Towards a pointing system for free-space quantum key distribution

A Thesis

submitted to

Indian Institute of Science Education and Research Pune
in partial fulfilment of the requirements for the
BS–MS Dual Degree Programme

by

Yash Amar Chalke

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA

March, 2026

Supervisor: Prof. Sushil Mujumdar

Yash Chalke

Certificate

This is to certify that this dissertation entitled **Towards a pointing system for free-space quantum key distribution** towards the partial fulfilment of the BS–MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by **Yash Chalke** at Indian Institute of Science Education and Research under the supervision of **Prof. Sushil Mujumdar**, Professor, Department of Nuclear and Atomic Physics, TIFR, during the academic year 2025–2026.

Prof. Sushil Mujumdar

Declaration

I hereby declare that the matter embodied in the report entitled 'Towards a pointing system for free-space quantum key distribution' are the results of the work carried out by me at the Department of Nuclear and Atomic Physics, Tata Institute of Fundamental Research (TIFR) Bombay, under the supervision of Prof. Sushil Mujumdar, and the same has not been submitted elsewhere for any other degree. Wherever others contribute, every effort is made to indicate this clearly, with due reference to the literature and acknowledgment of collaborative research and discussions.

Yash Amar Chalke
20211268

Contents

List of Figures

Abstract

In chapter 1: We start with introducing the field of quantum key distribution, the development done in it till the current date, the possible physical methods to to implement it in free space and to implement using the optical fibers and their comparison with respect to the physical implementation and efficiency. After that I introduce the problem statement for my thesis which is the balloon to ground quantum communication.

In chapter 2: We discuss the field of cryptography and the One time Pad system which is used in day to day life. Then we discuss what information actually is, how can we quantify it, and the current classical algorithms used. Then we introduce the quantum mechanics and it's fundamental properties. Then we delve into the main topics for the development of the quantum key distribution viz. Entanglement and No-cloning theorem. Then we go to the topic of Quantum Key distribution and explore the prominent protocols in use.

In chapter 3: In this chapter we discuss the actual experimental methods which are implemented during my work. We start with discussing the spontaneous parametric down conversion process where two photons are generated from a single pump photon. We discuss the apparatus required for it viz. the non-linear crystal and it's specification. Then we go into the optical beam experiment were we create an entangled photons beam starting from creating a gaussian beam profile to placing the crystal in right position to going in the experiment to tune the temperature of the crystal to enhance the entanglement and finally we measure the S-parameter to certify that we have created entangles photons.

Then we go into the technological domain of the project where we focus on the concept of mode-matching which is required for receiving the optical signal. We discuss the embedded systems and feedback loops required for this process. Finally we see the optical setup where the beacon laser beam is used to guide the required quantum beam to mode-match with the collimator.

Acknowledgment

I want to Thank Prof. Sushil Mujumdar for giving me this opportunity and providing adequate guidance from time to time. I would also like to Thank Mr. Sreeman Narsingham for his crucial role throughout the duration of the project and development of all the experimental setups. I sincerely admire constant guidance and time from their busy PhD final year work by the senior PhD students of my group Mr. Vikas S. Bhat, Mr. Rounak Chatterjee and Ms. Kiran Bajar. I would like express my gratitude to Prof. T. S. Mahesh for introducing me to this domain of quantum information. I would also like to thank Prof. Sonjoy Majumder for further strengthening my foundations in this field. I would also like to thank all friends of mine viz. Sonali, Mayuresh, Amit, Subhas, Abhay, Rodney, Sarvesh, Devesh, Naveen, Samsuzzaman, Jetharam, Prasad, Raghav and Achyushman for their support during this time.

Chapter 1

Introduction

1.1 History

With the rise of computers during 1980's the concern of **Data Security** became very important. Security was majorly focused on controlling the large physical frameworks. Then in 1976, Whitfield Diffie and Martin Hellman introduced public-key cryptography, which revolutionized the domain of data encryption [1]. With the fundamental quantum physics being established by then, the first idea to use quantum advantage for conjugate coding in order to prevent copying of data was proposed by Stephen Wiesner in 1960's[2]. Carrying that work ahead to the first experiment of quantum cryptography was shown by Bennett and Brassard [3] in 1992.

Over the period other Quantum key distribution(QKD) protocols were introduced viz. B92, BBM92, E91, etc were introduced strengthening the connections between entanglement distribution and QKD protocols[4] [5] [6]. As the data encrypted using is unhackable due to the fundamental physical phenomenon; The *No-Cloning Theorem* [7], researchers understood the importance of it in the coming age of information and the QKD experiments started taking shift from laboratory set-ups to real world experiments in free-space and optical fiber in order to expand the distance.

The first demonstration of free space QKD was conducted by Jacobs and Franson in 1996 in outdoor daylight [8]. Following that other major feats were achieved viz. 10km optical fiber QKD demonstration[9], improvement of single photon detectors, development of decoy-state protocols to defeat photon number splitting attacks[2]. Then with the successful demonstrations with increasing distances, the Ground-to-Ground optical links were shifted to Ground-to-Air optical links and eventually satellite quantum communication. One of the major breakthroughs in that domain was the *Micius* satellite of the China[10]. And lately China Quantum Communication Network launched a micro-satellite *Jinan-1* achieving the highest QKD demonstration till now of 12000 km[11]. The exploration of this field through engineering new systems to guarantee more security and establish communication on moving platforms(satellites, aircrafts, drones) still continue.

