Exploring the Performance of Structured Light Modes and Novel Protocols for Quantum Key Distribution

Rojan Abolhassani

Thesis submitted to the University of Ottawa in partial fulfillment of the requirements for the degree of Master of Science, Physics

Department of Physics
Faculty of Science
University of Ottawa

Supervisor: Ebrahim Karimi

Abstract

This thesis includes two main projects that explore the use of structured light, especially photonic orbital angular momentum (OAM), in quantum key distribution protocols. Particular attention has been paid to how different modes behave in turbulent channels and how adaptive optics systems can mitigate the distortions induced in the beam. Based on the results of these experiments, we propose a new protocol designed to combine the qualities that make a light mode ideal for turbulent channels and adaptive optics systems. The security analyses and performance evaluations of this new protocol are discussed.

In the first chapter, a brief overview of the field is provided. Following that, the second chapter aims to explore the necessary background for understanding the two projects in more detail. We discuss the different degrees of freedom of light and how they can be utilised to help achieve our goals. In the third chapter, the mathematical background relevant to the first project is covered. This includes the modes investigated in the turbulent channel and AO system. In the fourth chapter, an overview of the theory of security in quantum key distribution is presented, followed by an article on a new protocol for QKD. Finally, the conclusions and outlooks are outlined in the last chapter.

Acknowledgements

First and foremost, I would like to thank my supervisor Dr. Ebrahim Karimi, for being extremely supportive and helpful throughout these years, and for all the countless opportunities he made possible which encouraged me to learn and love science more. I am grateful for all the things I learned from him in science and in life.

I would also like to thank all of the members of the SQO group for making everyday life and work at ARC so fun and engaging, mostly during the endless coffee breaks. I would especially like to thank Lukas Scarfe for helping me get started on everything lab and research related, and also Dr. Alessio D'Errico and Dr. Francesco Di Colandrea for being the best and most helpful Post-docs. Thank you for taking so much time out of your days to teach me new things. I would also like to thank all my collaborators, who have contributed greatly to my knowledge.

Also, I want to thank my parents for being so supportive and for always putting my needs first, even from thousands of miles away. Thanks for always cheering even my smallest victories and being my biggest fans. This whole journey was made possible because of you.

And lastly, I want to thank my partner Danial, my best friend and companion in life. Thank you for being by my side through all the tough days, being my safe place and making life so sweet and easy. I could not have done any of this without you.

Author Contributions

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

Chapter 3: Ebrahim Karimi, Lukas Scarfe and Rojan Abolhassani conceived the idea. Rojan Abolhassani, Lukas Scarfe and Alessio D'Errico performed the experiments, collected and analyzed the data. Francesco Di Colandrea conducted the theoretical simulation codes and provided the results. Rojan Abolhassani wrote the first version of the paper. Lukas Scarfe, Alessio D'Errico and Francesco Di Colandrea revised and edited the paper. Khabat Heshami and Ebrahim Karimi supervised the project. All authors contributed to the discussions and text of the manuscript.

Chapter 4: Ebrahim Karimi and Lukas Scarfe conceived the idea. Lukas Scarfe and Rojan Abolhassani prepared the experimental setup and performed the experiment. Lukas Scarfe analyzed the data. Frederic Bouchard, Aaron Goldberg and Francesco Di Colandrea provided the theoretical proof. Khabat Heshami and Ebrahim Karimi supervised the project. All authors contributed to the discussions and text of the manuscript.

Contents

List of Figures

List of Tables

1

Introduction: An Overview

Maxwell's work in the 1860's showed that light is an electromagnetic wave, while Einstein's work in 1905 introduced photons as energy packages or quanta of that wave. Together, these discoveries established that photons are quantum particles associated with electromagnetic waves.

Light waves can be described by the Maxwell equations, which leads us to write the

Helmholtz equation for the electric field E of light beams,

$$\nabla^2 E + k^2 E = 0 \tag{1.1}$$

Since a perfect plane wave exists only in theory, in practice, we use light beams that approximate plane waves under certain conditions, which are called paraxial approximations, and obey the equation

$$(\nabla_T - 2ik_z\partial_z)\,\mathbf{E}(\mathbf{r}) = 0, \tag{1.2}$$

where $\nabla_T = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$ and $E(r)$ is the amplitude of the electric field. This is called the paraxial Helmholtz equation [1].

The paraxial beams have wave vectors that make only a small angle with the optical axis, so that throughout their propagation they remain close to the axis. One example of these beams is the Gaussian beam. The Gaussian beam has a Gaussian intensity profile, meaning it has its peak intensity on the optical axis, and the intensity decreases proportional to the radial index ρ. The electric field of the Gaussian beam is given by

$$\mathbf{E}(r,z) = E_0\,\hat{\mathbf{x}}\,\frac{w_0}{w(z)}\exp\left(\frac{-r^2}{w(z)^2}\right)\exp\left(-i\left(kz + k\frac{r^2}{2R(z)} - \psi(z)\right)\right) \tag{1.3}$$

where z is the distance along the beam from the focus (waist), $w(z)$ is the beam radius where the field drops to $1/e$ of its on-axis value, $w_0 = w(0)$ is the waist radius, $R(z)$ is the wavefront's radius of curvature, and $\psi(z) = \arctan(z/z_R)$ is the Gouy Phase [1].

By exploiting different properties of light, we can structure them to meet our needs. These tailored light beams are often called "structured light".

The world of structuring light has faced many advances in recent history, especially since the advent of Spatial Light Modulators (SLMs), which are devices used for generating structured light by applying arbitrary phase and amplitude masking to an incoming beam [2].

Structured light can be used in many different fields such as classical communication, quantum information, quantum key distribution (QKD), microscopy, imaging and optical sensing [3]. Using structured light for quantum information and communication is especially important, since information plays a huge role in today's world. A great number of our everyday tasks depend on our information being kept and sent securely, and technological advances aim to keep this information safe as well. With the advances of quantum computing, classical communication can no longer be considered secure. Using the laws of quantum mechanics, scientists have come up with different methods to share information securely, such as quantum key distribution (QKD), in which the presence of an eavesdropper can be detected.

Structured photons, in general, exist in a high dimensional Hilbert space, meaning they can surpass the two-dimensionality of classical communications (bits of 0 and 1) to provide faster communication and higher thresholds for eavesdropping.

The focus of this thesis will be to elaborate how the different degrees of freedom of photons can be implemented in QKD.

2

Chapter 2: Basics of the Study

2.1 Spatio-Temporal Modes

Investigating the classical and quantum properties of photons, we can describe them using different degrees of freedom: polarization, spatial and temporal modes. These quantities relate to the conserved values of energy and momentum in the electromagnetic waves.

In classical physics, linear momentum $p = mv$ gives one a sense of the linear motion of a particle. The rotational translation of linear momentum would be the angular momentum $L = rp$ which is the generator of rotation. Spin and Orbital angular momentum are familiar terms for us in classical physics; the former being responsible for an object's spin around its own axis, and the latter its rotation around an external point in an orbit.

Light also carries momentum, but it is an intrinsic quality rather than the classical picture we have. In classical physics, momentum is directly related to an object's mass, whereas photons are massless particles.

It has been well known that light carries linear momentum and can push away charged particles. The linear momentum is directly tied to the wavevector k, acquires values $p = \hbar kp$ and points in the direction of propagation of the beam. The angular momentum of light comes in the form of both spin angular momentum (SAM) and orbital angular momentum (OAM) [4]. In what follows, we aim to describe exactly how momentum and energy are carried through light beams.

2.1.1 Polarization

Light waves are composed of an electric and magnetic field orthogonal to one another in a tangential plane perpendicular to the direction of propagation. The rate of change of the tip of this electric (or magnetic) field in time is denoted by the *polarization vector*, which

also lies in a plane and takes two values.

Depending on the geometrical shape of the motion of the tip of the electric field, we can have elliptical, circular or linear polarized light. By considering two orthogonal polarization vectors, any arbitrary polarization could be constructed. For instance, polarizations in the x and y directions are denoted by horizontal $|H\rangle$ and vertical $|V\rangle$ polarizations respectively. Linear combinations of these basis states can represent $Diagonal\,|D\rangle$ and $Anti-Diagonal\,|AD\rangle$ polarizations, as well as *circular polarizations*. For example, the $Right-hand\,circular\ |RHC\rangle$ and $Left-hand\,circular\ |LHC\rangle$ polarizations are given by equal-amplitude superpositions of H and V with a $\pm\pi/2$ phase difference:

$$|RHC\rangle = \frac{1}{\sqrt{2}}(\,|H\rangle - i\,|V\rangle\,), \quad |LHC\rangle = \frac{1}{\sqrt{2}}(\,|H\rangle + i\,|V\rangle\,) \tag{2.1}$$

Similarly, the diagonal basis is defined as:

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \quad |AD\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{2.2}$$

To this end, one can use the $Poincare\,Sphere$, a sphere of unit radius where each point represents a polarization vector. The axes on this sphere are denoted by Stokes parameters

(S_0, S_1, S_2, S_3), which quantify polarization in a measurable way:

$$S_0 = \text{total intensity}\,,$$

$$S_1 = \text{horizontal vs. vertical intensity difference}\,,$$

$$S_2 = +45^\circ \text{ vs. } -45^\circ \text{ intensity difference}\,,$$

$$S_3 = \text{right- vs. left-circular intensity difference}\,.$$

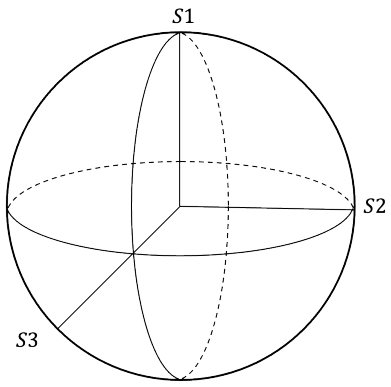


Figure 2.1: The Poincaré Sphere. Each polarization state can be shown as a point on this sphere of unit radius.

In quantum mechanics, by using the same definitions given as in classical physics, one can write down respective operators for spin or orbital angular momentum and proceed to find their eigenstates and eigenvalues.

Eigenstates of the Spin Angular Momentum correspond to photons with circular polarization, where a circularly polarized photon contains a spin value of $\hbar$ along the propagation

direction, with RHC photons having the negative value and LHC the positive.
Linear polarizations can be written as superposition of RHC and LHC polarizations. Once we deal with linearly polarized light such as

$$|H\rangle = \frac{1}{\sqrt{2}}(|RHC\rangle + |LHC\rangle) \tag{2.3}$$

the total value of spin angular momentum for the beam would be zero. But quantum mechanically, each single photon has a 50% chance of having a spin $+\hbar$ or $-\hbar$, even though the sum of them in the end would yield zero spin for the beam. Each light beam's polarization can thus be decomposed in terms of LHC and RHC vectors and be assigned SAM values for its single photons.

2.1.2 Spatial modes

Spatial modes define how light beams are distributed in space. We can access the spatial domain by altering the phase and amplitude of the beams.
Eigenstates of the Orbital Angular Momentum of light, unlike the SAM modes, are not related to polarization. Rather, they correspond to the spatial properties of light and create photons with a helical or twisted phase profile.
Any beam containing a phase structure of $e^{(i\ell\phi)}$ contains orbital angular momentum with value $\ell\hbar$ with ℓ being an integer representing the number of twists (or helices) around the beam [4]. Similarly, each random beam can be decomposed into different OAM modes,

especially since these modes create a complete orthonormal set. The possibility for each photon in a beam to carry a certain value of OAM could thus be calculated.

Examples of beams carrying OAM are some of the solutions to the paraxial Helmholtz equation; such as the Hermite-Gaussian beam or the Laguerre-Gaussian beam. Both of these beams form a complete and orthogonal set of solutions, and can be used to write other arbitrary beams in terms of them. The LG beams are the solutions written in cylindrical coordinates and are the most practical since most of the optics used in optics laboratories are circularly shaped. The expression for these beams in the cylindrical coordinate is

$$\begin{aligned} \mathrm{LG}_p^\ell(r,\phi,z) = &\sqrt{\frac{2p!}{\pi(|\ell|+p)!}}\,\frac{1}{w(z)}\left(\frac{\sqrt{2}r}{w(z)}\right)^{|\ell|} L_p^{|\ell|}\left(\frac{2r^2}{w(z)^2}\right)\exp\left[-\frac{r^2}{w(z)^2}\right] \\ &\times\exp\left[-ik\frac{r^2}{2R(z)}\right]\exp\Big(i\ell\phi\Big)\exp\Big[-i(2p+|\ell|+1)\psi(z)\Big] \end{aligned} \tag{2.4}$$

where $L_p^{|\ell|}(x)$ are the Laguerre polynomials, and the other parameters are

$$
\begin{aligned}
w(z) &= w_0\sqrt{1+\left(\frac{z}{z_R}\right)^2}, && \text{beam waist at } z,\\
R(z) &= z\left[1+\left(\frac{z_R}{z}\right)^2\right], && \text{radius of curvature},\\
\psi(z) &= \arctan\left(\frac{z}{z_R}\right), && \text{Gouy phase},\\
z_R &= \frac{\pi w_0^2}{\lambda}, && \text{Rayleigh range},\\
k &= \frac{2\pi}{\lambda}, && \text{wave number},
\end{aligned}
$$

Here, the indices ℓ and p are integer values and indicate the radial and azimuthal values of the beam respectively. ℓ which is the argument of the term $exp(i\ell\phi)$ also indicates the twists in the phase of the beam and the value of the OAM.

2.1.3 Temporal modes

By taking the Fourier transform of a time domain function, we arrive at the frequency domain. The frequency of light beams can be manipulated to create temporal modes of light, or as its conjugate, spectral modes. In the quantum picture, each temporal mode is an independent basis state in the time-frequency Hilbert space, similar to how spatial

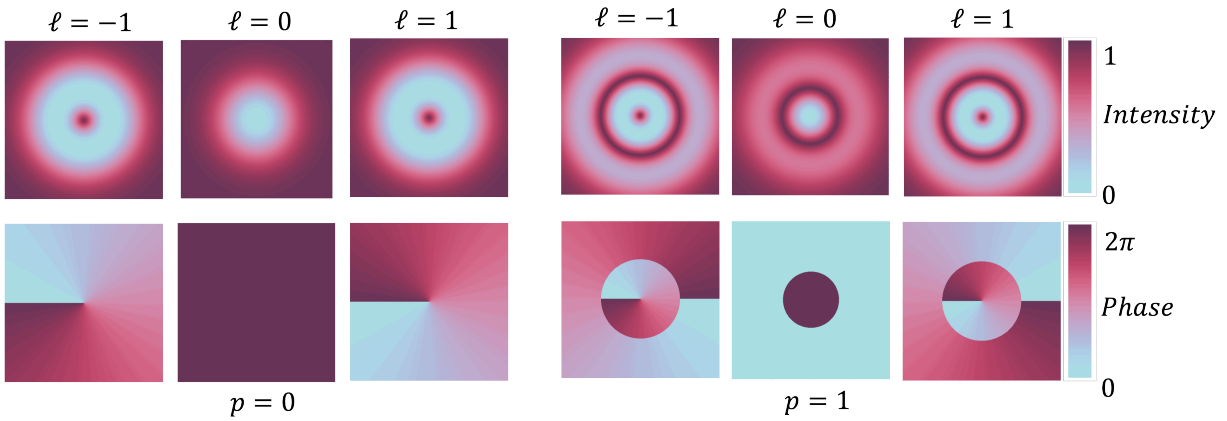


Figure 2.2: The OAM modes of Laguerre Gaussian beams, showing intensity (upper row) and phase (lower row) of different beams with $p = 0, 1$ and $\ell = -1, 0, 1$

modes form a basis in the transverse plane.

Temporal modes can take forms such as discrete time bins, frequency bins, or overlapping pulsed waveforms shaped through modulation. Exploiting the complex temporal phase and amplitude of light waves can be used in many applications such as high dimensional quantum communication, multiplexing, and quantum state engineering.

2.2 Quantum Cryptography

2.2.1 Quantum Key Distribution

One of the applications of using the degrees of freedom of light is in Quantum Key Distribution. QKD is a method of sharing information, in which the presence of an eavesdropper can be detected securely. Alice, a sender, wants to share a secret key with Bob, a receiver,

over a quantum channel. An eavesdropper Eve is trying to gain access to this information. When considering the use of these quantum channels, it is assumed that any technological limitations would be overcome in the future, and the only limiting factor would be the laws of physics.

What makes this method special is its advantage over classical communication channels. Nowadays, classical channels are secure due to the difficulty of solving complex mathematical problems by classical computers. These problems are often called the one-way problems, which are easy to construct but tedious to solve, such as finding the prime factors of a very large number [5]. One of the most well-known protocols based on this method used today for daily communications is the RSA (Rivest-Shamir-Adleman) protocol [6]. Solving problems of these kind are not unachievable, but rather very slow and time consuming. It is almost impossible to solve them with the classical computers we have today. With the advent of quantum computers, it will be easy to solve these problems in a near future. One solution is to use new approaches such as the Shor algorithm [7] to find the primary factors of these large numbers. The Shor algorithm runs in polynomial time, which is achievable only on quantum computers. Thus the security of the classical channels would be at risk of eavesdropping.

The safest method for Alice and Bob to communicate is by using a one-time pad, where they are the only parties who know their secret key. Now all we have to do is implement a channel to share this one-time key. To this aim we can use a quantum channel.

In QKD, security is maintained through the impossibility of cloning unknown quantum states with 100% fidelity [8], which is a key physical limitation. Different protocols have

been suggested as to how this theory could be carried out, the first and most well-known being the BB-84, which was introduced in 1984 by Bennet and Brassard [9].

2.2.2 BB-84

BB-84 was introduced as a two-dimensional QKD protocol. In quantum mechanics, measurements on some properties of particles change the value of other properties. Two set of conjugate bases are used in BB-84. Using the polarizations of photons, Bennet and Brassard define their principal bases as linear ($|H\rangle$ and $|V\rangle$) and circular ($|RHC\rangle$ and $|LHC\rangle$). In each basis, a bit value of 0 and 1 is assigned to the elements.

Alice prepares her information by randomly choosing one of the two bases, either linear or circular. She then prepares a state in that basis. Bob measures the incoming state in an arbitrary basis as well. Once they are done sending and receiving their signals over the quantum channel, Alice tells Bob her initial chosen bases, and Bob will keep the measurements where his basis choice is the same as Alice. If Bob chose the same basis as Alice, he would get the right value for his measurement, and the value becomes part of their secret key. On the other hand, if he chose the wrong Basis, the key is discarded. Finally, the 0 and 1 values are assigned and a secret key is constructed. This is called the sifting process Fig[2.3].

It is important to keep in mind that not all photons are received by Bob, as a result of the shortcomings of detectors. In such situations, the failed detections are also disregarded

1. Alice's signal	$\|H>$	$\|V>$	$\|RC>$	$\|LC>$	$\|V>$	$\|RC>$	$\|H>$	$\|LC>$	$\|V>$
2. Bob's basis	◯	↕	◯	↕	◯	◯	↕	◯	◯
3. Bob's measurements	$\|RC>$	$\|V>$	$\|RC>$	$\|V>$	$\|RC>$	$\|RC>$	$\|H>$	$\|LC>$	$\|LC>$
4. Comparison	✗	✓	✓	✗	✗	✓	✓	✓	✗
5. Sifted key	–	1	0	–	–	0	0	1	–

Figure 2.3: Table showing an example of the sifting process. 1)Alice randomly chooses and creates her polarization states of photons using Horizontal$|H\rangle$, Vertical$|V\rangle$, Right-hand circular $|RC\rangle$ or Left-hand circular $|LC\rangle$. 2) Bob chooses a random basis between circular ◯ and linear ↕ to conduct his measurements. 3) Bob's results showing his correct measurements for the right basis choices, and wrong measurements for wrong choices. 4) Alice and Bob compare their choices of basis over a public channel and keep the ones they agree upon. 5) After assigning bit values to each measurement, a sifted key is created.

and removed from the key.

2.2.3 Security in QKD

Noises in the channel also contribute to altered signals that are not necessarily results of eavesdropping. In order to make sure that the signals received by Bob in the sifted key are not altered by Eve, Alice and Bob are led to compare a random subset of their data over a public classical channel, and evaluate the error rate in order to fix remaining key errors or remove any information that Eve might have. They can achieve this through error correction and privacy amplification [10]. This gives rise to the necessity of having a threshold for the error rate.

If Eve had in fact been eavesdropping on Alice's signals, she would be introducing different error rates by doing the measurements before the signals reach Bob. There are a number of different ways she could go about this; the attacks are in general divided into three groups of individual, collective, and coherent attacks. One example of the individual attack is the intercept-resend method. In this method, Eve measures each signal, and resends a similar one to Bob. Eve either chooses the right basis and sends the correct signal, or chooses the wrong basis. In the two-dimensional BB84, there is a 50% chance she measures in a wrong basis and resends the signal to Bob. Bob also has a 50% chance of ending up with the wrong measurement outcome (assuming his basis is the same as Alice's and it is a sifted photon). This indicates that Eve introduces a $\frac{1}{4}$ error rate.

Another method of individual attack is the cloning method, where Eve makes an imperfect clone of the incoming state, keeps it for herself and sends the other off to Bob. Once Alice and Bob communicate over the classical channel and disclose the bases, Eve can measure the clone together with the ancilla to obtain the maximum information about Alice's key bit. This method is considered the optimal attempt Eve can make, although she is limited by the no-cloning theorem in quantum mechanics, which prevents her from creating a perfect clone [11].

In the collective attack, Eve treats each signal individually but does her measurements generally. The coherent attack is the most general form and introduces correlations between the signals. In this attack Eve treats the signals together rather than individually.

2.3 Higher Dimensions

So far we have been dealing with quantum binary digits or *qubits*. These qubits can take two values, just like the classical bits of 0 and 1. Bits are units of information, in the way that they show outcomes of an event in binary language. If there are N possible outcomes to a measurement, there are $\log_2 N$ bits needed for the information content. As an example, if there are 4 outcomes, each outcome can be showed with 00, 01, 10 or 11.

