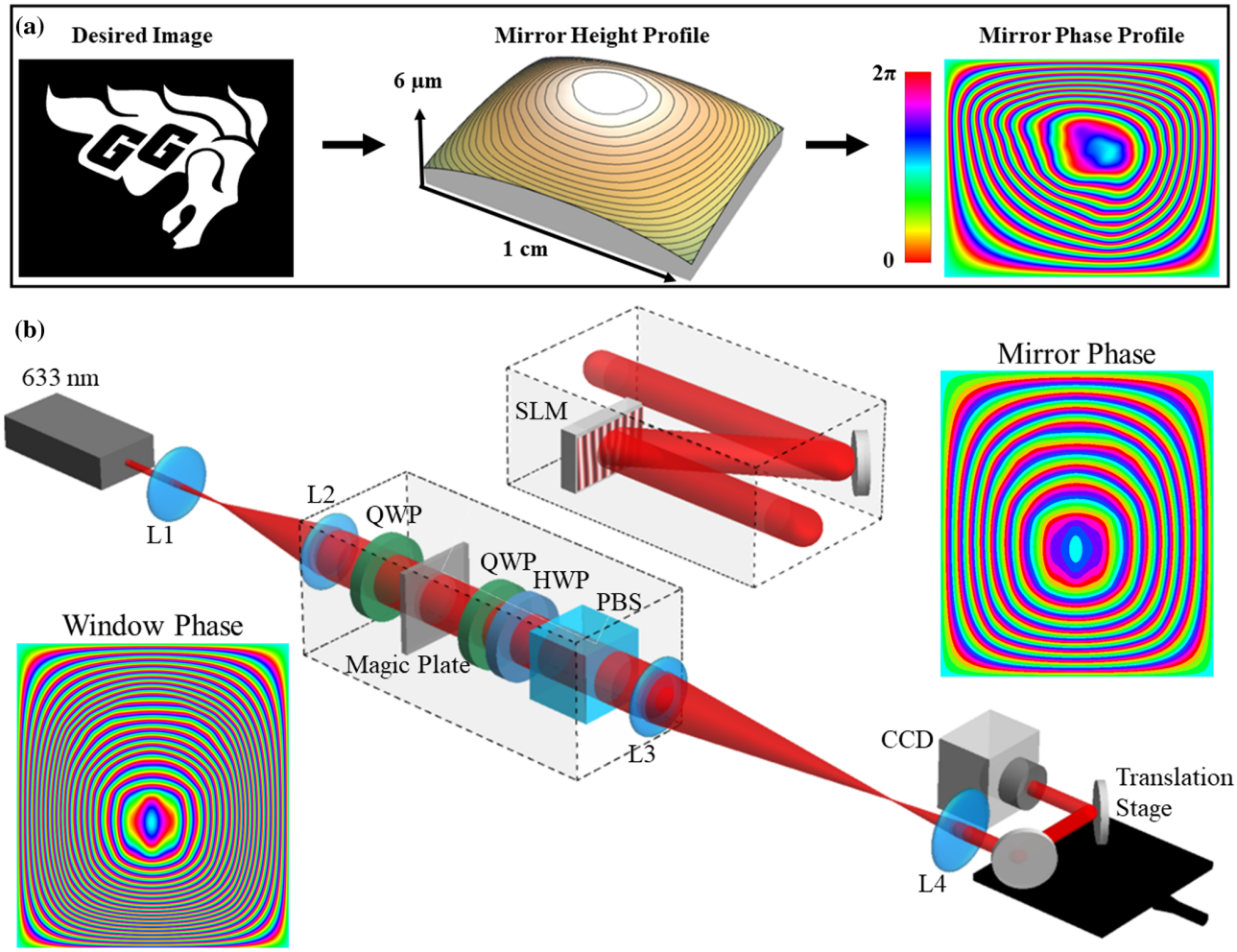


**Fig. 2.** Calculation principle of phase patterns and experimental setup. In (a) we illustrate the steps used to calculate the phase pattern needed for generating a desired image. The BMP image of the desired intensity is used to calculate the mirror height using the discrete sine transform to solve Eq. (1). The maximum height for the window corresponding to the Gee-Gees logo is 6 μm as shown. The mirror height is then used to calculate the mirror phase by taking the modulus for the specific wavelength, i.e., Phase = Mod(Height/$(2\pi\lambda)$, $2\pi$). In (b) we show the experimental setup. A 633 nm He–Ne laser was used for characterizing the magic mirror and magic plate. The setup for the magic mirror **b** consists of a SLM with a resolution of 600 by 800 pixels. After the SLM, a $4-f$ system is used to image the pattern displayed on the SLM, allowing for us to both make measurements starting precisely from the SLM plane and also filter out the first diffraction order using a pinhole placed at the focus of the $4-f$ system. Following the $4-f$ lens system, two mirrors are placed on a translation stage to construct a trombone, which is followed by a CMOS camera. In the magic window setup, the PBOE is placed in the same plane as the SLM. The addition of a QWP before and a QWP, HWP, and PBS after is required to perform polarization tomography on the output beam of the magic window. The phase pattern used for the University of Ottawa logo is shown for the magic window and mirror.

to find the height of the surface relief $h(\mathbf{r})$, where $\mathbf{r}=\mathbf{r}(\mathbf{R})$ at the image plane. The inverse of the Laplacian is solved numerically with Dirichlet boundary conditions using the two-dimensional discrete sine transform [1]. In the case of flat optics, we are not varying the height of the window, but rather the index of refraction $n(\mathbf{r})$. Thus, Eq. (1) becomes $I_{\text{Magic Plate}}(\mathbf{R}, z)=1+hz\nabla^2 n(\mathbf{R})$, where $n(\mathbf{r})$ is the transverse spatially dependent index of refraction of the plate, $h$ is again the height of the plate though it is now a constant, and $z$ is the distance from the image plane to the window. The resulting window phase pattern, as shown in Fig. 2(a), is plotted in radians.

## 3. LIQUID CRYSTAL MAGIC PLATE

As the next step, we bring together the concepts of magic window imaging and photonic polarization-wavefront coupling. Such a device, which we call the spin–orbit magic plate, is based on PBOEs, i.e., slabs of uniaxial anisotropic materials (LCs, in our case) with an extraordinary axis orientation that is spatially varying in the plate's plane. The action of a PBOE element with extraordinary axis orientation $\chi(\mathbf{r})/2$ and (spatially uniform) retardation $\delta$ is given by

$$\mathbf{e}_{\pm}\underset{\longrightarrow}{\text{MP}}\cos\left(\frac{\delta}{2}\right)\mathbf{e}_{\pm}+i\sin\left(\frac{\delta}{2}\right)\mathbf{e}_{\mp}e^{\pm i\chi(r)}, \tag{2}$$

where $\mathbf{e}_+$ and $\mathbf{e}_-$ stand for the left and right circular polarization unit vectors, respectively. The sample optical retardation, $\delta$, can be tuned by applying an AC voltage to the plate. Here, we can see that a perfectly tuned PBOE with $\delta=\pi$ results into the complete conversion of the input circular polarization to the opposite handedness with the addition of the desired phase $\pm\chi(\mathbf{r})$, where $\chi(\mathbf{r})$ is the inverse Laplacian of the image. Therefore, by flipping the incident polarization state from left- to right-handed, one can

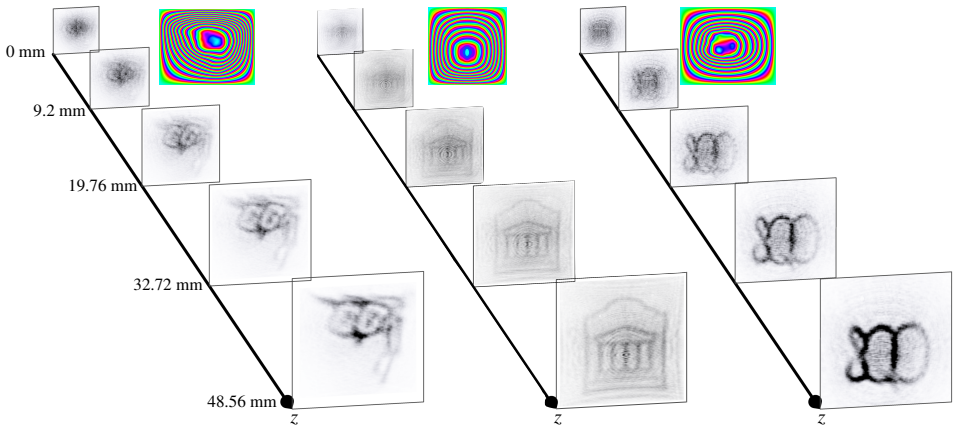


**Fig. 3.** Intensity images recorded at different propagation distances after reflection from an SLM-based magic mirror. The first image at the back shows the SLM plane, where there is a uniform intensity pattern. The propagation shows the contrast of the image improving upon propagation away from the SLM. The insets show the phase distributions, for the three different examples, encoded on the SLM in hue colors, which encode a phase range from 0 to $2\pi$. Videos showing the free space evolution of the above images can be found in Visualization 1, Visualization 2, and Visualization 3.

gain a $+\chi(\mathbf{r})$ and $-\chi(\mathbf{r})$ phase at the output, respectively. Due to the different signs in the phase, the two circular polarization components propagate in different ways, as dictated by the Fresnel diffraction integral, $E_{\pm}(\mathbf{r}, z) = \int K(\mathbf{r}, \mathbf{r}', z) E_{\pm}(\mathbf{r}', 0) d^2\mathbf{r}'$, where $K(\mathbf{r}, \mathbf{r}', z) = \exp[ik|\mathbf{r} - \mathbf{r}'|^2/2z] e^{ikz}/i\lambda z$. From $K(\mathbf{r}, \mathbf{r}', z) = K^*(\mathbf{r}, \mathbf{r}', -z)$, one can see that $E_+(\mathbf{r}, z) = E_-^*(\mathbf{r}, z)$. As a consequence, if one circular polarization experiences the formation of an image, which is being focused due to the radial variation in $\chi(\mathbf{r})$, the opposite circular polarization will be defocused, and the image [from Eq. (1)] will be the negative. The University of Ottawa logo was chosen to be used for the spin–orbit magic plate. The phase pattern written on the plate for the magic window is shown in Fig. 2 with the experimental setup. The plate is fabricated in our own LC facility [8]. A pair of ITO glass plates are spin-coated with a polyamide. The ITO plates then are kept at 4 μm distance using spacers and are glued to each other with epoxy glue. The chosen polyamide can be photoaligned through illumination from linearly polarized UV light. We are able to control the orientation of the polyamide by changing the polarization of an incident UV-beam on a pixel-by-pixel basis by using a digital micromirror device (DMD). The pattern written on the polyamide dictates the orientation of the LC molecules, which are added between the plates in the successive stage. The pattern was written with 32 phase steps, thus 32 polarization settings illuminating different parts of the plate. We characterized the action of the fabricated plate illuminating it with both spatially incoherent and coherent light. The magic plate optical retardation was set to $\delta = \pi$ by applying an AC voltage. As a source with low transverse spatial coherence, we used a LED, followed by a polarizing beam splitter, to illuminate the magic plate. The light was filtered with a bandpass filter centered at 633 nm (which increases the longitudinal coherence but does not affect the transverse spatial coherence). We choose the input polarization to be either linear or right/left circular by using a quarter-wave plate before illuminating the magic plate. The transmitted intensity was recorded on the CMOS camera. With the linear polarized input, we observe the simultaneous formation of the University of Ottawa logo and its negative image (with an imperfect overlap due to polarization dependent lensing), as shown in Fig. 4(a). The appearance of the negative image is due to the input right circular polarization component, which gains the phase $-\chi(\mathbf{r})$ [this has the effect of flipping the relative sign in Eq. (1)]. It is possible to isolate the image or its negative by choosing input left or right circular polarization, respectively [Fig. 4(a)]. In Fig. 4(b), we show theoretical simulation of the intensity evolution from a source with low transverse coherence. The source was simulated by sampling the transverse plane in regions where all the pixels are in phase and imposing random phase noise between the different regions. The transverse coherence length was, thus, proportional to the region width, which we fixed at 15 pixels. The simulations show the results averaging over 200 realizations of the random noise (uniformly distributed between 0 and $2\pi$). Similar effects are observed in the case of illumination with a coherent laser beam. We used a He–Ne laser ($\lambda = 633$ nm) prepared with left/right circular or linear polarization. The resulting intensity in the case of input left circular polarization corresponds to the desired pattern [Figs. 4(c) and 4(d)]. We also observe fringes due to the transverse coherence of the source. As in the incoherent illumination case, an input right circular polarization gives rise, within the magic window theory approximations, to the negative of the desired image. When a beam with linear polarization is sent onto the magic plate, as opposed to one of the circular polarizations, the resultant image is a coherent linear combination of the images one would achieve from a left and right circular input. Moreover, the magic plate optical retardation $\delta$ can be altered to not be $\pi$, but any other values. In Figs. 4(e) and 4(f), we show how, by tuning the optical retardation $\delta$, we can switch, at a given plane, between the input beam intensity distribution and the image encoded in the plate. The interplay between source coherence and polarization-conditioned action of the device leads to the formation of polarization singularities during the beam propagation. When an electric field has a non-uniform polarization pattern, an interesting phenomenon can arise whereby the polarization azimuth is undefined [15–17]. These singularities of the complex scalar field are called C-points. C-points are loci of exactly circular polarization; thus, the orientation of the major axis of the polarization ellipse cannot be defined. When the magic plate is illuminated by linearly polarized light, the outgoing beam has both the right and left circular component, whose propagation is dictated by, respectively, the plate phase and the negative of the plate phase. The intensity patterns of these two components evolve differently: if one of them experiences

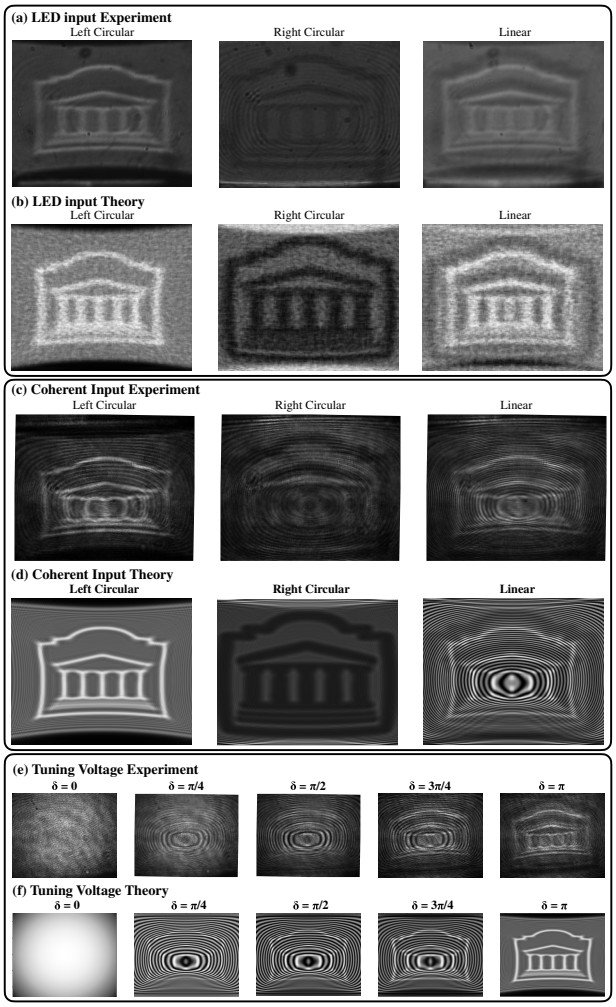


**Fig. 4.** Working principle of a flat spin–orbit magic plate. In (a) and (b) we show the intensity distributions of light transmitted by the plate with different polarization inputs from a LED source with low transverse coherence. The resulting image from the linear input is the sum of the left and right circular contributions. The image resulting from the right circular input is not an exact negative of the left circular because it experiences a slight defocusing from the window while the left component is slightly focused. In (c) and (d) we show the intensity distributions of light transmitted by the plate with different polarization inputs: left circular, right circular, and linear polarization from and a 633 nm He–Ne laser. See also Visualization 4 for the free space evolution. Panels (e) and (f) show the images resulting from different $\delta$ across the plate as given by Eq. (2), with the left circular polarization input. When $\delta = 0$, there is no conversion from left- to right-handed polarization; thus, the beam does not acquire the phase of the magic window. When $\delta = \pi$, the input polarization is fully converted; thus, we see the desired image. Tuning parameters between 0 and $\pi$ result in partial conversion, and we see interference between the intensity profile of the converted beam and the input beam.

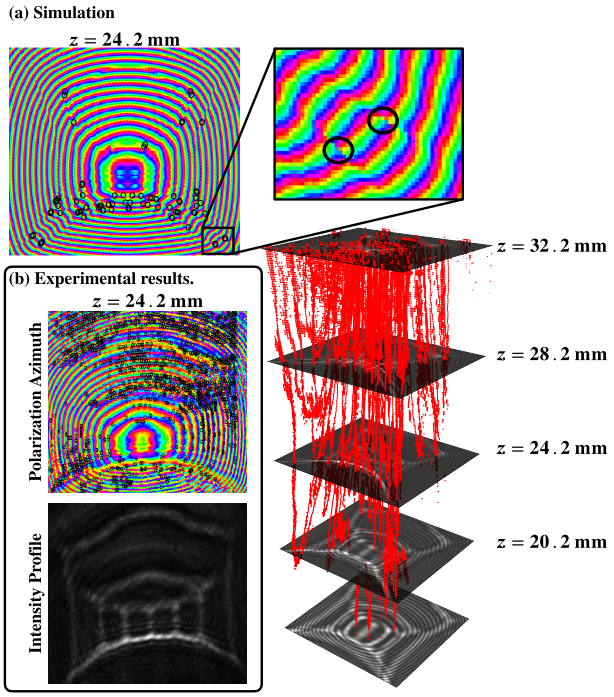


**Fig. 5.** In (a), we show simulation of the propagation of C-points from the spin–orbit magic plate. The red points in the three-dimensional graphics show the C-point trajectory along the propagation of the beam. The intensity profiles are shown at different propagation planes. The two-dimensional plot above represents the polarization azimuth, where C-points are labeled with black circles. The inset shows a magnified image of the polarization azimuth where the singularities are clearly visible at the location where the polarization azimuth is undefined. Upon close observation, we can see that these singularities have opposite charge. The hue color coding corresponds to polarization azimuth values ranging from 0 to $\pi$. In (b), we show the experimentally reconstructed polarization azimuth obtained through polarization tomography. The tracking of C-points here is very sensitive to the camera resolution as well as the exposure time, particularly in the regions of low intensity. We are, however, still able to see singularities form in the predicted areas, particularly along the bottom of the logo.

a focusing effect, the other circular component has a divergent intensity pattern. As a consequence of the different propagations, in particular the formation of diffraction fringes with different distributions for the two circular polarizations, C-points will arise in regions where only one of the two components has a zero intensity. This is a general feature that can be observed in PBOE elements with a radially varying phase. The interaction of these two co-propagating beams gives rise to C-points with different topological charges. In the plane of the LC magic plate, the polarization remains uniformly linear, since we still have a uniform intensity distribution, albeit with a different phase for the left and right components, i.e., $(e^{+i\chi(\mathbf{r})}\mathbf{e}_- + e^{-i\chi(\mathbf{r})}\mathbf{e}_+)/\sqrt{2}$. Here $\chi(\mathbf{r})$ is the spatially dependent phase imparted on the beam by the magic plate. The phase given to the right component is, thus, the negative of that gained by the left component. It is not until propagation to the image plane where differences in the diffraction pattern of the right and left components result in the appearance of the polarization C-points, as shown in Figs. 5(a) and 5(b). Due to conservation of total topological charge, C-points appear at given planes in pairs with opposite topological charges. The free-space dynamics of the C-points generated here is rich and requires individual investigation.

## 4. CONCLUSION

In summary, we have realized a LC-based magic plate exploiting the principle of light manipulation with flat optics, where the impinging light wavefront is modulated by an inhomogeneous refractive index distribution. By exploiting the physics of patterned anisotropic media, we fabricated a flat spin–orbit magic plate. This device, depending on whether the input polarization is circularly

left- or right-handed, creates a desired pattern or its negative, respectively. The flat magic plate can be tuned for operation at different wavelengths since its optical retardation can be adjusted by applying an external electric field to the plate. While we used this device under monochromatic illumination, in principle it can work as well under broadband illumination, if one carefully selects only the converted contribution by means of achromatic wave plates and polarizing beam splitters, even though the conversion efficiency will not be uniform at the different wavelengths. The working principle was demonstrated for both incoherent and coherent sources. In the latter case, interference effects lead to the formation of polarization singularities (C-points). Our experiment was based on the use of LC devices with thickness of several wavelengths. However, as it has been shown in [18,19], PBOEs can also be realized with dielectric metasurfaces with thickness smaller than the wavelength. Furthermore, one could consider using achromatic and polarization-insensitive metasurfaces to form magic windows and further reduce the wavelength dependence of the devices [20]. Hence, our results also introduce the possibility of scaling down the thickness of these flat magic windows to sub-wavelength scales.

**Funding.** Ontario Early Research Award; Natural Sciences and Engineering Research Council of Canada; Canada First Research Excellence Fund; Canada Research Chairs.

**Acknowledgment.** E. K. acknowledges the fruitful conversation with Sir Michael Berry. This work was supported by Canada Research Chairs, Ontario Early Research Award (ERA), Canada First Research Excellence Fund (CFREF), and Natural Sciences and Engineering Research Council of Canada (NSERC).

**Disclosures.** The authors declare no conflicts of interest.

**Data availability.** Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

## REFERENCES

1. M. V. Berry, "Oriental magic mirrors and the Laplacian image," Eur. J. Phys. **27**, 109–118 (2005).
2. W. E. Ayrton and J. Perry, "II. The magic mirror of Japan. Part I," Proc. R. Soc. London **28**, 127–148 (1879).
3. K. Kugimiya, "Characterization of polished surfaces by 'Makyoh,'" J. Cryst. Growth **103**, 461–468 (1990).
4. Z. J. Laczik, "Quantitative Makyoh topography," Opt. Eng. **39**, 2562–2567 (2000).
5. K. Kugimiya, "Characterization of polished mirror surfaces by the 'Makyoh' principle," Mater. Lett. **7**, 229–233 (1988).
6. M. V. Berry, "Laplacian magic windows," J. Opt. **19**, 06LT01 (2017).
7. M. Brand and D. A. Birch, "Freeform irradiance tailoring for light fields," Opt. Express **27**, A611–619 (2019).
8. H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R. W. Boyd, and E. Karimi, "Arbitrary optical wavefront shaping via spin-to-orbit coupling," J. Opt. **18**, 124002 (2016).
9. Y. Schwartzburg, R. Testuz, A. Tagliasacchi, and M. Pauly, "High-contrast computational caustic design," ACM Trans. Graph. **33**, 74 (2014).
10. E. Cohen, H. Larocque, F. Bouchard, F. Nejadsattari, Y. Gefen, and E. Karimi, "Geometric phase from Aharonov–Bohm to Pancharatnam–Berry and beyond," Nat. Rev. Phys. **1**, 437–449 (2019).
11. F. Flossmann, O. Kevin, M. R. Dennis, and M. J. Padgett, "Polarization singularities in 2D and 3D speckle fields," Phys. Rev. Lett. **100**, 203902 (2008).
12. H. Larocque, D. Sugic, D. Mortimer, A. J. Taylor, R. Fickler, R. W. Boyd, M. R. Dennis, and E. Karimi, "Reconstructing the topology of optical polarization knots," Nat. Phys. **14**, 1079–1082 (2018).
13. M. Dennis, "Polarization singularities in paraxial vector fields: morphology and statistics," Opt. Commun. **213**, 201–221 (2002).
14. F. Cardano, E. Karimi, L. Marrucci, C. de Lisio, and E. Santamato, "Generation and dynamics of optical beams with polarization singularities," Opt. Express **21**, 8815–8820 (2013).
15. J. F. Nye and J. Hajnal, "The wave structure of monochromatic electromagnetic radiation," Proc. R. Soc. London. A **409**, 21–36 (1987).
16. J. F. Nye, *Natural Focusing and Fine Structure of Light: Caustics and Wave Dislocations* (CRC Press, 1999).
17. M. R. Dennis, K. O'Holleran, and M. J. Padgett, "Singular optics: optical vortices and polarization singularities," Prog. Opt. **53**, 293–363 (2009).
18. E. Karimi, S. A. Schulz, I. De Leon, H. Qassim, J. Upham, and R. W. Boyd, "Generating optical orbital angular momentum at visible wavelengths using a plasmonic metasurface," Light Sci. Appl. **3**, e167 (2014).
19. R. C. Devlin, A. Ambrosio, N. A. Rubin, J. B. Mueller, and F. Capasso, "Arbitrary spin-to–orbital angular momentum conversion of light," Science **358**, 896–901 (2017).
20. W. T. Chen, A. Y. Zhu, J. Sisler, Z. Bharwani, and F. Capasso, "A broadband achromatic polarization-insensitive metalens consisting of anisotropic nanostructures," Nat. Commun. **10**, 355 (2019).

# Optimal Diffractive Focusing of Quantum Waves

Maxim A. Efremov,[1,2] Felix Hufnagel,[3] Hugo Larocque,[3,4] Wolfgang P. Schleich,[2,5] and Ebrahim Karimi[3]

[1] *German Aerospace Center (DLR), Institute of Quantum Technologies, 89081 Ulm, Germany*
[2] *Institut für Quantenphysik and Center for Integrated Quantum Science and Technology (IQST), Universität Ulm, 89081 Ulm, Germany*
[3] *Nexus for Quantum Technologies, University of Ottawa, K1N 5N6, Ottawa, ON, Canada*
[4] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[5] *Hagler Institute for Advanced Study at Texas A&M University, Texas A&M AgriLife Research, Institute for Quantum Science and Engineering (IQSE), and Department of Physics and Astronomy, Texas A&M University, College Station, Texas 77843-4242, USA*

(Dated: June 21, 2024)

Following the familiar analogy between the optical paraxial wave equation and the Schrödinger equation, we derive the optimal, real-valued wave function for focusing in one and two space dimensions without the use of any phase component. We compare and contrast the focusing parameters of the optimal waves with those of other diffractive focusing approaches, such as Fresnel zones. Moreover, we experimentally demonstrate these focusing properties on optical beams using both reflective and transmissive liquid crystal devices. Our results provide an alternative direction for focusing waves where phase elements are challenging to implement, such as for X-rays, THz radiation, and electron beams.



## Introduction

Fresnel zone plates [1] are optical elements that focus an incident beam due to binary variations in its amplitude and phase. They offer precise control over diffractive propagation and enable efficient beam focusing in systems, where traditional lensing elements are not immediately available. In this article, we address the fundamental question whether any other approach to wave shaping can surpass the limit set by a Fresnel zone plate. In particular, we show for the case of matter waves that the answer to this question is a clear "Yes!", by deriving analytical solutions of the corresponding variational problem. Moreover, we demonstrate the supremacy of our approach compared to Fresnel zone plates by an experiment with light.

A scalar wave, such as a matter wave or an unpolarized electromagnetic field, comprises two components: an amplitude and a phase. The common way to focus an electromagnetic wave is to modulate its phase using a lens by applying a parabolic phase variation in space. However, there are waves for which a phase-modulating lens does not exist due to technological limitations in implementing phase-altering components in such systems. For instance, implementing such components for X-rays and matter waves often requires subnanometer manufacturing.

More effective approaches to focus waves can be achieved via amplitude modulation in space. For example, blocking part of the wave by a circular aperture or annular rings known as Fresnel zones will focus it to the Arago-Poisson spot [1]. In these examples, the incoming waves are spatially selected without being modified by the materials. These diffractive focusing techniques are crucially determined by a non-Gaussian initial wave function, as well as by the underlying dimensionality of the problem [2–4], and have been employed for surface gravity water waves and plasmonic waves [5, 6].

We emphasize that while Fresnel zones provide one approach to focusing the waves by amplitude modulation, one may question whether other approaches, e.g. nonbinary amplitude modulations, provide even better focusing. In the present article, we obtain the optimal initial wave function for focusing a free particle, i.e. matter waves, in one and two dimensions, and compare and contrast the focusing parameters of the optimal two-dimensional wave function to those of the Fresnel zone approach. The analogy between the Schrödinger equation and the paraxial Helmholtz equation allows us to extend our results to electromagnetic waves. Finally, we experimentally verify the focusing properties of the two-dimensional pattern at optical wavelengths using a reflective spatial light modulator and a fabricated transmissive liquid crystal device.

## Results

**Theory of optimal focusing:** Our goal is to determine the optimal *initial* real-valued, aperture-constrained, and normalized wave function $\psi_0$ in two spatial dimensions that maximizes the intensity $|\psi|^2$ of the field on the symmetry axis at a prescribed focusing time. Our choice of the number of dimensions results from the fact that in one dimension the focusing is weaker, as shown in the Methods section.

Hence, we assume that $\psi_0$ is radially symmetric, as it provides the best diffractive focusing [3], and write the solution as

$$\psi(\rho,\tau) = 2\pi \int_0^\infty \rho' \mathrm{d}\rho' \, \mathrm{G}^{(2)}(\rho,\tau|\rho',0)\,\psi_0(\rho') \qquad (1)$$

of the time-dependent two-dimensional Schödinger equation of a free particle in terms of the corresponding Green

function

$$\mathrm{G}^{(2)}(\rho,\tau|\rho',0)=\frac{1}{2\pi\mathrm{i}\tau}\exp\left(\mathrm{i}\frac{\rho^2+\rho'^2}{2\tau}\right)J_0\left(\frac{\rho\rho'}{\tau}\right) \quad (2)$$

with the Bessel function $J_0$ of the first kind [7]. Here $\rho\equiv r/R$ and $\tau\equiv\hbar t/(MR^2)$ are the dimensionless radial coordinate and time, respectively, wherein $M$ and $R$ denote the mass of the particle and the radius of the circular aperture. In the case of the two-dimensional paraxial Helmholtz equation, $\tau$ is equivalent to the longitudinal distance $z\equiv(kR^2)\tau$ from the screen, where $k$ denotes the wave number.

We consider only wave functions $\psi_0$ that are truncated by the aperture $\rho\leq 1$ and vanish elsewhere, $\psi_0(\rho\geq 1)=0$. As a result, for a prescribed focusing time $\tau_\mathrm{f}$, or focal distance $z_\mathrm{f}\equiv kR^2\tau_\mathrm{f}$, the intensity $I[\psi_0]$ along the symmetry axis, $\rho=0$, takes the form

$$I[\psi_0]=\frac{1}{\tau_\mathrm{f}^2}\int_0^1 u\mathrm{d}u\int_0^1 v\mathrm{d}v\cos\left(\frac{u^2-v^2}{2\tau_\mathrm{f}}\right)\psi_0(u)\psi_0(v), \quad (3)$$

where we have used that $\psi_0$ is real.

In order to solve the optimization problem, we first construct the Lagrange function

$$\mathcal{L}[\psi_0]\equiv I[\psi_0]-\lambda\left[2\pi\int_0^1 u\mathrm{d}u\,\psi_0^2(u)-1\right], \quad (4)$$

where the Lagrange multiplier $\lambda$ takes into account the normalization condition for $\psi_0$, and then perform the variation of $\mathcal{L}[\psi_0]$ with respect to $\psi_0$, to arrive at the eigenvalue problem

$$\frac{1}{2\pi\tau_\mathrm{f}^2}\int_0^1 v\mathrm{d}v\cos\left(\frac{u^2-v^2}{2\tau_\mathrm{f}}\right)\psi_0(v)=\lambda\psi_0(u) \quad (5)$$

for the optimal wave function $\psi_0$ corresponding to the eigenvalue $\lambda$.

Since Eq. (5) is a linear integral equation with a degenerate kernel, its solution can be found analytically, as shown in the Methods section. Indeed, for a fixed value of $\tau_\mathrm{f}$, we obtain the maximum eigenvalue

$$\lambda_+(\tau_\mathrm{f})=\frac{1}{8\pi\tau_\mathrm{f}^2}\left[1+2\tau_\mathrm{f}\left|\sin\left(\frac{1}{2\tau_\mathrm{f}}\right)\right|\right] \quad (6)$$

and the normalized optimal initial wave function

$$\psi_0^{(\mathrm{opt})}(\rho)=N\left[\sqrt{1+a}\cos\left(\frac{\rho^2}{2\tau_\mathrm{f}}\right)+\sqrt{1-a}\sin\left(\frac{\rho^2}{2\tau_\mathrm{f}}\right)\right]. \quad (7)$$

Here, $a\equiv\cos[1/(2\tau_\mathrm{f})]\mathrm{sign}\{\sin[1/(2\tau_\mathrm{f})]\}$ and $N\equiv 1/\sqrt{8\pi^2\tau_\mathrm{f}^2\lambda_+(\tau_\mathrm{f})}$ are the amplitude parameter and the normalization constant, respectively, with $\mathrm{sign}(x)$ being the sign function.

Substituting $\psi_0^{(\mathrm{opt})}$ given by Eq. (7) into the expression, Eq. (3), for the intensity at $\rho=0$, we prove that the intensity, indeed, achieves its maximum value $I_\mathrm{max}^{(\mathrm{opt})}(\tau_\mathrm{f})\equiv I[\psi_0^{(\mathrm{opt})}]=\lambda_+(\tau_\mathrm{f})$ for any given focusing time $\tau_\mathrm{f}$, or the dimensionless distance $z_\mathrm{f}$ from the screen (within the paraxial approximation). In particular, for

$$\tau_{n_0}\equiv\frac{1}{2\pi n_0}, \quad (8)$$

where the integer $n_0$ counts the number of Fresnel zones that fit in the circular aperture $0\leq\rho\leq 1$, Eq. (6) yields

$$I_\mathrm{max}^{(\mathrm{opt})}(\tau_{n_0})=\frac{\pi}{2}n_0^2. \quad (9)$$

**Fresnel zones:** Next we compare the maximum focusing intensity, Eq. (9), of the optimal state $\psi_0^{(\mathrm{opt})}$ with the Fresnel zones approach. For this purpose, we consider two different designs.

An amplitude Fresnel zone (AFZ) plate alters the amplitude, while the phase Fresnel zone (PFZ) plate modifies the phase of the incoming wave. In the AFZ, only odd ($n=1,3,5,\ldots$) annular zones are transparent, whereas even ($n=2,4,6,\ldots$) zones are opaque, that is absorbing the incoming waves, with $n=1$ being the innermost zone containing the origin. The AFZ plate is a nonunitary object, i.e. the input intensity is not conserved. In the PFZ, we keep even and odd zones fully transparent; however, the phase in the even zones is shifted by $\pi$.

For the focusing time $\tau_{n_0}$, we derive in the Methods section the maximal intensities

$$I_\mathrm{max}^{(\mathrm{AFZ})}(\tau_{n_0})=\frac{2}{\pi}\begin{cases}n_0(n_0+1), & n_0=1,3,5,\ldots\\ n_0^2, & n_0=2,4,6,\ldots\end{cases} \quad (10)$$

and

$$I_\mathrm{max}^{(\mathrm{PFZ})}(\tau_{n_0})=\frac{4}{\pi}n_0^2 \quad (11)$$

at the symmetry axis $\rho=0$.

A comparison of Eqs. (9), (10) and (11) reveals that the optimal state $\psi_0^{(\mathrm{opt})}$ defined by Eq. (7) gives rise to focusing improved by the factor $\pi^2/8$ compared to the best Fresnel method.

**Experiments:** Now we demonstrate experimentally optimal diffractive focusing for the two-dimensional case using optical light. For this purpose we have fabricated a transmissive, liquid crystal optical element, that is a Pancharatnam-Berry optical element (PBOE) [8], described in the Methods section, which can be operated at many different wavelengths. It generates the optimal state $\psi_0^{(\mathrm{opt})}$ given by Eq. (7). The space-varying amplitude for the focusing time $\tau_{n_0}$ defined by Eq. (8) with $n_0=14$ is shown in Fig. 1(a) together with the expected and measured intensities, Figs. 1(b) and (c), respectively.

The complete experimental apparatus used to generate the optimal state is displayed in Fig. 1(d). The PBOE

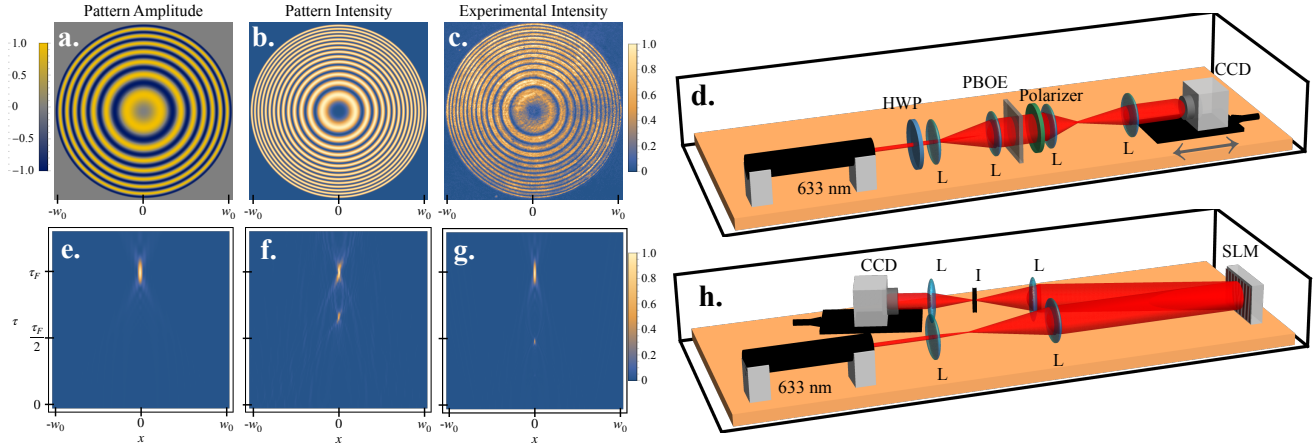


Figure 1. **Implementation of Optimal Diffractive Focusing**. We show the theoretical amplitude **(a)** and intensity **(b)** of the $n_0 = 14$ optimal wave together with the measured optical transmission through the fabricated focusing element **(c)** for the focusing time $\tau_{n_0} = 1/(2\pi n_0)$. **(d)** Experimental apparatus used to generate the optimal state with a PBOE. A linearly polarized 633 nm Gaussian beam passes a half-wave plate ($\lambda/2$) which rotates it to the horizontal polarization. The beam is then expanded by a factor of five by two lenses (L) to obtain a relatively flat profile before it goes through the PBOE followed by a polarizer. The latter is then imaged by a 4f-system in order to examine its propagation dynamics by a CCD camera. Numerically simulated **(e)** and experimentally observed **(f)** intensity distributions for a cross section of the beam as it propagates from the plane of the device to the focus for the optimal state. Numerical simulation taking into account contributions **(g)** from both the horizontal (Cosine) and vertical (Sine) polarization components of the modulated beam. Experimental setup **(h)** for focusing with Fresnel zone patterns using the SLM. The 633 nm laser source is expanded to cover the SLM. The 4f-lens system then images the SLM onto the CCD camera with an iris (I) placed at the focus to select the first order of diffraction.

placed between a half-wave plate and a polarizer is illuminated by a 633 nm He-Ne laser with an expanded Gaussian profile. A 4-f lens system is used to image the device on a $1920 \times 1080$ pixel CCD camera placed on a translation stage, which allows us to measure the intensity of the modulated beam along its propagation to the focus. We have obtained this intensity profile in 50 $\mu$m steps for 25.0 mm.