The new avenues for development in this field are quantum transduction, where the quantum information is converted from one physical form to other[12], MDI(Measure device independent)-

QKD which is a new protocol to overcome the loopholes in the initial QKD protocols[13] and quantum repeaters, which turns out to be promising approach to build large scale quantum communication networks[14].

1.2 Motivation

To perform quantum cryptography, we need a quantum system which is reliable source to transmit entangled qubits between two parties. Out of all existing systems photons are the most efficient quantum system in this matter. As they travel at speed at light and are comparatively very robust to environment noise. The communication link can be established by two methods within the parties: The free-space and the fiber transmission.

Recent studies have shown that we cant do long distance quantum entanglement distribution in the fibres [15] [16] [17]. So, the interest in demonstration of free-space quantum communication is pretty obvious. Satellite quantum communication has been a topic in which research and innovation has grown rapidly during past decade. The reason is clear that it allows long range communications and the path of satellite is predictable allowing to establish an optical link. But there are few drawbacks to this technology, first and the most important, the communication time is very less i.e 5-10 minutes per pass of a LEO(Low Orbit Satellite) [18]. Then the satellite parts are not replaceable, so we cant change the components when required and the most important is Satellites way to **expensive**.

So an *efficient alternative* can be considered a balloon floating at the height of 40-50 km in the stratosphere. Compared to satellite it can establish same distance of long range communication and it will be much cheaper than the satellite. Most important reason that unlike satellite, it will have long hours of interaction time between two parties and if any component is to be replaced we can safely do that in this case.

But this comes with it's challenge. We need to establish an optical link between the balloon and the receiver so that signal detection will be successful. But unlike satellite balloon doesn't have its definite trajectory in the free space. It will be susceptible to the turbulent environment making it's path unpredictable resulting in difficulty in establishing optical link. This thesis focuses on improving the initial part of this task. Here we will focus on tethered balloon and the corresponding methods to achieve the optical link between two parties.

Chapter 2

What is Quantum Communication

To understand the role of quantum mechanics in cryptography, we will go through the basics of quantum mechanics which are needed to understand the quantum key distribution methods.

2.1 Cryptography

2.1.1 Encryption

Cryptography is the practice of developing and using coded algorithms to protect and obscure the transmitted data[19]. The method by which this is done is called Encryption. In this method, we transform the message, data/information into an unreadable series of characters/bits. In this way, only authorized people are able to access it. This scrambles the data in such a manner that it is in an undecipherable format. This is a reversible process otherwise the data won't be able to be decrypted again. The efficiency of encryption is measured in the terms of the following characteristics[20]:

- Confidentiality: the data should not be accessible to the unauthorized personal and vice versa
- Integrity: data should not be tampered with and, the modification should be allowed only by the authorised person
- Authenticity: The sender and the receiver must be the intended sender and receiver ,and there should be no mismatch.

To explain in simpler terms, it takes the readable data and then scrambles it in such a format that it couldn't be understood. In order to understand the scrambled data ,the reader will require the reverse-process of the received data, otherwise it will appear in a random form. So when the above three conditions are satisfied, we say that the data is encrypted. Let's say you want to share the information 'HELLO' with someone. To encrypt this information, we will use a specific algorithm, for ex. we will write 3 characters ahead in alphabetical order(also known as the *Caesar* cipher, it was used by Julius Caesar for information transfer during the time of the Gallic wars). So the information now becomes, 'KHOOR'. This information is not comprehensible. Now, if this information is to be read, the reader needs to know the algorithm

used to encrypt this, and then the reader can reverse-process that algorithm. This is called as *decryption*, i.e. it transforms the data which appeared to be random before into a readable format. As you can see, this satisfies the above three conditions mentioned for the data to be called encrypted. But this above algorithm is very simple and not as strong for the current classical algorithms in order for them to not be able to decode it. If we have to ensure the strong encryption, then we need more complex algorithms which will satisfy the above three conditions and the encryption should be random so that the data is undecipherable.

2.1.2 One-time-pad

The application of cryptography is vast in day-to-day life. It ranges from sending and receiving secret information from personal to national security, electronic chips for purchase purposes and banking transactions. This process consists of two steps *encryption* and *decryption*, as mentioned in the previous section. In order for this to be strong encryption we should use a specific key for that purpose. [21].

One-time pad(OTP) is a powerful method of encryption which depends on the idea of using a random key for the length of the message that is sent and the key will be with the sender and receiver and it will be generated only once. After that the key is destroyed. This is a method of private key encryption and, it is highly effective as long as the keys are secure. Consider the similar previous case, where we have to transmit the string 'HELLO'. It typically uses the XOR mechanism to encrypt the data using the key. The key which we have with us will be '31625'. So, same as done in the previous case, we will shift the string, and it will become 'KFRNT' and then this can be decrypted using the same key but here we have to shift in reverse order. Now, as long as the keys are of the same length as of the data to be transmitted, it is very hard to decode the message by the normal classical computers, which makes this method of encryption very powerful. This is also called as private key (symmetric) encryption.