By going to higher dimensional Hilbert spaces, we can create higher dimensional qubits, or qu*dits*, that can take more than two values. There are several ways of experimentally implementing the qudits, one of which is using the OAM modes of light. As mentioned earlier, the OAM modes can in theory be infinite dimensional. If we use, say, a four dimensional basis consisting of OAM modes $|1\rangle$, $|2\rangle$, $|3\rangle$ and $|4\rangle$, we can assign them the bits 00, 01, 10 and 11 respectively. Each single photon, instead of carrying one bit of information (0 or 1), is carrying two bits; instead of sending two photons with qu*bit* = 0, we can just send one photon with qu*dit* = 00. Generally, a qudit in a d-dimensional space carries $\log_2 d$ amount of information. This suggests that in higher dimensional spaces, we have a higher density of information per photon and can send information with a higher speed.

Aside from enabling more information to be encoded per photon and allowing faster key generation, the use of qudits also provides higher security thresholds and increases resilience against eavesdropping [12].

We can apply higher dimensions to the BB-84 protocol as well. In order to do so, we keep the two basis choices, where each basis consists of d elements rather than two. The first basis consits of the OAM modes, which we call the logical basis, and the second basis is one mutually unbiased to the former, such as the angular modes

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} e^{i\phi_k} |k\rangle \tag{2.5}$$

where $\Phi_k = \frac{2\pi jk}{d}$. Recall the example from the previous section where Eve applied the intercept-resend method on the BB-84. If we had exploited a higher dimensional BB-84, i.e. four dimensions, the error rate would have been different; there is $\frac{1}{2}$ chance of Eve measuring in the wrong basis, and $\frac{3}{4}$ chance for Bob to measure the wrong outcome. This introduces $\frac{3}{8}$ error rate which is higher than the 2D case of $\frac{1}{4}$ [13].

This is an example of a simple individual attack. Considering more complicated and effective forms of attacks, such as an optimal cloning attack or a coherent attack, we can find the upper bounds for the error rate D [12],

$$(1-D)\log_2 \frac{1}{(1-D)} + D\log_2\left(\frac{d-1}{D}\right) \leq \frac{1}{2}\log_2 d \tag{2.6}$$

where d is the dimension. For more information on the origins of this equation, refer to chapter 4 of this thesis. It is seen that by going to higher dimensions d, there is greater tolerance for the error rate which is beneficial.

Other protocols have also been suggested for implementing QKD. The MUB protocol, or

the six-state protocol is another example, where three bases are used rather than two. The idea emerged from the fact that when creating the two dimensional MUB sets, there are three complete bases that are mutually unbiased to one another, each containing two elements. Qudits can be used to go to higher dimensions in the MUB protocol as well. Another example is the Chau-15 [14], which uses a 2^n dimensional Hilbert space. This protocol was shown to be the most resilient to errors, but has a lower key-rate. Another protocol is the Singapore protocol which uses the qudits in the SIC-POVM basis [15].

2.4 Different Communication Channels

Different media can be used for QKD, such as optical fibers, underwater channels and free space links. In recent years, experimental realization of implementing QKD in these media has been successfully demonstrated, most of which have used the spin-orbital modes of light as their information carriers.

2.4.1 Fibers

Most of the optical fibers used nowadays in laboratories are made of a step-index waveguide structure, such as single-mode or multi-mode fibers. In these fibers, the refractive index of the core is higher than that of the cladding. This difference causes total internal reflection inside the fiber which confines the light beam and propagates it along the fiber.

The size of the core determines how many transverse modes the fiber can carry. Smaller cores support only a single mode, whereas larger ones support multiple modes, creating the famous single and multi mode fibers. These modes are described as linearly polarized (LP) modes [16].

However, these fibers are not ideal for structured light, since the LP modes tend to become unstable over long periods of propagation. Modes with radial and azimuthal polarization can become degenerate and mix with each other, introducing excess crosstalk. Therefore, they are not suitable for use in quantum communications.

To overcome this problem, special fibers have been designed, such as ring-core or vortex fibers. In normal multi-mode fibers, different modes might have very similar effective refractive indices which causes them to mix up or interact with one another. In vortex beams, the core shape is altered so that these effective indices are separated and the mixing is prevented. The core in a vortex fiber is shaped to match the "doughnut" intensity profile of a vortex beam, allowing it to stably carry higher-order vector modes.

This quality makes them suitable for high-dimensional quantum key distribution, where preserving the structure of complex light is essential. Quantum key distribution using such vortex fibers has also been accomplished recently [17].

2.4.2 Underwater Channels

Another media that has been used traditionally for communication are underwater channels, which rely on using acoustics. Implementing QKD in these channels has been investigated, but remains challenging due to water's high absorption of electromagnetic wavelengths except for a window of blue-green waves.

Using blue-green laser lights has enabled sending quantum information in these channels, but due to absorption, scattering, and optical turbulence the performance of the channel is limited. Experiments show polarization states remain highly faithful ($< 1\%$ error), while structured modes like OAM or vector vortex states are more affected by turbulence.

2.4.3 Free Space

Although fibers have been widely used in classical communications, they are limited to short distances given the great amounts of loss caused by long propagation. One way of overcoming this problem in classical channels is amplifying the signal, which is impossible for quantum signals due to the no-cloning theorem. Aside from this shortcoming, fibers cannot be used in very long distance like ground-satellite channels. It is therefore necessary to look into free space channels, which overcome these problems. In this case, only linear loss occurs.

Free space quantum communication has been advancing rapidly [18], with secure QKD

having been done for 2 and 4 dimensions over a few hundred meters [19, 20], and classical communication with OAM over ground-satellite channels [21–23].

The main cause of error in these links is the atmospheric turbulence which distorts the spatial properties of the modes and misaligns the beam with respect to the sender and reciever. In the following sections, details of how turbulence affects the beams and ways to overcome it will be discussed.

2.5 Turbulence

Atmospheric turbulence can cause losses in intensity and alter the phase profile of light beams. Turbulence can be due to different elements such as differences in temperature, density, pressure, wind, and presence of particles in the air. This causes different refractive indices throughout the beam's path, which will introduce inconsistencies in paths taken by different parts of the wavefront. One way of describing this phenomenon is by dividing the turbulent medium to a number of smaller cells that are isotropic. These cells, called eddies, vary in size, but the bigger ones keep breaking down to smaller sized eddies, until the viscosity causes the smallest sizes to turn to heat.

2.5.1 C_n^2 PROFILE

According to Kolmogorov, these small eddies all statistically behave the same way, regardless of what initiated the turbulence in the first place. From this, the structure function of the refractive index can be defined, which describes the average fluctuations of the refractive index [24],

$$D_n(r) = \langle [\, n(x) - n(x') \,]^2 \rangle = C_n^2(h)\, r^{2/3} \tag{2.7}$$

Here, x and x' are points on the targeted path, r the distance between these two points and $C_n^2(h)$ is the atmospheric structure constant at height h. This constant is the universally accepted measure for the strength of turbulence. High values of the C_n^2 denote intense turbulence, and lower values indicate mild turbulence [25].

The C_n^2 varies throughout the day. Changes are affected by weather, location, altitude and time. Due to this inconsistency, measurements are usually done locally and time-specific using instruments such as the scintillometer. Moreover, measurements are usually done as averages at each altitude. One of the commonly used models is the Hufnagel-Valley Boundary mode, which gives the C_n^2 as a function of height.

From this emerges the Fried parameter r_0, a characteristic of the wavefront which determines the length L over which the wavefront remains coherent [26], and is given by

$$r_0 = \left[0.423\, k^2 \int_0^L C_n^2(h)\, dh \right]^{-3/5}, \quad k = \frac{2\pi}{\lambda} \tag{2.8}$$

2.5.2 Zernike Polynomials

The aberrations in the phase of a beam can have different factors such as tip, tilt, defocusing, astigmatism, and so on. A random aberration can be a certain combination of these terms and can be described using Zernike polynomials [27]. The Zernike polynomials are orthogonal on the unit circle, and any function can be written in terms of them. They are given by $Z_n^m(\rho,\varphi) = R_n^m(\rho)\,\cos(m\,\varphi)$for even Zernike terms and $Z_n^{-m}(\rho,\varphi) = R_n^m(\rho)\,\sin(m\,\varphi)$ for the odd terms, where

$$R_n^m(\rho) = \sum_{k=0}^{\frac{n-m}{2}} \frac{(-1)^k\,(n-k)!}{k!\left(\frac{n+m}{2}-k\right)!\left(\frac{n-m}{2}-k\right)!}\,\rho^{n-2k} \tag{2.9}$$

is the radial Zernike polynomial. Each term in this series corresponds to one of the aberrations of phase. An arbitrary phase profile can be decomposed as $\Phi(\rho,\varphi) = \sum_j a_j Z_j(\rho,\varphi)$ where the index $j = 1+\frac{n(n+2)+m}{2}$. Some of the Zernike polynomials and their corresponding aberration effect are given below;

j	(n,m)	$Z_n^m(\rho,\varphi)$	Name / Mode
1	(0, 0)	1	Piston
2	(1, -1)	$2\rho\sin\varphi$	Tip
3	(1, 1)	$2\rho\cos\varphi$	Tilt
4	(2, -2)	$\sqrt{6}\rho^2\sin 2\varphi$	Oblique Astigmatism
5	(2, 0)	$\sqrt{3}(2\rho^2-1)$	Defocus
6	(2, 2)	$\sqrt{6}\rho^2\cos 2\varphi$	Vertical Astigmatism

Table 2.1: First six Zernike polynomials and their corresponding aberrations.

2.6 Adaptive Optics

Knowing the Zernike polynomials that make up a beam, we can easily overcome the unwanted aberrations by applying the conjugate of the phase to the beam and flattening it. One of the ways to implement this technic is using Adaptive Optics systems.

Adaptive optics is used in different areas like astronomy, microscopy and communications. Most of the common AO systems rely on reversing the distorted phase profile of an incoming beam to retrieve the original phase. These systems are composed of three main elements; a wavefront sensor (WFS), a deformable mirror (DM) and a control computer. The principle of the AO is that a beam is received by the Wavefront sensor which measures the phase, and sends the measurements as signals to the control computer. The control computer then computes the conjugate of these signals and send the new signals to the deformable mirror, where the phase conjugations are physically applied. If this process keeps happening over and over again, i.e. after hitting the DM the beam is sent back to the WFS and measurements happen again, the system is called a closed-loop system, in contrast to open-loop systems where the whole process discussed above happens only once. Most of the AO systems are closed-loop systems, so that the WFS can measure the outcomes of the first correction and apply newer corrections to perfect the results.

One of easiest options for the wavefront sensor is the Shack-Hartmann sensor. This WFS is made of a number of sub-apertures, and each locally focuses a small section of the incoming beam onto a camera. The displacement of the beam from the center of the pixels of the sensor are measured as seen in figure 2.4. These measurements translate to the Zernike

polynomials in the control computer, which calculates the conjugated phase as well.

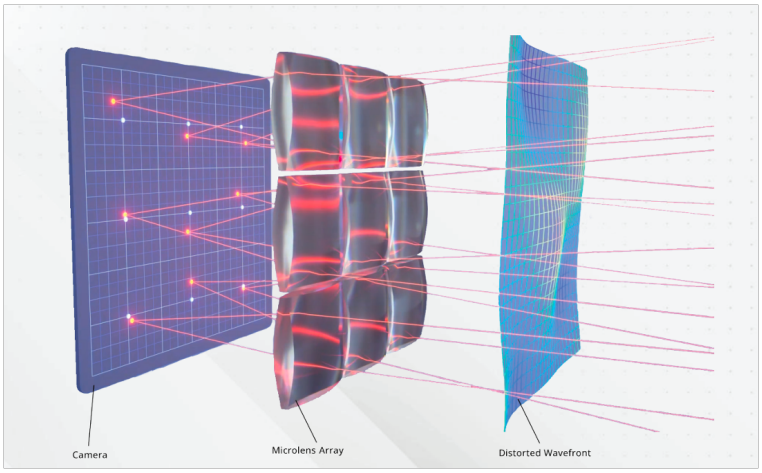


Figure 2.4: The working principles of a Shack-Harmtann wavefront sensor. Source: [28].

The conjugate of the phase is sent as signals from the control computer to the deformable mirror. Inertial AO systems correct distorted phases by mechanically moving mirrors. Deformable mirrors are replacements for the array mirrors used previously in AO systems, which contained gaps between the small mirror elements that produced excess diffraction patterns. In contrast, the deformable mirror is a continuous surface equipped with an array of actuators. These actuators moves when a voltage is applied. By giving different voltages to different actuators, the mirror's surface changes shape and can thus compensate the distorted phase front, using the signals from the control computer.

3

Chapter 3: Different spatial modes in turbulence

Adaptive optics systems have been used to compensate the distorted phase of beams for implementing QKD in turbulent channels [29]. It was seen that the corrections applied to each beam can vary depending on the shape and properties of the mode. Many factors

can contribute to this result, such as how much a beam with a certain profile is affected by turbulence or how the AO system can correct for it. With this goal in mind, the behavior of different spatial modes of light have been investigated in the following work. These structured beams are made in the MUB and SIC-POVM modes.

3.1 Mutually Unbiased Bases

Different modes of light can be used as the bases in QKD protocols. Two mutually unbiased bases are used in BB-84, and three in the six-state protocol. Two mutually unbiased bases can exist in every dimension [30], but a complete MUB set only exists for dimensions that are a prime or power of a prime, $d = p^r$, where the maximum number of existing MUB is $d+1$ [31]. In each MUB set, every basis is orthonormal on its own, and mutually unbiased to the other bases in the set. This means that a vector element $|\psi_i\rangle$ of basis M_1, is an equal superposition of the vector elements $|\phi\rangle_j$ of basis M_2, so that

$$|\langle\phi_j|\psi_i\rangle|^2 = \frac{1}{d} \tag{3.1}$$

This indicates that if a state is prepared in basis M_1 and measured in basis M_2, each possible measurement outcome occurs with the same probability [32].

The smallest prime dimension is 2. In this case, a complete set of mutually unbiased bases can be constructed from the eigenstates of the three Pauli spin operators σ_z, σ_x, and σ_y,

namely:

$$\sigma_z : \{|0\rangle, |1\rangle\}, \tag{3.2}$$

$$\sigma_x : \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) , \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}, \tag{3.3}$$

$$\sigma_y : \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) , \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).\} \tag{3.4}$$

It can be seen that by taking, say, the first vector of the σ_z basis and calculating its product with any of the other vectors in σ_x and σ_y, we get $\frac{1}{\sqrt{d}}$. For polarization, these 3 MUB correspond to horizontal and vertical polarization ($\{|H\rangle, |V\rangle\}$), diagonal and anti-diagonal ($\{|D\rangle, |A\rangle\}$), and left and right-circular polarizations ($\{|L\rangle, |R\rangle\}$) respectively.

The Pauli operators can be extended to higher-dimensional systems, and can construct the Weyl operators. Weyl operators are unitary operators and can be written in the form $X^k Z^l$, where k and l are integers ranging from 0 to $d-1$, with d being the dimension of the Hilbert space.

The operator Z is made of diagonal elements in the logical basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. Its eigenvalues are powers of $\omega = e^{2\pi i/d}$, so that $Z|j\rangle = \omega^j |j\rangle$. It is written as

$$Z = \sum_{j=0}^{d-1} \omega^i |j\rangle \langle j| \tag{3.5}$$

As an example, applying Z to the vector element $|k\rangle$ from the logical basis gives the result $\omega^k |k\rangle$.

The operator X acts as a cyclic shift on the basis states, mapping $|i\rangle$ to $|i+1 \bmod d\rangle$

$$X = \sum_{i=0}^{d-1} |i+1 \bmod d\rangle \langle i| \tag{3.6}$$

For instance, applying X in 3 dimensions $d = 3$ gives $X|0\rangle = |1\rangle$, $X|1\rangle = |2\rangle$, $X|2\rangle = |0\rangle$, and applying Z gives In prime-dimensional systems, the eigenbases of Z together with the set of operators $\{XZ^l \mid l = 0, \ldots, d-1\}$ form a complete set of mutually unbiased bases [33].

When applying this theory experimentally in our lab, we choose the logical basis as the OAM states of light. The OAM states of light refer to Laguerre-Gaussian beams with different helical index ℓ. The logical vector elements respectively correspond to the ℓ modes in each dimension from $\ell = \{-d, -d+1, ..., d-1, d\}$. In this manner, $\ell = 0$ is excluded in even dimensions.

3.2 SIC-POVM [34]

The use of MUB in BB-84 does not span the whole of the bloch sphere but rather a plane, and also due to the impossibility of constructing a complete set of MUB in Hilbert spaces with dimensions that are not powers of a prime, other theoretical grounds have been investigated. One option is the use of positive operator-valued measures (POVMs). Symmetric informationally complete (SIC) POVMs are an optimal group of POVMs, in the sense that they exist in all dimensions, maximize symmetry and minimize the overlap

of information and redundancy.

In d dimensions, a SIC-POVM consists of d^2 pure states $\{|\Phi_i\rangle\}$ in a way that the inner product between any pair of states is [34]:

$$|\langle\Phi_i|\Phi_j\rangle| = \frac{1}{\sqrt{d+1}}, \quad i \neq j. \tag{3.7}$$

The states in a SIC-POVM can be generated using Weyl-Heisenberg displacement operators. We can implement a "fiducial" state $|f\rangle$ and apply all d^2 displacement operators $\hat{D}_{jk}$, which shift the state in an algebraic way [15].

$$\hat{D}_{jk} = \omega^{jk/2} \sum_{m=0}^{d-1} \omega^{jm} |m \oplus k\rangle\langle m|, \tag{3.8}$$

Together, the set $\hat{D}_{jk}|\phi\rangle\}_{j,k=1}^{d}$ forms a SIC-POVM, covering all directions in the Hilbert space uniformly. The displacement operators use the d-th root of unity $\omega = e^{2\pi i/d}$ and addition modulo d to cycle consistently through the basis states.

It is noteworthy to remember in each dimension d, there is only one set of SIC-POVM basis, which has d^2 vectors, unlike the MUB where we had $d+1$ sets of bases.

As an example, in the two dimensional Hilbert space, there exist 4 SIC-POVM vectors. These vectors form a tetrahedral on the Bloch sphere, and they are set apart so that each of their separation angles with respect to one another is maximal.

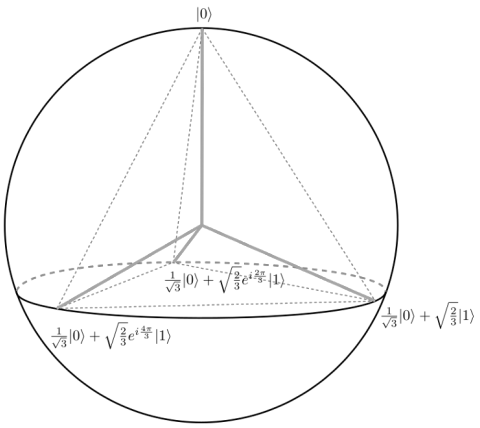


Figure 3.1: The four SIC-POVM vectors demonstrated on the Bloch sphere, showing a tetrahedral with maximally distanced angles. Figure adapted from [35].

The SIC-POVMs can be used in QKD, and have been implemented in the Singapore protocol [36]. In this protocol, a source sends out two anti-correlated photons to both Alice and Bob. In the two-dimensional scenario, each of the parties owns 4 detectors that detect the 4 possible outcomes, i.e. the 4 SIC-POVM vectors. We can name these 4 outcomes as A, B, C and D. If Alice's detector A starts signaling, we are sure that Bob's detector A will not signal due to the anti-correlation and the symmetry of SIC-POVMs. But given the properties of the SIC-POVMs, there is an equal possibility that Bob will get signal B, C, or D. Therefore, there is a 1/3 chance for Alice to guess Bob's signal. Afterwards, Alice and Bob can use either the Renes pairing or the iterative Singapore pairing to generate their key.

Investigating the Performance of Adaptive Optics on Different Bases of Spatial Modes in Turbulent Channels

Rojan Abolhassani,[1] Lukas Scarfe,[1] Francesco Di Colandrea,[1,2] Alessio D'Errico,[1,3] Khabat Heshami,[1,3] and Ebrahim Karimi[1,3,4,*]

[1] *Nexus for Quantum Technologies, University of Ottawa, Ottawa, K1N 6N5, ON, Canada*
[2] *Dipartimento di Fisica "Ettore Pancini", Università degli Studi di Napoli Federico II, Complesso Universitario di Monte Sant'Angelo, Via Cintia, 80126 Napoli, Italy*
[3] *National Research Council of Canada, 100 Sussex Drive, Ottawa, K1A 0R6, ON, Canada*
[4] *Institute for Quantum Studies, Chapman University, Orange, California 92866, USA*

Quantum key distribution (QKD) allows secure key exchange based on the principles of quantum mechanics, with higher-dimensional photonic states offering enhanced channel capacity and resilience to noise. Free-space QKD is crucial for global networks where fibres are impractical, but atmospheric turbulence introduces severe states' distortions, particularly for spatial modes. Adaptive optics (AO) provides a pathway to correct these errors, though its effectiveness depends on the encoding basis. Here, we experimentally evaluate a high-speed AO system for orbital angular momentum (OAM) modes, mutually unbiased bases (MUB), and symmetric, informationally complete, positive operator-valued measures (SIC-POVM) up to dimension $d = 8$ in a turbulent free-space channel. While OAM states are strongly distorted, their cylindrical symmetry makes them optimally corrected by AO, yielding error rates below QKD security thresholds. MUB and SIC-POVM exhibit greater intrinsic robustness to turbulence but are less precisely corrected, though their performance remains within protocol tolerances. These results establish AO as a key enabler of secure, high-dimensional QKD and highlight the role of basis choice in optimizing resilience and correction.

