# PHY4006 Final Report:<br>Optimal Spatial Modes of High-Dimensional Quantum Key Distribution through a Distorted Medium

Justin Tam*
*Department of Physics at the University of Ottawa*

(Dated: April 11, 2023)

Quantum Key Distribution is a process by which two parties can securely exchange cryptographic keys by sending a string of individual structured photons. Each photon carries with it the fundamental properties of quantum mechanical particles, in that the photon state itself is changed upon measurement. By implementing a protocol such as the BB84 developed by Bennett and Brassard [1] one can take advantage of this property, and exchange a cryptographic key with certain knowledge if it has been intercepted along transmission. Here we explore and optimize a possible basis known as 'Pixel modes' to use for the structured photons in the Quantum Key Distribution process. Via computer simulation, we find that for a given aperture, increasing the dimensions to be as high as possible through shrinking the beam waist, while maintaining a small separation between individual Gaussian beams, produces the highest secret key rate.

**Subject Areas:** Quantum Key Distribution, Structured Photons, Pixel Modes, BB84

## I. INTRODUCTION

In Modern Cryptography when sending randomly generated cryptography keys, there is a strong need to not just prevent third party access to the key, but to guarantee the knowledge of the event should it happen. If such a reliable method to do this existed, it would allow the exchange of single use cryptographic keys, a method known as the one-time pad. It is a cryptograhpic method that is theoretically unbreakable, as long as the key is used only once [2]. A promising solution to implement such a method is known as Quantum Key Distribution (QKD), that achieves such a feat by transmitting individual structured photons. Here we aim to optimize a high-dimensional QKD protocol using a particular basis known as 'Pixel modes'. This will be accomplished via simulation by varying over the dimensions of the proposed basis indirectly through the beam waist and beam spacing parameters, in order to optimize for the secret key rate (SKR) of the QKD protocol involving that particular basis. The photons will be propagated through a weakly-distorted medium approximated using a small combination of Zernike polynomials, across a fixed 1km distance and aperture size of 20 mm diameter.

## II. QUANTUM KEY DISTRIBUTION

### A. Classical Information Technology

Suppose Alice wants to send Bob a message such as 'Hello' over a large distance. One could achieve such a feat using, for example, electrical wires and the method of Morse Code. The wires carry electrical properties set by Alice, and can then be measured by Bob. By following a table that both Alice and Bob have, Alice can translate each letter of the string of characters 'Hello' to a sequence of dashes and dots. For example, the character 'H' is translated as 4 consecutive dots, and the letter 'E' as one dot [3] (see Appendix B for a full table). Alice can then send this sequence as an electrical signal switching between high and low values over time, in the exact fashion of dashes and dots representing her message. Bob receives the signal, and using the Morse Code table he and Alice have access to, translates the dashes and dots into the 'Hello'.

A more practical example for Alice to send the same message to Bob, is to replace dashes and dots with 1s and 0s, and a table of Morse Code with the American Standard Code for Information Interchange table (ASCII) [3] used to translate groups of '1's and '0's into characters. The '1's and '0's are called binary bits, and are again represented by high and low signals, only now each high/low lasts for a specified amount of time, known as the bit rate (b/s). To send the character 'H', Alice can send a sequence of 8 bits as '0100 1000' [4] (see Appendix C for a full table), and Bob will receive the signal and translate back into the character 'H', and so on until the the message 'Hello' is constructed. An example of a binary sequence in terms of the electric voltage is shown in Fig. (1).

### B. Quantum Information Technology

We now form the classical bit into its quantum mechanical counter part, often referred to as a qubit [6] - a quantum state that can be fully described as a linear combination of two orthonormal basis elements. Suppose we describe our qubit in the basis of $|0\rangle$, and $|1\rangle$. Where as a bit can take on the value of either a '0', or '1', a qubit can take on the value of either a '0', '1', or superposition

* jtam050@uottawa.ca

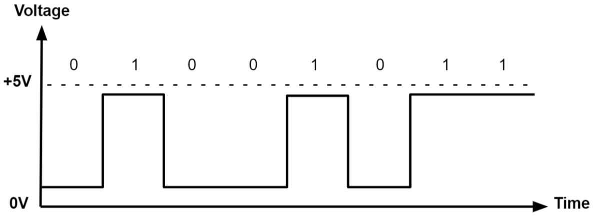


FIG. 1. An example of an 8-bit binary signal. Here, the signal is 01001011 representing the character 'K' using the standard ASCII translation. Obtained from Monolithic Power Systems [5].

of the two. It is not that the qubit is secretly either in the $|0\rangle$, or $|1\rangle$ state and we simply don't know, but rather its outcome does not yet exist in reality [7]. The quantum state only realizes itself upon measurement, with corresponding probabilities of being in either the $|0\rangle$, or $|1\rangle$ state. Where $\alpha^2$ and $\beta^2$ represent the probabilities finding the qubit in the state $|0\rangle$, and $|1\rangle$ respectively. Note that by definition of a probabilistic interpretation, $\alpha^2 + \beta^2 = 1$, where

$$|\psi_{qubit}\rangle = \alpha |0\rangle + \beta |1\rangle . \tag{1}$$

It is in this superposition state, where the qubit has a probability of being in the $|0\rangle$, or $|1\rangle$ state, that the advantage to QKD lies. Suppose an observer, Eve, were to take a measurement of the qubit, finding it to be in either the $|0\rangle$, or $|1\rangle$ state. Whichever state Eve measures, the qubit will now completely collapse to this state, and fundamentally change. If Eve were to measure the qubit a second time, she would be **guaranteed** to measure the same outcome as she did before, opposed to the probabilistic nature of her first measurement [7].