So, now the task remains to generate a key that will be random and be able to encrypt and decrypt the information with high security. But when the keys are compromised, then the first rule of the encryption i.e. confidentiality is violated and the data is no longer safe. Thus the challenge remains to safely distribute the key to the both parties involved here, then the data encryption will be unbreakable.

2.1.3 Disadvantages in classical methods

The first idea of formulating a device working on quantum mechanical laws was formulated itself in 1981 [22], and then it took two decades to build it's hardware and use it in real life purposes. Before that, the classical algorithms were used for encryption are majorly RSA, AES, etc. In this age of information, prime numbers became a major source of random key generation because it is very hard to do prime factorization of the large numbers.

One such algorithm is the RSA algorithm[23]. RSA cryptographic algorithm uses advanced number theory for the encryption process. The algorithm generates the random key as follows[21] [24]:

1. Large prime no.s are chosen (Suppose p and q)
2. compute p*q and (p-1)*(q-1)
3. select a number **e** such that 1 ¡ e ¡ (p-1)*(q-1)
4. the number e should satisfy the following properties: gcd(e, (p-1)*(q-1)) = 1 and both should be coprime
5. the final step : d = e^{-1} mod((p-1)*(q-1))

We define n = p*q. Here the e stands for the encryption and d stands for the decryption. So when encrypting the message **M**, we do it as **C** = M^e mod(n) and then while decrypting the message we perform the reverse operation as **M** = C^d mod(n). This is a method of public key (assymetric) encryption where your data is to transmitted securely on public network. The safety of this algorithm relies on the fact that even if the numbers (e,n) are known on the public channel, it is very hard to know the number d[21] [23].

But using high computational methods for processing or running brute force algorithms, the prime factorization could be performed and thus breaking the security of the algorithms mentioned above. Moreover, algorithms like Shor's algorithm which uses quantum computing for prime factorization, these encryption could be easily broken down[25]. Thus even if it is hard to decode the data in this era it couldn't be said impossible. Thus we need an even strong method for this purpose to keep information transmission secure. So, the idea of using more robust method of data encryption is needed and we resort to the basic principles of quantum mechanics which allows us to do so.

2.2 Basics of quantum information

2.2.1 Information theory and Entropy

As discussed till now, we will first focus on transmission of data. The structured data is termed as information. Information is relevant or connected to concepts as communication, knowledge, constraint and most importantly, the *Entropy* [26]. Entropy is the measure of randomness or extensiveness of the system. To understand why entropy is associated with information, consider the following example: Suppose you have a unbiased coin; then when you toss it multiple times half a times you get '*heads*' and half times '*tails*'. When you do it large number of times, the probability you will get either of the outcomes tends to $\frac{1}{2}$. Now suppose the coin you are going to toss is heavy from the *heads* side, then when you toss multiple times

you are much sure in this case that the outcome is *heads*. Extending this example to further large systems we can conclude that more the extensiveness of the system, less information content it will have[6] [27].

Bit is a basic unit of information. This gives the information a physical form which enables it to be transmitted and manipulated. It is mostly represented as two level voltage system in a electrical circuit permitting only two voltage levels. This was first time analytically represented by Gottfried Leibnitz who also established the formalism of this system [28]. Bit is represented by one of the two values **0** and **1**. N bits can encode till 2^N variables. The information content that could be transmitted in this system will be

$$I = \sum_{x=1}^{2^N} p_x log_2 p_x$$

(the choice of basis here corresponds to the choice of unit for measuring the information. For binary digits it is 2 and for decimal digits it is 10 [29]). Here p_x is the probability or the quantity of the x^{th} bit. And this is fundamentally equal to the Gibbs entropy. Gibbs entropy is the function of the probability distribution over phase space of an ensemble [30] which calculates the extensiveness of the molecular system.

$$H(X) = -k_b \sum p_x log_e p_x$$

where the k_b is the Boltzmann constant and p_i is the probability of the i^{th} ensemble. As the Shannon entropy is defined in same way it also satisfies the same properties of Gibb's entropy which later helps to quantify quantum information[6]. Where the H(x) is the average information carried by the variable x. Thus it is non-negative for any random variable and the mutual information could be quantified in order to know the uncertainty of the other variable once the first variable is measured. Thus uniform probability distribution implies high entropy and vice versa.

Shannon entropy quantifies the information compression which could be send through the bits, and the rate over which we can safely communicate over the noisy channels [31]. As the Shannon entropy is restricted to use on discrete random variables, it cant be used for quantification of quantum information which has continuous variables. The quantum analog of the Shannon entropy is called as the Von neumann entropy which is defined as:

$$S = -k_b \sum p_i log_e \rho_i$$

where the ρ is the density matrix(it will be discussed in the **Section 2.2.3**) which describes the ensemble.