I. INTRODUCTION

Quantum key distribution (QKD) is a method of sharing a secure key over a public channel, where the sender, Alice, aims to establish a shared secure key with the receiver, Bob. The two parties, along with an eavesdropper, Eve, with access to the public channel, are only limited by the laws of physics
QKD can be implemented using different protocols, all based on the same fundamental principles, where the security of the communication is ensured by the impossibility of cloning unknown quantum states with 100% fidelity [1]. These protocols mostly differ in the set of non-orthogonal bases they use. Some of the most well-known protocols include the BB84 [2], the MUB (tomographic) protocol [3], or the Singapore protocol [4] – see [5] for a comprehensive survey of various QKD protocols employing spatial modes of light. By going to higher dimensions, having access to a larger alphabet, it is possible to encode more bits per sifted photons. This suggests that higher dimensions can increase the amount of secure information density per photon [6]. Moreover, higher-dimensional QKD protocols exhibit greater resilience to noise, thereby increasing the security threshold required to obtain a positive key in the presence of potential eavesdroppers [7].
While polarization is limited to two-dimensional (qubit) information encoding, spatial modes of light can be harnessed to encode quantum information in high-dimensional spaces [8–10]. A widely used spatial mode encoding makes use of superpositions of modes carrying orbital angular momentum (OAM). We can theoretically have unbounded orthogonal OAM-carrying states, and thus, encode information in d-dimensions rather than only two dimensions, hence the name qu*d*its instead of qu*b*its. These OAM carrying beams have a helical phase structure $e^{i\ell\phi}$, where ϕ is the azimuthal angle in cylindrical coordinates and ℓ is the topological charge, an integer representing the number of 2π phase windings around the beam axis. In addition, proper superpositions of these modes that form a new set of orthogonal modes can also be used as new bases for information carriers in QKD protocols [11].
QKD using spatial modes of light has been demonstrated in different channels such as optical fibres, [12–14], underwater [12, 15–17], or free space [18]. Free-space QKD can be implemented in places where fibre channels are not accessible, and is essential in scenarios such as satellite communications. One of the main obstacles faced in free-space QKD is the atmospheric turbulence, which can completely distort the phase of the signal beam, reducing or even compromising the security of the channel.
When the turbulence effects are weak enough to introduce mostly phase distortion and negligible amplitude modulations, we can compensate for the environmental noise by using fast adaptive optics (AO) systems [19]. Since adaptive optics systems have limited spatial resolution, their performance may vary depending on the selected sets of spatial modes. Therefore, not all modes behave the same under the same circumstances.

Here, we investigate the behaviour and performance of different high-dimensional superpositions of the

* ekarimi@uottawa.ca

OAM modes in the form of mutually unbiased bases (MUB) [20] and symmetric informationally complete positive operator-valued measure (SIC-POVM) [4] in turbulent channels. Our goal is to identify the optimal modes which are less vulnerable to turbulence and more effectively corrected using AO. Our findings indicate that AO systems achieve the highest correction performance for pure OAM modes; however, these modes are also the most sensitive to turbulence. In contrast, certain MUB superpositions demonstrate greater resilience to turbulence, though their error rates remain somewhat higher than those of the OAM basis. Nevertheless, the application of AO enables recovery of channel security, balancing resilience and correctability across different mode sets.

II. RESULTS

A. Theory

We begin by outlining the definitions of the basis sets considered in this work. The set of modes which carry quantised non-zero orbital angular momentum, $\{|\ell\}\rangle_{\ell\neq 0}$, is considered as the *logical* basis. The position $\mathbf{r}$ representation of these modes is considered to be Laguerre-Gaussian (LG) modes, $\langle \mathbf{r}|\ell\rangle := \mathrm{LG}_{\ell,p=0}(\mathbf{r})$, in transverse profile [21]. Here, p is the radial index, but for simplicity, we consider it to be equal to zero; apart from a normalization factor, the expression for such a beam is given by $r^{|\ell|}\, e^{i\ell\phi}\, e^{-(r/w_0)^2}$ with w_0 being the mode's beam waist.

Mutually Unbiased Bases: Mutually Unbiased Bases (MUB) are a set of bases, each consisting of an orthonormal and complete set of elements, in which each vector basis or element has the following relation with other elements from the different basis sets:

$$|\langle \beta_i^{(a)}|\beta_j^{(b)}\rangle|^2 = \frac{1}{d}, \quad a \neq b \tag{1}$$

where $\beta_i^{(a,b)}$ are elements of the basis (a) or (b), $i, j \in (1, d)$ and d is the dimension of the Hilbert space. We investigate every MUB in dimensions $d = 2, 3, 4, 5, 8$, of which there are $d + 1$ MUB. In each MUB, there are d orthogonal vectors. Sets of $d + 1$ MUB are known to exist in dimensions which are integer powers of a prime $d = p^n$ [20, 22]. Determining maximal sets of MUB in arbitrary dimensions remains an open problem [23]; even in dimension six ($6 = 2 \times 3$), which is not a prime power, a complete construction is still unknown. In the simplest case where $d = 2$, each MUB is given by the eigenvectors of the Pauli matrices. For polarization encoding, these (2+1=3) MUB correspond to horizontal and vertical polarization ($\{|H\rangle, |V\rangle\}$), diagonal and anti-diagonal ($\{|D\rangle, |A\rangle\}$), and left and right-circular polarizations ($\{|L\rangle, |R\rangle\}$). In experiments concerning the OAM of light, we use the $\mathrm{LG}_{\ell,0}$ modes as our logical bases and use them to build sets of MUB (considering d is a power of a prime number). For dimension d, we use ℓ from $\{-d, -d+1, ..., d-1, d\}$; however, $\ell = 0$ was excluded, for even dimensions. The main reason was the potential non-negligible cross-talk with the natural mode of the single-mode fibre (SMF) during the final measurement. When using MUB, the outcome of measurement in a basis different from the logical basis has the same probability for each input OAM value; therefore, no information about its preparation could be obtained by the eavesdropper.

Angular Basis: In the realm of high-dimensional QKD, the most commonly utilized secondary basis is generated by applying the discrete quantum Fourier transform to the logical OAM basis:

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

where $|j\rangle = \frac{d}{2} + (l-1)\Theta(\ell) + \ell\Theta(-\ell)$ and Θ is the Heaviside function, i.e. we use ℓ from $\{-d, -d+1, ..., d-1, d\}$ and exclude $\ell = 0$ for even dimensions. This MUB is referred to as the angular mode set when the logical basis is given by OAM eigenstates and is characterized by basis elements with peak intensity located at a specific azimuthal angle $\phi = 2\pi k/d$. This angular basis yields the same states as the first MUB in the prime dimension cases. This Fourier-conjugate basis exhibits mutual unbiasedness with respect to the logical basis, indicating that a state prepared in one basis will produce uniformly random measurement outcomes when assessed in the other. Such complementary relationships are crucial for ensuring the security of QKD protocols, as they enable the detection of potential eavesdropping through heightened error rates in the conjugate measurements.

SIC-POVM: Positive operator-valued measures (POVMs) are sets of positive semidefinite operators that describe generalized measurements on a quantum state. A POVM is said to be informationally complete (IC) if its measurement outcomes uniquely determine the state. Among these, a particularly important class is the symmetric informationally complete POVMs (SIC-POVMs), in which all elements share the same pairwise inner product, making them maximally efficient. Such sets provide a minimal spanning of the Bloch sphere and are widely regarded as optimal for state reconstruction [24]. It has been shown that in group-covariant cases, there are SIC-POVMs in all finite dimensions. SIC-POVMs in dimension d are a set of d^2 normalized vectors $|\phi\rangle$ such that:

$$|\langle \phi_i|\phi_j\rangle|^2 = \frac{1}{(1+d)}, \quad i \neq j\ . \tag{3}$$

Completeness and informational completeness both follow from this property. One way of creating SIC-POVM

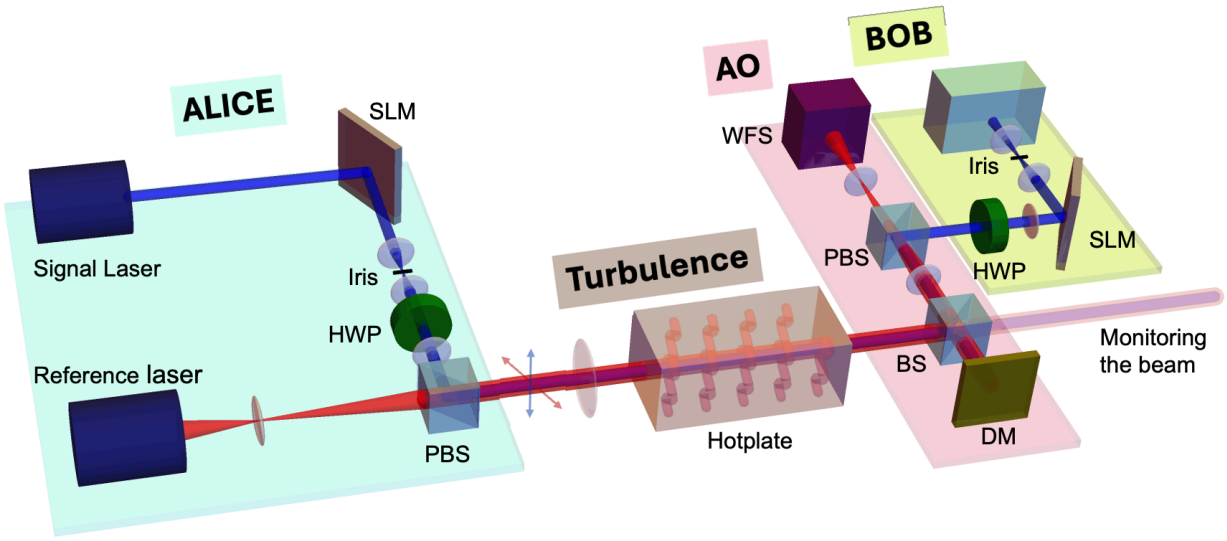


Figure 1. Experimental setup for transmitting quantum states of light and testing MUB, SIC-POVM, and Angular states through turbulent media. Turbulence is generated using a controllable hotplate placed inside a 30-cm-wide glass tank. The signal beam, encoded with spatial mode information (MUB, SIC-POVM, or Angular) via a spatial light modulator (SLM), is combined with the reference beam at a polarizing beam splitter (PBS) and both co-propagate through the turbulence cell. The composite beam is then split by a 50:50 beam splitter (BS): one part is directed to a side wavefront sensor (WFS) to monitor the output wavefront, while the other part is sent to the adaptive optics (AO) system (from ALPAO). The AO system consists of a deformable mirror (DM) and a WFS operating in closed-loop feedback, where the DM corrects distortions measured by the WFS. After AO correction, the signal and reference beams are separated using a PBS. The signal component is then directed to a second SLM, which performs projective measurements of the spatial modes and couples the selected mode into a single-mode fibre (SMF) for detection, while the reference beam is sent to the WFS.

elements is by applying the operator D_{ij}

$$D_{ij} = \omega^{jm}|k \oplus m\rangle\langle m|, \tag{4}$$

to a Fiducial vector $|\phi\rangle$ [25]. In this case $\oplus$ is the addition modulo d and $\omega = \exp(2\pi i/d)$. In dimension $d = 2$, the SIC-POVM corresponds to four pure states forming the vertices of a tetrahedron on the Bloch (Poincaré) sphere, which are mutually non-orthogonal. Such SIC-POVM bases have been employed in QKD protocols, for instance, in the Singapore protocol [4, 26], which exhibits higher error tolerance compared with traditional MUB (tomographic)- and BB84-based schemes.

B. Experiment

Experimental setup: The experimental setup consists of three main components: a sender (Alice), who prepares and encodes high-dimensional quantum information onto the spatial structure of photons; a turbulent channel, implemented using a controllable hotplate inside a 30 cm-wide glass tank; and a receiver (Bob), who ultimately decodes the transmitted states. The information-carrying beam is referred to as the signal beam. Alice prepares a continuous-wave 633 nm laser and directs it onto a phase-only spatial light modulator (SLM) to encode the desired state. By imprinting computer-generated holograms, the SLM modulates both the phase and the amplitude profile of the incoming beam [27, 28], thereby creating high-dimensional spatial modes for transmission (see Fig. 1). In parallel, a second laser produces a Gaussian reference beam that is introduced into the system to probe and compensate for turbulence. This reference beam is prepared with a polarization state orthogonal to that of the signal, ensuring that the two beams can be deterministically separated at later stages of the experiment. The signal and reference beams are combined at a polarizing beam splitter (PBS) and propagate collinearly through the turbulence cell, where both experience identical wavefront distortions. The turbulence itself is generated by the convection currents of a controlled hotplate placed at the base of the glass tank, producing refractive-index fluctuations representative of atmospheric conditions. After traversing the turbulence, the composite beam is directed to the AO system, consisting of a deformable mirror (DM, ALPAO) and a Shack–Hartmann wavefront sensor (WFS). A beam splitter (BS) divides the incoming light: one portion is directed to a second WFS for real-time wavefront measurements, while the DM reflects the other. WFS and DM are connected in a closed-loop con-

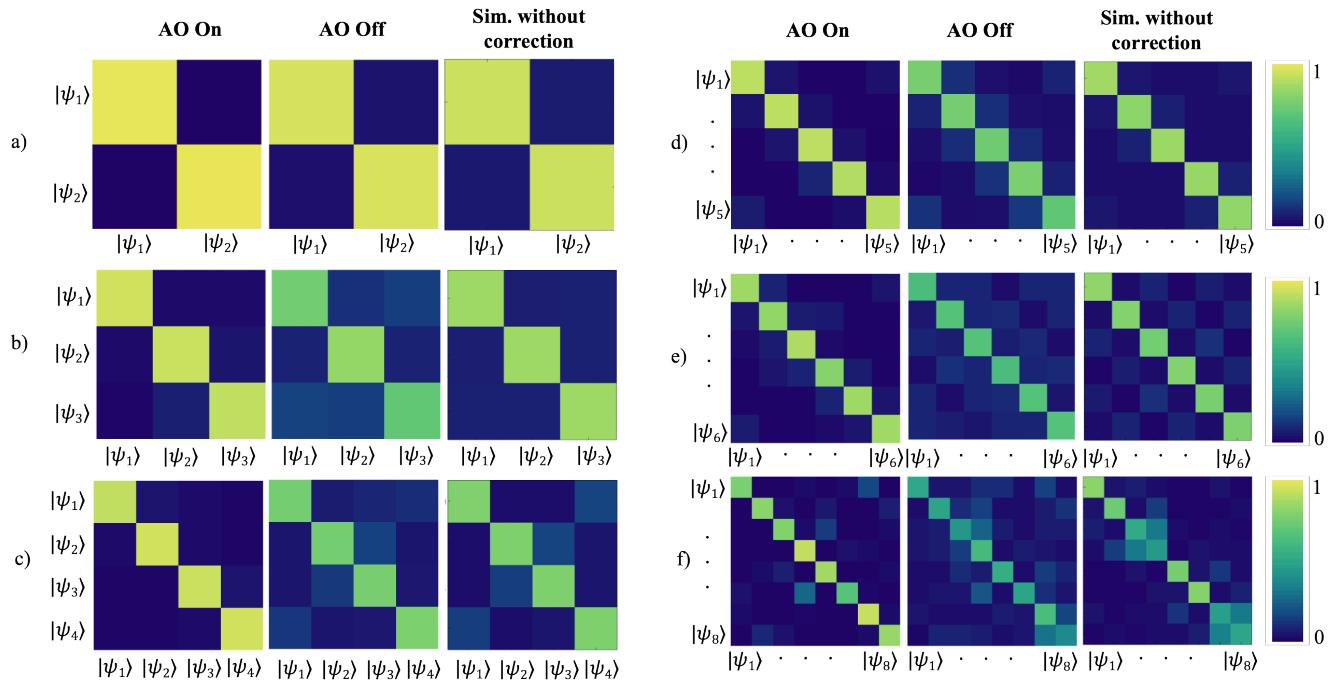


Figure 2. Cross-talk matrices of the first MUB for dimensions a) $d = 2$, b) $d = 3$, c) $d = 4$, d) $d = 5$, e) $d = 6$, and f) $d = 8$. Each panel displays three matrices for comparison: the first shows the experimental results obtained under turbulence with AO enabled (AO On), the second shows the corresponding experimental results under turbulence with AO disabled (AO Off), and the third presents numerical simulations of turbulence without correction (Sim). The comparison highlights the strong impact of turbulence on high-dimensional states and the significant improvement in mode fidelity achieved by AO correction, in close agreement with the simulated predictions.

trol configuration, allowing the DM to actively reshape its surface in response to the measured aberrations and thereby compensate for turbulence-induced distortions. Following this correction, the reference and signal beams are separated by a second PBS: the reference beam is sent to the WFS for continuous monitoring, while the signal beam is directed to Bob. At the receiver, Bob performs projective measurements on the signal beam over the chosen set of spatial modes. Here, the measurements are implemented using an intensity-flattening approach: a second SLM is programmed with phase masks that convert the incoming spatial modes into Gaussian-like profiles, which are then coupled into a SMF and detected [29]. This method provides high mode selectivity and allows faithful discrimination between the high-dimensional states transmitted through the channel. To characterize the level of turbulence introduced in the experiment, we compared the measured cross-talk matrices with theoretical predictions under different turbulence strengths. Agreement between simulation and experiment allowed us to estimate the effective refractive-index structure constant, $C_n^2 \approx 10^{-14.7}$ [30], which is typical of moderate atmospheric turbulence. Further details of the turbulence modelling and numerical simulations are provided in the Supplementary Material.

Cross-Talk Matrix and QDER Measurements: For each incoming basis, $\{|\psi_j\rangle\}$, Bob performs projective measurements of the signal beam onto the different modes, $\{|\langle\psi_i|\}$. In the case of MUB and angular (ANG) modes, the cross-talk is quantified by evaluating the projection probabilities $|\langle\psi_i|\psi_j\rangle|^2$ across all modes within the basis. To normalize the projective measurement matrix, each row is scaled so that its sum equals one. The resulting normalized matrix defines the cross-talk distribution:

$$C_{i,j} = \frac{|\langle\psi_i|\psi_j\rangle|^2}{\Sigma_{i=0}^{d-1}|\langle\psi_i|\psi_j\rangle|^2}. \tag{5}$$

The key metric used to assess the communication performance and analyze the security is the quantum dit error rate (QDER). It is obtained by calculating the average of the diagonal elements of the normalized cross-talk matrix, and subtracting this value from the theoretical maximum of unity,

$$\text{QDER} = 1 - \frac{\Sigma_{i=0}^{d-1} C_{ii}}{d}. \tag{6}$$

For the SIC-POVM, the cross-talk matrix is normalized so that each row sums to d, i.e.,

$$C_{i,j} = d \times \frac{|\langle\psi_i|\psi_j\rangle|^2}{\Sigma_{i=0}^{d^2-1}|\langle\psi_i|\psi_j\rangle|^2}. \tag{7}$$

In analogy to the MUB-based protocols, the QDER for SIC-POVMs can be estimated from the following expression:

$$\mathrm{QDER} = 1 - \frac{\mathrm{Tr}[C_{ii}]}{d^2}. \tag{8}$$

Here, $\mathrm{Tr}(\cdot)$ denotes the trace operation, applied to the cross-talk matrix. The quantum error is then obtained by subtracting the average of the diagonal elements of the measured matrix from the corresponding theoretical value.

Turbulence Compensation: Phase distortions induced by turbulence are corrected using a closed-loop AO system from ALPAO. The AO system comprises three primary components: a Shack–Hartmann wavefront sensor (WFS), a control computer, and a deformable mirror (DM). Unlike earlier AO systems based on segmented mirror arrays, the DM employed here consists of a continuous reflective surface actuated by 97 electromagnetic elements. This design eliminates aberrations that would otherwise arise from inter-element gaps [31]. By locally adjusting the mirror surface, the DM reshapes the reflected beam in real time. The signal and reference beams are separated at a polarizing beam splitter (PBS), with the reference beam directed to the WFS. The Shack–Hartmann WFS samples the wavefront by measuring the displacement of focal spots relative to their ideal positions on the detector array. These displacements are then decomposed into Zernike polynomials, a widely used set of orthonormal functions for describing optical aberrations. Each polynomial corresponds to a distinct type of aberration (e.g., defocus, astigmatism, coma), enabling a compact representation of the measured wavefront distortion. This wavefront information is processed by the control computer, which generates the corresponding corrective commands for the DM. By applying the conjugate phase to the incoming distorted beam, the DM compensates for the turbulence-induced aberrations. The feedback loop operates at kilohertz rates: the WFS used here functions at 1 kHz (with a maximum capability of 5 kHz), while the turbulence dynamics are on the order of 100 Hz. Thus, the AO corrections are effectively applied in real time relative to the evolution of the turbulent channel.

Experimental results: Using the setup described above, we performed experiments across different QKD protocols and Hilbert-space dimensions, evaluating the effects of turbulence and the corrective performance of the AO system. For each dimension, we measured the cross-talk matrices and extracted the corresponding QDER, both with AO disabled and enabled. Figure 2 shows the measured cross-talk matrices for different dimensions under both conditions, alongside numerical simulations based on the expected turbulence strength. From these results, QDER values were calculated for each basis and dimension. The corresponding results are summarized in Fig. 3, which presents the QDER for MUBs, OAM modes, and ANG modes in dimensions $d = 2, 3, 4, 5, 6$, and 8. We note that in the case of $d = 6$, which is not a prime power, only three MUBs are known [32, 33]; the analysis is therefore restricted to OAM and ANG modes, with the SIC-POVM case discussed separately.

