Towards the real-world implementation of high dimensional quantum key distribution in free-space

Lukas Scarfe

Thesis submitted in partial fulfillment of the requirements
For the Master of Science degree in Physics

Ottawa-Carleton Institute of Physics
Department of Physics
Faculty of Science
University of Ottawa
Ottawa, Canada

Abstract

This thesis consists of multiple projects that work towards the realistic implementation of real-world high-dimensional quantum key distribution protocols within the confines of Earth's atmosphere. First, we investigate the behaviour of the atmosphere of a 5.4 km free-space channel over the city of Ottawa, Ontario, Canada. This data was collected over a period of 9 months, and is ongoing as of the writing of this thesis. Using the data collected, we have created an AI-based approach to predict atmospheric conditions up to 12 hours in advance. We then performed a simulated quantum communication protocol under different atmospheric conditions to predict the performance of such a protocol. This AI tool will be capable of providing performance forecasts of future quantum networks. Next, we investigate the implementation of an adaptive optics system into a laboratory-scale quantum communications channel with turbulence. We investigated the effects of the turbulence on the transmission of the optical modes through the channel as well as the restorative effects of the adaptive optics system. These results are placed in the context of the theoretical performance of a quantum key distribution system, showing that the implementation of adaptive optics allows for quantum communications where it was otherwise impossible. These two works pave the way for future quantum networks operating under atmospheric conditions. We have shown that it is possible to confidently provide predictions of the quality of a quantum channel. However, in the future, this could be applied to a quantum network with many nodes and channels, potentially allowing for optimization of the network according to future weather conditions. The same network would additionally benefit from the implementation of adaptive optics, allowing for quantum communications when it would otherwise render the network ineffective.

Acknowledgements

I would like to thank my supervisor, Dr. Ebrahim Karimi, for his unwavering support and encouragement. He has contributed immensely to my learning over the past two years of my Master's degree, of course in a scientific sense but also inter-personal and personal skills. Without his support, I would not have been able to complete any of this work and I feel privileged to have been under his guidance and learned so much from him.

I would also like to thank all the members of the SQO group who form an amazing community. Some in particular include: Manuel F. Ferrer-Garcia and Felix Hufnagel, both of whom taught me very much about working in the lab and doing experiments, additionally both taught me very important lessons about writing science. Without the two of you, I would just be an engineer, but I am glad to be a physicist. Also, Francesco Di Colandrea and Tareq Jaouni, I had an amazing time working with you. Every meeting that we had really felt just like hanging out. Thanks to many more people in the SQO group as well, I would never have finished my work without our regular coffee breaks. I am glad to have made such great friends in this community. Beyond the SQO group, I feel fortunate to have such wonderful collaborators, all of whom have contributed greatly to my learning and research.

Some of the most important thanks go out to my family: Mom and Dad, you have encouraged me to pursue science and are the reason that I am where I am. The pair of you are my role models in all walks of life. I feel that I am the most fortunate person in the world to have been raised by you. Sam, Nick, Mathilde, Molly, Louis, Anna, our familial bond is amazing, but I know that I am more lucky to have you all as my friends. You guys are my absolute rocks and I know that no matter what happens you are on my team.

Finally, my eternal appreciation goes to Michelle. You have comforted me when things were not going so well, and celebrated with me when things went well. Without you I know that none of this would have been possible. You are my sun and moon and stars.

List of Publications

1. Jaouni, Tareq*, **Lukas Scarfe***, Frédéric Bouchard, Mario Krenn, Khabat Heshami, Francesco Di Colandrea, and Ebrahim Karimi. "Predicting atmospheric turbulence for secure quantum communications in free space." arXiv preprint arXiv:2406.14768 (2024).

2. **Scarfe, Lukas**, Felix Hufnagel, Manuel F. Ferrer-Garcia, Alessio D'Errico, Khabat Heshami, and Ebrahim Karimi. "Fast Adaptive Optics for High-Dimensional Quantum Communications in Turbulent Channels." arXiv preprint arXiv:2311.13041 (2023).

3. Wybo, Christopher, David S. Nay, Darren P. Scarfe, **Lukas T. Scarfe**, and Samantha J. O'neil. "Intraoperative neural monitoring system utilizing wavelet-based event detection." U.S. Patent 11,980,474, issued May 14, 2024.

4. Wybo, Christopher, David S. Nay, Darren P. Scarfe, **Lukas T. Scarfe**, Samantha J. O'neil, and Gary Gordon. "Intraoperative neural monitoring method." U.S. Patent 11,980,476, issued May 14, 2024.

5. Wybo, Christopher, David S. Nay, Darren P. Scarfe, **Lukas T. Scarfe**, and Samantha J. O'neil. "Intraoperative neural monitoring method utilizing wavelet-based event detection." U.S. Patent 11,850,057, issued December 26, 2023.

6. Wybo, Christopher, David S. Nay, Darren P. Scarfe, **Lukas T. Scarfe**, and Samantha J. O'neil. "Intraoperative neural monitoring method with statistical confidence determination." U.S. Patent 11,850,040, issued December 26, 2023.

7. Alzate-Carvajal, Natalia, Jaewoo Park, Ilhem Bargaoui, Ranjana Rautela, Zachary J. Comeau, **Lukas Scarfe**, Jean-Michel Ménard, Seth B. Darling, Benoît H. Lessard, and Adina Luican-Mayer. "Arrays of functionalized graphene chemiresistors for selective sensing of volatile organic compounds." ACS Applied Electronic Materials 5, no. 3 (2023): 1514-1520.

*These authors contributed equally to this work.

Statement of Originality and List of Contributions

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

Francesco Di Colandrea, Lukas Scarfe and Ebrahim Karimi conceived the idea. Lukas Scarfe collected and prepared the scintillometer and weather data. Tareq Jaouni developed the neural network architectures. Francesco Di Colandrea performed numerical simulations of QKD under turbulence. Tareq Jaouni, Lukas Scarfe, and Francesco Di Colandrea wrote the first version of the manuscript. Frédéric Bouchard, Mario Krenn, Khabat Heshami, and Ebrahim Karimi supervised the project. All authors discussed the results and contributed to the text of the manuscript.

Ebrahim Karimi conceived of the project. Lukas Scarfe, Felix Hufnagel, Manuel F. Ferrer-Garcia, Alessio D'Errico, and Ebrahim Karimi designed the experiments; Lukas Scarfe and Felix Hufnagel performed the experiments and collected the data; Lukas Scarfe, Felix Hufnagel, and Manuel F. Ferrer-Garcia analysed the data and wrote the first version of the manuscript. Khabat Heshami and Ebrahim Karimi supervised the project. All authors discussed the results and contributed to the text of the manuscript.

Table of contents

List of Figures

List of Tables

1

Introduction

1.1 Overview

Effective and detailed communication is one of the most important capabilities of human beings, being one of the main characteristics separating us from other species. Throughout history, we have developed more and more advanced methods of communication; complex speech, writing, printing, radio, television, and most recently the Internet of Things. Each of these technological advancements changed the way humans relate to one another. Speech allowed us to form complex relationships with each other, writing allowed complex societies to organize among people who did not know each other, the printing press and radio allowed mass dissemination of information to the public, and finally the Internet has made it possible for nearly any pair of humans on Earth to communicate one-on-one with each other instantaneously.

However, not all communications are designed to be made public, and efforts to encrypt messages have been around almost as long as writing itself [1]. Since ancient times, people have used different approaches to make a message secure. For example, the Romans used a tool, named *scytale*, to securely encrypt messages. The scytale consisted of a cylindrical rod around which a strip of parchment or leather was wound. The sender would write the message

Figure 1: Example of an ancient scytale: The scytale is an early encryption tool used by parties who possessed identical cylinders of the same radius. To encrypt a message, a strip of parchment was wrapped around the cylinder, and the message was written along the length of the cylinder. The strip was then unwrapped and sent to the recipient, who could decrypt the message by rewrapping it around a cylinder with the same radius, revealing the hidden text. © CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1698345

on the strip while it was wrapped around the rod. When unwrapped, the text appeared as an unreadable sequence of letters. The recipient, who had a rod of the same diameter, could decode the message by wrapping the strip around the rod, revealing the original text. An alternative and widely used approach is to switch letters in the alphabet to protect your messages from being read by the unintended receiver; this is known as the shift or Caesar cypher. Both examples require the receiver and sender of the message to agree on the encryption and decryption method prior to share the message.

With modern mathematical techniques and the sheer computational power available today, cyphers are no longer secure. Most encryption in the modern era is performed using a public-key technique commonly called the RSA (Rivest-Shamir-Adleman) protocol [2]. This encryption technique takes advantage of the fact that there is no known algorithm for efficiently factoring large numbers using classical computers [3]. By choosing a public and private key that is made up of prime numbers of sufficient length, the users can guarantee that a guess and check attack will, on average, take a sufficiently long time to decrypt the message.

RSA is the backbone of modern Internet infrastructure, but it has a major flaw; the difficulty

of factoring large numbers will soon be a problem of the past. Although practical quantum computers are not yet ready, the theory supporting them is quite mature. A simple method to efficiently factor numbers using Shor's algorithm on a quantum computer is well known [4]. The only way to guarantee absolute security is to encrypt communication with a one-time pad consisting of completely random bits [5]. The issue is then how to distribute this one-time pad without unwanted eavesdroppers getting a hold of it.

Quantum Key Distribution (QKD) is one possible solution for the sharing of secret keys, allowing two parties, namely *Alice* and *Bob*, to generate a shared key that they know with certainty has not been leaked to external parties. QKD, or what the authors referred to as Quantum Key Establishment, was introduced in 1984 by Charles Bennett and Gilles Brassard [6], where they outline the basics of how to use single-photons with information encoded in polarization to share a one-time pad. This protocol was aptly named BB84 after the originators. In 1992 came the first experimental demonstrations performed by Bennet and Brassard, generating a key of length 1379 bits over a 32.5 cm channel in 10 minutes [7]. Between these two events, in 1991, Artur Ekert published a protocol very similar to that of BB84, but utilizing the entanglement of photons and proving the security based on Bell's inequalities [8].

Since these events in the 80 s and 90 s, monumental theoretical developments have come to pass in the field of quantum cryptography. While initially, the security of QKD was only shown for infinite key length, which is not physically meaningful, a proof was given showing that the technique is secure even in the finite-key regime [9]. The introduction of device-independent QKD showed that one did not require a perfect source for guaranteed security [10]. Twin-field QKD pushed the limits of how long a quantum-secure channel can be. Research began utilizing different photonic degrees of freedom than polarization for encoding [11]. The application of decoy states showed that security can be achieved with weak coherent pulses, reducing the difficult burden of requiring an efficient true quantum source [12]. Specifically for this thesis, the development of a high-dimensional protocol showed the benefits of higher information density and greater error tolerance within the quantum channel [13, 14]. To obtain the benefits of high-dimensional QKD, one is required to use degrees of freedom other than polarization since polarization is only bidimensional. Optical orbital angular momentum, frequency, or time-bin provide unbounded mathematical (Hilbert) spaces, and thus would be excellent candidates, though each has their own benefits and drawbacks.

Along with theory, much development has occurred experimentally since the inception of the field of quantum cryptography. Up to today, QKD has been performed at a distance of 1000 km [15] (with a low key rate), with key rates up to 100 MB/s (at a distance of only 10

km in fibre) [16]. High-dimensional QKD systems have been investigated in both fiber and the atmosphere using many degrees of freedom [17, 18, 19, 20]. QKD with a key rate on the order of kb/s has even been performed between a ground station and a satellite [21]. In the last decade, technology has even begun to be commercialized by companies such as ID Quantique, Luxquanta, and Toshiba.

While QKD in a static environment, such as through fibre, is functional for links that may be connected once and will never be disconnected, there remain situations where fibre-based links are not feasible or do not make sense [22]. Examples are earth-satellite links, moving vehicles, or any temporary operating location where infrastructure cannot be put in place. In all of these cases, the implementation of QKD will require that the signal must pass through the Earth's atmosphere, making the channel "free-space". This term is in quotations, because a truly free-space channel would be through a vacuum. Henceforth, while not exact, the term "free-space" shall be used without quotations in reference to an optical channel that is in the atmosphere.

The atmosphere may seem like a great place to perform long-range optical experiments, after all we use our eyes to detect objects at a distance without problem every day. While this is true, it is not the whole story. If one looks up at the night sky, it is clear that the stars are twinkling, and this is not because of intensity fluctuations from the star. Looking at the road on a hot summer day, it is possible to see the reflection of the sky, but this is not because of a puddle on the road. These common effects are due to gradients in the refractive index of the air along the path that the light is taking. Just as the path of light bends when traveling between two media with different refractive indices, so will it bend when travelling along a path with changing refractive index. This free-space phenomenon, called atmospheric turbulence, is the result of gradients in temperature, humidity, wind speed, and other meteorological parameters [23]. More than changing the direction of light travelling through it, atmospheric turbulence will introduce spatially varying phase shifts into a propagating beam. The mode of light as sent will not be the one measured at the receiver, it will be the product of the original mode, along with the phase volume in the turbulent channel, and the propagation of the beam. This may limit the capacity to detect the incoming light, as the detection schemes are often dependent on the mode of the incoming light, such as single-mode fibres only allowing for the coupling Gaussian beams. If one is attempting to use the phase of the light to encode information, atmospheric turbulence can become an even greater problem, as the information will become distorted or even destroyed along propagation through the channel [24].

This thesis will go over works performed to implement quantum key distribution with high-

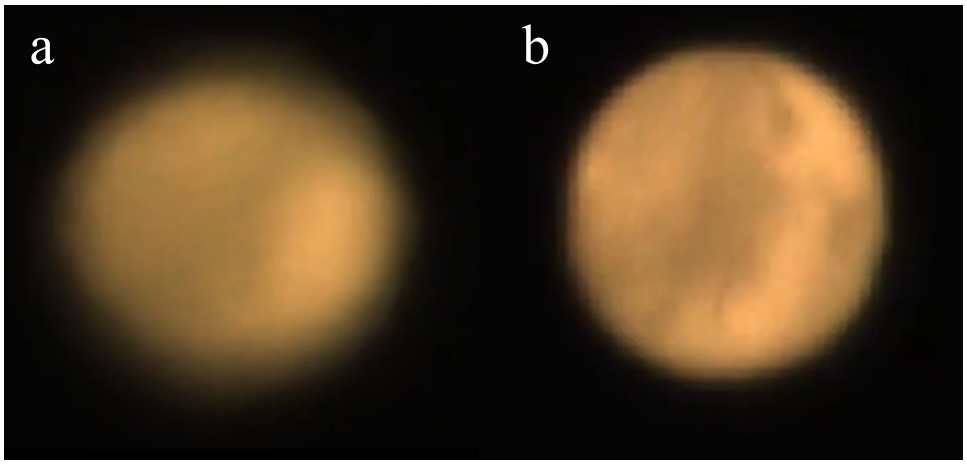

Figure 2: The planet Mars in varying turbulence conditions: Here, Mars is shown on subsequent evenings through a telescope. The difference in image quality here is due to the different turbulence strengths on these nights, with the evening of image a) having relatively high turbulence, and the evening of image b) being a relatively calm evening of turbulence. Photos acquired from the YouTube channel "AstronomyLive".

dimensional encoding in realistic free-space environments where turbulence is a factor. The goal is to develop techniques and implement technologies that have so far not been considered to enable quantum key distribution under conditions where it would otherwise be prohibited.

1.2 Light & its Degrees of Freedom

1.2.1 "And God said"

1 In the beginning God created the heaven and the earth.
2 And the earth was without form, and void; and darkness was upon the face of the deep. And the Spirit of God moved upon the face of the waters.
3 And God said,

$$\nabla \times \boldsymbol{E} = -\frac{\partial \boldsymbol{B}}{\partial t} \tag{1a}$$

$$\nabla \cdot \boldsymbol{D} = \rho_v \tag{1b}$$

$$\nabla \times \boldsymbol{H} = \frac{\partial \boldsymbol{D}}{\partial t} + \boldsymbol{J} \tag{1c}$$

$$\nabla \cdot \boldsymbol{B} = 0 \tag{1d}$$

: and there was light. Here, $\boldsymbol{D} = \varepsilon \boldsymbol{E}$ and $\boldsymbol{H} = \boldsymbol{B}/\mu$ are the displacement and magnetic fields, respectively, in a linear medium. $\boldsymbol{E}$ is the electric field, $\boldsymbol{B}$ is the magnetic field, ρ_v is the density of electric charge and $\boldsymbol{J}$ is the current density, ε and μ are the permittivity and permeability of the material, respectively.

Equations (1) are Maxwell's equations, which govern the behavior of both electric and magnetic fields. It is clear to see that these fields are intrinsically linked. Assuming there is no charge density, $\rho_v = 0$, and no current density, $\boldsymbol{J} = 0$, utilizing the equations (1a) and (1c), one will arrive at the following result for electric and magnetic fields in vacuum.

$$\nabla^2 \boldsymbol{E} - \mu_0 \varepsilon_0 \frac{\partial^2 \boldsymbol{E}}{\partial t^2} = 0, \tag{2}$$

$$\nabla^2 \boldsymbol{B} - \mu_0 \varepsilon_0 \frac{\partial^2 \boldsymbol{B}}{\partial t^2} = 0. \tag{3}$$

These wave equations indicate that electromagnetic waves are seen to propagate in vacuum with a speed of $c = 1/\sqrt{\mu_0 \varepsilon_0}$. These electromagnetic waves are most commonly experienced by humans as light, i.e. at the visible domain. Light and electromagnetic waves, in general, allow us to do more than see. They allow us to communicate and control objects remotely at a rapid speed over long distances thanks to radio and the Internet of Things. Using different properties of light, such as its intensity, frequency, and polarization, we have been able to pack more and more bits of information into our communications. Most recently, its quantum nature has begun to be exploited, but unlike the others, we now seek to utilize this property to increase the security of our communications.

1.2.2 Polarization

For a plane wave, an electromagnetic wave propagating along the direction z, both the electric and magnetic fields oscillate in the xy plane, orthogonal to the propagation direction. Thus, two vectors are needed to determine the electric and magnetic fields in the xy plane. Traditionally speaking, the vector that determines the tip of the electric field is known as the polarization of the electromagnetic wave. As we discussed above, the polarization can take only two values; commonly used horizontal ($|H\rangle$) or vertical ($|V\rangle$) polarization states, when the orientation of the electric field is aligned with the x or y axis, respectively. These two polarizations correspond to orthogonal modes, meaning that with a perfectly coherent beam both modes can be occupied separately and do not overlap. Here, we used the Dirac bra-ket notation to describe the bidimensional polarization states, and since they are independent, we get the following:

$$|\langle H|V\rangle|^2 = 0. \tag{4}$$

These orthogonal polarization modes span a 2-dimensional vector space, with these two states forming a qubit of information that can be encoded within the polarization of a single photon. Keeping with the properties of qubits, the photon need not be restricted to only vertical or horizontal polarization, but may exist in a state that is a linear superposition of the two with an arbitrary relative phase. In general, an arbitrary polarization state can be written as such:

$$|\Psi\rangle = \alpha\,|H\rangle + \beta e^{i\phi}\,|V\rangle = \begin{pmatrix} \alpha \\ \beta e^{i\phi} \end{pmatrix}, \tag{5}$$

where $|\alpha|^2 + |\beta|^2 = 1$. Special named cases arise when $\alpha = \beta$, and $\phi \in \{0, \pi/4, \pi/2, 3\pi/2\}$. These are diagonal ($|D\rangle$), circular-left ($|L\rangle$), antidiagonal ($|A\rangle$), and circular-right ($|R\rangle$) polarizations, respectively. The names of these special cases describe the behavior of the oscillation of the electric field vector with respect to the time in a given plane. The orthogonal pairs of $|D\rangle$ and $|A\rangle$ have the electric field vector oscillating at $\pm 45^\circ$ to the horizontal, respectively. The third pair of $|L\rangle$ and $|R\rangle$ correspond to an electric field vector which rotates at a fixed magnitude about the axis of propagation, with the direction of rotation given by the name, i.e. clockwise or counterclockwise.

When quantizing the electromagnetic field, it can be seen that circularly polarized photons carry spin angular momentum corresponding to $+\hbar$ for $|L\rangle$ and $-\hbar$ for $|R\rangle$ per photon, where $\hbar$ is the reduced Planck constant.

1.2.3 Orbital Angular Momentum

Beyond spin angular momentum, i.e. polarization, it has been known that the electromagnetic field can also carry orbital angular momentum (OAM) [25]. Unlike spin angular momentum, OAM is not limited to 2 dimensions, and a photon may have a quantized OAM value $\ell\hbar$, $\ell \in \{-\infty, \ldots, \infty\}$, where ℓ is an integer number that defines the quantum number associated with angular momentum.

A collimated optical beam ($\boldsymbol{E}(x, y, z)$) that is propagating along the z-direction is well described within the paraxial approximation and consequently with the paraxial wave equation;

$$\left(\nabla_\perp^2 + 2ik\frac{\partial}{\partial z}\right)\boldsymbol{E}(x, y, z) = 0, \tag{6}$$

where k is the wavenumber, $\nabla_\perp^2 = \partial_x^2 + \partial_y^2$ is the transverse Laplacian operator is the plane perpendicular to the optical path of the beam, i.e. in the x, y-plane. While there are many valid solutions to the paraxial wave equation allowing for many modes of light, possessing certain symmetries, to neatly propagate, the solutions of interest are the family of solutions with a

"twisted" phase pattern, leading to photons which carry OAM along the propagation direction. One of these families of solutions are the Laguerre-Gaussian modes. Due to their cylindrical symmetry, they are given in cylindrical coordinates r, ϕ, z as:

$$\begin{aligned} \mathrm{LG}_{\ell,p}(r,\phi,z) =& \frac{C_{\ell,p}}{w(z)}\left(\frac{r\sqrt{2}}{w(z)}\right)^{|\ell|} \exp\left(\frac{-r^2}{w^2(z)}\right) L_p^{|\ell|}\left(\frac{2r^2}{w^2(z)}\right) \\ & \times \exp\left(\frac{ikr^2}{2R(z)}\right) \exp(i\ell\phi) \exp\Big(i(kz - \Phi_G(z))\Big). \end{aligned} \tag{7}$$

Here, $C_{\ell,p} = ((2p!)/\pi(p+|\ell|)!)^{1/2}$ is a normalization constant, $w(z) = w_0(1+(z/z_R)^2)^{1/2}$ is the beam waist at a propagation distance z with $z_R = \pi w_0^2/\lambda$ being the Rayleigh range, $L_p^{|\ell|}$ is the generalized Laguerre polynomial, $R(z) = z(1+(z_r/z)^2)$ is the radius of curvature of the beam. Finally, $\Phi_G(z) = (2p+|\ell|+1)\arctan(z/z_R)$ is the Gouy phase. The term $\exp(i\ell\phi)$ turns the beam wavefront into a twisted structure with an ℓ-number of twists.