2.2.2 Qubits

The analogous basic unit for information to bits in quantum system is called **Qubit**. Similar to bit it is represented in two level system $|0\rangle$ and $|1\rangle$ The main property of qubit differing from the classical bit is the *Superposition*. Superposition is fundamental property in quantum mechanics which allows a system to exist partly in all possible states for ex. two states of polarizations for photon[32]. This is the property which differs from the classical bits and allow to do multiple calculations at single instance.

The mathematical space where these qubit are represented in the vector form is called as **Hilbert Space**. It is an complex vector space with an defined *Inner Product operation* between two states and the state in any instance of time in it is *normalized*[33]. Inner product is a operation which mathematically calculates the dot product between two states and physically it is interpreted as the overlap between the two states. For an N-qubit system the dimension of the hilbert space will be 2^N.

Consider a single qubit system, general state exits in the linear combination of the basis states and is denoted as

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

where a and b are complex numbers satisfying the normalization condition $|a|^2 + |b|^2 = 1$. The representation of this state in Hilbert space will be $\begin{pmatrix} a \\ b \end{pmatrix}$, where the basis of this 2-dimensional hilbert space will be $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Observables which are used to measured in physical space are termed as Operators in Hilbert space. These operators are linear in nature and they map the states to same Hilbert space. By definition Hilbert spaces are isomorphic i.e. there exists a unitary transformation which transforms one Hilbert space to other[34]. For example in quantum computing the *Z-basis* (basis: $|0\rangle$, $|1\rangle$) is related to the *X-basis* ($|+\rangle$, $|-\rangle$) via the unitary transformation $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ which is commonly known as the Hadamard operator [6]. This property will later be useful in explaining the phenomenon of measurement of quantum states in further section.

2.2.3 Representation of qubits

The qubits are represented on the Bloch sphere as shown in the diagram below. The classical bit only exists in the state 0 or the state 1, but the qubit has all possible superpositions which is represented as shown in the Fig. 2.1. The above pole is the 0 state of the qubit and the downside is the 1 state of the qubit, one example of the superposition state is shown in the diagram where it exists in the middle of the sphere. A random qubit state is shown as $|\Psi\rangle = cos(\frac{\theta}{2})|0\rangle + e^{\iota\phi} sin(\frac{\theta}{2})|1\rangle$, where the θ is the polar angle and ϕ is the azimuthal angle(the angles are according to the polar co-ordinate system)[6].

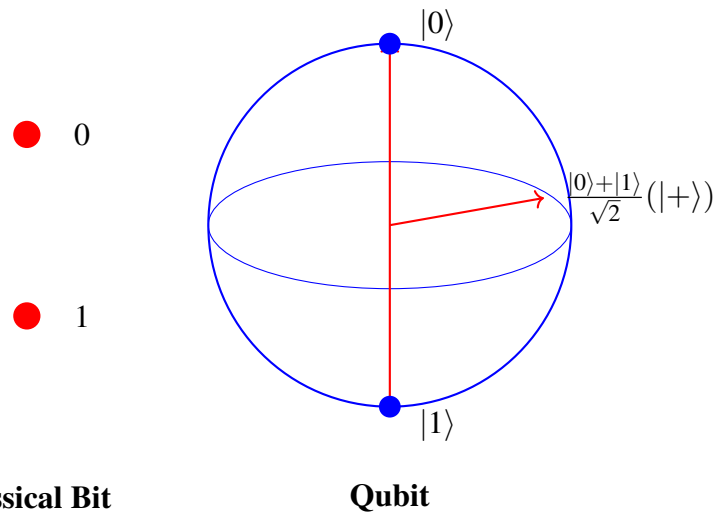


Figure 2.1: Comparison between a classical bit and a qubit represented on the Bloch sphere

For the qubits(as a system) to be able to work as a *quantum computer*, the physical system should satisfy some specific criterion. They are known as the DiVincenzo's criteria and are as follows[35]:

1. The physical two level system should be scalable
2. We should be able to initialize it or able to prepare a known state
3. It should have longer coherence times in order to the gate operation to take place on the qubits
4. It should have universal set of quantum gates
5. We should be able to address the specific qubits individually and perform the gate operations and measurement on them
6. We should be able to convert the stationary qubits into the flying qubits in order to transmit the information.

There are few physical systems which satisfy these viz. NMR spin qubits, photons, ion traps, neutral atom traps, optical cavity and atom quantum computer(physics governed by the quantum electrodynamics), etc [6].

The other representation of qubits is necessary for the case of the multi-qubit system which is called the density matrix formalism. As mentioned before in **Section 2.1.3**, the quantum states exists in the ensemble of states, and it is represented as

$$\rho = p_1 |\Psi_1\rangle \langle\Psi_1| + p_2 |\Psi_2\rangle \langle\Psi_2| + ...p_n |\Psi_n\rangle \langle\Psi_n|$$

where, p_i is the probability of the i^{th} ensemble and it is associated with the outer product of the particular quantum state. Here, $\rho = \rho^\dagger$ because it represents the physical state and the

diagonal elements are probabilities which should be the real numbers. This formalism accounts for the quantum correlations between the system, which is not accounted in the vector space representation of the multi-qubit systems. Using this we can differentiate between the mixed states and the pure states. The measurement and quantification using this will be discussed in detail in the **Section 2.2.5**, but using the density matrix it can be calculated as $Tr(\rho^2) = 1$ for the pure states and $Tr(\rho^2) < 1$ for the mixed states. They are also used in modeling the open system properties where the system interacts with the environment and the time evolution is governed by Lindblad dynamics[36].