Suppose now that Alice were to send Bob a message using a series of qubits and not bits, and a 3rd party Eve were to try and intercept the message and measure its contents, and send the message along to Bob so that Alice nor Bob would know their message was intercepted. If Alice used only qubits in a superposition state, Eve's measurements of the state would have an unavoidable affect on the qubits containing the message. If Alice and Bob were to decide on a predefined protocol for sending and receiving the qubits containing their message, there lies the potential to identify any and all interceptions of their communication, should it happen. Such a protocol was proposed by Bennet and Brassard in 1984 as the BB84 protocol [1], with its many variants are widely accepted today. The protocol cleverly allows detection of a 3rd party Eve by having Alice and Bob use a set of two mutually unbiased bases (MUB), and defining a method for communication accordingly.

### C. Mutually Unbiased Basis (MUB)

A Mutually Unbiased Basis (MUB) of another basis, is a MUB if and only if measuring a single state generated from the original basis, using the MUB, results in a equal probability of measuring any state in the MUB. In other words, projecting a state $|\psi\rangle$ measured in basis $X$ onto a state of the MUB, $Y \stackrel{\text{def}}{=} \{\phi_i | 0 \leq i \leq d-1\}$, will yield a probability of measurement equal to 1 over the dimensions of the original basis, $d$.

$$\langle \psi | \phi_i \rangle = \frac{1}{\sqrt{d}}. \tag{2}$$

For example, suppose we take the vertical horizontal polarization basis of $\{|H\rangle, |V\rangle\}$ and create a single photon (and thus a quantum particle) to be the single state $|V\rangle$. In other words, we would have a 100% probability of measuring such a photon to be in the vertical state, $|V\rangle$. We can write this analytically as

$$|\psi\rangle = |V\rangle . \tag{3}$$

Now, if we were to then measure an identical photon using the diagonal anti diagonal basis, $\{|D\rangle, |A\rangle\}$, we would have a 50% probability of measuring the photon as the $|D\rangle$ state and a 50% probability of measuring the photon as the state $|A\rangle$. In this example, the diagonal anti diagonal basis, $\{|D\rangle, |A\rangle\}$, is by definition a MUB of the vertical horizontal basis of $\{|H\rangle, |V\rangle\}$. In bra-ket notation where the inner product of two states is equivalent to the overlap of the two states (1 if the same state and orthonormal, 0 if orthogonal),

$$\langle H | V \rangle = \frac{1}{2} = 50\%. \tag{4}$$

To find a MUB of an any arbitrary basis using the method of unitary operators, we can write analytically

$$|k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{(i2\pi/d)jk} |j\rangle , \; for \; k \in \{0, ..., d-1\}, \tag{5}$$

where each state $|k\rangle$ represents a member or mode of the original basis of dimension $d$.

### D. BB84 Protocol

We are now ready to understand the core method of QKD, and how the destructive nature of quantum mechanical measurements is taken advantage of to detect the presence of a third party. Suppose that Alice wants to send Bob a message using qubits, in the form of polarization of structured light. In the BB84 for protocol, Alice and Bob need to agree upon two MUB that are mutually non-orthogonal (i.e. one basis + its MUB). We have already discussed an example of such a set in the basis sets of $X \overset{\text{def}}{=} \{\left|H\right\rangle, \left|V\right\rangle\}$, and $Y \overset{\text{def}}{=} \{\left|A\right\rangle, \left|D\right\rangle\}$. Both sets are mutually non-orthogonal, and form a complete description of the polarization state of each qubit. To send a binary message, both parties can agree to represent the bit '0' as a measurement of the $\left|H\right\rangle$ and $\left|D\right\rangle$, while the bit '1' is represented by a measurement of the states $\left|V\right\rangle$ and $\left|A\right\rangle$.

To send a message under the BB84 protocol, Alice must proceed to randomly choose which basis to encode each bit. For example, the letter 'H' represented by the binary sequence '0100 1000' can be encoded in the basis of 'HAHD VHDH', where Alice used the X and Y bases in the order of 'XYXY XXYX'. Once Bob receives the message, he then also chooses which basis to decode each bit. If he happens to choose the same basis as Alice, then he will measure the correct state. If he doesn't, then the outcome will be random. In the same example, suppose Bob chooses to decode each bit in the following sequence of bases: 'XYXX XYYY'. Where 'C' means correct, and 'R' means random, by comparison of both parties' choice of bases, Bob will obtain the sequence 'CCCR CRCR', or in terms of the measured outcome, '010R 1R0R'. Note that at this point, all of the qubits have been collapsed to their measured state.

The next step is for Bob to share to Alice what sequence of bases he chose on a public channel. Alice then responds to Bob by telling him what bases he choose correctly, and they both proceed to discard the bits for which Bob chose the incorrect basis. The result is an identical 'shifted' message that both Alice and Bob share.