Whereas Fig. 1(e) shows the exact evolution of the beam originating from the optimal state $\psi_0^{(\mathrm{opt})}$ given by Eq. (7), Figs. 1(f) and (g) display the experimentally measured and expected intensity along the propagation. As further elaborated in the Discussion section, we expect imperfections in our optical system to affect the propagation profile.

To compare the propagation of $\psi_0^{(\mathrm{opt})}$ with the ones created by the Fresnel zone plates, Eqs. (M9) and (M10) in the Methods section, we replace our PBOE by a reflective spatial light modulator (SLM), as depicted in Fig. 1(h). We used a Hamamatsu liquid crystal on silicon (LCOS) SLM with $1272 \times 1024$ resolution and a pixel size of 12.5 $\mu$m. Moreover, we are able to encode both the intensity and the phase of the pattern on the incident beam using an amplitude masking technique [9]. A phase diffraction grating is added to the pattern on the SLM which produces the desired field in the first order of diffraction. We then select this first order with a 4f lens system and an iris, thereby allowing us to remove all other diffraction orders while imaging the SLM plane onto our moveable CCD camera. Although SLMs do not reach the spatial resolution of our PBOE, their programmability can more readily streamline experiments comparing various focusing approaches.

In Fig. 2, we display the maximal focusing intensity $I_{\max}(\tau_{n_0})$ for nine different patterns corresponding

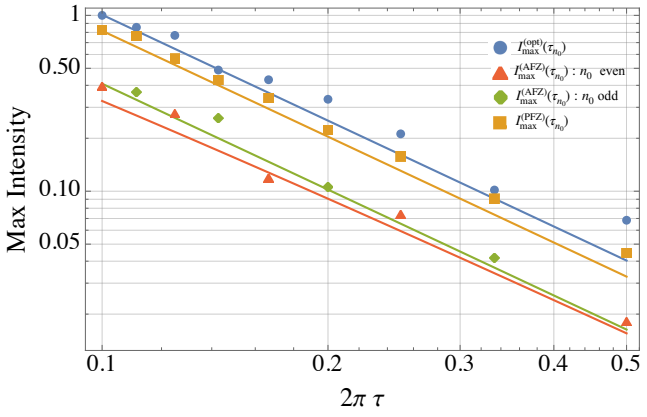


Figure 2. **Comparison of the three methods for two-dimensional diffractive focusing**. For a fixed focusing time $\tau_{n_0} = 1/(2\pi n_0)$, with $n_0 = 2, 3, \ldots, 10$, we display the theoretical optimal maximum intensities, $I_{\max}^{(\mathrm{opt})}(\tau_{n_0})$ (blue line), given by Eq. (9), as well as $I_{\max}^{(\mathrm{AFZ})}(\tau_{n_0})$ (red and green), and $I_{\max}^{(\mathrm{PFZ})}(\tau_{n_0})$ (orange), associated with the Fresnel zone plates, Eqs. (10) and (11). The points represent the corresponding measurements.

to focusing times $\tau_{n_0}$, as defined in Eq. (8), with $n_0 = 2, 3, \ldots, 10$. The results of these experiments involving the optimal wave function as well as both forms of the Fresnel zones are depicted in Fig. 2.

**Discussion**

The propagation of the beam, shown in Fig. 1(f), features an artificial peat at $\tau = \tau_\mathrm{f}/2$ arising from the modulation by our PBOE. Indeed, an imperfect polarization alignment in our generation apparatus leads to contributions of the $\sin(2\alpha)$-term in Eq. (M19). The angular orientation of the liquid crystals, $\alpha = \alpha(x, y)$, ranges from 0 to $\pi/2$ such that the horizontally polarized component of the field oscillates from $+1$ to $-1$ according to $\cos(2\alpha)$, while the term $\sin(2\alpha)$ oscillates from 0 to $+1$ and back to 0. As a consequence, the contribution from the $\sin(2\alpha)$-component, which does not have negative amplitudes, behaves like the Fresnel zones, giving rise to a focus at $\tau_\mathrm{f}/2$. In Fig. 1(g), we show the expected propagation including the contribution from the $\sin(2\alpha)$-term, which is in good agreement with our experimental results shown in Fig. 1(f).

The scalings of the peak intensities of the focusing methods, considered in our article, with $n_0$ are shown in Fig. 2 by solid lines together with the experimental results depicted by the differently coloured data points. The peak focal intensity increases with increasing $n_0$, corresponding to a tighter focusing time $\tau_{n_0}$, or equivalently, to a shorter focal length. Furthermore, the optimal wave function consistently outperforms both methods relying on Fresnel zone plates.

We conclude this discussion by emphasizing that with our PBOE we were able to achieve a better resolution in our pattern creation, allowing for a tighter focusing time $\tau_{n_0}$ with $n_0 = 14$, than with the SLM. This advantage is primarily due to the fact that a diffraction grating is necessary when the SLM is used to form an arbitrary wave function, which thus limits the maximum spatial frequency of the phase oscillations corresponding to the desired pattern. In addition, the SLM has limited control over both phase and spatial modulation, as prescribed by its bit depth and pixel pitch, respectively. As $n_0$ is increased, the number of oscillations in $\psi_0^{(\mathrm{opt})}$ from $+1$ to $-1$ increases and in particular, the outer rings of the pattern become ever thinner.

**Summary.** We have derived the optimal real-valued matter wave $\psi_0^{(\mathrm{opt})}$ for focusing in both one- and two-dimensions. The analogy between the Schrödinger equation and the paraxial wave equation allows us to transfer our treatment to light. In our optical experiment, we have realized the two-dimensional optimal wave function $\psi_0^{(\mathrm{opt})}$ using liquid crystal devices, verifying the superior focusing properties of $\psi_0^{(\mathrm{opt})}$ compared to diffractive focusing from Fresnel zone patterns.

The optimal diffractive patterns derived here may be of interest to many different communities where phase modulation, due to technological limitations, is not directly possible. We can also envision extending this technique to vector fields, such as spinors in both optical and matter waves, where combinations of amplitude masks and specially polarized vector modes bring highly structured variations in focused beams [10–12]. The application of $\psi_0^{(\mathrm{opt})}$ to these tight focusing problems remains to be explored.

## METHODS

### Optimal state in two dimensions

To obtain the analytical solution of the integral equation (5), we cast it in the form

$$\psi_0(u) = \frac{1}{2\pi\tau_\mathrm{f}^2\lambda}\left[A\cos\left(\frac{u^2}{2\tau_\mathrm{f}}\right) + B\sin\left(\frac{u^2}{2\tau_\mathrm{f}}\right)\right], \tag{M1}$$

where

$$A \equiv \int_0^1 v\,\mathrm{d}v\cos\left(\frac{v^2}{2\tau_\mathrm{f}}\right)\psi_0(v) \tag{M2}$$

and

$$B \equiv \int_0^1 v\,\mathrm{d}v\sin\left(\frac{v^2}{2\tau_\mathrm{f}}\right)\psi_0(v) \tag{M3}$$

are functions solely of $\tau_\mathrm{f}$.

Next, we insert $\psi_0$ given by Eq. (M1) into Eqs. (M2) and (M3), and obtain the system

$$\left[\lambda - \frac{1+\tau_\mathrm{f}\sin(1/\tau_\mathrm{f})}{8\pi\tau_\mathrm{f}^2}\right]A - \frac{\sin^2[1/(2\tau_\mathrm{f})]}{4\pi\tau_\mathrm{f}}B = 0 \tag{M4}$$

$$-\frac{\sin^2[1/(2\tau_\mathrm{f})]}{4\pi\tau_\mathrm{f}}A + \left[\lambda - \frac{1-\tau_\mathrm{f}\sin(1/\tau_\mathrm{f})}{8\pi\tau_\mathrm{f}^2}\right]B = 0 \tag{M5}$$

of algebraic equations for $A$ and $B$, which has non-trivial solutions, only when its determinant is zero, that is

$$\left(\lambda - \frac{1}{8\pi\tau_\mathrm{f}^2}\right)^2 - \left(\frac{\sin[1/(2\tau_\mathrm{f})]}{4\pi\tau_\mathrm{f}}\right)^2 = 0. \tag{M6}$$

This elementary quadratic equation has the two solutions

$$\lambda_\pm = \frac{1}{8\pi\tau_\mathrm{f}^2}\left[1 \pm 2\tau_\mathrm{f}\left|\sin\left(\frac{1}{2\tau_\mathrm{f}}\right)\right|\right]. \tag{M7}$$

By inserting the maximal eigenvalue $\lambda_+$ into Eq. (M4), we find the relation between $A$ and $B$, and thus the normalized optimal initial wave function $\psi_0^{(\mathrm{opt})}$ given by Eq. (7).

### Amplitude and phase Fresnel zones: Maximal intensity

For a given value of $\tau_\mathrm{f}$ the radii

$$\rho_n \equiv \sqrt{2\pi\tau_\mathrm{f} n} \tag{M8}$$

of the Fresnel zones, with $n = 1, 2, 3, \ldots, n_0$, extend to the maximum number $n_0$ of zones fitting within the circular aperture $0 \le \rho \le 1$ [1]. Therefore, the initial wave functions $\psi_0^{(\mathrm{AFZ})}$ and $\psi_0^{(\mathrm{PFZ})}$ for the amplitude and phase Fresnel zone patterns read

$$\psi_0^{(\mathrm{AFZ})}(\rho) = N_1\left[\mathbb{U}(\rho; 0, \rho_1) + \sum_{n=1}^{\infty}\mathbb{U}(\rho; \rho_{2n}, \rho_{2n+1})\right] \tag{M9}$$

and

$$\psi_0^{(\mathrm{PFZ})}(\rho) = \frac{1}{\sqrt{\pi}}\left[\mathbb{U}(\rho;0,\rho_1) + \sum_{n=1}^{\infty}(-1)^n \mathbb{U}(\rho;\rho_n,\rho_{n+1})\right] \quad \text{(M10)}$$

with $\mathbb{U}(\rho;a,b) \equiv \Theta(b-\rho) - \Theta(a-\rho)$ and $a < b$. Here, $\Theta(\rho)$ denotes the Heaviside function and $N_1$ is a normalization constant depending on $\tau_\mathrm{f}$.

To derive an analytical formula for the maximal intensity, we choose the focusing times $\tau_\mathrm{f} \equiv \tau_{n_0} \equiv 1/(2\pi n_0)$. In this case, Eq. (M8) reduces to $\rho_n = \sqrt{n/n_0}$, and the normalization condition

$$\pi N_1^2\left[\rho_1^2 + (\rho_3^2 - \rho_2^2) + (\rho_5^2 - \rho_4^2) + \ldots\right] = 1 \quad \text{(M11)}$$

for $\psi_0^{(\mathrm{AFZ})}$, Eq. (M9), defines the constant

$$N_1 \equiv \sqrt{\frac{2}{\pi}}\begin{cases}\sqrt{\frac{n_0}{n_0+1}}, & n_0 = 1,3,5,\ldots\\ 1, & n_0 = 2,4,6,\ldots\end{cases} \quad \text{(M12)}$$

as a function of $n_0$.

Next, we insert the initial profile $\psi_0^{(\mathrm{AFZ})}$ given by Eq. (M9) into Eq. (3), and obtain the expression

$$I_{\max}^{(\mathrm{AFZ})}(\tau_{n_0}) = \frac{1}{\tau_{n_0}^2}\left|\int_0^1 u\mathrm{d}u\, \exp\left(\mathrm{i}\frac{u^2}{2\tau_{n_0}}\right)\psi_0^{(\mathrm{AFZ})}(u)\right|^2$$

$$= N_1^2\left|\exp\left(\mathrm{i}\frac{\rho_1^2}{2\tau_{n_0}}\right) - 1 + \exp\left(\mathrm{i}\frac{\rho_3^2}{2\tau_{n_0}}\right) - \exp\left(\mathrm{i}\frac{\rho_2^2}{2\tau_{n_0}}\right) + \ldots\right|^2,$$

that is

$$I_{\max}^{(\mathrm{AFZ})}(\tau_{n_0}) = N_1^2\begin{cases}(n_0+1)^2, & n_0 = 1,3,5,\ldots\\ n_0^2, & n_0 = 2,4,6,\ldots,\end{cases} \quad \text{(M13)}$$

where we have used the fact that $\rho_n^2/(2\tau_{n_0}) = n\pi$.

As a result, Eq. (M13) combined with Eq. (M12) gives rise to the maximum intensity $I_{\max}^{(\mathrm{AFZ})}(\tau_{n_0})$, Eq. (10), produced by the amplitude Fresnel zones. Analogously, we derive the corresponding maximum intensity $I_{\max}^{(\mathrm{PFZ})}(\tau_{n_0})$, Eq. (11), for the Fresnel phase zones.

## Optimal state in one dimension

In this section we determine the optimal initial real-valued and normalized wave function $\varphi_0 \equiv \varphi_0(x)$ that maximizes the intensity $|\varphi(0)|^2$ of the field at $x = 0$, at the focusing time $t_\mathrm{f}$.

In this case we use the one-dimensional Green function

$$\mathrm{G}^{(1)}(\xi,\tau|\xi',0) = \frac{1}{\sqrt{2\pi\mathrm{i}\tau}}\exp\left[\mathrm{i}\frac{(\xi-\xi')^2}{2\tau}\right] \quad \text{(M14)}$$

for the time-dependent one-dimensional Schrödinger equation of a free particle. Here, $\xi \equiv x/L$ and $\tau \equiv \hbar t/(ML^2)$ are the dimensionless position and time, respectively, and $M$ and $L$ denote the mass of the particle and the slit width.

We again apply the method of the Lagrange multipliers and arrive at the eigenvalue problem

$$\frac{1}{2\pi\tau_\mathrm{f}}\int_{-1}^{1}\mathrm{d}\xi' \cos\left(\frac{\xi^2-\xi'^2}{2\tau_\mathrm{f}}\right)\varphi_0(\xi') = \mu\varphi_0(\xi) \quad \text{(M15)}$$

for the optimal initial wave function $\varphi_0$ with the eigenvalue $\mu$, that determines the maximum intensity achieved at $\tau_\mathrm{f}$. Here, we have assumed that $\varphi_0(\xi) = 0$ for $|\xi| > 1$.

Since we are interested in the maximum of the intensity, we solve the integral equation (M15) only for the largest eigenvalue $\mu_+(\tau_\mathrm{f})$. As a result, for a given $\tau_\mathrm{f}$, we find the optimal initial wave function

$$\varphi_0^{(\mathrm{opt})}(\xi) = \sqrt{\frac{1+r}{4\pi\tau_\mathrm{f}\mu_+}}\cos\left(\frac{\xi^2}{2\tau_\mathrm{f}}\right) + \sqrt{\frac{1-r}{4\pi\tau_\mathrm{f}\mu_+}}\sin\left(\frac{\xi^2}{2\tau_\mathrm{f}}\right) \quad \text{(M16)}$$

for $|\xi| \le 1$, with $\varphi_0^{(\mathrm{opt})}(\xi) = 0$ for $|\xi| > 1$, and the corresponding maximal eigenvalue

$$\mu_+(\tau_\mathrm{f}) = I_{\max}^{(\mathrm{1D})}(\tau_\mathrm{f}) = \mathcal{I}\left[\sqrt{2/(\pi\tau_\mathrm{f})}\right]. \quad \text{(M17)}$$

Here we have expressed the intensity

$$\mathcal{I}(z) \equiv \frac{1}{4}\left\{z^2 + z\sqrt{[C(z)]^2 + [S(z)]^2}\right\}$$

and the parameter

$$r(\tau_\mathrm{f}) \equiv \frac{C\left[\sqrt{2/(\pi\tau_f)}\right]}{\sqrt{\left\{C\left[\sqrt{2/(\pi\tau_f)}\right]\right\}^2 + \left\{S\left[\sqrt{2/(\pi\tau_f)}\right]\right\}^2}} \quad \text{(M18)}$$

in terms of the Fresnel integrals $C$ and $S$ [7].

## Pancharatnam-Berry optical element

Our device consists of a patterned layer of birefringent nematic liquid crystals whose orientation locally determines that of the medium's optical axis. This feature causes the element to have the action

$$\hat{\mathcal{U}}_q \cdot \begin{pmatrix}\mathbf{e}_\mathrm{H}\\ \mathbf{e}_\mathrm{V}\end{pmatrix} = \cos\left(\frac{\delta}{2}\right)\begin{pmatrix}\mathbf{e}_\mathrm{H}\\ \mathbf{e}_\mathrm{V}\end{pmatrix} + i\sin\left(\frac{\delta}{2}\right)\begin{pmatrix}\cos[2\alpha(x,y)] & \sin[2\alpha(x,y)]\\ \sin[2\alpha(x,y)] & -\cos[2\alpha(x,y)]\end{pmatrix}\begin{pmatrix}\mathbf{e}_\mathrm{H}\\ \mathbf{e}_\mathrm{V}\end{pmatrix} \quad \text{(M19)}$$

on the horizontal $\mathbf{e}_\mathrm{H}$ and vertical $\mathbf{e}_\mathrm{V}$ polarization components of an optical beam. Here $\delta$ is the optical retardation of the liquid crystal molecules and $\alpha \equiv \alpha(x,y)$ is the device's spatially dependent liquid crystal axis orientation expressed in terms of the transverse Cartesian coordinates $x$ and $y$.

When the device is perfectly tuned, that is for $\delta = \pi$, and followed by a *horizontally oriented polarizer*, it can effectively be used to mask the amplitude profile of incoming *horizontally polarized light* by a factor of $\cos[2\alpha(x,y)]$. This procedure was employed to generate our real-valued optimal state $\psi_0^{(\mathrm{opt})} \equiv \psi_0^{(\mathrm{opt})}(x,y)$ by means of a device defined by an optical axis of $\alpha(x,y) = (1/2)\arccos\left[\psi_0^{(\mathrm{opt})}(x,y)/\psi_{\max}^{(\mathrm{opt})}\right]$, where $\psi_{\max}^{(\mathrm{opt})}$ is the maximum value of the optimal state.


[1] Born, M. & Wolf, E. *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light* (Elsevier, 2013).

[2] Cirone, M. A., Rzążewski, K., Schleich, W. P., Straub, F. & Wheeler, J. A. Quantum anticentrifugal force. *Phys. Rev. A* **65**, 022101 (2001).

[3] Białynicki-Birula, I., Cirone, M. A., Dahl, J. P., Fedorov, M. & Schleich, W. P. In- and outbound spreading of a free-particle $s$-wave. *Phys. Rev. Lett.* **89**, 060404 (2002).

[4] Case, W. B., Sadurni, E. & Schleich, W. P. A diffractive mechanism of focusing. *Opt. Express* **20**, 27253 (2012).

[5] Weisman, D. *et al.* Diffractive focusing of waves in time and in space. *Phys. Rev. Lett.* **118**, 154301 (2017).

[6] Weisman, D. *et al.* Diffractive guiding of waves by a periodic array of slits. *Phys. Rev. Lett.* **127**, 014303 (2021).

[7] Abramowitz, M. & Stegun, I. A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, vol. 55 (US Government Printing Office, 1968).

[8] Larocque, H. *et al.* Arbitrary optical wavefront shaping via spin-to-orbit coupling. *Journal of Optics* **18**, 124002 (2016).

[9] Bolduc, E., Bent, N., Santamato, E., Karimi, E. & Boyd, R. W. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Opt. Lett.* **38**, 3546–3549 (2013).

[10] Dorn, R., Quabis, S. & Leuchs, G. Sharper focus for a radially polarized light beam. *Phys. Rev. Lett.* **91**, 233901 (2003).

[11] Wang, H., Shi, L., Lukyanchuk, B., Sheppard, C. & Chong, C. T. Creation of a needle of longitudinally polarized light in vacuum using binary optics. *Nature Photonics* **2**, 501–505 (2008).

[12] Karimi, E., Piccirillo, B., Marrucci, L. & Santamato, E. Improved focusing with hypergeometric-gaussian type-ii optical modes. *Opt. Express* **16**, 21069 (2008).

**Data availability** The data that support the findings of this study are available from the corresponding author upon reasonable request.

**Code availability** The code used for the data analysis is available from the corresponding author upon reasonable request.

**Ethics declarations** The authors declare no competing interests.

**Corresponding authors** Correspondence and requests for materials should be addressed to maxim.efremov@dlr.de.

**Acknowledgement** Maxim A. Efremov and Felix Hufnagel contributed equally to this work. We thank P. Boegel for fruitful discussions. W.P.S. is grateful to the Hagler Institute for Advanced Study at Texas A&M University for a Faculty Fellowship, and to Texas A&M AgriLife Research for the support of this work. This project was conceived during a visit of E.K. to Ulm University made possible by *IQST*. F. H. and E.K. acknowledge the support of the Canada Research Chair (CRC) Program, NRC-uOttawa Joint Centre for Extreme Quantum Photonics (JCEP) and NSERC.

# Chapter 3

# Entanglement Sources

QKD protocols and many other applications in quantum information are heavily reliant on the ability to produce single photons. The ideal goal of deterministic sources has been studied with many different physical systems including the atomic transitions of single atoms, solid-state silicon and diamond defects, and quantum dots [23]. However, many quantum optics demonstrations have used non-deterministic sources which employ the emission of photon pairs in non-linear optical processes. We primarily rely on non-deterministic single photon sources for quantum communication experiments. These sources use non-linear optical effects including spontaneous parametric down conversion (SPDC) and spontaneous four-wave mixing (FWM), to produce pairs of photons which allow us to herald the presence of 1 photon based on a coincidence measurement made with the other photon. SPDC has been used to demonstrate many quantum effects including 2 photon interference [24], quantum teleportation [25], polarization entanglement [26], and quantum key distribution [27].

SPDC is a second order non-linear effect in which a single input photon is converted to 2 photons of lower energy, being sure to maintain the conservation of energy and momentum. In non-linear processes, the different optical frequencies generated will typically have a different index of refraction in the material. The problem of conserving the energy and

momentum in these materials is referred to as phase matching. In SPDC we annihilate 1 photon and generate 2 photons. This process must follow the conservation of energy and momentum which gives the following requirements,

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i, \tag{3.1}$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_s, \tag{3.2}$$

where $\hbar\omega_p$, $\hbar\omega_s$ and $\hbar\omega_i$ are the pump, signal, and idler photon energies and similarly $\vec{k}_p$, $\vec{k}_p$, and $\vec{k}_i$ are the wave vectors. These are the equations defining the phase-matching conditions for the non-linear interaction [28]. The non-linear material can be chosen in such a way to allow for phase matching at the desired wavelengths of operation. Phase matching in bulk optics is typically achieved using a birefringent crystals which gives us a few different types of SPDC: Type-0 when signal, idler, and pump all share the same polarization; Type-I when the signal and idler have the same polarization and are orthogonal to the pump; and Type-II when the signal and idler have orthogonal polarizations. In Type-II phase matching, the signal and idler photons form 2 cones of orthogonally polarized pairs which yield the polarization entangled state $|\psi\rangle = (|H_1, V_2\rangle + e^{i\alpha}|V_1, H_2\rangle)/\sqrt{2}$ at the points where the cones intersect. Here $\alpha$ is a relative phase arising from the crystal birefringence and it can be set to any value by introducing an additional birefringent phase shift [26]. One can also produce the polarization entangled state using 2 thin Type-I crystals "sandwiched" together with their optic axis oriented at 90°with respect to each other. In this case a 45°polarized pump beam will create photons in either crystal with equal likelihood, resulting in the entangled state $|\psi\rangle = (|H_1, H_2\rangle + e^{i\alpha}|V_1, V_2\rangle)/\sqrt{2}$ which can be used to create any of the Bell states again applying a birefringent phase shift or a half-wave plate [29].

It has been known for many years that the SPDC process conserves OAM and in fact that one can generate high-dimensional correlations and entanglement in the OAM degree of freedom. However, when considering the Laguerre-Gaussian basis this is only half-of the picture consisting of the azimuthal degree of freedom but not the radial component. If we can also take advantage of the radial component, denoted as the *p-modes*, then

we can more efficiently generate high-dimensional quantum states for use in quantum information tasks. In this chapter 2 articles are presented discussing SPDC sources. The first article demonstrates for the first time the characterization of the OAM and radial mode correlations from an SPDC source. The second shows an experimental approach to manipulate the symmetry of momentum entangled photons.

Optics Letters

# Full-mode characterization of correlated photon pairs generated in spontaneous downconversion

Alessio D'Errico,[1,*] Felix Hufnagel,[1] Filippo Miatto,[1,2] Mohammadreza Rezaee,[1] and Ebrahim Karimi[1,3]

[1]Physics Department, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa, Ontario K1N 6N5, Canada
[2]Current address: Xanadu, 777 Bay St., Toronto, Ontario M5G2C8, Canada
[3]e-mail: [redacted]
*Corresponding author: [redacted]

Received 9 March 2021; revised 16 April 2021; accepted 17 April 2021; posted 19 April 2021 (Doc. ID 424619); published 6 May 2021

**Spontaneous parametric downconversion is the primary source to generate entangled photon pairs in quantum photonics laboratories. Depending on the experimental design, the generated photon pairs can be correlated in the frequency spectrum, polarization, position-momentum, and spatial modes. Exploring the spatial modes' correlation has hitherto been limited to the polar coordinates' azimuthal angle, and a few attempts to study Walsh mode's radial states. Here, we study the full-mode correlation, on a Laguerre–Gauss basis, between photon pairs generated in a type-I crystal. Furthermore, we explore the effect of a structured pump beam possessing different spatial modes onto bi-photon spatial correlation. Finally, we use the capability to project over arbitrary spatial mode superpositions to perform the bi-photon state's full quantum tomography in a 16-dimensional subspace.** 

https://doi.org/10.1364/OL.424619

Photon pair correlations in spontaneous parametric downconversion (SPDC) processes are ubiquitous in all photonic degrees of freedom, thus providing a powerful tool for quantum information and computation technologies [1,2]. SPDC can also be exploited to generate high-dimensional quantum states, i.e., qudits, which may be advantageous with respect to qubits in quantum information processing [1,3,4]. Orbital angular momentum (OAM) is among the most promising degrees of freedom for high-dimensional quantum technologies [4,5]. However, there have been arguments as to whether photonic's OAM is the optimal degree of freedom to increase communication capacity [6]. Most of the optics used possess cylindrical symmetry, and therefore, the description in terms of circular beams [7], including the so-called Laguerre–Gauss (LG) modes, provides a convenient complete basis. There has been a growing interest in exploiting single photons' radial mode [8–13], which (together with OAM) would provide access to full capacity for a given optical system. Experimentally, exploring the modal structure of the SPDC state has been intensely focused on its OAM content [1,3]. On the contrary, the radial mode decomposition is considered mainly theoretically [14] with a few experimental studies [15–18]. In the first attempts to investigate the LG mode radial index spectrum of SPDC experimentally [15,16], state projections were not rigorously performed on the LG basis, but only on the radial phase jump, i.e., the Walsh mode radial index [15]. Indeed, full-mode characterization on an arbitrary basis, including LG modes, requires precise determination of both amplitude and phase structure of spatial modes, which has recently been demonstrated for an attenuated laser beam [19]. The filtering effect of single-mode fibers (SMFs) was shown to alter the detected correlations [17]. In an attempt to reconstruct radial mode correlations generated by a Gaussian pump [18], the detection holograms employed in the projection performed poorly in tomographic measurements [20]. In this Letter, we surpass the above challenges and perform the rigorous measurement of radial and OAM state, i.e., full-mode, correlations hidden in the SPDC generated from a type-I nonlinear crystal, analyzing the results for different pump modes, and characterizing the bi-photon correlations using full quantum state tomography in a 16-dimensional Hilbert space.

In cylindrical coordinates $r$, $\phi$, $z$, one can define the complete set of LG modes labeled by two indices $|p,\ell\rangle$, determining, respectively, the radial and azimuthal photon's state. State $|\ell\rangle$ is defined as the eigenstate of the OAM operator $\hat{\ell} = -i\hbar\partial_\phi$, where $\hbar$ is the reduced Planck constant, which is conjugate to the azimuthal operator $\hat{\phi}$; hence, $\Delta\hat{\phi}\Delta\hat{\ell} \geq 1/4$ [21]. Similarly, one can define an operator $\hat{p} = -(\rho^{-1}\partial_\rho(\rho\partial_\rho) - \rho^2 + \rho^{-2}\partial_\phi^2 - 2i\partial_\phi + 2)/4$ that is diagonal in the set of $|p\rangle$ states. However, this observable does not generate any continuous symmetry, i.e., it prevents one from finding a proper conjugate quantity $\hat{\Xi} := \hat{\Xi}(\hat{\rho})$ [22,23]. Nevertheless, the quantum nature of $|p\rangle$ states is well established [8–13]; moreover, an uncertainty relation still holds $\Delta\hat{p}\Delta\hat{\Xi} \geq 1/4$, and quantum states saturating the uncertainty relation can be engineered [23,24]. The explicit expression for LG modes in the position representation $\mathrm{LG}_{p,\ell}(r,\phi,z) := \langle r,\phi,z|p,\ell\rangle$, where the beam radius is minimized, i.e., at $z = 0$, is given by

$$\mathrm{LG}_{p,\ell}(r,\phi,0) = C_{|\ell|}^{(p)}\left(\frac{r}{w}\right)^{|\ell|} L_p^{|\ell|}\left(2\left(\frac{r}{w}\right)^2\right) e^{-(\frac{r}{w})^2 - i\ell\phi}, \tag{1}$$

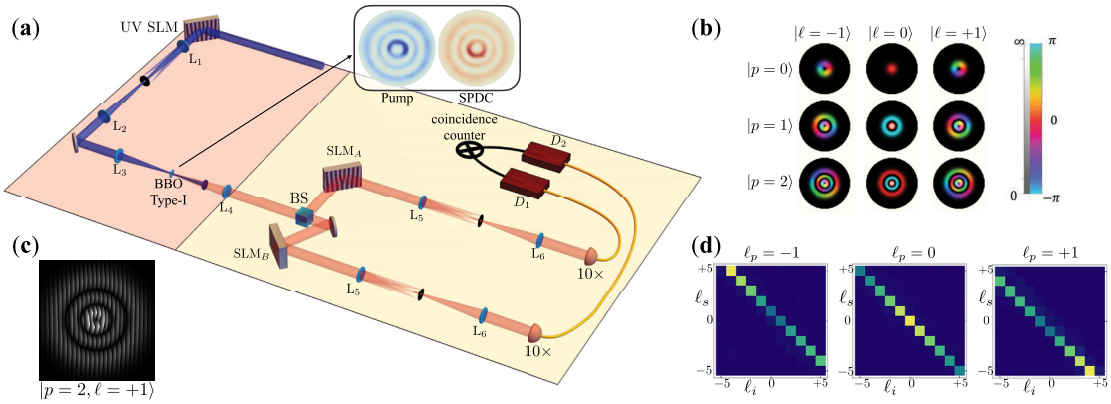


**Fig. 1.** Experimental setup and OAM correlations. (a) Schematic of the experimental setup. A 400 nm laser beam is converted in an LG mode exploiting an ultraviolet (UV) spatial light modulator (SLM) implementing an intensity masking technique. The beam is then focused on a type-I beta barium borate (BBO) crystal, and the residual transmitted UV is filtered with a long-pass filter. The SPDC signal is collimated by a lens ($L_4$) and then sent to the detection stage through a beam splitter (BS). The individual photons are thus projected on the desired spatial modes by means of SLMs A and B and single-mode optical fibers through the mode detection technique described in the text. L, lenses; Ph, pinhole; $D_1$ and $D_2$, couplers (with 10X objective) to single-mode fibers and detectors. (b) Amplitude and phase distribution of the lowest order LG modes with $p \in \{0, 1, 2\}$ and $\ell \in \{-1, 0, +1\}$. (c) Example of hologram applying intensity masking as displayed on the SLMs. The intensity masking effect can be understood by noticing that a blazed grating appears only in those regions where we wish to have a nonzero intensity. Indeed, the region with constant phase (black) will not deflect the light through the pinholes. The hologram generates $\mathrm{LG}_{2,+1}(x)$ mode. (d) Experimental OAM correlation matrices (normalized w.r.t the maximum) for different OAM values of the pump $\ell_p$. These results have been obtained without applying intensity masking; hence, both the pump and the projected modes are described as Hypergeometric-Gaussian modes.

where $C_{|\ell|}^{(p)}$ is a constant, and $L_p^{|\ell|}(x)$ is the associated Laguerre polynomial [25]. Let us consider a type-I nonlinear crystal pumped by an ultraviolet laser beam whose complex amplitude is described by Eq. (1), i.e., $\mathrm{LG}_{p_p,\ell_p}(r, \phi, 0)$. Assuming a frequency degenerate case, probabilistically, the crystal creates two identical photons, namely, *signal* (s) and *idler* (i), from one of the pump photons [1,2]. Following the conservation of energy and linear momentum, which dictates the correlation in position and anti-correlation in momentum space, the bi-photon state can be expressed in the spatial mode basis as [1,14]

$$|\Psi\rangle_{\mathrm{SPDC}} \propto \sum_{\ell_i, p_i, \ell_s, p_s} c_{p_s,\ell_s}^{p_i,\ell_i} |p_s, \ell_s\rangle \otimes |p_i, \ell_i\rangle, \qquad (2)$$

where $|p_s, \ell_s\rangle$ and $|p_s, \ell_s\rangle$ are the signal and idler photons' states in the LG basis, respectively, and $c_{p_s,\ell_s}^{p_i,\ell_i}$ is the bi-photon correlation amplitude. For a collinear phase matching, the bi-photon correlation amplitude is

$$c_{p_s,\ell_s}^{p_i,\ell_i} = \int \mathrm{d}\mathbf{x}\, \mathrm{LG}_{p_p,\ell_p}(\mathbf{x}) \mathrm{LG}_{p_i,\ell_i}^{*}(\mathbf{x}) \mathrm{LG}_{p_s,\ell_s}^{*}(\mathbf{x}), \qquad (3)$$

where * stands for complex conjugate. This equation shows the effect of field continuity, i.e., that the amplitude (and phase) of the bi-photon wavefunction on the crystal plane is determined by the amplitude (and phase) of the pump, which we verified experimentally, as shown in the inset of Fig. 1(a). An explicit expression for the bi-photon correlation amplitude can be found in terms of Lauricella's hypergeometric function (see Supplement 1 for more details). The amplitude $\left|c_{p_s,\ell_s}^{p_i,\ell_i}\right|^2$ can be measured experimentally by implementing projection operators on LG modes, $\hat{P}_{p_s\ell_s}^{p_i\ell_i} = (|p_s, \ell_s\rangle \otimes |p_i, \ell_i\rangle)(\langle p_s, \ell_s| \otimes \langle p_i, \ell_i|)$, applied on each photon in the downconverted pair, i.e., $\mathrm{Tr}(\hat{R}_\Psi \hat{P}_{p_s\ell_s}^{p_i\ell_i})$, where $\hat{R}_\Psi$ and Tr(.) stand for the bi-photon density matrix and the trace, respectively. The measurement of the OAM content of a single photon is well established [3], and is typically based on the use of phase holograms (implementing a shift in the OAM space) coupled to SMFs—the phase flattening technique. However, projecting over spatial modes with an arbitrary amplitude shape has been for a long time a challenging task. Here, we adopt a recently introduced approach that allows, at the expense of losses, detection of LG modes (or any arbitrary set of paraxial beams) with arbitrary accuracy [19] (see Supplement 1 for more details).

Figure 1 shows the sketch of the experimental setup (a more detailed setup is shown in Supplement 1). A liquid crystal spatial light modulator (SLM) is used to shape a 400 nm pump into LG modes [20]. Shaping the pump amplitude has been recently used to generate OAM maximally entangled states [26,27]. Idler and signal photons emitted by a type-I beta barium borate (BBO) crystal are analyzed by means of SLMs coupled to SMFs through a de-magnifying system (de-magnification factor is 1/4) and 10X objectives, thus implementing the spatial mode projection technique [19]. We stress that SMFs are necessary, instead of, e.g., multimode fibers, to correctly implement the projection operator (see Supplement 1). To take into account mode-dependent detection efficiencies, i.e., the fact that detection efficiency is not constant for all spatial modes, we performed calibration measurements for each state (see Supplement 1 for more details on the calibration process). We select downconverted photons at the same frequency with 10 nm bandwidth filters centered around 800 nm in front of the fiber couplers. To check the alignment of the setup, we first measured the correlations between signal and idler OAM states, i.e., $|\ell_s\rangle$ and $|\ell_i\rangle$, determined by the OAM of the pump, $|\ell_p\rangle$. Due to OAM conservation [1,3,14], we detect coincidences only if

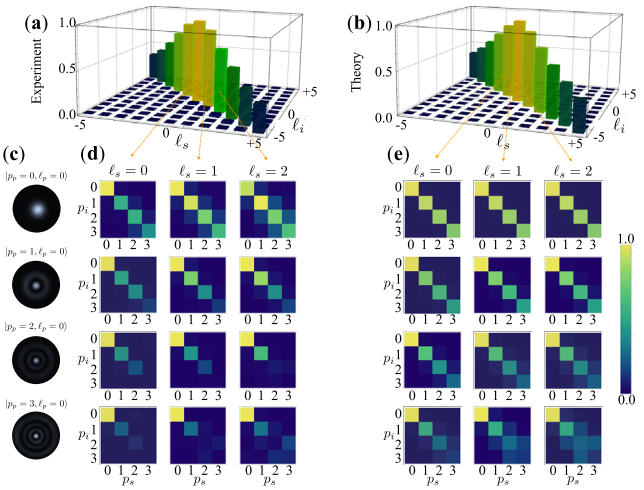


**Fig. 2.** Radial mode correlations with $LG_{p,0}$ pump beam. (a), (b) Respectively, experimental and theoretical OAM correlations for the case of a $LG_{0,0}$ pump. (c) Experimental pump beam intensities on the crystal plane. For each beam, we show, along the same row, (d) experimental and (e) theoretical p-mode correlations of the SPDC beam. Different columns correspond to different OAM subspaces, uniquely identified by the signal OAM index $\ell_s$. For the lowest order modes (and $\ell_s$ values), we observe strong diagonal correlations.

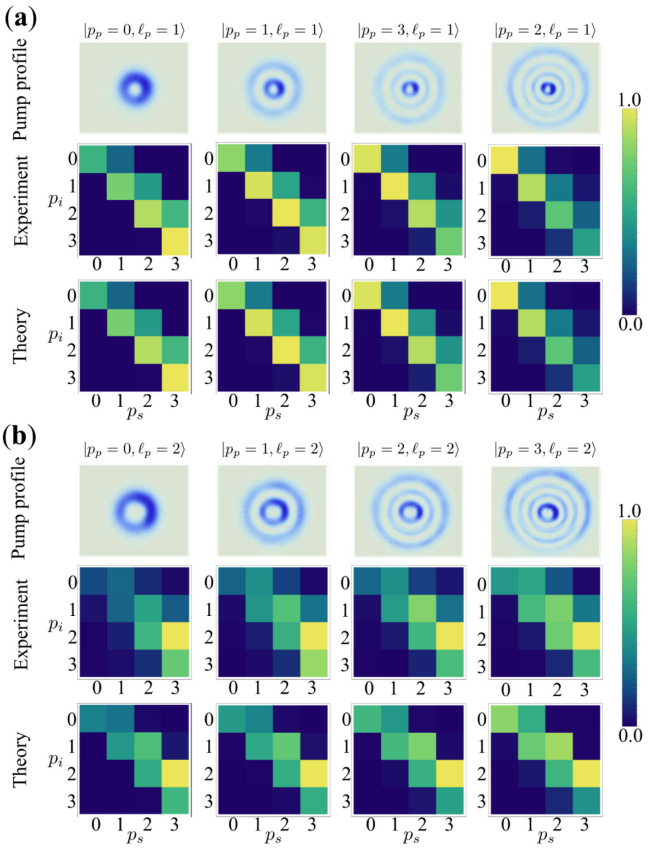


**Fig. 3.** Radial mode correlations with $LG_{p,\ell}$ pump beam. (a), (b) Respectively, experimental and theoretical radial mode correlations for pump $LG_{p,\ell}$ modes for $\ell_p = 1$ and $\ell_p = 2$. The corresponding intensities of the pump, measured on the crystal plane, are shown above the plots. In (a), we show the correlations for the subspace $\ell_s = 2$ and $\ell_i = -1$, while in (b), the results correspond to the subspace $\ell_s = 4$ and $\ell_i = -2$.