2.2.4 No-Cloning Theorem

We discussed in the **Section 2.1.3** that the major disadvantage to classical key encryption is that keys cant be faithfully transmitted between the both parties. There is the threat of decoding by some means always by an Eavesdropper. So, the information transferred through the qubits is the in the advantage for cryptography because they cant be cloned i.e. it is fundamentally impossible to create a copy of an arbitrary unknown quantum state[7]. It's proof goes as: Suppose we have two states: $|\Psi\rangle$ and $|\Phi\rangle$, and there exists an arbitrary operator U which can clone them.

$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$$

So, the same operation should be true for any other state. We thus operate the U on another state and then the sate which is equal superposition of the both states considered earlier.

$$U|\Phi\rangle|0\rangle = |\Phi\rangle|\Phi\rangle$$

$$U\frac{|\Psi\rangle+|\Phi\rangle}{\sqrt{2}}|0\rangle = (\frac{|\Psi\rangle+|\Phi\rangle}{\sqrt{2}})(\frac{|\Psi\rangle+|\Phi\rangle}{\sqrt{2}})$$

But as discussed in the **Section 2.2.2**, the quantum operators are linear, so we can operate the unitary operator individually inside the brackets.

$$U\left(\frac{|\Psi\rangle+|\Phi\rangle}{\sqrt{2}}\right)|0\rangle = \frac{|\Psi\rangle|\Psi\rangle+|\Phi\rangle|\Phi\rangle}{\sqrt{2}}$$

And as you can see, the above two equations gives us the contradiction. So, we can infer from that, no such U operator exists [6]. This tells us that if we transfer our information by encoding in the qubits it will inevitable by the eavesdropper to copy the information as opposed to the classical case.

2.2.5 Measurement of the quantum systems

In quantum mechanics a state exists in continuum of states between basis states but an objective phenomenon is occurred only after observation and then the state instantaneously collapses to one of the single eigenstates(of the observable). Due to this the previous information of the superposition is lost. Thus the measurement is an non-unitary/Irreversible process[6]. So even if our communication link is eavesdropped, due to this property we will be able to tell that the information is compromised and discard it. Unlike in the classical case, where the compromised information goes undetected.

Consider the $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ state. After measurement in *Z-basis*, it will collapse to either of one basis states. After N measurements, you will get both the states around $\frac{N}{2}$ i.e. with half propablity each. In general, a quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$ will give the output $|0\rangle$ with probablity $|a|^2$ and $|1\rangle$ with probablity $|b|^2$. When the same state is measured in the *X-basis* will give output $|0\rangle$ with probablity 1 and the other orthogonal state $|-\rangle$ with 0 probablity. (Note: This is the ideal scenario, while doing actual experiment, we dont get this clean results. Many factors are involved viz quantum fluctuations, interaction with environment, detector inefficiency, etc so some times we can also get $|1\rangle$).

The measurement in *X-basis* can simply be done by changing the measurement procedure by applying Hadamard operator before final detection. This is allowed because of the isomorphism property of the Hilbert space mentioned in the previous section. Hadamard operator here is the unitary transformation between the both bases.

In the previous section we introduced the concept of ensembles. Consider the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}) + \frac{1}{\sqrt{2}}|0\rangle$$

Performing the measurement in Z-basis will give us some probability of $|0\rangle$ and some of $|1\rangle$. But we wont be able to simply reconstruct the previous state or predict the previous state from it because it also has some fraction of the $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ state, which can't be accounted for using this. So, Tomography is performed on the state in which we construct the density matrix of the system. After that $Tr(\sqrt{\sqrt{\rho_m}\rho_r\sqrt{\rho^\dagger}})$ gives us the probability of the ρ_r that is the required state. Where ρ_m is the measured state vector through the tomography. Tomography scales as 3^n more type of measurements where is the number of qubits. It is done to calculate the all the elements of the density matrix.

2.3 Entanglement

The concept of entanglement has played an important role in the development of quantum mechanics[37]. This is the property which is purely quantum mechanical with no classical counterpart. Due to this property of quantum mechanics, it got lot more leverage in computation

as well in technological applications(for ex. teleportation [4], ghost imaging [38], quantum parallelism [39], simulating physical equations [22], etc).