Several clear trends emerge. First, higher-dimensional states are generally more susceptible to turbulence-induced errors. Second, activating the AO system significantly improves performance, reducing QDER values across all bases and dimensions. The AO correction is particularly effective for OAM modes, which, despite being highly distorted by turbulence, benefit strongly from the circular symmetry of the deformable mirror corrections. By contrast, certain MUB superpositions, while less corrected by AO, exhibit intrinsic robustness to turbulence due to their reduced spatial extent. These observations highlight an interplay between the geometric structure of the spatial modes and the corrective fidelity of the AO system. Modes with circularly symmetric profiles are more prone to turbulence but also more accurately corrected, whereas modes with localized lobes are less affected by turbulence but more challenging to correct. Intensity and phase profiles of these modes are shown in the Supplementary Material.

The results further demonstrate that AO reduces the QDER most effectively in lower dimensions, bringing values well below the security thresholds for QKD protocols such as BB84 (two MUBs) and six-state (tomographic) schemes (three MUBs) [5]. Specifically, in dimension two (Fig. 3(a)), the OAM and MUB states yield comparable QDERs; the ANG or first MUB basis emerges as the optimal choice in this regime. In dimension three (Fig. 3(b)), which includes the Gaussian $\ell = 0$ mode, we observe increased cross-talk, but the first MUB still performs better under turbulence and AO correction, making it a strong candidate alongside the OAM basis. In dimension four (Fig. 3(c)), the Gaussian mode was excluded, the first MUB again shows superior resilience, while the fourth MUB is the most fragile, though still recoverable with AO. For dimension five (Fig. 3(d)), the Gaussian mode component introduces additional noise, and although all bases are impacted, only the OAM and first MUB are well corrected. In dimension six (Fig. 3(e)), where only three MUB sets are known, results are only reported for OAM and ANG modes. Finally, in dimension eight (Fig. 3(f)), even with AO, some bases yield QDER approaching the security threshold, though OAM, ANG, and the first two MUBs remain viable candidates. Taken together, these results show that while turbulence strongly limits the fidelity of high-dimensional QKD, AO can substantially suppress the induced errors, bringing QDER values below security thresholds across a wide range of protocols and dimensions. This confirms the feasibility of secure, high-dimensional QKD over turbulent free-space channels when combined with an AO system.

Beyond testing the maximal sets of MUB available in a given dimension d, it is also important to evaluate the

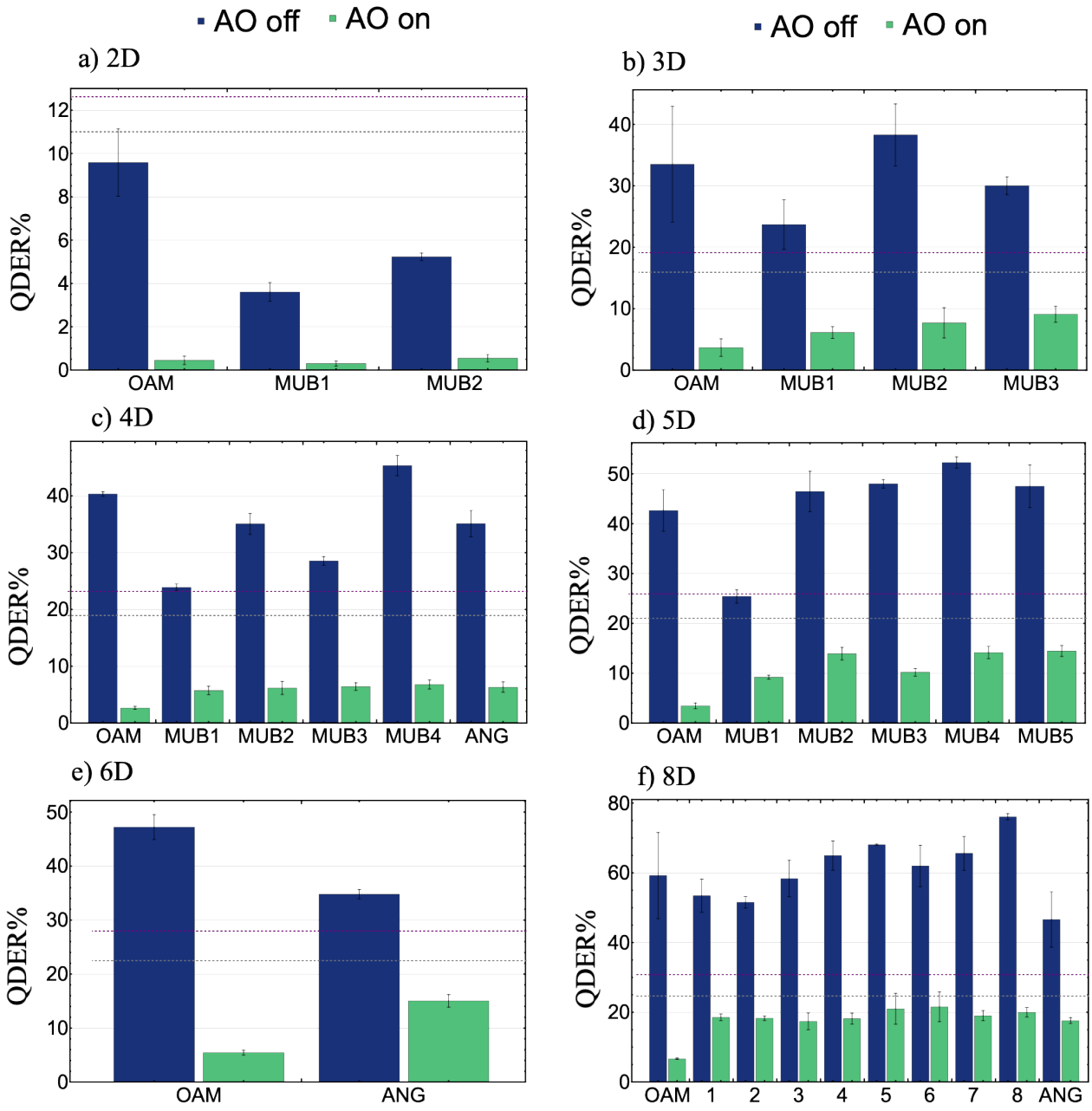
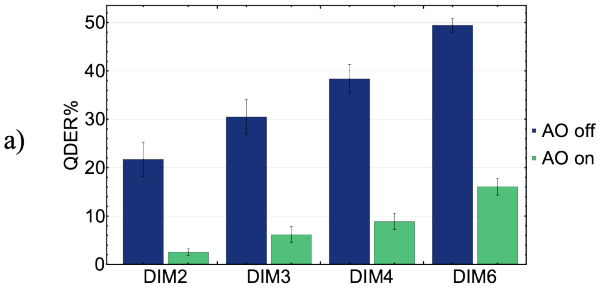


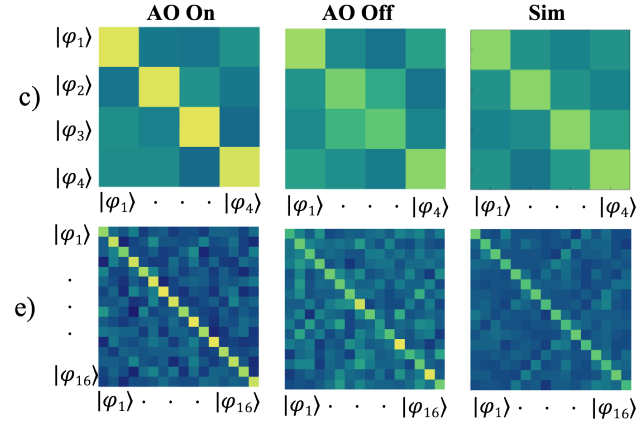
Figure 3. Quantum dit error rate (QDER) measured for different basis sets and Hilbert-space dimensions under turbulent conditions, with AO On (green) and with AO Off (blue). Panels a-f correspond to dimensions 2, 3, 4, 5, 6, and 8, respectively. Each bar shows the average QDER for OAM, MUB, and ANG bases (where applicable), with error bars representing statistical uncertainties. The dotted lines show the QDER thresholds for the BB84 (gray) and six-state (purple) protocols. The error lines on the bars indicate the standard deviation of the diagonal elements of each crosstalk matrix. The results demonstrate the strong effect of turbulence on high-dimensional states and the significant reduction in QDER achieved by AO correction.

capability of our AO system with other classes of states, thereby demonstrating its versatility for a broader range of quantum communication protocols. In particular, since no complete set of MUBs exists in dimension six, we consider alternative measurement frameworks such as SIC-POVMs, which in bi-dimensional space form the basis of the Singapore protocol [4]. Our experimental results (Fig. 4) show that SIC-POVM states are strongly affected by turbulence, leading to substantial cross-talk and elevated QDER. However, when AO correction is applied, the QDER is significantly reduced across all tested dimensions ($d = 2, 3, 4$, and 6), with values falling below the theoretical security threshold of the Singapore protocol. This demonstrates that while SIC-POVMs are in-



b)

Dimension	AVG AO On Turb Off QDER (%)	AVG AO On Turb On QDER (%)	AVG AO Off Turb on QDER (%)
2	2.49	2.55	21.72
3	4.34	6.18	30.51
4	4.73	8.87	38.40
6	12.99	16.08	49.44



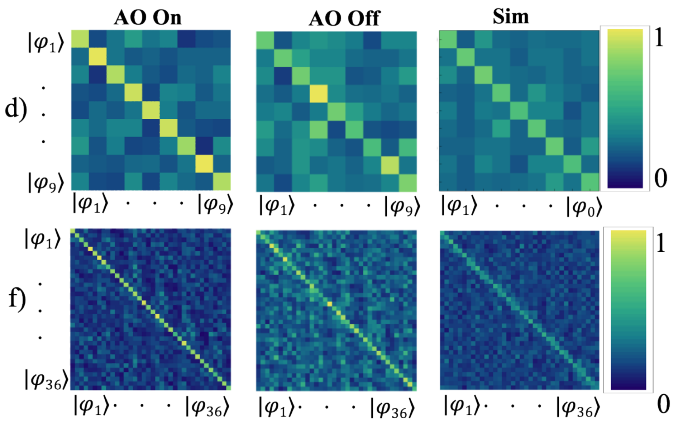


Figure 4. Cross-talk matrices and QDER for SIC-POVM modes under turbulence with and without AO correction. (a) Measured QDER for SIC-POVM modes transmitted through a turbulent channel, comparing AO-enabled (green) and AO-disabled (blue) scenarios. (b) Table summarizing the average QDER values obtained experimentally for SIC-POVM states in dimensions $d = 2$, $d = 3$, $d = 4$, and $d = 6$ under different conditions. (c–f) Experimental cross-talk matrices for SIC-POVM modes in dimensions 2, 3, 4, and 6, respectively, shown for AO enabled (AO On), AO disabled (AO Off), and numerical simulations of turbulence without correction (Sim). These results demonstrate the vulnerability of SIC-POVM states to turbulence and the significant reduction in error achieved by AO correction.

herently fragile in turbulent environments, AO correction restores their viability for secure quantum key distribution. The cross-talk matrices further confirm this conclusion: with AO enabled, the measured mode overlaps approach the expected theoretical distributions, in close agreement with numerical simulations. These results highlight both the susceptibility of SIC-POVM states to channel-induced distortions and the ability of AO systems to extend their practical utility in high-dimensional quantum communication protocols.

The security thresholds for different protocols are summarized in Table S1 for comparison [5]. Our results demonstrate that with AO correction, QKD can be implemented in turbulent channels while keeping error rates below the relevant security thresholds. At the same time, the results reveal that the AO system is not universal: it provides the most effective correction for specific mode families, particularly OAM modes. We also observe that certain modes exhibit greater intrinsic robustness to turbulence owing to their spatial localization.

III. CONCLUSIONS

In summary, we have systematically investigated the behaviour of all known MUBs and SIC-POVMs in multiple dimensions, up to $d = 8$, under turbulence, and assessed the effectiveness of their correction using AO. These results provide practical guidance for selecting the most suitable basis sets under different channel conditions and for different QKD protocols. In particular, we find that in low-turbulence regimes, the OAM basis–although most strongly distorted by turbulence–benefits most from AO correction and thus emerges as the optimal channel for information transmission. This suggests that QKD schemes could be designed such that the logical (OAM) basis carries the majority of information, while MUB are employed primarily for security checks, thus leveraging an unbalanced usage of the bases. An example is provided by the recently proposed Fourier-qubit QKD [34], where the OAM modes are applied more dominantly. Beyond QKD, the implications of our results extend to other domains that rely on spatial modes of light. In biological imaging and microscopy, where turbulence and aberrations are often unavoidable, AO can mitigate distortions when using Fourier conjugates of OAM modes [35–37]. Similarly,

our findings indicate that AO correction can enhance the performance of vortex-beam-based coronagraphy [38–40], further underscoring the broad applicability of these techniques.

Acknowledgment: This manuscript has been proofread with the assistance of a large language model (LLM). The authors acknowledge support from the Canada Research Chairs (CRC) program, the National Research Council of Canada High-Throughput and Secure Networks (HTSN) Challenge Program, the Qeyssat User INvestigation Team (QUINT) Alliance Consortia, and the Alliance for Research and Applications of Quantum Network Entanglement (ARAQNE) Alliance Consortia Quantum grants. FDC acknowledges support from the PNRR MUR project PE0000023-NQSTI.

Competing interests: The authors declare no competing interests.

Data Availability: All data associated with this work are available upon request to the corresponding author.

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

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE.

[3] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018–3021, October 1998.

[4] Berthold-Georg Englert, Christian Kurtsiefer, Kai Wen Moh, and Marek Żukowski. Efficient and robust quantum key distribution with minimal state tomography, 2004. Preprint.

[5] Frédéric Bouchard, Khabat Heshami, Duncan G. England, Robert Fickler, Robert W. Boyd, Berthold-Georg Englert, Luis L. Sánchez-Soto, and Ebrahim Karimi. Experimental investigation of quantum key distribution protocols with twisted photons. *Quantum*, 2:111, 2018.

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

[7] Sebastian Ecker, Frédéric Bouchard, Lukas Bulla, Florian Brandt, Oskar Kohout, Fabian Steinlechner, Robert Fickler, Mehul Malik, Yelena Guryanova, Rupert Ursin, and Marcus Huber. Overcoming noise in entanglement distribution. *PRX Quantum*, 4(1):010304, 2023.

[8] Gabriel Molina-Terriza, Juan P. Torres, and Lluis Torner. Management of the angular momentum of light: Preparation of photons in multidimensional vector states of angular momentum. *Physical Review Letters*, 88(1):013601, December 2001.

[9] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412:313–316, July 2001.

[10] G. Molina-Terriza, A. Vaziri, J. Reháček, Z. Hradil, and A. Zeilinger. Triggered qutrits for quantum communication protocols. *Physical Review Letters*, 92(16):167903, Apr 2004.

[11] Mohammad Mirhosseini, Omar S. Magaña-Loaiza, Malcolm N. O'Sullivan, Brandon Rodenburg, Mehul Malik, Martin P. J. 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, March 2015.

[12] A. Sit et al. Quantum cryptography with structured photons through a vortex fiber. *Optics Letters*, 43:4108–4111, 2018.

[13] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Physical Review Applied*, 11(6):064058, 2019.

[14] Q.-K. Wang 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(6):064034, 2021.

[15] A. Sit et al. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4:1006–1010, 2017.

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

[17] F. Hufnagel et al. Characterization of an underwater channel for quantum communications in the ottawa river. *Optics Express*, 27:26346–26354, 2019.

[18] Graham Gibson, Johannes Courtial, Miles J. Padgett, Mikhail Vasnetsov, Valeriy Pas'ko, Stephen M. Barnett, and Sonja Franke-Arnold. Free-space information transfer using light beams carrying orbital angular momentum. *Optics Express*, 12(22):5448–5456, 2004.

[19] Lukas Scarfe, 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. *Communications Physics*, 8, 2025. Accessed: 2025-08-12.

[20] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 8(4):535–640, 2010.

[21] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Physical Review A*, 45(11):8185–8189, 1992.

[22] William K Wootters and Brian D Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[23] Philippe Raynal, Xin Lü, and Berthold-Georg Englert. Mutually unbiased bases in six dimensions: The four most distant bases. *Phys. Rev. A*, 83:062303, Jun 2011.

[24] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical*

Physics, 45(6):2171–2180, 2004.

[25] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 06 2004.

[26] Markus Rambach, Mahdi Qaryan, Michael Kewming, Christopher Ferrie, Andrew G. White, and Jacquiline Romero. Robust and efficient high-dimensional quantum state tomography. *Phys. Rev. Lett.*, 126:100402, Mar 2021.

[27] Etienne Bolduc, Nathaniel Bent, Enrico Santamato, Ebrahim Karimi, and Robert W. Boyd. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Optics Letters*, 38(18):3546–3549, 2013.

[28] J. P. Kirk and A. L. Jones. Phase-only complex-valued spatial filter. *Journal of the Optical Society of America*, 61(8):1023–1028, 1971.

[29] Frédéric Bouchard, Natalia Herrera Valencia, Florian Brandt, Robert Fickler, Marcus Huber, and Mehul Malik. Measuring azimuthal and radial modes of photons. *Optics Express*, 26(24):31925–31941, 2018.

[30] Valerian Ilich Tatarski. *Wave propagation in a turbulent medium*. Courier Dover Publications, 2016.

[31] Robert K. Tyson. *Principles of Adaptive Optics*. CRC Press, Boca Raton, 4th edition, 2015.

[32] Stephen Brierley and Stefan Weigert. Maximal sets of mutually unbiased quantum states in dimension 6. *Phys. Rev. A*, 78:042312, Oct 2008.

[33] Stephen Brierley and Stefan Weigert. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A*, 79:052316, May 2009.

[34] Lukas Scarfe, Rojan Abolhassani, Frédéric Bouchard, Aaron Goldberg, Khabat Heshami, Francesco Di Colandrea, and Ebrahim Karimi. High-dimensional quantum key distribution with qubit-like states. *arXiv preprint*, 2025. Preprint posted on April 4, 2025.

[35] Zixuan Wu, Qi Liu, Yue Zhang, Hao Li, Wei Chen, Jianwei Xu, Jun Zhang, Wei Peng, Sheng Tang, and Guangcan Guo. Quantum-enhanced optical microscopy for subnanometer resolution imaging of protein complexes. *Light: Science & Applications*, 14:97, May 2025.

[36] Linyang Li, Xiao Liang, Wei Qin, Heng Guo, Weizhi Qi, Tian Jin, Jianbo Tang, and Lei Xi. Double spiral resonant mems scanning for ultra-high-speed miniaturized optical microscopy. *Optica*, 10(9):1195–1202, 2023.

[37] A. A. Pushkina, G. Maltese, J. I. Costa-Filho, P. Patel, and A. I. Lvovsky. Superresolution linear optical imaging in the far field. *Physical Review Letters*, 127(25):253602, 2021.

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

[39] David M. Palacios and Sarah L. Hunyadi. Low-order aberration sensitivity of an optical vortex coronagraph. *Optics Letters*, 31(19):2981–2983, 2006.

[40] D. Mawet, P. Riaud, O. Absil, and J. Surdej. Annular groove phase mask coronagraph. *The Astrophysical Journal*, 633(2):1191–1200, 2005.

[41] Tareq Jaouni, Lukas Scarfe, Frédéric Bouchard, Mario Krenn, Khabat Heshami, Francesco Di Colandrea, and Ebrahim Karimi. Predicting atmospheric turbulence for secure quantum communications in free space. *Opt. Express*, 33(5):10759–10776, Mar 2025.

[42] Max Born and Emil Wolf. *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light*. Cambridge University, 7 edition, 1999.

[43] Robert J. Noll. Zernike polynomials and atmospheric turbulence. *J. Opt. Soc. Am.*, 66(3):207–211, Mar 1976.

Supplementary Material for: Investigating the Performance of Adaptive Optics on Different Bases of Spatial Modes in Turbulent Channels

A. Details on numerical simulations

Our approach for numerical simulation of turbulence closely follows the method presented in Ref. [41], which we briefly review here. In our simulations, aberrations are modeled as a single phase screen $\xi(x, y)$ located at the sender plane $z = 0$:

$$\tilde{E}(x, y, z = 0) = E(x, y, z = 0)e^{i\xi(x,y)}, \tag{S1}$$

where $\tilde{E}$ and E are the aberrated and input fields, respectively. The phase screen is generated as a superposition of Zernike modes [42]:

$$\xi(\rho, \phi) = \sum_{n,m} c_{n,m} Z_{n,m}(\rho, \phi), \tag{S2}$$

where ρ is the normalized radial distance in the transverse plane: $\rho = \sqrt{x^2 + y^2}/\mathrm{Max}\left(\sqrt{x^2 + y^2}\right)$, where the maximum is taken across the spatial window considered for the simulations. The Zernike mode of order (n, m), with $n \geq |m| > 0$, is defined as

$$Z_{n,m}(\rho, \phi) = R_{n,|m|}(\rho) \cdot (\Theta(m) \cos m\phi + (1 - \Theta(-m)) \sin m\phi), \tag{S3}$$

where $R_{n,|m|}$ is the radial Zernike polynomial

$$R_{n,|m|}(\rho) = \sum_{k=0}^{\frac{n-|m|}{2}} \frac{(-1)^k (n-k)!}{k! \left(\frac{n+|m|}{2} - k\right)! \left(\frac{n-|m|}{2} - k\right)!} \rho^{n-2k} \tag{S4}$$

if $n - |m|$ is even and 0 if $n - |m|$ is odd. The weights of individual Zernike modes in Eq. (S2) are extracted from a zero-mean normal distribution depending on the turbulence conditions. Indeed, the variance $\sigma^2_{n,m}$ of the coefficient $c_{n,m}$ depends on the turbulence strength via the relation [43]

$$\sigma^2_{n,m} = \gamma_{n,m} \left(\frac{D}{r_0}\right)^{5/3}, \tag{S5}$$

where $\gamma_{n,m}$ is a mode-dependent coefficient, D is the receiver aperture, and r_0 is the Fried parameter. The latter can be determined from the C_n^2 [30]:

$$r_0 = 1.68 \left(C_n^2 L k^2\right)^{-3/5}, \tag{S6}$$

where L is the channel length and $k = 2\pi/\lambda$ is the light wavevector.