$\ell_s + \ell_i = \ell_p$ [see Fig. 1(c) and Supplement 1 for a discussion about the correlation shapes]. After setting $\ell_s$ and $\ell_i$, we explore the correlation matrices for the $p$-index of the LG mode, i.e., we measured the quantities $\mathcal{P}^{p_i,\ell_i}_{p_s,\ell_s} = \left|c^{p_i,\ell_i}_{p_s,\ell_s}\right|^2$ with $\ell_s + \ell_i = \ell_p$. The experimental results (Figs. 2 and 3), are compared with theoretical estimates based on Eq. (3), where the LG modes of signal and idler are considered with a waist parameter 0.2 times the waist of the pump. This value has been chosen as the one that gives the best agreement with the experimental data corresponding to the case $\ell_p = 0$, $p_p = 0$. We performed the experiments for $\ell_p = 0$, 1, 2 varying the pump radial index $p_p$ from $p_p = 0$ to $p_p = 3$. Figure 2 shows the results relative to the case $\ell_p = 0$ for some fixed values of signal and idler OAM subspaces. For low radial pump modes $p_p = 0$, 1, we observe diagonal correlations between the radial indices of signal $p_s$ and idler photon $p_i$, with small variations in the different subspaces. In general, off-diagonal correlations become more relevant by increasing either the pump radial index or the OAM subspace—it should be noted that these contributions change for different choices of the projection waists. Similar results for nonzero values of the pump OAM $\ell_p = 1$, 2 are shown in Fig. 3. In this case, we see that the different OAM absolute values of signal and idler photons are associated with an asymmetry in the correlation matrices.

Finally, we exploit our possibility to project the SPDC state onto arbitrary superposition states to perform the quantum tomography of a state defined in a 16-dimensional subspace of spatial modes. We fix the OAM state as $|\ell_i, \ell_p - \ell_i\rangle$ and span the radial index of the bi-photon to $p_i$, $p_s = 0$, 1, 2, 3. Such a state can be reconstructed using the procedure reported in [28,29]. The results of quantum state tomography for different pump states of $\ell_p = 0$ and $p_p = 0$, 1 are shown in Fig. 4.

The experimental results have a fidelity with theoretical prediction $\mathcal{F} = 0.71 \pm 0.01$ for $p_p = 0$ and $\mathcal{F} = 0.67 \pm 0.01$ for $p_p = 1$. The relatively low values of the fidelity can be ascribed to experimental issues such as dark counts as well as cross talk effects due to low count rates, which can be reduced employing detectors with better quantum efficiency and lower dark counts. Notwithstanding, $d = 16$ states with fidelity reported here would violate generalized Bell inequalities [29], and thus can be employed in high-dimensional quantum information processing such as high-dimensional quantum teleportation and communication.

We conclude by remarking that our analysis applies to any set of paraxial modes that can be reliably produced using a phase-only SLM, including transverse momentum modes, as recently shown in [30]. Our approach allows one to characterize the full spatial mode of bi-photon states, employing quantum state tomography beyond the OAM space. Introducing and employing radial modes, together with OAM, significantly increases the Hilbert space at the disposal of photonic quantum information processing without the need to reach mode orders with a large divergence.

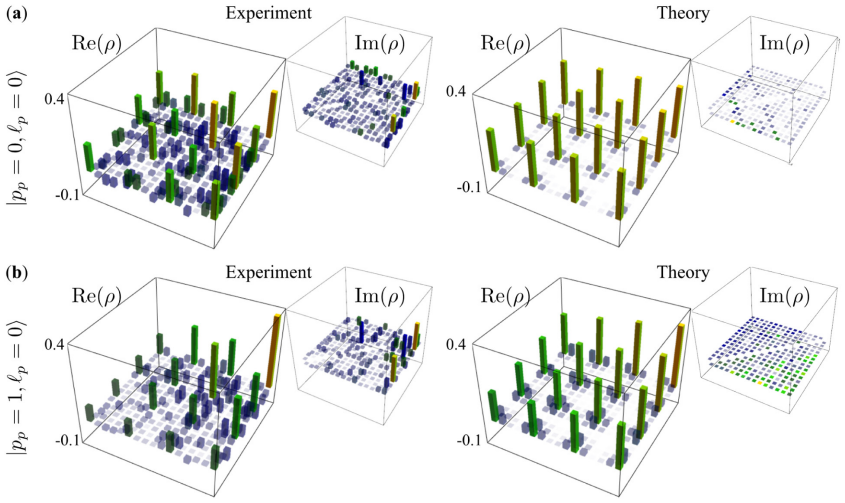


**Fig. 4.** State tomography for the OAM subspace. Experimental and theoretical plots of the bi-photon density matrix in an OAM subspace ($\ell_i = -\ell_s = 1$) for the LG pump beam with $\ell_p = 0$ and (a) $p_p = 1$ and (b) $p_p = 0$. We considered the subspace spanned by values of $p_s$ and $p_i$ going from zero to 3.

**Funding.** Canada Research Chairs; Canada First Research Excellence Fund (CFREF) Program; NRC-uOttawa Joint Centre for Extreme Quantum Photonics (JCEP); .

**Acknowledgment.** This work was supported by Canada Research Chairs (CRC), Canada First Research Excellence Fund (CFREF) Program, and NRC-uOttawa Joint Centre for Extreme Quantum Photonics (JCEP). The authors thank Sajedeh Shahbazi and Florian Brandt for their first attempt to design the experimental setup. M.R. would like to acknowledge the support of Mitacs Accelerate Fellowship.

**Disclosures.** The authors declare no conflicts of interest.

**Data Availability.** Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

**Supplemental document.** See Supplement 1 for supporting content.

## REFERENCES

1. S. P. Walborn, C. Monken, S. Pádua, and P. S. Ribeiro, Phys. Rep. **495**, 87 (2010).
2. C. Couteau, Contemp. Phys. **59**, 291 (2018).
3. A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature **412**, 313 (2001).
4. F. Flamini, N. Spagnolo, and F. Sciarrino, Rep. Prog. Phys. **82**, 016001 (2018).
5. 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).
6. N. Zhao, X. Li, G. Li, and J. M. Kahn, Nat. Photonics **9**, 822 (2015).
7. M. A. Bandres and J. C. Gutiérrez-Vega, Opt. Lett. **33**, 177 (2008).
8. E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd, Phys. Rev. A **89**, 013829 (2014).
9. M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, Proc. Natl. Acad. Sci. USA **111**, 6243 (2014).
10. D. Fu, Y. Zhou, R. Qi, S. Oliver, Y. Wang, S. M. H. Rafsanjani, J. Zhao, M. Mirhosseini, Z. Shi, P. Zhang, and R. W. Boyd, Opt. Express **26**, 33057 (2018).
11. N. K. Fontaine, R. Ryf, H. Chen, D. T. Neilson, K. Kim, and J. Carpenter, Nat. Commun. **10**, 1865 (2019).
12. X. Gu, M. Krenn, M. Erhard, and A. Zeilinger, Phys. Rev. Lett. **120**, 103601 (2018).
13. Y. Zhou, M. Mirhosseini, S. Oliver, J. Zhao, S. M. H. Rafsanjani, M. P. Lavery, A. E. Willner, and R. W. Boyd, Opt. Express **27**, 10383 (2019).
14. F. M. Miatto, A. M. Yao, and S. M. Barnett, Phys. Rev. A **83**, 033816 (2011).
15. D. Geelen and W. Löffler, Opt. Lett. **38**, 4108 (2013).
16. V. Salakhutdinov, E. Eliel, and W. Löffler, Phys. Rev. Lett. **108**, 173604 (2012).
17. Y. Zhang, F. S. Roux, M. McLaren, and A. Forbes, Phys. Rev. A **89**, 043820 (2014).
18. D. Zhang, X. Qiu, W. Zhang, and L. Chen, Phys. Rev. A **98**, 042134 (2018).
19. F. Bouchard, N. H. Valencia, F. Brandt, R. Fickler, M. Huber, and M. Malik, Opt. Express **26**, 31925 (2018).
20. E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, Opt. Lett. **38**, 3546 (2013).
21. J. Leach, B. Jack, J. Romero, A. K. Jha, A. M. Yao, S. Franke-Arnold, D. G. Ireland, R. W. Boyd, S. M. Barnett, and M. J. Padgett, Science **329**, 662 (2010).
22. E. Karimi and E. Santamato, Opt. Lett. **37**, 2484 (2012).
23. E. Karimi, R. Boyd, P. De La Hoz, H. De Guise, J. Řeháček, Z. Hradil, A. Aiello, G. Leuchs, and L. L. Sánchez-Soto, Phys. Rev. A **89**, 063813 (2014).
24. W. N. Plick and M. Krenn, Phys. Rev. A **92**, 063841 (2015).
25. A. Siegman, *Lasers* (University Science Books, 1986).
26. S. Liu, Z. Zhou, S. Liu, Y. Li, Y. Li, C. Yang, Z. Xu, Z. Liu, G. Guo, and B. Shi, Phys. Rev. A **98**, 062316 (2018).
27. E. V. Kovlakov, S. S. Straupe, and S. P. Kulik, Phys. Rev. A **98**, 060301 (2018).
28. N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White, Phys. Rev. Lett. **93**, 053601 (2004).
29. M. Agnew, J. Leach, M. McLaren, F. S. Roux, and R. W. Boyd, Phys. Rev. A **84**, 062101 (2011).
30. N. H. Valencia, V. Srivastav, M. Pivoluska, M. Huber, N. Friis, W. McCutcheon, and M. Malik, Quantum **4**, 376 (2020).

Research Article | Vol. 30, No. 12 / 6 Jun 2022 / Optics Express 21276
Optics EXPRESS

# Manipulating the symmetry of transverse momentum entangled biphoton states

XIAOQIN GAO,[1] YINGWEN ZHANG,[2,*] ALESSIO D'ERRICO,[1] FELIX HUFNAGEL,[1] KHABAT HESHAMI,[2,1] 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, K1A 0R6, Ottawa, ON, Canada
*[redacted]

**Abstract:** Bell states are a fundamental resource in photonic quantum information processing. These states have been generated successfully in many photonic degrees of freedom. Their manipulation, however, in the momentum space remains challenging. Here, we present a scheme for engineering the symmetry of two-photon states entangled in the transverse momentum degree of freedom through the use of a spatially variable phase object. We demonstrate how a Hong-Ou-Mandel interferometer must be constructed to verify the symmetry in momentum entanglement via photon "bunching/anti-bunching" observation. We also show how this approach allows generating states that acquire an arbitrary phase under the exchange operation.



## 1. Introduction

Quantum entanglement, considered one of the most counterintuitive features of quantum mechanics [1], is now one of the most important resources for quantum information tasks. In quantum optics it has been used as a fundamental tool in quantum cryptography [2], quantum dense coding [3], quantum teleportation [4], and quantum computation [5]. A great number of experiments have investigated the production of photonic entangled states, which have played a critical role in many important applications in quantum information processing. Photon pair generation through Spontaneous Parametric Down Conversion (SPDC) has been used to demonstrate entanglement in polarization [6], path [7], spatial modes (e.g., Hermite-Gauss modes [8,9], Laguerre-Gauss modes [10,11]), energy-time [12] and time-bin [13] degrees of freedom, and some of them simultaneously [14–17]. The SPDC state can also provide a good approximation of a momentum-position Einstein-Podolsky-Rosen (EPR) state when looking at the transverse momentum decomposition [15].

Momentum entanglement, as a continuous degree of freedom, can allow, in principle, to reach the ultimate limits of high-dimensional entanglement [15]. In addition, high-dimensional quantum systems can allow entanglement to have high complexity and can be exploited for various quantum information tasks [18–20]. The momentum entangled state that naturally arises from SPDC is symmetric [21], i.e., the same state is obtained under the exchange of idler and signal photon. However, it is more challenging to generate antisymmetric momentum entanglement. One possible approach that exploits the pump symmetry has been explored in Ref. [8]. The competition between the symmetry of polarization entanglement and pump shaping was shown to affect the two-photon interference behavior.

Here, we demonstrate an approach to freely manipulate the relative phase defining the two-photon entangled state by introducing a spatially dependent phase distribution on one of the photons in the pair (namely, the idler) path. A phase jump applied between opposite values of the idler photon's transverse momentum affects the exchange symmetry. A $\pi$-phase jump

#458776 https://doi.org/10.1364/OE.458776
Journal © 2022 Received 17 Mar 2022; revised 10 May 2022; accepted 10 May 2022; published 31 May 2022

Optics EXPRESS

allows conversion of the symmetric SPDC state into an antisymmetric one. Intermediate phase jumps will generate antisymmetric states, which gain a general phase factor under exchange operation. We also demonstrate how a two-photon interference setup needs to be constructed in order to verify the symmetry of such a momentum entangled state. This work provides a new method for quantum state engineering and entanglement verification in the momentum degree of freedom, which may be exploited in quantum imaging protocols, high-dimensional quantum communications, quantum information processing, and quantum simulations.

## 2. Scheme

The scheme we propose is based on a Type-II SPDC source of photon pairs. Exploiting the fact that idler and signal photons are orthogonally polarized, we can spatially separate the two photons with a polarizing beamsplitter (PBS). The vertically polarized photons are then converted to horizontally polarized by a half-wave-plate, therefore the resulting two-photon state (in the transverse momentum degree of freedom) can be written as $|\Psi\rangle = \frac{1}{\sqrt{2}} \int d^2\mathbf{k} (|\mathbf{k}\rangle_s|-\mathbf{k}\rangle_i + |-\mathbf{k}\rangle_s|\mathbf{k}\rangle_i)$. Note that we have assumed here a perfectly collimated pump in the thin-crystal limit. A phase object in the far-field of the crystal, placed in the idler path, implements the transformation $|\mathbf{k}\rangle_i \rightarrow e^{\phi(\mathbf{k})}|\mathbf{k}\rangle_i$. When post-selecting on correlated pairs of momentum values (i.e., $\mathbf{k_0}$ and $-\mathbf{k_0}$), we obtain the state:

$$|\Psi_\varphi\rangle = \frac{1}{\sqrt{2}}(|\mathbf{k_0}\rangle_s|-\mathbf{k_0}\rangle_i + e^{i\varphi(\mathbf{k_0})}|-\mathbf{k_0}\rangle_s|\mathbf{k_0}\rangle_i), \tag{1}$$

where $\varphi(\mathbf{k_0}) = \phi(\mathbf{k_0}) - \phi(-\mathbf{k_0})$, and we ignore a global phase factor.

The state symmetry can be analyzed through Hong-Ou-Mandel (HOM) interference. When the two photons are incident on a beamsplitter (BS), with the important requirement that the number of reflections up to the exit port of the BS has the same parity for both photons, they exit from the same output port if the relative phase is $\varphi = 0$ (bunching), while they always exit from different ports if $\varphi = \pi$ (anti-bunching). This can be immediately seen when measuring the coincidence counts between the two output paths $a$ and $b$ of the BS. More generally, for arbitrary phases $\varphi$, the (normalized) coincidence count rate is

$$C(\varphi) = 1 - \cos(\varphi), \tag{2}$$

which can be inverted to obtain $\varphi$ (modulo $\pi$) that characterizes the state completely.

## 3. Results

To experimentally test our scheme, we generated momentum entangled photon pairs in SPDC using a 5mm thick type-II PPKTP crystal pumped by a 405 nm continuous wave laser (the detailed experimental setup is illustrated in Fig. 1). The frequency-degenerate photon pairs are split in idler and signal path by a polarizing beamsplitter (PBS). A reconfigurable liquid crystal spatial light modulator (SLM) allows us to apply different phase patterns on the idler path. In particular, we implemented phase jumps along a vertical line centered on the SPDC cone. Idler and signal photons are then made to interfere at a 50:50 BS (after the signal polarization has been rotated to horizontal). The number of mirrors in the two paths was chosen in order to keep momentum anti-correlation at the BS output ports, i.e., ensuring that both photons are subject to the same number of reflections. The two output modes (paths $a$ and $b$) were then coupled to single-mode fibers in such a way that, on each path, opposite values of the transverse momentum were selected.

One thing to note is that this scheme requires photons with momentum $\mathbf{k}$ and $-\mathbf{k}$ to be present in both arms of the interferometer. Therefore, one cannot use a knife-edge prism or a D-shaped mirror to split the photons into two paths. This makes momentum entanglement

Optics EXPRESS

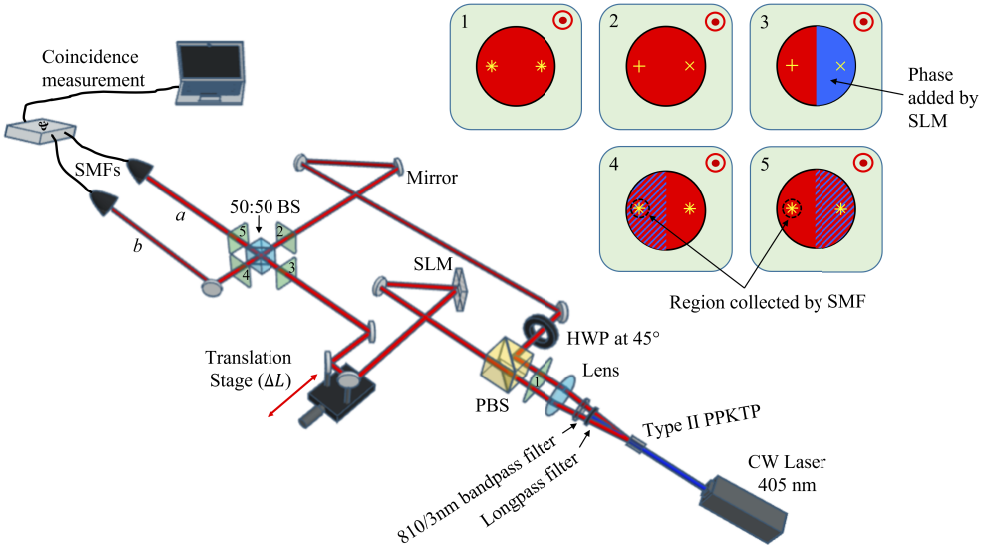


**Fig. 1. Experimental setup for generating momentum entanglement by quantum interference.** A horizontally polarized continuous-wave pump beam (405 nm, waist diameter 3.8 mm) induces polarization-based SPDC in a Type-II periodically poled potassium titanyl phosphate (ppKTP) crystal (5 mm thick). A lens is used to map the collinear SPDC state in the transverse momentum degree of freedom. Correlated photons with orthogonal polarizations are then separated into different optical paths with a polarizing beamsplitter (PBS) after a longpass filter and 3 nm bandpass filter. A half-wave plate (HWP) oriented at 45° rotates the vertically-linear polarization (V) of the signal photon to horizontal polarization (H). The two photons are then made to interfere at a 50:50 beamsplitter (BS). A delay line on the idler path allows for adjustments of the optical path difference $\Delta L$ between the two photons. A spatial light modulator (SLM) is placed in the idler photon path before the BS to allow manipulation of the phase between the momentum entangled state. The number of mirror reflections at the BS exit must have the same parity to have the two photons maintain momentum anti-correlated. Photons from opposite sides of the SPDC beam are collected by two single-mode fibers (SMFs) connected to avalanche photodiodes. Hong-Ou-Mandel interference can be observed after a coincidence measurement. The insets show the beam projections (beam coming out of the page) at the plane before the PBS (1) and the four numbered planes surrounding the 50:50 BS. (2,3) Before the BS with a phase applied in half of the beam (blue color) in (3). (4,5) After the BS showing how the two beams are overlapped and the region collected by the SMFs. Locations that are momentum correlated are marked with the same symbol (+ and ×).

Optics EXPRESS

manipulation using Type-I or Type-0 SPDC, where the photon pairs have the same polarization, much more difficult. The same technique can also be used for manipulating the transverse position entanglement between SPDC photons. This will require the parity of the number of reflections to be unequal in order to convert from a symmetric to an anti-symmetric position entangled state.

We recorded coincidence counts as a function of the path length difference $\Delta L$ between the two paths in the interferometer and for different phase jumps. The results are shown in Fig. 2, illustrating how applying a phase jump allows one to switch from two-photon bunching to two-photon anti-bunching, a clear indicator that the momentum entanglement has been converted from symmetric to anti-symmetric. The visibilities $v$ of the HOM dip in photon bunching and of the coalescence peak are defined as $v_{\text{peak}} = (C_{max} - C)/C$ and $v_{\text{dip}} = (C - C_{min})/C$, where $C_{max}$ and $C_{min}$ are the maximum and minimum coincidence counts at the peak and dip, respectively. $C$ is the coincidence count outside the dip/peak where the difference in the two path lengths is much larger than the coherence length of the SPDC photons.

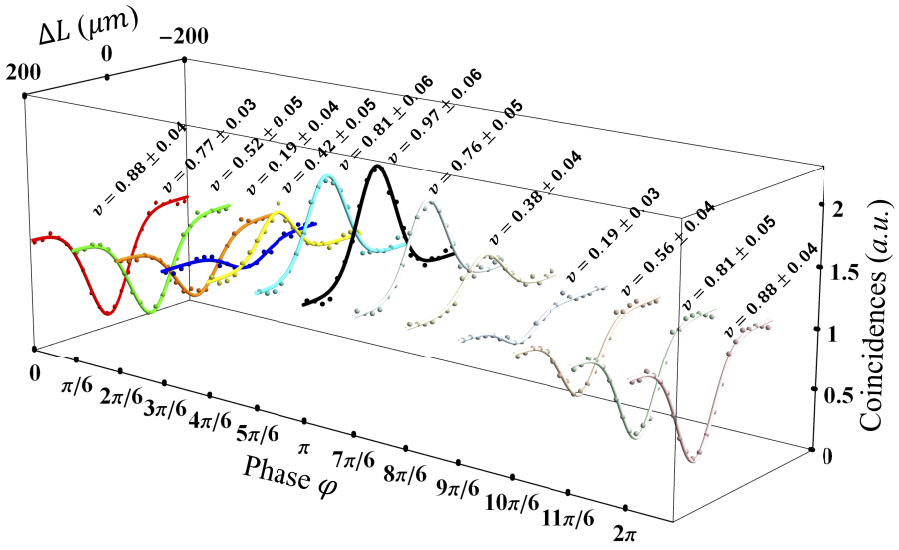


**Fig. 2. Two-fold normalized coincidence counts for different phase jumps.** The different colored data points and Gaussian fits correspond to phase ($\varphi$) changes every $\pi/6$ from 0 to $2\pi$. $\Delta L$ is the path length difference between the two photons before the BS. The coincidences are normalized by dividing the coincidence rate at $\Delta L = 0$ by that when $\Delta L$ is outside the HOM dip/peak. Error bars are smaller than the point markers and therefore not visible in the plot.

In Fig. 3, we verify that the coincidences at $\Delta L = 0$ follow Eq. (2). The visibilities for $\varphi = 0$ and $\pi$ give a direct estimate of the fidelity between the realized state and the expected symmetric/antisymmetric entangled state. We obtained $v \sim 88\%$ and $v \sim 97\%$, for $\varphi = 0$ and $\pi$, respectively. Intermediate cases correspond to the creation of entangled states which mimic two-particle states obeying anyonic statistics [22].

The visibilities do not quite reach 1 at $\varphi = 0$ and $\pi$, which is due to the imperfections in the alignment and the BS not being exactly 50:50. We have found the alignment which gave the highest visibility in the peak often deviated slightly from the alignment which gave the highest visibility in the HOM dip; this can be a result of small imperfections in the alignment and SLM calibration. We have aligned the setup by maximizing the HOM peak, thus resulting in the visibility at $\varphi = \pi$ being higher than $\varphi = 0$. Non-uniformity in the SLM will have only a small

Optics EXPRESS

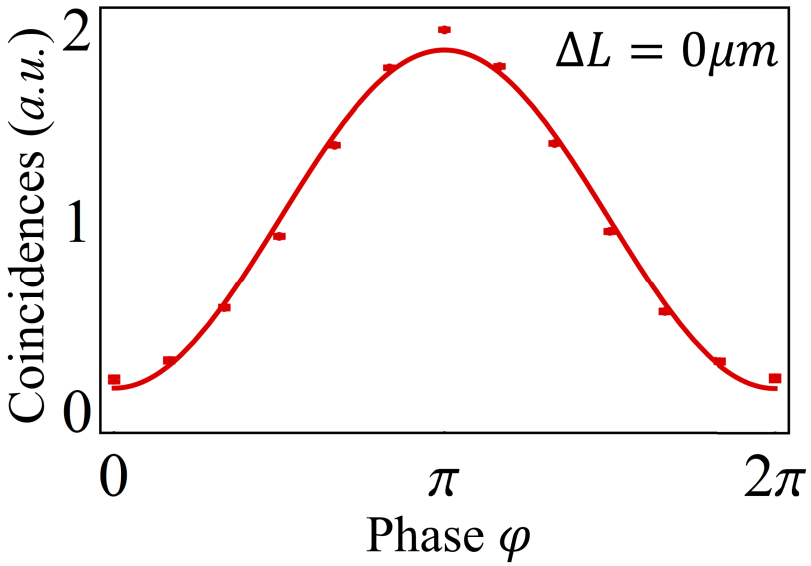


**Fig. 3. Coincidence counts as a function $\varphi$.** Plot showing the variation of coincidence counts as a function of the applied phase $\varphi$ when the path length difference $\Delta L$ between the two photons is 0. The equation of the fitted curve is $C(\varphi) = \alpha\,(1 - \cos(\varphi)) + \beta$, where $\alpha = 0.89 \pm 0.02$ and $\beta = 0.12 \pm 0.03$. The coincidences are normalized by dividing the coincidence rate at $\Delta L = 0$ by that when $\Delta L$ is outside the HOM dip/peak. Error bars are not visible, being smaller than the size of the data point circle.

affect in our experiment as we are collecting photons from two small regions on the SLM. If photons were collected from larger regions by using multi-mode fibers or camera, then the SLM uniformity would need to be considered.

## 4. Conclusions and outlook

Measurement of state symmetry using HOM interference has been demonstrated in various degrees of freedom, such as polarization [23], frequency [24–26], and Orbital Angular Momentum [11]. Here, we introduced and demonstrated a new method that allows, for the first time, the manipulation of transverse momentum entanglement between SPDC photon pairs through the use of a reconfigurable phase object (SLM), which allows to locally tune the state symmetry. We also demonstrated how a HOM interferometer must be constructed in order to verify the momentum entanglement symmetry. Simultaneously generating a state with spatially variable symmetry with thousands of momentum entangled modes can be performed in the near future and directly observed with recently developed time-tagging camera technologies [27,28]. This ability to manipulate and measure thousands of entangled modes would be greatly beneficial in quantum imaging protocols as well as in high-dimensional quantum communications, quantum information processing, and quantum simulations. However, this will require a high visibility multimode HOM interference in the spatial domain, a task that necessitates a careful engineering of SPDC spatial correlations, which requires the generation of a SPDC state with very high spatial correlation and compensation for the different SPDC cone sizes associated to the orthogonal polarizations.

**Funding.** Joint Centre for Extreme Photonics; High-Throughput and Secure Networks Challenge Program at the National Research Council of Canada; Canada First Research Excellence Fund; Canada Research Chairs.

**Acknowledgments.** The authors would like to thank Dilip Paneru and Frédéric Bouchard for valuable discussions.

Optics EXPRESS

**Disclosures.** The authors declare no conflicts of interest.

**Data Availability.** Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

## References


1. A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Phys. Rev. **47**(10), 777–780 (1935).
2. A. K. Ekert, "Quantum cryptography based on bell's theorem," Phys. Rev. Lett. **67**(6), 661–663 (1991).
3. C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," Phys. Rev. Lett. **69**(20), 2881–2884 (1992).
4. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," Phys. Rev. Lett. **70**(13), 1895–1899 (1993).
5. R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**(22), 5188–5191 (2001).
6. P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, "Observation of a "quantum eraser": A revival of coherence in a two-photon interference experiment," Phys. Rev. A **45**(11), 7729–7739 (1992).
7. T. B. Pittman, D. V. Strekalov, A. Migdall, M. H. Rubin, A. V. Sergienko, and Y. H. Shih, "Can two-photon interference be considered the interference of two photons?" Phys. Rev. Lett. **77**(10), 1917–1920 (1996).
8. S. P. Walborn, A. N. de Oliveira, S. Pádua, and C. H. Monken, "Multimode hong-ou-mandel interference," Phys. Rev. Lett. **90**(14), 143601 (2003).
9. Y. Zhang, S. Prabhakar, C. Rosales-Guzmán, F. S. Roux, E. Karimi, and A. Forbes, "Hong-ou-mandel interference of entangled hermite-gauss modes," Phys. Rev. A **94**(3), 033855 (2016).
10. E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd, "Exploring the quantum nature of the radial degree of freedom of a photon via hong-ou-mandel interference," Phys. Rev. A **89**(1), 013829 (2014).
11. Y. Zhang, F. S. Roux, T. Konrad, M. Agnew, J. Leach, and A. Forbes, "Engineering two-photon high-dimensional states through quantum interference," Sci. Adv. **2**(2), e1501165 (2016).
12. J. D. Franson, "Bell inequality for position and time," Phys. Rev. Lett. **62**(19), 2205–2208 (1989).
13. J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed energy-time entangled twin-photon source for quantum communication," Phys. Rev. Lett. **82**(12), 2594–2597 (1999).
14. D. V. Strekalov, T. B. Pittman, A. V. Sergienko, Y. H. Shih, and P. G. Kwiat, "Postselection-free energy-time entanglement," Phys. Rev. A **54**(1), R1–R4 (1996).
15. J. C. Howell, R. S. Bennink, S. J. Bentley, and R. W. Boyd, "Realization of the einstein-podolsky-rosen paradox using momentum- and position-entangled photons from spontaneous parametric down conversion," Phys. Rev. Lett. **92**(21), 210403 (2004).
16. J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, "Generation of hyperentangled photon pairs," Phys. Rev. Lett. **95**(26), 260501 (2005).
17. X.-L. Wang, X.-D. Cai, Z.-E. Su, M.-C. Chen, D. Wu, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "Quantum teleportation of multiple degrees of freedom of a single photon," Nature **518**(7540), 516–519 (2015).
18. M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, "Generation and confirmation of a (100 x 100)-dimensional entangled quantum system," Proc. Natl. Acad. Sci. **111**(17), 6243–6247 (2014).
19. J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, "Multidimensional quantum entanglement with large-scale integrated optics," Science **360**(6386), 285–291 (2018).
20. M. Erhard, M. Krenn, and A. Zeilinger, "Advances in high-dimensional quantum entanglement," Nat. Rev. Phys. **2**(7), 365–381 (2020).
21. M. D'Angelo, Y.-H. Kim, S. P. Kulik, and Y. Shih, "Identifying entanglement using quantum ghost interference and imaging," Phys. Rev. Lett. **92**(23), 233601 (2004).
22. L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, and R. Osellame, "Two-particle bosonic-fermionic quantum walk via integrated photonics," Phys. Rev. Lett. **108**(1), 010502 (2012).
23. K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," Phys. Rev. Lett. **76**(25), 4656–4659 (1996).
24. S. Ramelow, L. Ratschbacher, A. Fedrizzi, N. K. Langford, and A. Zeilinger, "Discrete tunable color entanglement," Phys. Rev. Lett. **103**(25), 253601 (2009).
25. A. Fedrizzi, T. Herbst, M. Aspelmeyer, M. Barbieri, T. Jennewein, and A. Zeilinger, "Anti-symmetrization reveals hidden entanglement," New J. Phys. **11**(10), 103052 (2009).
26. F. Kaneda, H. Suzuki, R. Shimizu, and K. Edamatsu, "Direct generation of frequency-bin entangled photons via two-period quasi-phase-matched parametric downconversion," Opt. Express **27**(2), 1416–1424 (2019).
27. M. Perenzoni, L. Pancheri, and D. Stoppa, "Compact spad-based pixel architectures for time-resolved image sensors," Sensors **16**(5), 745 (2016).
28. A. Nomerotski, "Imaging and time stamping of photons with nanosecond resolution in timepix based optical cameras," Nucl. Instrum. Methods Phys. Res., Sect. A **937**, 26–30 (2019).

# Chapter 4

# Quantum Key Distribution

Quantum communication is one of the most widely studied areas of quantum information and is one of the primary focuses of this thesis. The seminal work in quantum communication describing a protocol for quantum key distribution came in 1984 by Bennett and Brassard, thus creating the famous protocol BB84 [30]. QKD aims to provide information theoretic security, meaning that the security of the protocol does not rely on assumptions about the computational power of a an adversary. This initial proposal uses the polarization of single photons to encode information. We can encode a bit value "0" with a horizontally polarized photon, i.e., the quantum state $|H\rangle$, and a bit value of "1" with a vertically polarized photon, $|V\rangle$. These polarization states $\{|H\rangle, |V\rangle\}$ form an orthogonal basis for the polarization degree of freedom of the photon. This means that a projective measurement onto this basis can perfectly distinguish between incoming states. This projective measurement can be achieved by passing the photons through a polarizing beam splitter. The orthogonality of our polarization basis means that the projective measurement gives a definite outcome, i.e., the probabilities are "0" and "1" for our beam splitter projection as shown by

$$\begin{aligned} |\langle H|H\rangle|^2 &= 1 \\ |\langle V|H\rangle|^2 &= 0. \end{aligned} \tag{4.1}$$

In addition to the $\{|H\rangle, |V\rangle\}$ basis, there exist other orthognal bases for photonic polarization, namely the diagonal and antidiagonal polarizations which can be written in terms of the vertical and horizontal states as $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ respectively, as well as the left-and right-circularly polarized states, $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$. These states form what we will refer to as mutually unbiased bases (MUBs). What this means is that a measurement of some state in the wrong basis results in an uncertain outcome with probability 1/2 for each outcome. For example, projecting the state $|D\rangle$ onto state $|H\rangle$ or state $|V\rangle$ gives the measurement outcome $|\langle H|D\rangle|^2 = 1/2$ and $|\langle V|D\rangle|^2 = 1/2$. This equivalent probability of 1/2 for a measurement in the H/V basis means that we do not gain any information about the state when we measure in the incorrect basis and is the defining property of the MUBs. What this means from a communication perspective is that if a sender, "Alice", prepares a state in the H/V basis and a receiver "Bob" measures in that same H/V basis, they will be able to determine which state was sent by *Alice*. If however *Bob* measures in the incorrect basis, he gains no information about *Alice's* state.

## 4.1 BB84

We now have a good foundation to describe the BB84 protocol, and how it can achieve information theoretic security from eavesdropping attacks. We should first say that the role of quantum key distribution in secure communication is not to communicate the secret message, but to share a secure key, a random list of 1s and 0s, to be used by *Alice* and *Bob* for one-time-pad encryption. The one-time-pad is a proven secure method of encryption where *Alice* and *Bob* each have an encryption key of 1s and 0s that is the same length as their message. *Alice* can bit-wise add the one-time-pad to her message and send the encrypted message across a channel to *Bob* who can bit-wise add his matching key to the message to regain the original message. Though this encryption protocol is proven to be secure, the limiting factor is that this one-time-pad must be the length of the message

and can only be used once. This is where quantum key distribution comes into play as a method to enable the sharing of these one-time-pads or keys in a secure way. Now lets outline the steps involved in BB84:

1. *Alice* randomly chooses a basis H/V or A/D and randomly chooses a state in that basis to prepare as single photon state, i.e., $\{|H\rangle = 0, |V\rangle = 1\}$ or $\{|D\rangle = 0, |A\rangle = 1\}$. This random choice of basis and state should be done using 2 quantum random number generators to ensure the randomness of the choices. Alice then sends the single photon states across the quantum channel to Bob.

2. Bob then randomly chooses which basis to make a measurement in, H/V or A/D, and performs the projective measurement on the incoming single photon state. This single photon measurement will give a "click" at only 1 detector and Bob records the result.

3. Next Alice and Bob communicate across a classical channel which must be authenticated but not necessarily private, where they share the preparation and measurement basis used for each photon. They do not reveal the state that was sent or measured, which is the information that will become the key.

4. Alice and Bob now perform the sifting operation where they remove all of the bins where the prepariation and measurement was not completed in the same basis. This leaves them with 50% of the original states.

5. Next Alice and Bob take a subset of the remaining key and reveal which states were prepared and measured. These states will be thrown out as the information is being broadcast to the world, but this allows them to determine the error rate between the sent and received states. This error rate allows Alice and Bob to determine if an eavesdropper has been intercepting the signal and gaining some information about the quantum states. The maximumm tollerable error rate for the BB84 protocol is 11%.

6. Finally based on the measured error rate between Alice and Bob, classical error correction protocols are used, and privacy amplification protocols are implemented to remove any of Eve's information.

At this point Alice and Bob have a secret key which can be used for one-time-pad encryption. There are many other QKD protocols that have been developed over the last 40 years, some of which will be discussed later on in this thesis. For example, we can replace this prepare and measure approach with an entanglement based QKD scheme. Instead of Alice choosing which state and basis to prepare, she will have an entanglement source which produces photons in a state similar to those introduced in Chapter 2. In this form, our intuition from the no-cloning theorem is very useful for proving the security, and it has been shown that entanglement basis protocols can be translated back to a prepare and measure approach for QKD applications [31]. Here Alice and Bob perform a Bell test to confirm that they have entangled photon states and with this information they can guarantee that no other system is correlated with $\rho_{AB}$.

## 4.2 Security Proofs

We have stated that the BB84 protocol described above is a secure protocol but still need to provide some basis for this security. There are a few different physical principles that we can use to demonstrate the security of QKD. As mentioned in Chapter 1, the uncertainty principle makes it impossible for us to precisely know conjugate variables in quantum systems. This is closely related to the measurement problem in quantum mechanics which dictates that any measurement by Eve on unknown quantum states will introduce some disturbance in the system. These disturbances can then be detected by Alice and Bob. Alternatively, we can think of Eve's intent as being to create a perfect copy of the states sent from Alice to Bob to then be used for her own measurements. This however is forbidden for quantum systems by the *no-cloning theorem* [32,33]. The quantum no cloning theorem states that we cannot create an identical copy of an unknown quantum state.

If we have no knowledge of some quantum state $|\phi\rangle$, and we have some ancillary state $|e\rangle$ then there is no unitary operator $U$ that can act on the composite system to give $U\left(|\phi\rangle_A \otimes |e\rangle_B\right) \rightarrow |\phi\rangle_A \otimes |\phi\rangle_B$. In the context of QKD and in particular BB84, this no cloning theorem tells us that when a single photon is sent in a random basis, some eavesdropper can not create any device to perfectly replicate this state. We can also use entangled pairs which have quantum correlations satisfying the violation of Bell's inequality to demonstrate that there could be no outside (Eve's) knowledge about that entangled state. In other words, if Alice and Bob can violate Bell's inequality with some entangled photon pairs, then Eve can not have any information about the quantum state. From these physical principles which provide the underlying basis of our security, we will be in a position to evaluate the security of specific protocols from an information theory perspective [34].