2.3.1 Non-local nature of quantum mechanics

The principle of locality[40] states that the particle/object is affected by the measurement only in the immediate surroundings. Entanglement is a multi-qubit phenomenon where even though two or more particles may appear physically at different places, but they are inseparable in there individual states. Consider two particles **A** and **B**. There combined state can be defined as $|\Psi_A\Psi_B\rangle$. If they are entangled then

$$|\Psi_A\Psi_B\rangle \neq |\Psi_A\rangle\,|\Psi_B\rangle$$

This results in an incredible conclusion. If entangled particles are physically apart then by measuring one particle we can know the outcome of the other particle. This results proved to violating locality and thus quantum mechanics is termed as non-local in nature [41] [42] because it violates the principle of locality mentioned above. This might seem that if two particles are away from each other with the distance of light years between them and they are entangled. If one party measures the particle with itself, then they know the state of the other party instantaneously; the information which would rather have taken light years to travel. Even if this is the case, quantum mechanics doesn't allow faster than light communication[43]. This property is the key in quantum key distribution experiments. Because, as seen in the **Section 2.2.4**, the quantum states cant be cloned, and then when the two parties have shared an entangled pair, the measurement of their own particle they now know that what is exactly the result of measurement of the other party(Given that the measurement basis of both are same).

2.3.2 Measures of quantum entanglement

To successfully implement the QKD protocols, entanglement must be quantitatively measured. This is crucial in comparing and analyzing different protocols. The difference in entanglement and classical correlation is that knowing the complete state of the system does not provide any information about the individual states of the components; they can be in complete uncertainty unlike that in the classical case[40].

Following are the some measures of the entanglement[37] :

1. Concurrence: It compares that how well the two qubits are entangled.

$$C = max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4)$$

   If C = 0, then they are separable qubits and if C = 1, then they are maximally entangled qubits

2. Entanglement entropy: This is an information theoretic measurement. This calculates how far a state is from being separable[44].

3. Negativity: We calculate the partial transpose of the total density matrix we have and then measure it's eigenvalues. If the eigenvalues are negative then the system is entangled.

4. Distillable entanglement: This is the amount pure extractable entanglement of the quantum state. It is used to quantify that how useful a state might be for the quantum communication. This is defined as the maximum number of the bell pairs obtained via the LOCC(Local observables and classical communication: it is the allowed operations in the quantum information theory [6])

As seen these all measurements uses the density matrix for calculation and the quantification of entanglement. But we know that the process to calculate density matrix(State Tomography) takes lot amount of resources and time. So we need a better measurement of the entanglement which could be done in less number of measurements and is reliable.

2.3.3 Bell's Inequality

This is an clever method where we perform the local operations and quantify the entanglement of a 2-qubit system. The 2-qubit maximal entangled states are called as bell states. There are four bell states:

$$
\begin{aligned}
|\Phi^+\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Phi^-\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Psi^-\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$

These can be created in different two-qubit systems and it will be discussed for singlet state of two-photon polarization entanglement in the optical system in the **Chapter 3**.

Bell introduced in his paper [42] that the nature of the quantum mechanics is non-local and analyzed the two separated entangled particles. To understand the bells inequality consider the following example:

Suppose one person shares two particles with Alice and Bod as shown in Fig. 2.2 and both the particles can take values either +1 or -1 on measurement, and now one of them is shared with two parties each *Alice* and *Bob*. They can measure from any of the observables with them. If the particles are classical in nature, then

$$\langle AC + BC + BD - AD \rangle \leq \langle (A+B)C + (B-A)D \rangle = 2$$

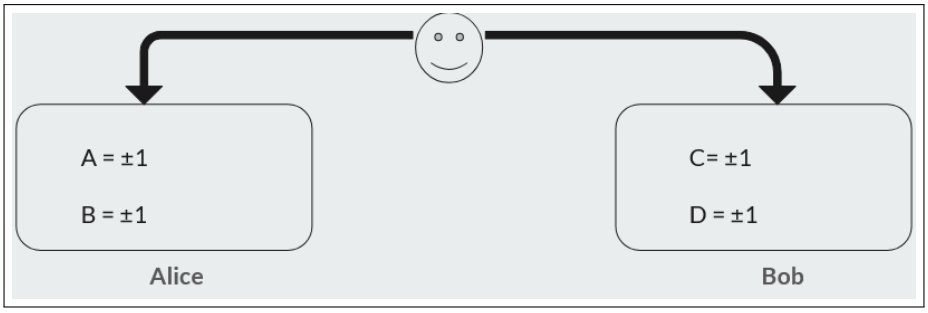


Figure 2.2: Thought experiment to understand bell's inequality

Now consider the the quantum mechanical case. Suppose the state shared between those parties is a bell state $\frac{|01\rangle-|10\rangle}{\sqrt{2}}$ and the observables measured by them are A = Z, B = X, C = $\frac{Z+X}{\sqrt{2}}$ and D = $\frac{Z-X}{\sqrt{2}}$.

In this case the

$$\langle AC + BC + BD - AD \rangle = 2\sqrt{2}$$

So, this experiment tells that clever measurement of entangled photons, we can violate the classical bound of the Bell's inequality[6] thereby quantifying the entanglement between two-parties.

2.3.4 Spontaneous Parametric down conversion

This is a is a second-order nonlinear optical process in which a high-energy photon (pump) spontaneously splits into two lower-energy photons viz. signal photon and idler photon. This arises due to the second order susceptibility of the material used to generate the entangled photons. It is fundamentally an quantum mechanical process and cant be explained by the classical mechanics[45].