### E. Measurement of Success

The goal of the QKD protocol is for Alice and Bob to end up with the exact same random string of information – a cryptographic key. This means that errors are not fatal until a determined threshold (we discard more than half of the information during the BB84 protocol), but are not preferred. A lower error rate reduces the amount of photons needed to generate a key of the same size, and guarantees that that the error rate is not so low that no useful information can be sent at all. Errors in the QKD process can occur with misalignment, optical interference, and beam divergence. We can define the probability of error per photon as the qubit error rate (QBER). An error in the QKD process arises when, for example, a photon in state $\left|V\right\rangle$ is measured in state $\left|H\right\rangle$. The QBER can then be generalized as the probability of measuring a single state incorrectly as another state. If Alice sends a photon in an arbitrary state $\psi_A$, and the photon Bob receives is defined as $\psi_B$, the probability that the photon in $\left|\psi_B\right\rangle$ is measured as the state $\left|\psi_A\right\rangle$ is given by the inner product of the two states in Hilbert space. Where both states are continuous functions in polar coordinates,

$$\langle\psi_A|\psi_B\rangle = \int\int \psi_A^*(r,\phi)\psi_B(r,\phi)drd\phi. \tag{6}$$

We can then calculate the error rate of a particular state sent Alice by taking the negation of Eq. (6) across all possible measurement states for Bob. To generalize across the entire QKD protocol, we can average this error rate across each state or mode sent by Alice. The result is the QBER. Where $QBER_A$ is the error rate of a particular mode sent by Alice for basis of dimension $d$,

$$QBER_A = \textstyle\sum_{i\neq A}^{d} 1 - \langle\psi_A|\psi_i\rangle\,, \tag{7}$$

$$QBER = \textstyle\sum_{k=1}^{d} QBER_k. \tag{8}$$

While the QBER tells us the probability of a single photon, we now seek a value that quantifies the amount of information sent per photon. Depending on the dimension of the basis chosen, each photon can hold a different amount of information. For example, if the basis is $d = 2$ then the resulting photon is binary, and can be either a 0 or 1. If the the basis is $d = 8$, then each photon can be a number between 0-7. The information of a $d = 7$ photon is equivalent to 3 binary units, as a string of 3 0/1s has 8 unique permutations, and thus can represent 8 numbers. Where $(x)_{10}$ and $(x)_2$ represent the value $x$ in base decimal and binary respectively,

$$(7)_{10} = (111)_2. \tag{9}$$

By choosing a basis of higher dimension we can then increase the amount of information sent per photon. This is based on the fact that each photon has the potential to represent a wider range of values. By taking into account the dimensions of the basis chosen, we can define the secret key rate (SKR), to be the amount of useful information left for a cryptographic key. After taking into account the BB84 protocol (sifting + security algorithms), QBER, and dimensions of the basis chosen, the SKR is analytically given in **units bits/sifted photon** as

$$SKR^{(d)}(QBER) = log_2(d) - 2h^{(d)}(QBER), \tag{10}$$

where,

$$h^{(d)}(x) = -log_2\frac{x}{d-1} - (1-x)log_2(1-x), \tag{11}$$

is the the Shannon entropy for $d$ dimensions [8].

## III. SPATIAL MODES OF LIGHT

Just as informational bits of data can be encoded into electric signals, our goal here is to encode some form of information into structured light. If bits represent two degrees of freedom – formed on the basis of a high voltage, 1, and a low voltage, 0 – we seek to explore the possible degrees of freedom that can be used in structured light. We have multiple options in the form of frequency, $w$, polarization, $\pi$, and spatial distributions of the light intensity in both the radial, and angular dimensions, $p$ and $l$, respectively. We define any unique combination of $p$ and $l$ to correspond to a unique spatial mode. The indices $p$ and $l$ can both be described in integer quantities along with the polarization, where as the frequency is taken to be continuous. An exhaustive iteration over these 4 degrees of freedom can form any possible instance of structured light. Any quantum state of structured light can then be described as a linear combination of this set. In bra-ket notation, we can describe an arbitrary linear combination as such.

$$|\psi\rangle = \int dw \sum_{\pi,l,p} c_{\pi,l,p}(w) \, |w,\pi,l,p\rangle \,, \tag{12}$$

where the angular frequency is continuous and thus integrated, and the integers $\pi$, $l$, and $p$ are summated. Note that in Eq. (12) the linear constants $[c_{\pi,l,p}(w)]^2$ arbitrarily represent the probability of finding the structured light in that specific state of frequency, polarization, and spatial mode. We continue to find more specific representations of spatial modes in the following subsections.

### A. Plane Wave Representation

Suppose we want a purely classical representation of a pulse of light. From Maxwell's equations, we know a light pulse can be thought of as a collection of electromagnetic waves (EM waves). Here we also define these EM waves to be both parallel in their direction of propagation, and distributed transversely across a small radius. To describe such an entity we seek a function that returns a vector whose magnitude and direction is the electric field vector. Since the electric field of light oscillates in a direction orthogonal to the direction of the electric field it contains, we can split the function into the product of a radial and phase component - a standard plane wave representation. In the cylindrical coordinate system of $\rho$, $\phi$, $z$, we align the $z$ direction to the direction of propagation, and its origin at the center of our collection of light waves. Where $k$ is the wave number, $w$ is the angular frequency, and the function $\overrightarrow{F}(\rho,\phi,z)$ represents the intensity distribution for a given plane,

$$\overrightarrow{E}(\rho,\phi,z,t) = \overrightarrow{F}(\rho,\phi,z)e^{i(kz-wt)}. \tag{13}$$

### B. Polarization Modes

If we continue with our example of plane wave representation of a pulse of light, all EM waves are parallel and propagate along the z axis. We can then describe the direction of oscillation (polarization) of the electric field component in only two dimensions along any plane in the z axis. For example, if we momentarily switch to a Cartesian system we can describe the electric field vector on some plane $z$ where $\hat{e}_x$ and $\hat{e}_y$ are the standard x and y basis. We can also go further and expand out the plane wave phase component, bringing in a $z$ and $t$ dependence.