Security proofs can be formulated for specific quantum protocols from the basis of the physical principles of quantum mechanics. These proofs will assume that an eavesdropper is very powerful and has access to any technologies allowed by quantum theory, whether such technologies exist yet or not. We can begin with a simple example of a basic attack that an eavesdropper can perform called the intercept-resend attack. In the polarization BB84 protocol described above, Eve will intercept the photons sent from Alice and make a measurement in some basis. The measurement is the same as Bob's measurement and a single click will be recorded at the output of a polarizing beam splitter, lets say in the H/V basis. Eve then records this information and prepares a photon in the measured state to resend on to Bob. Now the problem with Eve's attack is that she does not know which basis to measure in, and thus she will measure in the wrong basis 50% of the time. Let's say Alice sent the state $|D\rangle$ and Eve measured this in the H/V basis giving the measurement result $|H\rangle$ with probability 1/2. She then sends this state to Bob where a measurement in the D/A basis and will give $|D\rangle$ with probability 1/2 and $|A\rangle$ with probability 1/2. When Eve measures in the correct basis, no errors are introduced. Thus in total Eve introduces a quantum bit error rate of 25%, i.e., 50% chance of measuring in the incorrect basis multiplied by a 50% chance of Bob's measurement yielding the correct state.

If Alice and Bob now considered this the only attack that Eve could perform then they would set 25% as the error threshold for this protocol. However, there are more sophisticated attacks which Eve can perform to gain more information about the quantum states which result in the 11% threshold. The Lo-Chau security proofs were developed first for a scheme in which Alice and Bob share entangled pairs and then perform quantum error correction to distil entanglement from a joint state $\rho_{ABE}$ which is correlated to a quantum state $\rho_E$ held by Eve, to an entangled state $\rho_{AB}$ which is not correlated to Eve [35]. The quantum error correction in the entanglement approach requires 2 steps, one for the bit errors and one for the phase errors. There is a cost associated with each error correction step which is associated to the Shannon entropy, $H(e) = -e\log_2(e) - (1-e)\log_2(1-e)$. This results in an entanglement pair generation rate of

$$G = 1 - H(e_b) - H(e_p), \tag{4.2}$$

where $e_b$ and $e_p$ are the bit and phase error rates. This proof was shown to be equivalent to a prepare and measure QKD scheme by Shor and Preskill who translated the quantum error correction to a classical error correction step and a privacy amplification step, both performed after measurement of the photons and thus not requiring a quantum memory [36]. The classical error correction and privacy amplification also have a cost associated to the Shannon entropy and the bit error rate $e_b$ which gives us the similar key rate formula for the prepare and measure scheme $G = 1 - 2H(e)$. The key rate crosses zero at 11% thus giving the 11% bound the BB84 protocol.

This assumes, as in the original BB84 protocol, that Alice and Bob send optimal single photon states such as those resulting from heralded pairs from a spontaneous parametric down conversion (SPDC) single photon source. However, it is difficult to create ideal single photons, and even those from SPDC have some likelihood of 2 pairs being created at once. The security proofs become significantly more involved when we depart from the optimal world envisioned by Bennet and Brassard and introduce real devices with imperfections. There exist numerous "side-channel" attacks which exploit imperfections in the physical devices used to establish the quantum channel. There are 3 different classes of attacks

which Eve can perform to gain information about the channel. When we consider the security of the channel we must consider each of these attacks and decide to which level of attack we want to secure against. In increasing levels of strength these are the individual, collective, and coherent attacks. An individual attack is the simplest type of attack Eve can perform which involves interacting with each qubit sent between Alice and Bob separately. The prepare and measure attack is an example of this type of attack. Next there are collective attacks in which an ancilla interacts with each qubit independently, but then Eve performs a joint measurement on the ancilla. Finally a coherent attack is the most powerful where Eve prepares a joint entangled state as an ancilla which interacts on qubits in the channel before a joint measurement is performed by Eve. This final class of attacks are not necessarily technologically realizable yet, but do represent the upper bound on Eve's power from the limits of the laws of physics. This is the level that we consider with the security proofs considering the shared entanglement between Alice and Bob.

One example is the *photon number splitting attack* which allows Eve to gain information when Alice sends more than 1 photon per pulse. If 2 photons are present in the same state sent from Alice to Bob, then Eve can break off 1 photon and make any desired measurement without introducing any disturbance to the quantum signal. The difficulty here is that creating single photon states on demand is a very difficult technological problem, though work on single photon emitters is ongoing [23]. One can use SPDC which allows us to guarantee that there is only 1 photon per pulse by heralding. However, as evident by the name, this is a spontaneous process and usually with robust technology we do not want to wait for a random event to occur. So one may consider using a regular laser pulse but attenuating the source down to the level of 1 photon per pulse. This results in the well known *coherent state* which has a photon number distribution described by

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{4.3}$$

where $|n\rangle$ denotes an "$n$" photon state. Now we can have a photon number state which is a distribution centred at the mean photon number $N = |\alpha|^2$. For QKD we want just

a single photon, i.e., $|1\rangle$, and we never want more than 1 photon. The problem is if we prepare a coherent state with $|\alpha|^2 = 1$ then we will also get the $|2\rangle$ state with significant probability around 18%. If we instead go with a much weaker signal such as $|\alpha|^2 = 0.1$, we will get the $|2\rangle$ state with much lower probability of 0.45%. However now we only have a signal $|1\rangle$ state around 10% of the time, resulting in a reduction in the maximum key rate we can achieve. This remaining non-zero probability of a 2-photon state also allows for some small amount of information to be leaked to Eve which must be accounted for in the security analysis and gives a reduction in the achievable key rate. The problem of imperfect sources was addressed with the decoy state protocol where decoy states with a different average photon number are sent through the channel randomly with the signal [37, 38]. The differences in quantum bit error rates between the decoy and signal states can then be compared to detect a photon number splitting attack. We will not go through the many different attacks that have been conceived for taking advantage of device imperfections and the layers of security and new security proofs that have been developed to overcome these weaknesses.

## 4.3 High-Dimensional QKD

For many applications in quantum information science, we are only concerned with 2-dimensional quantum systems. In quantum computing, while there have been proposals of using high-dimensional qudits, 2-d states vastly dominate the research and industry efforts. In the original BB84 protocol for quantum communication, the 2-d polarization degree of freedom of photons is used. We can however consider extending to high-dimensions particularly for quantum communication where we can hope to achieve greater informational capacity per single photon. We can extend protocols such as BB84 to high-dimension Hilbert spaces which can provide certain beneficial properties in terms of information density, key rates, and tolerance to errors [39]. As a first example we can consider the high-dimensional BB84 protocol. Here we will still use two MUBs, but the dimensionality of each basis will

be $d > 2$. The first basis will still be the logical basis in whatever degree of freedom is being used, i.e., $|\psi\rangle_j = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. One of the mutually unbiased bases in dimension "d" when $d$ is prime is given by the quantum Fourier transform,

$$|\phi\rangle_j = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega_d^{jk} |k\rangle \tag{4.4}$$

where $\omega_d = e^{i2\pi/d}$. The projection of a state on the wrong MUB now gives $|\langle\psi|\phi\rangle|^2 = 1/d$ instead of $1/2$ as in the $d = 2$ case.

In dimensions that are prime or the power of a prime number, i.e., 2,3,4,5,7,8 ..., it has been proven that we can produce d+1 different MUB and for prime dimensions we can use the formula

$$\left|\phi_j^{(\alpha)}\right\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} (\omega_d^j)^{d-k} (\omega_d^{-(\alpha-1)})^{s_k} |k\rangle, \tag{4.5}$$

for the $\alpha \geq 1$ basis, and the $j_{th}$ state in the basis. Here $s_j = j + \ldots + (d-1)$.

Security proofs have been extended from the BB84 protocol to show the security of high-dimensional BB84 style protocols [40]. The secret key rate for a high-dimensional BB84 protocol is given by,

$$G = \log_2(d) - 2h^{(d)}(e), \tag{4.6}$$

where $h^{(d)}(e) = -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the $d$-dimensional Shannon entropy. Furthermore, high-dimensional states have allowed for the development of unique new protocols such as the Round-Robin Differential-Phase-Shift, Chau-15, and tomographic quantum cryptography protocols [41–43]

An important piece of quantum information is quantum tomography. As illustrated by the Heisenberg uncertainty principle, we can not learn all of the information about a quantum system with a single measurement. With quantum state tomography, we attempt to reconstruct the density matrix, $\rho$, by making many measurements on an ensemble of many copies of the state. By making various different measurements on these copies we can reconstruct all of the information about the state. To illustrate this, consider the

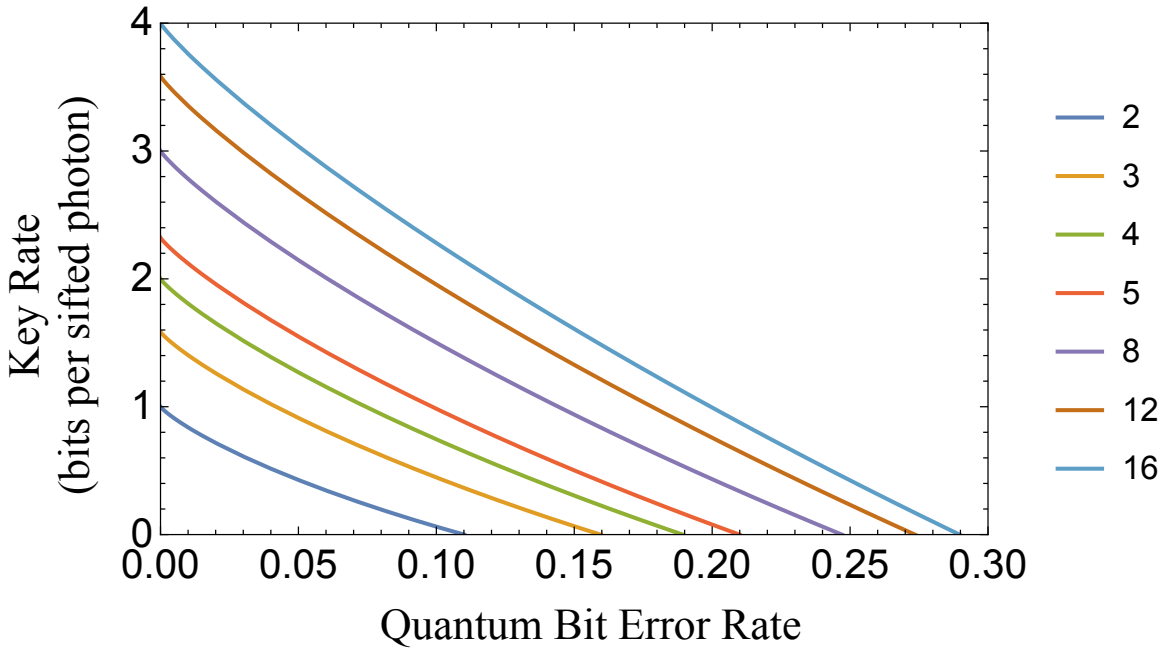


Figure 4.1: **BB84 Key Rates**. The error threshold for BB84 and other QKD protocols increases with the dimensionality of the encoding space. This allows for a higher error tolerance in noisy channels.

polarization of a photon. We can measure polarization by placing single photon detectors at the output ports of a polarizing beam splitter. This however will only give us a conclusive result if we have a vertical or horizontally polarized photon. If we then choose to place a half-wave plate before the polarizing beam splitter, we can measure the diagonal and anti-diagonal component of the copies of the quantum system. Finally with the introduction of a quarter-wave plate, we can measure the left and right circular component. We now have 6 experimentally determined probabilities, $P_H, P_V, P_D, P_A, P_R$, and $P_L$. With these six measurements, we can now precisely determine the density matrix of the quantum state. Quantum state tomography is an extensive area of study as the number of measurements required to characterize a state scales with the square of the dimensionality of the state,

specifically using the approach presented for polarization it scales as $d(d+1)$. This is the MUB approach to state tomography, though as we will discuss, there may be a more optimal set of measurements. Each of these measurements can be represented by a projection operator $\hat{E}_i$. We call a complete set of these measurement operators comprises a positive operator-valued measure (POVM). One approach to reconstructing the density matrix is using linear inversion and relying on the Born rule which states that the probability of getting a certain measurement outcome from the measurement operator $\hat{E}_i$ for a quantum state $\rho$ is given by $P_i = \text{Trace}(\hat{E}_i\hat{\rho})$. Note that for a pure state $|\psi\rangle$, we can rewrite the trace as $\text{Trace}(\hat{E}_i |\psi\rangle \langle\psi|) = \langle\psi| \hat{E}_i |\psi\rangle$. In 2 dimensions we use the familiar Pauli matrices $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ to determine the density matrix as $\hat{\rho} = \mathbb{I} + s_1\hat{\sigma}_1 + s_2\hat{\sigma}_2 + s_3\hat{\sigma}_3$ where $s_i$ are the Stokes parameters composed of the expectation values of the Pauli matrices, i.e., $s_i = \hat{\sigma}_i$. For the polarization of a photon, the Stokes parameters are determined by the probabilities discussed above by: $s_1 = P_H - P_V$; $s_2 = P_A - P_D$; and $s_3 = P_L - P_R$.

We can extend to high-dimensional quantum state tomography using the MUBs defined in Equation 4.5. The MUB projectors are given by $\hat{\Pi}_j^{(\alpha)} = |\psi_j^{(\alpha)}\rangle\langle\psi_j^{(\alpha)}|$. The MUBs form an overcomplete set of $d+1$ bases and the orthonormality and completeness relations are given by

$$\sum_{\alpha=0}^{d}\sum_{j=0}^{d-1}\frac{\hat{\Pi}_j^{(\alpha)}}{d+1} = \mathbb{I} \tag{4.7}$$

$$\text{Tr}[\hat{\Pi}_j^{(\alpha)}\hat{\Pi}_i^{(\beta)}] = \delta_{ij}\delta_{\alpha\beta} + \frac{(1-\delta_{\alpha\beta})}{d}. \tag{4.8}$$

Now similar to the 2-dimensional case, we can obtain measurement probabilities for each state given by $P_j^{(\alpha)} = \text{Tr}[\hat{\rho}\,\hat{\Pi}_j^{(\alpha)}]$ and the density matrix can be reconstructed by

$$\hat{\rho} = \sum_{\alpha=0}^{d}\sum_{j=0}^{d-1} P_j^{(\alpha)}\hat{\Pi}_j^{(\alpha)} - \mathbb{I}. \tag{4.9}$$

This approach requires $d(d+1)$ measurements and is often a convenient approach to state reconstruction [44]. There are also more optimal approach such as using states that are optimally spread out on the Hilbert space to have minimal overlap. This has been achieved

with symmetric informationally complete (SIC) POVMs, and state reconstruction can be reduced to requiring only $d^2$ measurements [45, 46].

## 4.4 Adaptive Optics

Adaptive optics systems were proposed for correcting imaging aberrations in astronomical applications in 1953, and early experimental implementations began in the 1960's and 1970's led by military applications to track satellites and eventually reaching the academic astronomy community [47, 48]. In free-space quantum communication, adaptive optics has

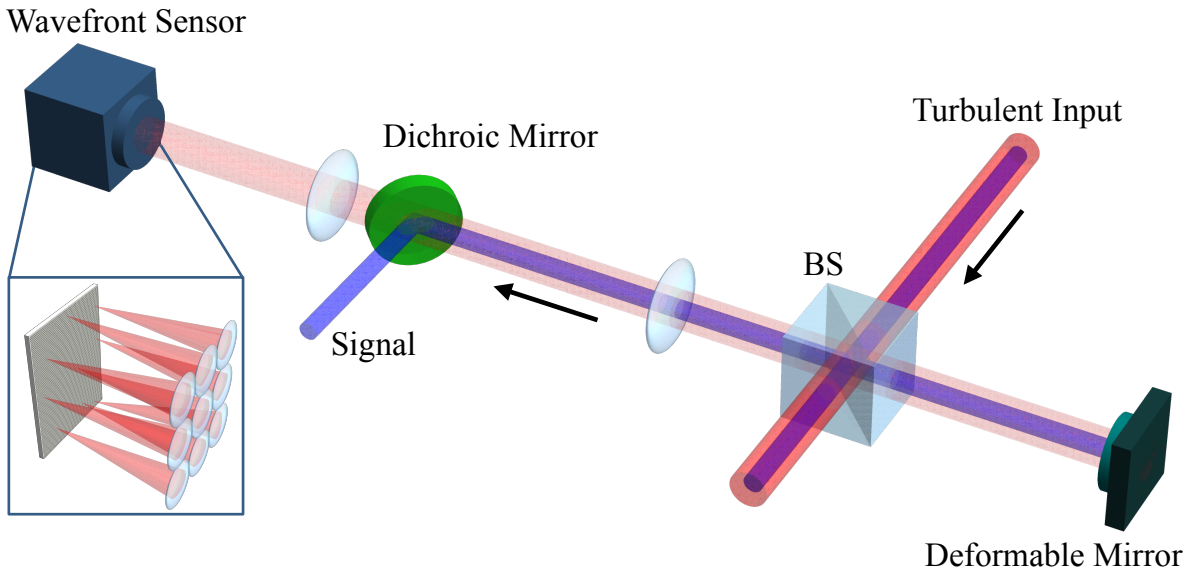


Figure 4.2: **Adaptive Optics**. The input beam is sent to a deformable mirror and then onto a wavefront sensor which measures the phase. A dichroic mirror is used to separate the guide beam from the signal to be used for QKD.

a very important role in improving key rates and allowing for the use of spatial modes. Free-space optical channels have non-uniform temperature and pressure cells along the

propagation which results in a spatially varying index of refraction. This introduces a non-uniform transverse phase to the beam, which results in distortions or deflections at the receiver. The lowest order of these distortions are the *tip-tilt* deviations which describe beam wandering in the x and y direction. The higher orders of distortions are described by the Zernike polynomials which are a set of orthogonal modes on the unit disk.

An adaptive optics system is made up of a Shack-Hartmann wavefront sensor and a deformable mirror. The wavefront sensor is used to measure the phase of the incoming optical beam. It consists of an array of microlenses followed by an EMCCD camera which measures the transverse position of the focus from the mircolens array. The position of the focus allows us to determine the wavefront tip and tilt at each microlens. The wavefront sensor in our work contains a 16 by 16 microlens array giving 256 points for estimating the wavefront. When a Gaussian mode is sent across the channel, any deviations from a flat phase can be attributed to the atmospheric turbulence. The inverse of the phase measured at the wavefront sensor is then applied to the incident beam using the deformable mirror. The deformable mirror has a soft surface with a number of actuator pistons which are able to extend or retract at each point of the mirror to dynamically correct the phase. The deformable mirror used in our work has a 22.5 mm diameter and 97 actuators.

In the rest of the chapter, 3 articles on high-dimensional quantum communication are presented. The first presents a new form of the Round Robin QKD protocol which allows Alice and Bob to place an upper bound on the information leaked to Eve without monitoring the error rate in the channel. The second outlines the use of high-dimensional states for quantum certified deletion, and includes an experimental demonstration using OAM. The third is an experimental demonstration of a full-functioning, fast adaptive optics system for the correction of atmospheric turbulence on high-dimensional OAM states.

# High-dimensional Encoding in the Round-Robin Differential-Phase-Shift Protocol

Mikka Stasiuk[1,2], Felix Hufnagel[3,1], Xiaoqin Gao[3,1], Aaron Z. Goldberg[1,3], Frédéric Bouchard[1], Ebrahim Karimi[3,1], and Khabat Heshami[1,3]

[1]National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada
[2]Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, N2L3G1 Waterloo, Ontario, Canada
[3]Nexus for Quantum Technologies, University of Ottawa, Ottawa, K1N 6N5, ON, Canada

In quantum key distribution (QKD), protocols are tailored to adopt desirable experimental attributes, including high key rates, operation in high noise levels, and practical security considerations. The round-robin differential phase shift protocol (RRDPS), falling in the family of differential phase shift protocols, was introduced to remove restrictions on the security analysis, such as the requirement to monitor signal disturbances, improving its practicality in implementations. While the RRDPS protocol requires the encoding of single photons in high-dimensional quantum states, at most, only one bit of secret key is distributed per sifted photon. However, another family of protocols, namely high-dimensional (HD) QKD, enlarges the encoding alphabet, allowing single photons to carry more than one bit of secret key each. The high-dimensional BB84 protocol exemplifies the potential benefits of such an encoding scheme, such as larger key rates and higher noise tolerance. Here, we devise an approach to extend the RRDPS QKD to an arbitrarily large encoding alphabet and explore the security consequences. We demonstrate our new framework with a proof-of-concept experiment and show that it can adapt to various experimental conditions by optimizing the protocol parameters. Our approach offers insight into bridging the gap between seemingly incompatible quantum communication schemes by leveraging the unique approaches to information encoding of both HD and DPS QKD.

## 1 Introduction

The advent of quantum key distribution demonstrated the ability to use quantum physics in public key cryptography and established one of the most studied aspects of quantum technologies. Bennet and Brassard, with the BB84 protocol, showed that encoding in two mutually unbiased bases (MUB) and randomly alternating between these encodings enables the generation of a secure random key between two parties [1]. Any intervention to gain access to the random key results in detectable noise at the receiver and allows for the removal of unsecure key generation attempts [2, 3]. Monitoring noise has become the key element in developing a variety of quantum key distribution approaches [4, 5, 6, 7, 8]. Recently, Sasaki *et al.* [9] showed a different approach to encoding random binaries in a

Frédéric Bouchard: [redacted]

quantum state for quantum key distribution which did not require monitoring the signal disturbance. Utilizing a quantum state in a large Hilbert space of dimension $L$, mapping random phases (therefore random phase differences) between basis vectors of the state, and a randomized interferometric measurement at the receiver lead to a fundamental bound on the mutual information between the sender and a potential eavesdropper. This introduced an entirely different approach to enforcing security in quantum key distribution [10, 11, 12, 13]. Subsequently, several experiments used temporal [14, 15, 16, 17, 18, **?**, 19] and spatial [20] structures of photons to implement this protocol, also known as the Round-Robin Differential Phase Shift (RRDPS) protocol.

Advances in the preparation and measurement of high-dimensional quantum states of photons using the temporal and spatial degree of freedom motivated implementations of quantum key distribution protocols where photons carried more than one bit each. This proved beneficial at increasing secret key rates and noise tolerance [21, 22, 23, 24, 25, 26, 27, 28, 29, 30]. Notably, the issue of noise tolerance is of particular interest in the context of satellite-based QKD [31, 32, 33, 34, 35]. In this work, we explore the possibility of increasing the encoding space of the secret keys in the RRDPS setting. We show that a high-dimensional quantum key distribution with and without monitoring signal disturbance is possible. Our approach both exploits the previously untapped potential of the original RRDPS encoding scheme and offers an avenue to explore the connection between the RRDPS and BB84 protocols. We structure the paper as follows. We first introduce the high-dimensional RRDPS (HD-RRDPS) protocol. A simple sketch of the security analysis is presented. We then carry out a proof-of-principle experiment to investigate the performance and limitations of our scheme in a practical setting. Our experiment exploits the orbital angular momentum (OAM) degree of freedom of single photons, which has been demonstrated as an invaluable testbed to investigate quantum communication schemes. However, we note that our protocol can also be implemented in other degrees of freedom, such as time-bins, given appropriate measurements [36]. Finally, in the discussion, we discuss adaptations to protocol parameters that enable better performance of the HD-RRDPS protocol for varying amounts of channel loss and characterize the circumstances under which the fundamental gap between the RRDPS and BB84 protocols can be closed. This conceptual gap can be seen both in the encoding scheme and in the security analysis for each protocol.

## 2 Protocol

We introduce the HD-RRDPS protocol as an extension of the established RRDPS protocol to a larger alphabet. In the original protocol, a superposition of pulses with randomly assigned phases of 0 or $\pi$ resulted in constructive or destructive interferences at the measurement stage. The natural extension of this encoding scheme is achieved by considering a MUB in larger dimensions. The formal key generation of the HD-RRDPS protocol is presented below.

(1) Alice prepares a state $|\psi\rangle$ consisting of a superposition of $L$ modes which determines the dimension of the Hilbert space. In the time domain, this corresponds to a packet of $L$ pulses. Each mode is modulated by a phase $2\pi k_j/d$, where $k_j \in \{0, 1, 2, ..., (d-1)\}$, and the parameter $d$ is called the encoding dimension and satisfies $2 \leq d < L$, i.e.,

$$|\psi\rangle = \frac{1}{\sqrt{L}} \sum_{j=1}^{L} e^{i\frac{2\pi k_j}{d}} |j\rangle. \tag{1}$$

(2) Upon receiving the signal state from Alice, Bob randomly selects a subset of $d$

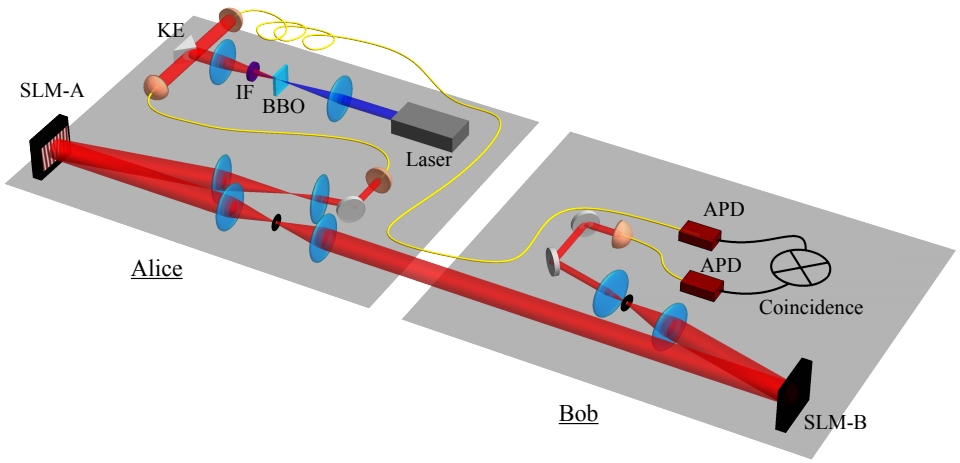


Figure 1: **Experimental Setup**. Alice generates heralded single photons at a center wavelength of 810 nm coupled to a single-mode fiber (SMF) via spontaneous parametric downconversion (SPDC) by pumping a barium borate (BBO) crystal with a diode laser at a center wavelength of 405 nm. The signal and idler photons are then spatially separated using a knife-edge (KE) mirror. We note that the pump laser is filtered using an interference filter (IF). The idler photon is subsequently used to gate Bob's measurement using coincidence measurement. Upon exiting the SMF, the signal photon is sent to a sequence of 4-f lens systems and a spatial light modulator (SLM). Alice's prepared state, $|\psi\rangle$, is encoded by imprinting the appropriate phase and intensity profile onto the signal photon using a holographic technique with SLM-A. The encoded photons are then sent to Bob's stage, where a second SLM (SLM-B) is used to measure the MUB elements, i.e. $|\varphi_m^{(d)}\rangle$. Finally, the signal and idler photons are measured using single-photon avalanche photodiode (APD) detectors and coincidence measurement.

modes out of the $L$ total modes, i.e. $\{|j_0\rangle, |j_1\rangle, ..., |j_{(d-1)}\rangle\} \subset \{|1\rangle, |2\rangle, ..., |L\rangle\}$, where we also have that $j_0 < j_1 < ... < j_{d-1}$. After selecting the $d$-dimensional subset, Bob performs a measurement in the MUB given by $\{|\varphi_m^{(d)}\rangle; m \in \{0, 1, ..., d-1\}\}$, where

$$|\varphi_m^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} e^{i\frac{2\pi mn}{d}} |j_n\rangle. \tag{2}$$

The outcome of the MUB measurement is used to generate the raw key, $m$, which is attributed to a measurement of the state $|\varphi_m\rangle$. Moreover, Alice and Bob only keep the measurement outcomes where the state received by Bob is an element of the MUB that is being measured, i.e. $\frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} e^{i\frac{2\pi k_{j_n}}{d}} |j_n\rangle \in \{|\varphi_m^{(d)}\}$.

(3) Finally, Bob shares the values of $\mathcal{J} = \{j_0, j_1, ..., j_{(d-1)}\}$ with Alice. They can then form their final shared secure key by performing the standard classical post-processing consisting of error reconciliation and privacy amplification.

## 3 Results

A sketch of the security proof of the HD-RRDPS is presented here in the single-photon case. We follow the procedure presented in [11]. A detailed calculation can be found in Appendix A.

We consider the strategy adopted by the eavesdropper, Eve, where she implements a general collective attack given by $U_{\text{Eve}}|j\rangle|e_{00}\rangle = \sum_{\ell=1}^{L} c_{j\ell}|\ell\rangle|e_{j\ell}\rangle$. The Holevo bound on

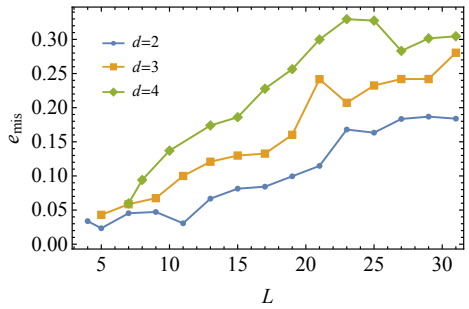


Figure 2: **Experimental characterization of mode mismatch**. Experimental averages for the mode mismatch, $e_{\mathrm{mis}}$ are shown for different values of the dimension, $d$, and the size of the encoding Hilbert space, $L$.

Eve's reduced density matrix can be used to estimate the leaked information to Eve. For the protocol parameters $L$ and $d$, the bound on Alice and Eve's mutual information is given by

$$I_{\mathrm{AE}}(x_1, x_2) \leq \frac{\zeta^{(d)}\left(\binom{L-1}{d-1}x_1, \binom{L-2}{d-2}x_2, ..., \binom{L-2}{d-2}x_2\right)}{\binom{L-1}{d-1}(x_1 + x_2)}, \tag{3}$$

where we have defined $x_1$ and $x_2$ as non-negative parameters satisfying $x_1 + x_2 = 1$, $\binom{n}{k} = n!/(k!(n-k)!)$ is the binomial coefficient, and

$$\begin{aligned} \zeta^{(d)} \quad & (x_0^2, x_1^2, ..., x_{(d-1)}^2) \\ = \quad & -\sum_{i=0}^{d-1} x_i^2 \log_2 x_i^2 + \left(\sum_{i=0}^{d-1} x_i^2\right) \log_2 \left(\sum_{i=0}^{d-1} x_i^2\right). \end{aligned} \tag{4}$$

This bound arises from considering all of the paths and probabilities for Eve to obtain each of a variety of possible density matrices through a collective attack on Alice's transmitted state. We note that the expression for $I_{\mathrm{AE}}$ does not depend on the error rate, thus removing the requirement for monitoring signal disturbance. Nevertheless, it is possible to find a tighter bound on Alice and Eve's mutual information by determining the lower bound on the error rate of Bob's measurement in terms of $x_1$ and $x_2$. The detailed calculation is also shown in Appendix A. The secret key rate is then given by,

$$R(E) = \log_2(d) - h^{(d)}(E) - \max_{x_1, x_2} I_{\mathrm{AE}}(x_1, x_2), \tag{5}$$

where $h^{(d)}(E) := -E\log_d(E/(d-1)) - (1-E)\log_2(1-E)$ is the $d$-dimensional Shannon entropy. This expression of the secret key rate does not require monitoring signal disturbance. However, we can obtain the lower bound on the error rate given by

$$E \geq \frac{(d-1)}{d}\left(\frac{L-d}{L-1}\right)\left(\frac{x_2}{x_1 + x_2}\right). \tag{6}$$

This inequality can be used to find a lower bound on $x_1$, i.e. $x_1^{(L)}(E) = 1 - E(d/(d-1))(L-1)/(L-d)$. By monitoring signal disturbance and experimentally determining the error rate $E$, an improved secret key rate is achieved, i.e.,

$$\begin{aligned} \mathcal{R}(E) = \log_2(d) \quad & - \quad h^{(d)}(E) \\ & - \quad I_{\mathrm{AE}}\left(x_1^{(L)}(E), 1 - x_1^{(L)}(E)\right). \end{aligned} \tag{7}$$

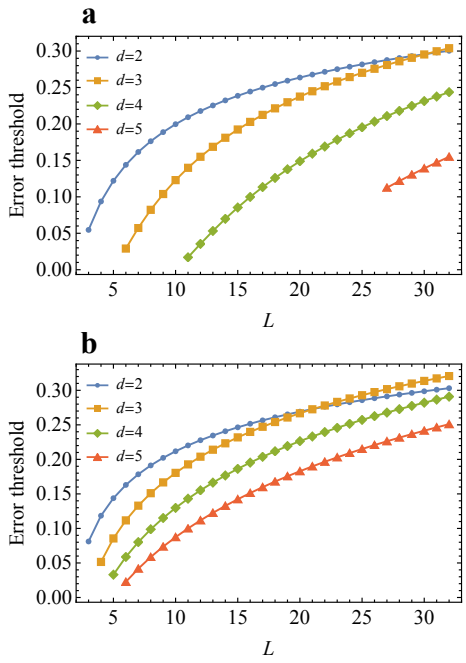


Figure 3: **Error threshold of the HD-RRDPS protocol**. Error threshold as a function of protocol parameters $L$ and $d$ (**a**) without and (**b**) with monitoring signal disturbance.

## 4 Experiment

We perform a proof-of-principle experimental demonstration of our protocol using the OAM degree of freedom of photons, see Fig. 1. In particular, we used the Laguerre-Gaussian (LG) modes as a basis for our OAM states. LG modes have a cylindrical symmetry and are composed of orthogonal states with a radial index, $p$, and an azimuthal index, $\ell$. In our experiment, we only use the azimuthal index, creating single photon states which carry angular momentum with a magnitude $\ell\hbar$ per photon along the propagation direction. These states have the characteristic azimuthally dependent phase $e^{i\ell\phi}$. The OAM degree of freedom is a popular approach in the application of high-dimensional QKD protocols, where their robustness has been repeatedly demonstrated in a wide range of quantum channels [37, 38, 39, 40, 41, 42].

Single photon pairs are produced through spontaneous parametric down-conversion (SPDC). A 360 mW Cobalt UV diode laser at a center wavelength of 405 nm is used to pump a type-I barium borate (BBO) crystal, which spontaneously produces pairs of photons, called the signal and idler, whose wavelengths are centered at 810 nm. We use a knife-edge mirror placed at the center of the beam to separate the photon pairs. The signal and idler photons are each coupled to a single-mode fiber (SMF), which selects only the Gaussian optical mode from the SPDC process. Our heralded single-photon source has a coincidence rate of 22 kHz with a 5 ns coincidence time window. The detectors each have a dark count rate of 50 Hz. The idler photon is sent directly to Bob to make a coincidence measurement jointly with the measurement of the signal photon, thus reducing the background noise in the measured data. The signal photon is used by Alice to encode the information. After exiting a fiber coupling stage, the beam is expanded using a 4-f lens system with focal lengths of 50 mm and 200 mm. The photons are sent to Alice's spatial light modulator (SLM), which imprints the desired phase to the incoming Gaussian

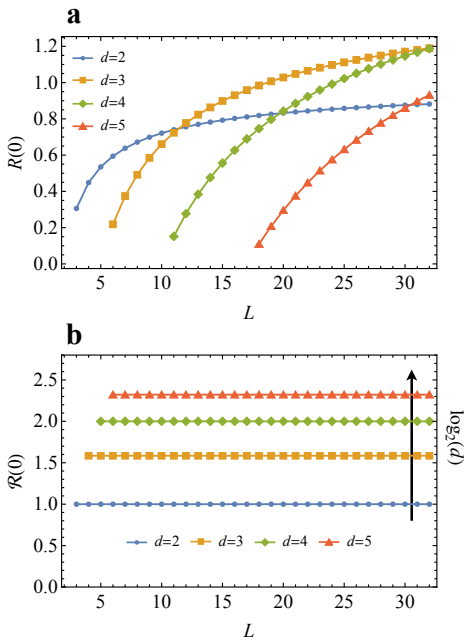


Figure 4: **Null error rate secret key rate of the HD-RRDPS protocol**. Null error rate secret key rate as a function of protocol parameters $L$ and $d$ (**a**) without and (**b**) with monitoring signal disturbance.

photon to produce an OAM state. We use a phase and intensity masking technique as well as a diffraction grating to produce high-quality optical modes [43]. The diffraction grating is used to send the desired phase to the first order of diffraction, which ensures that inefficient phase conversion inherent in the SLM does not result in the degradation of the mode quality. This comes at the cost of the overall efficiency of the process, as some photons will go into the other orders of diffraction. After Alice's SLM, a 4-f lens system is used to remove all other diffraction orders. We also use this 4-f system to image Alice's SLM onto Bob's SLM. The beam waist used on the SLMs was 640 $\mu$m and 650 $\mu$m for Alice and Bob, respectively.

Bob measures the state of the incoming photon using the intensity flattening technique [44]. Bob displays the conjugate phase of the mode that he would like to measure on the SLM. When the incoming mode corresponds to Bob's measurement, this effectively removes the transverse phase of the incoming beam resulting in a flattened wavefront which can then be made to couple to a SMF. Before coupling the beam to the single mode fiber, Bob demagnifies the beam using a 4-f system with focal lengths 100 mm and 250 mm, respectively. Finally, the photon is sent to a single-photon avalanche photodiode (APD) detector. The coincidence measurement of the signal photon is performed with the idler photon. After the state preparation and detection, the coincidence rate is 1250 Hz for the case of Alice and Bob projecting on a Gaussian state. We note that since the idler photon is not sent to the SLM, where Alice's bits are encoded, it does not contain any information about the key sent from Alice to Bob. The resulting raw counts are converted to a mode mismatch, $e_{\text{mis}}$, for a given dimension, $d$, and size of the encoding Hilbert space, $L$, see Fig. 2. In the QKD protocol, the mode mismatch will result in a fixed amount of error that is independent of the channel loss. We expect that the mode mismatch will be one limiting factor in the scaling of our protocol to larger values of $d$ and $L$. Nevertheless, other degrees of freedom may result in lower mode mismatch and improved performance

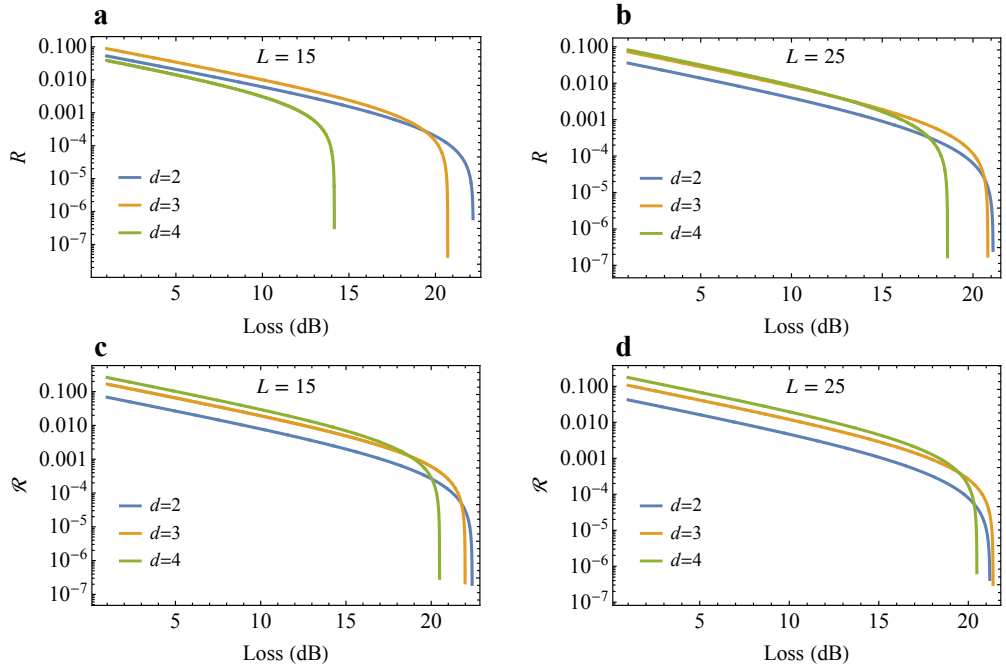


Figure 5: **Performance of the HD-RRDPS protocol**. The secret key rates as a function channel loss are shown in (**a**-**b**) without and in (**c**-**d**) with monitoring signal disturbance. The performance of the HD-RRDPS protocol is simulated using a fix value of the mode mismatch, $e_{\text{mis}} = 0.05$, for various values of the dimension, $d$, and the size of the encoding Hilbert space, $L$. In the simulation, we considered a dark count rate of $p_d = 10^{-4}$.

of the protocol [45, 46]. Other types of measurements may also be considered to overcome limitations from mode mismatch [47, 48, 49].