LG modes are orthogonal in the transverse space, i.e.,

$$\Big\langle \mathrm{LG}_{\ell,p} \Big| \mathrm{LG}_{\ell',p'} \Big\rangle := \int_0^{2\pi} \int_0^{+\infty} \mathrm{LG}^*_{\ell,p}(r,\phi,z)\, \mathrm{LG}_{\ell',p'}(r,\phi,z)\, d\phi\, r dr = \delta_{\ell,\ell'}\delta_{p,p'}. \tag{8}$$

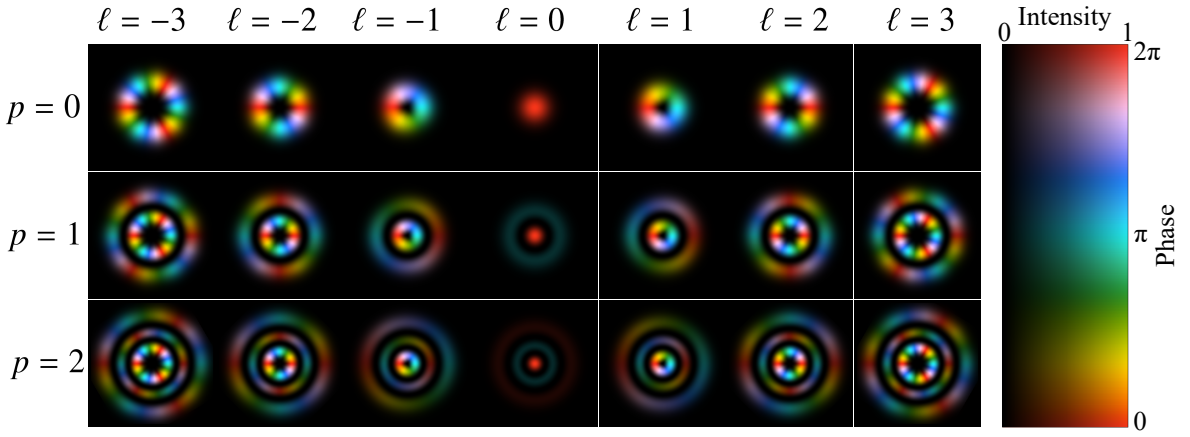

Figure 3: Intensity and phase distribution for $\mathrm{LG}_{\ell,p}$ modes with $p \in \{0,1,2\}$ and $\ell \in \{-3,-1,-2,0,1,2,3\}$. The hue color and false color show the phase variation from 0 to 2π and the normalized intensity, respectively.

The integer number p is referred to as the radial number of LG modes, and corresponds to the number of concentric rings of the mode, The value of p represents the number of additional

rings the mode has (there is always at least one), moving outward from the center of the beam. Between each additional concentric ring the phase experiences a π jump radially. This work does not focus on the radial number of the LG. However, we should consider both p and ℓ when optimizing the capacity of the communication channel.

Of particular interest in this solution is the phase factor of $\exp(i\ell\phi)$. From this component of the equation, it is clear that as the coordinate of ϕ goes from 0 to 2π, the phase will cycle from 0 to 2π a number of times equal to ℓ. This phasefront variation is where the orbital angular momentum arises.

Varying only the value of ℓ, a single photon with angular momentum $\hbar\ell$ along the propagation direction gains access to an infinite-dimensional Hilbert space, with each state being described as $\langle\phi|\ell\rangle := \frac{1}{\sqrt{2\pi}}\exp(i\ell\phi)$. Naturally, then, $\langle\ell|\ell'\rangle = \delta_{\ell,\ell'}$.

1.2.4 Time

In addition to spin and orbital angular momenta, photons possess other different degrees of freedom. One of the most utilized is frequency, particularly in the context of division multiplexing in telecommunications, e.g. in fiber-based telecommunication, expanding the communication bandwidth. Frequency and its conjugate, the time domain, are intrinsically linked through the Fourier transform, and thus the time domain (modes or bins) is also used for communication and photonic technologies. The main reason is that it is easier to generate, manipulate, and detect photons in the time bin compared to the frequency. By leveraging interferometers, it is possible to create a single photon or a coherent state in an arbitrary superposition of two or more distinct time bins. The probability distribution and relative phases between these time bins can be precisely controlled using phase shifters and beamsplitters within the interferometer. Since the pulses corresponding to each time bin do not overlap temporally, the time-bin states are inherently distinct, expanding the communication space, and form orthogonal bases.

Moreover, beyond simple time-bin states, one can construct a set of orthogonal modes within the temporal domain that lie within the coherence length of the photon. These modes, characterized by the Gaussian coherence length, can be mathematically expressed using Hermite polynomials, that is, $\langle t|\tau\rangle_n = c_n\, e^{-(t/\tau_c)^2}\mathrm{H}_n(t)$, where c_n is a normalization factor and τ_c is the coherence time. This orthogonal set of modes, that is, ${}_m\langle\tau|\cdot|\tau\rangle_n = \delta_{m,n}$, forms a complete basis in the temporal domain, making them valuable tools for quantum information processing, including applications such as the distribution of quantum keys.

1.3 Quantum Key Distribution

Quantum Key Distribution (QKD) is a method by which a one-time pad can be generated by two parties, namely *Alice* and *Bob*, with which they can encrypt their data and send them through a public channel. While traditional encryption protocols depend on the difficulty of performing operations on a classical computer, such as factoring prime numbers, QKD can theoretically be shown to provide unconditional security guaranteed by the laws of quantum mechanics; conjugate quantities cannot be measured simultaneously. Notably, this also dictates one of the no-go theorems, the no-cloning theorem, which prevents one from cloning arbitrary quantum states without introducing imperfections to the clones. The no-cloning theorem states that for any unknown quantum state, it is impossible to create a perfect copy [26]. This means that unlike in classical communications, trying to read a message encoded in a quantum state fundamentally changes the message, and any lost information cannot be recovered. Utilizing this property, two parties can exchange information encoded in quantum states and are then able to exchange information on the generation and measurements of these states to determine if they have been modified between being sent and being received.

1.3.1 Mutually Unbiased Bases

A very important concept for the majority of quantum information processing, including QKD protocols, is the idea of mutually unbiased bases (MUB). A basis that is mutually unbiased to another basis has the property that each of its basis vectors are formed by a balanced superposition of all basis vectors in the other basis [27]. If a photon is in a state (m,n) that is part of a basis (α,α'), a measurement in a MUB will result in an equal chance of measuring any of the states in the measurement basis.

$$\left|\left\langle \Psi_m^{\alpha} \middle| \Psi_n^{\alpha'} \right\rangle\right|^2 = \begin{cases} 1/d, & \alpha \neq \alpha' \\ \delta_{m,n}, & \alpha = \alpha' \end{cases} \tag{9}$$

In truth, we have already seen the concept of MUB in the context of polarization states of light. Spanning the 2 dimensional polarization space are the orthogonal vectors of $\{|H\rangle, |V\rangle\}$. However, another perfectly valid choice of basis vectors is the vectors $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. If one measures a vertically or horizontally polarized photon on diagonal-antidiagonal basis, there is an equal chance to measure either the $|D\rangle$ or $|A\rangle$ state. In this sense, these bases are unbiased, that is, $\{|H\rangle, |V\rangle\}$ are mutually unbaised bases to $\{|D\rangle, |A\rangle\}$. As a result, any information encoded in the original state, when measured in a MUB, is functionally lost. Importantly, the same property exists with the choice of left- and right-hand circularly

polarized basis. All three bases are mutually unbiased to each other, i.e. $\mathcal{M}_0 = \{|H\rangle, |V\rangle\}$ and $\mathcal{M}_1 = \{|A\rangle, |D\rangle\}$, and $\mathcal{M}_2 = \{|L\rangle, |R\rangle\}$, $\mathcal{M}_0, \mathcal{M}_1$ and $\mathcal{M}_2$ are mutually unbiased bases for a 2 dimensional space.

This is of course not limited to two dimensions as stated in equation (9). One way to generate one of the MUB in a Hilbert space of higher dimensions is to apply a discrete quantum Fourier transform to the states in the original (logical) basis. In a space of dimension d with states of $|\psi_k\rangle$, the discrete "Fourier basis" is then:

$$\left|\phi_j\right\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \omega_d^{kj} \left|\psi_i\right\rangle, \tag{10}$$

where $\omega_d = e^{2\pi i/d}$. This formulation will work in any dimension, but is not the only method of generating MUB. It is well known that in any dimension where d is a prime number, or a power of a prime, there are $(d + 1)$ bases that are mutually unbiased to each other [28]. It is unknown if this property holds true in all dimensions. One of the challenging dimension is $d = 6 = 2 \times 3$ that is not a power of a prime number, which only 3 MUB are found. It is widely believed however that this is the maximum bound to the number of MUB [29].

In such dimensions where d is a prime number, one can generate all $(d + 1)$ MUB states with the following recipe. Beginning with the logical basis, $\mathcal{M}_0 = \{\left|\psi_0^0\right\rangle, \left|\psi_1^0\right\rangle, \ldots, \left|\psi_{d-1}^0\right\rangle\}$, the d states in $\mathcal{M}_\alpha = \{\left|\phi_0^\alpha\right\rangle, \left|\phi_1^\alpha\right\rangle, \ldots, \left|\phi_{d-1}^\alpha\right\rangle\}$ are then given by:

$$\left|\phi_j^\alpha\right\rangle := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} (\omega_d^j)^{d-k} (\omega_d^{-\alpha})^{s_k} \left|\psi_k^0\right\rangle, \tag{11}$$

where $\alpha \in \{1, 2, \ldots, d\}$, $\omega_d = e^{2\pi i/d}$, $s_k = k + (k + 1) + \ldots + (d - 1)$.

1.3.2 BB-84

The original QKD protocol outlined by Bennet & Brassard in their seminal 1984 conference proceeding is the simplest and most straightforward protocol. The steps are outlined

1. **Key Generation**

   Alice and Bob each generate a random string of bits to serve as their initial key. It is important to note that this is a completely random process that cannot be guessed by a third party. This then requires them to each utilize a quantum random number generator.

2. **Encoding**

   Alice uses her random string of bits for two choices; the first is the decision on which basis to encode the information. Alice will either encode her information in MUB0 or

MUB1 which, in the context of polarization will be the choice of the horizontal-vertical basis, or the diagonal-antidiagonal basis. Secondly, Alice encodes the bit of information in the polarization of the photon, with one of the states representing "0" and the other representing "1".

3. **Transmission**
   The photon is sent through the channel, where it may be intercepted or acted upon by an eavesdropper. Even without a bad actor affecting the channel, the photon's state may change upon propagation, introducing errors that must be attributed to an eavesdropper.

4. **Decoding**
   Bob receives the photon, and makes the choice of basis to measure in. This can be done passively by using a simple beam splitter, or in more complex systems it could be done actively with fast hardware such as an electro-optic modulator. If Bob measures the photon state in the same basis in which it was encoded, assuming that no errors are introduced by the channel, he will measure the correct state and gains one bit of information. If Bob measures the photon state on an incorrect basis, due to the properties of MUBs, the outcome of the measurement can be either of the states, i.e. "0" or "1" randomly. In this case, the information is lost and is irrecoverable.

5. **Public Discussion**
   After a sufficient number of photons are exchanged, Alice and Bob announce in a public classical channel the basis in which each photon was prepared and measured. For each instance that they prepared and measured on different bases, this bit is discarded, as Bob will not have a 50% chance of guessing the encoded bit. All of the remaining bits in which they prepared and measured in the same basis are maintained and make up their initial shared key.

6. **Error Estimation**
   In a channel that has neither errors nor an eavesdropper, Alice and Bob now share a key that matches exactly. In order to check for eavesdroppers, they must sacrifice a portion of their key, publishing it on their public channel. Using this section of their key, they ensure that the rate of errors (Q) is lower than the threshold required for guaranteed security according to equation (12). If the error rate is not sufficiently lower to provide the guarantee of security, the key is abandoned, and Alice and Bob must restart from Step 1. It is important to note that this means QKD cannot prevent denial of service attacks.

7. **Error Correction & Privacy Amplification**
   If the error rate is within a tolerable range, Alice and Bob can begin performing classical error correction algorithms such as parity checks to ensure that they have perfectly matching keys. Finally, with a hashing function, Alice and Bob use their matching keys to generate a new final key with a shorter length, reducing any mutual information that Eve could have gained during the exchanging of photons [30].

8. **Secure Communication**
   Alice and Bob now share a one-time pad with which they may encrypt their data. Alice now takes her message (M) that is the same length as their shared key (K) and performs a bitwise addition to generate the encrypted message (E), $M \bigoplus K = E$. This encrypted message is sent over a public classical channel, after which Bob performs the same operation $E \bigoplus K = M$ to retrieve the message.

Alice's bits	0	1	0	0	1	0	1	1	0
Alice's encoding basis	H,V	H,V	D,A	H,V	D,A	H,V	D,A	H,V	H,V
Sent photon state	$\|H\rangle$	$\|V\rangle$	$\|D\rangle$	$\|H\rangle$	$\|A\rangle$	$\|H\rangle$	$\|A\rangle$	$\|V\rangle$	$\|H\rangle$
Bob's measurement basis	H,V	D,A	D,A	H,V	H,V	D,A	D,A	H,V	D,A
Bob's measured bits	0	1	0	0	0	1	1	1	0
Agreement on basis	Yes	No	Yes	Yes	No	No	Yes	Yes	No
Sifted Key	0		0	0			1	1	

Table 1: Simple example of a short BB-84 QKD protocol in a channel without errors up to step 5.

1.3.3 High Dimensional BB-84

Quantum key distribution can be performed in two dimensions, but can be extended into higher dimensions. In this type of protocol, each MUB may have more states that encode more than one bit of information per photon. If one has, for example, two MUBs ($\mathcal{M}_0$, $\mathcal{M}_1$) then in dimensions d, it has been shown that beyond the advantage of a higher information density, a higher error tolerance can also be achieved [13] using a higher-dimensional protocol. Given an error rate of a d-dimensional channel, Q, one can calculate the information density of the channel per sifted photon, $R(Q)$, i.e.,

$$R_d(Q) = \log_2(d) - 2h_d(Q), \tag{12}$$

where $h_d(Q) = -Q\log_2(Q/(d-1)) - (1-Q)\log_2(1-Q)$ is the d-dimensional Shannon entropy function. Setting $R_d(Q) = 0$ and solving for the value of Q will give the maximum tolerable error rate for a d dimensional QKD protocol. These error rates for dimensions of size 2^n are shown as the x intercepts in Figure 4.

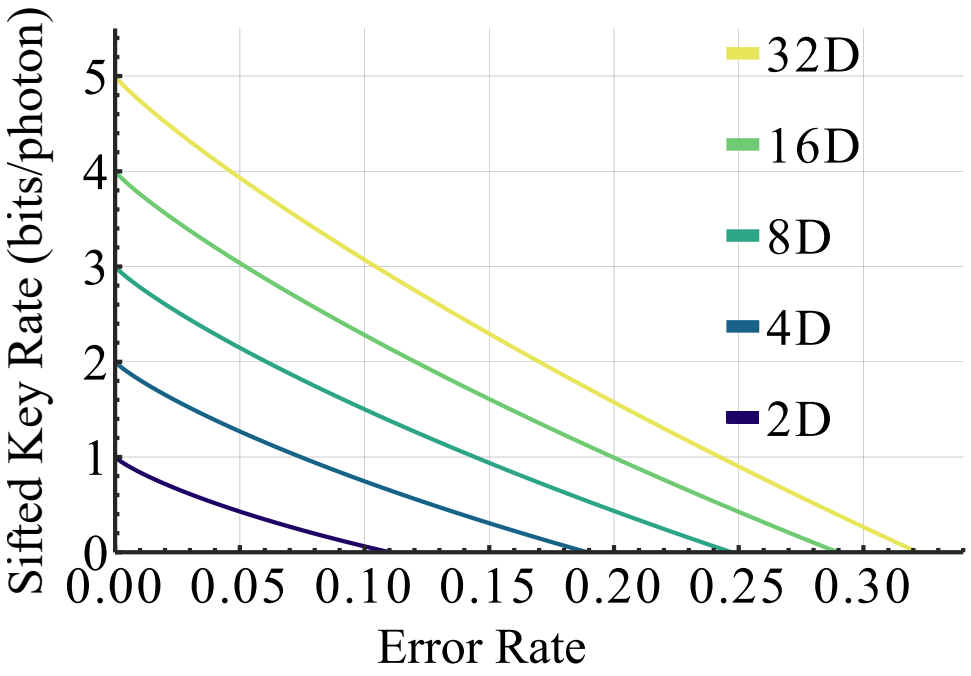

Figure 4: Information density as a function of error rate for a high-dimensional BB-84 QKD protocol in increasing dimensions. In a channel with no errors, each new bit of information that one seeks to encode into a single photon required a doubling of the dimensionality. It can also be seen that as the dimensionality continues to increase, the maximum tolerable error rate is increased, but by less each time.

Beyond employing the high-dimensional BB84 protocol, accessing higher-dimensional alphabets enables the development and utilization of novel protocols that can share more bits of information and enhance noise tolerance per sifted photon. For instance, when the dimension is a power of a prime number, Alice and Bob can randomly select the $(d+1)$ MUB to generate and detect photonic states. This approach, known as the tomographic QKD protocol, has a correct MUB probability success rate of $1/(d+1)$. Although this success rate is lower than the $1/2$ rate of the high-dimensional BB84 protocol, it results in higher key rates compared to the bidimensional space [31]. Another example is the QKD protocol, which allows one to encode more than one bit of information per sifted photon and can also tolerate higher error rates [32].

1.4 Atmospheric Turbulence

Turbulence is a complex phenomenon that occurs in fluid dynamics, where the motion of a fluid becomes chaotic, irregular, and unpredictable. In Earth's atmosphere, these chaotic motions and irregularities lead to large-scale events like hurricanes, down to smaller meteorological phenomena like tornadoes. The irregularity of the air in the atmosphere causes free-space optical experiments to suffer from propagating through a non-static, and anisotropic medium, especially at longer channel lengths. Sending an optical beam through the atmosphere will result in a deformed beam shape (in both phase and intensity), and large beam-wander at the receiver. These effects negatively impact the amount of information that one can send through the channel and massively limit its usability. These difficulties, along with developments in the efficiency and cost of fibres have led to the mass-adoption of fibre based networks for communications while free-space optical channels have been mostly abandoned [33]. Recently, however, a renewed drive to investigate the utility of free-space channels has emerged, formed mostly from the desire for higher and higher bandwidth channels which can be achieved through spatial-mode multiplexing and the desire for satellite QKD links.

1.4.1 Kolmogorov Turbulence

The mathematical exploration of atmospheric turbulence commenced in 1941, originating from the pioneering work of mathematician A.N. Kolmogorov. Due to the natural tendency of turbulent fluids to form eddies of many different sizes, Kolmogorov postulated that in the limit of very high Reynolds numbers (when the fluid flow is most likely to be turbulent, not laminar), the flow of the smallest eddies will be isotropic. This is in contrast to large-scale eddies whose properties will be governed by the boundary conditions and characteristics of the system, such as the wind and the ground profile [34]. This hypothesis led Kolmogorov to calculate the smallest possible scale of eddies, η, for a fluid given only the viscosity of the fluid, ν, and the rate of energy dissipation of the system ε, that is, given by

$$\eta \equiv \left(\frac{\nu^3}{\varepsilon}\right)^{\frac{1}{4}}. \tag{13}$$

In the atmosphere the smallest eddies are typically in the range 0.1-10 mm in size [35].

This theory was taken into the field of optics by V. I. Tatarskii, who investigated the propagation of waves in turbulent media using Kolmogorov's assumptions, in particular their statistical properties [36]. One of the many important results of his work is the definition of the

structure function of the refractive index of the atmosphere.

$$D_{nn}(r) = \overline{\left(n(\vec{x}_1) - n(\vec{x}_2)\right)^2} = C_n^2 r^{2/3} \tag{14}$$

This function describes the variance of the refractive index of air, $n(\vec{x})$, on a given path, where $\vec{x}_1, \vec{x}_2$ are the end points of the channel, $\vec{r}$ is a vector between these points, and C_n^2 is a constant called the structure parameter. This structure parameter is then a quantifiable value indicating the variations in the refractive index of the air, and in turn the strength of the turbulence over a given channel at a given time. Its average value on a given night is often quantified at potential astronomical observatory sights. While there are many ways to quantify the strength of turbulence in a channel, C_n^2 has seen the widest adoption by the scientific community. For raised free space channels parallel to the ground, average values of C_n^2 are most often within the range of $1 \times 10^{-18}\mathrm{m}^{-2/3}$ for low strength turbulence, and $1 \times 10^{-14}\mathrm{m}^{-2/3}$ for high strength turbulence.

Another critical parameter for quantifying atmospheric turbulence is the Fried parameter, r_0 [37], which corresponds to the average size of turbulent eddies in the channel. These eddies can be seen to act like lenses as a result of the fast moving air on the outside of the eddy having a lower density in comparison to the slower moving air in its center. With this physical intuition, it is clear to see that in a communications channel using a receiver aperture D, large values of r_0 such that $r_0 > D$ will not cause large transverse variations in the refractive index of the atmosphere. This will in turn cause only low-order aberrations on an optical mode sent through the channel. In contrast, if $r_0 < D$, multiple eddies will fit within the transverse dimension of the optical mode, and there will be many interacting lensing effects. This will cause many higher-order aberrations on any mode that one is attempting to use to communicate in the channel. The strength of this effect can be quantified by the ratio D/r_0, where r_0 is given by

$$r_0 = (0.423k^2\, r\, C_n^2)^{3/5}, \tag{15}$$

Here, k is the optical beam wavevector.