The propagation of the MUB states up to a distance z without turbulence can be directly obtained from the analytical expressions of the OAM modes, which constitute the logical basis. When turbulence is present, however, there is no analytical expression for the propagation, and Fresnel diffraction of aberrated modes must be numerically simulated:

$$\tilde{E}(x, y, z) = \frac{e^{ikz}}{i\lambda z} e^{\frac{i\pi}{\lambda z}(x^2+y^2)} \mathcal{F}(x, y, z), \tag{S7}$$

where

$$\mathcal{F}(x, y, z) = \iint \mathrm{d}x' \mathrm{d}y' \, \tilde{E}(x', y', 0) e^{i\frac{\pi}{\lambda z}(x'^2+y'^2)} e^{\frac{2\pi i}{\lambda z}(xx'+yy')}. \tag{S8}$$

Finally, each element (i, j) of the crosstalk matrices is obtained as the normalized mean of the overlap integrals between the i-th and the j-th modes, where the mean is performed over 100 random realizations of the chosen turbulence regime and the normalization is applied to each row independently. The overlap integral between a sent aberrated mode $\tilde{E}_j$ and a detected (non-aberrated) mode E_i is given by

$$\mathcal{I}_{i,j} = \iint \mathrm{d}x\mathrm{d}y\, E_i^*(x, y, z)\tilde{E}_j(x, y, z), \tag{S9}$$

where * denotes complex conjugation of the field. Since optical propagation acts as a unitary transformation on the beam, the overlap integrals can be computed at any distance along the propagation. For convenience, the overlap is evaluated at $z = 0$.

B. Table of Results

Dimension	**Basis**	**AVG AO On Turb Off QDER(%)**	**AVG AO On Turb On QDER(%)**	**AVG AO Off Turb on QDER(%)**	**BB84 Threshold QDER(%)**	**MUB protocol Threshold QDER(%)**
DIM 2	MUB 0 (OAM)	0.13± 0.03	0.45 ± 0.19	9.58± 1.56	11.00	12.62
	MUB 1	0.14± 0.09	0.30 ±0.12	3.61±0.43		
	MUB 2	0.32± 0.20	0.55± 0.173	5.23± 0.17		
DIM 3	MUB 0 (OAM)	1.67± 0.51	3.68±1.42	33.51±9.41	15.95	19.14
	MUB 1	5.11± 1.36	6.13±0.96	23.69±4.02		
	MUB 2	6.93± 2.87	7.70 ±2.470	38.28±5.05		
	MUB 3	7.96± 1.58	9.11±1.30	30.02±1.44		
DIM 4	MUB 0 (OAM)	1.10± 0.25	2.65 ± 0.28	40.33± 0.38	18.93	23.17
	MUB 1	4.32± 0.92	5.72± 0.74	23.91± 0.56		
	MUB 2	5.22± 1.01	6.16± 1.15	35.07± 1.85		
	MUB 3	4.54± 0.40	6.41± 0.66	28.54± 0.75		
	MUB 4	4.43± 0.99	6.78± 0.80	45.34± 1.77		
	ANG	4.35± 0.527	6.31± 0.914	35.12± 2.31		
DIM 5	MUB 0 (OAM)	1.074 ±0.21	3.46±0.57	42.66±4.17	20.99	25.94
	MUB 1	8.82±0.81	9.21±0.39	25.42±1.33		
	MUB2	11.67 ±1.63	13.92±1.26	46.46 ±4.05		
	MUB 3	8.73±0.48	10.19±0.78	48.00±0.85		
	MUB 4	13.43±1.67	14.16±1.22	52.30±1.12		
	MUB 5	14.01± 1.10	14.46±1.07	47.52 ±4.28		
DIM 6	OAM	3.27± 0.20	5.44± 0.448	47.23± 2.31	22.50	27.97
	ANG	14.65± 1.23	15.03± 1.16	34.79± 0.87		
DIM 8	MUB 0 (OAM)	2.68±1.14	6.67±0.25	46.64±7.94	24.70	30.77
	MUB 1	16.90±9.10	18.57±0.95	53.44±4.75		
	MUB 2	16.40±5.56	18.30±0.64	51.54±1.61		
	MUB 3	17.81±1.95	17.39±2.42	58.36 ±5.23		
	MUB 4	16.60±6.16	18.17 ±1.56	64.95 ±4.19		
	MUB 5	22.06±3.58	20.99 ±4.44	68.08 ±0.22		
	MUB 6	22.54±2.14	21.59 ±4.28	61.99 ±5.95		
	MUB 7	17.96±1.67	19.03 ±1.46	65.60 ±4.84		
	MUB 8	18.56 ±1.72	20.00 ±1.34	76.08 ±0.88		
	ANG	18.15±2.65	17.64 ±0.82	46.64 ±7.94		

Table S1. Table of experimental results showing Quantum dit error rates for all bases in different dimensions. The results refer to cases of adaptive optics turned on and off with turbulence on and off. The last two columns indicate the security threshold for doing QKD with different protocols like the BB84 and six-state or MUB protocol.

C. Phase-Intensity Plots of MUB

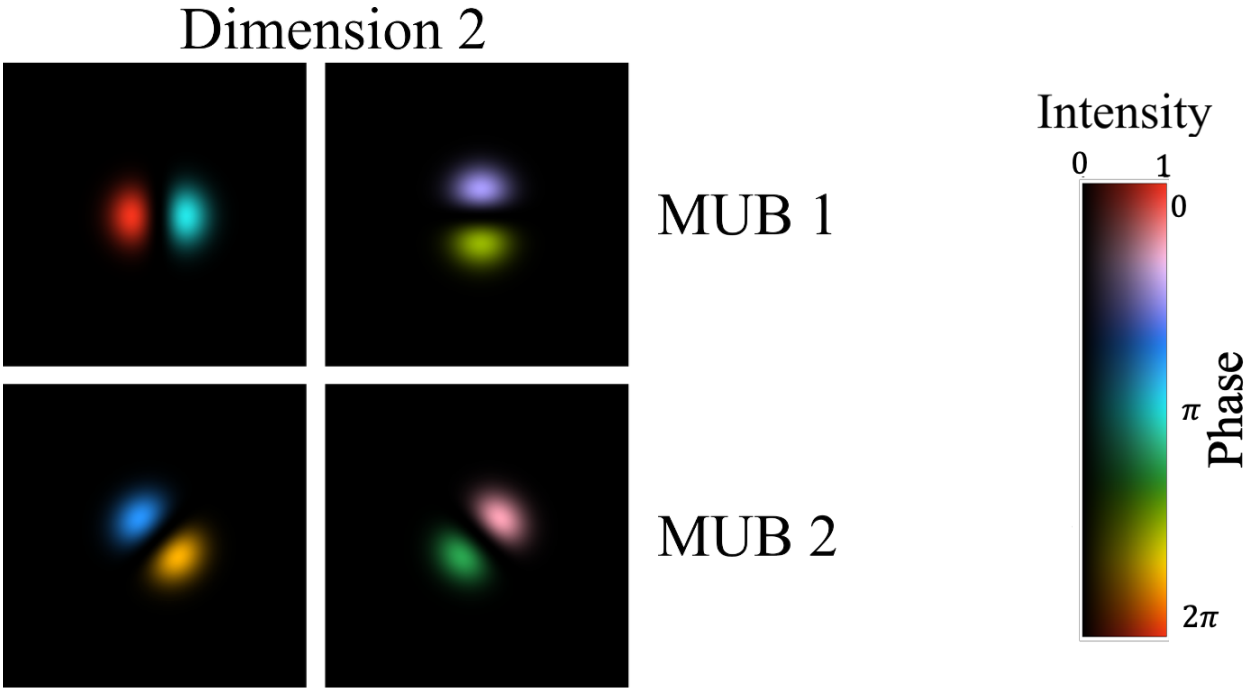


Figure S1. Phase and intensity plots of the MUB in dimension 2 using the OAM basis. Note that all phase-intensity plots use the same colour-scale as this plot.

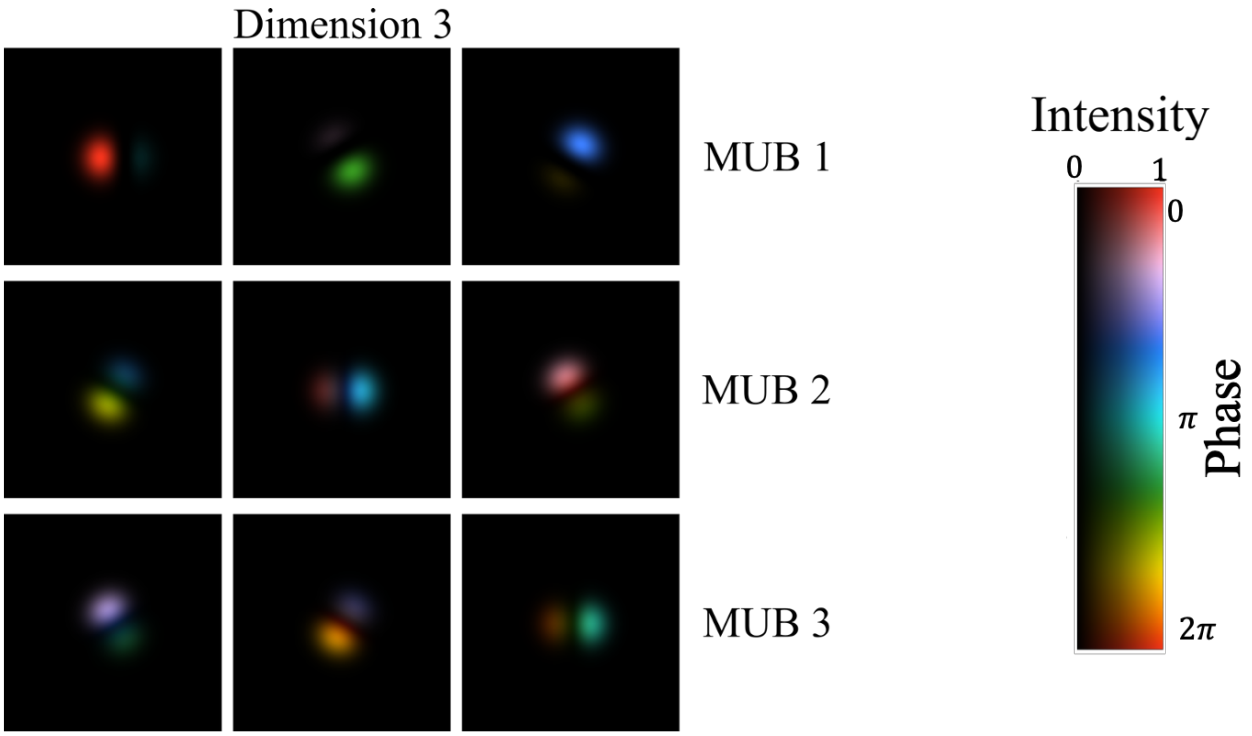


Figure S2. Phase and intensity plots of the MUB in dimension 3 using the OAM basis.

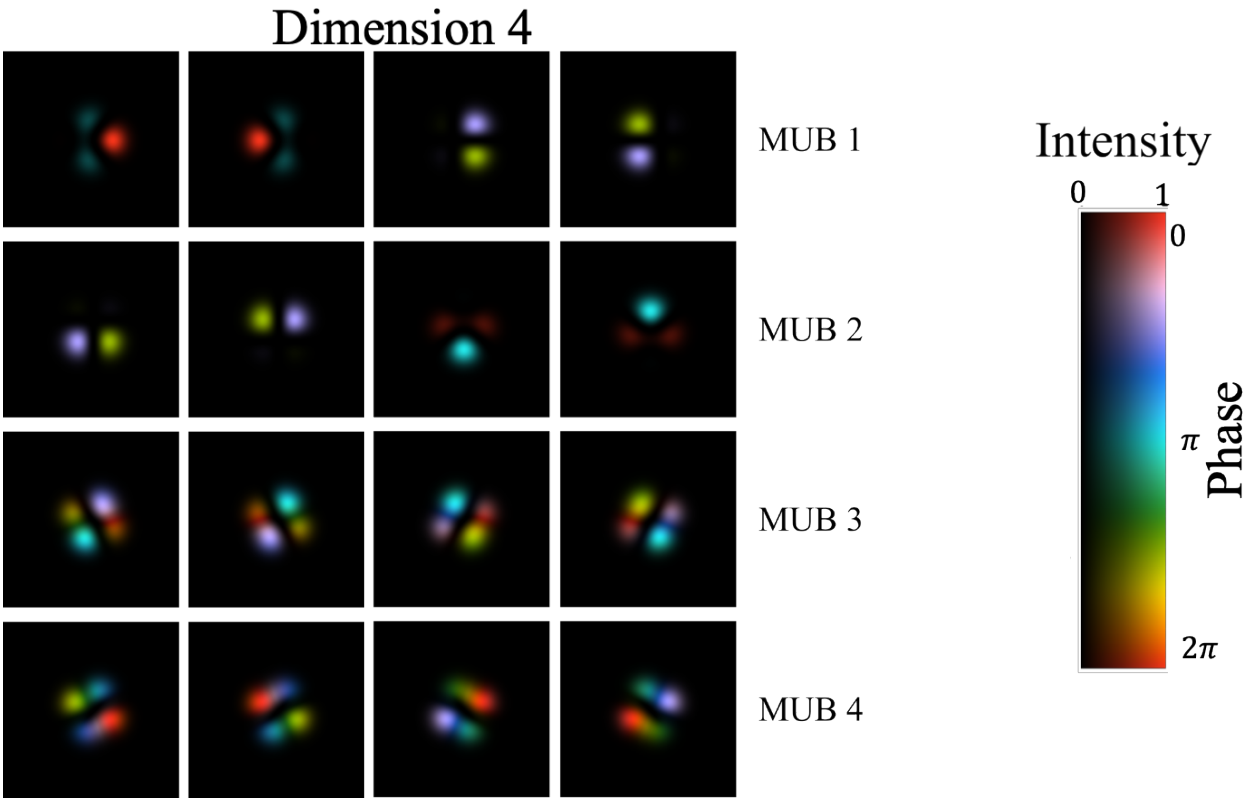


Figure S3. Phase and intensity plots of the MUB in dimension 4 using the OAM basis.

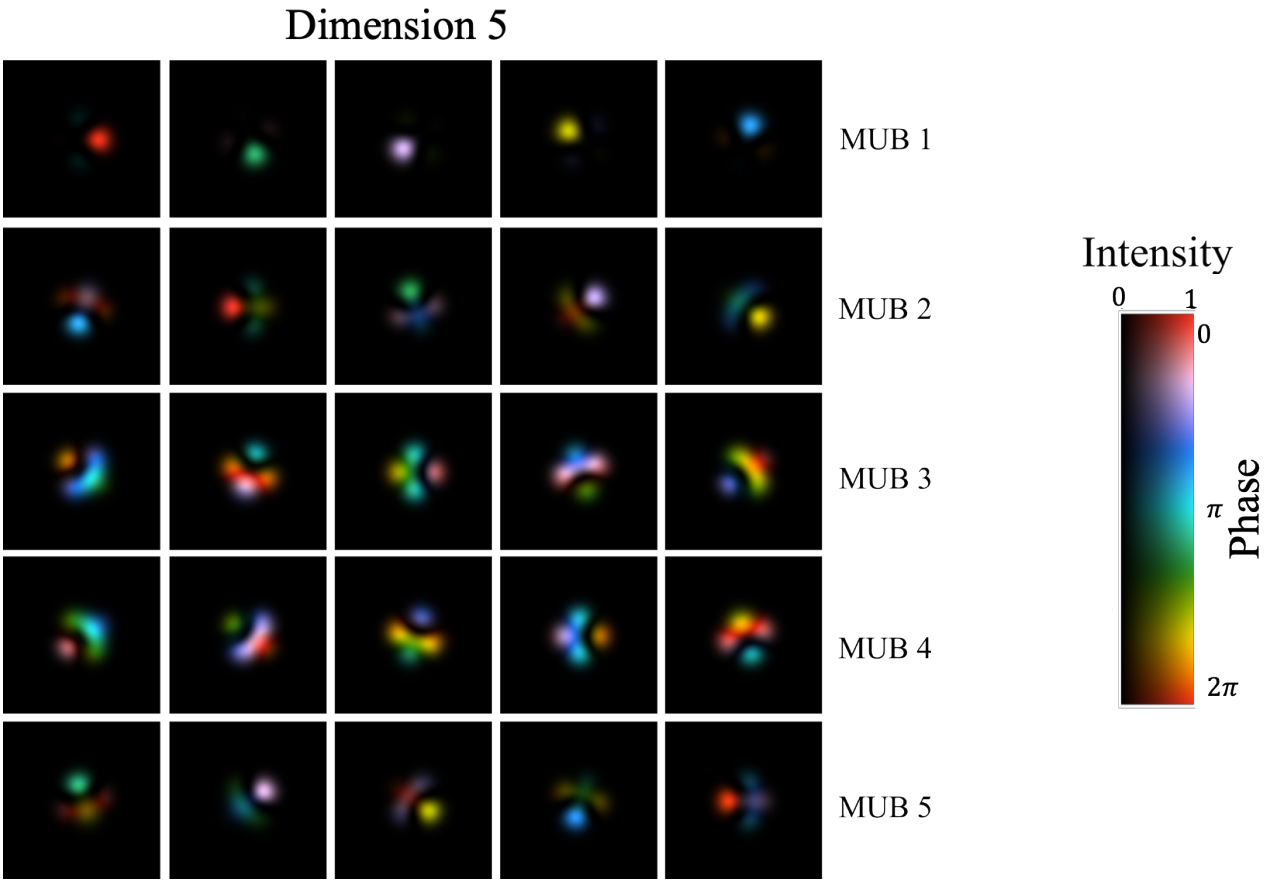


Figure S4. Phase and intensity plots of the MUB in dimension 5 using the OAM basis.

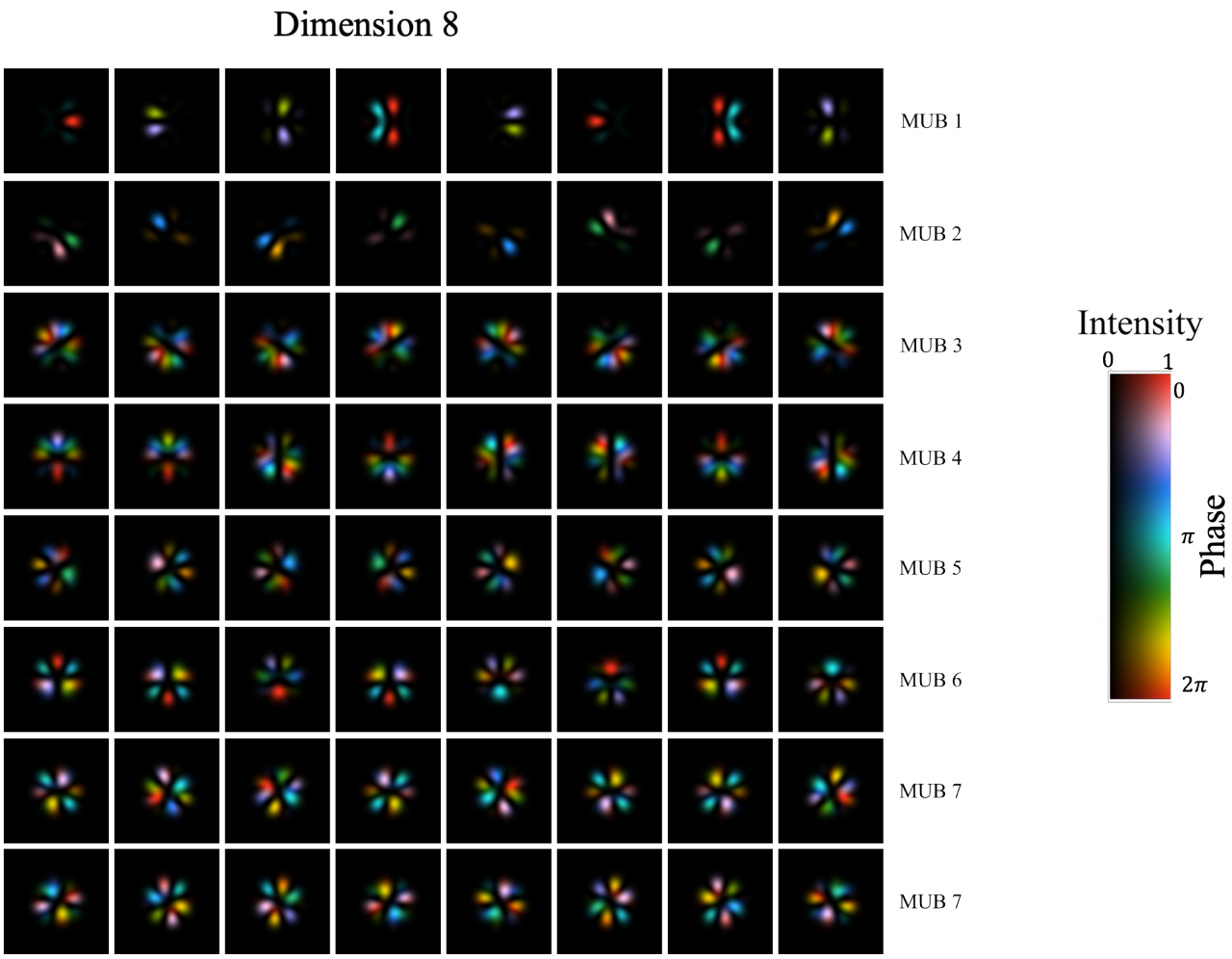


Figure S5. Phase and intensity plots of the MUB in dimension 8 using the OAM basis.