## 5 Discussion and Outlook

We now discuss the performance of our HD-RRDPS protocol for various protocol parameters, i.e. $L$ and $d$, at two extreme conditions. In the first case, it is instructive to consider the case where the error rate is increased to the point where the secret key rate goes to zero. In this regime, the channel condition is noisy and we are interested in the error threshold of our protocol. In Fig. 3, we show the error threshold with and without signal disturbance for various values of $L$ and $d$. At the other extreme, we consider a condition where the level of noise is low enough to result in an null error rate secret key rate. In this scenario, we are interested in the largest achievable secret key rate. For a short quantum communication link, the key rate is limited by the single photon detectors, e.g. saturation or dead time, and when limited by the number of detected photons per second, a promising strategy involves increasing the number of secret key bits carried per photon. By doing so, it is possible to increase the overall secret key rate for the same photon detection rate. In Fig. 4, we show the null error rate ($E = 0$) secret key rate with and without monitoring signal disturbance for various protocol parameters.

In practice, QKD protocols are operated at some point between the two extreme cases considered above. Imperfections in the generation and measurement devices, and noise in the channel or the detectors will result in a non-zero error rate. We will evaluate the performance of our QKD protocol with respect to the error and secret key rates through

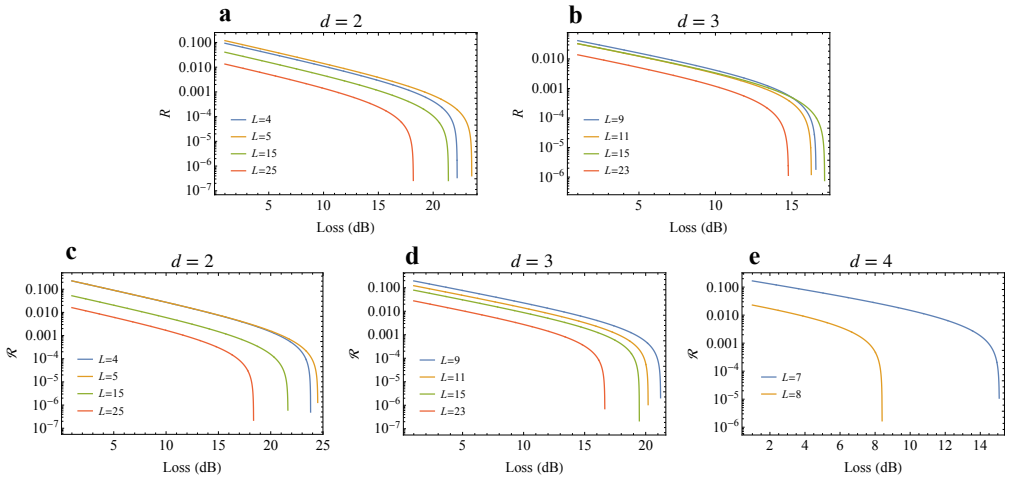


Figure 6: **Performance of the HD-RRDPS protocol from experimentally measured mode mismatch**. The secret key rates as a function channel loss are shown (**a**-**b**) without and (**c**-**e**) with monitoring signal disturbance. The performance of the HD-RRDPS protocol is simulated using the measured experimental values of the mode mismatch, $e_{\text{mis}}$, for various values of the dimension, $d$, and the size of the encoding Hilbert space, $L$. In the simulation, we considered a dark count rate of $p_d = 10^{-4}$.

numerical simulations. In the simulations, an overall transmission of $\eta(l) = 10^{-l/10}$, where $l$ is the total loss in dB, is assigned to the communication channel. Bob detects the single-photon states using $d$ single photon detectors (SPD) with dark count rates $p_d$. For the case where Bob successfully projects the incoming state onto a $d$-dimensional MUB subspace, the single-photon yield is given by,

$$Y = (1-p_d)^{d-1}\left(\frac{d}{L}\eta + \left(1-\frac{d}{L}\eta\right)d\,p_d\right), \tag{8}$$

where the terms $(d/L)\eta$ and $(1-(d/L)\eta)d\,p_d$ respectively correspond to the case where the signal photon is not absorbed by the channel and the case where the signal photon is absorbed by the channel and a dark count occurs. Similarly, the error rate is given by,

$$EY = (1-p_d)^{d-1}\left(\frac{d}{L}\eta\, e_{\text{mis}} + \left(1-\frac{d}{L}\eta\right)d\,p_d\right), \tag{9}$$

where $e_{\text{mis}}$ is the probability that an error occurs due to a mismatch between the generation and the measurement bases. In practice, this may be the result of misalignment between the sender and the receiver, or imperfection in generation and detection devices. As a first step, we consider the performance of our protocol for a fixed value of $e_{\text{mis}} = 0.05$ that is independent of the protocol parameters $d$ and $L$. Figure 5 demonstrates that at a low loss level, the performance of the HD-RRDPS protocol can be improved by increasing the encoding dimension, $d$, with and without monitoring signal disturbance. This advantage can persist for larger values of the size of the Hilbert space, $L$.

From our experimental measurements, we note that the mode mismatch can be dependent on the protocol parameters $d$ and $L$. This is particularly true for the case of OAM states of photons. In this case, we evaluate the performance of our protocol for varying values of the mode mismatch, $e_{\text{mis}}$. In our proof-of-principle experiment, we characterize

the value of $e_{\text{mis}}$ for various protocol parameters such as $L$ and $d$. From these parameters, we can simulate the performance of our HD-RRDPS protocol versus channel loss, see Fig. 6.

By extending the RRDPS protocol to allow for multiple bits of raw key per photon, we gradually close the conceptual gap between differential phase-shift and high-dimensional QKD protocols. We note that our protocol can be straightforwardly extended to consider two MUB measurements rather than just one. When implementing two MUB measurements and the limiting case of $d = L$, we retrieve the high-dimensional BB84 protocol. But interestingly, in the case where $d \neq L$, we obtain a hybrid high-dimensional protocol that is a combination of the two cornerstone QKD protocols, i.e. differential phase shift and BB84. By tuning the protocol parameter $d$, one can optimize the performance of a quantum communication system under varying experimental conditions by employing the two unique information encoding schemes of HD and DPS QKD.

## Acknowledgments

Mikka Stasiuk and Felix Hufnagel contributed equally to this work. This work is supported by the High Throughput Secure Networks Challenge Program at the National Research Council of Canada and the University of Ottawa NRC Joint Centre for Extreme Photonics. We thank Duncan England, Philip Bustard, and Benjamin Sussman for insightful discussions. The authors acknowledge that the NRC headquarters is located on the traditional unceded territory of the Algonquin Anishinaabe and Mohawk people.

## References

[1] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7-11 (2014).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[3] F. Bouchard, R. Fickler, R. Boyd, and E. Karimi, Science Advances **3**, e1601915 (2017).

[4] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Reviews of Modern Physics **92**, 025002 (2020).

[5] A. K. Ekert, Physical Review Letters **67**, 661 (1991).

[6] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Physical Review Letters **88**, 127902 (2002).

[7] H. K. Lo, M. Curty, and B. Qi, Physical Review Letters **108**, 130503 (2012).

[8] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400-403 (2018).

[9] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475-478 (2014).

[10] A. Mizutani, N. Imoto, and K. Tamaki, Physical Review A **92**, 060303(R) (2015).

[11] Z. Q. Yin, S. Wang, W. Chen, Y. G. Han, R. Wang, G. C. Guo, and Z. F. Han, Nature Communications **9**, 457 (2018).

[12] T. Matsuura, T. Sasaki, and M. Koashi, Physical Review A **99**, 042303 (2019).

[13] Y.-G. Shan, Z.-Q. Yin, H. Liu, S. Wang, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Physical Review A **105**, 032441 (2022).

[14] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nature Photonics **9**, 827-831 (2015).

[15] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Nature Photonics **9**, 832-836 (2015).

[16] J. Y. Guan, Z. Cao, Y. Liu, G. L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, Physical Review Letters **114**, 180502 (2015).

[17] Y. H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, Physical Review A **93**, 030302(R) (2016).

[18] Q. P. Mao, L. Wang, and S. M. Zhao, Scientific Reports **7**, 15435 (2017).

[19] K. Wang, I. Vagniluca, J. Zhang, S. Forchhammer, A. Zavatta, J. B. Christensen, and D. Bacco, Physical Review Applied **15**, 044017 (2021).

[20] F. Bouchard, A. Sit, K. Heshami, R. Fickler, and E. Karimi, Physical Review A **98**, 010301(R) (2018).

[21] G. M. Nikolopoulos, K. S. Ranade, and G. Alber, Physical Review A **73**, 032325 (2006).

[22] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Physical Review A **87**, 062322 (2013).

[23] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, Physical Review A **91**, 022336 (2015).

[24] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, npj Quantum Information **3**, 25 (2017).

[25] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Science Advances **3**, e1701491 (2017).

[26] 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).

[27] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Physical Review X **9**, 041042 (2019).

[28] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D Bacco, Physical Review Applied **14**, 014051 (2020).

[29] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitt, A. Zavatta, D. Bacco, and L. K. Oxenløwe, npj Quantum Information **7**, 63 (2021).

[30] F. Bouchard, D. England, P. J. Bustard, K. L. Fenwick, E. Karimi, K. Heshami, and B. Sussman, Physical Review Applied **15**, 024027 (2021).

[31] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, Quantum Technology: Driving Commercialisation of an Enabling Science II **11881**, 1188106 (2021).

[32] M. Gündoğan, T. Jennewein, F. K. Asadi, E. Da Ros, *et al.*, arXiv:2111.09595 (2021).

[33] C. Y. Lu, Y. Cao, C. Z. Peng, and J. W. Pan, Reviews of Modern Physics **94**, 035001 (2022).

[34] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, Quantum Computing, Communication, and Simulation III **12446**, 129–137 (2023).

[35] T. Islam, J. S. Sidhu, B. L. Higgins, T. Brougham, T. Vergoossen, D. K. L. Oi, T. Jennewein, and A. Ling, arXiv:2204.12509 (2022).

[36] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, Journal of Physics B: Atomic, Molecular and Optical Physics **46**, 104010 (2013).

[37] 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**, 1006–1010 (2017).

[38] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, Optics Express **26**, 22563–22573 (2018).

[39] A. Sit, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi, Optics Letters **43**, 4108–4111 (2018).

[40] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs and E. Karimi, Optics Express **27**, 26346–26354 (2019).

[41] F. Bouchard, F. Hufnagel, D. Koutny, A. Abbas, A. Sit, K. Heshami, R. Fickler, and E. Karimi, Quantum **3**, 138 (2019).

[42] F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, and E. Karimi, New Journal of Physics **22**, 093074 (2020).

[43] E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, Optics Letters **38**, 3546–3549 (2013).

[44] F. Bouchard, N. H. Valencia, F. Brandt, R. Fickler, M. Huber, and M. Malik, Optics Express **26**, 31925-31941 (2018).

[45] F. Bouchard, D. England, P. J. Bustard, K. Heshami, and B. Sussman, PRX Quantum **3**, 010332 (2022).

[46] F. Bouchard, K. Bonsma-Fisher, K. Heshami, P. J. Bustard, D. England, and B. Sussman, Physical Review A **107**, 022618 (2023).

[47] J. S. Sidhu, S. Izumi, J. S. Neergaard-Nielsen, C. Lupo, and U. L. Andersen, PRX Quantum **2**, 010332 (2021).

[48] S. Izumi, J. S. Neergaard-Nielsen, and U. L. Andersen, PRX Quantum **2**, 020305 (2021).

[49] J. S. Sidhu, M. S. Bullock, S. Guha, and C. Lupo, Quantum **7**, 1025 (2023).

# High-Dimensional Quantum Certified Deletion

Felix Hufnagel,[1,*] Anne Broadbent,[1,2] and Ebrahim Karimi[1]

[1]*Nexus for Quantum Technologies, University of Ottawa, Ottawa, K1N 6N5, ON, Canada*
[2]*Department of Mathematics and Statistics, University of Ottawa, Ottawa, Ontario, K1N 6N5 Canada*

Certified deletion is a protocol which allows two parties to share information, from Alice to Bob, in such a way that if Bob chooses to delete the information, he can prove to Alice that the deletion has taken place by providing a verification key. It is not possible for Bob to both provide this verification, and gain information about the message that was sent. This type of protocol is unique to quantum information and cannot be done with classical approaches. Here, we expand on previous work to outline a high-dimensional version of certified deletion that can be used to incorporate multiple parties. We also experimentally verify the feasibility of these protocols for the first time, demonstrating the original 2-dimensional proposal, as well as the high-dimensional scenario up to dimension 8.

*Introduction* – In the current climate of remote services and mass data storage, the ability to know if someone has deleted information that you have sent to them or asked them to hold onto for some period of time may be as important as communication security. Going forward, a verifiable proof that a company has deleted personal data may be integral to our continued faith in cloud storage and data-collecting companies. The inability to make copies of a general quantum state, described by the no-cloning theorem [1, 2], is a fundamental aspect of many proposed quantum technologies, including quantum key distribution (QKD) [3] and blind quantum computing [4]. Such technological solutions use the physical properties of quantum mechanical systems to gain a security advantage over the previously used digital approaches. QKD has become a frontrunning solution to secure communication in a future where access to quantum computing resources will render current security protocols useless. This field has received significant attention both from the theoretical physics and mathematics community which has developed new protocols and security proofs to optimise the original communication protocol proposed in 1984 [3], and from experimental physics which has pushed the bounds of what can actually be achieved with fibre channels [5–7], underwater channels [8], and free-space channels [9, 10] linking line of sight stations within cities and from ground to satellite [11]. Furthermore, this technology is beginning to enter the commercially available phase of development with a few pioneering companies such as ID Quantique, Toshiba, and MagiQ Technologies Inc., to name a few, producing specific-use products. Eventually it is expected that a large infrastructure of quantum communication channels will be used to allow secure communication around the world. On the back of this infrastructure one can begin to consider other applications for the quantum channels such as blind quantum computation, quantum money, and the quantum internet etc.

A more recent proposal, again resting on the no-cloning theorem for quantum states, has defined a protocol for certified deletion [12]. The certified deletion protocol allows for a receiving party to guarantee that information sent to them has in fact been deleted and that no copy has been held by the receiving party. Such a protocol is not possible in the world of digital communication where a person can always hold on to the raw bits that have been sent, and recreate a copy. This has motivated protocols using certified deletion for data security and privacy, software licensing, and new public encryption schemes using quantum resources [13–15]. There have also been similar ideas around proving erasure of quantum data stored at some remote location [16]. This allows for one party to store a backup of their data at some location while being able to request a proof that this data is deleted at a later date. Here, we experimentally demonstrate the certified deletion protocol proposed in [12], using the orbital angular momentum degree of freedom of photons. In addition, we extend the protocol beyond the qubit, aiming to develop the certified deletion protocol to utilise high-dimensional quantum communications systems.

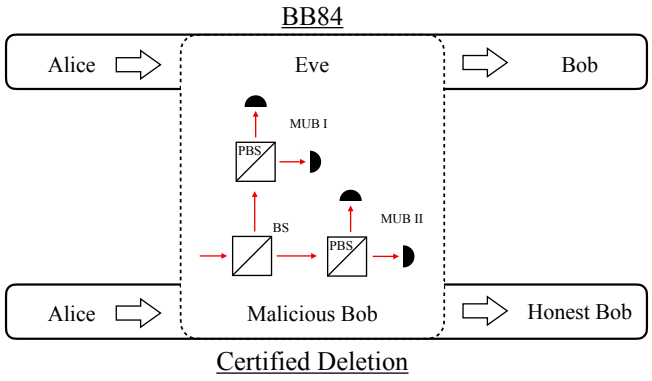


FIG. 1. Here we describe the relationship between BB84 and certified deletion. In the certified deletion protocol the malicious Bob, who is trying to determine both the deletion key and the secret message, maps onto Eve in the BB84 protocol. For the security proof, we can describe the certified deletion protocol as Alice sending the quantum state to Malicious Bob and then on to the Honest Bob.

*Protocol* – A fundamental aspect of certified deletion is shared with QKD, that of conjugate coding using mutually unbiased bases (MUBs). By encoding information into conjugate bases, we are able to take advantage of the quantum no-cloning principle, leading to mathematical limits on the eavesdropper's abilities in QKD or to Bob's ability to *both* convince Alice of deletion *and* extract information about the message in certi-

fied deletion. These limits provide us with a guideline of experimental error thresholds which we must keep our quantum system below to allow for secure communication, and consequently certified deletion. The specifications of a particular protocol will dictate the form of the security proofs and thus will change the error thresholds for different protocols. These specifications include the types of states used, the dimensionality of those states, as well as the choice of measurements that will be performed. Different protocols will have advantages in terms of improved message rates or improved tolerance to errors, but will also ultimately depend on the practical ability to create certain quantum states and perform complex measurements. Let us now extend the certified deletion protocol to the high-dimensional vector space. We will begin by using concepts from high-dimensional QKD schemes that have been developed as extensions to the original BB84 [17].

A generalised quantum measurement can be given as set of linear operators on a quantum system $A$ denoted by $\left\{\widehat{M}_A^x\right\}$, satisfying $\sum_x \left(\widehat{M}_A^x\right)^\dagger \left(\widehat{M}_A^x\right) = \mathbb{1}_A$, where, $x \in \{1, 2, \ldots\}$, and $\dagger$ stands for the conjugate transpose. When $\sum_x \widehat{M}_A^x = \mathbb{1}_A$, these operators are known as a positive-operator valued measure (POVM). MUBs are a particular class of POVMs whose defining feature is that the overlap of two different bases, denoted by $\widehat{M}_A^x$ and $\widehat{N}_A^y$, gives $c = max_{x,y} \left\| \sqrt{\widehat{M}_A^x}\sqrt{\widehat{N}_A^y} \right\|_\infty^2 = 1/d$, where $x, y \in \{1, \ldots, d\}$, $d$ is the dimension of the vector space, and $\|\widehat{O}\|_\infty = \max_i |o_i|$ is the infinity norm.

For certified deletion, the string of bits composing the message from Alice are encoded in the computational basis, $\Pi_1 = \left\{\widehat{M}_A^x = |\psi_x\rangle\langle\psi_x|\right\}$, and the deletion key is encoded in the Hadamard basis, $\Pi_2 = \left\{\widehat{N}_A^y = \left|\phi_y\right\rangle\left\langle\phi_y\right|\right\}$. The choice of ordering for sending in the computational and Hadamard basis is randomised, determined by a random number generator. Thus due to the use of the mutually unbiased bases, Bob can only get information either about the message, by measuring in the computational basis, or the deletion key, by measuring in the Hadamard basis. We show that an attempt from Bob to obtain information about both the key and message is equivalent to an eavesdropper attack on a QKD scheme, and thus, our security proof can use proofs developed for quantum communication. We can draw a picture here relating certified deletion to BB84, Fig. 1. In the certified deletion case we must consider as an adversary a malicious Bob who is trying to determine both the deletion key and secret message, and an honest Bob. The malicious Bob here maps onto Eve in BB84, where Eve is trying to find out information without introducing error, which can be generallized to Eve trying to find out information about one basis without introducing errors into the conjugate basis. To frame it in another way, Bob must provide Alice with the deletion key, meaning he makes each measurement in the Hadamard basis. While Eve tries to determine Alice's states in the computational basis only to gain information on the secret message.

As in QKD protocols, a certain upper bound is established for the number of errors allowable, here in the proof of deletion Bob provides to Alice.

The mutual information between Alice and Bob is given by

$$I_{AB} = \sum_{ij} P(x_i, y_j) \log_2\left(\frac{P(x_i, y_j)}{P(x_i)P(y_j)}\right), \tag{1}$$

where the $P(x_i, y_j)$ are the probabilities of the outcome $x_i$ for Alice and $y_i$ for Bob, and $P(x_i)$ and $P(y_i)$ are the independent probabilities of each outcome for Alice and Bob. Thus in the high dimensional case, *i.e.*, qudits, we consider a uniform probability of detection errors in Bob's measurement, and can give the mutual information for Alice and Bob in terms of Bob's state fidelity $F$ by,

$$I_{AB} = \log_2(d) + F\log_2(F) + (1-F)\log_2\left(\frac{1-F}{d-1}\right). \tag{2}$$

Bob's state fidelity is given by $F = \langle\psi_i|\widehat{\rho}_B|\psi_i\rangle$ in the computational basis and by $F = \langle\phi_i|\widehat{\rho}_B|\phi_i\rangle$ in the Hadamard basis where $\widehat{\rho}_B$ is the quantum state received by Bob via the quantum channel. This fidelity also corresponds to the trace of the probability of detection matrix that will be measured in the experimental section to characterise the quantum channel and yields the quantum bit error rate (QBER) through QBER $= 1 - F$.

It has been shown that a limit on Eve's, *i.e.*, malicious Bob's, information can be derived from an uncertainty principle approach which limits the information that can be gained by Eve and Bob from making measurements $\widehat{E}_A$ and $\widehat{B}_A$ respectively on a quantum system $A$ [18]. Using the eigenstates $\left|e_j\right\rangle$ and $|b_i\rangle$ for $\widehat{E}_A$ and $\widehat{B}_A$ respectively, this limit is given by,

$$I_{AB} + I_{AE} \leq 2\log_2\left(d \max_{i,j} \left|\left\langle b_i\middle|e_j\right\rangle\right|\right). \tag{3}$$

From here, we know that a measurement by Eve in the complementary MUB to Bob will give $\left|\left\langle b_i\middle|e_j\right\rangle\right|^2 = 1/d$ and thus $I_{AB} + I_{AE} \leq \log_2(d)$. Finally, the proposition $R \geq \max\{I_{AB} - I_{AE}, I_{AB} - I_{BE}\}$, detailing the necessary restriction on the mutual information for generating a message, gives the result that we can establish a non-zero message rate for $I_{AB} > I_{AE}$. Here, $I_{ij}$ defines the mutual information between $i$ and $j$, where $A$, $B$, and $E$ represent Alice, Bob, and Eve, respectively [19]. We then can determine that we must have $I_{AB} > \log_2(d)/2$ to guarantee a positive message rate. Combining this with Eq. (2), we reach a lower bound on the fidelity required to give a positive message rate:

$$F\log_2\left(\frac{1}{F}\right) + (1-F)\log_2\left(\frac{d-1}{1-F}\right) < \frac{\log_2 d}{2}. \tag{4}$$

Once it is established that Alice and Bob have a sufficiently high mutual information (fidelity, corresponding to a limit on Eve's information), it has been shown that hash functions can be used to further reduce Eve's information all the way to zero.

Though this privacy amplification comes at the expense of reducing Alice and Bob's message length. Equation 4 allows us to determine the maximum tolerable QBER, beyond which point a secret message cannot be established. For example, the error thresholds for dimensions 2, 4, and 8 are 11.00%, 18.93%, and 24.70% respectively[18].

*High-dimensional photonic states* – In our protocol, we will use orbital angular momentum (OAM) states to encode our quantum information. OAM of photons is defined by its

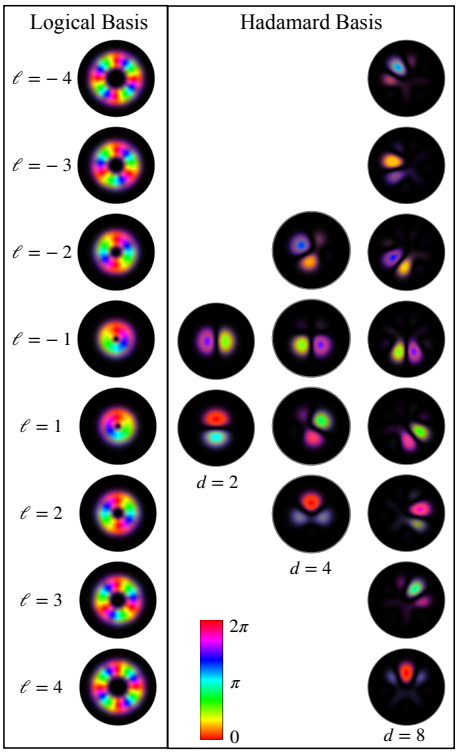


FIG. 2. The logical and Hadamard bases for dimensions 2, 4 and 8 are shown. The pure OAM states are shown on the left where $\ell = \{-1, +1\}$ make up the logical basis for $d = 2$; $\ell = \{-2, -1, +1, +2\}$ for $d = 4$; $\ell = \{-4, -3, -2, -1, +1, +2, +3, +4\}$ for $d = 8$. The Hadamard basis states for dimensions 2, 4, and 8, are shown on the right side. The states are plotted with intensity and phase, where the colour ranging from red through the colors and back to red represents a phase of 0 to $2\pi$.

characteristic property of having an azimuthally dependent phase $\langle \mathbf{r}|\ell\rangle := e^{i\ell\phi}/\sqrt{2\pi}$, where $\ell$ is an integer from $-\infty$ to $+\infty$, and $\phi$ is the azimuthal angle in the polar coordinates $\mathbf{r}$. Such photonic states carry angular momentum of magnitude $\ell\hbar$ per photon along propagation direction. These photonic quantum states form complete and orthogonal bases, which we represent with $|\ell\rangle$. The OAM states for $\ell = \{-4, -3, \ldots, 3, 4\}$, with the computational and the corresponding Hadamard states, are shown in Fig. 2. In two dimensions the protocol is similar to that used in BB84 QKD. One takes first the computational basis given by $\{|\psi_0\rangle := |-1\rangle\,; |\psi_1\rangle := |+1\rangle\}$. The conjugate basis is then taken as the Hadamard, $\left\{|\phi_1\rangle := (|-1\rangle + i\,|+1\rangle)/\sqrt{2}; |\phi_2\rangle := (|-1\rangle - i\,|+1\rangle)/\sqrt{2}\right\}$. As these states form a pair of MUBs, a projective measurement of a state in the correct basis gives a certain result, due to the orthogonality of the states in each basis, while measurement in the wrong basis gives no information, or a 50% probability of detection for each state in the 2-dimensional case. When we move to higher dimensions we again will use two MUBs. However, each MUB will now have $d$ different states. In the higher dimensions, the states for the Hadamard basis are given by $|\phi_i\rangle = \sum_{j=1}^{d} e^{ij\pi/d}\left|\psi_j\right\rangle$. For dimension 4, the states would be $\ell = \{-2, -1, +1, +2\}$ and for dimension 8, the states would be $\ell = \{-4, -3, -2, -1, +1, +2, +3, +4\}$. More generally, the computational basis will be the pure OAM states from $\ell \in \{-d/2, ...0, ..., d/2\}$ for the odd dimensions, and $\ell \in \{-(d-1)/2, \ldots, -1, 1, \ldots, (d-1)/2\}$ excluding $\ell = 0$ for even $d$.

*Experiment* – The experimental setup consists of a single photon source and OAM state preparation for Alice, and an OAM measurement system for Bob. Single photons are produced by pumping a BBO crystal with a 405 *nm* UV laser. Degenerate photon pairs are selected using a 10 *nm* bandpass filter centred at 810 *nm* wavelength. A knife edge mirror is placed after the filter to separate the photon pairs which are anti-correlated in momentum. Each of these halves of the beam are then coupled to a single mode fibre where the signal photon is sent to Alice's state preparation system and the idler photon is sent to a detector. When coupled to the single mode fibres, the source has a rate of approximately 22 KHz, which reduces to 1 KHz after propagation through the experimental setup. The losses are mostly due to the spatial light modulators (SLMs) used for state preparation and detection. Alice uses a SLM to generate her desired OAM states. SLMs are not 100% efficient, thus a holography approach is used, adding a diffraction grating to the phase mask which results in the desired OAM mode being formed in the 1st order of diffraction with very high state purity. After the SLM a 4-f lens system with a pinhole at the focus is used to filter out all diffraction orders except for the first order.

Bob also has an SLM and uses the phase flattening technique to measure the states sent by Alice. This technique involves applying the conjugate phase of the OAM mode that is to be measured and can be seen as removing any transverse phase from the incoming OAM carrying photon. This allows the photon to be coupled to a single mode fibre upon propagation, as the flat phase corresponds to a Gaussian mode in the far field. It must be stated that this is a projective measurement in which Bob must choose which state he will measure and only measures a single state at a time, thus limiting the efficiency of this particular measurement technique. There do however exist different approaches which can sort OAM modes upon choosing the basis in which one wants to measure. At present, many of these approaches suffer from efficiency problems which limit the eventual transmission rates. The idler photon is sent to Bob to perform a coincidence mea-

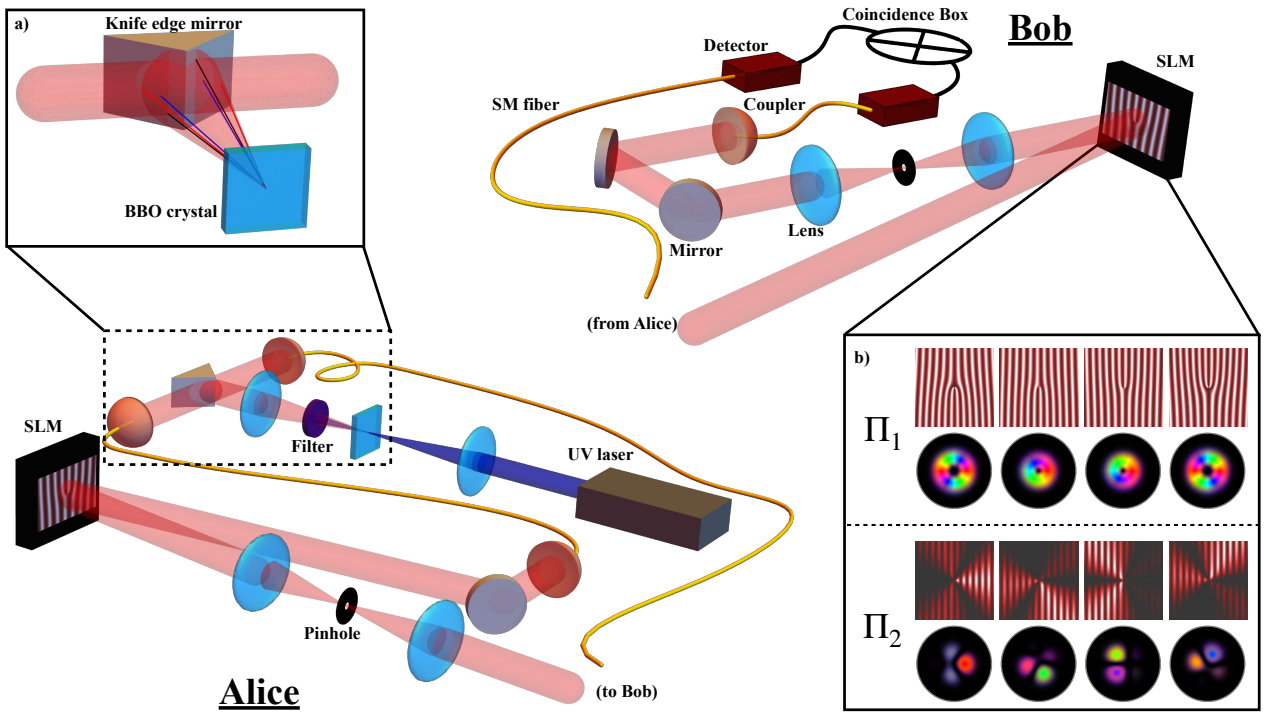


FIG. 3. Experimental Setup: Alice and Bob's measurement and detection setups are shown. Alice pumps a BBO crystal with a UV diode laser at 405 nm resulting in 810 nm pairs of single photons through SPDC, and the pump is filtered out using a 10 nm width bandpass filter centred at 810 nm. The entangled pairs are separated using a knife edge mirror as shown in inlay **a**. Entangled pairs are anti-correlated in their momentum and thus one photon from each pair falls on each side of the knife edge, as shown in the inlay. The single photons are coupled to a single mode fibre (SMF). The idler photon is then sent directly to Bob and the signal photon is sent to Alice's state preparation stage which uses a spatial light modulator (SLM) to prepare the OAM carrying beams. A diffraction grating is applied to the phase hologram which results in the formation of the desired mode in the first order of diffraction. A 4-f lens system with a pinhole at the focus then removes all the diffraction orders other than the first order. The holograms used for the dimension 4 states along with the corresponding modes is shown in inlay **b**. Bob measures the incoming photon's state using an SLM and SMF, again using a 4-f system to remove all of the diffraction orders other than the first. The collected photons and idler photons are detected using single-photon avalanche diode (SPAD) detectors which then trigger a coincidence box to measure the coincidences.

surement with the signal photon, reducing noise from background light and detector dark counts. Both photons are detected using single-photon avalanche diode (SPAD) detectors. Bob makes all measurements, in the computational and Hadamard basis, using the SLM with different phase patterns.

The experimental probability of detection matrices for the $d = 2, 4$ and 8 QKD setup are shown in Fig. 4. The columns correspond to the different states sent by Alice, while the rows correspond to the choice of measurement made by Bob. Thus we expect to find 100% detection probability on the diagonal elements where Bob's measurement setting is the same state as that sent by Alice. When Bob measures Alice's states in the incorrect basis, he can gain no information and we expect to see a uniform probability of $1/d$ for all measurements in the wrong basis. When Bob reads the message, he performs all measurements in the logical basis, giving the measurement results shown on the left. This results in no information being gained about the deletion key, which can be seen by the incoherence of Alice's deletion key states. When Bob chooses to delete the message, he will instead choose to measure every state using the Hadamard basis, giving the results shown on the right. In this case we can see that the message states sent by Alice do not give any information. The error rates obtained are QBER $= 0.96\%, 2.4\%$, and $7.2\%$ for dimension 2, 4, and 8, respectively. We can calculate the achievable message rate from our QBER ($Q$) using $K^{(d)}(Q) = \log_2(d) - 2\,h^{(d)}(Q)$ where the $d$-dimensional Shannon entropy is given by $h^{(d)}(x) = -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$. We have obtained message rates of 0.84, 1.60, and 1.85 per message photon for dimension 2, 4, and 8, respectively. Here, we see the advantage that can be achieved by moving to higher dimensional protocols, as the message rates here increase as the dimension of the protocol increases.

*Discussion* – A practical quantum information processing hardware called quantum memory, capable of arbitrary storing/releasing quantum states, has not yet been fully realised. Though the deletion concept may seem incomplete

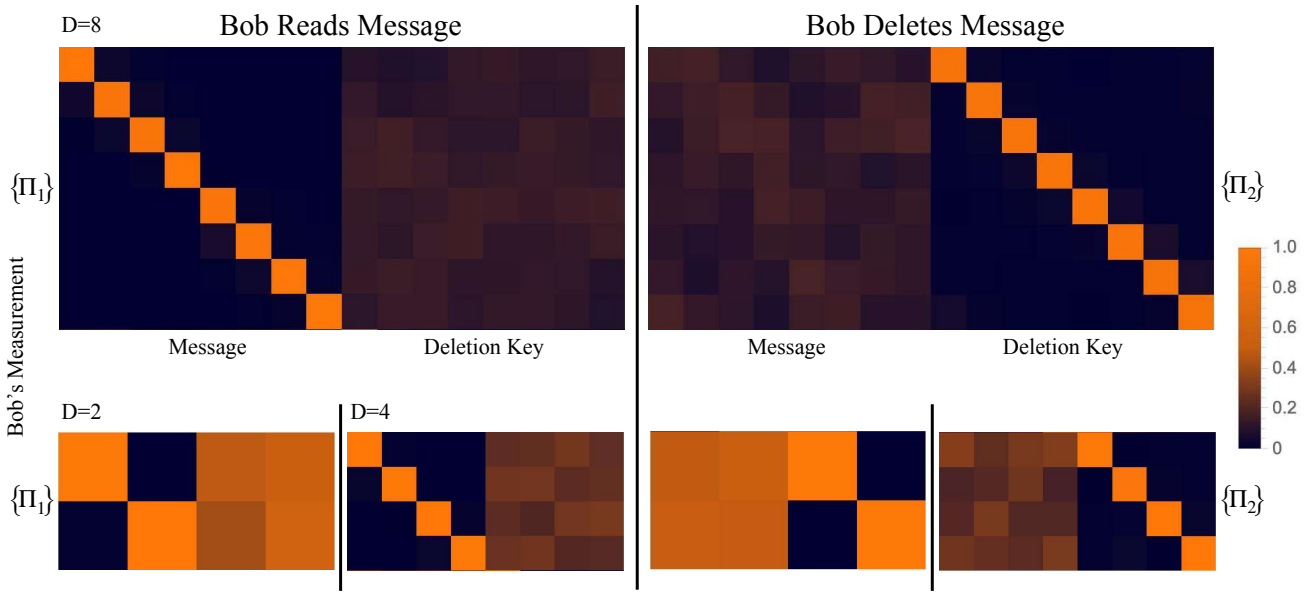


FIG. 4. Probability of detection for dimension $d = 2, 4$, and 8: Bob's choice of measurement is shown in the rows of the detection matrix while the columns correspond to Alice's prepared state. On the left, Bob chooses to measure in the logical basis and thus reads the message sent by Alice. The states sent by Alice in the Hadamard basis are projected onto the logical basis and thus give no information, resulting in the uniform $1/d$ probability of detection. On the right, Bob measures in the Hadamard basis, thus erasing any information sent in the logical basis. The error rates observed are QBER = 0.96%, 2.4%, and 7.2% for dimension 2, 4, and 8 respectively, which correspond to a key rate per sifted photon of 0.84, 1.60, and 1.85.

without a quantum memory, we can still conceive of other near-term applications in which Bob decides when the information is transmitted and whether he will keep or delete the information. For instance, Alice may continually send out an encryption key or software license, for which Bob must continue verifying that he has deleted until the time he would like to use it. Therefore, providing schemes to confirm a message has not been read will be vital for a quantum communication network. In this work, we have experimentally demonstrated the certified deletion protocol for a qubit QKD system as proposed by Broadbent and Islam [12]. We have also extended the protocol to include high-dimensional quantum states and have demonstrated this high-dimensional protocol, gaining an advantage in the message rate per sifted photon. The increase in message rate at higher dimensions also comes with a higher tolerance for errors (and therefore noise), which can be valuable for establishing communication in certain noisy environments. Another property of high dimensional states is that there are more than two MUBs that can be used to encode information. In fact, in dimensions where $d$ is a power of a prime number, *i.e.*, $d = 2, 3, 4, 5, 8, \ldots$, there exists $(d + 1)$-MUBs. Unique QKD protocols, *e.g.* six-state [20], using these extra MUB have been created that have additional key rate and security benefits over BB84. For certified deletion, one could come up with interesting new protocols involving multiple parties with messages or deletion keys encoded in the different bases.