1.4.2 Measuring C_n^2

A value for C_n^2 can be determined by the implementation of a scintillometer. On one end of a free-space channel an incoherent emitter is placed, and on the other end a telescope with a photodiode. For a given time period, the intensity of light is monitored and both the average, $\langle I \rangle$ and the standard deviation, s are determined. The theoretical correspondence between the

intensity of incoming light and the value of C_n^2 is based on the variance of the logarithmic amplitude, B [36], given by,

$$B = \frac{1}{4} \ln\left[1 + \left(\frac{s}{\langle I \rangle}\right)^2\right]. \tag{16}$$

The turbulence strength, calculated as C_n^2 is then given by, [38]

$$C_n^2 = 4.48 B r^{-3} D^{7/3}, \tag{17}$$

where r is the path length, and D is the aperture size of the emitter.

During strong turbulence conditions, the value of B is known to saturate, meaning that it can no longer be used to calculate turbulence strength. [39]. This saturation is caused by the much smaller eddies in strong turbulence, as they disproportionately affect the signal. The technique used to avoid this issue is to implement incoherent optics with large aperture sizes. The incoherent light will not introduce intensity fluctuations from interference, and the larger aperture size biases the device to measure the effects of larger turbulent eddies [40]. A correction is then applied to the resulting measurement to reverse the introduced bias. Another advantage of an incoherent source is the ease of alignment and use, the source does not need to be collimated and only needs to be pointed in the general direction of the receiver.

1.4.3 Abberations with Zernike Polynomials

Optical aberrations are not unknown to researchers, and in the laboratory environment they are most often caused by misalignment of optical elements such as (non-flat) mirrors and lenses. These common static aberrations can be described by the eponymous Zernike polynomials, which are functions defined over a unit circle given by Fritz Zernike [41]. The Zernike polynomials ($Z_{n,l}$) are orthogonal functions defined over a unit circle, normalized such that $\int_0^{\pi} \int_0^1 Z_{n,l}\, \rho\, d\rho\, d\phi = \pi$. They are sometimes labelled Z_j, with j being the ANSI index, $j = [n(n+2) + l]/2$. Finally, they can be labelled with the Noll indexing, here represented by Z_N. Any continuous function over a unit circle can be decomposed in terms of the Zernike polynomials, allowing for arbitrary optical aberrations to be described.

$$\Phi(\rho, \phi) = \sum_j \alpha_j Z_j \tag{18}$$

$Z_{n,l}$	Z_j	Z_N	Polynomial	Name
$Z_{0,0}$	Z_0	Z_1	1	Piston
$Z_{1,-1}$	Z_1	Z_3	$2\rho\sin(\phi)$	Tip
$Z_{1,1}$	Z_2	Z_2	$2\rho\cos(\phi)$	Tilt
$Z_{2,-2}$	Z_3	Z_5	$\sqrt{6}\rho^2\sin(2\phi)$	45° astigmatism
$Z_{2,0}$	Z_4	Z_4	$\sqrt{3}(2\rho^2-1)$	Defocus
$Z_{2,2}$	Z_5	Z_6	$\sqrt{6}\rho^2\cos(2\phi)$	0° astigmatism

Table 2: Definitions of the first six Zernike polynomials, and their associated names.

2

Predicting Turbulence for Quantum Key Distribution

2.1 Free Space Link

To perform QKD over the city of Ottawa, we have established two locations with an active line-of-sight. One spot on the roof of Colonel By (CBY) at the University of Ottawa and the other on the roof of NRC building M55. These two stations are separated by a distance of 5.4 km. Before performing QKD over this channel, we have installed a scintillometer at CBY, and an infrared LED array system at M55. This system operates 24/7 with the scintillometer measuring the intensity of the light output by the emitter over time, and correlating the statistics of the measured intensity to the turbulence in the channel, namely the C_n^2. This system has been operating continuously since July of 2023, and has now collected one year of turbulence data, providing valuable information on when the turbulence will be strongest and when it will be weakest. We seek to use this information to allow us to make informed decisions about when is the best time to perform QKD experiments over this link in the future. In particular, we have developed a method to be able to determine 6 hours in advance whether or not a given night is a good night to perform free-space QKD experiments in this channel. Beyond our own

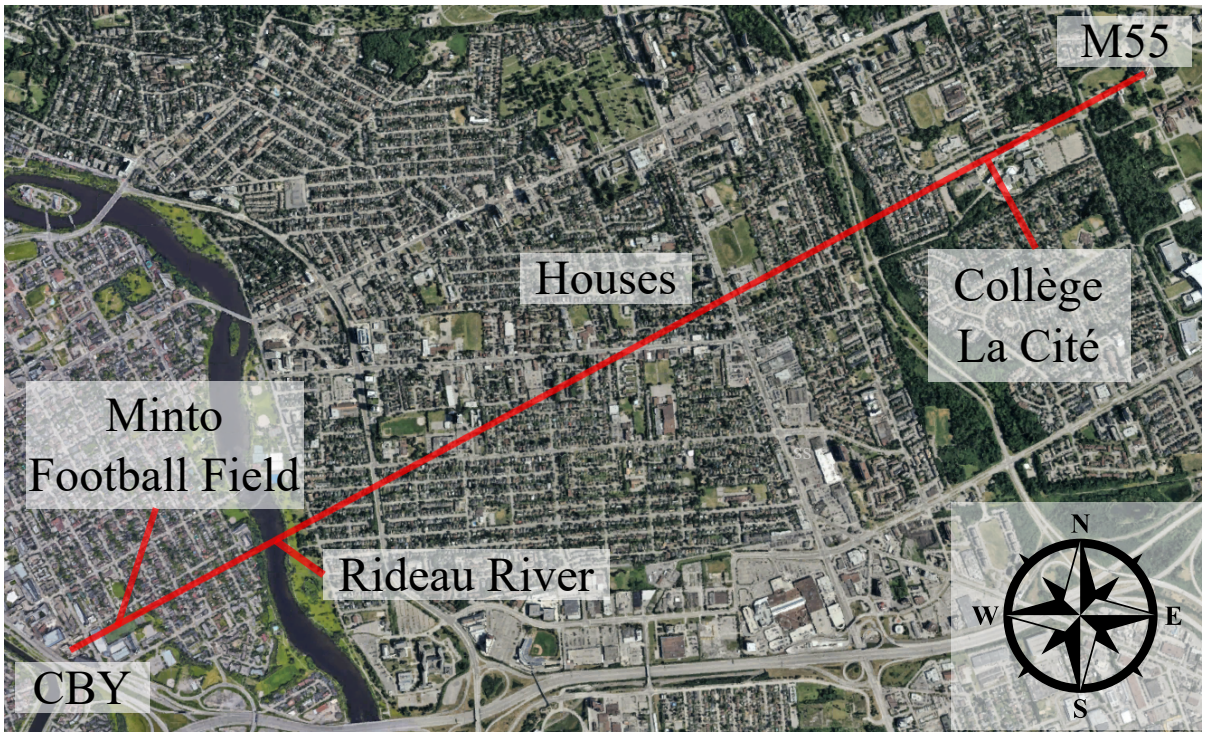

Figure 5: 5.4 km Free-space Channel: A top-down view of our free-space link in Ottawa, extending from M55 to CBY, with key features clearly labeled. The detector is positioned at CBY, the southernmost point of the link, strategically placed to minimize the sun's interference, as in the northern hemisphere, the sun remains in the southern sky. Image sourced from Google Earth.

use, we believe that this technique can be used by ground stations looking to perform QKD with satellites, or even stations that are operating in a ground-ground configuration. Knowledge of future channel performance will allow large-scale quantum networks to optimize their performance, allowing users to amass keys before a predicted network outage.

2.1.1 Channel Parameters and Description

Our 5.4 km channel has a change in height of 39 m from one side to the other, with the top of the CBY being at 85 m above sea level, and M55 being at 124 m above sea level. It passes over a wide variety of types of buildings and developments, which can be seen in Figure 5. From M55 to CBY, the channel goes above the campus of Collège La Cité which has many buildings and a large open parking lot. After this campus, 3.3 km of houses follow, most of

which are two- or three-story buildings, many of which have trees. This section is therefore the most varied in terrain. The channel goes over the Rideau River, followed by 600 m of more housing. Finally, the last object of interest along the path is the Minto Football Field on the University of Ottawa campus.

This widely varying terrain, as well as the inclination of the path, make analytical estimates for the strength of the turbulence in the channel particularly difficult. The distance from the ground is an integral component of any analytical estimation of the strength of current turbulence [42]. The height is not a constant value along our path, and it will vary wildly from very close to the top of the trees, to very far from the ground while above the River or the Collège campus. This is a contributing factor to why we have purchased our own equipment to measure the C_n^2 in our specific channel.

2.2 Turbulence Data

2.2.1 Collection and Preparation

A value for C_n^2 in the channel is collected once each minute by our scintillometer, a BLS 450 Large Aperture Scintillometer from Scintech. On one end of the channel there is an array of 850 nm LEDs blinking at 21 Hz, and at the other end there is a 15 cm diameter telescope collecting this light onto a photodiode. By using a blinking signal, the system is able to remove any background noise that exists, such as light from the sun and man-made structures. For the purposes of removing high-frequency noise, these values are time averaged over 1 hour using a moving average technique. Each value of C_n^2 is time correlated with data received from the Meteorological Service of Canada, including weather parameters such as relative humidity, solar radiation, temperature, pressure, wind speed, and amount of snow on the ground. In addition to these, we add information on the time of day and date within the year. After this process, we then have 9 months of correlated values of C_n^2 and weather at the time of measurement. This dataset was then formatted for use in the training a Gated Recurrent Neural Network (GRNN).

2.2.2 Implementation of Neural Network

The links between the current and past weather conditions and the turbulence conditions are inherently linked; however, due to the complexity and size of the systems involved, the correlations are not trivial to determine. In fact, there is no universal theory to describe atmospheric turbulence in all cases [43]. When systems become so complex, and patterns are not clear, one

of the best kinds of tools we have at our disposal are Neural Networks (NNs) [44]. This type of algorithm that is modeled on a brain, with nodes acting as neurons and the nodes being connected. The algorithm takes examples of inputs and outputs that you are looking to identify, and continuously remaps the connections between the nodes. Having more examples of the data that you are looking to model benefits the network, as just like a human, it will learn to model it. While the topic of Neural Networks can take up many pages, we note here that it is simply used as a tool to extract information regarding patterns based on input and output data.

2.3 Simulated QKD in Turbulence

To demonstrate how our turbulence prediction tool can be used in the context of quantum networks, in particular how we will be using it, we model a QKD protocol over this channel in differing levels of turbulence. This will allow us to correlate the current conditions, and future conditions as provided by the AI-tool to QKD performance and provide information on the feasibility of performing experiments either right now or in the future. In order to do this, we must simulate the propagation of the desired states through this channel under varying turbulence conditions, using its true physical parameters. We choose an 8-dimensional BB-84 protocol based on the OAM modes as described in Eq. (7), with the states of the Mutually Unbiased Bases given in Eq. (10).

2.3.1 Turbulence with Zernike modes

Turbulence in an optical channel is not a discrete phenomenon, as the refractive index along the optical path will vary continuously creating essentially a phase *volume*, however this makes for a very complex reality if one is looking to perform simulations. To reduce the computational load, one can think of breaking the optical channel into multiple sections, each consisting of a single-phase screen followed by propagation. This technique can only truly be equivalent to a volumetric representation of atmospheric turbulence in the limit of infinite planes.

In the lowest level of approximation, turbulence can be simulated via the application of a series of single-phase screens. This was investigated by Robert Noll in 1975 [45], whose main result in this work was to find the statistics of the strength of the Zernike modes that will, on average, result in effects corresponding to certain values of D/r_0. These results have been widely used in the simulation of atmospheric turbulence, as well as in the understanding of how to correct it with techniques such as adaptive optics [46, 47, 48].

The values of the Zernike coefficients (α_j) are found by assuming a plane wave (Φ) that is deformed by a phase screen composed of Zernike modes as described in Eq. (18). The mean

square residual error of this wave (corrected up to Zernike mode number J) is given by:

$$\Delta_J = \langle \Phi^2 \rangle - \sum_{j=1}^{J} \langle |\alpha_j|^2 \rangle. \tag{19}$$

Δ_1	$1.0299(D/r_0)^{5/3}$	$\Delta 7$	$0.0587(D/r_0)^{5/3}$
Δ_2	$0.582(D/r_0)^{5/3}$	Δ_8	$0.0525(D/r_0)^{5/3}$
Δ_3	$0.134(D/r_0)^{5/3}$	Δ_9	$0.0463(D/r_0)^{5/3}$
Δ_4	$0.111(D/r_0)^{5/3}$	$\Delta_1 0$	$0.0401(D/r_0)^{5/3}$
Δ_5	$0.0880(D/r_0)^{5/3}$	$\Delta_1 1$	$0.0377(D/r_0)^{5/3}$
Δ_6	$0.0648(D/r_0)^{5/3}$	$\Delta_1 2$	$0.0352(D/r_0)^{5/3}$

Table 3: Mean square residual error for wavefronts corrected from Zernike modes $j = \{1, 2, \ldots, j\}$

The mean square residual error for each value of Δ_j, is calculated by Noll and is given in Table3, which allows us to calculate the average variance for each Zernike mode. This value is compared to the value of D/r_0, as described in Section 1.4.1. This then allows us to generate phase screens with a given Fried parameter. For larger values of J i.e. $J > 12$ [49], the pattern follows: $0.2994J^{-\sqrt{3}/2}(D/r_0)^{5/3}$.

2.3.2 Simulated QKD Channel Characterization

We generate simulated beams with the phase and intensity profile of Eq. (7) for the logical basis and generate the MUB using the Fourier transform method of Eq. (10). We generate phase masks according to the method described above and apply these phase masks to the generated beams. The are subsequently divided into a grid of 500×500 pixels, and this image is propagated numerically using the Fourier method [50]. The fidelity of the aberrated beam and a beam without any aberrations that propagated the same distance is then calculated. By doing this for all states in each basis, we calculate a crosstalk matrix by which we extract the error rate.

Predicting atmospheric turbulence for secure quantum communications in free space

Tareq Jaouni,[1,*] Lukas Scarfe,[1,*] Frédéric Bouchard,[2] Mario Krenn,[3]
Khabat Heshami,[2,1] Francesco Di Colandrea,[1,4,†] and Ebrahim Karimi[1,2,3]

[1] *Nexus for Quantum Technologies, University of Ottawa, Ottawa ON, Canada, K1N 5N6*
[2] *National Research Council of Canada, 100 Sussex Drive, Ottawa ON, Canada, K1A 0R6*
[3] *Max Planck Institute for the Science of Light, Staudtstrasse 2, 91058 Erlangen, Germany*
[4] *Dipartimento di Fisica, Università degli Studi di Napoli Federico II, Complesso Universitario di Monte Sant'Angelo, Via Cintia, 80126 Napoli, Italy*

Atmospheric turbulence is the main barrier to large-scale free-space quantum communication networks. Aberrations distort optical information carriers, thus limiting or preventing the possibility of establishing a secure link between two parties. For this reason, forecasting the turbulence strength within an optical channel is highly desirable, as it allows for knowing the optimal timing to establish a secure link in advance. Here, we train a Recurrent Neural Network, TAROCCO, to predict the turbulence strength within a free-space channel. The training is based on weather and turbulence data collected over 9 months for a 5.4 km intra-city free-space link across the City of Ottawa. The implications of accurate predictions from our network are demonstrated in a simulated high-dimensional Quantum Key Distribution protocol based on orbital angular momentum states of light across different turbulence regimes. TAROCCO will be crucial in validating a free-space channel to optimally route the key exchange for secure communications in real experimental scenarios.

I. INTRODUCTION

The ability to forecast weather conditions is a relevant achievement in modern society, impacting agriculture [1], energy management [2], climate science [3], and public health [4]. Traditional forecasts involve tangible parameters such as temperature, wind speed, and precipitation, while the complex phenomenon of atmospheric turbulence has mainly been restricted to astronomical observations [5], and only recently extended to free-space communications [6, 7]. Atmospheric turbulence originates from the rapid variation in time of different weather parameters, which results in optical signals experiencing a continuously varying refractive index when traveling through the atmosphere [8]. This severely affects the reliability of optical experiments realized in "free space", which has led to the dominance of fibre-based communications networks. Scintillation of low-power light, beam wandering, and wavefront distortion are representative examples of common optical aberrations, globally quantified by the structure parameter C_n^2 [9].

Atmospheric turbulence significantly limits optical communications, both in the classical [10] and quantum [11] regime. Typical effects are high crosstalk and lower power transmission. For these reasons, adaptive-optics correction systems have been proposed and experimentally demonstrated, showing promising results for free-space Quantum Key Distribution (QKD) in turbulent channels [12–14]. These achievements set the baseline for future ground-to-ground [15] and ground-to-satellite [16] configurations. In the broader context of quantum networks, predicting the trend of atmospheric turbulence is key to establishing a secure connection between two parties, leading to informed decisions about the future usage of available channels within the network.

Based on historical weather data, standard approaches to forecasting atmospheric turbulence relied upon empirical models [17], remote sensing [18] and, more recently, artificial neural networks [19–22]. In particular, Grose and Watson explored the application of different instances of Recurrent Neural Networks (RNNs) to predict C_n^2 values up to a few hours in advance [20]. These architectures are specifically designed to model sequential data, which makes them suitable candidates for capturing the temporal dependencies within the input weather data in the form of a time series. Although excellent levels of accuracy have been reported in this first case study, the final implementation suffered from relevant limitations, most importantly the lack of real night-time data, a training dataset only spanning a single season, and a rigid fixed-time prediction in the future [20].

In this paper, we train TAROCCO [23], an RNN processing dataset encompassing 9 months of weather data with a minute-by-minute time resolution to forecast C_n^2 values within a 5.4 km intra-city channel over the City of Ottawa. Our scheme outputs predictions within a flexible number of hours in the future (up to 12 hours) and with a custom time resolution (down to one minute). This computational toolbox provides the preliminary validation step of a turbulent channel for near-term QKD experiments. The significance of this result is numerically demonstrated by simulating a high-dimensional BB84 QKD protocol employing spatial modes of light under different turbulent regimes. In principle, all free-space experiments utilizing structured light can benefit from this tool, since knowing the turbulence strength in advance can allow for predictions of the success rate of these experiments [24–27]. The same analysis can apply

* These authors contributed equally to this work.
† francesco.dicolandrea@unina.it

to nearby satellite ground stations, which would allow for determining the optimal channel for maximum key exchange on a given satellite pass.

II. THEORY

A. Atmospheric turbulence

Atmospheric turbulence can be quantified in terms of the structure parameter of the refractive index C_n^2. The C_n^2 is defined as the variance of the refractive index over a given optical path, normalized to the path length [28]:

$$C_n^2 = \frac{\overline{(n(\vec{x}) - n(\vec{x}+\vec{r}))^2}}{r^{\frac{2}{3}}} \approx \frac{\mathrm{var}(n)}{r^{\frac{2}{3}}}, \tag{1}$$

where $n, \vec{x}, \text{and } \vec{r}$ are the refractive index of the atmosphere, the position along the path, and the distance from the sender to the receiver, respectively, with the average taken over all positions within the path.

The effect of atmospheric turbulence on optical beams can be modeled as a random sequence of phase masks dislocated along the path. By randomizing the phase screens in multiple realizations, it is possible to retrieve the average effect of the turbulence on the input beam with good approximation [29]. Zernike modes, which are traditionally employed to model optical aberrations [30], provide a natural choice to generate the phase masks. In particular, the value of C_n^2 can be directly related to the variance of each Zernike mode [31].

To measure the value of C_n^2 in our channel, we employ scintillometry [32]. By continuously measuring the optical intensity of a beam propagating from the sender to the receiver, relevant statistical parameters can be extracted to retrieve the structure parameter over a given time period.

B. Quantum Key Distribution

Quantum key distribution (establishment) is a technique introduced by Bennett and Brassard with the well-known BB84 protocol [33], which utilizes the principles of quantum mechanics to enable provably secure communications between two parties, by establishing a shared secret key. Security is guaranteed when the error in transmission and measurement of the quantum information is below a given threshold, depending on the dimension of the protocol [34]. Extending QKD to high-dimensional states allows for higher information capacity (typically expressed in "bits per photon"), higher tolerance to errors, and innovative protocols [35].

In a d-dimensional error-free QKD protocol, the number of informational bits per photon is $R(d) = \log_2(d)$. Turbulence-induced errors within a free-space channel result in a diminished key rate. For a high-dimensional BB84 protocol [36]:

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

where $h(x) = -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the Shannon entropy, and e_q is the error rate. When $R(d, e_q) < 0$, security is not guaranteed.

It must be noted that QKD protocols are typically not used to send messages, but only to establish a shared key through which classical communications can be securely encrypted. These keys can also be generated and stored for later use, even if the quantum channel is incapable of generating new keys [37].

Further reading on the practical implementations of QKD can be found in Ref. [38].

III. METHODOLOGY

A. Data Collection and Preparation

We employ the Scintech BLS450 Large Aperture Scintillometer to record the value of C_n^2 over our channel [39]. The system has been active 24/7 measuring the turbulence of the channel for 9 months. An aerial view of the monitored channel is provided in Fig. 1. The C_n^2 values have been recorded once per minute. Fog and heavy snowfall can cause system outages, corresponding to missing data points in our training set. To remove spurious information deriving from high-frequency noise, a moving average is performed for each data point over a one-hour time window.

Other weather parameters, such as temperature, solar radiation, and humidity, have been obtained from Environment and Climate Change Canada [40]. The weather station at which the parameters are measured lies 5 km SW from the receiver. For these parameters, no additional processing or filtering was applied. The averaged C_n^2 values are time correlated with the other meteorological data, and finally separated into batches for training the RNN.

The input layer of the network consists of 12 hours of minute-by-minute weather data, with n hours of future C_n^2 values as the target output. The dataset is divided into a training part where the network learns, a validation dataset to provide feedback on the network's training, and a test dataset to evaluate the network's performance on unseen data. All input and output features are normalized according to:

$$X \to \frac{X - \min(X_T)}{\max(X_T) - \min(X_T)}, \tag{3}$$

where $\min(X_T)$ and $\max(X_T)$ denote, respectively, the minimum and maximum of the feature X over the training dataset.