$$\overrightarrow{E}(x,y) = E_x\hat{e}_x + E_y\hat{e}_y, \tag{14}$$

$$\overrightarrow{E}(x,y,z,t) = [E_x\hat{e}_x + E_y\hat{e}_y]e^{i(kz-wt)}. \tag{15}$$

If we had an EM wave polarized in the horizontal direction, its presence would only be in the $E_x$ term, and if the wave was vertically polarized, it would only be in the $E_y$ term. We can then relabel by defining $\hat{e}_x$ as $\hat{e}_H$, and $\hat{e}_y$ as $\hat{e}_V$ for horizontal and vertical polarization, respectively.

$$\overrightarrow{E}(x,y,z,t) = E_x e^{i(kz-wt)}\hat{e}_H + E_y e^{i(kz-wt)}\hat{e}_V. \tag{16}$$

It is at this point that we switch from a purely classical view to that of a quantum mechanical one. Our equation for electric field is a linear combination of horizontal, and vertical terms. By treating the polarization of the EM wave to under quantum theory, we can write the EM wave state, $|\psi\rangle$ as a sum of two orthonormal states - the horizontal and vertical wave states - with coefficients $\alpha$ and $\beta$ replacing the $E_x$ and $E_y$ terms respectively.

$$|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle\,, \tag{17}$$

Note that the states $|H\rangle$ and $|V\rangle$ form a complete basis for EM wave, in that we can represent any polarization using these two degrees of freedom. The probability of finding the EM wave in state $|H\rangle$ is $\alpha^2$, and in state $|A\rangle$ is $\beta^2$, where $\alpha^2+\beta^2=1$. The choice of basis is arbitrary, and we can just as easily choose an alternative basis in the form of diagonally and anti-diagonally polarized light, $|D\rangle$ and $|A\rangle$, as well as left and right circularly polarized light, $|L\rangle$ and $|R\rangle$.

$$|D\rangle = \tfrac{|H\rangle+|V\rangle}{\sqrt{2}}, |A\rangle = \tfrac{|H\rangle-|V\rangle}{\sqrt{2}} \tag{18}$$

$$|L\rangle = \tfrac{|H\rangle+i|V\rangle}{\sqrt{2}}\; |R\rangle = \tfrac{|H\rangle-i|V\rangle}{\sqrt{2}}. \tag{19}$$

By writing the EM wave in this way, we have successfully represented a quantum-mechanic structured light in a basis of two polarization modes, and thus a dimension of 2. We have thus achieved a more specific representation of the general spatial mode described previously in equation (2).

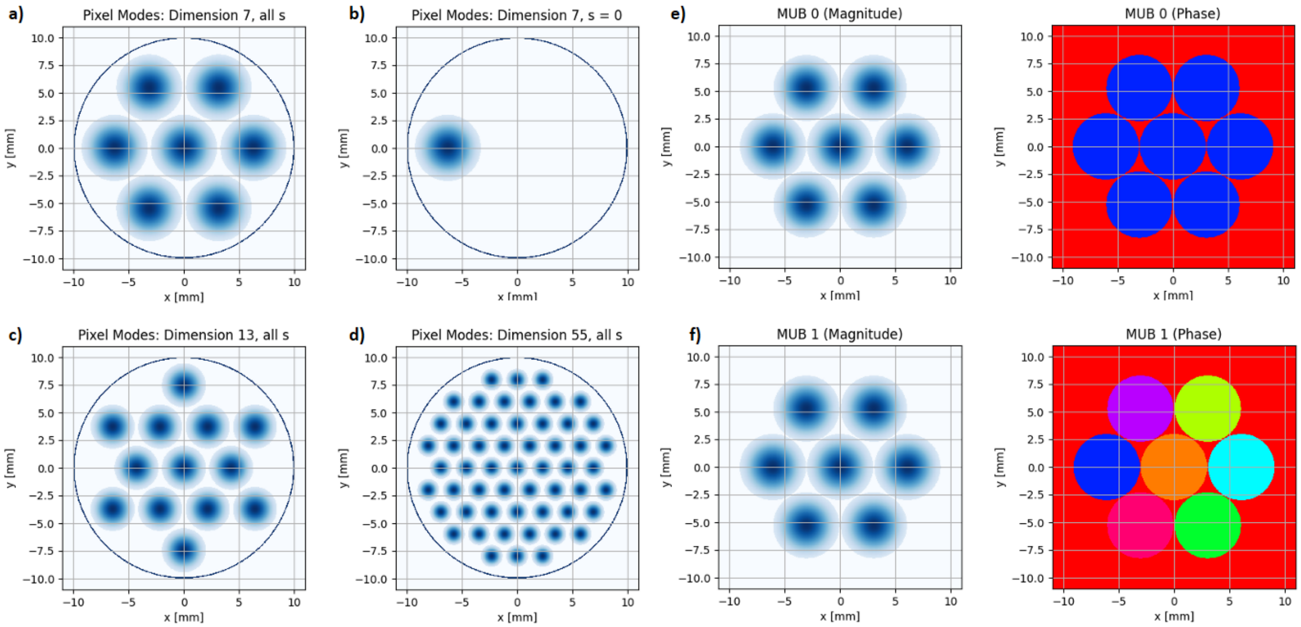


FIG. 2. **a)** The intensity plot of all Pixel modes in the same plot, for dimension 7. **b)** A single mode of the dimension 7 Pixel modes, $s = 0$. **c)/d)** The intensity plot for dimensions 13 and 55 of Pixel modes for all $s$. **e)/f)** The intensity and phase plots of the first and second modes of the MUB for Pixel modes of dimension 7.