The electromagnetic magnetic field is quantized and the interaction Hamiltonian due to this is defined as

$$H_{\text{int}}(t) = \varepsilon_0 \int d^3r\, \chi^{(2)}\, E_p^{(+)}(\mathbf{r},t)\, E_s^{(-)}(\mathbf{r},t)\, E_i^{(-)}(\mathbf{r},t) + \text{h.c.}$$

where E_p is the pump field and other two are the fields of the entangled photons created. We treat the pump beam as classical and other two are quantized using the second quantization method,

$$\hat{E}^{(+)}(\mathbf{r},t) = i \sum_{\mathbf{k},\lambda} \left(\frac{\hbar\omega}{2\varepsilon_0 V} \right)^{1/2} \hat{a}_{\mathbf{k},\lambda}\, \mathbf{e}_{\mathbf{k},\lambda}\, e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)}$$

and then we substitute it in the above Hamiltonian which gives

$$H_{\text{int}} \propto \int d^3r\, e^{i(\mathbf{k}_p-\mathbf{k}_s-\mathbf{k}_i)\cdot\mathbf{r}}\, e^{-i(\omega_p-\omega_s-\omega_i)t}\, a_s^\dagger a_i^\dagger + \text{h.c.}$$

The exponential part in the Hamiltonian gives us the phase matching (Fig: 2.3)condition for the entanglement.

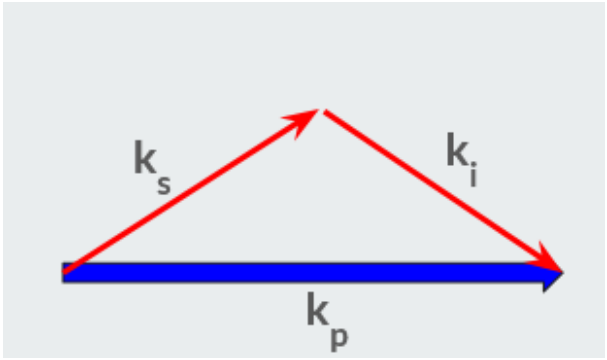


Figure 2.3: Condition for phase matching in Spontaneous Parametric down conversion

2.4 Quantum Key Distribution

2.4.1 Security assurance in quantum key distribution

Though the QKD comes with the fundamental security assurance, there are some drawbacks to that. Most importantly the delicate operation of the entangled photons comes with it's challenges. In atmosphere, the turbulence causes the beam to diffract, the qubits to de-cohere and diorder changes the state or mode making the actual implementation of the QKD hardware more difficult.

Furthermore, if we try to deviate from the entanglement distribution and focus on establishing communication using single photon source it will cause a great threat to no-cloning theorem's assurance. Because if the single photon source is actually not single photon(which is currently not possible to make perfect single photon source which would operate on time), then the eavesdropper might just take exploit that fact by measuring the other photons and we wont be able to detect that !

2.4.2 Protocols in quantum key distribution

The advantage of quantum key distribution over classical is that the qubits cant be cloned[7]. And even if any eavesdropper tries to access the data, the qubits will be collapsed and the receiver will know that the data is corrupted. This makes the data transferred using QKD unhackable.

Following are some algorithms used to implement the QKD:

- **BB84 algorithm**[6]: Alice chooses a random bit string at first and then from the bit sequence required to be termed as the *Key* she encode them in $|0\rangle$ *or* $|1\rangle$ if the random bit has 0 and if it has 1 as the string, she encodes it as $|+\rangle, |-\rangle$.

  After receiving the quantum data, Bob measures randomly in X or Z basis and discards the bits for which his and Alice's measurement basis is not same.

Then they perform a security check on the received bits to confirm any eavesdropping event. Remaining bits are kept as the key.

- **BBM92 protocol**: The BBM92 is an entanglement based protocol where Alice and Bob measure shared EPR pairs in complementary (i.e., Z and X) bases. Eve's tampering is tested by checking the correlations in these two bases rather than testing the violation of the Bell inequality, and as such, the security of the BBM92 protocol can only be assured under the condition that measurements in the complementary bases are accurately implemented, meaning that the measurement bases must be precisely aligned[46].

- **EPR protocol**[6]: Here the bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is distributed between two parties and then using the non-orthogonal basis, the measurement is done to ensure the entanglement. Then after that the two parties individually measure the basis and they are ensured that they share the same key.

2.4.3 Time synchronization

There is a purely quantum property of light *Anti-Bunching* of photons[47]. Where the photons arrive at regular intervals of time rather than random intervals, this leads $g^2(0) < 1$. Using this principle time taggers are used to find the coincidence counts of the entangled photons. When we send the two beams in S-parameter or any such experiment, the path length traveled by the photons will be completely different so they are detected at different times. To be able to successfully implement entanglement distribution, we need to be able to detect the photon pairs. So, using this anti-bunching principle the time-tagger calculates the maximum overlap of the photons in an interval and the coincidences are measured.

Chapter 3

Quantum Key Distribution: The Experimental implementation

Till now we have discussed about what the Entanglement is and the process to create the entangled photons. This will help us to discuss the implementation of QKD protocols using the entanglement distribution.