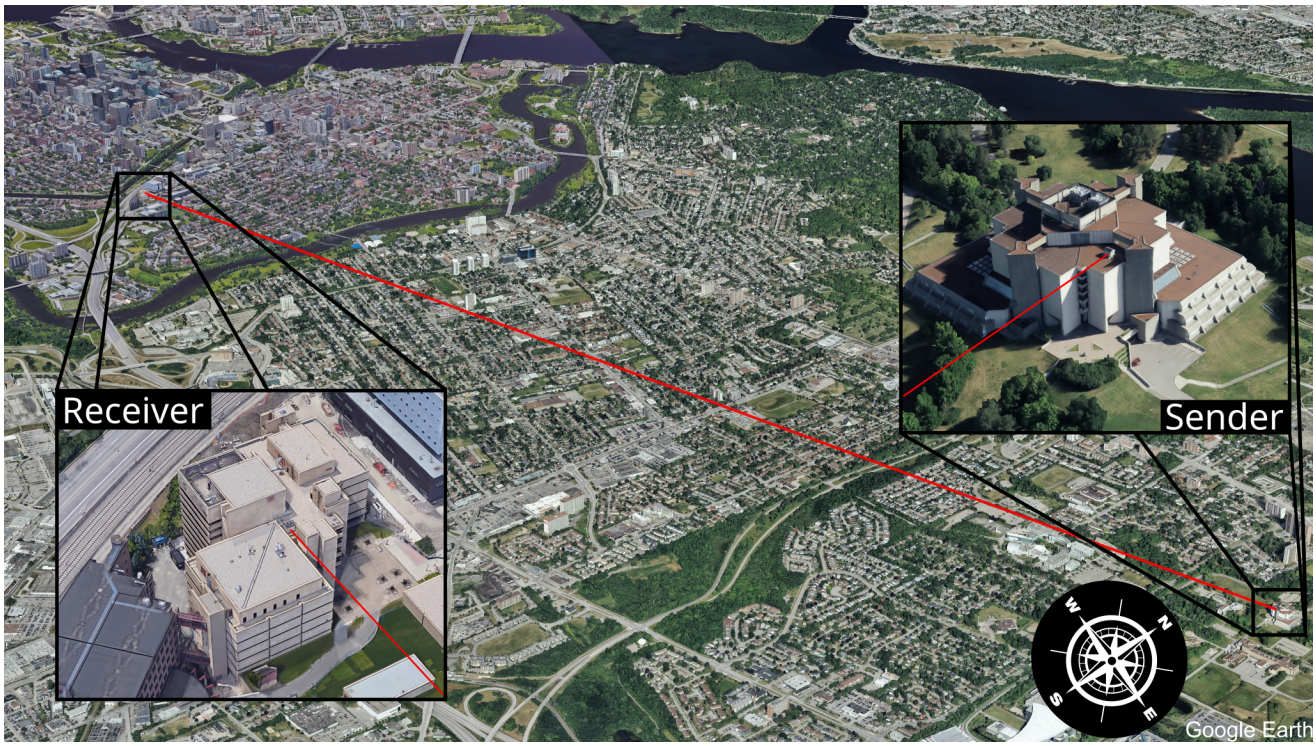

Figure 1. **Channel path.** The path over which the turbulence data was collected from July 2023 to March 2024. The receiver is on the University of Ottawa campus, while the sender is on the Canadian National Research Council 5.4 km ENE. This configuration was chosen to minimize the background levels caused by the sunlight.

B. Recurrent Neural Network

We train a Gated Recurrent Unit (GRU) neural network, named TAROCCO, to forecast the evolution of the C_n^2 values over time. GRUs are a simplified derivative of the long short-term memory (LSTM) recurrent units, which capture long-term features of the data. Figure 2 illustrates our neural network architecture, which takes 12 hours of prior combined meteorological and scintillometer data as input and outputs the C_n^2 forecast over 6 hours. Following the Permutation Feature Importance method detailed in Appendix A, temperature (°C), solar radiation (kJ/m^2), relative humidity (%), $\log_{10} C_n^2$, and the UTC time (s) are used as input features. The time feature t is made periodic over one day with the following map:

$$\begin{aligned} t_x &= \cos\left(\frac{2\pi t}{T}\right), \\ t_y &= \sin\left(\frac{2\pi t}{T}\right), \end{aligned} \tag{4}$$

where $T = 86400$ s.

Our network outputs the turbulence forecast through a fully connected dense layer that takes as input the final hidden state of the incident GRU layer. The number of output neurons is given by $N_{\text{out}} = H/R$, where H is the desired number of hours in the future (6 hours) and R is the desired output time resolution (15 minutes).

The cost function used for training is the Mean Squared Error (MSE):

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N} |\vec{y}_{i,\text{pred}} - \vec{y}_{i,\text{true}}|^2, \tag{5}$$

where $\vec{y}_{\text{pred}}$ and $\vec{y}_{\text{true}}$ denote the predicted and true output C_n^2 forecast, and N is the size of the evaluated dataset. The complete list of hyperparameters used for training is reported in Appendix B.

IV. RESULTS

A. C_n^2 forecast

The network is validated on two test datasets, one spanning October 2023 and the other from February 14th to March 14th, 2024. For these tests, we employed two separate architectures, respectively trained on a set deprived of the corresponding test set. The dataset from October 2023 is specifically chosen as it features a significantly variable evolution of the C_n^2 compared to other months, which makes it a challenging validation. The performance of the network is evaluated as the average

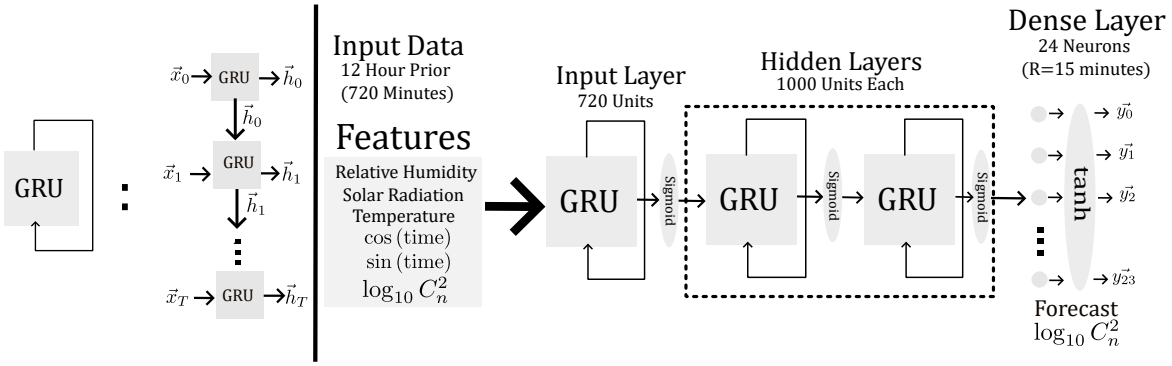

Figure 2. **Neural network architecture.** The network processes 12 hours of input data. The data is fed through a series of Gated Recurrent Unit (GRU) layers, allowing the network to learn long-term trends through time in the input series. The hidden state variable $\vec{h}$ is standardized using nonlinear activation layers at each step. The network outputs the forecast in a single shot, through the final fully connected dense layer.

root mean squared error, defined as $\overline{\text{RMSE}} = \frac{1}{N}\sqrt{\text{MSE}}$. This error is computed using the predicted and actual $\log_{10} C_n^2$ values, normalized according to Eq. (3). In the following, we report the results for 6 hours in advance with a 15-minute time resolution. However, we have observed adequate results for up to 12 hours in advance, even with a time resolution down to 1 minute.

Figure 3(a) and (b) plot the prediction of C_n^2 values over the above-mentioned periods. The plots are obtained by cascading 6-hour predictions sequentially in time. The colorscale encodes the accuracy on the final prediction: $\Delta(\text{RMSE}) = 1 - \text{RMSE}$, with higher values of Δ indicating better performances. A typical day features C_n^2 peaks at 10^{-14} during the afternoon, dropping in the evening to values approaching 10^{-16}, followed by a local peak overnight around 10^{-14}. The insets of both panels show representative examples of individual 6-hour predictions, generated from portions of the test set equally spaced in time. In both cases, the network performs very well in matching the actual C_n^2, with an average RMSE within the order of 10^{-2} ($\Delta \geq 0.90$). It also shows a certain degree of robustness to minor deviations from the trivial periodic trend. However, stronger variations in the feature trends represent a greater challenge for the network, in some cases with deviations within the order of 10^{-1} ($\Delta < 0.90$).

B. Numerical QKD experiment

We numerically investigate the performance of an 8-dimensional BB84 protocol, by simulating a realistic key exchange across the channel with increasing turbulence strengths. In particular, weak ($C_n^2 = 10^{-16}$), moderate ($C_n^2 = 10^{-15}$), and strong ($C_n^2 = 10^{-14}$) turbulence are investigated. The high-dimensional protocol exploits Laguerre-Gaussian (LG) spatial modes of light, carrying a discrete amount of orbital angular momentum (OAM) $\ell\hbar$ [41], encoding a qu*d*it of information. The Fourier-conjugate basis (ANGLE modes) is used as a Mutually Unbiased Basis (MUB). The explicit expression of these modes in the position representation is provided in Appendix C.

The parameters used in our simulated experiments are: $w_0 = 8$ cm, $\lambda = 810$ nm, $L = 5.4$ km, $D = 30$ cm, where w_0 is the beam waist at $z = 0$, λ is the operating wavelength, L is the channel length, and D is the receiver aperture. Figure 4(a) and (b) show the OAM and ANGLE modes in the sender plane ($z = 0$), halfway across the channel ($z = L/2$), and at the receiver end ($z = L$), with the opacity and the hue colorscale encoding the amplitude and the phase of the field, respectively. The $\ell = 0$ mode is removed from the OAM basis, due to non-negligible crosstalks with adjacent modes [14]. In our simulations, the effect of turbulence is modeled as a single phase mask located at $z = 0$, which is generated from a random combination of Zernike modes, where the contribution of each mode is extracted within the corresponding variance associated with the simulated C_n^2 [31]. However, a more general approach would require including multiple phase objects across the beam propagation, as discussed in Sec. II A. For each level of turbulence, we run 100 numerical experiments, from which the average crosstalk matrices are extracted.

Figure 5 provides a visualization of the effect of different turbulence levels on the input OAM beams, from weak (a) to moderate (b) to strong (c) turbulence. As a representative example, we plot the realization corresponding to the maximum error within the same turbulence strength, i.e., the one associated with the larger beam distortion. It is worth noticing that the statistical contribution of each Zernike mode decreases with the mode index [31]. Accordingly, low-rank aberrations such as tip and tilt typically dominate the beam dynamics,

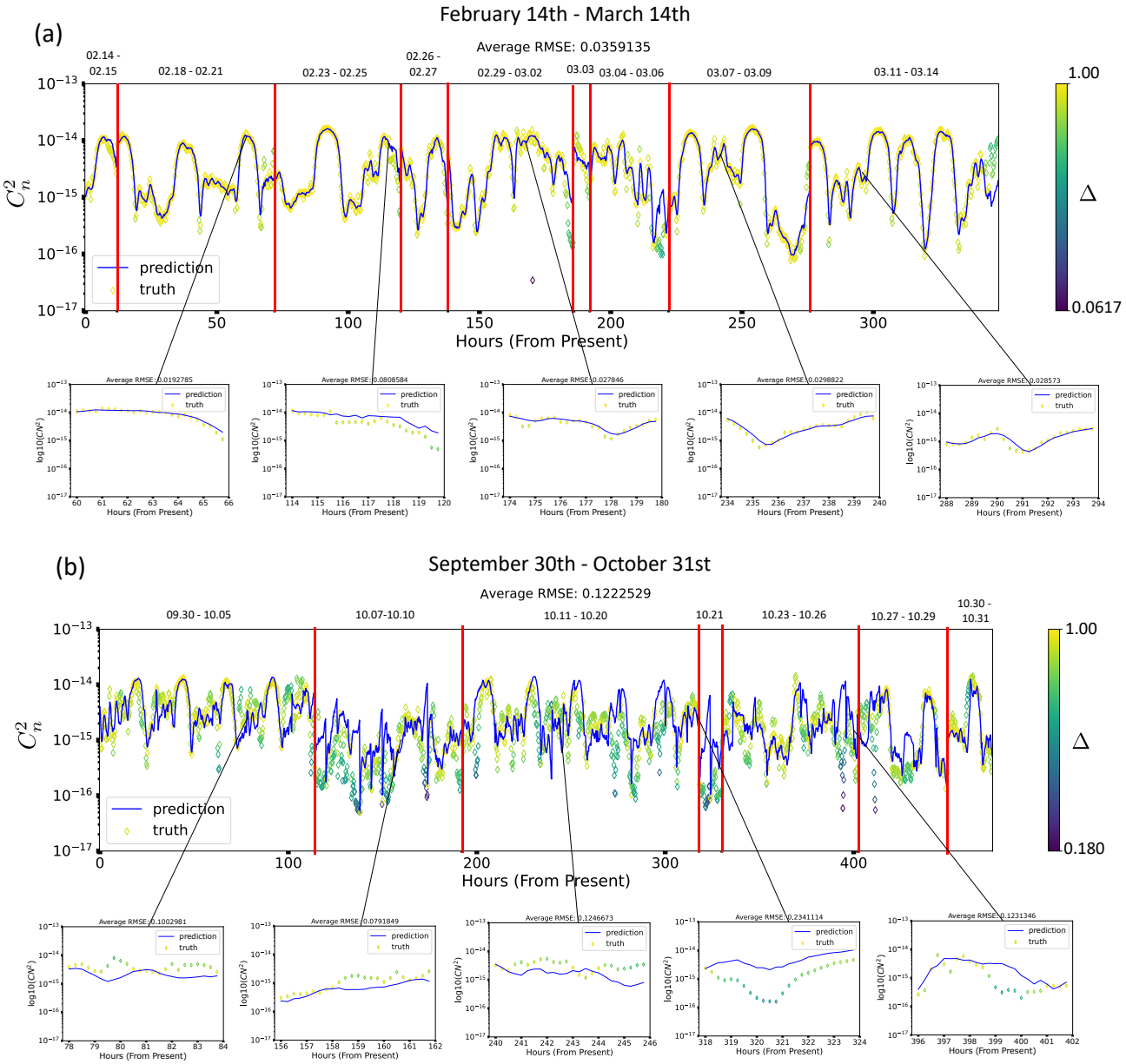

Figure 3. **Predictions on the test sets.** Network predictions on the months (a) from mid-February to mid-March 2024 and (b) of October. We have our trained model forecast 6 hours in the future, then cascade individual predictions to cover one month. Red lines are missing data from the scintillometer system. We also indicate the dates between these discontinuities in the dataset. A one-hour moving average is applied to the training set to remove high-frequency noise. The scatter points refer to the raw data (before the moving average is performed). The insets show examples of individual 6-hour predictions, equally spaced throughout the month. Excellent performances are observed on average, with larger deviations occurring in correspondence with strong feature variations.

resulting in an overall decentering effect. This is also evident in Fig. 6, showing the effect of the same aberrations on ANGLE modes.

The crosstalk integrals between the modes are plotted in Fig. 7. In the case of weak turbulence (a-d), both bases guarantee secure communications. Interestingly, for moderate (b-e) and strong (c-f) turbulence, the ANGLE basis proves more robust than OAM. This is ascribed to the concentration of optical power in a smaller region, associated with a reduced effective beam waist. More rigorously, the security of a certain basis across a

channel is quantified by the Quantum Dit Error Rate (QDER), which is the percentage of incorrect measurements in the shared key after the security verification. In 8 dimensions, a QDER greater than 24.7% results in the impossibility of guaranteeing secure communications as the key rate (given in Eq. (2)) will be negative. This value is related to the amount of information that can be transferred per photon sent through the channel. The average QDERs extracted from the numerical simulation are provided in Table I, where the information capacity is expressed in "bits per photon" (b/p). An ideal 8-dimensional channel would support 3 b/p of information capacity. As expected, secure communications can only be established in the weak-turbulence regime ($C_n^2 = 10^{-16}$).

C_n^2	OAM QDER	OAM b/p	ANG QDER	ANG b/p
10^{-16}	8.18%	1.72	2.33%	2.54
2×10^{-16}	17.8%	0.64	5.40%	2.09
5×10^{-16}	55.07%	0	21.77%	0.266
10^{-15}	77.00%	0	41.47%	0
10^{-14}	92.07%	0	51.96%	0

Table I. Average QDER and information capacity computed for the OAM and ANGLE (ANG) bases from 100 numerical realizations of different turbulence levels over the channel. Security is guaranteed only in the low-turbulence regime. Negative information capacity is reported as 0.

V. CONCLUSION

We employed a recurrent neural network to forecast future turbulence conditions within an optical channel. The accuracy of the predictions over significantly long periods demonstrates that our surrogate model has achieved a robust learning of the temporal variation of C_n^2 values correlated to relevant weather parameters. Moreover, we have shown how the predictions from TAROCCO can be used to foresee the error rate of a QKD experiment, by simulating a high-dimensional protocol within our free-space link. This result could also apply to QKD ground-to-satellite systems to optimize key exchange rates. While numerical simulations have only been performed for well-known spatial modes of light, future studies could address the performance of other encoding schemes for QKD under turbulence, such as vector beams and the time-frequency domain.

Scintillometer data acquisition will continue over the region of Ottawa, continually expanding the current dataset for enhanced training. Additionally, improved performance could be achieved by adopting an autoencoder architecture, similar to those used in machine translation [42, 43]. To compensate for limited data, it will also be interesting to explore data augmentation techniques, particularly those involving generative adversarial networks [44].

Acknowledgments. The authors would like to thank Alicia Sit for valuable discussions and for help purchasing the scintillometer system. The authors would also like to thank Nazanin Dehghan, Alessio D'Errico, and Ashlin Jacob for their help in setting up the scintillometer system. Finally, the authors would like to thank Environment and Climate Change Canada for providing us with the meteorological data. In particular, we appreciate the help of John Richard of Applied Climatology Services. 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.

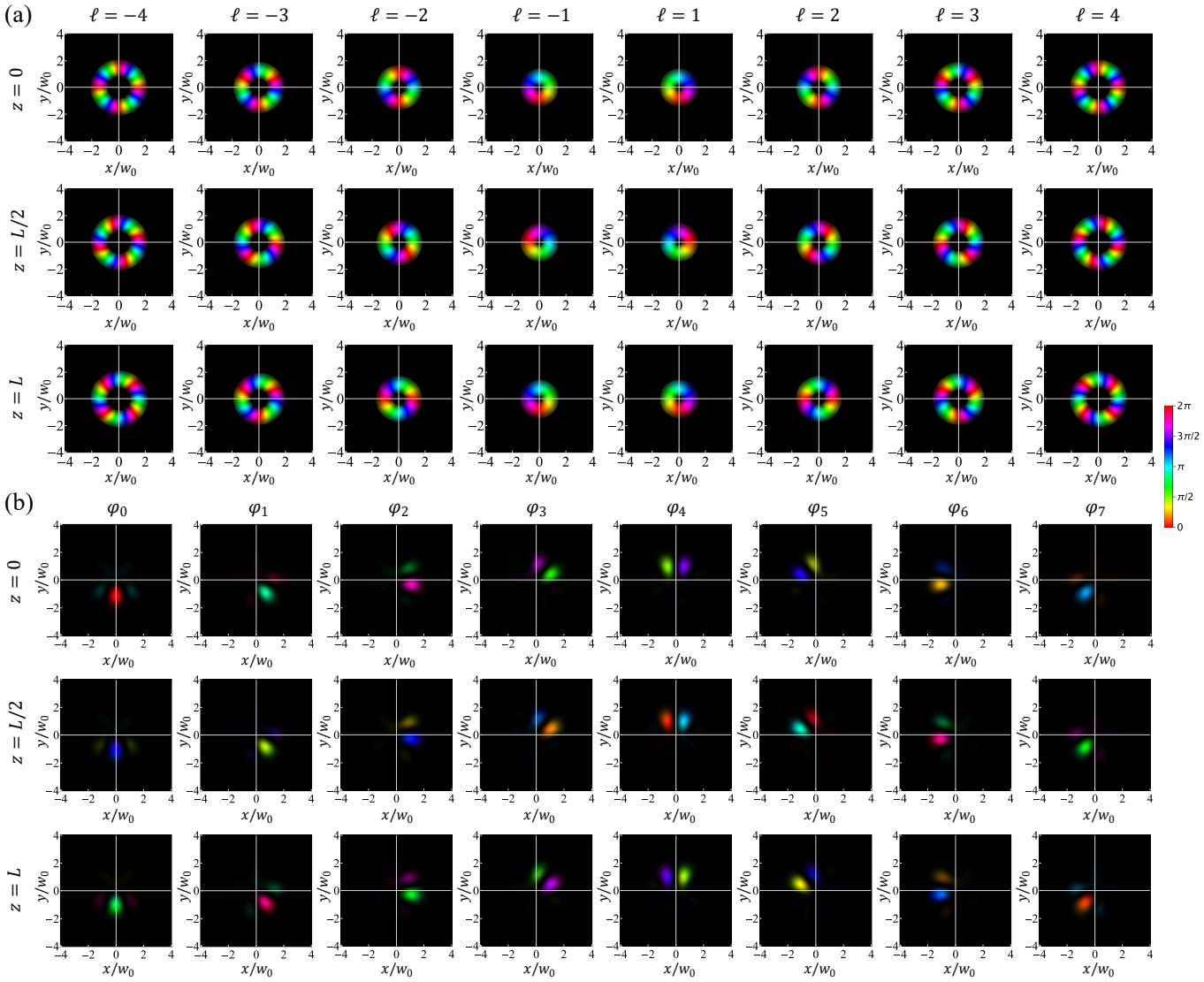

Figure 4. **8-dimensional QKD.** (a) 8-dimensional OAM space, spanning modes from $\ell = -4$ to $\ell = 4$, excluding $\ell = 0$. (b) ANGLE modes $\{\varphi_0, ..., \varphi_7\}$ provide a possible MUB for the high-dimensional protocol. The input field at $z = 0$, and the resulting field upon propagation at $z = L/2$ and $z = L$, with $L = 5.4$ km being the length of the free-space link, are provided for each mode. Opacity and hue colorscale encode the amplitude and the phase of the field, respectively.