### C. Pixel Modes

We describe here an alternative basis to encode quantum information, defined here as 'Pixel modes'. These modes were compared by Zhao et al. in their capacity limits versus the more common basis for QKD, Laguerre-Gaussian modes [9]. The basis for Pixel modes are defined by fitting a maximum number of Gaussian beams or 'pixels' with beam waist $w_0$, inside a larger aperture of diameter $D$. A single mode of the basis is then defined by leaving one of the Gaussian beams 'on', and turning the rest of the Gaussian beams 'off' (not generating any Gaussian beams where there would have been). Each mode of the basis is by definition indexed using the positive integer $s$. For example, if we take a Gaussian beam of beam waist $w_0 = 3mm$, and aperture diameter of $D = 20mm$, we can fit a total of 7 Gaussian beams inside, as shown in Fig. (**??**). Such a basis will then have a dimension, $d$, equal to the number of Gaussian beams inside the aperture. In this case $d = 7$.

We can computationally calculate the MUB for the Pixel modes, by creating first creating the pixel modes as a 2D array of complex values, and applying Eq. (5). The result is shown in Fig. (2). As we expect from the analytical calculation, the first mode of the MUB, MUB 0, is a scaled down summation of all modes of the Pixel mode basis with unitary phase. The second MUB shown, MUB 1, also contains a scaled down summation of all pixel modes, except its phase alternates between each Gaussian beam.

## IV. SIMULATION OF HIGH-DIMENSIONAL QKD

The simulation of the QKD is accomplished in Python3 with the help of SciPy and NumPy libraries. The codebase is a collaborative effort between myself, Justin Tam, and another honors student, Itay Kozlov. See Appendix C for more details, and a link to the codebase on Github. To simulate a QKD protocol for a particular basis, the pixel modes are first created at point A, and propagated through free space via a Fresnel approximation [10]. An externally applied distortion in the form of a specific combination of Zernike polynomials [11], and received at point B. The image received at point B is then used to calculate the QBER for the protocol, and then the SKR. The objective of the simulation will be to, using the Pixel modes, find the optimal basis at a set distance of 1 km, aperture of 20 mm, weak distortion, while varying both the beam waist and beam spacing.

### A. Pixel Mode Creation

The pixel modes and their MUB, as seen in Fig. (**??**) and (2), are calculated as a complex 2D NumPy array. In order to maximally fit as many Gaussian beams within a given radius, a hexagonal pattern is created by defining a 2D basis (see Fig 3). Similar to a 2D hexagonal lattice of atoms, each center point can now be calculated by taking an integer linear combination of these two basis vectors. If we define the radius of each Gaussian beam as $w_0/2$

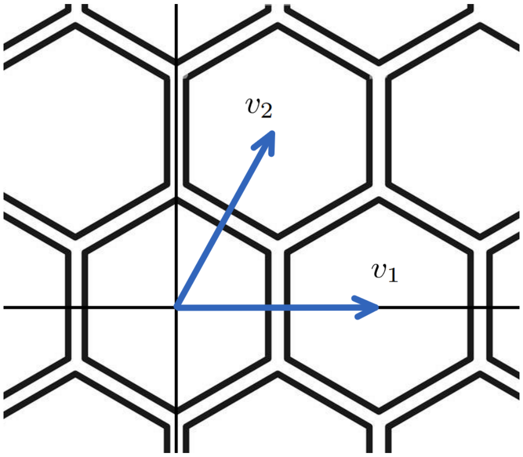


FIG. 3. Using a 2D basis to create a hexagonal pattern.

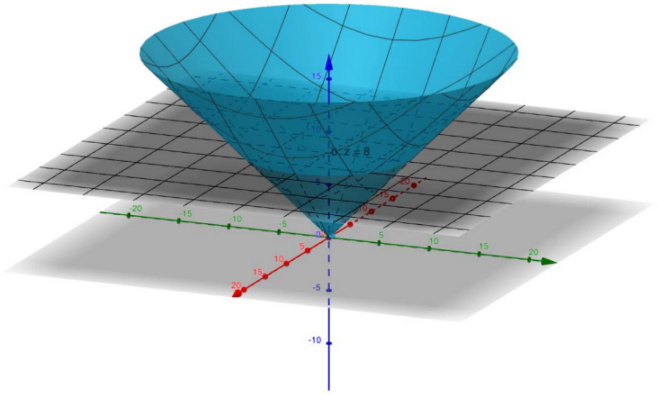


FIG. 4. Creating a thresholded Gaussian beam at a radius $w_0/2$ by defining an inverter cone at the beams origin, and setting all values above the appropriate height equal to 0.

where $w_0$ is the beam waist, and the spacing between adjacent Gaussian beams as $sp$, we can write the two basis vectors in polar coordinates as

$$v_1 = \begin{pmatrix} w0 + sp \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} w0 + sp \\ 2\pi/6 \end{pmatrix}, \tag{20}$$

where,

$$v_i = \begin{pmatrix} r \\ \phi \end{pmatrix}. \tag{21}$$

For a pixel mode basis of dimension $d$, $d$ Gaussian beams are created and shifted to the points defined by an integer combination of hexagonal lattice vectors. This is possible via simulation by first creating the Gaussian beams via standard polar coordinates, then switching to Cartesian coordinates, and shifting appropriately. Each Gaussian beam is cut off at a radius equal to half its beam waist, $w_0/2$. This is done computationally by creating an inverted cone shifted to the beams origin point with a slope of one, and setting all vertical points greater than the radius equal to zero. An example of the process is shown graphically in Fig. (4).