4

Chapter 4: A new protocol: Fourier Qubits

According to the results given in the last chapter, it was seen that the Adaptive optics system performs better for modes that are cylindrical, and have a uniform intensity distribution. To this end, the inspiration was to create a protocol that exploits modes with

these properties. The result was the following,

$$|\Phi_\ell^\pm\rangle = \frac{1}{\sqrt{2}}(|\ell\rangle \pm |-\ell\rangle) \tag{4.1}$$

However, without having a relative phase between the two states, the protocol does not span enough modes to enable a strong security proof, nor does it provide enough unbiasedness. It can be seen that the $|\Phi_\ell\rangle$ modes are unbiased to the $|\pm\ell\rangle$ modes from the logical basis, but not to one another or to $|\Phi_\ell\rangle$ modes with different ℓ values. From this came the F-qubit protocol discussed in the paper, where

$$|\Phi_{jk}^m\rangle = (|j\rangle + \omega_d^m |k\rangle)/\sqrt{2} \tag{4.2}$$

This protocol has the advantage of keeping the simplicity of being a qubit-like basis, so that creating and measuring the states are experimentally easier, especially in protocols involving the time-bins, yet they still possess higher information density due to the higher dimensionality.

4.1 Key rate

In QKD, even if no eavesdropper is present, there are still factors that contribute to Alice and Bob ending up with errors in their key rate, such as faults in the sources, losses in detectors or noises in the channel. In high-dimensional QKD, the probability that Bob

gets the wrong measurement is called the dit error rate, or E_d. When comparing a subset of their secret key, Alice and Bob can measure the E_d.

For a random variable X with probabilities $\{p_i\}$, the Shannon entropy is defined as

$$H(X) = -\sum_i p_i \log_2(p_i).$$

which can be defined as a measure of the possibility of an outcome. If the outcomes of a phenomenon are equally probable, then we have maximum entropy.

In this case, there is a $(1 - E_d)$ probability of Bob measuring the right outcome, and there are $d - 1$ cases with probability $\frac{E_d}{1-d}$ of giving the wrong outcome. Plugging these into the sum, we get

$$-(1-E_d)\log_2(1-E_d) - (d-1)\frac{E_d}{d-1} log_2(\frac{E_d}{d-1}) = -(1-E_d)\log_2(1-E_d) - E_d \log_2(\frac{E_d}{d-1}) \tag{4.3}$$

which is known as the d-ary Shannon entropy.

In BB-84, applying the same theory to the conjugate gives E'_d. Given the correction cost for this introduced error and the privacy amplification, we are led to define the asymptotic key rate R as [37]

$$R = \log_2(d) - H_d(E_d) - H_d(E'_d),$$

which is an indicator of the rate of key generation. $\log_2 d$ is the maximum amount of information you can encode in a single qudit, and H_d is the Shannon entropy in dimension d.

4.2 Eve's attack

Although collective attacks are some of the most complicated attempts Eve can make, it has been shown that once security against coherent attacks is guaranteed, we have unconditional security. Thus, it is only necessary to consider a general case of coherent attack for security proofs.

In a coherent attack, it is considered that Eve has access to all the signals at the same time. In this case, Eve treats the whole sequence of signals as one large quantum state. Eve can interact with it using a single probe, which may create correlations—even between signals that Alice and Bob think are separate. In order to do this, Eve jointly applies a unitary operator to both her ancilla and the signal photon

$$U_{Eve} |\eta_k\rangle |e_{00}\rangle = \Sigma_{j=0}^{d-1} c_{jk} |\eta_j\rangle |e_{jk}\rangle \tag{4.4}$$

With the BB-84 being a securely proven protocol, the security proof for the Fourier qubits has been examined in this work and established by showing that the phase and dit error rates are below the high-dimensional BB-84 limit.

communications physics

Article

A Nature Portfolio journal

https://doi.org/10.1038/s42005-025-02376-8

High-dimensional quantum key distribution with Qubit-like states

Lukas Scarfe [1] ✉, Rojan Abolhassani [1], Frédéric Bouchard [2], Aaron Z. Goldberg [2], Khabat Heshami [1,2], Francesco Di Colandrea [1,3] & Ebrahim Karimi [1,2,4]

Quantum key distribution (QKD) protocols most often use two conjugate bases in order to verify the security of the quantum channel. In the majority of protocols, these bases are mutually unbiased to one another, which is to say they are formed from balanced superpositions of the entire set of states in the opposing basis. Here, we introduce a high-dimensional QKD protocol using qubit-like states, referred to as Fourier-qubits (or *F*-qubits). In our scheme, each *F*-qubit is a superposition of only two computational basis states with a relative phase that can take *d* distinct values, where *d* is the dimension of the computational basis. This non-mutually-unbiased approach allows us to bound the information leaked to an eavesdropper, maintaining security in high-dimensional quantum systems despite the states' seemingly two-dimensional nature. By simplifying state preparation and measurement, our protocol offers a practical alternative for secure high-dimensional quantum communications. We experimentally demonstrate this protocol for a noisy high-dimensional QKD channel using the orbital angular momentum degree of freedom of light and discuss the potential benefits for encoding in other degrees of freedom.

Quantum Key Distribution (QKD) promises an information-theoretically secure method to distribute shared keys guaranteed by the fundamental laws of physics[1–3]. In order to distribute a secure key over an untrusted channel, Alice and Bob must prepare, exchange, and measure quantum states with few errors, which are not trivial tasks[4]. This difficulty has spawned many QKD protocols that can be more easily implemented with realistic devices and improve the secure key rates despite the practical challenges[5–7].

High-dimensional (HD) QKD protocols have attracted growing interest in recent years[8,9]. Indeed, by encoding information into a higher-dimensional Hilbert space, secure keys can be distributed with a higher density of information per photon[10]. In addition, these protocols can tolerate a greater error rate introduced by either an eavesdropper or simple channel noise[11]. While these benefits are enticing, the reality is that, up to this point, nearly all commercial QKD systems operate with two-dimensional QKD protocols[12]. Likewise, most fundamental research is focused on two-dimensional implementations[13]. The main reason is that encoding information in a high-dimensional Hilbert space poses significant technical challenges[14], with the complexity of experimental setups scaling proportionally to the dimensionality of the protocol. In contrast, a two-dimensional QKD system can process the polarisation degree of freedom, offering the advantage of cost-effective and straightforward passive generation and detection equipment.

The go-to QKD protocol, BB84, requires two mutually unbiased bases (MUB), where each basis consists of states in a balanced superposition of every state in the opposing basis. The two most common bases chosen are the computational (logical) basis and the Fourier basis[11,15,16]. In the *d*-dimensional implementation, the use of the Fourier basis requires precisely generating and measuring superpositions of *d* states.

In this work, we introduce a set of "qubit-like" states to be used in QKD alongside the logical basis in lieu of the Fourier basis. These states are qubit-like in the sense that they are only constructed as superpositions of two logical states, with a relative phase difference between them that is one of the *d* roots of unity. Because of the binary nature of these states, and their relation to the well-known quantum Fourier transform (QFT), we refer to these states as Fourier-qubits (or *F*-qubits). This reduction in the complexity of the states allows for simpler generation and detection[17]. While previous works with qubit-like states used them to increase the error tolerance up to the theoretical limit of 50%, the key rate remains that of a two-dimensional protocol, which is 1 bit per sifted photon[18,19]. Additionally, a recent work using a subset of the *F*-qubit states has shown that using qubit-like states in a HD protocol can greatly increase the information density of a time-bin coherent pulse-based QKD channel, albeit without an increase in error tolerance at higher dimensions[20]. Here, the *F*-qubits are used to complement the logical basis, whose states' generation and detection are the most simple,

[1]Nexus for Quantum Technologies, University of Ottawa, Ottawa, ON, Canada. [2]National Research Council of Canada, Ottawa, ON, Canada. [3]Dipartimento di Fisica, Università degli Studi di Napoli Federico II, Complesso Universitario di Monte Sant'Angelo, Napoli, Italy. [4]Institute for Quantum Studies, Chapman University, Orange, CA, USA. ✉e-mail: lscar039@uottawa.ca

and estimate the information leaked to a potential eavesdropper. This feature allows our QKD protocol to maintain the high-dimensional benefit of increased information density of $\log_2(d)$ bits per sifted photon, as well as the feature of error tolerance increasing with dimension, all while using relatively simple quantum states.

We theoretically prove that our protocol is secure from the most general coherent attack by an eavesdropper by demonstrating that the F-qubits can be used to indirectly measure the phase error rate. Additionally, we experimentally demonstrate the generation and detection of these modes in a noisy lab-scale channel using spatial modes of light in a 4-dimensional Hilbert space. In our test, the channel supports our F-qubit-based QKD protocol with a measured sifted key rate above 1 bit per sifted photon. We foresee our protocol being useful in implementations where high-dimensional QKD is desirable, such as high-bitrate and low-noise channels that are bandwidth-limited by the detector recovery time. Additionally, any system where the complexity of the quantum state scales with dimensionality will benefit from the implementation of the F-qubits.

Methods

Protocol

In our protocol, information is encoded onto qudits living in a d-dimensional Hilbert space. In particular, Alice and Bob prepare and measure their qudits in two separate bases. In the logical basis, information is encoded in states of the form $|\psi_n\rangle = |n\rangle$, where $n \in \{0, 1, \ldots, d-1\}$. Alice randomly selects n, serving as her raw key, and transmits the state $|n\rangle$ over an untrusted channel. Upon reception, Bob projects his incoming state on the same basis and uses the measurement outcome n' as his raw key. By iterating this process, Alice and Bob generate a raw key and use an authenticated classical channel to compare a small subset of their keys, estimating the error rate E_d to perform error reconciliation.

In order to bound Eve's leaked information, Alice and Bob also prepare and measure states in a second basis containing the F-qubit states:

$$|\phi_{jk}^m\rangle = (|j\rangle + \omega_d^m|k\rangle)/\sqrt{2}, \tag{1}$$

where $\omega_d = e^{2\pi i/d}$, $j \in \{0, 1\ldots, d-2\}$, $k \in \{1, 2, \ldots, d-1\}$, with $j < k$, and $m \in \{0, 1, \ldots, d-1\}$. A depiction of these modes in a time-bin implementation can be seen in Fig. 1. More precisely, Alice randomly selects a triplet (j, k, m), preparing the state $|\phi_{jk}^m\rangle$. Bob performs a measurement in the same F-qubit basis, projecting onto $|\phi_{j'k'}^{m'}\rangle$. Via classical communications, Alice and Bob can determine the probability of obtaining errors in the F-qubit basis. This information is used to estimate the phase error rate, E_d', to bound the information leaked to an eavesdropper as in BB84.

Finally, as in other high-dimensional BB84-like protocols, the secret key rate per sifted photon is given by[21]

$$R = \log_2(d) - h^{(d)}(E_d) - h^{(d)}(E_d'), \tag{2}$$

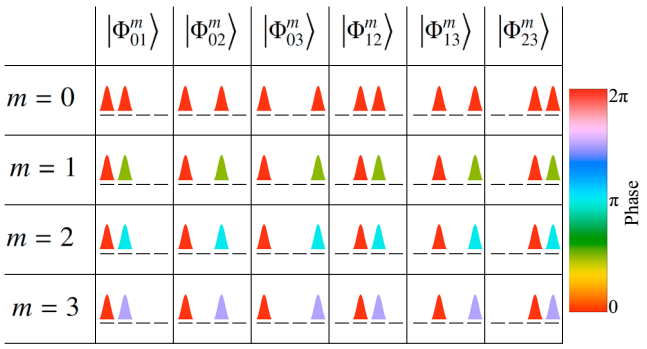


Fig. 1 | F-qubits in a 4-dimensional time-bin-based protocol. The logical basis consists of chopped Gaussian modes that are separated into time-bins $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. False colours encode the relative phase information.

where $h^{(d)}(x) = -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the d-dimensional Shannon entropy function, and E_d and E_d' are the channel dit error and phase error rates, respectively.

Results

Proof of security

Assuming the transmitted qudit is generated by an ideal single-photon source, the action of an eavesdropper, Eve, can be generally modeled as a coherent attack given by the unitary transformation U_{Eve}:

$$U_{\text{Eve}}|\eta_k\rangle|e_{00}\rangle = \sum_{j=0}^{d-1} c_{kj}|\eta_j\rangle|e_{kj}\rangle, \tag{3}$$

where $|e_{kj}\rangle$ is Eve's ancilla state and $|\eta_k\rangle$ is extracted from the Fourier-conjugate basis:

$$|\eta_k\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}\omega_d^{kn}|n\rangle. \tag{4}$$

Without loss of generality, we assume $c_{kj} \geq 0$ and $\langle e_{kj}|e_{rs}\rangle = \delta_{kr}\delta_{js}$.

The dit error rate of the Fourier basis, E_d', depends on the probability that Bob obtains a measurement of $|\eta_n\rangle$ conditioned on the fact that Alice prepares $|\eta_\ell\rangle$:

$$p(\eta_n|\eta_\ell) = \text{Tr}\left[|\eta_n\rangle\langle\eta_n|U_{\text{Eve}}|\eta_\ell\rangle\langle\eta_\ell| \otimes |e_{00}\rangle\langle e_{00}|U_{\text{Eve}}^\dagger\right] = c_{\ell n}^2. \tag{5}$$

We are now interested in relating the probability outcomes $p(\eta_n|\eta_\ell)$ in the Fourier basis to the measured probability outcomes of the qubit-like states. To do so, we use the fact that the F-qubit states can be rewritten in terms of the Fourier basis states as

$$\left|\phi_{jk}^m\right\rangle = \frac{1}{\sqrt{2d}}\sum_\ell\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)|\eta_\ell\rangle. \tag{6}$$

The probability that Bob obtains $|\phi_{j'k'}^{m'}\rangle$ conditioned on the fact that Alice prepares $|\phi_{jk}^m\rangle$ is thus given by

$$p\left(\phi_{j'k'}^{m'}|\phi_{jk}^m\right) = \frac{4}{d^2}\sum_{\ell n}\cos^2\left[\frac{\pi(m-(k-j)\ell)}{d}\right]\cos^2\left[\frac{\pi(m'-(k'-j')n)}{d}\right]p(\eta_n|\eta_\ell). \tag{7}$$

This relation can be inverted to find the probability outcomes $p(\eta_n|\eta_\ell)$ in the Fourier basis given the probability outcomes of the F-qubits,

$$p(\eta_n|\eta_\ell) = \frac{4}{d^4}\sum_{j<k}\sum_{j'<k'}\sum_{m,m'}\left(\beta + \sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p(m-(k-j)\ell)\right)\right)\left(\beta + \sum_{p'=0}^{d-1}\exp\left(\tfrac{2\pi i}{d}p'(m'-(k'-j')n)\right)\right)p\left(\phi_{j'k'}^{m'}|\phi_{jk}^m\right), \tag{8}$$

where $\beta = (2-d)/(d-1)$. For the full derivation of this relation, refer to Supplementary Note 3. Recall that the result of Eq. (2) is expressed in terms of the dit error rate (E_d) and the phase error rate (E_d') of the computational basis. Eve's leaked information is given by $I_{\text{AE}} \leq h^{(d)}(E_d')$[22], where I_{AE} is the mutual information between Alice and Eve. Explicitly, the dit error rate in the Fourier basis is given by

$$E_d' = \frac{1}{d}\sum_{\ell\neq n}p(\eta_n|\eta_\ell). \tag{9}$$

Using the fact that the dit error rate in the Fourier basis is equal to the phase error in the computational basis[23], we have then linked the probability outcomes of the F-qubits to phase error rate of the computational basis.

With both the dit and phase error rates in the channel, Alice and Bob can perform error correction and generate a secure key so long as both errors are below the tolerable threshold[24].

Finally, the secret key rate per sifted photon is given by

$$\begin{aligned} R &= \log_2(d) - h^{(d)}(E_d) - I_{\mathrm{AE}} \\ &\geq \log_2(d) - h^{(d)}(E_d) - h^{(d)}(E'_d). \end{aligned} \tag{10}$$

We have shown the protocol to be secure under what is considered a collective attack[25], which could be extended to general attacks[26].

Implementation

We test the generation and detection of these modes in a hypothetical orbital angular momentum (OAM) based protocol through a noisy short-distance free-space optical channel. In particular, we use Laguerre-Gaussian (LG) beams, each carrying a discrete value of OAM, ℓ[27], forming a 4-dimensional Hilbert space. The phase and intensity of the spatial modes are shown and labeled in Fig. 2. The F-qubit modes are generated by impinging a 633 nm beam from a HeNe laser onto a spatial light modulator (SLM) displaying a grated hologram designed to precisely control phase and intensity[28] of an output beam. The traditional Fourier basis consists of small areas of intensity located around a ring. Due to their small intensity distributions, SLMs have a low efficiency in both generation and detection of the modes as compared to the F-qubits, which have a larger intensity distribution that utilizes more of the SLMs' active area. The beam carrying the F-qubit, along with a Gaussian beam of the same wavelength and opposite polarisation, are sent through a channel with noise simulated by a turbulent cell, as well as an adaptive optics system as a corrective element[29]. A simplified experimental setup is shown in Fig. 3. Further information on the use of the noisy channel and the adaptive optics system can be found in Supplementary Note 1. As our security proof is as of now only valid for a single-photon model, our tolerable error rates should be considered in the case of a perfect single-photon source.

The F-qubit mode is sent to another SLM where a projective measurement is performed using intensity and phase masking[30]. Each generated mode is projectively measured on all states. These measurements are normalized to create a probability outcome matrix shown in Fig. 4 according to the procedure outlined in Supplementary Note 2. This probability outcome matrix of the F-qubit basis is then used to calculate the phase error rate, as shown in Eqs. (8), (9). We calculate the phase error rate, E'_d, by minimizing the distance between left and right sides of Eq. (7). This minimization is performed in order to avoid unphysical solutions present due to detector noise. Using measurements of the computational basis, we directly determine the bit error rate in the channel.

In our noisy channel, we find that the dit error rate, E_d, is 2.89%, and the phase error rate, E'_d, is 6.91%. After error correction and privacy amplification, the resulting sifted key rate in this channel, as given in Eq. (2), would be $R = 1.28$ bits per photon.

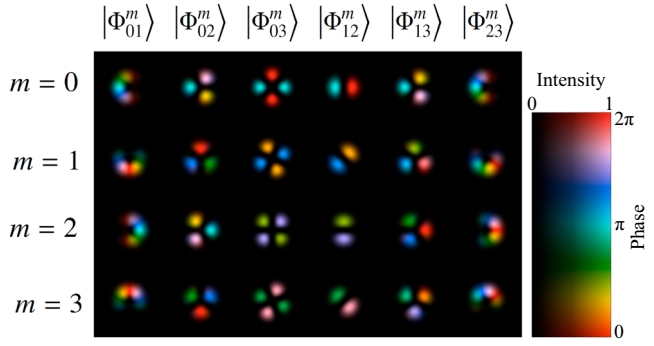


Fig. 2 | F-qubits in a 4-dimensional orbital angular momentum (OAM) based protocol. The logical basis consists of a set of LG modes, carrying discrete units of OAM, $|\ell\rangle$, $\ell \in \{-2, -1, 1, 2\}$. False colours and opacity encode the phase and amplitude information, respectively.

Conclusions

We have introduced a high-dimensional quantum key distribution protocol that uses qubit-like states in the secondary basis. Due to their qubit-like nature, the preparation and detection of F-qubits is significantly less complex than traditional MUB states, while maintaining the benefits of high-dimensional protocols, namely the increase in information density and error tolerance. By fixing the number of modes within each state to two, we fix the measurement complexity regardless of the dimension of the system, which has been shown to reduce errors in the detection stage[31]. We have experimentally implemented these qubit-like modes in a noisy lab-scale OAM-based QKD channel, achieving a sifted key rate above 1 bit per sifted photon.

The F-qubit basis is overcomplete and is constructed of $d^2(d-1)/2$ states, with a factor of d^2 more states than the traditional BB84 protocol. This is not a problem in the limit of infinite key length, but it should be considered for real-world implementations. Nevertheless, this issue can be alleviated with an unbalanced basis choice[23], wherein the F-qubits are only used to estimate the error rate of the channel and not for key generation, and are generated at a lower rate than the logical basis. This, in addition to the

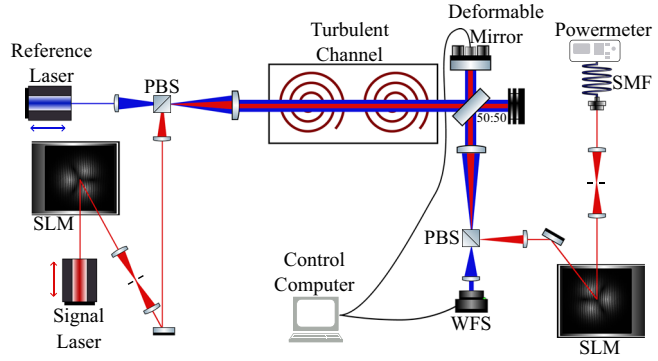


Fig. 3 | Experimental setup to generate and measure the F-qubit modes encoded using orbital angular momentum (OAM) in a noisy channel. The reference and signal lasers are both of wavelength 633 nm, with the red and blue representing orthogonal polarisations. The mode of the reference beam is a Gaussian, expanded to approximate a plane wave that is used as a probe of the turbulence measured by the wavefront sensor (WFS). The signal laser is impinged on a spatial light modulator (SLM), which is used to apply the phase and intensity of the F-qubit modes encoded as a superposition of LG modes carrying OAM. These beams are made to propagate co-linearly using a polarising beam splitter (PBS) and sent through the turbulent channel. They are subsequently separated after being corrected by the adaptive optics mirror. The F-qubit mode is projectively measured using a second SLM and coupled into a single-mode fibre (SMF).