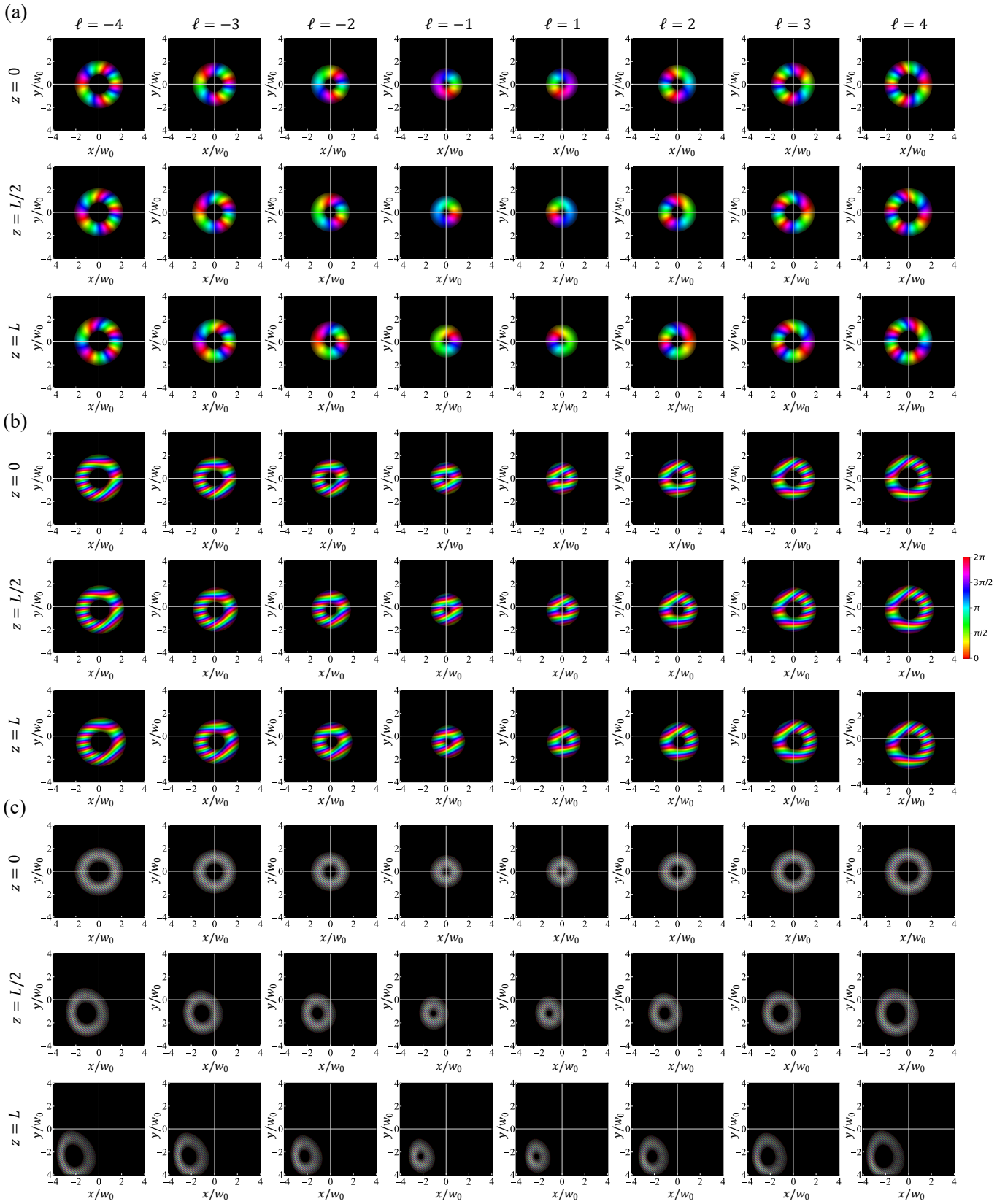

Figure 5. **Aberrated OAM modes.** Aberrations affect the OAM beam propagation over the channel. Different regimes are considered: (a) weak ($C_n^2 = 10^{-16}$), (b) moderate ($C_n^2 = 10^{-15}$), and (c) strong turbulence ($C_n^2 = 10^{-14}$). The panels refer to the realization yielding the least secure communication, i.e., the one minimizing the diagonal overlap integrals.

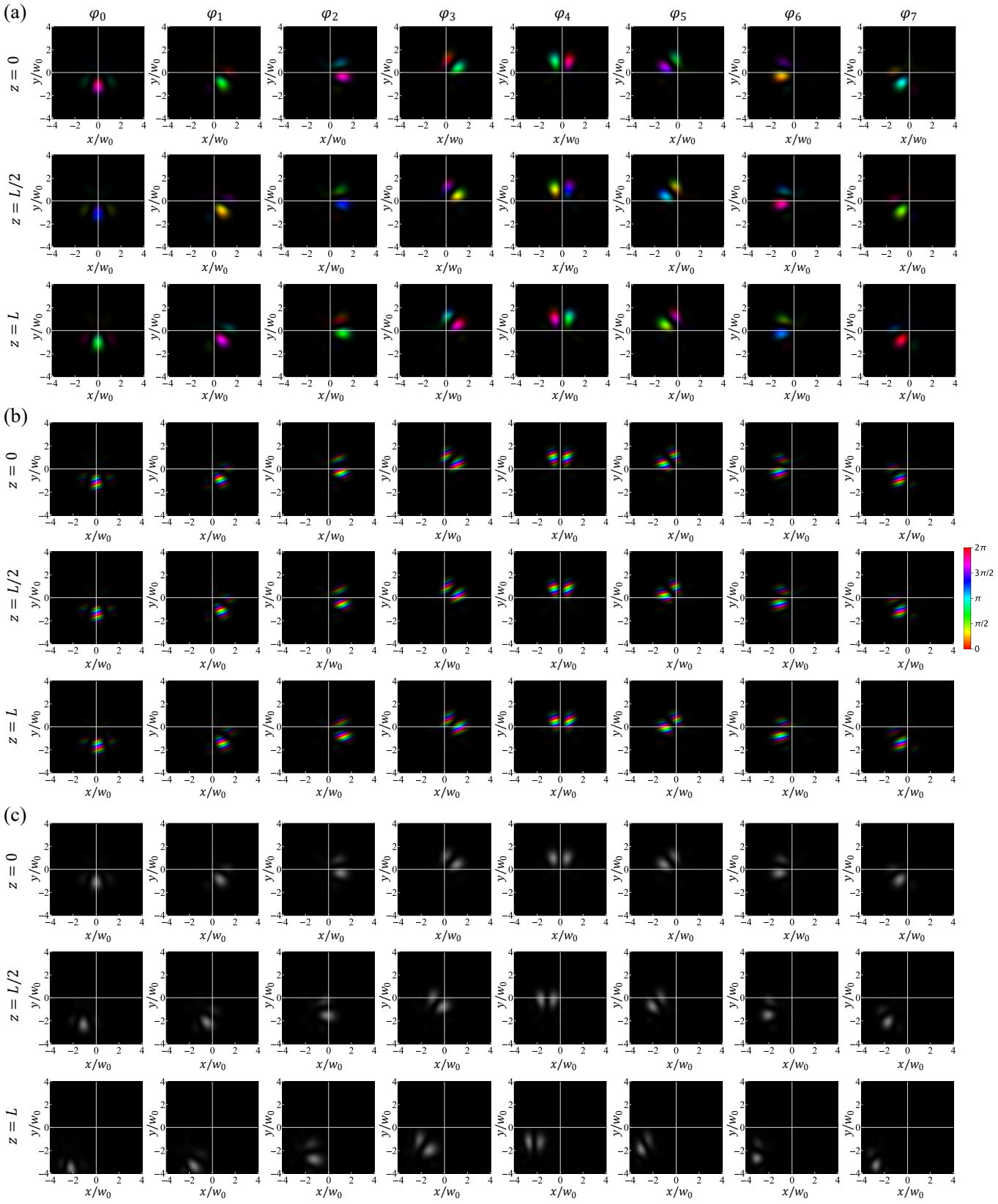

Figure 6. **Aberrated ANGLE modes.** Aberrations affect the ANGLE beam propagation over the channel. Different regimes are considered: (a) weak ($C_n^2 = 10^{-16}$), (b) moderate ($C_n^2 = 10^{-15}$), and (c) strong turbulence ($C_n^2 = 10^{-14}$). The panels refer to the realization yielding the least secure communication, i.e., the one minimizing the diagonal overlap integrals.

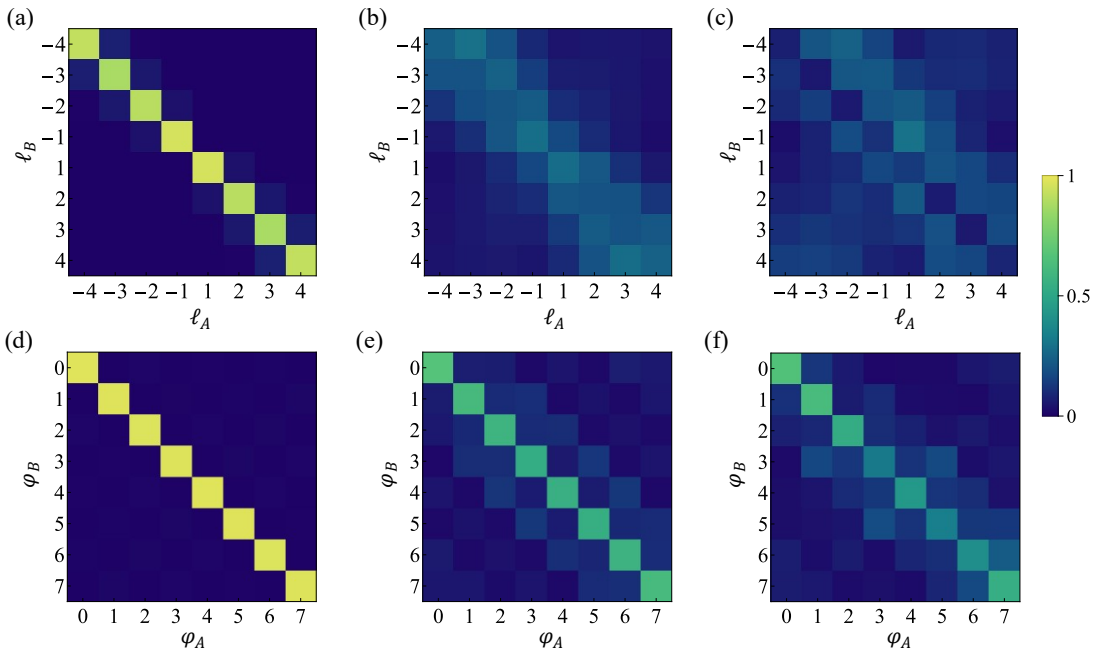

Figure 7. **Crosstalk matrix.** Average crosstalk integrals between different OAM and ANGLE modes across a turbulent channel. The average is computed over 100 realizations of (a-d) weak ($C_n^2 = 10^{-16}$), (b-e) moderate ($C_n^2 = 10^{-15}$), and (c-f) strong turbulence ($C_n^2 = 10^{-14}$). Each row of individual panels refers to the normalized average crosstalk over 100 independent realizations.

Appendix A: Permutation Feature Importance

The importance of each feature is assessed through the Permutation Feature Importance (PFI) technique [45]. Given a model trained with every possible input feature, we corrupt the dataset by permuting one of the features. The importance of each feature is quantified by evaluating the model on the corrupted dataset and comparing its performance with the original model:

$$I = \frac{\epsilon_{\text{perm}}}{\epsilon_{\text{orig}}}, \tag{A1}$$

where I is the feature importance, and ϵ_{perm} and ϵ_{orig} are the RMSE of the corrupted and original model, respectively. In addition to the input features indicated in Fig. 2, we also considered pressure (hPa), snow on ground (SOG, cm), wind speed (m/s), and the day according to the Julian Calendar. We then excecute PFI on the first 1000 examples of the dataset. For each feature, we repeat the permutation three times to minimize the effects induced by the variability of the permutation. The results are shown in Fig. 8. Prior values of C_n^2 appear to be the most important feature, followed by time, relative humidity, and solar radiation. This is in congruence with the analysis carried out in Ref. [20]. It must be noted that this kind of analysis tends to penalize the importance of correlated features, such as pressure and temperature [46]. To address this issue, we permute pressure, temperature, humidity, and wind speed simultaneously, effectively considering their importance together [47]. Indeed, increased values for importance were reported.

Appendix B: Training Hyperparameters

The network is trained and validated using data spanning from July 2023 to March 2024. We list the model hyperparameters in Table II. One month is removed from the original dataset and used for testing (cf. Sec. IV A). Figure 9 illustrates the partitions of the complete dataset into training, validation, and test datasets, for the two case studies reported in Fig. 3.

The training process is realized using the Tensorflow library [48], and model optimization is handled using the Adam optimizer [49]. Training is carried out on the *Narval* supercluster using a NVidia A100SXM4 GPU. An adaptive training strategy is used, whereby the learning rate is reduced by a factor of 0.1 if the validation loss does not decrease significantly within 15 epochs (this number is referred to as *patience*). The number of hours of prior data is kept fixed at 12. Altogether, training is completed in approximately 5 hours. We have also explored longer inputs of 18, 24, and 30 hours. However, no significant reduction in the validation loss was observed.

We also considered a fully connected neural network, with 2 hidden layers of 1000 neurons separated by ReLU activation layers. Here, the input layer admits a flattened dataset where the first 6 entries represent the input features of the first time step. However, the validation error of our flagship model at convergence is three orders of magnitude smaller than this architecture.

Table II. Hyperparameters.

Hours of Prior Data	12 Hours
Forecast Length	6 Hours
Input Time Resolution	1 Minute
Output Time Resolution	15 Minutes
Batch Size	32
Train-Validation Split *(with October)*	85:15
Train-Validation-Test Split *(no October)*	75:15:10
Initial Learning Rate	10^{-4}
Number of Epochs at Convergence *(with October)*	149
Number of Epochs at Convergence *(no October)*	262
Patience	15 Epochs
Reduction Factor	0.1
Training Error at Convergence *(with October)*	1.2×10^{-4}
Training Error at Convergence *(no October)*	7.2×10^{-5}
Validation Error at Convergence *(with October)*	1.6×10^{-4}
Validation Error at Convergence *(no October)*	1.3×10^{-4}

Appendix C: OAM and ANGLE modes of light

The 8-dimensional QKD protocol explored in Sec. IV B leverages the MUBs provided by a set of LG modes and the corresponding Fourier-transformed basis. LG modes are labeled by two integers ℓ and p, representing the azimuthal (OAM) and radial index, respectively. Our protocol only relies on the OAM content of the beam, hence we set $p = 0$ for all the LG modes. In the position basis, their expression reads

$$\langle x, y, z|\ell\rangle = N_\ell \frac{w_0}{w(z)} \left(\frac{r\sqrt{2}}{w(z)}\right)^{|\ell|} e^{-r^2/w^2(z)} L^0_{|\ell|}\left(\frac{2r^2}{w^2(z)}\right) e^{-ik\frac{r^2}{2R(z)}} e^{-i\ell\phi} e^{i\psi(z)}, \tag{C1}$$

where N_ℓ is a normalization constant, $r = \sqrt{x^2+y^2}$ and $\phi = \arctan(y/x)$ are the radial and azimuthal coordinates, respectively, and L^p_ℓ are the generalized Laguerre polynomials. The beam waist $w(z)$, the radius of curvature $R(z)$ and the Gouy phase $\psi(z)$ can be determined

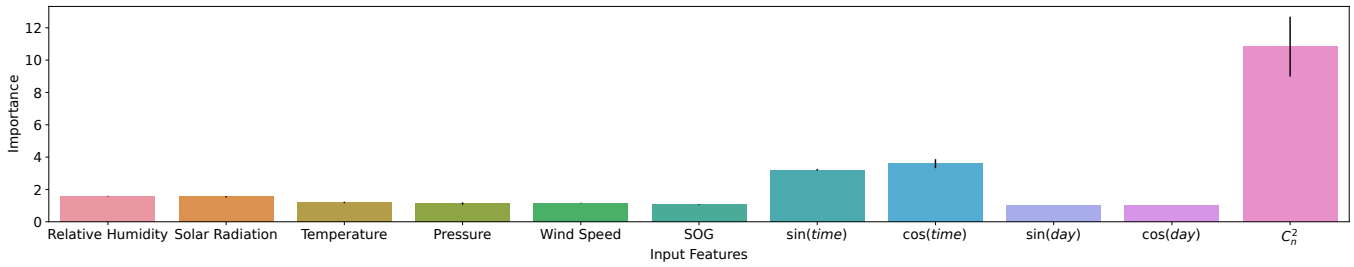

Figure 8. **Importance of input features.** For each input feature, the mean and standard deviation (error bars) of the importance is computed over three repeated permutations.

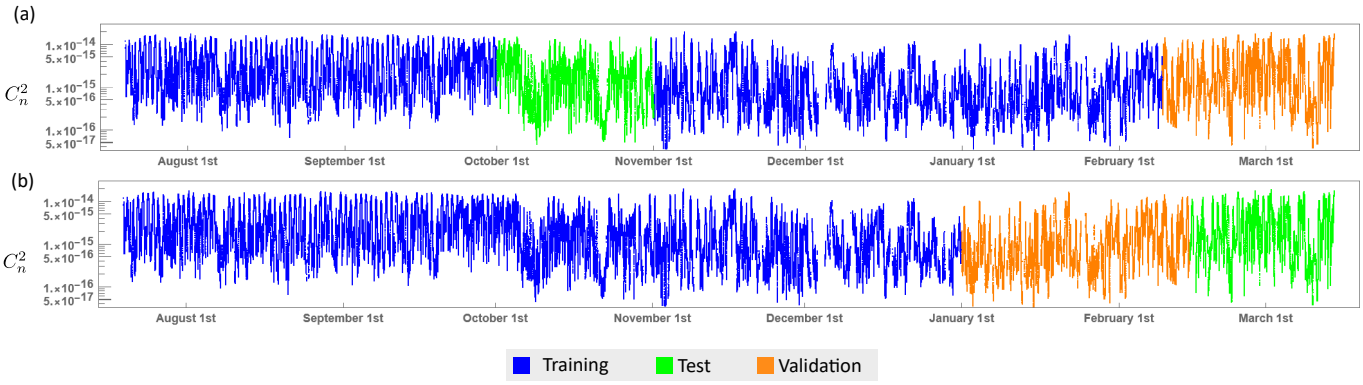

Figure 9. **Partitions of the complete dataset.** (a) The month of October is selected as test set, and an 85:15 train:validation split is applied to the remaining dataset. (b) A 75:15:10 train:validation:test split is applied to the complete dataset, which corresponds to a test set spanning from mid-February to mid-March (cf. Sec. IV A).

from [50]:

$$w(z) = w_0\sqrt{1+\frac{z^2}{z_R^2}}; \tag{C2a}$$

$$R(z) = z\left(1+\frac{z_R^2}{z^2}\right); \tag{C2b}$$

$$\psi(z) = (|\ell|+1)\arctan\frac{z}{z_R}, \tag{C2c}$$

where $z_R = \pi w_0^2/\lambda$ is the Rayleigh range.

The conjugate basis, referred to as the ANGLE basis, is obtained as

$$|\varphi_j\rangle = \frac{1}{\sqrt{d}}\sum_\ell |\ell\rangle\, e^{2\pi i j g(\ell)/d}, \tag{C3}$$

where $d = 8$, the summations runs from $\ell = -d/2$ to $\ell = d/2$ excluding the $|\ell = 0\rangle$ mode, and $g(\ell) = d/2 + (\ell-1)\Theta(\ell) + \ell\Theta(-\ell)$, with Θ the Heaviside step function.