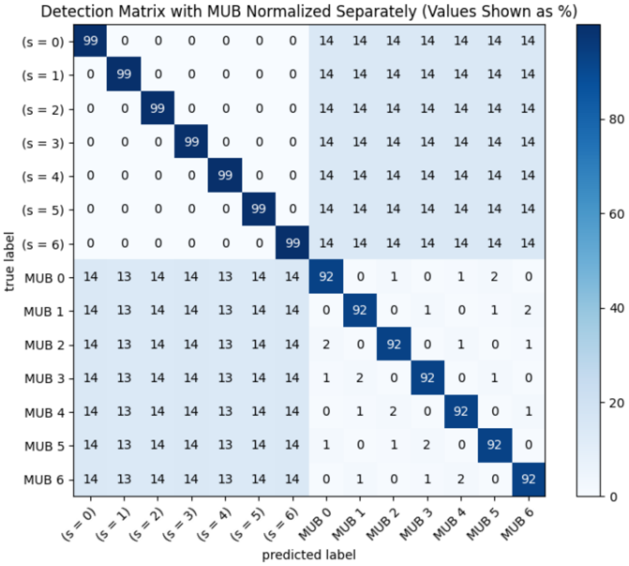


FIG. 5. Cross talk matrix for a beam spacing of 0.1 mm, beam waist of 3 mm, distance of 1 km, weak distortion, and Pixel mode basis of dimension 7. The resulting QBER is 3.56%, and SKR is 2.18 bits/photon.

### B. Determining QBER

To determine the QBER via simulation we apply a visual approach to the analytical derivation in Eq. (7) and (8). We can plot this process visually using what's commonly referred to as a 'cross talk matrix' where the probability of correct measurement (negation of error rate) is plotted for all combinations of sent and received photon modes, including their MUB. An example of such a cross talk matrix simulated using a propagation distance of 1 km, weak distortion, 20 mm aperture, 3 mm beam waist, 0.1 mm spacing, and dimension 7 is shown in Fig. (5). For example, the upper most left value of 99% represents the probability that the mode $s = 0$ was measured as $s = 0$. In the surrounding upper left quadrant the entire main diagonal has a 99% of the receiver making the correct measurement. The probability of measuring a MUB mode as the correct MUB mode, shown in the bottom right most quadrant, is 92%. This indicates to us that the error rate upon measurement is higher for the MUB of the Pixel modes than it is for the original basis of the Pixel modes. The bottom left and upper right quadrants indicate the probability of measuring an original basis mode as a MUB, and vice versa. The probability of each case is nearly always 14%, approximately equal to 1/7, as expected of a MUB of dimensions 7.

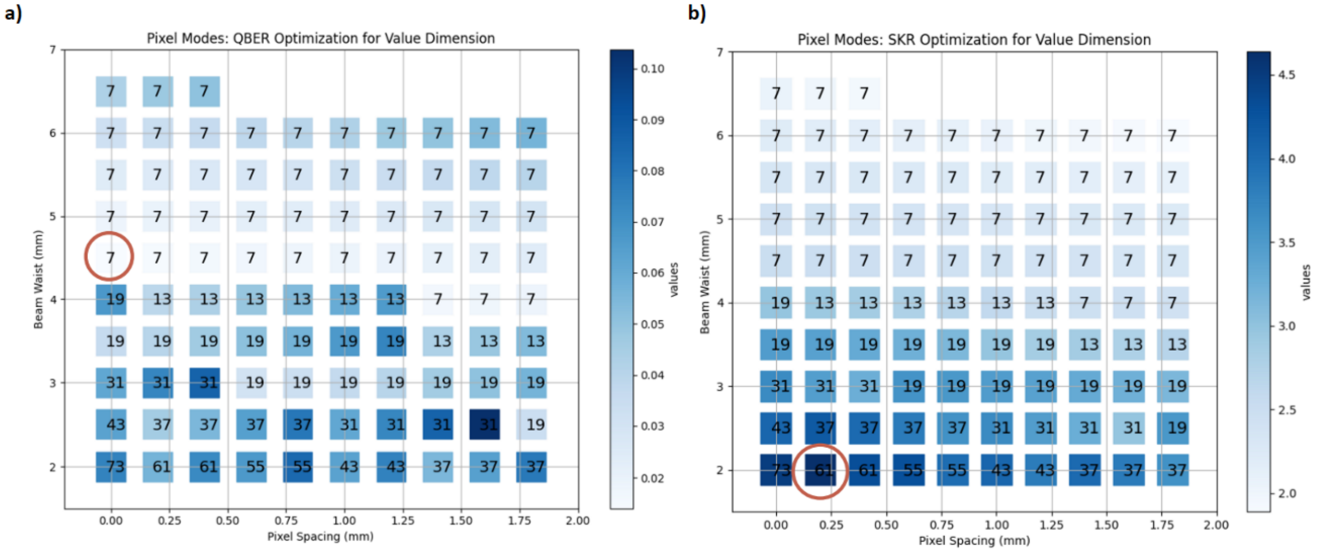


FIG. 6. **a)** Optimization of QBER over different Pixel modes with varying beam waist, and beam spacing. Each square represents a single Pixel mode basis, with an integer dimension inside the square. The lowest QBER of 1.14% is circled in red, with a dimension of 1, beam spacing of 0 mm, and beam waist of 4.5 mm. **b)** Optimization of SKR over different Pixel modes with varying beam waist, and beam spacing. Each square represents a single Pixel mode basis, with an integer dimension inside the square. The highest SKR of 4.64 bits/photon is circled in red, with a dimension of 61, beam spacing of 0.2 mm, and beam waist of 2 mm.