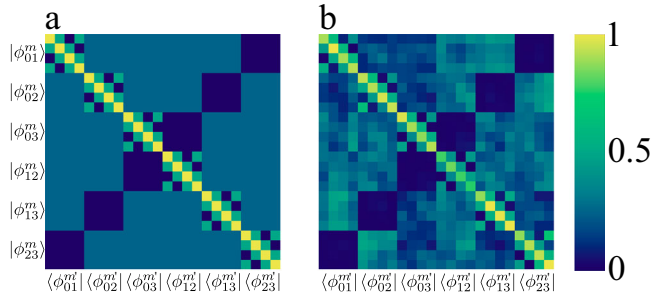


Fig. 4 | Probability outcome matrices of F-qubit basis in 4 dimensions. Each subgroup of 4×4 is representative of $|\langle\phi^m_{ij}|\phi^{m'}_{i'j'}\rangle|^2$ where $m, m' \in \{0, \ldots d-1\}$. **a** Theoretical probability outcome matrix with no errors. **b** Experimentally measured probability outcome matrix through our noisy channel using orbital angular momentum encoding as described by Fig. 2.

significant increase of the number of modes used, could significantly increase the block size of the exchanged bits required to perform real-world QKD with this protocol.

A common issue facing QKD systems is that the bandwidth of the channel is restricted by the limitation of single-photon-detector recovery times[32]. These types of channels are particularly suited to implementing high-dimensional QKD in order to increase the information density per photon; meanwhile the simplicity of the *F*-qubits makes them useful in many different high-dimensional encoding schemes. For example, the implementation in a time-bin encoding simply requires a variable-length interferometer. Beyond QKD, we feel that these modes will have use in fields other than quantum communications, such as quantum sensing and imaging.

Data availability

Data from the results presented in this paper may be obtained from the authors upon reasonable request.

Received: 9 May 2025; Accepted: 14 October 2025;
Published online: 25 November 2025

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Computer Sci.* **560**, 7–11 (2014).
2. Gottesman, D. & Lo, H.-K. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457–475 (2003).
3. Zahidy, M. et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nat. Commun.* **15**, 1651 (2024).
4. Zhang, H. et al. Noise-reducing quantum key distribution. *Rep. Prog. Phys.* **88**, 016001 (2024).
5. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005).
6. Yin, Z.-Q. et al. Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **88**, 062322 (2013).
7. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
8. Vagniluca, I. et al. Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Phys. Rev. Appl.* **14**, 014051 (2020).
9. Sit, A. et al. High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
10. Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
11. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using *d*-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
12. Oesterling, L., Hayford, D. & Friend, G. Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 156–161 (2012).
13. Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).
14. Cozzolino, D., Da Lio, B., Bacco, D. & Oxenløwe, L. K. High-dimensional quantum communication: Benefits, progress, and future challenges. *Adv. Quantum Technol.* **2**, 1900038 (2019).
15. Cozzolino, D. et al. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Phys. Rev. Appl.* **11**, 064058 (2019).
16. Forbes, A., Youssef, M., Singh, S., Nape, I. & Ung, B. Quantum cryptography with structured photons. *Appl. Phys. Lett.* **124**, 110501 (2024).
17. Wang, S. et al. Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme. *Quantum Sci. Technol.* **3**, 025006 (2018).
18. Chau, H. F. Quantum key distribution using qudits that each encode one bit of raw key. *Phys. Rev. A* **92**, 062324 (2015).
19. Chau, H. F., Wang, Q. & Wong, C. Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit- and qudit-based protocols. *Phys. Rev. A* **95**, 022311 (2017).
20. Sulimany, K. et al. High-dimensional coherent one-way quantum key distribution. *npj Quantum Inf.* **11**, 16 (2025).
21. Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 1–4 (2010).
22. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
23. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
24. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
25. Biham, E. & Mor, T. Bounds on information and the security of quantum cryptography. *Phys. Rev. Lett.* **79**, 4034–4037 (1997).
26. Renner, R. & Cirac, J. I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).
27. Allen, L., Beijersbergen, M. W., Spreeuw, R. J. C. & Woerdman, J. P. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Rev. A* **45**, 8185–8189 (1992).
28. Bolduc, E., Bent, N., Santamato, E., Karimi, E. & Boyd, R. W. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Opt. Lett.* **38**, 3546–3549 (2013).
29. Scarfe, L. et al. Fast adaptive optics for high-dimensional quantum communications in turbulent channels. *Commun. Phys.* **8**, 79 (2025).
30. Bouchard, F. et al. Measuring azimuthal and radial modes of photons. *Opt. Express* **26**, 31925–31941 (2018).
31. Lib, O., Sulimany, K., Araújo, M., Ben-Or, M. & Bromberg, Y. High-dimensional quantum key distribution using a multi-plane light converter. *Opt. Quantum* **3**, 182–188 (2025).
32. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J. & Gauthier, D. J. Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **3**, e1701491 (2017).

Acknowledgements

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 Alliance Consortia Quantum Grant (QUINT, ARAQNE). Francesco Di Colandrea further acknowledges support from the PNRR MUR project PE0000023-NQSTI.

Author contributions

L.S. & E.K. conceived of the idea. F.B. & A.Z.G. worked on the proof of security. L.S. & R.A. performed the experiment. F.D.C. performed the numerical simulations. L.S., R.A., & F.D.C. analyzed the data. L.S. & F.B. wrote the first draft of the manuscript. K.H. & E.K. supervised the project. All authors contributed to the final version of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-025-02376-8.

Correspondence and requests for materials should be addressed to Lukas Scarfe.

Peer review information *Communications Physics* thanks Kfir Sulimany and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.

Supplementary Information for: "High-Dimensional Quantum Key Distribution with Qubit-like States"

Supplementary Note 1: Inspiration

These modes were initially conceptualized to behave well with an adaptive optics (AO) system. Previous work using our AO system has indicated that it will have a larger impact correcting modes with cylindrical symmetry and uniform intensity distributions [1, 2]. Looking to make a QKD protocol that takes advantage of these properties, we designed a d-dimensional orthogonal basis of modes with cylindrical symmetry and uniform intensity distributions, see Fig. **S1**. These modes are a subset of the full F-qubit basis where $j = -k = \ell$, and $m \in \{0, d/2 - 1\}$, given in Eq. S1

$$\left|\phi_\ell^\pm\right\rangle = \frac{1}{\sqrt{2}}\left(|\ell\rangle \pm |-\ell\rangle\right) \tag{S1}$$

The error rates in the noisy lab-scale turbulent environment shows that these modes and those in the logical basis are both affected by turbulence and corrected by the AO system equally. The level of "Unbiasedness" of these two bases, however, is too low to reasonably perform any QKD experiment guaranteeing security. The idea of a encoding high dimensional information in a "qubit-like" state stayed and the more general set of F-qubit modes discussed in the paper, $\left|\phi_{j,k}^m\right\rangle$, were conceived.

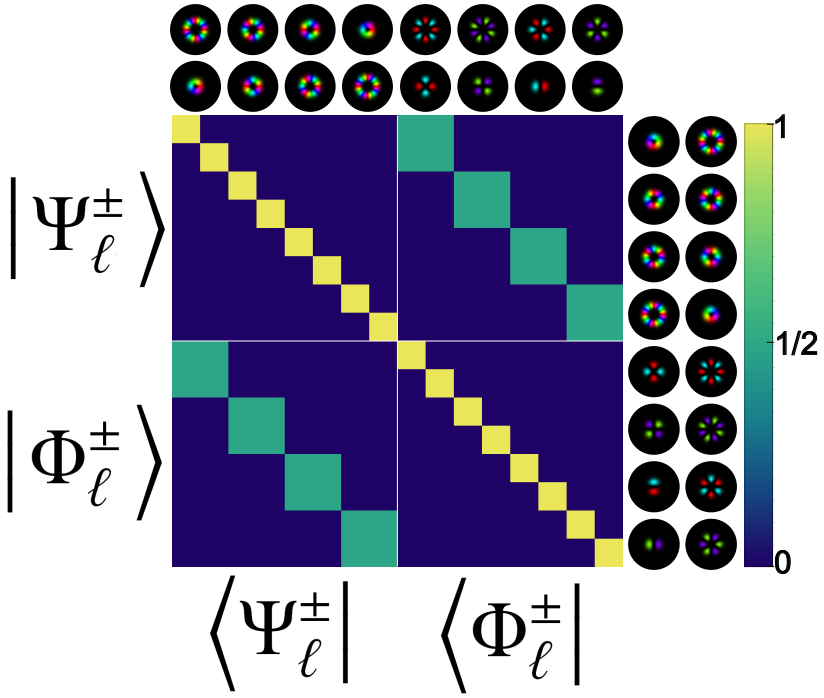


Figure S1. **Original modes in an 8-dimensional OAM-based protocol.** The originally conceptualized set of modes and the probability of detection matrices. False color is given to the optical modes to represent the relative phase information.

Supplementary Note 2: Normalization of F-qubit Measurements

For the normalization of the probability outcomes from measurements in the qubit-like basis, we use the completeness relation of the $|\phi_{jk}^m\rangle$ states:

$$
\begin{aligned}
\sum_m \sum_{j<k} |\phi_{jk}^{(m)}\rangle\langle\phi_{jk}^{(m)}| &= \frac{1}{2}\sum_m \sum_{j<k} \left(|j\rangle + \omega_d^m |k\rangle\right)\left(\langle j| + \omega_d^{-m}\langle k|\right) \\
&= \frac{1}{2}\sum_m \sum_{j<k} \left(|j\rangle\langle j| + \omega_d^{-m}|j\rangle\langle k| + \omega_d^m |k\rangle\langle j| + |k\rangle\langle k|\right) \\
&= \frac{1}{2}\sum_m \sum_{j<k} (|j\rangle\langle j| + |k\rangle\langle k|) \\
&= \frac{1}{2} d \sum_{j<k} (|j\rangle\langle j| + |k\rangle\langle k|) \\
&= \frac{1}{2} d(d-1)\hat{I},
\end{aligned}
$$

where $\hat{I}$ is the d-dimensional identity matrix and where we have used the property that $\sum_m \omega_d^m = 0$ and $\sum_m \omega_d^{-m} = 0$. This completeness relation can then be used to normalize raw counts.

$$
\begin{aligned}
\sum_{m'} \sum_{j'<k'} p(j', k', m'|\hat{\rho}) &= \sum_{m'} \sum_{j'<k'} \mathrm{Tr}\left[|\phi_{j'k'}^{(m')}\rangle\langle\phi_{j'k'}^{(m')}| \cdot \hat{\rho}\right] \\
&= \mathrm{Tr}\left[\sum_m \sum_{j<k} |\phi_{j'k'}^{(m')}\rangle\langle\phi_{j'k'}^{(m')}| \cdot \hat{\rho}\right] \\
&= \mathrm{Tr}\left[\frac{1}{2} d(d-1)\hat{I} \cdot \hat{\rho}\right] \\
&= \frac{1}{2} d(d-1)\mathrm{Tr}\left[\hat{\rho}\right] \\
&= \frac{1}{2} d(d-1).
\end{aligned} \tag{S2}
$$

Finally, the normalization condition is explicitly given by

$$
\sum_{m'} \sum_{j'<k'} p(j', k', m'|\hat{\rho}) = \frac{d(d-1)}{2}. \tag{S3}
$$

Derivation of inversion relation of Equation (8)

We start from the following relations linking the Fourier basis to the qubit-like basis,

$$
\begin{aligned}
&p(\phi_{j'k'}^{m'}|\phi_{jk}^{m}) \\
&= \frac{4}{d^2} \sum_{\ell n} \cos^2\left[\frac{\pi(m - (k-j)\ell)}{d}\right] \\
&\qquad \cos^2\left[\frac{\pi(m' - (k'-j')n)}{d}\right] p(\eta_n|\eta_\ell).
\end{aligned} \tag{S4}
$$

This relation can also be inverted by finding the coefficients $\alpha_{jj'kl'mm'}^{(\ell,n)}$ such that

$$
p(\eta_n|\eta_\ell) = \sum_{j<k} \sum_{j'<k'} \sum_{m,m'} \alpha_{jj'kk'mm'}^{(\ell,n)} p(\phi_{j'k'}^{m'}|\phi_{jk}^{m}).
$$

We now derive an analytical expression for $\alpha^{(\ell,n)}_{jj'kk'mm'}$ by starting with the assumption that it can be written as the following product with appropriate separation of variables, i.e.,

$$\alpha^{(\ell,n)}_{jj'kk'mm'} = \alpha^{(\ell)}_{jkm}\alpha^{(n)}_{j'k'm'}. \tag{S5}$$

Let us also define the following expressions,

$$\beta^{(\ell)}_{jkm} = \frac{2}{d}\cos^2\left[\frac{\pi(m-(k-j)\ell)}{d}\right]. \tag{S6}$$

By doing so, we get the following forward relation,

$$p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}) = \sum_{\ell n}\beta^{(\ell)}_{jkm}\beta^{(n)}_{j'k'm'}p(\eta_n|\eta_\ell). \tag{S7}$$

By multiplying both side of this equation by $\alpha^{(\ell')}_{jkm}\alpha^{(n')}_{j'k'm'}$ and summing over $j<k$, $j'<k'$, m and m', we get,

$$\begin{aligned}\sum_{j<k}\sum_{j'<k'}\sum_{m,m'}\alpha^{(\ell')}_{jkm}\alpha^{(n')}_{j'k'm'}p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}) = \\ \sum_{j<k}\sum_{j'<k'}\sum_{m,m'}\sum_{\ell n}\alpha^{(\ell')}_{jkm}\alpha^{(n')}_{j'k'm'}\beta^{(\ell)}_{jkm}\beta^{(n)}_{j'k'm'}p(\eta_n|\eta_\ell).\end{aligned}$$

We thus need to find $\alpha^{(\ell')}_{jkm}$ and $\alpha^{(n')}_{jkm'}$, such that,

$$\begin{aligned}\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m} &= \delta_{\ell,\ell'} \\ \sum_{j'<k'}\sum_{m'}\alpha^{(n')}_{j',k',m'}\beta^{(n)}_{j',k',m'} &= \delta_{n,n'},\end{aligned}$$

to retrieve the backward relation, i.e.,

$$\begin{aligned}\sum_{j<k}\sum_{j'<k'}\sum_{m,m'}\alpha^{(\ell')}_{jkm}\alpha^{(n')}_{j'k'm'}p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}) = \\ \sum_{\ell n}\delta_{\ell,\ell'}\delta_{n,n'}p(\eta_n|\eta_\ell) = p(\eta_{n'}|\eta_{\ell'}).\end{aligned} \tag{S8}$$

Let us try the following solution for $\alpha^{(\ell)}_{j,k,m}$,

$$\alpha^{(\ell)}_{j,k,m} = \frac{2}{d^2}\left(\frac{2-d}{d-1} + \sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p\,(m-(k-j)\ell)\right)\right). \tag{S9}$$

We now need to show that,

$$\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m} = \delta_{\ell,\ell'}.$$

Inserting the explicit form of $\alpha^{(\ell')}_{j,k,m}$ and $\beta\, j,k,m^{(\ell)}$, we get

$$
\begin{aligned}
&\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m} \\
=\;&\sum_{j<k}\sum_{m}\left(\frac{2}{d^2}\left(\frac{2-d}{d-1}+\sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell'\right)\right)\right)\right. \\
&\left.\left(\frac{2}{d}\cos^2\left(\frac{\pi(m-(k-j)\ell)}{d}\right)\right)\right) \\
=\;&\frac{2}{d^3}\sum_{j<k}\sum_{m}\left(\frac{2-d}{d-1}+\sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell'\right)\right)\right) \\
&\left(1+\cos\left(\frac{2\pi}{d}\left(m-(k-j)\ell\right)\right)\right) \\
=\;&\frac{2}{d^3}\sum_{j<k}\sum_{m}\left(\frac{2-d}{d-1}+\sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell'\right)\right)\right) \\
&\left(1+\frac{1}{2}\exp\left(\frac{2\pi i}{d}\left(m-(k-j)\ell\right)\right)+\frac{1}{2}\exp\left(\frac{-2\pi i}{d}\left(m-(k-j)\ell\right)\right)\right). \\
=\;&\frac{2}{d^3}\sum_{j<k}\left[\sum_{m}\left(\frac{2-d}{d-1}\right)+\frac{1}{2}\left(\frac{2-d}{d-1}\right)\sum_{m}\exp\left(\frac{2\pi i}{d}\left(m-(k-j)\ell\right)\right)\right. \\
&+\frac{1}{2}\left(\frac{2-d}{d-1}\right)\sum_{m}\exp\left(\frac{-2\pi i}{d}\left(m-(k-j)\ell\right)\right) \\
&+\sum_{m}\sum_{p}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell'\right)\right) \\
&+\frac{1}{2}\sum_{m}\sum_{p}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell'\right)\right)\exp\left(\frac{2\pi i}{d}\left(m-(k-j)\ell\right)\right) \\
&\left.+\frac{1}{2}\sum_{m}\sum_{p}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell'\right)\right)\exp\left(\frac{-2\pi i}{d}\left(m-(k-j)\ell\right)\right)\right]
\end{aligned}
\tag{S10}
$$

We can now make use of the following orthogonality relation,

$$
\sum_{m=0}^{d-1}\exp\left(\frac{2\pi i}{d}ms\right)=d\delta_{s,0}.
$$

Continuing with our derivation,

$$
\begin{aligned}
&\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m} \\
=\;& \frac{2}{d^3}\sum_{j<k}\Bigg[d\left(\frac{2-d}{d-1}\right) \\
&+\sum_{p} d\delta_{p,0}\exp\left(\frac{-2\pi i}{d}p(k-j)\ell'\right) \\
&+\frac{1}{2}\sum_{p} d\delta_{p,d-1}\exp\left(\frac{-2\pi i}{d}p(k-j)\ell'\right)\exp\left(\frac{-2\pi i}{d}(k-j)\ell\right) \\
&+\frac{1}{2}\sum_{p} d\delta_{p,1}\exp\left(\frac{-2\pi i}{d}p(k-j)\ell'\right)\exp\left(\frac{2\pi i}{d}(k-j)\ell\right)\Bigg] \\
=\;& \frac{2}{d^2}\sum_{j<k}\Bigg[\left(\frac{2-d}{d-1}\right)+1 \\
&+\frac{1}{2}\exp\left(\frac{2\pi i}{d}(k-j)(\ell'-\ell)\right)+\frac{1}{2}\exp\left(\frac{-2\pi i}{d}(k-j)(\ell'-\ell)\right)\Bigg] \\
=\;& \frac{2}{d^2}\sum_{j<k}\left[\left(\frac{1}{d-1}\right)+\cos\left(\frac{2\pi}{d}(k-j)(\ell'-\ell)\right)\right].
\end{aligned}
\tag{S11}
$$

We note here that the expression in the sum only depends on the difference between j and k, namely $r = k - j$. We can then re-arrange the sum over j and k as follows,

$$
\sum_{j<k} \longrightarrow \sum_{r=1}^{d-1}(d-r).
$$

We now have,

$$
\begin{aligned}
&\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m} \\
=\;& \frac{2}{d^2}\sum_{r=1}^{d-1}(d-r)\left[\left(\frac{1}{d-1}\right)+\cos\left(\frac{2\pi}{d}r(\ell'-\ell)\right)\right].
\end{aligned}
\tag{S12}
$$

In order to show that the right-hand side here is equal to $\delta_{\ell,\ell'}$, let us consider two distinct cases, i.e., the case where $\ell = \ell'$ and $\ell \neq \ell'$. If we find that the right hand side is equal to 1 in the former case and 0 in the latter case, we have thus proven that it is equal to the Kronecker delta function, $\delta_{\ell,\ell'}$.