[1] J.-L. Kong, X.-M. Fan, X.-B. Jin, T.-L. Su, Y.-T. Bai, H.-J. Ma, and M. Zuo, Agronomy **13**, 625 (2023).
[2] D. Lazos, A. B. Sproul, and M. Kay, Renew. Sustain. Energy Rev. **39**, 587 (2014).
[3] E. Kendon, N. Roberts, H. Fowler, and et al., Nat. Clim. Change **4**, 570 (2014).
[4] B. Merz, C. Kuhlicke, M. Kunz, M. Pittore, A. Babeyko, D. N. Bresch, D. I. V. Domeisen, F. Feser, I. Koszalka, H. Kreibich, F. Pantillon, S. Parolai, J. G. Pinto, H. J. Punge, E. Rivalta, K. Schröter, K. Strehlow, R. Weisse, and A. Wurpts, Rev. Geophys. **58**, e2020RG000704 (2020).
[5] F. Roddier, in *Prog. Optics*, Vol. 19 (Elsevier, 1981) pp. 281–376.
[6] X. Zhu and J. Kahn, IEEE Trans. Commun. **50**, 1293 (2002).
[7] N. Leonhard, G. Sorelli, V. N. Shatokhin, C. Reinlein, and A. Buchleitner, Phys. Rev. A **97**, 012321 (2018).
[8] J. C. Wyngaard, Annu. Rev. Fluid Mech. **24**, 205 (1992).
[9] A. N. Kolmogorov, Proc. R. Soc. Lond. A **434**, 9 (1991).
[10] J. A. Anguita, M. A. Neifeld, and B. V. Vasic, Appl. Opt. **47**, 2414 (2008).
[11] G. A. Tyler and R. W. Boyd, Opt. Lett. **34**, 142 (2009).
[12] C. J. Pugh, J.-F. Lavigne, J.-P. Bourgoin, B. L. Higgins,

and T. Jennewein, Adv. Opt. Technol. **9**, 263 (2020).
[13] J. Zhao, Y. Zhou, B. Braverman, C. Liu, K. Pang, N. K. Steinhoff, G. A. Tyler, A. E. Willner, and R. W. Boyd, Opt. Express **28**, 15376 (2020).
[14] L. Scarfe, F. Hufnagel, M. F. Ferrer-Garcia, A. D'Errico, K. Heshami, and E. Karimi, arXiv:2311.13041.
[15] R. N. Lanning, M. A. Harris, D. W. Oesch, M. D. Oliker, and M. T. Gruneisen, Phys. Rev. Appl. **16**, 044027 (2021).
[16] M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, K. E. Stoltenberg, J. F. Morris, M. Bareian, M. A. Harris, D. W. Oesch, M. D. Oliker, M. B. Flanagan, B. T. Kay, J. D. Schiller, and R. N. Lanning, Phys. Rev. Appl. **16**, 014067 (2021).
[17] F. S. Binkowski, Atmos. Environ. **13**, 247 (1979).
[18] A. Rafalimanana, C. Giordano, A. Ziad, and E. Aristidi, in *International Conference on Space Optics—ICSO 2020*, Vol. 11852 (SPIE, 2021) pp. 1856–1866.
[19] Y. Wang and S. Basu, in *Laser Communication and Propagation through the Atmosphere and Oceans III*, Vol. 9224 (SPIE, 2014) pp. 300–307.
[20] M. G. Grose and E. A. Watson, Appl. Opt. **62**, 3370 (2023).
[21] K. Bi, L. Xie, H. Zhang, X. Chen, X. Gu, and Q. Tian, Nature **619**, 533 (2023).
[22] C. Bodnar, W. P. Bruinsma, A. Lucic, M. Stanley, J. Brandstetter, P. Garvan, M. Riechert, J. Weyn, H. Dong, A. Vaughan, J. K. Gupta, K. Tambiratnam, A. Archibald, E. Heider, M. Welling, R. E. Turner, and P. Perdikaris, arXiv:2405.13063.
[23] In Italian, Tarocco means tarot cards, which are used in fortune telling.
[24] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, Proc. Natl. Acad. Sci. **113**, 13648 (2016).
[25] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, New J. Phys. **16**, 113028 (2014).
[26] M. P. J. Lavery, C. Peuntinger, K. Günthner, P. Banzer, D. Elser, R. W. Boyd, M. J. Padgett, C. Marquardt, and G. Leuchs, Sci. Adv. **3**, e1700552 (2017).
[27] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, Optica **4**, 1006 (2017).
[28] V. I. Tatarski, *Wave propagation in a turbulent medium* (Courier Dover Publications, 2016).
[29] L. Burger, I. Litvin, and A. Forbes, S. Afr. J. Sci. **104**, 129 (2008).
[30] M. Born and E. Wolf, *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light*, 7th ed. (Cambridge University Press, 1999).
[31] R. J. Noll, J. Opt. Soc. Am. **66**, 207 (1976).
[32] H. C. Ward, Meas. Sci. Technol. **28**, 064005 (2017).
[33] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
[34] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[35] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[36] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[37] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, IEEE Open J. Commun. Soc. **2**, 2049 (2021).
[38] O. Amer, V. Garg, and W. O. Krawec, IEEE Trans. Aerosp. Electron. Syst. **36**, 30 (2021).
[39] Scintech, "Advanced atmospheric sensing," `https://www.scintec.com/`.
[40] Government of Canada, `https://climate.weather.gc.ca/index_e.html`.
[41] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Phys. Rev. A **45**, 8185 (1992).
[42] C. E. A. Mohamed Akram Zaytar, Int. J. Comput. Appl. **143**, 7 (2016).
[43] I. Sutskever, O. Vinyals, and Q. V. Le, in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2*, NIPS'14 (MIT Press, Cambridge, MA, USA, 2014) p. 3104–3112.
[44] B. K. Iwana and S. Uchida, Plos one **16**, e0254841 (2021).
[45] A. Altmann, L. Toloşi, O. Sander, and T. Lengauer, Bioinformatics **26**, 1340 (2010).
[46] T. Altmann and G. Casalicchio, *Limitations on Interpretable Machine Learning Methods* (2019).
[47] T. Parr, K. Turgutlu, C. Csiszar, and J. Howard, "Beware default random forest importances," (2018), `https://explained.ai/rf-importance/index.html`.
[48] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, M. Isard, Y. Jia, R. Jozefowicz, L. Kaiser, M. Kudlur, J. Levenberg, D. Mané, R. Monga, S. Moore, D. Murray, C. Olah, M. Schuster, J. Shlens, B. Steiner, I. Sutskever, K. Talwar, P. Tucker, V. Vanhoucke, V. Vasudevan, F. Viégas, O. Vinyals, P. Warden, M. Wattenberg, M. Wicke, Y. Yu, and X. Zheng, "TensorFlow: Large-scale machine learning on heterogeneous systems," (2015), software available from tensorflow.org.
[49] D. P. Kingma and J. Ba, arXiv:1412.6980.
[50] M. Padgett and L. Allen, Opt. Commun. **121**, 36 (1995).

Author Contributions. FDC, LS and EK conceived the idea. LS collected and prepared the scintillometer data. TJ developed the neural network architectures. FDC performed numerical simulations of QKD under turbulence. TJ, LS, and FDC wrote the first version of the manuscript. FB, MK, KH, and EK supervised the project.

3

Adaptive Optics for Abberation Correction

3.1 Adaptive Optics

The issue of atmospheric turbulence is not new. Astronomers have long gazed up at the stars through their telescopes and have seen scintillations, and temporal variations due to the turbulence. In 1953 the first proposal for an adaptive optics-based correction stage was proposed by Horace W. Babcock [51]. Although the technology of the time was insufficient for the purpose of real-time correction, this proposal had all the required components of an adaptive optics correction system, namely a wavefront sensing technique in a closed feedback loop with a wavefront correction stage. Since the 1990s, technology for real-time measurement and correction of wavefronts has been developed, and the technique of adaptive optics is often used in ground-based astronomical telescopes [52].

3.1.1 Wavefront Sensing

The Shack-Hartmann wavefront sensor (SHWFS) used in our adaptive optics system is used. This type of sensor consists of a CCD camera placed in the image plane of an array of lenses

with equal focal length. Recall that in optics, a lens may have been seen to perform a Fourier transform on an input beam, mapping the momentum of an input wave to a position in the focal plane of the lens. By sampling the momentum of the wavefront at many points of a beam, one can reconstruct point-by-point the overall wavefront shape of the input beam. The wavefront is then deconstructed in terms of Zernike polynomials, and the difference between the expected reference beam and the measured one is calculated [53].

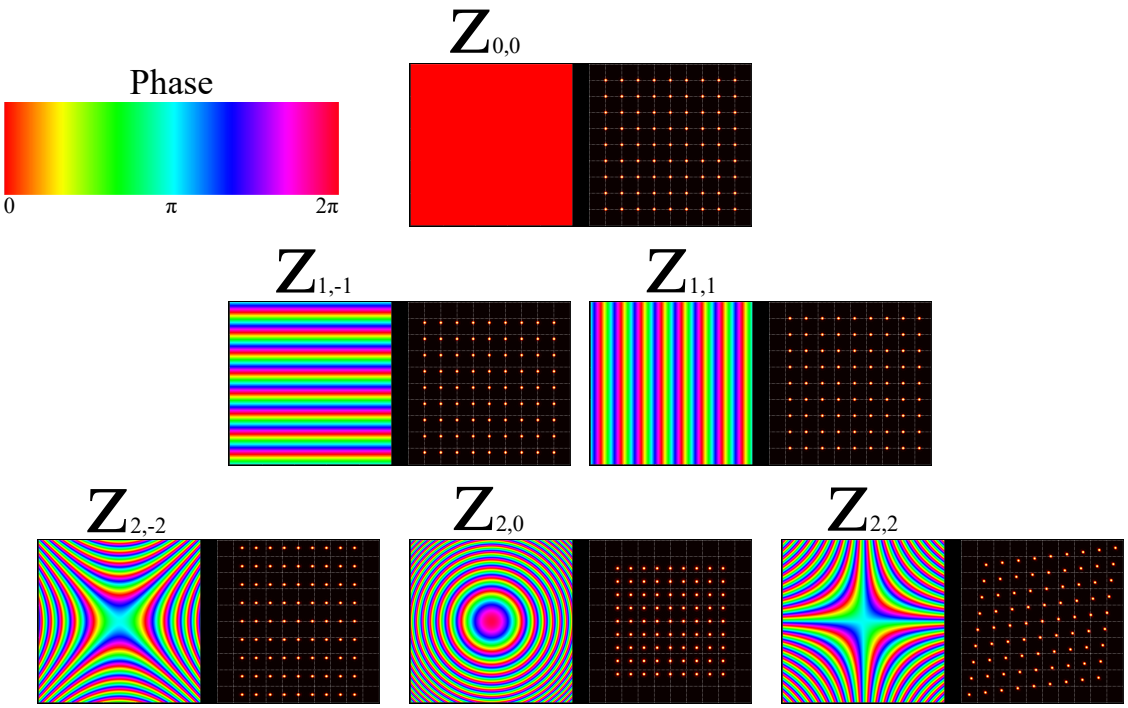

Figure 6: Phase profiles of the first six Zernike modes and their simulated effects on a Shack-Hartmann Wavefront Sensor. For each plot, the left side shows the wavefront corresponding to one Zernike mode. Importantly, these functions are defined in a circular coordinate system, and only a square subsection is being displayed. The wavefront variation is shown using the displayed false colorscale. The right side of each plot represents the image captured by the camera sensor following the microlens array of the wavefront sensor for each Zernike mode.

To implement this technique, the channel must contain a reference beam, with a known phase profile. The best choice for this beam is typically an expanded Gaussian beam, overfilling the aperture of the wavefront sensor in order to approximate a plane wave with a flat phase profile and uniform intensity. Through propagation in the channel, the reference beam will

accumulate a spatially varying phase profile that can be measured using the wavefront sensor.

A perfect plane wave input will appear on the wavefront sensor's camera as an array of points in a perfect grid, as shown in Figure 6, $Z_{0,0}$. Tip and tilt aberrations (Fig. 6, $Z_{1,-1}, Z_{1,1}$) will cause the grid of intensity spots to shift up and down, or left and right, respectively. Astigmatic aberrations (Fig. 6, $Z_{2,-2}$,$Z_{2,2}$) stretch the grid in one direction, and compress in the other. Focus (Fig. 6, $Z_{2,0}$) acts similar to a lens, either bringing all of the points together or spreading them apart.

The exact wavefront sensor used in our experiments is the ALPAO SH-CMOS FAST. This wavefront sensor has a 10×10 array of lenses utilizing a sensor that is capable of operation up to 22 kHz within the visible range. It is capable of measuring a tip/tilt wavefront deviation up to 9μm, corresponding to a capacity to correct for phase aberrations up to 15 wavelengths in strength for the 633 nm light used in the experiment.

3.1.2 Deformable Mirror

If the wavefront sensor is the eyes of the AO system, then the deformable mirror is the body and hands. This piece of equipment has many types of constructions, but the one in our system consists of a thin dielectric mirror on one side with many electromagnetic actuators on the other. These actuators which span the entire mirror are capable of adjusting, point-by-point, the optical path length of a beam that is reflected. In effect, this provides each actuator with control of the relative phase of the reflected light as compared to the other actuators. By applying the

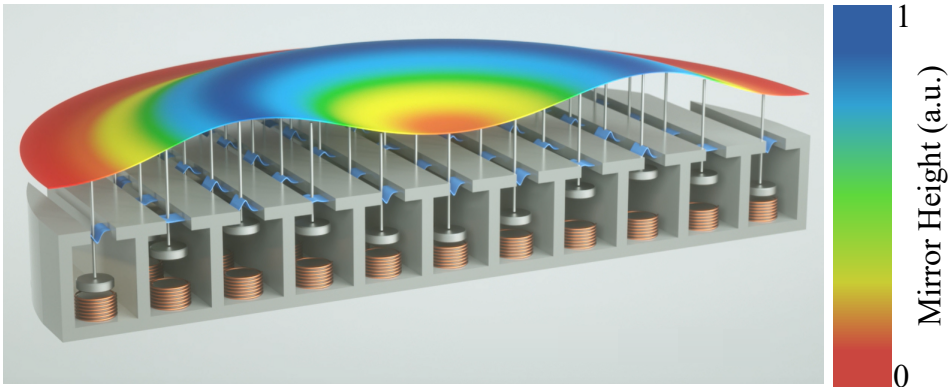

Figure 7: Render of a deformable mirror: This rendering of our ALPAO deformable mirror shows the inner workings. Each piston is controlled by an electromagnet that may push on the membrane that is the mirror. Here, the mirror is given false colour to represent the relative height of the membrane.

conjugate phase of the aberrations measured from the reference beam by the Shack-Hartmann wavefront sensor, the deformable mirror is capable of removing the overall phase effects of the turbulence in the channel. This operation requires that the mirror is both capable of making precise sub-wavelength adjustments of the position of the actuators, as well as operating faster than the frequency at which the phase structure of the turbulence is changing [54]. Immediately following the point-by-point optical path length changes from the mirror, the light is imaged on the SHWFS without any further propagation. Importantly, this means that this technique will not necessarily recover the original intensity distribution of the input beam. Scintillation effects are therefore not correctable with this technique.

Our adaptive optics system uses the ALPAO DM 97-25 as its deformable mirror. It has 97 electromagnetic actuators arranged in an 11×11 layout, with the corners cut. Each actuator can move to a given position with an average root mean squared error of 7 nm allowing for effective phase corrections to a precision of 1.1% of a beam with wavelength 633 nm.

3.2 Properties of the Fourier Basis with OAM.

BB-84 QKD requires two MUB, the first MUB, which is called the logical basis, typically consists of the natural modes created by the choice of degree of freedom. If using OAM of light for encoding, the logical basis will simply be the LG modes each carrying integer OAM. These are shown as $|\psi_i\rangle$ in Figure 8. The most obvious MUB to use for quantum key

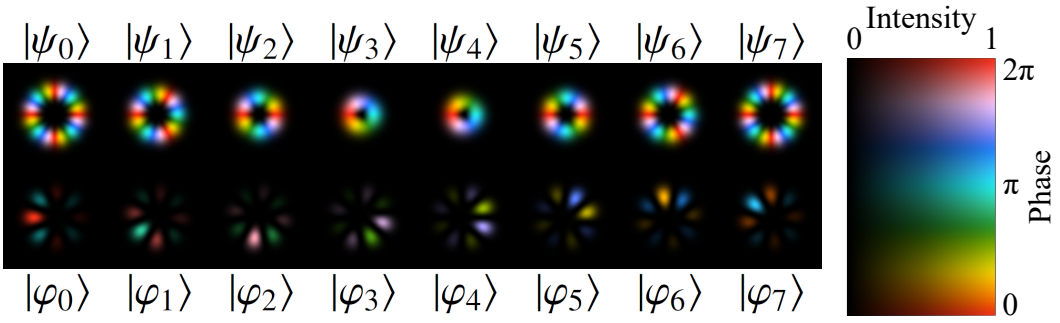

Figure 8: Intensity and Phase distributions of the logical (OAM) basis and Fourier or Angle (ANG) basis for an 8 dimensional QKD protocol. The hue is representative of the relative phase of the wavefront at each point. Note that the intensity of the angle basis is concentrated in a small area while the intensity of the logical basis is much more spread out.

distribution is the basis which corresponds to the quantum Fourier transform of the states as

defined in Eq. (10), since it can be defined in any dimension. These states are shown as $|\phi_j\rangle$ in Figure 8. These states are much more concentrated in space, with their intensities spanning far less space than the states in the logical basis. This in effect reduces their "effective beam waist" D_{eff}. This reduced effective diameter will, in effect, reduce the amount of turbulence experienced by such a propagation mode, as D_{eff}/r_0 will then be reduced.

More than experiencing reduced turbulence, the angle basis does not span the full size of the deformable mirror, nor even a significant portion of it. Because of the concentrated intensity, the adaptive optics system will only be able to use a portion of it's corrective power on these beams. This means that while this basis may be less affected by turbulence, it will also be less effective when used in turbulence with adaptive optics.

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 ϕ is the azimuthal coordinate and ℓ 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 trade-off 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 free-space QKD, the use of adaptive optics has been mainly explored theoretically [37, 38], while experiments antecedent to this work have not demonstrated a significant improvement of the error rate [39].

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

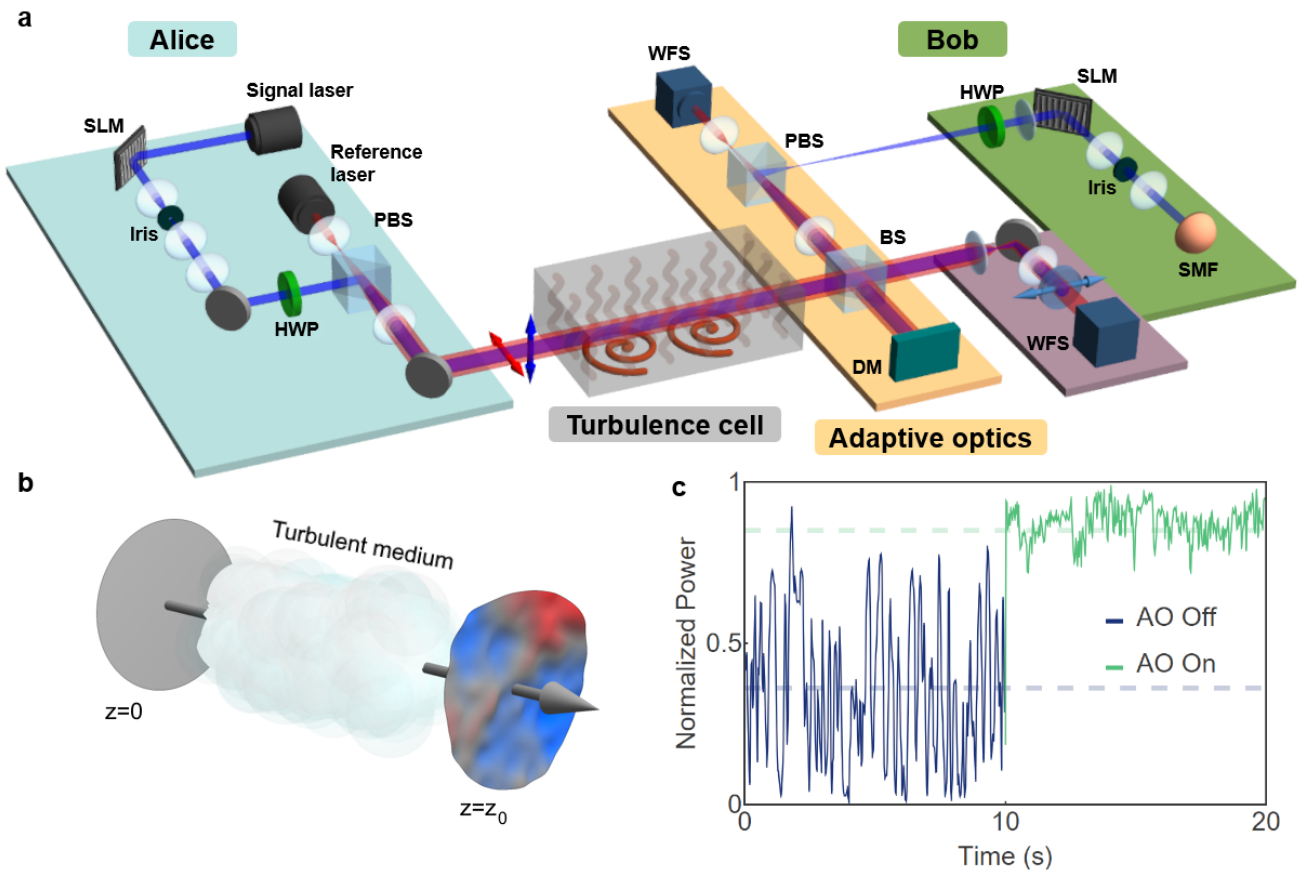

FIG. 1. **High-dimensional quantum communication with adaptive optics through a turbulent channel**. **a** Experimental setup used to investigate the corrective action of a fast adaptive optics (AO) system (from ALPAO [20]) on structured optical beams after propagation through a turbulent channel. A 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 the Supplementary materials.