This work was supported by Canada Research Chairs; Canada First Research Excellence Fund (CFREF); National Research Council of Canada High-Throughput and Secure Networks (HTSN) Challenge Program; and Natural Sciences and Engineering Research Council of Canada (NSERC).

*

[1] Park, J. L. The concept of transition in quantum mechanics. *Foundations of physics* **1**, 23–33 (1970).
[2] Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
[3] Bennett Ch, H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing int 175–9 (1984).
[4] Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, 517–526 (IEEE, 2009).
[5] Sit, A. *et al.* Quantum cryptography with structured photons through a vortex fiber. *Optics Letters* **43**, 4108–4111 (2018).
[6] Rosenberg, D. *et al.* Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters* **98**, 010503 (2007).
[7] Gobby, C., Yuan, a. & Shields, A. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters* **84**, 3762–3764 (2004).
[8] Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Optics express* **26**, 22563–22573 (2018).
[9] Sit, A. *et al.* High-dimensional intracity quantum cryp-

tography with structured photons. *Optica* **4**, 1006–1010 (2017). URL http://www.osapublishing.org/optica/abstract.cfm?URI=optica-4-9-1006.

[10] Schmitt-Manderbach, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* **98**, 010504 (2007).

[11] Yin, J. *et al.* Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017). URL http://www.sciencemag.org/lookup/doi/10.1126/science.aan3211.

[12] Broadbent, A. & Islam, R. Quantum encryption with certified deletion. In *Theory of Cryptography Conference*, 92–122 (Springer, 2020).

[13] Garg, S., Goldwasser, S. & Vasudevan, P. N. Formalizing data deletion in the context of the right to be forgotten. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 373–402 (Springer, 2020).

[14] Poremba, A. Quantum proofs of deletion for learning with errors. *arXiv preprint arXiv:2203.01610* (2022).

[15] Bartusek, J. & Khurana, D. Cryptography with certified deletion. *arXiv preprint arXiv:2207.01754* (2022).

[16] Coiteux-Roy, X. & Wolf, S. Proving erasure. In *2019 IEEE International Symposium on Information Theory (ISIT)*, 832–836 (IEEE, 2019).

[17] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Physical Review A* **61**, 062308 (2000).

[18] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of Quantum Key Distribution Using d -Level Systems. *Physical Review Letters* **88**, 127902 (2002). URL http://link.aps.org/doi/10.1103/PhysRevLett.88.127902. 0107130.

[19] Csiszár, I. & Korner, J. Broadcast channels with confidential messages. *IEEE transactions on information theory* **24**, 339–348 (1978).

[20] Bechmann-Pasquinucci, H. & Gisin, N. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A* **59**, 4238 (1999).

# Fast Adaptive Optics for High-Dimensional Quantum Communications in Turbulent Channels

Lukas Scarfe,[1] Felix Hufnagel,[1] Manuel F. Ferrer-Garcia,[1] Alessio D'Errico,[1] Khabat Heshami,[2,1] and Ebrahim Karimi[1,2,*]

[1]*Nexus for Quantum Technologies, University of Ottawa, Ottawa, K1N 6N5, ON, Canada*
[2]*National Research Council of Canada, 100 Sussex Drive, Ottawa ON Canada, K1A 0R6*

Quantum Key Distribution (QKD) promises a provably secure method to transmit information from one party to another. Free-space QKD allows for this information to be sent over great distances and in places where fibre-based communications cannot be implemented, such as ground-satellite. The primary limiting factor for free-space links is the effect of atmospheric turbulence, which can result in significant error rates and increased losses in QKD channels. Here, we employ the use of a high-speed Adaptive Optics (AO) system to make real-time corrections to the wavefront distortions on spatial modes that are used for high-dimensional QKD in our turbulent channel. First, we demonstrate the effectiveness of the AO system in improving the coupling efficiency of a Gaussian mode that has propagated through turbulence. Through process tomography, we show that our system is capable of significantly reducing the crosstalk of spatial modes in the channel. Finally, we show that employing AO reduces the quantum dit error rate for a high-dimensional orbital angular momentum-based QKD protocol, allowing for secure communication in a channel where it would otherwise be impossible. These results are promising for establishing long-distance free-space QKD systems.



**Introduction–** Quantum Key Distribution (QKD) allows two parties to generate a shared secret key between themselves by taking advantage of the properties of quantum systems [1]. Since the introduction of the first protocol by Bennett and Brassard [2], many QKD protocols have been explored theoretically [3] and experimentally [4]. The original implementations relied on encoding schemes using light's polarisation degree of freedom, constraining the quantum states to a two-dimensional vector space. However, higher-dimensional QKD protocols, employing unbounded photonics degrees of freedom, were suggested to increase information density per carrier [5, 6]. There are many photonic degrees of freedom in addition to polarisation, which can be used for encoding information, including frequency, vector modes, and time bins [7–10]. Here, we employ spatial structure of the lights transverse mode through the orbital angular momentum (OAM) which has been studied in diverse settings including free-space [11, 12], fibre [13, 14], and underwater [15–18]. Optical beams carrying OAM are characterized by an azimuthal-dependent phase of $e^{i\ell\phi}$ where $\phi$ is the azimuthal coordinate and $\ell$ is an integer. Because the OAM modes comprise a complete orthonormal basis, they can be used to implement high-dimensional QKD protocols [19].

The channels most often used to transmit quantum information are fibre and free-space. Optical fibre has the advantage of being a well-developed optical technology with infrastructure that has been built up alongside the increasing reliance on high-speed internet connection. However, in the case of quantum communication, the significant attenuation losses that come with optical fibres creates a fundamental limit on the distance achievable by QKD protocols. This is because quantum signals cannot be amplified in the same way as classical signals; a consequence of quantum no-cloning theorem [21]. In addition, fibre-based solutions rely on an established network, increasing the implementation costs of near-term quantum systems. Despite the significance of fibre-based networks for QKD, it is critical to develop and improve on free-space links for ground-to-ground and ground-to-space quantum communication [22–24]. Space-based quantum communication can help circumvent the distance-rate tradeoff due to exponential loss in fibre-based networks. The successful implementation of QKD over free-space channels depends on the accurate transmission and detection of single photons after propagation through the atmosphere. Rapid changes in the temperature and pressure of the atmosphere result in variations of the refractive index of the air, creating atmospheric turbulence which distorts the beam upon propagation [25]. This spatially distributed non-uniform propagation medium induces continuously varying phase aberrations along the optical path of the communication link. It has been shown in previous works that a turbulent environment has a considerable impact, substantially degrading the quantum state, which results in significant errors within the communication channel [26–30]. Consequently, the information encoded within the structure of the photons is likely to be lost due to unintended changes in that structure introduced in propagation. In order to implement a realistic high-dimensional free-space QKD system, the system will require compensation for atmospheric turbulence in the channel. One method of correcting distortions in the atmosphere, which is of particular interest, is adaptive optics (AO). While AO has been employed successfully to correct real-time astronomical observations for decades [31–33], its potential application for free-space communications has only recently been explored [34–36].

In this article, we demonstrate the use of a fast AO system to correct atmospheric disturbances in a free-space quantum key distribution channel when the information is encoded in the photon spatial modes, namely structured photons. First, we show the improved detector coupling efficiency that our AO system is capable of when used to correct the effects of turbulence on a simple Gaussian beam. We then perform quantum process tomography for dimensions two through five under turbulent conditions, both with and without AO active. We calculate the quantum dit error rate (QDER) of the system for even dimensions from 2 through 10 under turbulent conditions, with both AO on and off. We demonstrate a signif-

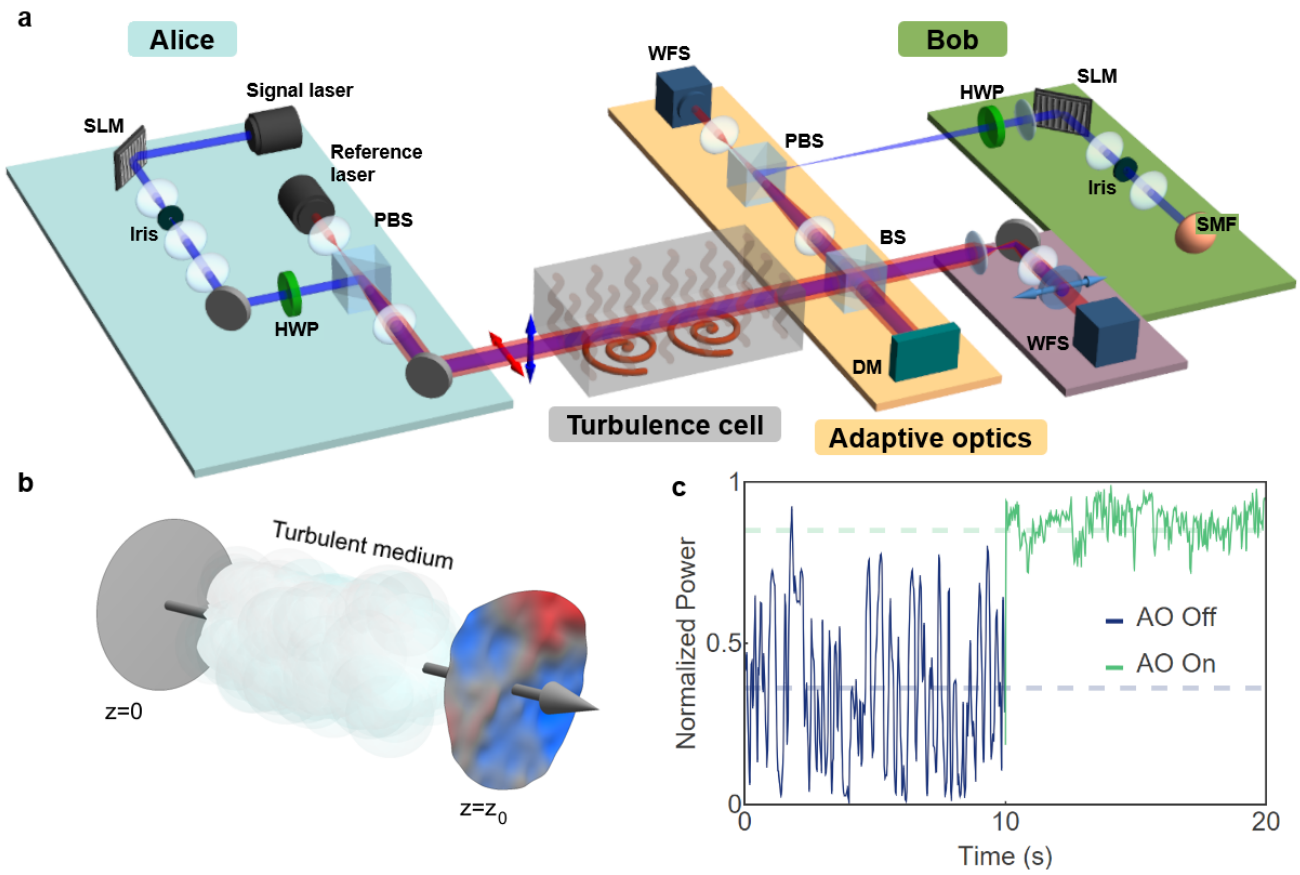


FIG. 1. **High-dimensional quantum communication with adaptive optics through a turbulent channel**. **a** Experimental setup used to investigate the corrective action of a fast adaptive optics (AO) system (from ALPAO [20]) on structured optical beams after propagation through a turbulent channel. A 633 nm laser impinges on a spatial light modulator (SLM), tailoring the complex field (both amplitude and phase) of the input beam. Additionally, a second laser source of the same wavelength emits vertically polarized light, which is expanded to approximate a plane wave for use as a reference beam. These beams are combined at a polarizing beam splitter (PBS) and sent through a turbulent cell. Here, the turbulence is generated by employing a controllable hotplate placed inside a glass tank with a width of 30 cm. The composite beam is split using a 50:50 beam splitter; one part goes to a wavefront sensor (WFS) to record the output wavefront, while the second part is fed to the AO section of the experiment. Our AO apparatus consists of a deformable mirror (DM), and a WFS connected in a closed-loop control system. As the WFS measures the structure of the wavefront, the DM changes shape to compensate for the distortions introduced by the turbulence. In our particular experiment, the reference and signal beam are split using a PBS following the corrections applied by DM. Finally, the signal component is sent to a second SLM that performs a projective measurement of spatial modes to determine the probability of detection. **b** Illustration of the effects on the phase of a plane wave after propagating through a turbulent medium. The colours on the output represent the leading and lagging deformations on the wavefront due to the non-uniform refractive index of the medium. **c** Normalized optical power coupled into a single mode fibre, as measured by a power meter during the application of turbulence on a Gaussian input beam. The wavefront correction component is activated ten seconds after the beginning of the measurement. A measurement over a longer time interval is depicted in Fig. **S2** of the Supplementary materials.

icant improvement in the error rate of the quantum protocol for all dimensions, even in a robust turbulence regime, which results in high crosstalk (high error rates) among the OAM states without AO.

## Results

*Adaptive Optics in the detection stage.*– Let us consider that a free-space channel between Alice and Bob has been deployed, allowing them to exchange information encoded using structured light beams. While propagating, the wavefront is distorted due to its interaction with the atmosphere. To compensate for the effects of the optical turbulence, Bob implements a wavefront-correction stage before decoding the message sent by Alice. A scheme of the proposed experimental setup, which uses an adaptive optics system, is depicted in Fig. 1**a**. To take full advantage of the AO system, Alice and Bob use two co-linear (co-propagating) light beams at the same frequency with orthogonal polarisation states. The first component, referred to as the *reference* beam, possesses a Gaussian profile, which has been expanded to approximate a flat wavefront that completely covers our deformable mir-

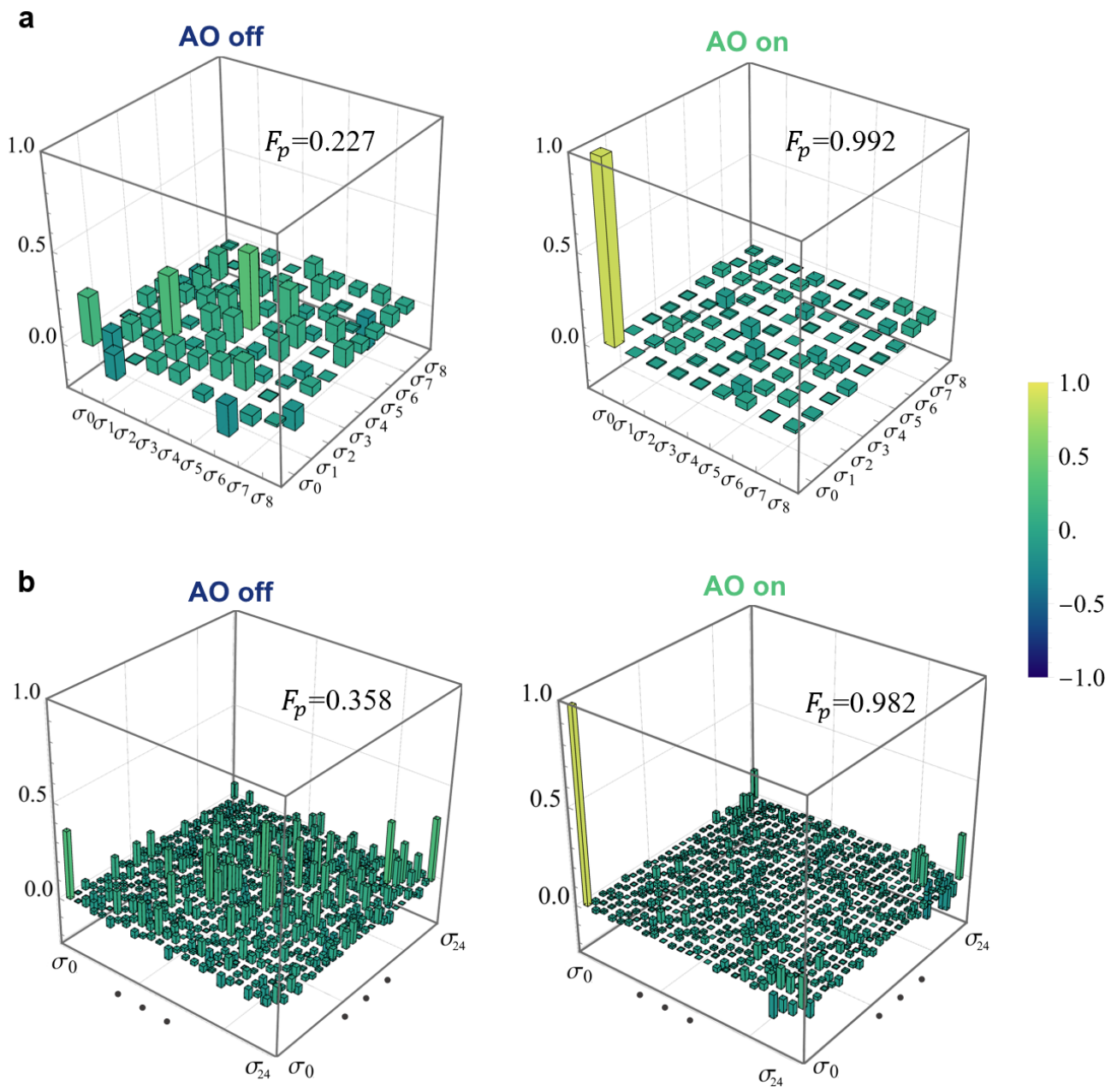


FIG. 2. **Channel Process Tomography for** $d = 3, 5$**.** The real part of the process matrix of the channel transmission is shown for dimension 3 with the AO system as (**a**) non-active and (**b**) active when going through the turbulence cell. We perform the process tomography using mutually unbiased bases measurements following the methods outlined in [5] (see the Supplemental Material for more information). Fidelity is maintained over 99% in all cases except for that of turbulence active without adaptive optics (upper right process matrix), where the fidelity falls to 27%. Here, we see that the effect of the turbulence on the channel is a complete "channel depolarizing" of the OAM states, i.e., the existence of huge crosstalk, which is successfully undone with the adaptive optics enabled. The process matrices for dimensions 2, and 4 are provided in the Supplementary Material.

ror, and also completely overlaps spatially with the second beam, i.e. *signal* beam. This allows us to measure and correct the phase distortions within the channel, either from the optical elements or the environment. The second light beam, the signal beam, serves as our information carrier, where the message is encoded by tailoring its complex amplitude using a spatial light modulator (SLM). It must be noted that since both beams share the optical path, they are subjected to the same atmospheric variations and, therefore, both experience the same distortions. Bob is then capable of correcting the distortion on the signal beam using the phase information obtained from the reference beam. For further details of our experimental

implementation, refer to the Supplementary Materials.

As a first step, our signal takes the form of a Gaussian beam. In the presence of optical turbulence and the absence of a correction mechanism, the coupling of the signal to a single-mode fibre at the receiver fluctuates with respect to time due to the wavefront distortion (See Fig. 1**b**). As shown in Fig. 1**c**, when the AO system is inactive, the measured power presents strong fluctuations due to the influence of the introduced turbulence. These effects lead to an average coupling power into the single mode fibre around 36.6% of the value expected without any turbulence applied. Ten seconds after the beginning of the measurement, the AO system is activated, increasing the average measured power to 87.1% and stabilizing the coupling efficiency. If this channel were to be used for free-space polarisation QKD, implementing AO improves the coupling efficiency and thus would have resulted in a doubling of the secret key rate. From these results, it is possible to observe the promising benefits of including a fast AO system in the detection stage for many kinds of free-space communications.

*Process Tomography.–* We perform quantum process tomography to determine the effect of the turbulent channel on the OAM states up to $d = 5$, i.e., $\ell = \{-2, -1, 0, 1, 2\}$. The results show that the channel fidelity deteriorates significantly under the presence of turbulence. Quantum process tomography is used to determine the effect of a process on quantum states [38]. A quantum process $\mathcal{E}$ can be represented using the process matrix $\chi_{mn}$ to describe how input states $\rho_{in}$ are transformed to output states $\rho_{out}$ by

$$\rho_{out} = \mathcal{E}(\rho_{in}) = \sum_{m,n} \chi_{mn} \hat{\sigma}_m \rho \hat{\sigma}_n^\dagger, \tag{1}$$

with the Gell-Mann matrices, $\hat{\sigma}_m$ being the high-dimensional extension of the Pauli matrices and satisfying $\sum_m \hat{\sigma}_m^\dagger \hat{\sigma}_m = \hat{1}$. We seek to determine the process matrix $\chi_{mn}$ by making projective measurements in the high-dimensional mutually unbiased bases (MUB). These projection measurements are described by the operators $\Pi_m^{(\alpha)}$ where the index $\alpha$ denotes the basis and $m$ denotes the state in that basis. It has been proven that for dimensions $d$ that are prime or the power of a prime number, there exists $d + 1$ MUBs [39]. Thus, in the dimensions explored here, $d = \{2, 3, 4, 5\}$, it is convenient to use the MUB approach to perform process tomography. For an arbitrary dimension, symmetric, informationally complete, positive operator-valued measures (SIC-POVMs) can be used to perform process tomography. The MUB measurement operators in dimension $d$ satisfy

$$\begin{aligned} Tr[\Pi_m^{(\alpha)} \Pi_n^{(\alpha)}] &= \delta_{mn}, \\ Tr[\Pi_m^{(\alpha)} \Pi_n^{(\beta)}] &= \frac{1}{d}, \end{aligned} \tag{2}$$

respectively for the operators of the same basis and different basis, i.e., $\alpha \neq \beta$. Quantum process tomography using MUBs is described in detail in [5].

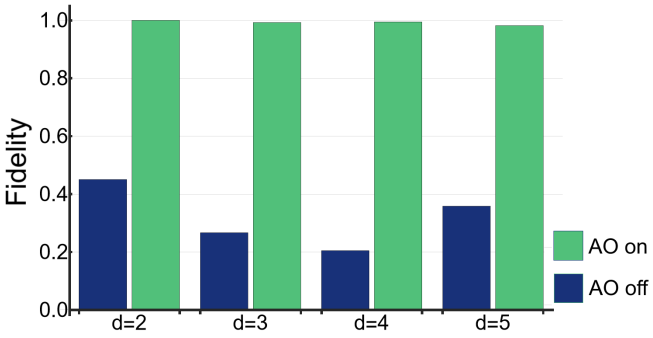


FIG. 3. **Channel Fidelity for OAM-based QKD system.** The process fidelity between the tomographically measured turbulent channel with AO off (blue) and AO on (green) are measured for a QKD channel of $d = 2$, $d = 3$, $d = 4$ and $d = 5$. Turbulence 'depolarizes' the channel significantly, i.e. introduces huge crosstalk, while activating a fast AO system compensates for the turbulence effects and recovers the encoded states. Due to the long time required to perform these measurements in higher dimensions, the data for $d = 5$ was taken on a different day with minor changes to the alignment. This is the main reason why the fidelity for $d = 5$ is higher than for $d = 3, 4$, which were taken one after the other.

The channel fidelity for OAM-based QKD without applied turbulence remains high. As the next step, turbulence is applied, and the state tomography is repeated for each dimension. Without any applied turbulence in the channel, in all dimensions, the channel fidelity remains above $\mathcal{F}_p \geq 0.95$. After applying turbulence to the channel and repeating the tomography, the fidelity of the channel is reduced as low as $\mathcal{F}_p \leq 0.45$, indicating a high crosstalk among the modes. The state tomography is repeated with AO enabled in both a turbulent and still environment. The results for the process tomography for $d = 3$ are shown in Fig. 2. In the case of $d = 3$, we find that the fidelity of the state is maintained such that $\mathcal{F}_p \geq 0.98$ both with and without turbulence when using adaptive optics. The fidelities of the turbulent channel for all measured dimensions are shown in Fig. 3. Further process matrices can be found in the Supplementary Material.

*Quantum Dit Error Rate and Crosstalk Matrices.–* To successfully generate a secure key using QKD, it is essential for Bob to accurately detect the state generated by Alice when they choose to operate on the same basis. Any incorrectly detected states will result in a discrepancy between Alice's and Bob's keys, which is quantified as the quantum dit error rate (QDER) $Q$. It must be noted that the maximum value for QDER that is tolerable increases with the dimensionality of the key distribution protocol [5, 6]. In the case of $d$-dimensional BB84 protocol, the number of bits of secret key established per sifted photon $R$ is given by [40],

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

where $Q$ is the quantum dit error rate and $h(x) = -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the Shannon entropy. From Eq. (3), it is possible to find the QDER threshold when

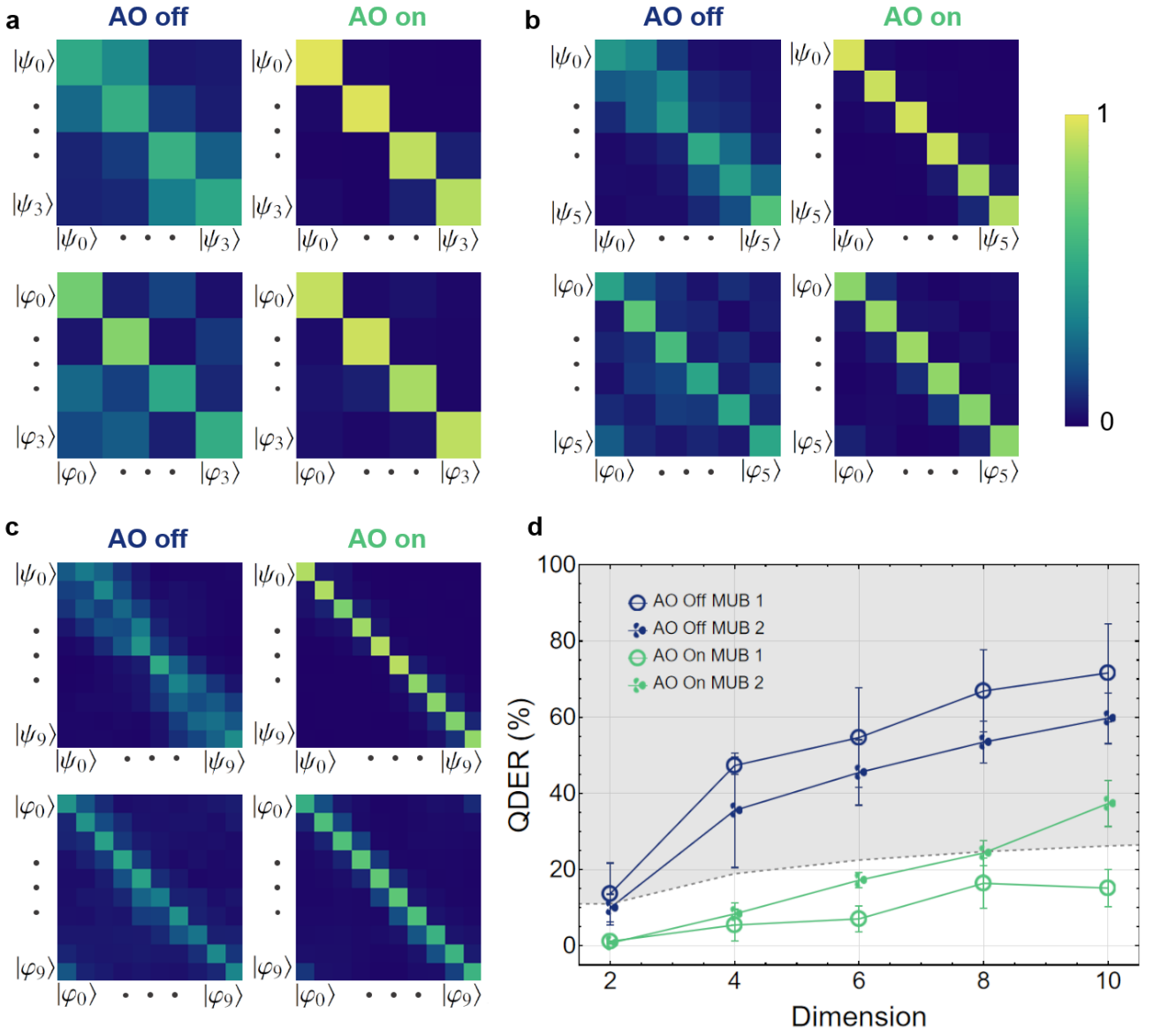


FIG. 4. **Crosstalk and quantum dit error rate.** The probability of detection on each basis for both bases when going through a turbulent channel for **a** $d = 4$, **b** $d = 6$, and **c** $d = 10$. **d** Plot of the QDER as calculated from the probability of detection matrices for the cases of adaptive optics on and off with turbulence active. The dashed gray boundary line separates the region for which the theoretical threshold value for QDER allows for a secure key to be established between Alice and Bob. While the turbulent channel prevents communication for any dimension greater than $d = 2$ when the correction system is not considered, Bob's use of AO allows for secure keys to be established for all cases less than $d = 10$.

$R = 0$.

Here, the quantum communication channel makes use of two MUB based on two sets of structured beams. The first one, which we consider the logical basis $\{|\psi_\ell\rangle\}$, is given by the family of OAM states with topological charge $\ell$, where $\ell$ is an integer number. To reduce crosstalk, we consider all values of $\ell = -d/2 \ldots d/2$, excluding the value of $\ell = 0$. Meanwhile, the second MUB, known as the angular mode basis (ANG), consists of a set of beams that are a balanced superposition of such OAM modes given by a quantum Fourier transform of the OAM modes.

$$|\varphi_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi i \frac{jk}{d}} |j\rangle \,, \tag{4}$$

where $j = d/2 + (\ell - 1)\,\Theta(\ell) + \ell\,\Theta(-\ell)$, and $\Theta(x)$ is the Heaviside function.

In order to obtain the QDER of a turbulent free-space channel, we need to calculate the crosstalk matrix. A crosstalk matrix is determined by sending each of the states in both bases

$\{|\psi_i\rangle\}$ and $\left\{\left|\varphi_j\right\rangle\right\}$, and performing projective measurements of the same states. Based on the properties of MUB, it must be noted that a measurement of a projection made on the incorrect basis, i.e. $\left|\left\langle\psi_i\middle|\varphi_j\right\rangle\right|^2$, is equally likely to result in any of the states of the projection basis with a probability of $1/d$. We perform the projective measurements for all even dimensions up to 10, i.e., $d = \{2, 4, 6, 8, 10\}$. The experimental crosstalk matrices in dimensions $d = 4$, $d = 6$, and $d = 10$ for both MUBs in our turbulent channel are shown in panels **a**, **b**, and **c** of Fig. 4, respectively.

Following these results, we proceed to calculate the QDER of our turbulent channel. Fig. 4**d** depicts the QDER as calculated in each dimension $d$. The results show that the QDER exceeds the security boundary given by equation (3) in all dimensions where $d > 2$, measured when no compensation is applied in Bob's detection stage. Therefore, it is not possible to establish a secure communication channel in the presence of applied turbulence. Nevertheless, when the AO system is active, the QDER is reduced to values below the theoretical threshold for positive key rates in all tested cases except for that of the 10-dimensional ANG basis, while. We find that the average decrease in QDER over all tested cases is 32.5%. This is a promising result, indicating that the use of an AO system can allow for significant improvements in the detection of high-dimensional spatial modes for use in free-space communication.

Our measurements of QDER for different QKD dimensions are shown in Fig. 4**d**. Interestingly, our results show that the logical basis is more influenced by the introduced turbulence than the ANG basis and the AO performs better on reducing the crosstalk in the logical basis rather than in the ANG basis (this is particularly evident for $d = 10$). These effects can be qualitatively understood when considering that both (mild) turbulence and adaptive optics mainly affect the phase of the beam. The orthogonality of OAM modes depends on their azimuthal phase structure, so is extremely sensitive to phase distortions while ANG modes have a smooth phase dependence but different intensity distributions. The AO performs less well on ANG modes in higher dimensional basis since these modes are increasingly localised in the azimuthal coordinate, thus a higher resolution is needed to compensate for the aberrations induced by turbulence.

Our experiment demonstrates that the use of a sufficiently advanced adaptive optics system can allow for high-dimensional quantum communications in channels where turbulence would otherwise prevent it.

*Turbulence Measurement* – In our experiment, a second WFS is used in our setup in such a way to monitor the reference beam before the correction of the DM was applied (see Fig. 1 **a**). From the collected data, it is possible to extract instantaneous wavefronts and the corresponding decomposition in terms of Zernike polynomials as functions of time. In Fig. 5, we show standard deviations of the first nine Zernike coefficients, excluding the first one, a global phase shift, over a period of 195 seconds with active turbulence. The strength of the fluctuations in our experiment is in the range of those measured in a previous experiment, where a 3m underwater channel was characterized [41]. In this experiment, a secure key could not be generated when $d = 4$ due to the effects of the underwater turbulence. In our experiment, we also find that a secure key cannot be generated for $d = 4$ unless wavefront correction using a fast AO is implemented in the channel. Thus, our results are promising not only for free-space applications but also for other turbulent environments, i.e. underwater channels.

In addition to measuring the Zernike coefficients, we calculate the Fried parameter $r_0$ [42–44]. This parameter represents the average diameter of the theoretical circular air pockets across which the wavefront phase experiences one radian of variation. From the Fried parameter, we can quantify the strength of the turbulence introduced in our system with the parameter $D/r_0$, where $D$ represents the diameter of the effective aperture used to estimate $r_0$. In our experiment, we obtained $r_0$ by measuring the beam wander of a Gaussian state sent through the channel over time [42]. Here, $D$ is given by the waist of the Gaussian beam considered. Following this, we find that the turbulence used in our experiments has a value of $D/r_0 = 1.70$. This value indicates that our turbulent cell generates moderate-strong turbulence [45]. This allows us to compare with previous attempts to use active compensation to increase the key rate. Previous studies showed that under similar turbulence conditions, the improvement in QDER when using AO was not enough to establish a secure channel when $d = 5$ [45]. This impossibility may result from utilizing an AO system with lower resolution.

**Conclusion –** In this work, we have tested the capabilities of a fast and high-resolution adaptive optics system in the context of free-space communication channels. We have shown that AO can significantly improve the coupling of a Gaussian beam propagating through a non-uniform, changing medium. Then, we proved the advantage of the use of AO in performing high-dimensional quantum key distribution using spatial modes of photons. Through process tomography, it is shown that the inclusion of the compensation increases fidelity with the identity matrix from under 50% to over 95% in dimensions up to $d = 5$. Finally, we demonstrate that by utilizing AO, it is possible to implement a high-dimensional BB84 QKD protocol through a turbulent channel, where it would otherwise not have been possible. We note that the observed turbulence is similar to previously performed experiments both indoors and underwater, as confirmed by Zernike decomposition and the estimation of the Fried parameter. We foresee using an AO system in practical free-space links for classical and quantum communications, in particular, in QKD networks utilizing satellites.

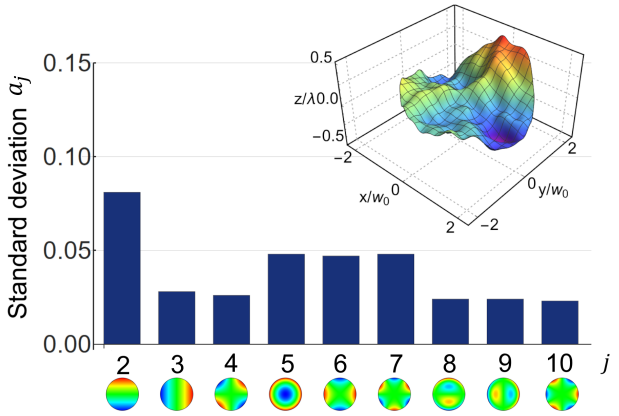


FIG. 5. **Decomposition of the turbulence on the Zernike basis.** Standard deviation of the first nine coefficients $a_j$ of the Zernike decomposition after propagation through the turbulent cell. The WFS reports the turbulence decomposition in the Zernike polynomials basis as a function of time. The inset depicts an aberrated wavefront at a particular time $t_0$, where $w_0$ is the beam waist of the Gaussian mode that would be included in the protocol if using odd dimensions

**Acknowledgments.** The authors would like to thank Alicia Sit for the valuable discussion and her help in setting up the AO system, as well as the ALPAO support team for their responsibility and support. This work was supported by Canada Research Chairs; Canada First Research Excellence Fund (CFREF); National Research Council of Canada High-Throughput and Secure Networks (HTSN) Challenge Program; and the Qeyssat User INvestigation Team (QUINT) Alliance Consortia Quantum grant.

**Author Contributions** E.K. conceived the idea; L.S., F.H., M.F, A.D, and E.K. designed the experiments; L.S. and F.H performed the experiments and collected the data; L.S., F.H., and M.F analysed the data and wrote the first version of the manuscript. K.H. and E.K. supervised the project. All authors discussed the results and contributed to the text of the manuscript.