## V. RESULTS AND DISCUSSION

All Pixel mode bases tested are shown in Fig. (6) for calculations of QBER, **a)**, and SKR, **b)**. The QBER simulation shows that for Pixel modes, the choice of basis that produces the least amount of error is the one with the least dimensions, with the smallest beam waist and no beam spacing. Increasing either the beam spacing or the beam waist while keeping the dimension 7 increases the QBER. This is most likely because the aperture is getting more and more filled, causing Gaussian beams near the outside to go outside of the aperture at the receiving end. This trend continues for all bases of constant dimension.

Using the QBER calculations in Fig. (6) **a)** we can then directly apply Eq. (10) to calculate the SQR. We then obtain the 2D discrete plot shown in Fig. (6). The basis with the highest SKR of 4.64 bits/sifted photon is for a dimension of 61, smallest beam waist, and beam spacing of 0.2 mm. This result heavily contrasts the QBER calculations, indicating that the increase in dimensions out scales the decrease in QBER for the bases with higher dimensions. We also note that the most optimal SKR is a basis with a non-zero beam spacing. This is an expected result, as the for a non-zero propagation distance we expect the beam waist of any Gaussian beam to diverge the further it travels.

## VI. CONCLUSION

Quantum Key Distribution is a promising field that can bring a much needed security to the exchange of cryptographic keys. In this project we explored a QKD protocol using a basis known as Pixel modes. We then continued to optimize the parameters of the basis in order to maximize the secret key rate, the amount of useable bits for a key, per photon. The optimal basis was determined to be that of the smallest possible beam waist for each Gaussian beam, and a non-zero 'dead space' spacing between each Gaussian beam of 0.2 mm. This basis was tested against a 1 km free space propagation distance using the Fersnel approximation method, and a weak distortion created using low-coefficient Zernike polynomials.

The project remains ongoing, with the end goal of obtaining simulation results over multiple distances, distortions, and comparing not only Pixel modes, but also Laguerre-Gaussian modes and Orbital Angular Momentum modes (see the final report of Itay Kozlov for simulations on alternative choices of basis). Laguerre-Gaussian are currently the most popular choice of basis for QKD protocols. The comparison of these different modes with propagation distances and distortions, should offer interesting results in the optimization of QKD protocols with alternative bases. Itay and I hope to continue this project into the summer of 2023 with the help of Felix Hufnagel.

## ACKNOWLEDGMENTS

I wish to acknowledge the support of Itay Kozlov, Felix Hufnagel, Professor Ebrahim Karimi, Nazanin Dehghan, and Alessio D'Errico in taking the time to teach the concepts of QKD and related theory of quantum mechanics and optics. Special thanks to Felix Hufnagel for helping with the project specifics, and always being available to chat.

## Appendix A: Code Base

### Link:

https://github.com/justintam5/QKD_Honors_Project

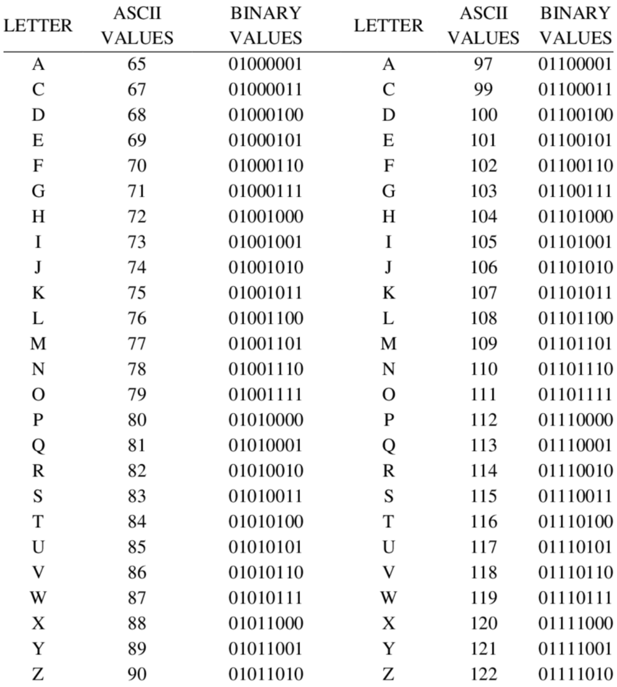
### Read Me:

A Physics honors project for the University of Ottawa on an experimental and theoretical implementation of free-space QKD. The code in this repository will be used to numerically simulate the effect of finite apertures and aberrations on spatial photon modes.

Authors: Itay, Justin, Felix, Alessio, and Nazanin

## Appendix B: ASCII Code Table

A table describing how to encode characters in binary bits, and vice versa, using the ASCII standard.