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 significant 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

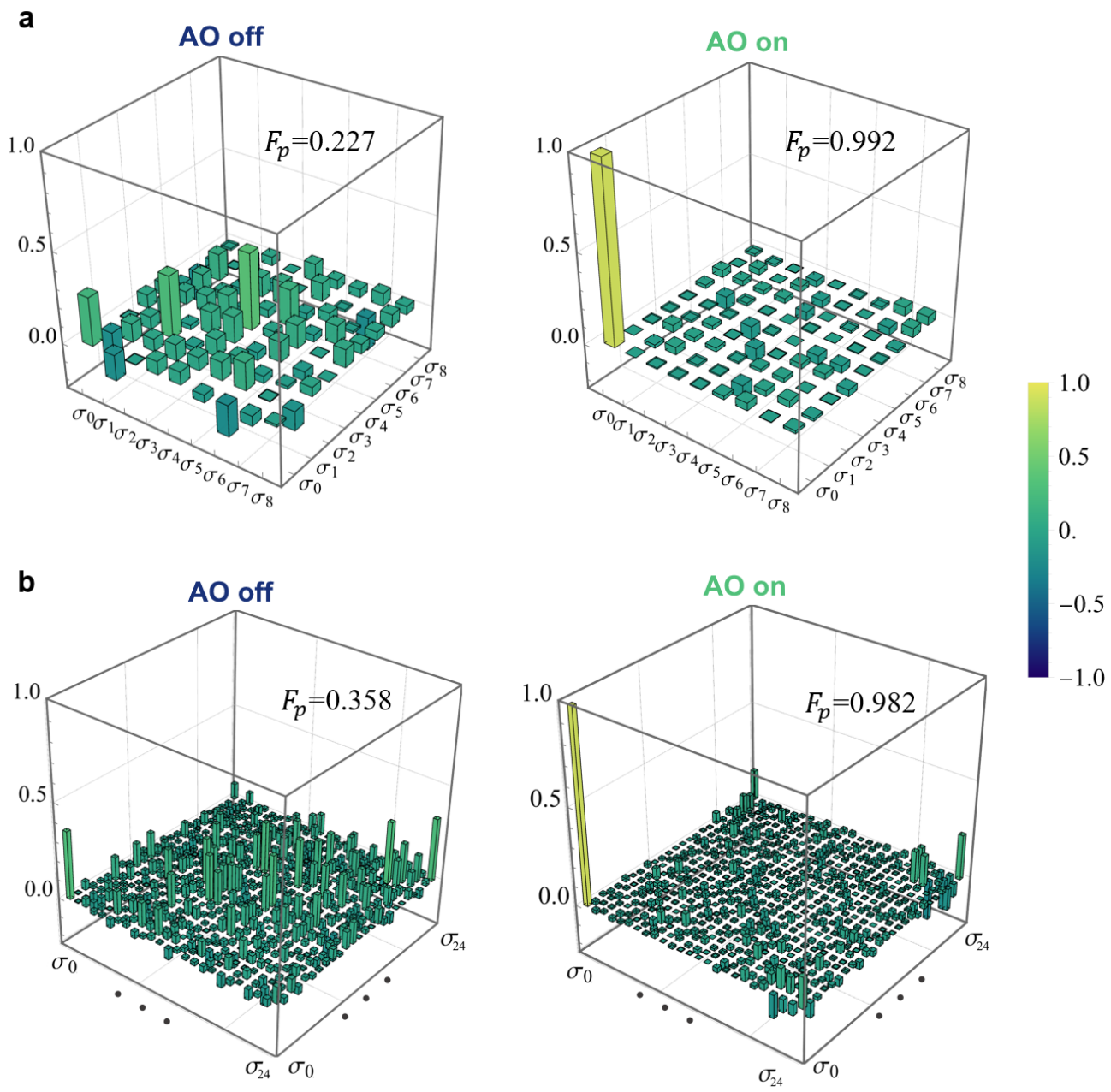

FIG. 2. **Channel Process Tomography for** $d = 3, 5$**.** The real part of the process matrix of the channel transmission is shown for dimension 3 with the AO system as (**a**) non-active and (**b**) active when going through the turbulence cell. We perform the process tomography using mutually unbiased bases measurements following the methods outlined in [40] (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.

the same frequency with orthogonal polarisation states. The first component, a classical signal referred to as the *reference* beam, possesses a Gaussian profile, which has been expanded to approximate a flat wavefront that completely covers our deformable mirror, 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 [41]. A quantum process $\mathcal{E}$ can be represented using the process matrix χ_{mn} to describe how input states ρ_{in} are transformed to output states ρ_{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 χ_{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 α 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 [42]. 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

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

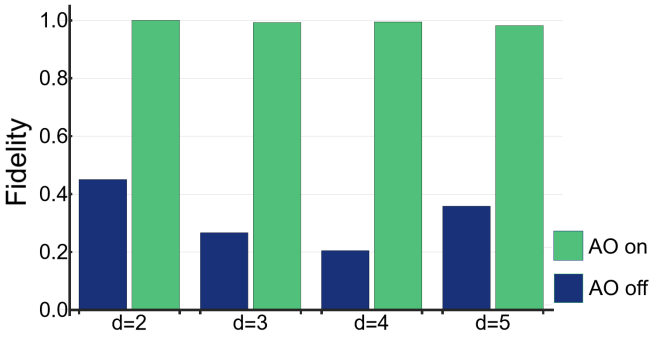

FIG. 3. **Channel Fidelity for OAM-based QKD system.** The process fidelity between the tomographically measured turbulent channel with AO off (blue) and AO on (green) are measured for a QKD channel of $d = 2$, $d = 3$, $d = 4$ and $d = 5$. Turbulence 'depolarizes' the channel significantly, i.e. introduces 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.

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 [40].

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 [43],

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

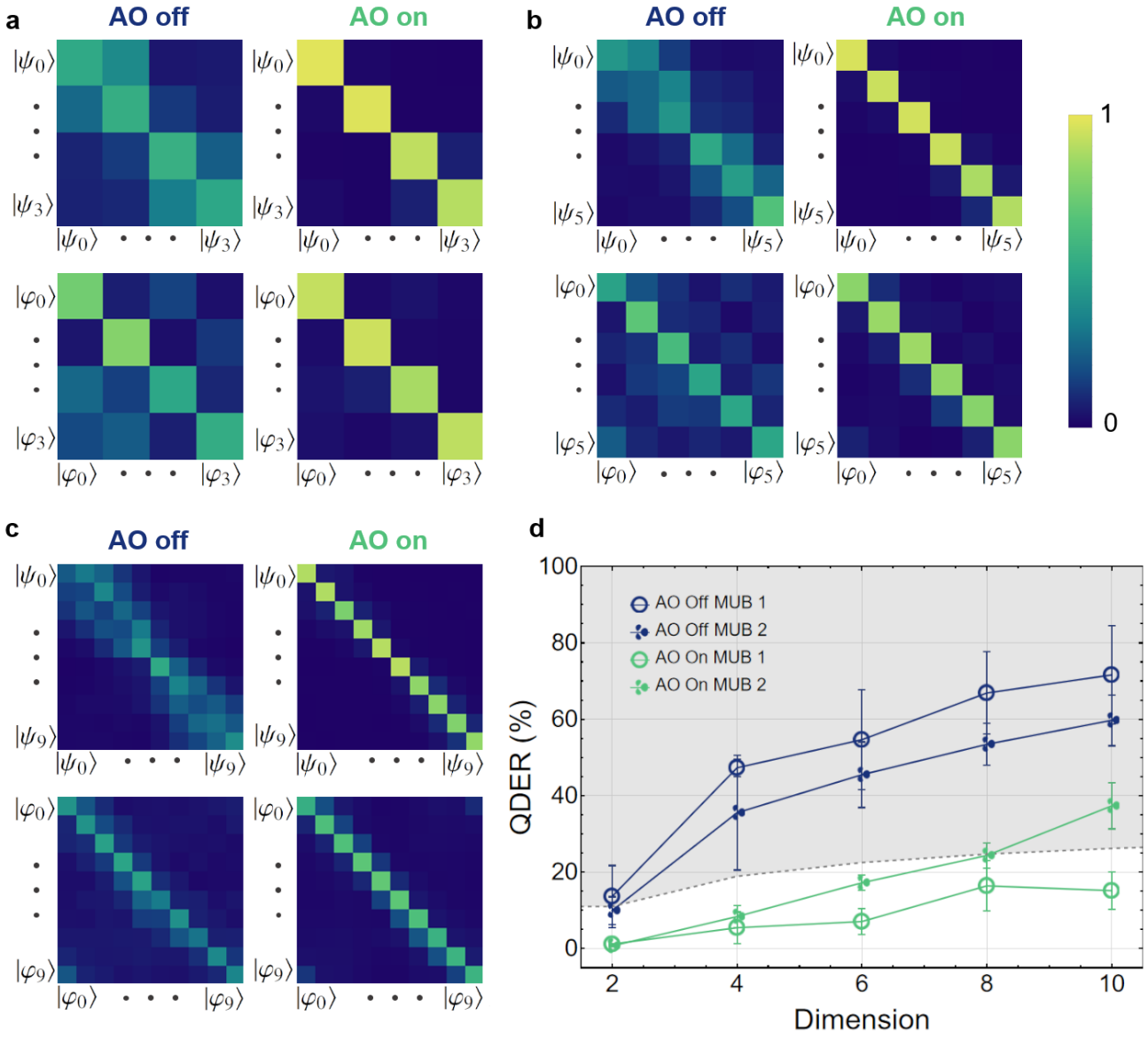

FIG. 4. **Crosstalk and quantum dit error rate.** The probability of detection on each basis for both bases when going through a turbulent channel for **a** $d = 4$, **b** $d = 6$, and **c** $d = 10$. **d** Plot of the QDER as calculated from the probability of detection matrices for the cases of adaptive 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 $d = 10$.

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 $R = 0$.

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 ℓ, where ℓ 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.

Utilising Eq. 3, we calculate the sifted key rate that can be achieved after the implementation of AO in our channel shown in Table I. We show the key rate in a BB84 protocol using a 50/50 balance of each basis, however it must be noted that one can use a weighted protocol in which the logical basis is utilized nearly all of the time, bringing the key rate R asymptotically close to its key rate. [44].

Dimension	$R(Q)$ OAM	$R(Q)$ ANG	$R(Q)$ 50/50
2	0.818	0.885	0.851
4	1.22	0.905	1.06
6	1.52	0.461	0.991
8	0.792	0.032	0.412
10	1.14	0	0

TABLE I. Sifted key rate calculated from experimental results for all dimensions, given in bits per sifted photon.

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 as 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 [45]. 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 [46–48]. 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 [46]. 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 [39]. 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 $d = 5$ [39]. 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 con-

text 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 showing a potential doubling of the resultant key-rate for polarization, or time-bin QKD where the Gaussian most likely used mode. 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.

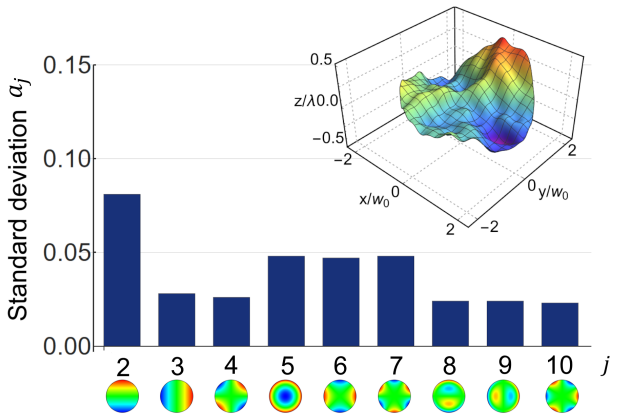

FIG. 5. **Decomposition of the turbulence on the Zernike basis.** Standard deviation of the first nine coefficients a_j of the Zernike decomposition after propagation through the turbulent cell. The WFS reports the turbulence decomposition in the Zernike polynomials basis as a function of time. The inset 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. 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). URL `https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012`.

[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. *Phys. Rev. A* **61**, 062308 (2000). URL `https://link.aps.org/doi/10.1103/PhysRevA.61.062308`.

[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). URL `http://www.osapublishing.org/optica/abstract.cfm?URI=optica-4-9-1006`.

[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. *Phys. Rev. Lett.* **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. *Phys. Rev. A* **97**, 043847 (2018). URL https://link.aps.org/doi/10.1103/PhysRevA.97.043847.

[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] Leonhard, N., Sorelli, G., Shatokhin, V. N., Reinlein, C. & Buchleitner, A. Protecting the entanglement of twisted photons by adaptive optics. *Physical Review A* **97**, 012321 (2018).

[38] Sorelli, G., Leonhard, N., Shatokhin, V. N., Reinlein, C. & Buchleitner, A. Entanglement protection of high-dimensional states by adaptive optics. *New Journal of Physics* **21**, 023003 (2019).

[39] 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).

[40] Fernández-Pérez, A., Klimov, A. & Saavedra, C. Quantum process reconstruction based on mutually unbiased basis. *Physical Review A* **83**, 052332 (2011).

[41] Nielsen, M. A. & Chuang, I. L. *Quantum computation and quantum information* (Cambridge university press, 2010).

[42] Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Annals of Physics* **191**, 363–381 (1989).

[43] Bouchard, F. *et al.* Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018). URL https://doi.org/10.22331/q-2018-12-04-111.

[44] Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology* **18**, 133–165 (2005).

[45] Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Optics Express* **26**, 22563–22573 (2018).

[46] Fried, D. L. Optical resolution through a randomly inhomogeneous medium for very long and very short exposures. *J. Opt. Soc. Am.* **56**, 1372–1379 (1966).

[47] 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).

[48] Ageorges, N. & Dainty, C. *Laser guide star adaptive optics for astronomy*, vol. 551 (Springer Science & Business Media, 2013).

4

Conclusion

This work has reviewed and covered all of the necessary information to understand two works that contribute to the progress of performing high-dimensional quantum key distribution in free-space channels. We have investigated the turbulence characteristics of a specific free-space channel over the city of Ottawa, On. With the data collected, we have developed a neural network-based tool to make predictions on the quality of the channel up to 12 hours in advance. This tool can be used not only by us to perform QKD at optimal times in our channel, but can be used by others so long as they have sufficient historical weather and turbulence data. This will be an essential tool for future ground-satellite QKD as nearby ground stations may be able to predict which one will have a better chance of achieving successful key distribution on a given satellite pass. In the long term, this technology can aid large-scale quantum networks predict outages and optimally route their communications.

Beyond predicting the turbulence conditions at a future time, we have investigated the corrective capabilities of an adaptive optics system on a turbulent high-dimensional QKD channel in real-time. We have shown that in our lab-scale environment, the application of turbulence resulted in a channel over which QKD could not be performed. We found that the implementation of a fast adaptive optics system by the receiver was able to reduce the error rate below the required threshold for performing secure communications. Additionally, we find that even a

low-dimensional free-space QKD channel using Gaussian beams will benefit from an adaptive optics system. We foresee future free-space QKD experiments implementing this technology, and will continue to investigate its use in quantum communications and sensing.

Through both works, we have learned about the respective behaviour of two MUB, the logical basis and angle basis, constructed with OAM in turbulence. The difference in performance of these modes both with turbulence and the Adaptive Optics system is interesting and has introduced us to many questions; These are not the only MUB, and MUB are not the only possible choice of modes. How well behaved are the other MUBs spanning the $(d + 1)$ set for different dimensions? Can we create a basis that is optimal for propagation through turbulence without AO? Can we create a basis that is optimal for use with AO? These are all questions that we are looking to address in future work. We are currently in the process of developing a QKD protocol using a secondary basis that is not MUB. This protocol may provide an easier method to prepare and measure each individual state, making QKD easier experimentally.

In our upcoming experiments, we will seek to combine these works, by using our 5.4 km free-space link to investigate the performance of the adaptive optics system in a real-world environment. We will take advantage of the neural network tool each day to determine whether or not to conduct free-space experiments that night. Eventually we will look to perform secure quantum communications in real-time over our channel, making steps towards a true quantum network in Ottawa.

For the future of our neural network tool, we plan on using our model to help other Canadian research groups investigating free-space QKD. In the coming years, the Canadian Space Agency will launch the Quantum Encryption and Science Satellite (QEYSSat), which will be a technological test-bed for ground-satellite quantum communications. We plan on distributing our model to each ground station involved in the project, each of which will have a local weather station monitoring the meteorological conditions. With so much data, we will develop models to optimally determine which ground station should communicate with the satellite at any given time, taking into account factors such as network traffic, the volume of stored secure keys between each station, and predicted turbulence conditions at each station. This will be a large step towards the full-scale deployment of quantum networks.

Appendix A: Supplementary information for "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

CONTENTS

Section 1. TURBULENCE ANALYSIS

A. 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 (ρ, ϕ) 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.

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.

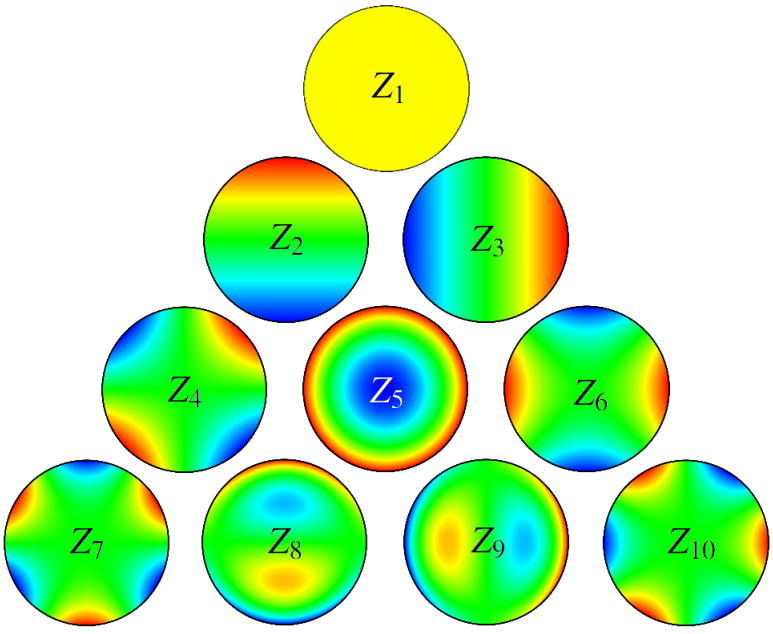

Figure S1. The First 10 Zernike polynomials, with arbitrary unit strength ranging from -1 to 1 ordered vertically by values of n and horizontally by the values of m.

B. 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]

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

where λ corresponds to the beam's wavelength while θ 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.

C. 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 11×11 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 16×16 micro lenses 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.

D. Extended Gaussian coupling

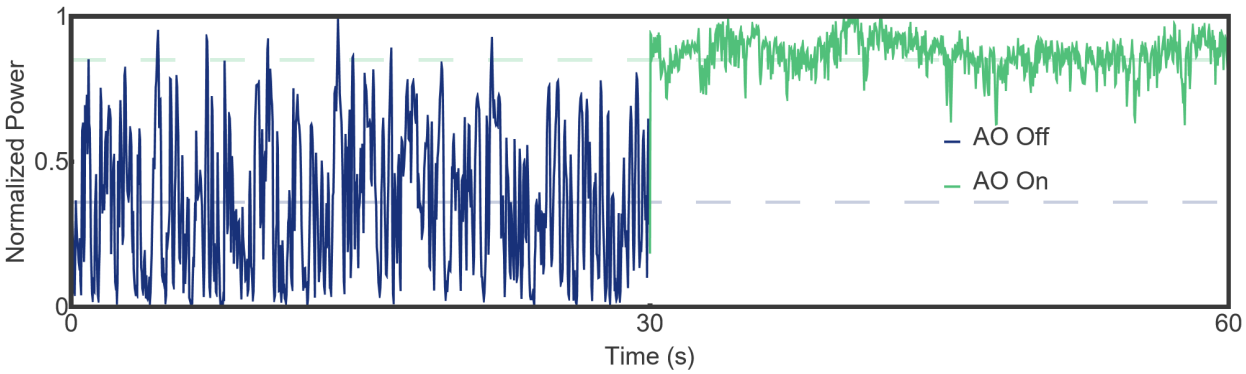

Figure S2. Extended figure showing 60 seconds of a Gaussian beam coupling into a single mode fibre through the active turbulent cell. After 30 seconds without any corrections, the AO system is activated.

E. 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**.

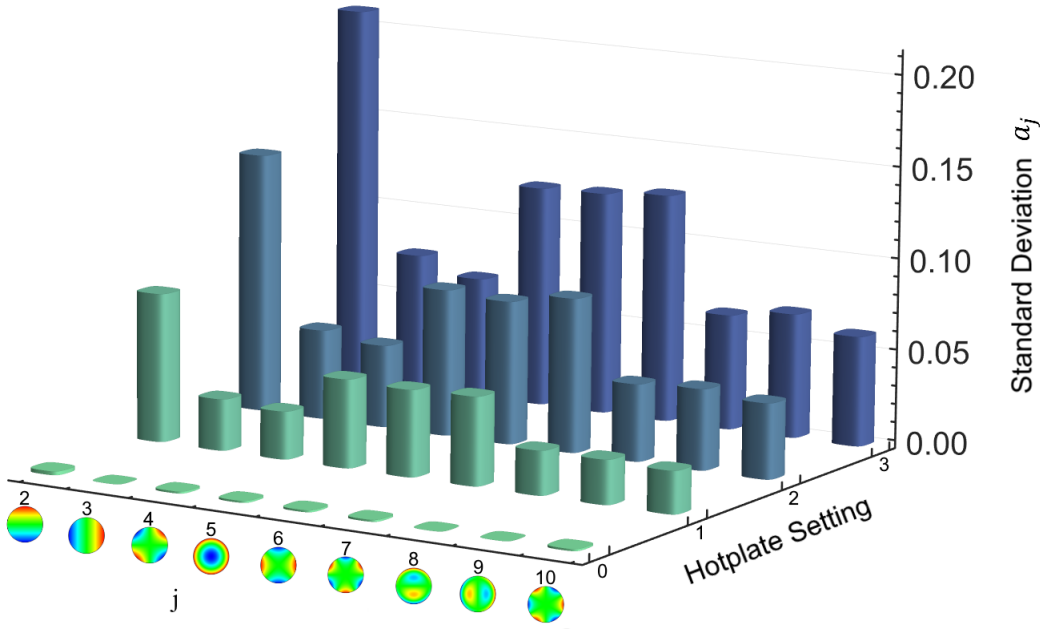

Figure S3. Standard deviations of the first nine coefficients a_j of the Zernike decomposition upon propagation through the turbulent cell as a function of the temperature of the hotplate. Here, the value of 0 corresponds to the hotplate completely off, while 3 stands for the highest temperature possible.