**Supplementary materials** accompanies this manuscript.

* ekarimi@uottawa.ca

[1] Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
[2] Bennett Ch, H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing int 175–9 (1984).
[3] Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**, 120–126 (1978).
[4] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *Journal of Cryptology* **5**, 3–28 (1992).
[5] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Physical Review A* **61**, 062308 (2000).
[6] Ecker, S. *et al.* Overcoming noise in entanglement distribution. *Physical Review X* **9**, 041042 (2019).
[7] Reimer, C. *et al.* Integrated frequency comb source of heralded single photons. *Optics Express* **22**, 6535–6546 (2014).
[8] Brecht, B., Reddy, D. V., Silberhorn, C. & Raymer, M. G. Photon temporal modes: a complete framework for quantum information science. *Physical Review X* **5**, 041017 (2015).
[9] Ndagano, B., Nape, I., Cox, M. A., Rosales-Guzman, C. & Forbes, A. Creation and detection of vector vortex modes for classical and quantum communication. *Journal of Lightwave Technology* **36**, 292–301 (2017).
[10] Islam, N., Lim, C., Cahall, C., Kim, J. & Gauthier, D. Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances* **3**, e1701491 (2017).
[11] Vallone, G. *et al.* Free-space quantum key distribution by rotation-invariant twisted photons. *Physical Review Letters* **113**, 060503 (2014).
[12] Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New Journal of Physics* **17**, 033033 (2015).
[13] Wang, Q.-K. *et al.* High-dimensional quantum cryptography with hybrid orbital-angular-momentum states through 25 km of ring-core fiber: A proof-of-concept demonstration. *Physical Review Applied* **15**, 064034 (2021).
[14] Cozzolino, D. *et al.* Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Physical Review Applied* **11**, 064058 (2019).
[15] Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
[16] Sit, A. *et al.* Quantum cryptography with structured photons through a vortex fiber. *Optics Letters* **43**, 4108–4111 (2018).
[17] Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Optics Express* **26**, 22563–22573 (2018).
[18] Hufnagel, F. *et al.* Characterization of an underwater channel for quantum communications in the ottawa river. *Optics Express* **27**, 26346–26354 (2019).
[19] Mair, A., Vaziri, A., Weihs, G. & Zeilinger, A. Entanglement of the orbital angular momentum states of photons. *Nature* **412**, 313 (2001).
[20] ALPAO. Adaptive Optics Systems. `https://www.alpao.com/products-and-services/adaptive-optic-system/` (2023). Accessed: 2023-10-20.
[21] Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
[22] Schmitt-Manderbach, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* **98**, 010504 (2007).
[23] Liao, S.-K. *et al.* Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
[24] Vallone, G. *et al.* Experimental satellite quantum communications. *Physical Review Letters* **115**, 040502 (2015).
[25] Kolmogorov, A. N. A refinement of previous hypotheses concerning the local structure of turbulence in a viscous incompressible fluid at high reynolds number. *Journal of Fluid Mechanics* **13**, 82–85 (1962).
[26] Malik, M. *et al.* Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding. *Optics Express* **20**, 13195–13200 (2012).
[27] Klug, A., Nape, I. & Forbes, A. The orbital angular momentum of a turbulent atmosphere and its impact on propagating structured light fields. *New Journal of Physics* **23**, 093012 (2021).
[28] Lavery, M. P. *et al.* Free-space propagation of high-dimensional

structured optical fields in an urban environment. *Science Advances* **3**, e1700552 (2017).
[29] Cox, M. A. *et al.* Structured light in turbulence. *IEEE Journal of Selected Topics in Quantum Electronics* **27**, 1–21 (2020).
[30] Jin, J. *et al.* Demonstration of analyzers for multimode photonic time-bin qubits. *Physical Review A* **97**, 043847 (2018).
[31] Beckers, J. M. Adaptive optics for astronomy: principles, performance, and applications. *Annual review of astronomy and astrophysics* **31**, 13–62 (1993).
[32] Tyson, R. K. *Introduction to adaptive optics*, vol. 41 (SPIE press, 2000).
[33] van Dam, M. A., Le Mignant, D. & Macintosh, B. A. Performance of the keck observatory adaptive-optics system. *Applied Optics* **43**, 5458–5467 (2004).
[34] Majumdar, A. K., Ricklin, J. C., Weyrauch, T. & Vorontsov, M. A. Free-space laser communications with adaptive optics: Atmospheric compensation experiments. *Free-space laser communications: principles and advances* 247–271 (2008).
[35] Wang, Y. *et al.* Performance analysis of an adaptive optics system for free-space optics communication through atmospheric turbulence. *Scientific Reports* **8**, 1124 (2018).
[36] Liu, C., Chen, M., Chen, S. & Xian, H. Adaptive optics for the free-space coherent optical communications. *Optics Communications* **361**, 21–24 (2016).
[37] Fernández-Pérez, A., Klimov, A. & Saavedra, C. Quantum process reconstruction based on mutually unbiased basis. *Physical Review A* **83**, 052332 (2011).
[38] Nielsen, M. A. & Chuang, I. L. *Quantum computation and quantum information* (Cambridge university press, 2010).
[39] Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Annals of Physics* **191**, 363–381 (1989).
[40] Bouchard, F. *et al.* Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018).
[41] Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Optics Express* **26**, 22563–22573 (2018).
[42] Fried, D. L. Optical resolution through a randomly inhomogeneous medium for very long and very short exposures. *Journal of Optical Society of America* **56**, 1372–1379 (1966).
[43] Kolmogorov, A. N. The local structure of turbulence in incompressible viscous fluid for very large reynolds numbers. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* **434**, 9–13 (1991).
[44] Ageorges, N. & Dainty, C. *Laser guide star adaptive optics for astronomy*, vol. 551 (Springer Science & Business Media, 2013).
[45] Zhao, J. *et al.* Performance of real-time adaptive optics compensation in a turbulent channel with high-dimensional spatial-mode encoding. *Optics Express* **28**, 15376–15391 (2020).

# Chapter 5

# Conclusion

In this thesis many different aspects of high-dimensional quantum optics have been discussed. In Chapter 2 we have shown new results in liquid crystal fabrication through magic windows and optimal focusing. Using liquid crystal devices we are able to push the limits of what type of spatial modes we can produce. Improving these tools allows us to encode more information on light for communication, or extend our sensitivity for detection and sensing applications. In Chapter 3 we have also demonstrated the possibilities for spatial mode entanglement through the characterization of SPDC sources in the Laguerre-Gaussian modes and in momentum correlations. These sources are a critical piece of high-dimensional quantum applications. In Chapter 4 we demonstrated two new protocols in high-dimensional quantum communications. The round robin protocol fundamentally relies on high-dimensional states to allow for quantum key distribution without monitoring for signal disturbances introduced by an eavesdropper. Finally, we put all of these different pieces together and introduce an adaptive optics system to explore the real-world feasibility of a high-dimensional quantum communication protocol with spatial modes. This is a subset of my work in the field which also includes quantum communication in underwater channels, using liquid crystal devices for chiral sensing and coherent control on semiconductors, compressed sensing with spatial modes, and quantum tomog-

raphy. There is still future research that is required in using spatial modes for quantum communication. Adaptive optics systems need to be tested with spatial modes in longer channels, and the implementation of these systems in remote sensing and super-resolution still needs to be explored. There is also still work to be done in exploring the optimal choice for information encoding in real-world, turbulent environments. Comparisons between various states such as spatial modes, polarization, time-bins, or temporal modes will reveal whether one is optimal in free-space channels.

High-dimensional states have many attractive qualities for applications in quantum information. Beyond orbital angular momentum which we focused on here, one can find many other useful degrees of freedom such as time-bins, frequency combs, and temporal modes. Each of these degrees of freedom has its own challenges and benefits. In particular, many of these states suffer in free-space channels from atmospheric turbulence. Time bin states typically require very high interference visibilities which can be reduced when the phase becomes distorted. OAM of course suffers from mode cross-talk when there are phase distortions across the beam. While it remains to be seen whether high-dimensional states will prove technologically viable for the implementation of robust and low cost quantum communication networks, the ability to work with these various degrees of freedom will certainly find use in other applications such as sensing. It has been shown in this thesis and in many other works that there is still significant progress to be made in the technologies around structured light. New devices and protocols for sensing will continue to develop which increase the viability of various photonic degrees of freedom for commercial applications and for studying fundamental science.

# APPENDICES

# Appendix A

# Supplementary materials: Full-mode characterization of correlated photon pairs generated in spontaneous downconversion

Supplemental Document

Optics Letters

# Full-mode characterization of correlated photon pairs generated in spontaneous downconversion: supplement

ALESSIO D'ERRICO,[1,*] FELIX HUFNAGEL,[1] FILIPPO MIATTO,[1,2] MOHAMMADREZA REZAEE,[1] AND EBRAHIM KARIMI[1,3]

[1]*Physics Department, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa, Ontario K1N 6N5, Canada*
[2]*Current address: Xanadu, 777 Bay St., Toronto, Ontario M5G2C8, Canada*
[3]*e-mail: ekarimi@uottawa.ca*
[*]*Corresponding author:* [redacted]



Supplement DOI: https://doi.org/10.6084/m9.figshare.14447232

Parent Article DOI: https://doi.org/10.1364/OL.424619

# Supplementary Information for Full-mode Characterisation of Correlated Photon Pairs Generated in Spontaneous Downconversion

This document provides supplementary material information to *Full-mode Characterisation of Correlated Photon Pairs Generated in Spontaneous Downconversion*.

## 1. SOLUTION OF EQUATION (3)

Eq. (3), after solving the azimuthal integration, which gives OAM conservation, can be put in the form

$$c_{p_s,\ell_s}^{p_i,\ell_i} = \mathcal{N}\int_0^\infty dr\, r^{|\ell_i|+|\ell_s|+|\ell_p|+1} e^{-r^2(/1w_i^2+1/w_s^2+1/w_p^2)} \times L_{p_i}^{|\ell_i|}(2(r/w_i)^2) L_{p_s}^{|\ell_s|}(2(r/w_s)^2) L_{p_p}^{|\ell_p|}(2(r/w_p)^2), \tag{S1}$$

which can be solved analytically in terms of the first Lauricella hypergeometric function $F_A^{(3)}$ as we show below. In general the function $F_A^{(3)}$ has to be evaluated numerically, for example exploiting its integral representation, hence this result has no particular advantage with respect to the simple numerical evaluation of Eq. S1. However a more numerically accessible analytical formula can be given in the case $p_p = 0$, using $L_0^{|\ell_p|}(x) = 1$. From the results in Ref. [1] one can easily obtain:

$$c_{p_s,\ell_s}^{p_i,\ell_i}(p_p = 0, \ell_p) = \mathcal{N}\binom{p_i + |\ell_i|}{p_i}\binom{p_s + |\ell_s|}{p_s}\frac{\Gamma(\ell_T+1)}{\sigma^{\ell_T+1}} \times F_2[\ell_t + 1, -p_i, -p_s; |\ell_i| + 1, |\ell_s| + 1; \lambda_i/\sigma, \lambda_s/\sigma] \tag{S2}$$

where $F_2[a, b, b', ; c, c'; x, y]$ is the second Appell function (which can be computationally implemented easily in MAPLE), $\ell_t = (\left|\ell_p\right| + |\ell_i| + |\ell_s|)/2$, $\sigma = (1/w_p^2 + 1/w_i^2 + 1/w_s^2)$ and $\lambda_{i,s} = 2/w_{i,s}^2$. $\mathcal{N}$ is a normalization constant given below for the general case of arbitrary $p_p$.

For the general case, We start from Eq. S1 which, with $r^2 \equiv x$, can be rewritten as:

$$c_{p_s,\ell_s}^{p_i,\ell_i} = \mathcal{N}\int_0^\infty x^{\ell_T} e^{-\sigma x} L_{p_p}^{|\ell_p|}(\lambda_p x) L_{p_i}^{|\ell_i|}(\lambda_i x) L_{p_s}^{|\ell_s|}(\lambda_s x) dx \tag{S3}$$

where $\lambda_p = 2/w_p^2$ and

$$\mathcal{N} = 2\pi\sqrt{\frac{2\,p_p!p_i!p_s!}{\pi^3(p_p + \left|\ell_p\right|)!(p_i + |\ell_i|)!(p_s + |\ell_s|)!}}\frac{\sqrt{2}^{2\ell_T}}{w_p^{|\ell_p|+1} w_i^{|\ell_i|+1} w_s^{|\ell_s|+1}}.$$

Eq. S3 can be immediately solved using Eq. 4 in Ref. [1]. We obtain

$$c_{p_s,\ell_s}^{p_i,\ell_i} = \mathcal{N}\binom{p_p + \left|\ell_p\right|}{p_p}\binom{p_i + |\ell_i|}{p_i}\binom{p_s + |\ell_s|}{p_s}\frac{\Gamma(\ell_T+1)}{\sigma^{\ell_T+1}} \times F_A^{(3)}[\ell_T + 1, -p_p, -p_i, -p_s; \left|\ell_p\right| + 1, |\ell_i| + 1, |\ell_s| + 1; \frac{\lambda_p}{\sigma}, \frac{\lambda_i}{\sigma}, \frac{\lambda_s}{\sigma}]. \tag{S4}$$

$F_A^{(3)}$ is the first Lauricella's hypergeometric function, defined by the series:

$$F_A^{(3)}[\ell_T+1,-p_p,-p_i,-p_s;\left|\ell_p\right|+1,|\ell_i|+1,|\ell_s|+1;\frac{\lambda_p}{\sigma},\frac{\lambda_i}{\sigma},\frac{\lambda_s}{\sigma}] := \sum_{k_1,k_2,k_3=0}^{\infty} \frac{(\ell_T+1)_{k_1+k_2+k_3}(-p_p)_{k_1}(-p_i)_{k_2}(-p_s)_{k_3}}{(1+\left|\ell_p\right|)_{k_1}(1+|\ell_i|)_{k_2}(1+|\ell_s|)_{k_3}} \times \frac{(\lambda_p/\sigma)^{k_1}(\lambda_i/\sigma)^{k_2}(\lambda_s/\sigma)^{k_3}}{k_1!k_2!k_3!} \tag{S5}$$

where $(\alpha)_k := \Gamma(\alpha+k)/\Gamma(\alpha)$ is the Pochhammer symbol.

## 2. INTENSITY MASKING TECHNIQUE FOR GENERATING AND MEASURING OPTICAL MODES

An exact method for generating arbitrary paraxial beams from an input plane wave was devised in [2]. The desired beam can be obtained by selecting the first diffraction order of a phase mask described by the function,

$$g(x,y) = M(x,y)\,\mathrm{Mod}\left(\frac{2\pi}{\Lambda}x + F(x,y), 2\pi\right), \tag{S6}$$

with,

$$M(x,y) = 1 - \frac{1}{\pi}\mathrm{sinc}^{-1}(A(x,y)) \tag{S7}$$

$$F(x,y) = \Psi(x,y) - \pi M(x,y), \tag{S8}$$

where $A(x,y)$ and $\Psi(x,y)$ are, respectively, the amplitude and phase of the beam that one wants to generate, i.e. $A(x,y)\,e^{i\Psi(x,y)}$.
Now we discuss how this technique can be used "in reverse", i.e. to measure instead of generating a desired mode. Assume the input field has a complex amplitude $X(\mathbf{r})$. To project on a mode $\Pi(\mathbf{r})$, the intensity masking system is set to display $\Pi^*(\mathbf{r})$. The resulting field will be $X(\mathbf{r})\Pi^*(\mathbf{r})$. When this field is focused on the single mode fiber tip, it will be given by its 2D Fourier transform: $\mathcal{F}(X\Pi^*) = \mathcal{F}(X) * \mathcal{F}(\Pi^*)$ (where $*$ is the convolution operation). The detected intensity (or count rate) is proportional to

$$R \propto \left| \int\int d^2\mathbf{r}\,[\mathcal{F}(X) * \mathcal{F}(\Pi^*)](\mathbf{r})\,e^{-\frac{r^2}{\sigma^2}} \right|^2, \tag{S9}$$

where $\sigma$ is the waist of the fiber mode (approximated with a Gaussian). In the limit $\sigma \to 0$ the count rate becomes proportional to the absolute square of the Hermitian product between the two modes: $R \propto \left|\langle \mathcal{F}(\Pi)|\mathcal{F}(X)\rangle\right|^2 = \left|\langle \Pi|X\rangle\right|^2$. This condition can be achieved by making the mode of the fiber, *on the phase mask plane*, much larger than the mode $\Pi$. This is experimentally achieved by a magnification system mentioned in point 2). In practice, a finite $\sigma$ will lead to cross-talk effects that have to be quantified either theoretically, or from calibration measurements. Employing the same approach on photon pairs, is straightforward to see that coincidence measurements will be proportional to the projection on biphoton states $|\Pi_1\rangle \otimes |\Pi_2\rangle$, with $\Pi_{1,2}$ arbitrary spatial modes. Indeed we can show that the coincidence count rate is:

$$C \propto \left| \sum_{p_s,\ell_s,p_i,\ell_i} c^{p_i,\ell_i}_{p_s,\ell_s} \langle \Pi_1|\ell_i,p_i\rangle\langle \Pi_2|\ell_s,p_s\rangle \right|^2 \tag{S10}$$

which is equal to $\left|c^{p_i,\ell_i}_{p_s,\ell_s}\right|^2$ when one projects on the states $|\Pi_{1,2}\rangle = |\ell_{1,2},p_{1,2}\rangle$.

In the following we give a detailed derivation of Eq. S10. To calculate the expected coincidence rate $C$ we start from the SPDC state at the nonlinear crystal plane:

$$|\Psi\rangle_{\mathrm{SPDC}} \propto \int d\mathbf{x}\,\tilde{\mathcal{E}}(\mathbf{x})|\mathbf{x}\rangle_i \otimes |\mathbf{x}\rangle_s, \tag{S11}$$

which can be decomposed in any orthogonal set of modes $\{|\tilde{f}_a\rangle\}_{a\in\mathcal{I}}$, where $\mathcal{I}$ is a set of indices ($a=(p,\ell)$ in the case of LG modes):

$$|\Psi\rangle_{\mathrm{SPDC}} \propto \sum_{a,b}\int d\mathbf{x}\,\tilde{\mathcal{E}}(\mathbf{x})\tilde{f}_a^*(\mathbf{x})\tilde{f}_b^*(\mathbf{x})|\tilde{f}_a\rangle_i\otimes|\tilde{f}_b\rangle_s := \sum_{a,b}c_{a,b}|\tilde{f}_a\rangle_i\otimes|\tilde{f}_b\rangle_s. \tag{S12}$$

The effect of the propagation through the setup is described by operations on the vectors $|\tilde{f}_a\rangle_{i,s}$. Since these operation are spatial transformations of optical modes it is convenient to writhe $|\Psi\rangle_{\mathrm{SPDC}}$ in the $\mathcal{L}^2\otimes\mathcal{L}^2$ space, (i.e. considering the biphoton wavefunction $\Psi_{SPDC}(\mathbf{x}_1,\mathbf{x}_2) := \langle\mathbf{x}_1,\mathbf{x}_2|\Psi_{SPDC}\rangle$) where the action of free space propagation and optical elements can be explicitly written:

$$\Psi_{\mathrm{SPDC}}(\mathbf{x}_i,\mathbf{x}_s) \propto \sum_{a,b}c_{a,b}\tilde{f}_a(\mathbf{x}_i)\tilde{f}_b(\mathbf{x}_s). \tag{S13}$$

In particular, the evolution from the crystal plane to the two SLMs planes, which are placed in the Fourier plane of the crystal, is given by the 2D Fourier transform:

$$\begin{aligned}\mathcal{F}[\tilde{f}_a(\mathbf{x}_i)\tilde{f}_b(\mathbf{x}_s)] &= \int d\mathbf{x}e^{i\mathbf{x}\cdot\mathbf{X_i}}\tilde{f}_a(\mathbf{x})\int d\mathbf{x}'e^{i\mathbf{x}'\cdot\mathbf{X_s}}\tilde{f}_b(\mathbf{x}')\\ &:= f_a(\mathbf{X}_i)f_b(\mathbf{X}_s)\end{aligned} \tag{S14}$$

where $\mathbf{X}_{i,s}$ are coordinates on the SLMs planes (with dimensional factors included).
The remaining part of the setup before the fiber couplers (SLMs plus filtering pinholes) implements the transformation: $f_a(\mathbf{X}_i)f_b(\mathbf{X}_s)\to g_1^*(\mathbf{X}_i)f_a(\mathbf{X}_i)g_2^*(\mathbf{X}_s)f_b(\mathbf{X}_s)$, where $g_{1,2}$ are the optical modes displayed on the SLMs A and B, respectively. The coupling with the single mode fibers, with the properly designed demagnification system, is equivalent to integrating the above transformation over the whole transverse space. In conclusion we obtain:

$$C \propto \left|\sum_{a,b}c_{a,b}\int g_1^*(\mathbf{X}_i)f_a(\mathbf{X}_i)d\mathbf{X}_i\int g_2^*(\mathbf{X}_s)f_b(\mathbf{X}_s)d\mathbf{X}_s\right|^2 \tag{S15}$$

which, if $g_1=f_a$ and $g_2=f_b$, yields $C\propto|c_{a,b}|^2$.

## 3. DETAILED SETUP

In Fig. S1 we report a sketch of the full experimental setup. We measured a back-propagating beam waist on the SLM planes of $\sigma=1.5$ mm, while using waist parameters on the projected modes of the order of 0.6 mm.

## 4. SIMULATION OF OAM CORRELATIONS DETECTED WITHOUT AMPLITUDE MASKING

In Figures (1)-d and (2)-a,b of the main article we have shown how OAM correlations are nonzero only if $\ell_p=\ell_i+\ell_s$, i.e. one observes nonzero values along one diagonal (principal or secondary, depending on the pump OAM). It is interesting to observe the shape of the OAM correlations along these diagonals: in previous works, see e.g. [3], one always observes that the highest coincidence rate occurs in correspondence of the lowest order modes, and this behavior is expected for any $\ell_p$. On the contrary, in our experiment we observe that, for $\ell_p\neq 0$ the correlations along the diagonals exhibit a dip in the lowest order modes. This is due to a fundamental difference between our detection system and the one used in previous works. In the latter case the detected photons where always postselected on a gaussian mode by the use of single mode fibers. In our experiment, due to the applied demagnification, we instead measure a different radial mode. If no masking is applied on the detection SLMs, then we are projecting on Hypergeometric-Gaussian modes, $\mathrm{HyGG}_{-|\ell|,\ell}(r,z\phi)$ [4]. More specifically we may write the function $g$ displayed on the SLM as $g(r,\theta)\propto e^{-r^2}e^{i\ell_{i,s}\theta}$, where $\theta$ is the azimuthal coordinate in the SLM plane, and $r$ an adimensional radial coordinate that takes into account the finite size of the optical system (which is of the order of the backalignment beam size). The coefficients determining the coincidence rate are given by (we recall that the fields must be considered on the crystal plane):

$$c_{\ell_i,\ell_s} = \int d^2\mathbf{x}\,\mathrm{LG}_{p_p,\ell_p}(\mathbf{x})\mathcal{F}(g_{\ell_i})^*(\mathbf{x})\mathcal{F}(g_{\ell_s})^*(\mathbf{x}) \tag{S16}$$

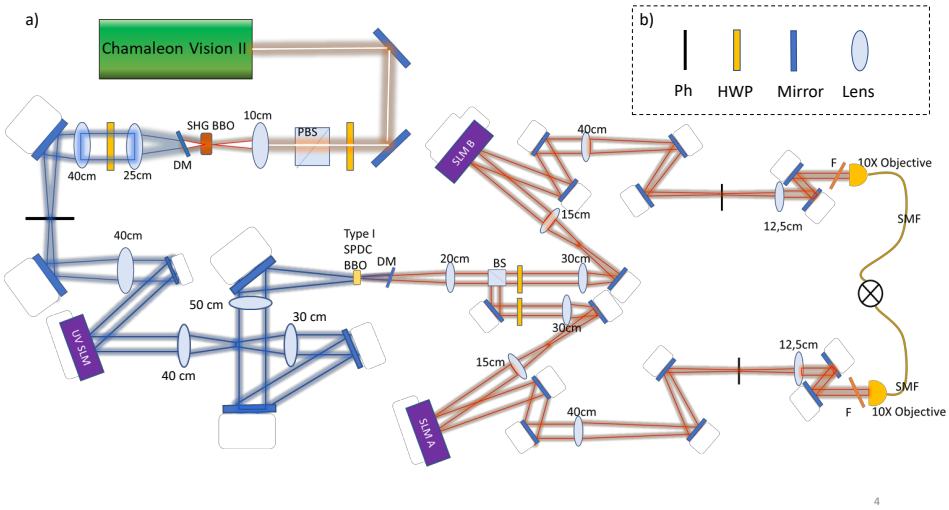


**Fig. S1. Detailed experimental setup** a) Sketch of the experimental setup. b) Legend

where:

$$\begin{aligned}\mathcal{F}(g_\ell)(\mathbf{x}) &= \int_0^\infty e^{-r^2} r dr \int_0^{2\pi} e^{i\ell\theta} e^{\rho r \sin(\phi-\theta)} d\theta \\ &= (-1)^\ell e^{i\ell\phi} \int_0^\infty e^{-r^2} r J_\ell(\rho r) dr \\ &= (-1)^\ell e^{i\ell\phi} \sqrt{\pi} \frac{\rho}{8} e^{-\rho^2/8} \left( I_{(\ell-1)/2}(\rho^2/8) - I_{(\ell+1)/2}(\rho^2/8) \right), \end{aligned} \tag{S17}$$

where $I_n(z)$ are modified Bessel function of the first kind, $\rho$ the radial coordinate on the crystal plane, $\phi$ the azimuthal coordinate. Using this expression in Eq. S16 we obtained results in nice agreement with the observed experimental correlations (see Fig. S2).

## 5. MEASUREMENT OF CROSS-TALK MATRICES AND DETECTION EFFICIENCIES

In order to estimate the detection efficiencies we used the setup in Fig. S1 replacing the BBO crystal with a mirror and sending an 810 nm diode laser through the output coupler $D_A$. The main idea is to use SLMA to generate the desired mode and SLMB to measure it, without modifying the parameters employed in the experiment. For each generated mode (labelled as $p_i$) we measure all the radial modes $p_s = 0, \ldots, 3$, for a fixed OAM $\ell = 0, \ldots, 5$, thus retrieving the cross talk matrices in Fig. S3. The (normalized) diagonal values of these matrices are proportional to the inverse of the detection efficiencies.

## 6. DETAILS ON QUANTUM TOMOGRAPHY MEASUREMENT AND DENSITY MATRIX RECONSTRUCTION

Full quantum tomography in a $d$-dimensional Hilbert space requires projection on $d^2$ states. In our case, choosing $p_i, p_s = 0 \ldots, 3$ we have $d = 16$, hence 256 measurements are required for full tomography. The density matrix can be then reconstructed through a maximum likelihood algorithm. The measurement states for performing quantum tomography on a 16-dimensional Hilbert space are given by the tensor products $|\psi\rangle_i \otimes |\zeta\rangle_s$, where $|\psi\rangle$ and $|\zeta\rangle$ can be chosen among the sets: $\{|p\rangle\}_{p=0}^3$ and $\{|p_1\rangle + e^{i\alpha}|p_2\rangle\}_{p_1<p_2}$, with $\alpha = 0, \pi/2$. The experimental density matrix was obtained by minimizing the quantity $\mathcal{L}(\mathbf{S}) := \sum_i [n_i - pr_i(\mathbf{S})]^2$, where the index $i$ runs over all the measured states, $n_i$ are the (normalized) count rates and $Pr_i$ the expected measurement probabilities for a target density matrix,

$$\rho_{\text{exp}} = \sum_{i,j,l,k=0}^{3} S_{i,j,k,l}\, \sigma_i \otimes \sigma_j \otimes \sigma_k \otimes \sigma_l, \tag{S18}$$

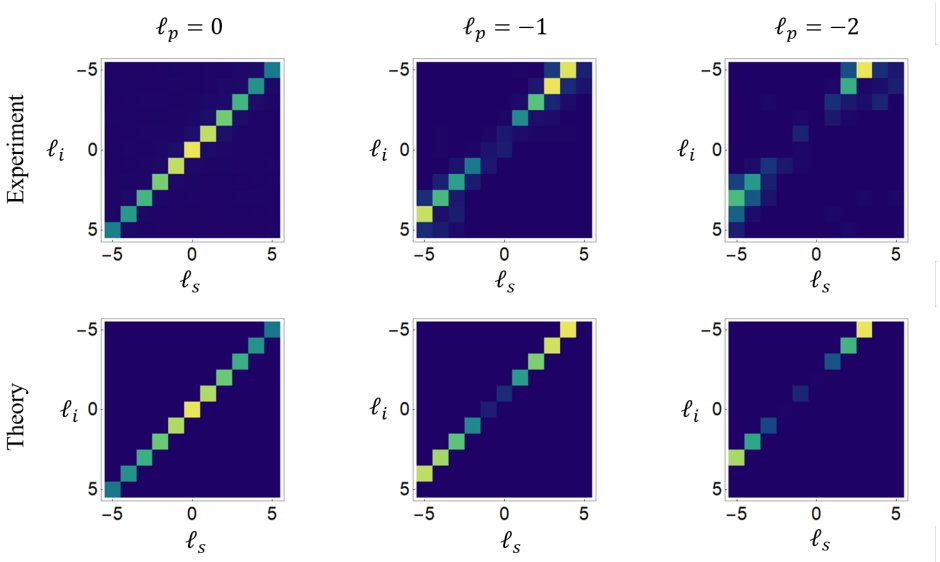


**Fig. S2. OAM correlations: theory and experiment.** We compare experimentally measured OAM correlations with theoretical simulations obtained evaluating S16 by assuming a waist of the HyGG modes on the crystal plane $\approx 0.1 w_p$.

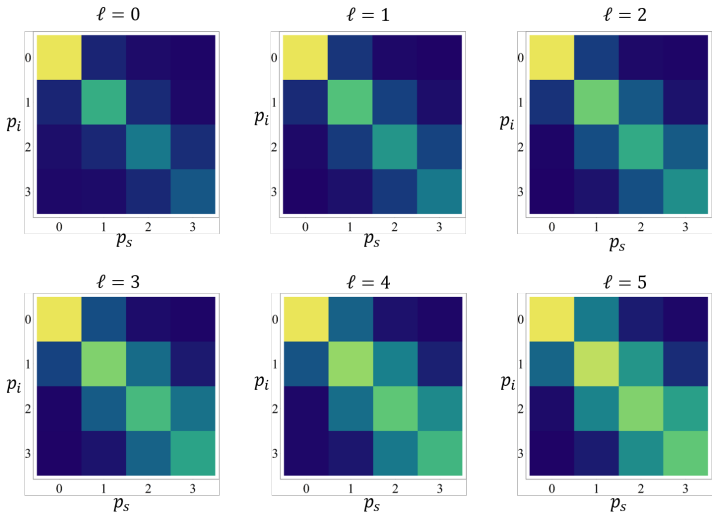


**Fig. S3. detection efficiencies and cross-talk matrices** Experimentally reconstructed crosstalk matrices. The diagonal elements are proportional to the detection efficiencies used to correct the data of the main experiment.

where $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ are Pauli matrices (with $\sigma_0 = I$) and $S_{i,j,k,l}$ are the free parameters defining the vector **S** to be found through the minimization procedure. Since the outcome of SPDC is a pure state we imposed the condition $\mathrm{Tr}[\rho_{exp}^2] = 1$.

## REFERENCES


1. L. Poh-aun, S. hung Ong, and H. M. Srivastava, "Some integrals of the products of laguerre polynomials," Int. J. Comput. Math. **78**, 303–321 (2001).
2. 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).
3. F. Bouchard, J. Harris, H. Mand, N. Bent, E. Santamato, R. W. Boyd, and E. Karimi, "Observation of quantum recoherence of photons by spatial propagation," Sci. Reports **5**, 15330 (2015).
4. E. Karimi, G. Zito, B. Piccirillo, L. Marrucci, and E. Santamato, "Hypergeometric-gaussian modes," Opt. Lett. **32**, 3053–3055 (2007).

# Appendix B

# Supplementary material: Fast Adaptive Optics for High-Dimensional Quantum Communications in Turbulent Channels

# Supplementary Information for: Fast Adaptive Optics for High-Dimensional Quantum Communications in Turbulent Channels

## S1- TURBULENCE ANALYSIS

### Optical wavefronts and Zernike polynomials

The Zernike Polynomials are a set of orthogonal functions that are defined on a unit circle. Given that the majority of optical systems feature circular apertures, they serve as valuable tools for wavefront analysis and are therefore significant within the field of optics [1]. Thus, it is possible to express an arbitrary wavefront $\Phi(R\rho, \phi)$ over a circular aperture of radius $R$ in terms of the Zernike polynomials $Z_j$. Explicitly, we can write

$$\Phi(R\rho, \phi) = \sum_j a_j Z_j(\rho, \phi), \tag{S1}$$

where $a_j \in \mathbb{R}$ are the coefficients of the expansion and $(\rho, \phi)$ are the cylindrical coordinate system. It must be noted that in this manuscript, we follow the normalized single-index Zernike polynomials according to the ANSI standard [2]. Table S1 contains some information regarding the correspondence between the indexes and the Zernike Polynomials. Figure **S1** illustrates the first ten Zernike polynomials – the hue colour shows the function value in the interval of $[-1, +1]$.

### Calculation of the Fried Parameter

Let us define the Fried parameter $r_0$ as a fundamental spatial coherence length measure that quantifies the spatial resolution of the effect of the atmospheric turbulence that our beam experiences. In general, the Fried parameter is given by [3]

$$r_0 = 0.98\frac{\lambda}{\beta}, \tag{S2}$$

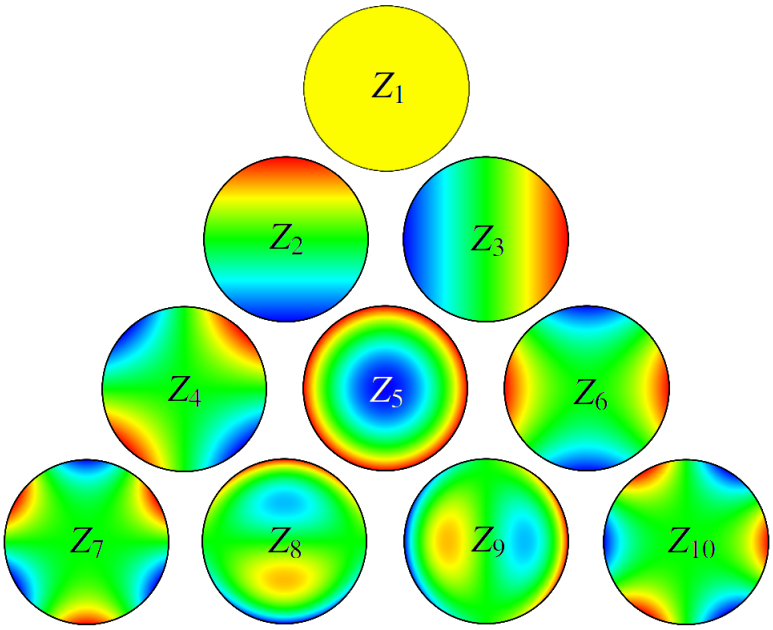


**Figure S1**. The First 10 Zernike polynomials, ordered vertically by values of $n$ and horizontally by the values of $m$.

| ANSI index | | Standard indeces | | Polynomial | Name |
|---|---|---|---|---|---|
| Index | Normalization Factor | n | m | | |
| 1 | 1 | 0 | 0 | 1 | Piston |
| 2 | 2 | 1 | -1 | $\rho \sin\varphi$ | Tip Y |
| 3 | 2 | 1 | 1 | $\rho \cos\varphi$ | TipX |
| 4 | $\sqrt{6}$ | 2 | -2 | $\rho^2 \sin(2\varphi)$ | Astigmatism +45d |
| 5 | $\sqrt{3}$ | 2 | 0 | $2\rho^2 - 1$ | Defocus |
| 6 | $\sqrt{6}$ | 2 | 2 | $\rho^2 \cos(2\varphi)$ | Astigmatism 0/90d |
| 7 | $\sqrt{8}$ | 3 | -3 | $\rho^3 \sin(3\varphi)$ | Trefoil Y |
| 8 | $\sqrt{8}$ | 3 | -1 | $3\rho^3 \sin\varphi - 2\rho \sin\varphi$ | Coma X |
| 9 | $\sqrt{8}$ | 3 | 1 | $3\rho^3 \cos\varphi - 2\rho \cos\varphi$ | Coma Y |
| 10 | $\sqrt{8}$ | 3 | -3 | $\rho^3 \cos(3\varphi)$ | Trefoil X |

TABLE S1. Zernike polynomials are ordered according to their ANSI index, a common alternative indexing scheme, as well as the polynomial in cylindrical coordinates.

where $\lambda$ corresponds to the beam's wavelength while $\beta$ is the average deflection angle experienced by the beam. In our case, the latter is obtained by measuring the position of the centroid of a Gaussian beam after going through the turbulence cell over short intervals of time. Then, it is possible to calculate the average displacement $\bar{s}$ of the beam's centroid from its original position in the absence of turbulence. Finally, the average deflection angle is then given by,

$$\beta = \tan\left(\frac{\bar{s}}{L}\right), \tag{S3}$$

where $L$ is the length of the turbulent cell.

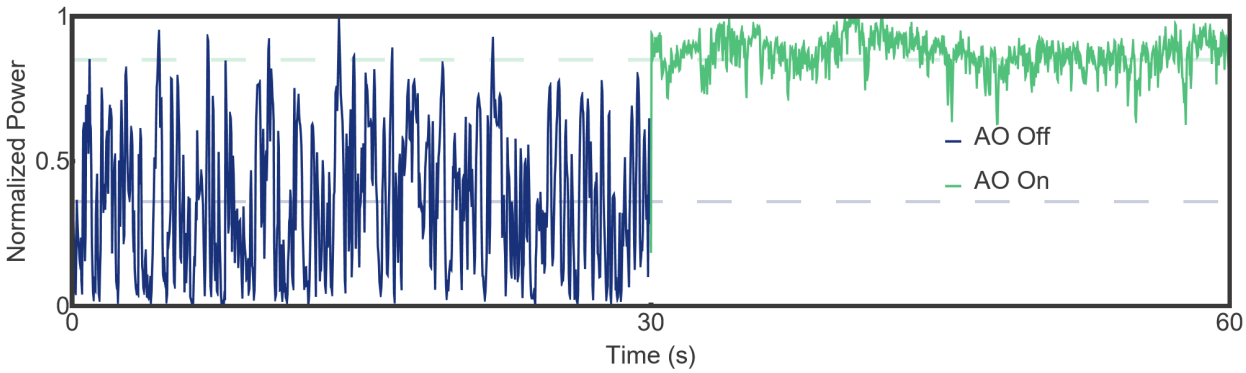


**Figure S2**. Extended figure showing 60 seconds of a Gaussian beam coupling into a single mode fibre through the active turbulent cell. After 30 seconds without any corrections, the AO system is activated.

### Adaptive optics system

The AO system used in our experiment is manufactured by ALPAO and consists of three main components: a deformable mirror (DM) a Shack-Hartmann wavefront sensor (WFS), as well as a feedback-control system. The DM in our configuration (DM9725) has a diameter of 22.5 mm, and utilizes 97 electromagnetic pistons behind the reflective surface in order to modify its profile. These pistons are organized in an $11 \times 11$ grid pattern with cut corners to conform to the circular shape of the mirror. It has a settling time of 1.5 ms, and can therefore operate optimally up to and even slightly above 600 Hz. On the other hand, the Shack-Hartmannn WFS (SH-EMCCD) has an array of $16 \times 16$ microlenses in order to correctly measure the reference beam wavefront. It operates at a frequency of 1kHz. The correction calculations are performed by ALPAO Real Time Computer (RTC) and the interface with the whole system is given by using ALPAO Core Engine (ACE) in MATLAB version R2019a Update 3. The system is dependent on the operating frequency to be faster than that of the Greenwood frequency, $f_G$. This frequency is

the rate at which the turbulence structure within the optical path changes form [4]. We can then consider $1/f_G = \tau_G$ to be the Greenwood time constant which is the amount of time that the turbulence structure is constant. During the experiments, the AO system was operating at 200 Hz. While we do not measure the Greenwood frequency of the turbulence generated in the lab, we can be sure that it is less than 200 Hz as the AO system operated without issue.

### Extended Gaussian coupling

### Turbulent cell

In our experiment, the turbulence cell consists of a hotplate contained within a glass-walled water tank. In it, the variations of the refractive index are produced by the temperature gradient generated by the hotplate. As the layer of air close to the plate gets hotter, it rises and displaces the colder layers of air, allowing to generate isolated turbulence inside the tank. The strength of the effective turbulence can be controlled by setting the hotplate at different temperatures. As shown in Fig. **S3**, as the temperature of the hotplate is increased, the standard deviation of the coefficients $a_j$ of the Zernike decomposition also increases. All experiments were performed with the hotplate setting 1 shown in Fig. **S3**.