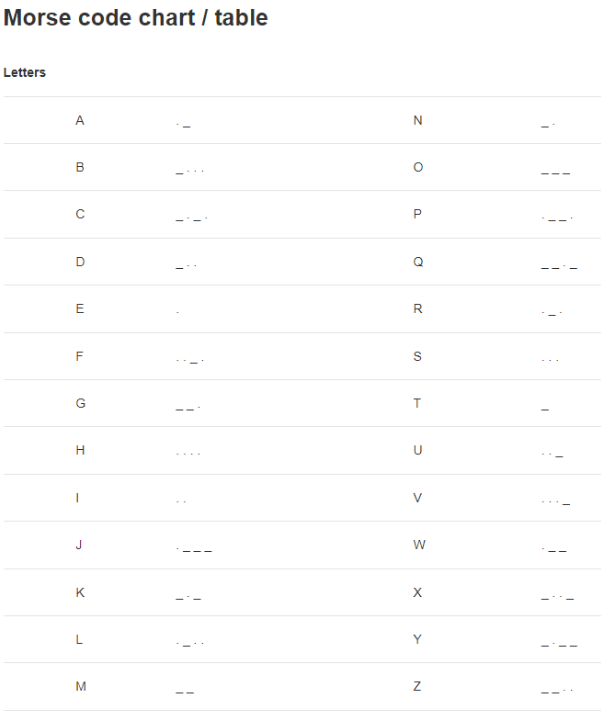


| LETTER | ASCII VALUES | BINARY VALUES | LETTER | ASCII VALUES | BINARY VALUES |
|---|---|---|---|---|---|
| A | 65 | 01000001 | A | 97 | 01100001 |
| C | 67 | 01000011 | C | 99 | 01100011 |
| D | 68 | 01000100 | D | 100 | 01100100 |
| E | 69 | 01000101 | E | 101 | 01100101 |
| F | 70 | 01000110 | F | 102 | 01100110 |
| G | 71 | 01000111 | G | 103 | 01100111 |
| H | 72 | 01001000 | H | 104 | 01101000 |
| I | 73 | 01001001 | I | 105 | 01101001 |
| J | 74 | 01001010 | J | 106 | 01101010 |
| K | 75 | 01001011 | K | 107 | 01101011 |
| L | 76 | 01001100 | L | 108 | 01101100 |
| M | 77 | 01001101 | M | 109 | 01101101 |
| N | 78 | 01001110 | N | 110 | 01101110 |
| O | 79 | 01001111 | O | 111 | 01101111 |
| P | 80 | 01010000 | P | 112 | 01110000 |
| Q | 81 | 01010001 | Q | 113 | 01110001 |
| R | 82 | 01010010 | R | 114 | 01110010 |
| S | 83 | 01010011 | S | 115 | 01110011 |
| T | 84 | 01010100 | T | 116 | 01110100 |
| U | 85 | 01010101 | U | 117 | 01110101 |
| V | 86 | 01010110 | V | 118 | 01110110 |
| W | 87 | 01010111 | W | 119 | 01110111 |
| X | 88 | 01011000 | X | 120 | 01111000 |
| Y | 89 | 01011001 | Y | 121 | 01111001 |
| Z | 90 | 01011010 | Z | 122 | 01111010 |

FIG. 7. Obtained from *Injosoft AB, ASCII TABLE* [4]

## Appendix C: Morse Code Table

A table describing how to encode characters in dots and dashes, and vice versa, using Morse Code.



Morse code chart / table

Letters

| | | | |
|---|---|---|---|
| A | ·_ | N | _· |
| B | _··· | O | ___ |
| C | _·_· | P | ·__· |
| D | _·· | Q | __·_ |
| E | · | R | ·_· |
| F | ··_· | S | ··· |
| G | __· | T | _ |
| H | ···· | U | ··_ |
| I | ·· | V | ···_ |
| J | ·___ | W | ·__ |
| K | _·_ | X | _··_ |
| L | ·_·· | Y | _·__ |
| M | __ | Z | __·· |

FIG. 8. Obtained from *Electronic Notes* [3]

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India,* (1984).

[2] A. Froehlich, *One-Time Pad* (TechTarget, 2022) https://www.techtarget.com/searchsecurity/definition/one-time-pad: :text=In%20cryptography%2C%20a%20one%2D time,one%2Dtime%20pad%20and%20key.

[3] *Morse Code Chart / Table* (electronicrs-notes.com, 2022) https://www.electronics-notes.com.

[4] *ASCII table according to Windows-1252* (Injosoft AB, 2022) https://www.ascii-code.com/.

[5] *Analog Signals vs. Digital Signals* (Monolithic Power Systems, 2022) https://www.monolithicpower.com/en/analog-vs-digital-signal.

[6] A. D'Errico and E. Karimi, *Electromagnetic Vortices: Wave Phenomena and Engineering Applications*, 1st ed. (John Wiley  Sons, Inc., 2022) Chap. 14, pp. 434–436.

[7] D. J. Griffiths, *Introduction to Quantum Mechanics*, 3rd ed. (2018) pp. 17–20, dOI: 10.1017/9781316995433.

[8] A. Sit, F. Hufnagel, and E. Karimi, *Structured Light for Optical Communication* (Elsevier Inc, 2021) Chap. 6, pp. 139–167.

[9] B. M. S. R. Allen, L. and J. Woerdman, *Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes*, Vol. 11 (Physical Review A, 1992).

[10] S. Konijnenberg, A. J. Adam, and H. Urbach, *Optics* (Delft University of Technology, 2023) Chap. 6, pp. 123–125.

[11] K. Niu and C. Tian, Zernike polynomials and their applications, Journal of Optics **24** (2022), dOI 10.1088/2040-8986/ac9e08.

[12] N. Zhao, X. Li, and G. Li, Capacity limits of spatially multiplexed free-space communication, Nature Photon **9**, 822 (2015), https://doi.org/10.1038/nphoton.2015.214.