Section 2. 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

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

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 $\Pi_t^\alpha := |\psi_t^\alpha\rangle \langle\psi_t^\alpha|$, the state resulting from the action of the turbulent channel on a basis element is

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

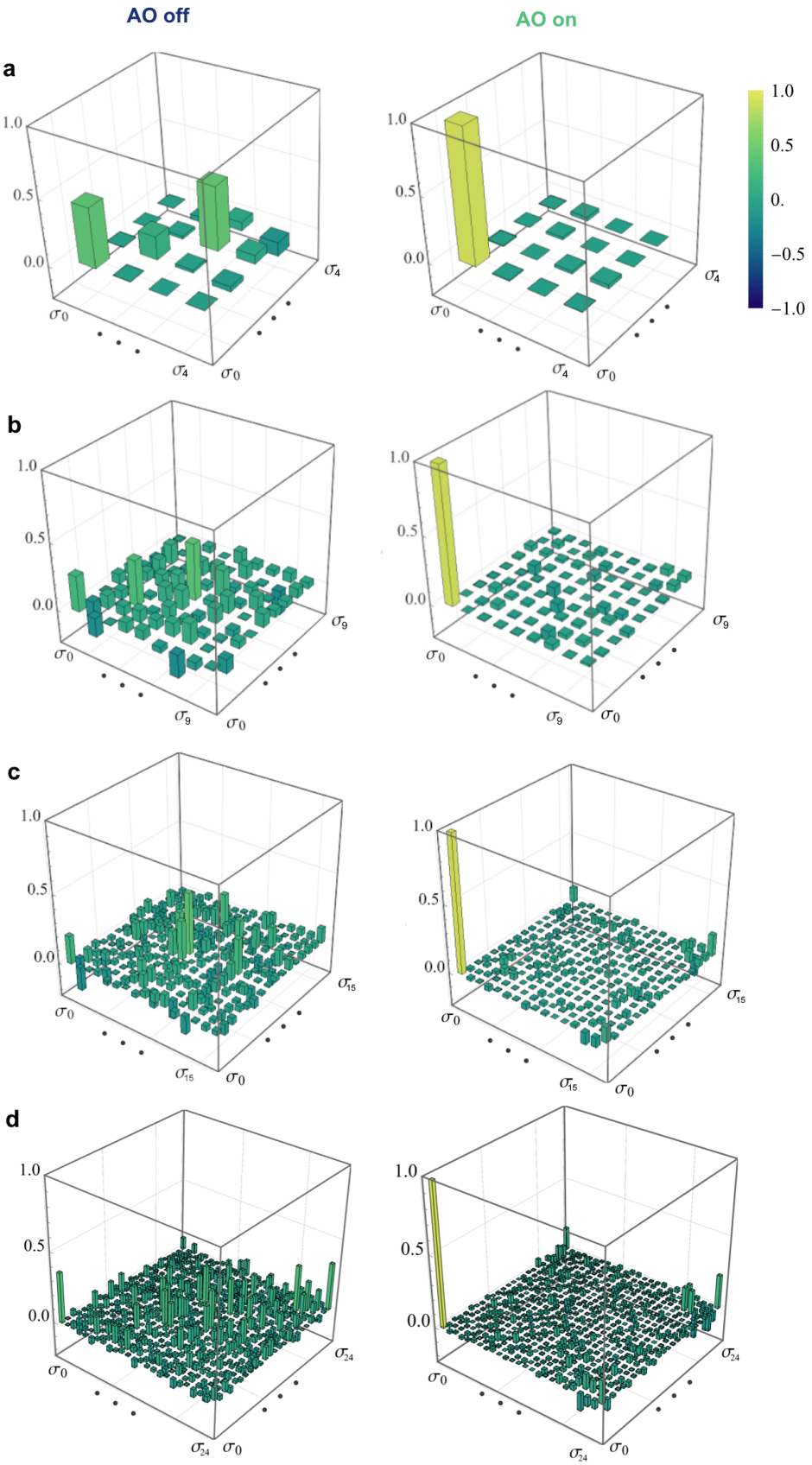

Figure S4. Process matrices for all dimensions. **a** $d = 2$, **b** $d = 3$, **c** $d = 4$, **d** $d = 5$

where σ_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 χ_{mn}. The Fidelity between the experimentally reconstructed process matrix χ_{exp} and a theoretical one χ_{th} is

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

In our case χ_{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:

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

Section 3. CROSSTALK & QBER

A. 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 consists 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.

B. 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 $|\langle\psi_j|\psi_i\rangle|^2$ is normalized by the total power measured from one incoming state,

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

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. Each individual measurement is performed over 30 ms, and repeated 100 times to give a reasonable sampling of the turbulence.

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.

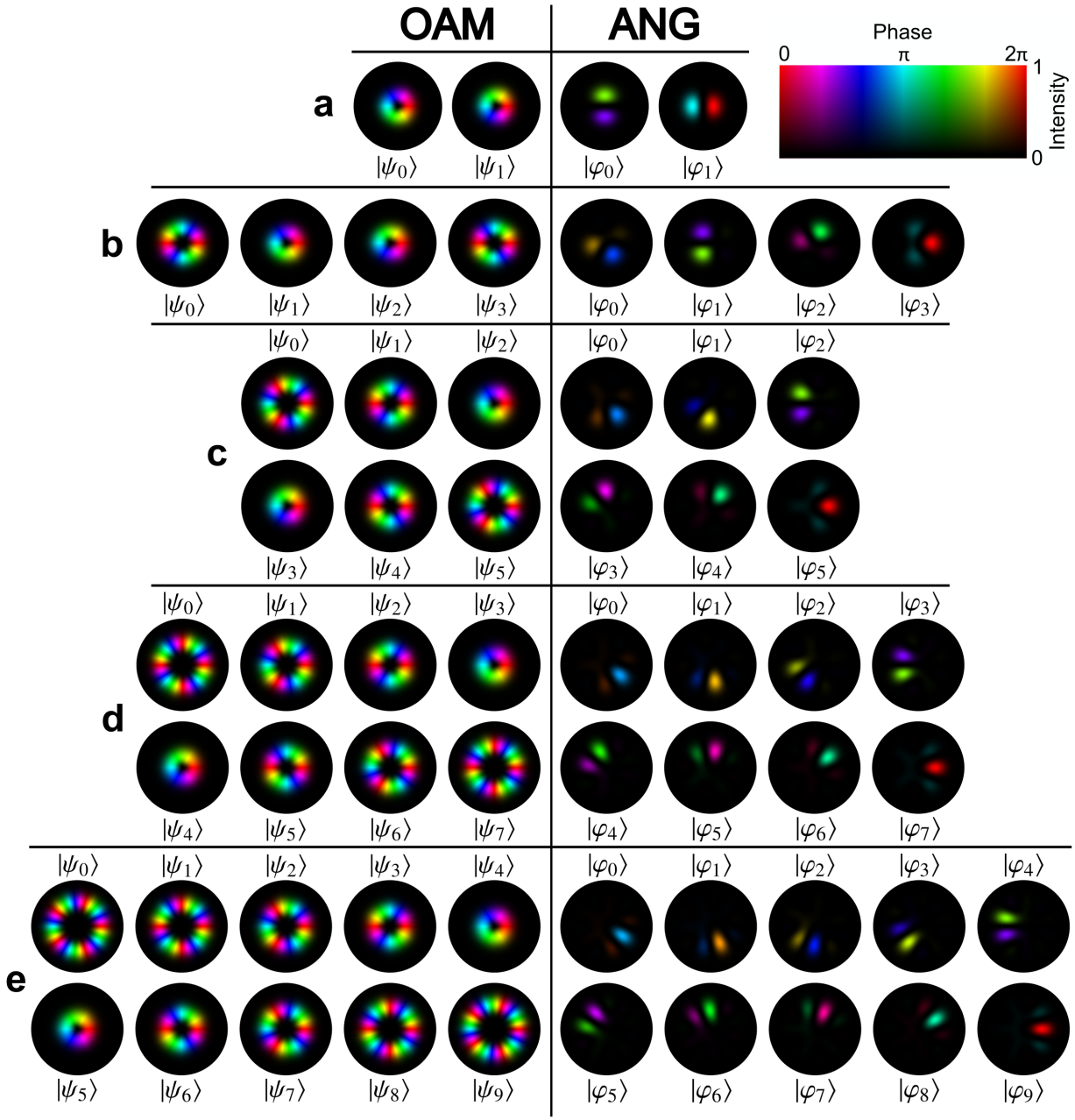

Figure S5. All modes utilized in the crosstalk measurements. The logical basis consisting of OAM modes is shown on the left, while the angular basis is shown on the right for the same dimension. **a** $d = 2$, **b** $d = 4$, **c** $d = 6$, **d** $d = 8$, **e** $d = 10$

C. QBER 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 bit error rate, we subtract the fidelity from the theoretical best performance of 1. This gives a QBER for the basis in a dimension d.

$$\text{QBER} = 1 - \sum_{j=i=0}^{d-1} C_{ij}/d = 1 - \text{Tr}[C_{ij}/d] \tag{S10}$$

We calculate the QBER for each of the bases, in each dimension. We find that our AO system is capable of

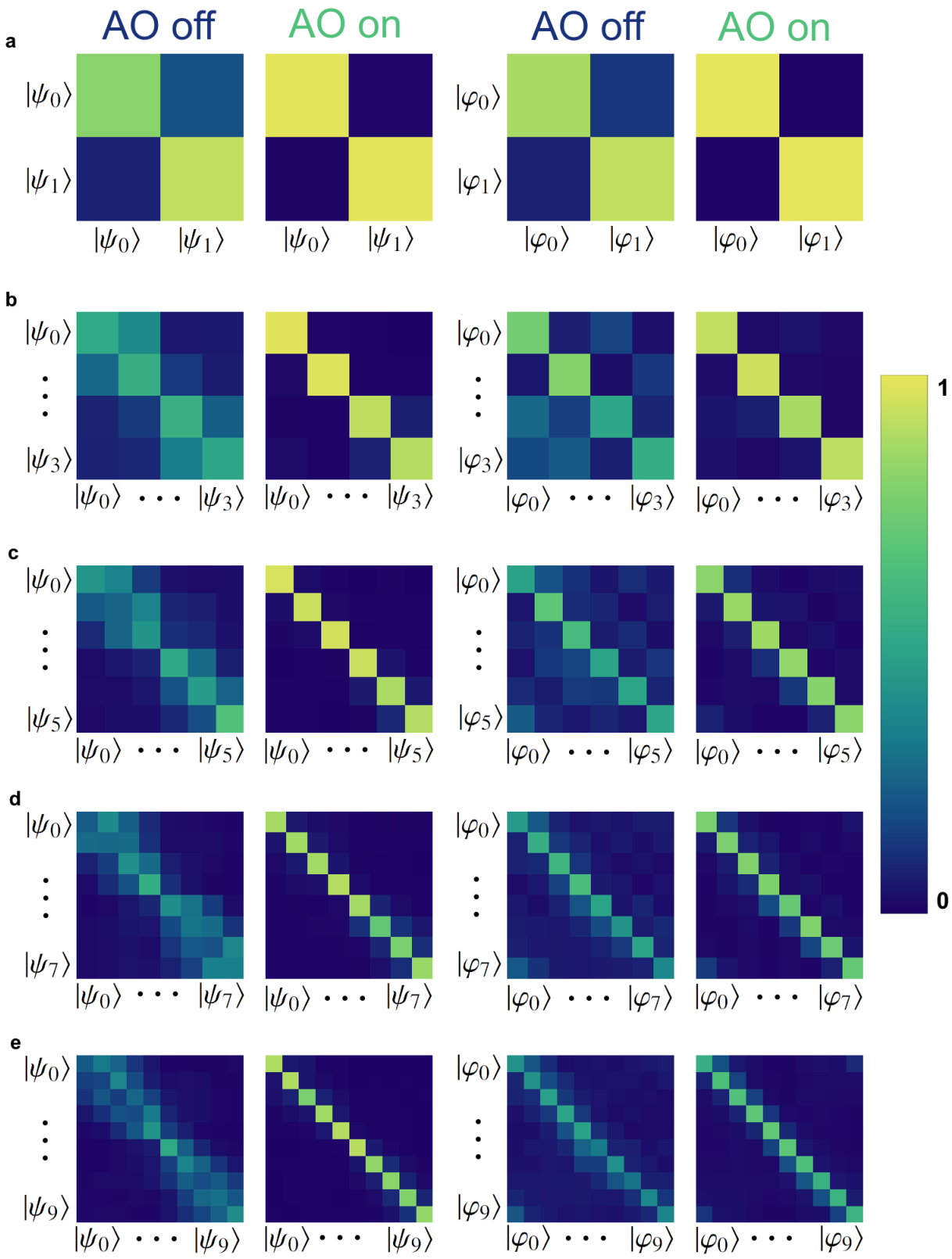

Figure S6. Crosstalk matrices for both bases in all dimensions. **a** $d = 2$, **b** $d = 4$, **c** $d = 6$, **d** $d = 8$, **e** $d = 10$

correcting the effects of turbulence in the logical basis for al dimensions. As mentioned in the manuscript, the QBER 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 QBER in all cases are listed in Tables S2 and S3.

Dimension	QBER OAM AO off	QBER 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 QBER for the logical basis given as %.

Dimension	QBER ANG AO off	QBER 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 QBER for the angular basis given as %.

[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] S. E. Persson, D. M. Carr, and J. H. Jacobs, Las campanas observatory seeing measurements, Experimental Astronomy **1**, 195–212 (1990).

[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).

References

[1] John F Dooley. History of cryptography and cryptanalysis. *History of Computing*, 2018. (Cited on page 1.)

[2] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, feb 1978. (Cited on page 2.)

[3] J. P. Buhler, H. W. Lenstra, and Carl Pomerance. Factoring integers with the number field sieve. In Arjen K. Lenstra and Hendrik W. Lenstra, editors, *The development of the number field sieve*, pages 50–94, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg. (Cited on page 2.)

[4] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. (Cited on page 3.)

[5] Nithin Nagaraj, Vivek Vaidya, and Prabhakar Vaidya. Re-visiting the one-time pad. *I. J. Network Security*, 6:94–102, 01 2008. (Cited on page 3.)

[6] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560:7–11, 2014. (Cited on page 3.)

[7] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, Jan 1992. (Cited on page 3.)

[8] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. (Cited on page 3.)

[9] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008. (Cited on page 3.)

[10] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 503–509. IEEE, 1998. (Cited on page 3.)

[11] Simon Gröblacher, Thomas Jennewein, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8(5):75, 2006. (Cited on page 3.)

[12] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005. (Cited on page 3.)

[13] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000. (Cited on pages 3 and 13.)

[14] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002. (Cited on page 3.)

[15] Yang Liu, Wei-Jun Zhang, Cong Jiang, Jiu-Peng Chen, Chi Zhang, Wen-Xin Pan, Di Ma, Hao Dong, Jia-Min Xiong, Cheng-Jun Zhang, Hao Li, Rui-Chun Wang, Jun Wu, Teng-Yun Chen, Lixing You, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.*, 130:210801, May 2023. (Cited on page 3.)

[16] Wei Li, Likang Zhang, Hao Tan, Yichen Lu, Sheng-Kai Liao, Jia Huang, Hao Li, Zhen Wang, Hao-Kun Mao, Bingze Yan, Qiong Li, Yang Liu, Qiang Zhang, Cheng-Zhi Peng, Lixing You, Feihu Xu, and Jian-Wei Pan. High-rate quantum key distribution exceeding 110 mb s–1. *Nature Photonics*, 17(5):416–421, May 2023. (Cited on page 4.)

[17] Alicia Sit, Frédéric Bouchard, Robert Fickler, Jérémie Gagnon-Bischoff, Hugo Larocque, Khabat Heshami, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, Christoph Marquardt, Gerd Leuchs, Robert W. Boyd, and Ebrahim Karimi. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006–1010, Sep 2017. (Cited on page 4.)

[18] Mujtaba Zahidy, Domenico Ribezzo, Claudia De Lazzari, Ilaria Vagniluca, Nicola Biagi, Ronny Müller, Tommaso Occhipinti, Leif K. Oxenløwe, Michael Galili, Tetsuya Hayashi, Dajana Cassioli, Antonio Mecozzi, Cristian Antonelli, Alessandro Zavatta, and Davide

Bacco. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nature Communications*, 15(1):1651, Feb 2024. (Cited on page 4.)

[19] Tian Zhong, Hongchao Zhou, Robert D Horansky, Catherine Lee, Varun B Verma, Adriana E Lita, Alessandro Restelli, Joshua C Bienfang, Richard P Mirin, Thomas Gerrits, et al. Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding. *New Journal of Physics*, 17(2):022002, 2015. (Cited on page 4.)

[20] Mohammad Mirhosseini, Omar S Magaña-Loaiza, Malcolm N O'Sullivan, Brandon Rodenburg, Mehul Malik, Martin PJ Lavery, Miles J Padgett, Daniel J Gauthier, and Robert W Boyd. High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 17(3):033033, 2015. (Cited on page 4.)

[21] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, Sep 2017. (Cited on page 4.)

[22] Hemani Kaushal, VK Jain, and Subrat Kar. *Free space optical communication*, volume 60. Springer, 2017. (Cited on page 4.)

[23] John C Wyngaard. Atmospheric turbulence. *Annual Review of Fluid Mechanics*, 24(1):205–234, 1992. (Cited on page 4.)

[24] Ming Li, Zhongyuan Yu, and Milorad Cvijetic. Influence of atmospheric turbulence on oam-based fso system with use of realistic link model. *Optics Communications*, 364:50–54, 2016. (Cited on page 4.)

[25] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Phys. Rev. A*, 45:8185–8189, Jun 1992. (Cited on page 7.)

[26] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982. (Cited on page 10.)

[27] J Schwinger. UNITARY OPERATOR BASES. *Proc Natl Acad Sci U S A*, 46(4):570–579, April 1960. (Cited on page 10.)

[28] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International journal of quantum information*, 8(04):535–640, 2010. (Cited on page 11.)

[29] Markus Grassl. On sic-povms and mubs in dimension 6. *arXiv preprint quant-ph/0406175*, 2004. (Cited on page 11.)

[30] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995. (Cited on page 13.)

[31] Frédéric Bouchard, Khabat Heshami, Duncan England, Robert Fickler, Robert W. Boyd, Berthold-Georg Englert, Luis L. Sánchez-Soto, and Ebrahim Karimi. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum*, 2:111, December 2018. (Cited on page 14.)

[32] Mikka Stasiuk, Felix Hufnagel, Xiaoqin Gao, Aaron Z. Goldberg, Frédéric Bouchard, Ebrahim Karimi, and Khabat Heshami. High-dimensional Encoding in the Round-Robin Differential-Phase-Shift Protocol. *Quantum*, 7:1207, December 2023. (Cited on page 14.)

[33] David L Begley. Free-space laser communications: a historical perspective. In *The 15th Annual Meeting of the IEEE Lasers and Electro-Optics Society*, volume 2, pages 391–392. IEEE, 2002. (Cited on page 15.)

[34] Andrey Nikolaevich Kolmogorov. Dissipation of energy in the locally isotropic turbulence. In *Dokl. Akad. Nauk. SSSR*, volume 32, pages 19–21, 1941. (Cited on page 15.)

[35] William K George. Lectures in turbulence for the 21st century. *Chalmers University of Technology*, 2013. (Cited on page 15.)

[36] Valerian Ilich Tatarski. *Wave propagation in a turbulent medium*. Courier Dover Publications, 2016. (Cited on pages 15 and 17.)

[37] D. L. Fried. Optical resolution through a randomly inhomogeneous medium for very long and very short exposures. *J. Opt. Soc. Am.*, 56(10):1372–1379, Oct 1966. (Cited on page 16.)

[38] Paul H. Deitz and Neal J. Wright. Saturation of scintillation magnitude in near-earth optical propagation∗. *J. Opt. Soc. Am.*, 59(5):527–535, May 1969. (Cited on page 17.)

[39] G. R. Ochs and R. S. Lawrence. Saturation of laser-beam scintillation under conditions of strong atmospheric turbulence∗. *J. Opt. Soc. Am.*, 59(2):226–227, Feb 1969. (Cited on page 17.)

[40] Ting i Wang, G. R. Ochs, and S. F. Clifford. A saturation-resistant optical scintillometer to measure cn2†. *J. Opt. Soc. Am.*, 68(3):334–338, Mar 1978. (Cited on page 17.)

[41] von F. Zernike. Beugungstheorie des schneidenver-fahrens und seiner verbesserten form, der phasenkontrastmethode. *Physica*, 1(7):689–704, 1934. (Cited on page 17.)

[42] George C. Valley. Isoplanatic degradation of tilt correction and short-term imaging systems. *Appl. Opt.*, 19(4):574–577, Feb 1980. (Cited on page 21.)

[43] Thomas C Farrell, Darryl J Sanchez, Patrick R Kelly, Anita Gallegos, William Gibson, Denis Oesch, Eric J Aglubat, Alex W Duchane, David F Spendel, and Terry Brennan. Characterizing earth's boundary layer (cebl)—2014 update. In *Imaging and Applied Optics 2014*, page PM1E.3. Optica Publishing Group, 2014. (Cited on page 21.)

[44] Zewen Li, Fan Liu, Wenjie Yang, Shouheng Peng, and Jun Zhou. A survey of convolutional neural networks: Analysis, applications, and prospects. *IEEE Transactions on Neural Networks and Learning Systems*, 33(12):6999–7019, 2022. (Cited on page 22.)

[45] Robert J. Noll. Zernike polynomials and atmospheric turbulence∗. *J. Opt. Soc. Am.*, 66(3):207–211, Mar 1976. (Cited on page 22.)

[46] A. E. Willner, H. Huang, Y. Yan, Y. Ren, N. Ahmed, G. Xie, C. Bao, L. Li, Y. Cao, Z. Zhao, J. Wang, M. P. J. Lavery, M. Tur, S. Ramachandran, A. F. Molisch, N. Ashrafi, and S. Ashrafi. Optical communications using orbital angular momentum beams. *Adv. Opt. Photon.*, 7(1):66–106, Mar 2015. (Cited on page 22.)

[47] Mario Krenn, Robert Fickler, Matthias Fink, Johannes Handsteiner, Mehul Malik, Thomas Scheidl, Rupert Ursin, and Anton Zeilinger. Communication with spatially modulated light through turbulent air across vienna. *New Journal of Physics*, 16(11):113028, 2014. (Cited on page 22.)

[48] Karen M. Hampson, Raphaël Turcotte, Donald T. Miller, Kazuhiro Kurokawa, Jared R. Males, Na Ji, and Martin J. Booth. Adaptive optics for high-resolution imaging. *Nature Reviews Methods Primers*, 1(1):68, Oct 2021. (Cited on page 22.)

[49] Christopher C Wilcox and Sergio R Restaino. *A new method of generating atmospheric turbulence with a liquid crystal spatial light modulator*. InTech, 2009. (Cited on page 23.)

[50] Joseph W Goodman. *Introduction to Fourier optics*. Roberts and Company publishers, 2005. (Cited on page 23.)

[51] Horace W Babcock. The possibility of compensating astronomical seeing. *Publications of the Astronomical Society of the Pacific*, 65(386):229–236, 1953. (Cited on page 38.)

[52] Stefan Hippler. Adaptive optics for extremely large telescopes. *Journal of Astronomical Instrumentation*, 08(02):1950001, 2019. (Cited on page 38.)

[53] Richard G Lane and Michel Tallon. Wave-front reconstruction using a shack–hartmann sensor. *Applied optics*, 31(32):6902–6908, 1992. (Cited on page 39.)

[54] Darryl P Greenwood. Bandwidth specification for adaptive optics systems. *JOSA*, 67(3):390–393, 1977. (Cited on page 41.)