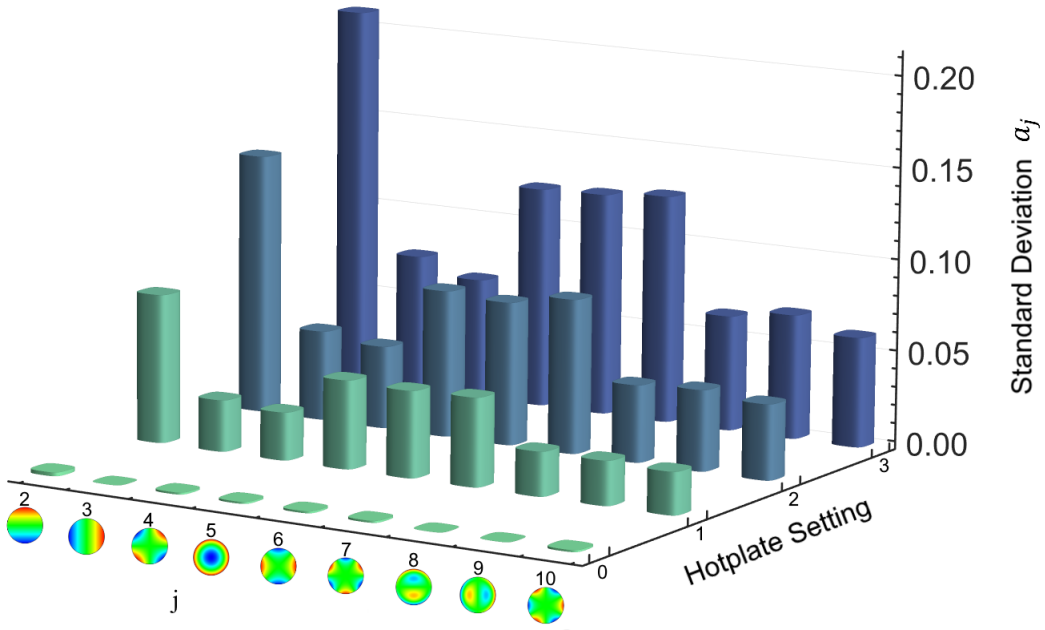


**Figure S3**. Standard deviations of the first nine coefficients $a_j$ of the Zernike decomposition upon propagation through the turbulent cell as a function of the temperature of the hotplate. Here, the value of 0 corresponds to the hotplate completely off, while 3 stands for the highest temperature possible.

## S2- PROCESS TOMOGRAPHY

The process matrices for $d = \{2, 3, 4, 5\}$ are shown in Fig. **S4**. The process tomography was obtained by sending through the turbulent channel and then measuring all the states belonging to the mutually unbiased basis sets for dimension $d$. If $d = p$, where $p$ is a prime numbers, then one can find $p + 1$ MUBs. Starting from the canonical basis $\mathcal{B}_0 := \{|j\rangle\}_{j=0\ldots p-1}$, one can generate the basis $\mathcal{B}_\alpha := \{|\psi_0^\alpha\rangle, \ldots, |\psi_{p-1}^\alpha\rangle\}$, with $0 \leq \alpha \leq p-1$ whose $p$ elements are given by

$$|\psi_t^\alpha\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{p-1} (\omega^t)^{p-j} (\omega^{-\alpha})^{s_j} |j\rangle \tag{S4}$$

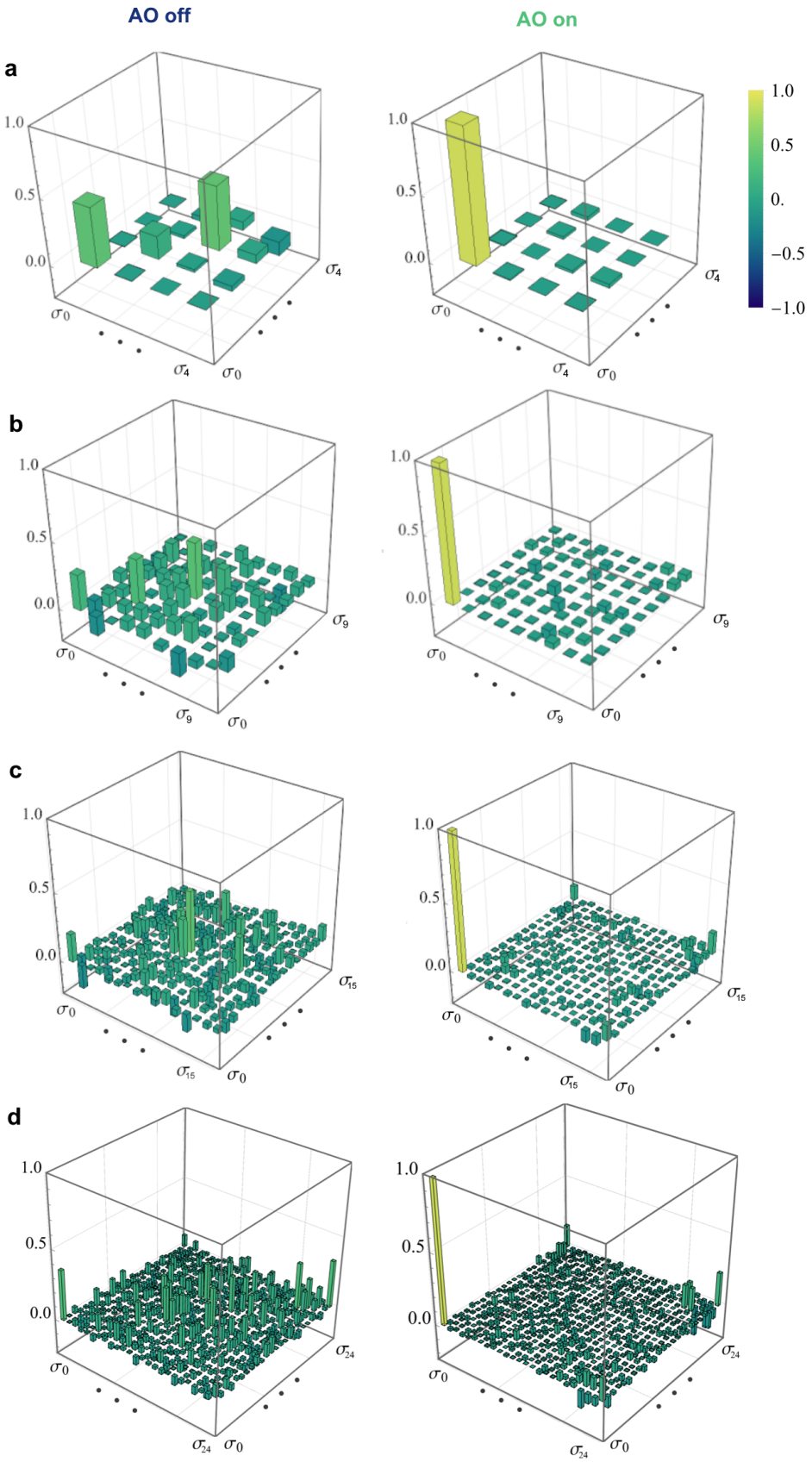


**Figure S4**. Process matrices for all dimensions. **a** $d = 2$, **b** $d = 3$, **c** $d = 4$, **d** $d = 5$

where $s_j = j + \ldots + (p-1)$ and $\omega = e^{2\pi i/p}$. The process tomography is performed by preparing all the elements of the set $\mathcal{S} := \{\mathcal{B}_0, \ldots, \mathcal{B}_p\}$ and performing projective measurements on the same set. Let $\Pi_t^\alpha := \left|\psi_t^\alpha\right\rangle\left\langle\psi_t^\alpha\right|$, the state resulting from the action of the turbulent channel on a basis element is

$$\mathcal{E}(\Pi_t^k) = \sum_{m,n} \chi_{mn}\sigma_m \Pi_t^k \sigma_n^\dagger \tag{S5}$$

where $\sigma_m$ are Gell-Mann matrices. A measurement in any of the MUBs yields the detection probabilities

$$p_{m,n}^{\alpha,\beta} = \mathrm{Tr}(\Pi_m^\alpha \mathcal{E}(\Pi_n^\beta)) = \sum_{a,b} \chi_{ab}\mathrm{Tr}(\Pi_m^\alpha \sigma_a \Pi_n^\beta \sigma_b^\dagger). \tag{S6}$$

Through the steps detailed in Ref. [5] the above equation was inverted to find the process matrix $\chi_{mn}$. The Fidelity between the experimentally reconstructed process matrix $\chi_{exp}$ and a theoretical one $\chi_{th}$ is

$$\mathcal{F} := \mathrm{Tr}\left(\sqrt{\sqrt{\chi_{exp}}\chi_{th}\sqrt{\chi_{exp}}}\right)^2. \tag{S7}$$

In our case $\chi_{th}$ was considered to be the $d$-dimensional identity matrix, corresponding to an ideal channel).

Note that Eq. S4 gives a complete set of MUBs for dimensions which are a prime number. For $d$ equal to the power of a prime, complete sets of MUBs can be still found. For $d = 4$ one has:

$$\begin{aligned}
\mathcal{B}_0 &= \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}\\
\mathcal{B}_1 &= \{(1/2,1/2,1/2,1/2),(1/2,-1/2,-1/2,1/2),(1/2,1/2,-1/2,-1/2),(1/2,-1/2,1/2,-1/2)\}\\
\mathcal{B}_2 &= \{(1/2,i/2,i/2,-1/2),(1/2,-i/2,-i/2,-1/2),(1/2,i/2,-i/2,1/2),(1/2,-i/2,i/2,1/2)\}\\
\mathcal{B}_3 &= \{(1/2,1/2,-i/2,i/2),(1/2,-1/2,i/2,i/2),(1/2,1/2,i/2,-i/2),(1/2,-1/2,-i/2,-i/2)\}\\
\mathcal{B}_4 &= \{(1/2,-i/2,1/2,i/2),(1/2,i/2,-1/2,i/2),(1/2,i/2,1/2,-i/2),(1/2,-i/2,-1/2,-i/2)\}.
\end{aligned} \tag{S8}$$

## S3- CROSSTALK & QDER

### Bases

As mentioned in the manuscript, we utilize the logical basis, corresponding to OAM modes as out first basis. Our second basis consists of a balanced superposition of the OAM modes corresponding to a quantum Fourier transform known as the angular basis (ANG). The modes for both bases in all dimensions are shown in Fig. **S5**. The phase structure in the ANG basis is made up of flat two regions, with sharp jumps between them. The power in the ANG basis consists of $d$ lobes and becomes more concentrated a single lobe in higher dimensions.

This localization effectively constrains the mode to fewer corrective elements of the adaptive optics system as $d$ increases, not allowing for adequate compensation. This same localization of the ANG states likely allows the state to have a smaller effective diameter, $D$, meaning that the experienced turbulence will be lesser as there is a decrease in $D/r_0$. We believe this is what causes the ANG states to be more robust to turbulence without AO, while also not being as easily corrected when using the AO system.

### Crosstalk measurement

For a given basis, the crosstalk matrix is determined through the projective measurement of all states in the basis on the incoming state. After the projective measurement, the light is coupled into a single mode fibre and a power is measured by an optical power meter (Thorlabs PM100D). Each projective measurement $\left|\left\langle\psi_j\middle|\psi_i\right\rangle\right|^2$ is normalized by the total power measured from one incoming state,

$$C_{ij} = \frac{\left|\left\langle\psi_j\middle|\psi_i\right\rangle\right|^2}{\sum_{j=0}^{d-1}\left|\left\langle\psi_j\middle|\psi_i\right\rangle\right|^2}, \tag{S9}$$

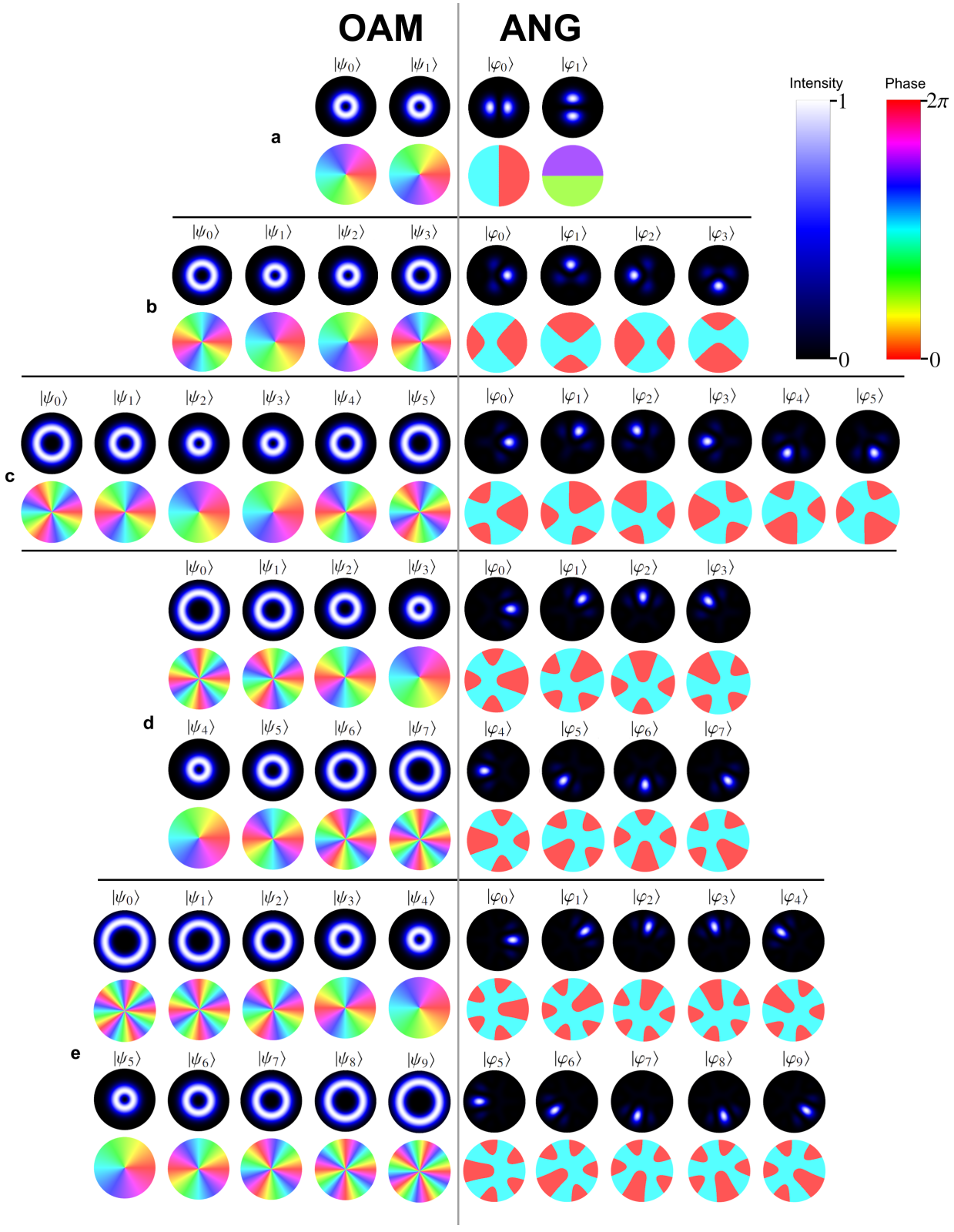


**Figure S5**. All modes utilized in the crosstalk measurements. The logical basis consisting of OAM modes is shown on the left, while the angular basis is shown on the right for the same dimension. **a** $d = 2$, **b** $d = 4$, **c** $d = 6$, **d** $d = 8$, **e** $d = 10$

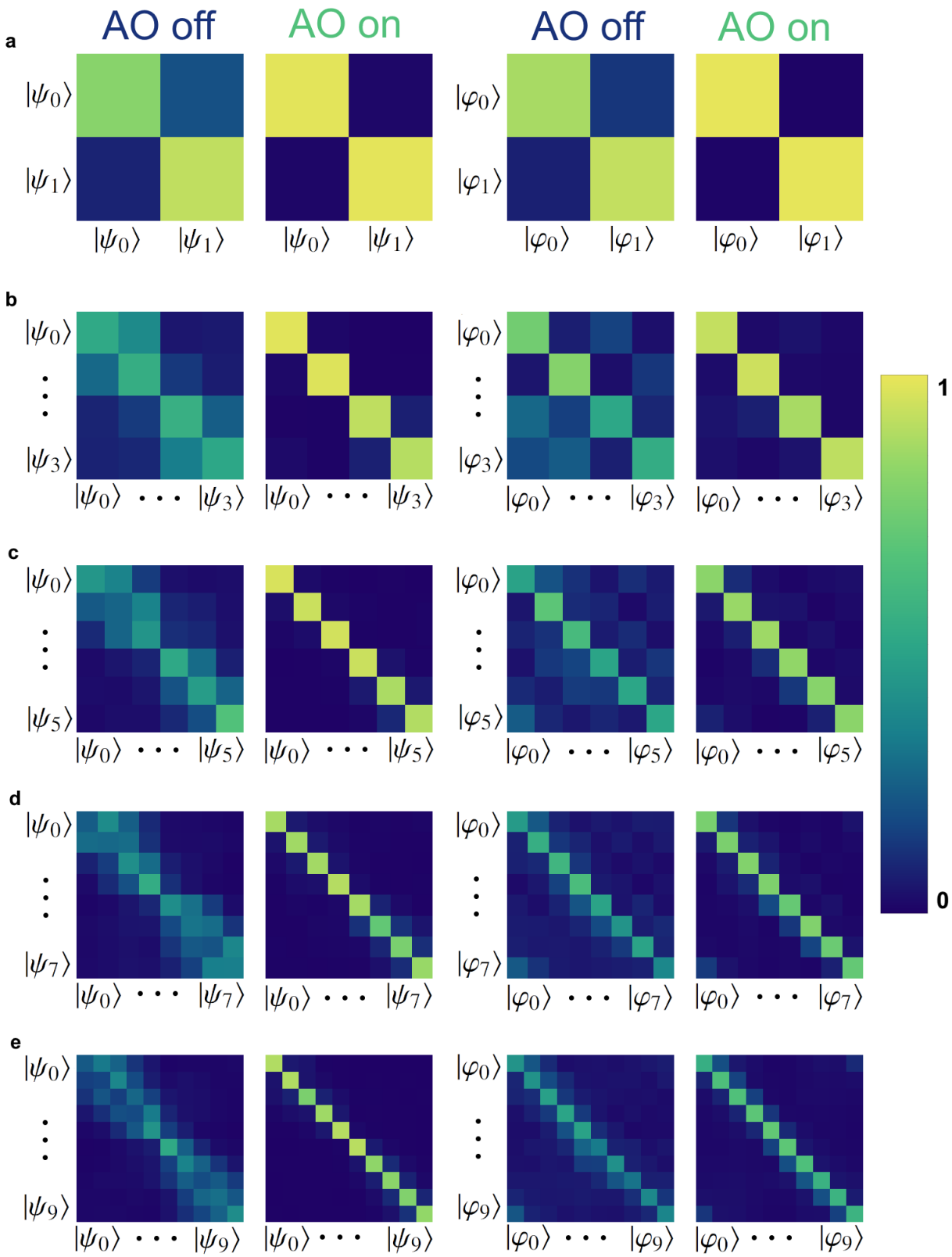


**Figure S6**. Crosstalk matrices for both bases in all dimensions. **a** $d = 2$, **b** $d = 4$, **c** $d = 6$, **d** $d = 8$, **e** $d = 10$

to ensure that the sum of the power measured on an input state (the sum of any row in the matrix) is unitary. This gives the likelihood of detection for any one output state given an input state. These elements are arranged such that Alice's input states are given by the row number, $i$, while Bob's projective measurement state is given by the column number, $j$.

Figure **S6** shows the corresponding crosstalk matrices for all dimensions. We see that the OAM modes are likely to spread to neighboring modes up to the midpoint of the dimension. This shows that the induced turbulence is unlikely to result in power spreading from modes where $\ell > 0$ to modes where $\ell < 0$ and vice-versa.

### QDER calculation

With the crosstalk matrix measurement performed, the average of the diagonal elements is used to determine the fidelity of the basis. To determine the quantum dit error rate, we subtract the fidelity from the theoretical best performance of 1. This gives a QDER for the basis in a dimension d.

$$\text{QDER} = 1 - \sum_{j=i=0}^{d-1} C_{ii}/d = 1 - \frac{1}{d}\,\text{Tr}[C] \tag{S10}$$

We calculate the QDER for each of the bases, in each dimension. We find that our AO system is capable of correcting the effects of turbulence in the logical basis for al dimensions. As mentioned in the manuscript, the QDER in the ANG basis is brought below the threshold for secure communications in all cases, save for $d = 10$. The exact values for the calculated QDER in all cases are listed in Tables S2 and S3.

| Dimension | QDER OAM AO off | QDER OAM AO on | Security Boundary |
|---|---|---|---|
| 2 | 13.6 ± 8.1 | 1.2 ± 0.1 | 11.0 |
| 4 | 47.3 ± 2.3 | 5.4 ± 4.1 | 18.9 |
| 6 | 54.6 ± 13.1 | 7.1 ± 3.4 | 22.5 |
| 8 | 66.9 ± 10.8 | 16.4 ± 6.6 | 24.7 |
| 10 | 71.6 ± 12.9 | 15.1 ± 4.9 | 26.2 |

TABLE S2. Calculated QDER for the logical basis.

| Dimension | QDER ANG AO off | QDER ANG AO on | Security Boundary |
|---|---|---|---|
| 2 | 9.9 ± 3.6 | 0.6 ± 0.2 | 11.0 |
| 4 | 35.5 ± 2.3 | 8.3 ± 2.9 | 18.9 |
| 6 | 45.5 ± 8.6 | 17.2 ± 2.0 | 22.5 |
| 8 | 53.4 ± 5.5 | 24.3 ± 3.3 | 24.7 |
| 10 | 59.7 ± 6.6 | 37.3 ± 6.0 | 26.2 |

TABLE S3. Calculated QDER for the angular basis.

* ekarimi@uottawa.ca

[1] M. Born and E. Wolf, Principles of optics: electromagnetic theory of propagation, interference and diffraction of light (Elsevier, 2013).
[2] ANSI Z80.28-2010, Ophthalmics - Methods Of Reporting Optical Aberrations Of Eyes, Standard (American National Standards Institute, Washington, DC, 2010).
[3] H. Zhan, E. Wijerathna, and D. Voelz, Wave optics simulation studies of the fried parameter for weak to strong atmospheric turbulent fluctuations, in Propagation Through and Characterization of Atmospheric and Oceanic Phenomena (Optica Publishing Group, 2019) pp. PM1C–3.
[4] D. P. Greenwood, Bandwidth specification for adaptive optics systems, *JOSA* **67**, 390 (1977).
[5] A. Fernández-Pérez, A. Klimov, and C. Saavedra, Quantum process reconstruction based on mutually unbiased basis, *Physical Review A* **83**, 052332 (2011).

# Appendix C

# Supplementary material: High-dimensional Encoding in the Round-Robin-Differential-Phase-Shift Protocol

## A Security proof calculation

We present the detailed calculation of the HD-RRDPS protocol based on the procedure introduced in [11]. As mentioned in the main text, Alice prepares a state $|\psi\rangle$ given by

$$|\psi\rangle = \frac{1}{\sqrt{L}} \sum_{j=1}^{L} e^{i\frac{2\pi k_j}{d}} |j\rangle. \tag{10}$$

The strategy adopted by the eavesdropper, *Eve*, is a general collective attack given by the unitary transformation $U_{\text{Eve}}$, where

$$U_{\text{Eve}}|j\rangle|e_{00}\rangle = \sum_{\ell=1}^{L} c_{j\ell}|\ell\rangle|e_{j\ell}\rangle, \tag{11}$$

and $|e_{j\ell}\rangle$ is Eve's ancilla state. Moreover, without loss of generality we assume that $c_{j\ell} \geq 0$ and $\langle e_{im}|e_{jn}\rangle = \delta_{ij}\delta_{mn}$. Upon receiving the signal state, Bob then selects a subset of modes indexed by $\mathcal{J} = \{j_0, j_1, ..., j_{(d-1)}\}$ and performs a measurement in the MUB given by $\{|\varphi_m^{(d)}\rangle\}$, where

$$|\varphi_m^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} e^{i\frac{2\pi mn}{d}} |j_n\rangle. \tag{12}$$

We can now write the evolution of the signal state considering Eve's general collective attack and Bob's measurement, i.e.,

$$\begin{aligned} U_{\text{Eve}}|\psi\rangle|e_{00}\rangle \longrightarrow \quad & \exp\left[i\frac{2\pi k_{j_0}}{d}\right] \sum_{n=0}^{d-1} \tilde{c}_{j_0 j_n}|j_n\rangle + \exp\left[i\frac{2\pi k_{j_1}}{d}\right] \sum_{n=0}^{d-1} \tilde{c}_{j_1 j_n}|j_n\rangle + ... \\ + \quad & \exp\left[i\frac{2\pi k_{j_{(d-1)}}}{d}\right] \sum_{n=0}^{d-1} \tilde{c}_{j_{(d-1)} j_n}|j_n\rangle + \sum_{\ell \notin \mathcal{J}} \exp\left[i\frac{2\pi k_\ell}{d}\right] \sum_{n=0}^{d-1} \tilde{c}_{\ell j_n}|j_n\rangle, \end{aligned} \tag{13}$$

where we have defined $\tilde{c}_{ij} = c_{ij}|e_{ij}\rangle$. Eve's non-normalized reduced density matrix is then given by

$$\rho_{\text{E}} = \sum_{n=0}^{d-1} P\{\sum_{\ell=1}^{L} \exp\left[i\frac{2\pi k_\ell}{d}\right] \tilde{c}_{\ell j_n}\}, \tag{14}$$

where we have defined $P\{|x\rangle\} = |x\rangle\langle x|$. Eve does not have any knowledge about the phases $\exp(2\pi ik\ell/d)$ for $|\ell\rangle$ not in Bob's MUB, so averaging over all of those possible phases is equivalent to randomizing the phase of the terms $|e_{\ell j_n}\rangle$ for $\ell \notin \mathcal{J}$, i.e.,

$$\rho_{\text{E}} = \sum_{n=0}^{d-1} P\{\sum_{p=0}^{d-1} \exp\left[i\frac{2\pi k_{j_p}}{d}\right] \tilde{c}_{j_p j_n}\} + \sum_{n=0}^{d-1} \sum_{\ell \notin \mathcal{J}} c_{\ell j_n}^2 P\{|e_{\ell j_n}\rangle\}. \tag{15}$$

In the event of Alice preparing a state $|\psi\rangle$, where we have a phase modulation with $k_{j_n} = mn$, for $n \in \{0, 1, ..., (d-1)\}$, Eve's ancilla states are given by

$$\rho_m^{(\mathcal{J})} = \sum_{n=0}^{d-1} P\{\sum_{p=0}^{d-1} \exp\left[i\frac{2\pi mp}{d}\right] \tilde{c}_{j_p j_n}\} + \sum_{n=0}^{d-1}\sum_{\ell\notin\mathcal{J}} c_{\ell j_n}^2 P\{|e_{\ell j_n}\rangle\}. \tag{16}$$

The mutual information between Alice and Eve is then estimated using the Holevo bound,

$$\begin{aligned} Q^{(\mathcal{J})} I_{\mathrm{AE}}^{(\mathcal{J})} \leq \quad & S\left(\frac{1}{d}\sum_{m=0}^{d-1}\rho_m^{(\mathcal{J})}\right) - \frac{1}{d}\sum_{m=0}^{d-1} S\left(\rho_m^{(\mathcal{J})}\right) \\ = \quad & \sum_{m=0}^{d-1} \zeta^{(d)}\left(c_{j_0 j_m}^2, c_{j_1 j_m}^2, ..., c_{j_{(d-1)} j_m}^2\right), \end{aligned} \tag{17}$$

where $S$ is the von Neumann entropy, we have defined $\zeta^{(d)}(x_0^2, x_1^2, ..., x_{(d-1)}^2) = -\sum_{i=0}^{d-1} x_i^2 \log_2 x_i^2 + \left(\sum_{i=0}^{d-1} x_i^2\right)\log_2\left(\sum_{i=0}^{d-1} x_i^2\right)$, and $Q^{(\mathcal{J})} = \sum_{\ell=1}^{L}\sum_{n=0}^{d-1} c_{\ell j_n}^2$ is the yield of Bob projecting the signal state in the subset indexed by $\mathcal{J}$ and takes care of the normalization constants for Eve's reduced density matrix. Finally, Eve's information on the raw key is given by,

$$I_{\mathrm{AE}} = \frac{\sum_{j_0<j_1<...<j_{(d-1)}} Q^{(\mathcal{J})} I_{\mathrm{AE}}^{(\mathcal{J})}}{\sum_{j_0<j_1<...<j_{(d-1)}} Q^{(\mathcal{J})}} \leq \frac{\sum_{j_0<j_1<...<j_{(d-1)}}\sum_{m=0}^{d-1}\zeta^{(d)}\left(c_{j_0 j_m}^2, c_{j_1 j_m}^2, ..., c_{j_{(d-1)} j_m}^2\right)}{\binom{L-1}{d-1}\sum_{i=1}^{L}\sum_{j=1}^{L} c_{ij}^2}, \tag{18}$$

where $\binom{L-1}{d-1} = \frac{(L-1)!}{(d-1)!(L-d)!}$ is a binomial coefficient. We note that $\zeta^{(d)}(x_0^2, x_1^2, ..., x_{(d-1)}^2)$ is a concave function and we can thus use Jensen's inequality and that $\zeta^{(d)}(a\mathbf{x}) = a\zeta^{(d)}(\mathbf{x})$ to simplify further Eve's information by counting all of the terms where each coefficient $c_{ij}^2$ appears,

$$I_{\mathrm{AE}} \leq \frac{\zeta^{(d)}\left(\binom{L-1}{d-1}x_1, \binom{L-2}{d-2}x_2, ..., \binom{L-2}{d-2}x_2\right)}{\binom{L-1}{d-1}(x_1+x_2)}, \tag{19}$$

where we have defined $x_1 = \sum_i c_{ii}^2$ and $x_2 = \sum_{i\neq j} c_{ij}^2$. We note that $x_1$ and $x_2$ are non-negative parameters satisfying $x_1 + x_2 = 1$ once appropriate normalization is reinstated. We can now relate the parameters $x_1$ and $x_2$ to the error rate.

We now try to further tightly bound the mutual information $I_{\mathrm{AE}}$ by finding a relationship between the error rate $E$ and the non-negative parameters $x_1$ and $x_2$. Bob's probability of measuring anything other than the $m$th state after Eve's measurement is,

$$p_m^{(\mathcal{J})} = \sum_{p\neq m}\left|\langle\varphi_p|\left(\sum_{r=0}^{d-1}\exp\left[i\frac{2\pi mr}{d}\right]\sum_{n=0}^{d-1}\tilde{c}_{j_r j_n}|j_n\rangle + \sum_{\ell\notin\mathcal{J}}\exp\left[i\frac{2\pi m\ell}{d}\right]\sum_{n=0}^{d-1}\tilde{c}_{\ell j_n}|j_n\rangle\right)\right|^2, \tag{20}$$

$$p_m^{(\mathcal{J})} = \frac{1}{d}\sum_{p\neq m}\left(\left|\sum_{n=0}^{d-1}\sum_{r=0}^{d-1}\exp\left[i\frac{2\pi(mr-pn)}{d}\right]\tilde{c}_{j_r j_n}\right|^2 + \sum_{\ell\notin\mathcal{J}}\left|\sum_{n=0}^{d-1}\exp\left[i\frac{2\pi(m\ell-pn)}{d}\right]\tilde{c}_{\ell j_n}\right|^2\right), \tag{21}$$

$$p_m^{(\mathcal{J})} = \frac{d-1}{d}\left(\sum_{n=0}^{d-1}\sum_{r=0}^{d-1} c_{j_r j_n}^2 + \sum_{\ell\notin\mathcal{J}}\sum_{n=0}^{d-1} c_{\ell j_n}^2\right). \tag{22}$$

The error rate $E^{(\mathcal{J})}$ is then given by,

$$E^{(\mathcal{J})} = \frac{1}{Q^{(\mathcal{J})}} \frac{1}{d} \sum_{m=0}^{d-1} p_m^{(\mathcal{J})}, \tag{23}$$

$$E^{(\mathcal{J})} = \frac{(d-1)}{d} \frac{\left( \sum_{n=0}^{d-1} \sum_{r=0}^{d-1} c_{j_r j_n}^2 + \sum_{\ell \notin \mathcal{J}} \sum_{n=0}^{d-1} c_{\ell j_n}^2 \right)}{\sum_{\ell=1}^{L} \sum_{n=0}^{d-1} c_{\ell j_n}^2}, \tag{24}$$

The overall error is then given by,

$$E = \frac{\sum_{j_0<j_1<\ldots<j_{(d-1)}} Q^{(\mathcal{J})} E^{(\mathcal{J})}}{\sum_{j_0<j_1<\ldots<j_{(d-1)}} Q^{(\mathcal{J})}}, \tag{25}$$

$$E = \frac{(d-1)}{d} \frac{\sum_{j_0<j_1<\ldots<j_{(d-1)}} \left( \sum_{n=0}^{d-1} \sum_{r=0}^{d-1} c_{j_r j_n}^2 + \sum_{\ell \notin \mathcal{J}} \sum_{n=0}^{d-1} c_{\ell j_n}^2 \right)}{\sum_{j_0<j_1<\ldots<j_{(d-1)}} \sum_{\ell=1}^{L} \sum_{n=0}^{d-1} c_{\ell j_n}^2}, \tag{26}$$

$$E = \frac{(d-1)}{d} \left( \frac{\binom{L-1}{d-1} \sum_{i=1}^{L} c_{ii}^2 + \binom{L-2}{d-2} \sum_{i \neq j}^{L} c_{ij}^2 + \binom{L-2}{d-1} \sum_{i \neq j} c_{ij}^2}{\binom{L-1}{d-1} \sum_{i=1}^{L} \sum_{j=1}^{L} c_{ij}^2} \right) \geq (d-1) \left( \frac{\binom{L-2}{d-1} \sum_{i \neq j} c_{ij}^2}{\binom{L-1}{d-1} \sum_{i=1}^{L} \sum_{j=1}^{L} c_{ij}^2} \right), \tag{27}$$

$$E \geq \frac{(d-1)}{d} \left( \frac{\binom{L-2}{d-1} x_2}{\binom{L-1}{d-1} (x_1 + x_2)} \right), \tag{28}$$

$$E \geq \frac{(d-1)}{d} \left( \frac{L-d}{L-1} \right) \left( \frac{x_2}{x_1 + x_2} \right). \tag{29}$$

We note that for the case of $d = 2$, we recover the results from [11].

# References


[1] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[2] Paul Adrien Maurice Dirac. A new notation for quantum mechanics. In *Mathematical proceedings of the Cambridge philosophical society*, volume 35, pages 416–418. Cambridge University Press, 1939.

[3] Dilip Paneru, Eliahu Cohen, Robert Fickler, Robert W Boyd, and Ebrahim Karimi. Entanglement: quantum or classical? *Reports on Progress in Physics*, 83(6):064001, 2020.

[4] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[5] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[6] Jonathan P Dowling and Gerard J Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.

[7] Ivan H Deutsch. Harnessing the power of the second quantum revolution. *PRX Quantum*, 1(2):020101, 2020.

[8] Gregorius CG Berkhout, Martin PJ Lavery, Johannes Courtial, Marco W Beijersbergen, and Miles J Padgett. Efficient sorting of orbital angular momentum states of light. *Physical review letters*, 105(15):153601, 2010.

[9] Guillaume Labroille, Bertrand Denolle, Pu Jian, Philippe Genevaux, Nicolas Treps, and Jean-François Morizur. Efficient and mode selective spatial mode multiplexer based on multi-plane light conversion. *Optics express*, 22(13):15599–15607, 2014.

[10] Hlib Kupianskyi, Simon AR Horsley, and David B Phillips. High-dimensional spatial mode sorting and optical circuit design using multi-plane light conversion. *APL Photonics*, 8(2), 2023.

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

[12] Lorenzo Marrucci, C Manzo, and D Paparo. Pancharatnam-berry phase optical elements for wave front shaping in the visible domain: switchable helical mode generation. *Applied Physics Letters*, 88(22), 2006.

[13] Lorenzo Marrucci, Ebrahim Karimi, Sergei Slussarenko, Bruno Piccirillo, Enrico Santamato, Eleonora Nagali, and Fabio Sciarrino. Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications. *Journal of Optics*, 13(6):064001, 2011.

[14] Ze'ev Bomzon, Vladimir Kleiner, and Erez Hasman. Pancharatnam–berry phase in space-variant polarization-state manipulations with subwavelength gratings. *Optics letters*, 26(18):1424–1426, 2001.

[15] F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, and E. Karimi. Investigation of underwater quantum channel in a 30-meter flume tank using structured photons. *New Journal of Physics*, 22:093074, 2020.

[16] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günther, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and Karimi E. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006, 2017.

[17] Shawn Sederberg, Fanqi Kong, Felix Hufnagel, Chunmei Zhang, Ebrahim Karimi, and Paul B Corkum. Vectorized optoelectronic control and metrology in a semiconductor. *Nature Photonics*, 14(11):680–685, 2020.

[18] S. W. Hell and J. Wichmann. Breaking the diffraction resolution limit by stimulated emission: stimulated-depletion fluorescence microscopy. *Optics Letters*, 19(11):708–782, 1994.

[19] Miles Padgett and Richard Bowman. Tweezers with a twist. *Nature photonics*, 5(6):343–348, 2011.

[20] Gary S Waldman. Variations on the fresnel zone plate. *JOSA*, 56(2):215–218, 1966.

[21] Ora E Myers. Studies of transmission zone plates. *American Journal of Physics*, 19(6):359–365, 1951.

[22] Max Born and Emil Wolf. *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light*. Elsevier, 2013.

[23] Igor Aharonovich, Dirk Englund, and Milos Toth. Solid-state single-photon emitters. *Nature photonics*, 10(10):631–641, 2016.

[24] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical review letters*, 59(18):2044, 1987.

[25] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[26] Paul G Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, 75(24):4337, 1995.

[27] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. Quantum cryptography with entangled photons. *Physical review letters*, 84(20):4729, 2000.

[28] Christophe Couteau. Spontaneous parametric down-conversion. *Contemporary Physics*, 59(3):291–304, 2018.

[29] Paul G Kwiat, Edo Waks, Andrew G White, Ian Appelbaum, and Philippe H Eberhard. Ultrabright source of polarization-entangled photons. *Physical Review A*, 60(2):R773, 1999.

[30] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, 175:8, 1984.

[31] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[32] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[33] James L Park. The concept of transition in quantum mechanics. *Foundations of physics*, 1(1):23–33, 1970.

[34] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of modern physics*, 92(2):025002, 2020.

[35] Hoi-Kwong Lo and Hoi Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *science*, 283(5410):2050–2056, 1999.

[36] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[37] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 91(5):057901, 2003.

[38] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[39] Helle Bechmann-Pasquinucci and Wolfgang Tittel. Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.

[40] Nicolas J Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical review letters*, 88(12):127902, 2002.

[41] Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475–478, 2014.

[42] Yeong Cherng Liang, Dagomir Kaszlikowski, Berthold-Georg Englert, Leong Chuan Kwek, and Choo Hiap Oh. Tomographic quantum cryptography. *Physical Review A*, 68(2):022324, 2003.

[43] HF Chau. Quantum key distribution using qudits that each encode one bit of raw key. *Physical Review A*, 92(6):062324, 2015.

[44] Frédéric Bouchard, Felix Hufnagel, Dominik Koutnỳ, Aazad Abbas, Alicia Sit, Khabat Heshami, Robert Fickler, and Ebrahim Karimi. Quantum process tomography of a high-dimensional quantum communication channel. *Quantum*, 3:138, 2019.

[45] Jaroslav Řeháček, Berthold-Georg Englert, and Dagomir Kaszlikowski. Minimal qubit tomography. *Physical Review A*, 70(5):052321, 2004.

[46] ZED Medendorp, FA Torres-Ruiz, LK Shalm, GNM Tabia, CA Fuchs, and AM Steinberg. Experimental characterization of qutrits using symmetric informationally complete positive operator-valued measurements. *Physical Review A*, 83(5):051801, 2011.

[47] Horace W Babcock. The possibility of compensating astronomical seeing. *Publications of the Astronomical Society of the Pacific*, 65(386):229–236, 1953.

[48] Claire Max. Introduction to adaptive optics and its history. In *American Astronomical Society 197th Meeting*. NSF Center for Adaptive Optics University of California at Santa Cruz and ..., 2001.