We start with the first case of $\ell = \ell'$.

$$
\begin{aligned}
&\sum_{j<k}\sum_{m}\alpha^{(\ell)}_{j,k,m}\beta^{(\ell)}_{j,k,m} \\
=\;& \frac{2}{d^2}\sum_{r=1}^{d-1}(d-r)\left[\left(\frac{1}{d-1}\right)+1\right] \\
=\;& \frac{2}{d^2}\left(\frac{d}{d-1}\right)\sum_{r=1}^{d-1}(d-r) \\
=\;& \frac{2}{d}\left(\frac{1}{d-1}\right)\left(d(d-1)-\frac{(d-1)d}{2}\right) \\
=\;& 1.
\end{aligned}
\tag{S13}
$$

We now need to show the second case where $\ell \neq \ell'$.

$$\begin{aligned}
&\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m} \\
&= \frac{2}{d^2}\sum_{r=1}^{d-1}(d-r)\left[\left(\frac{1}{d-1}\right)+\cos\left(\frac{2\pi}{d}r(\ell'-\ell)\right)\right] \\
&= \frac{2}{d^2}\left[\frac{1}{d-1}\sum_{r=1}^{d-1}(d-r)\right. \\
&\qquad \left.+\sum_{r=0}^{d-1}(d-r)\cos\left(\frac{2\pi}{d}r(\ell'-\ell)\right)-d\right] \\
&= \frac{2}{d^2}\left[\frac{1}{d-1}\frac{d(d-1)}{2}+\sum_{r=0}^{d-1}(d-r)\cos\left(\frac{2\pi}{d}r(\ell'-\ell)\right)-d\right] \\
&= \frac{2}{d^2}\left[-\frac{d}{2}+\sum_{r=0}^{d-1}(d-r)\cos\left(\frac{2\pi}{d}r(\ell'-\ell)\right)\right] \\
&= \frac{1}{d^2}\left[-d+\sum_{r=0}^{d-1}(d-r)\exp\left(\frac{2\pi i}{d}r(\ell'-\ell)\right)\right. \\
&\qquad \left.+\sum_{r=0}^{d-1}(d-r)\exp\left(\frac{-2\pi i}{d}r(\ell'-\ell)\right)\right].
\end{aligned} \tag{S14}$$

If we take a closer look now at the following sum, i.e.,

$$\sum_{r=0}^{d-1}(d-r)\exp\left(\frac{2\pi i}{d}r(\ell'-\ell)\right), \tag{S15}$$

We realize that is not quite the orthogonality relation we are used to. We can try to calculate the sum in our case of $\ell \neq \ell'$.
We start by defining a generating function, $G(z)$, given by,

$$\begin{aligned}
G(z) &= \sum_{r=0}^{d-1}(d-r)z^r \\
&= \sum_{r=0}^{n}(n+1-r)z^r,
\end{aligned} \tag{S16}$$

where we have defined $n = d-1$. By doing so, we can use the well known result for finite geometric series, namely,

$$S(z) = \sum_{r=0}^{n} z^r = \frac{1-z^{n+1}}{1-z}, \tag{S17}$$

which is true for $z \neq 1$, which also holds true since $\ell \neq \ell'$.
Our generating function then takes the following form,

$$G(z) = \sum_{r=0}^{n}(n+1-r)z^r = (n+1)S(z) - \sum_{r=0}^{n} r\, z^r. \tag{S18}$$

We can now differentiate $S(z)$ with respect to z,

$$S'(z) = \sum_{r=0}^{n} r z^{r-1}. \tag{S19}$$

Thus, we can rewrite our generating function as,

$$G(z) = (n+1)S(z) - zS'(z). \tag{S20}$$

Let us now perform the differentiation of $S(z)$ explicitly,

$$\begin{aligned} S'(z) &= \frac{-(n+1)z^n}{1-z} + \frac{1-z^{n+1}}{(1-z)^2} \\ &= \frac{-(n+1)z^n(1-z) + (1-z^{n+1})}{(1-z)^2}. \end{aligned} \tag{S21}$$

Putting everything together, we get,

$$\begin{aligned} G(z) &= \frac{(n+1)(1-z^{n+1})}{1-z} + \frac{(n+1)z^{n+1}(1-z) - z(1-z^{n+1})}{(1-z)^2} \\ &= \frac{(n+1)(1-z^{n+1})(1-z) + (n+1)z^{n+1}(1-z) - z(1-z^{n+1})}{(1-z)^2} \\ &= \frac{(n+1)(1-z) - z(1-z^{n+1})}{(1-z)^2}. \end{aligned} \tag{S22}$$

Going back to d, we have,

$$G(z) = \frac{d(1-z) - z(1-z^d)}{(1-z)^2}. \tag{S23}$$

At this point, we remind ourselves that $z = \exp(2\pi i(\ell - \ell')/d)$. Thus, we can see that,

$$z^d = 1. \tag{S24}$$

Thus, our generating function greatly simplifies to,

$$G(z) = \frac{d}{1-z}. \tag{S25}$$

Going back to our equation,

$$
\begin{aligned}
&\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m}\\
=\;&\frac{1}{d^2}\Bigg[-d+\sum_{r=0}^{d-1}(d-r)\exp\left(\frac{2\pi i}{d}r(\ell'-\ell)\right)\\
&\qquad+\sum_{r=0}^{d-1}(d-r)\exp\left(\frac{-2\pi i}{d}r(\ell'-\ell)\right)\Bigg].\\
=\;&\frac{1}{d^2}\left[-d+\sum_{r=0}^{d-1}(d-r)z^r+\sum_{r=0}^{d-1}(d-r)(z^*)^r\right]\\
=\;&\frac{1}{d^2}\left[-d+\frac{d}{1-\exp\left(\frac{2\pi i}{d}r(\ell'-\ell)\right)}+\frac{d}{1-\exp\left(\frac{-2\pi i}{d}r(\ell'-\ell)\right)}\right]\\
=\;&\frac{1}{d}\left[-1+\frac{\left(1-\exp\left(\frac{-2\pi i}{d}r(\ell'-\ell)\right)\right)+\left(1-\exp\left(\frac{-2\pi i}{d}r(\ell'-\ell)\right)\right)}{\left(1-\exp\left(\frac{2\pi i}{d}r(\ell'-\ell)\right)\right)\left(1-\exp\left(\frac{-2\pi i}{d}r(\ell'-\ell)\right)\right)}\right]\\
=\;&\frac{1}{d}\left[-1+\frac{1-\cos\left(\frac{2\pi}{d}(\ell-\ell')\right)}{1-\cos\left(\frac{2\pi}{d}(\ell-\ell')\right)}\right]\\
=\;&\frac{1}{d}\left[-1+1\right]\\
=\;&0.
\end{aligned}
$$

We have thus proven that,

$$
\sum_{j<k}\sum_{m}\alpha^{(\ell')}_{j,k,m}\beta^{(\ell)}_{j,k,m}\;=\delta_{\ell,\ell'},
\tag{S26}
$$

for all ℓ and ℓ'.
Our final forward and backward relations linking the Fourier basis to the qubit-like basis is given by the following,

$$
\begin{aligned}
&p(\phi^{m'}_{j'k'}|\phi^{m}_{jk})\\
=\;&\frac{4}{d^2}\sum_{\ell n}\cos^2\left[\frac{\pi(m-(k-j)\ell)}{d}\right]\\
&\qquad\cos^2\left[\frac{\pi(m'-(k'-j')n)}{d}\right]p(\eta_n|\eta_\ell).
\end{aligned}
\tag{S27}
$$

$$
\begin{aligned}
p(\eta_n|\eta_\ell)=\;&\frac{4}{d^4}\sum_{j<k}\sum_{j'<k'}\sum_{m,m'}\left(\frac{2-d}{d-1}+\sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p\,(m-(k-j)\ell)\right)\right)\\
&\left(\frac{2-d}{d-1}+\sum_{p'=0}^{d-1}\exp\left(\frac{2\pi i}{d}p'\,(m'-(k'-j')n)\right)\right)p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}).
\end{aligned}
\tag{S28}
$$

Supplementary Note 3: Full Proof of Security

In the case of an ideal single photon source, we consider the action of an eavesdropper, Eve, as a general collective attack in the Fourier basis given by the unitary transformation U_{Eve}, i.e.,

$$U_{\text{Eve}}|\eta_i\rangle|e_{00}\rangle = \sum_{j=0}^{d-1} c_{ij}|\eta_j\rangle|e_{ij}\rangle, \tag{S29}$$

where $|e_{ij}\rangle$ is Eve's ancilla state. Without loss of generality, we assume that $c_{ij} \geq 0$ and $\langle e_{ij}|e_{mn}\rangle = \delta_{im}\delta_{jn}$. To estimate Eve's leaked information for the case where Alice encodes and Bob measures states, $|\psi_i\rangle$ in the computational basis, we can consider the error rate in the hypothetical case where Alice encodes and Bob measures states, $|\eta_i\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}\omega_d^{in}|n\rangle$, from a mutually unbiased basis (MUB), which we call here the Fourier basis. This hypothetical dit error rate, E'_d, depends on the probability that Bob obtains a measurement of $|\eta_{i'}\rangle$ conditioned on the fact that Alice prepares her state as $|\eta_i\rangle$, i.e.,

$$\begin{aligned} & p(i'|i) \\ &= \text{Tr}\left[|\eta_{i'}\rangle\langle\eta_{i'}|U_{\text{Eve}}|\eta_i\rangle\langle\eta_i| \otimes |e_{00}\rangle\langle e_{00}|U_{\text{Eve}}^\dagger\right] \\ &= \sum_{j,j'} \text{Tr}\left[|\eta_{i'}\rangle\langle\eta_{i'}|c_{ij}|\eta_j\rangle|e_{ij}\rangle\langle\eta_{j'}|\langle e_{ij'}|c_{ij'}\right] \\ &= \text{Tr}\left[c_{ii'}^2|e_{ii'}\rangle\langle e_{ii'}|\right] \\ &= c_{ii'}^2 \end{aligned} \tag{S30}$$

We are now interested in relating the probability outcomes $p(i'|i)$ in the Fourier basis to the measured probability outcomes of the qubit-like states. To do so, we use the fact that the qubit-like states can be rewritten in terms of the Fourier basis states,

$$|\phi_{jk}^{(m)}\rangle = \frac{1}{\sqrt{2d}}\sum_{\ell}\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)|\eta_\ell\rangle. \tag{S31}$$

The probability that Bob obtains $|\phi_{j'k'}^{(m')}\rangle$ conditioned on the fact that Alice prepares her state as $|\phi_{ij}^{(m)}\rangle$ is given by,

$$\begin{aligned} & p(\phi_{j'k'}^{m'}|\phi_{jk}^{m}) \\ &= \text{Tr}\left[|\phi_{j'k'}^{(m')}\rangle\langle\phi_{j'k'}^{(m')}|U_{\text{Eve}}|\phi_{jk}^{(m)}\rangle\langle\phi_{jk}^{(m)}| \otimes |e_{00}\rangle\langle e_{00}|U_{\text{Eve}}^\dagger\right] \\ &= \frac{1}{2d}\sum_{\ell\ell'}\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)\left(\omega_d^{j\ell'} + \omega_d^{(k\ell'-m)}\right) \\ &\quad \text{Tr}\left[|\phi_{j'k'}^{(m')}\rangle\langle\phi_{j'k'}^{(m')}|U_{\text{Eve}}|\eta_\ell\rangle\langle\eta_{\ell'}| \otimes |e_{00}\rangle\langle e_{00}|U_{\text{Eve}}^\dagger\right] \\ &= \frac{1}{2d}\sum_{\ell\ell'}\sum_{nn'}\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)\left(\omega_d^{j\ell'} + \omega_d^{(k\ell'-m)}\right) \\ &\quad \text{Tr}\left[|\phi_{j'k'}^{(m')}\rangle\langle\phi_{j'k'}^{(m')}|c_{\ell n}|\eta_n\rangle|e_{\ell n}\rangle\langle\eta_{n'}\langle e_{\ell' n'}|c_{\ell' n'}\right] \\ &= \left(\frac{1}{2d}\right)^2\sum_{\ell\ell'}\sum_{nn'}\sum_{ss'}\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)\left(\omega_d^{j\ell'} + \omega_d^{(k\ell'-m)}\right) \\ &\quad \left(\omega_d^{-j's} + \omega_d^{(m'-k's)}\right)\left(\omega_d^{j's'} + \omega_d^{(k's'-m')}\right) \\ &\quad \text{Tr}\left[|\eta_{s'}\rangle\langle\eta_s|c_{\ell n}|\eta_n\rangle|e_{\ell n}\rangle\langle\eta_{n'}\langle e_{\ell' n'}|c_{\ell' n'}\right] \\ &= \left(\frac{1}{2d}\right)^2\sum_{\ell\ell'}\sum_{nn'}\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)\left(\omega_d^{j\ell'} + \omega_d^{(k\ell'-m)}\right) \\ &\quad \left(\omega_d^{-j'n} + \omega_d^{(m'-k'n)}\right)\left(\omega_d^{j'n'} + \omega_d^{(k'n'-m')}\right) \\ &\quad \text{Tr}\left[c_{\ell n}c_{\ell' n'}|e_{\ell n}\rangle\langle e_{\ell' n'}|\right] \\ &= \left(\frac{1}{2d}\right)^2\sum_{\ell n}\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)\left(\omega_d^{j\ell} + \omega_d^{(k\ell-m)}\right) \\ &\quad \left(\omega_d^{-j'n} + \omega_d^{(m'-k'n)}\right)\left(\omega_d^{j'n} + \omega_d^{(k'n-m')}\right)c_{\ell n}^2 \end{aligned} \tag{S32}$$

Simplyfing,

$$
\begin{aligned}
& p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}) \qquad \text{(S33)}\\
&= \left(\frac{1}{2d}\right)^2 \sum_{\ell n} \left(1+\omega_d^{(m-k\ell+j\ell)}\right)\left(1+\omega_d^{-(m-k\ell+j\ell)}\right)\\
&\quad \left(1+\omega_d^{(m'-k'n+j'n)}\right)\left(1+\omega_d^{-(m'-k'n+j'n)}\right) c^2_{\ell n}\\
&= \left(\frac{1}{d}\right)^2 \sum_{\ell n} \left(1+\cos\left(\frac{2\pi(m-k\ell+j\ell)}{d}\right)\right)\\
&\quad \left(1+\cos\left(\frac{2\pi(m'-k'n+j'n)}{d}\right)\right) c^2_{\ell n}
\end{aligned}
$$

We have then arrived to a relation between the outcome probabilities in the Fourier basis, $p(n|\ell)$), necessary to determine the dit error rate E'_d, and the qubit-like probability outcomes, $p(\phi^{m'}_{j'k'}|\phi^{m}_{jk})$, measured experimentally, i.e.,

$$
\begin{aligned}
& p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}) \qquad \text{(S34)}\\
&= \frac{4}{d^2} \sum_{\ell n} \cos^2\left[\frac{\pi(m-(k-j)\ell)}{d}\right]\\
&\qquad \cos^2\left[\frac{\pi(m'-(k'-j')n)}{d}\right] p(n|\ell)
\end{aligned}
$$

This can be inverted by finding the coefficients $\alpha^{(\ell,n)}_{jj'kk'mm'}$ such that,

$$
p(n|\ell) = \sum_{j<k} \sum_{j'<k'} \sum_{m,m'} \alpha^{(\ell,n)}_{jj'kk'mm'} p(\phi^{m'}_{j'k'}|\phi^{m}_{jk}) \qquad \text{(S35)}
$$

The exact values of $\alpha^{(\ell,n)}_{jj'kk'mm'}$ are given in Equation S28. We note that these are the computational and Fourier bases form the two bases required for the high-dimensional BB84 protocol. Thus, Eve's leaked information on Alice encoding and Bob measuring in the computational basis is given by $I_{\mathrm{AE}} \leq h^{(d)}(E'_d)$, where we have used the fact that the phase error in the computational basis is equal to the dit error rate in the Fourier basis. Explicitly, the dit error rate in the Fourier basis is given by,

$$
\begin{aligned}
E'_d &= \frac{1}{d} \sum_{\ell \neq n} p(n|\ell) \qquad \text{(S36)}\\
&= \frac{1}{d}\left(\sum_{\ell n} p(n|\ell) - \sum_{\ell} p(\ell|\ell)\right)
\end{aligned}
$$

Finally, the secret key rate per sifted key for Alice and Bob is given by,

$$
R = \log_2(d) - h^{(d)}(E_d) - I_{\mathrm{AE}} \geq \log_2(d) - h^{(d)}(E_d) - h^{(d)}(E'_d). \qquad \text{(S37)}
$$

Supplementary References

[1] L. Scarfe, F. Hufnagel, M. F. Ferrer-Garcia, A. D'Errico, K. Heshami, and E. Karimi, "Fast adaptive optics for high-dimensional quantum communications in turbulent channels," *Communications Physics*, vol. 8, p. 79, Feb 2025.

[2] R. Abolhassani, L. Scarfe, F. Di Colandrea, A. D'Errico, K. Heshami, and E. Karimi, "Investigating the performance of adaptive optics on different bases of spatial modes in turbulent channels," *arXiv preprint arXiv:2508.21015*, 2025.

5

Chapter 5: Conclusion and Overview

In this thesis, we have introduced two works which contribute to implementing QKD in turbulent channels. The required basics of the field, from the degrees of freedom of light to details on turbulence and free space links, were covered in order to understand the two

works presented. For each separate work, the necessary theoretical background was also given, which familiarizes one with some of the important concepts in quantum-information theory.

From the use of adaptive optics in a lab-simulated turbulent setup, it was realized that there exists a bias for the AO towards modes with different spatial distributions. To this end, mutually unbiased bases in dimensions 2,3,4,5,8 and angular modes in dimensions 4 and 8 were analyzed, alongside SIC-POVM modes in dimensions 2,3,4 and 6. Once QKD is implemented in the real world with atmospheric turbulence, one can decide which set of bases best matches the current situations. It was especially seen that the more cylindrical the modes are, such as the logical OAM bases, the better the adaptive optics corrects for them, given the AO's own cylindrical geometry. Besides that, modes that are less spatially spread out are less affected by turbulence; in our case, the first MUB basis. Note that although spatial light modulators are often viewed as Cartesian devices for mode generation, the phase-only modulation technique used for simultaneous amplitude and phase control effectively filters the field and produces cylindrical modes. Thus, any observed mode bias arises primarily from the performance and structural characteristics of the AO system.

Following the results of the first project and having in mind the motivation of creating modes with cylindrical symmetry, a new qubit-like protocol was proposed. A protocol that acts well with the AO system, has uniform intensity and in qubit like in creating and measuring. But the initial idea for this new protocol faced basic issues that prevented

it from being used securely in QKD. To this end, the protocol was further investigated, and with the introduction of a phase factor between the modes, it was feasible to achieve QKD. Thus, the final protocol was created, namely the Fourier Qubits (F-Qubits). The performance of these modes was also investigated, and the security was proven to be below the threshold limit of the BB-84.

Our future goals include implementing these results in a real-world QKD setup. We are currently attempting to use a 5.4km free space link over the city of Ottawa, and to apply our knowledge of modes, turbulence and adaptive optics to the actual atmospheric turbulence.
The different modes of light, the MUB and SIC-POVM modes, can be implemented through fiber-based QKD as well. One can ask: how differently will they act through that medium? Will any noise in the fiber affect the error rate noticeably? If so, could it be compensated for? Other matters that can be addressed in terms of real-world implementations could be the plasma effects in the atmosphere, which can affect the performance of our system.

The F-qubit protocol can be used to open the door for other high-dimensional, qubit-like approaches. Although we are not yet using all the information that F-qubits actually convey, there is still much more to uncover in this regard. The security of the F-qubit protocol can also be pushed further, even though developing full security proofs in high-dimensional systems is a considerably difficult task. We can also think of applying the F-qubits to different methods of QKD and to use the simplicity of their qubit-like states

to create time bins or temporal and spectral modes. It is also worthwhile to consider their behavior in other media, such as optical fibers in fiber communications.

Bibliography

1. Saleh, B. E. A. & Teich, M. C. Fundamentals of photonics (Wiley, New York, NY, 2007).

2. Lazarev, G., Chen, P., Strauss, J., Fontaine, N. & Forbes, A. Beyond the display: Phase-only liquid crystal on silicon devices and their applications in photonics. Optics Express **27,** 16206–16220.

3. Rubinsztein-Dunlop, H. et al. Roadmap on structured light. Journal of Optics **19,** 013001 (2016).

4. Optical Angular Momentum (eds Allen, L., Barnett, S. M. & Padgett, M. J.) Printed by CRC Press in 2020 (CRC Press, Boca Raton, FL, 2003).

5. Buhler, J. P., Lenstra, H. W. & Pomerance, C. in The Development of the Number Field Sieve (eds Lenstra, A. K. & Lenstra, H. W.) 50–94 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1993).

6. 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).

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

8. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. Nature **299,** 802–803 (1982).

9. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science **560,** 7–11 (2014).

10. Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. IEEE Transactions on Information Theory **41,** 1915–1923 (1995).

11. Bouchard, F. et al. Quantum process tomography of a high-dimensional quantum communication channel. Quantum **3,** 138 (2019).

12. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of Quantum Key Distribution Using d-Level Systems. Physical Review Letters **88.**

13. Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. Physical Review A **61.** Received 1 November 1999; published 16 May 2000, 062308 (2000).

14. Chau, H. F. Quantum key distribution using qudits that each encode one bit of raw key. Physical Review A **92,** 062324 (2015).

15. Scott, A. J. & Grassl, M. Symmetric informationally complete positive-operator-valued measures: A new computer study. Journal of Mathematical Physics **51,** 042203 (2010).

16. Xavier, G. B. & Lima, G. Quantum information processing with space-division multiplexing optical fibres. Communications Physics **3,** 1–11 (2020).

17. Sit, A. et al. Quantum cryptography with structured photons through a vortex fiber. Optics Letters **43,** 4108–4111 (2018).

18. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. Science **356,** 1140–1144 (2017).

19. Vallone, G. et al. Free-space quantum key distribution by rotation-invariant twisted photons. Physical Review Letters **113,** 060503 (2014).

20. Sit, A. et al. High-dimensional intracity quantum cryptography with structured photons. Optica **4,** 1006–1010 (2017).

21. Vallone, G., Marangon, D. G., Tomasin, M. & Martini, F. D. Experimental satellite quantum communications. Physical Review Letters **115,** 040502 (2015).

22. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. Nature **549,** 43–47 (2017).

23. Krenn, M. et al. Twisted light transmission over 143 km. PNAS **113,** 13648–13653 (2016).

24. Kolmogorov, A. N. The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers. Doklady Akademii Nauk SSSR **30,** 301 (1941).

25. Tyson, R. K. & Frazier, B. W. Principles of Adaptive Optics 5th. Comprehensive coverage of adaptive optics, including atmospheric turbulence models and compensation techniques. ISBN: 9780367690489 (CRC Press, Boca Raton, FL, 2022).

26. Fried, D. L. Optical resolution through a randomly inhomogeneous medium for very long and very short exposures. Journal of the Optical Society of America **56,** 1372–1379 (Oct. 1966).

27. Von Zernike, F. Beugungstheorie des Schneidenverfahrens und seiner verbesserten Form, der Phasenkontrastmethode. Physica **1,** 689–704 (1934).

28. ALPAO. Wavefront Sensors – Optimized for Adaptive Optics `https://www.alpao.com/products-and-services/wavefront-sensors/`. Accessed: 29 Aug 2025. 2025.

29. Scarfe, L. et al. Fast adaptive optics for high-dimensional quantum communications in turbulent channels. Communications Physics **8,** 79 (2025).

30. Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases. International Journal of Quantum Information **8,** 535–640 (2010).

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

32. Schwinger, J. Unitary Operator Bases. PNAS **46,** 570–579 (Apr. 1960).

33. Mafu, M. et al. Higher-dimensional orbital angular momentum based quantum key distribution with mutually unbiased bases. Phys. Rev. A **88,** 032305 (2013).

34. Renes, J. M., Blume-Kohout, R., Scott, A. J. & Caves, C. M. Symmetric informationally complete quantum measurements. Journal of Mathematical Physics **45,** 2171–2180 (2004).

35. XOR'easter. Regular tetrahedron and its circumscribing sphere Wikimedia Commons, `https://commons.wikimedia.org/wiki/File:Regular_tetrahedron_inscribed_in_a_sphere.svg`. Licensed under CC BY-SA 4.0. 2019.

36. Englert, B.-G. et al. Efficient and robust quantum key distribution with minimal state tomography. arXiv preprint quant-ph/0412075 (2004).

37. Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. Physical Review A **82,** 030301 (2010).