Next we will look in detail on the experimental optics methods which help us to create entangled photons including the apparatus used for it. Then we will use the previous knowledge of the quantum mechanics for their effective characterization. Then we will discuss the development of the device to detect the light from a far away distance in the turbulent environments and couple it to the detector.

3.1 Creating Entangled photons

3.1.1 Non-linear crystals

In a material, when light interacts with it, and the response of that material is directly proportional to properties of light such as intensity of light and susceptibility of the material, then it is a linear phenomenon. So, it doesn't lead to any change in fundamental properties of light such as polarization and wavelength. But in contrary, in Non-linear optics these fundamental properties do change depending on the intensity of the input light giving rise to various different properties such as second harmonic generation, optical parametric amplification, optical rectification, kerr effect, etc [48] [49] [45]. Nonlinear phenomena become relevant only when the input light is very intense i.e the optical phenomenon should be high than 10^8 V/m [50].

Spontaneous Parametric Down Conversion(SPDC) is a non-linear process where two-entangled photons are generated spontaneously due to the down conversion of the frequency of the incident light. For that to happen the non-linear crystals i.e. crystals with second or higher order susceptibility(often χ^2) are used which convert the wavelengths emitted by the laser by a second order process. There are some properties an non-linear crystal should satisfy[51]:

- Non-linearity coefficient is the strength coefficient which depends on both the materials and the operation conditions. It is mostly the χ^2 non-linearity for the frequency conversion process or the ker non-nonlinearity in the optical fiber. Higher the coefficient more efficient will be the entanglement generation efficiency.

- Phase matching: In a birefringent material, the refractive index depends on the polarization of the passing light. When the photons will be generated after passing through such material they will have different wave-vectors. For maximum efficiency of the down conversion the mismatch between these phases should be as minimum as possible i.e. $\vec{k_1} = \vec{k_2} + \vec{k_3}$.

- It should have high optical transparency for all the wavelength involved i.e. the pump photons and the entangled photons.

Most commonly used crystals for this are BBO(Barium Borate) crystal KTP(Potassium Titanyl) crystal. Periodically poled KTP crystal is used for satisfying the quasi phase matching conditions at respective temperatures. In our case Type-2 crystals are easier to use because of their narrow linewidth, easy separation of the signal and idler with a polarizing beam splitter, and robustness to temperature. By tuning the temperature of these crystals we can satisfy the quasi-phase matching condition, where the phase exactly do not need to match but due to the periodic pooled nature of the crystal the remaining phase is automatically ensuring the constructive interfernce [52].

3.1.2 Placement of the crystals

The PPKTP is the periodically polled KTP crystal in which there alternate orientation of birefringent materials to periodically aligned reversed ferroelectric domain enabling the quasi-phase matching conditions. We use a type II crystal as it has higher effective non-linear coefficient and after phase-matching it has better bandwidth of frequency[53] Due to the birefringence, these two travel with different group velocities[54]. This produces the delay in between time of photons will traveling.

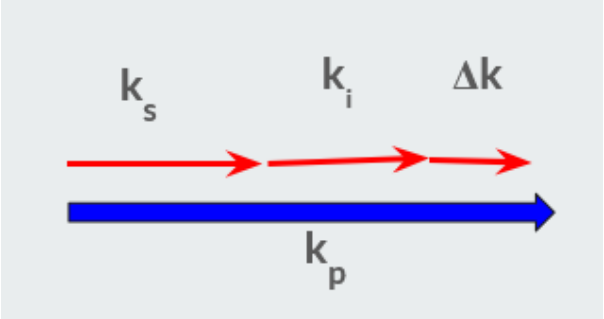


Figure 3.1: This is the phenomenon of quasi-phase matching in the non-linear crystals which doesn't require exact phase matching

As this temporal delay is due to the different group velocities, another KTP crystal is kept in there path as a *compensator*, which reverses the group velocities of both of the photons and the delay is compensated. Now, the photons are generated throughout the crystal and the average generation point of the entangled photons is in the middle of the PPKTP crystal. So, to cancel that delay the photons should travel exactly the same distance, so the length of the KTP crystal is kept half the length of the PPKTP crystal.

3.1.3 Gaussian beam profile

When a beam profile is transmitted in free space it's profile after traveling for large distance is it's fourier transform[55]. So, we choose to proceed with gaussian beam profile because it's fourier transform will remain gaussian in nature making the beam profile predictable and easy to couple with fiber in the other end.

To create an gaussian beam profile we use the method of spatial filtering. Here, when the beam is passed to an pinhole, the diffraction pattern created is an Airy's profile[47] and the central part of Airy's profile is cut using the iris aperture shown in the diagram above, giving us an approximate gaussian beam profile. The airy's beam profile is has the first minima close to zero near the focal length of the second collimating lens, so the placement of the iris aperture is done there.

This is the set-up for creating a Gaussian beam. First the beam is focused on a pinhole of size 25 μm and then it is collimated again using another lens. A variable iris aperture is finally used to obtain a clean Gaussian beam.

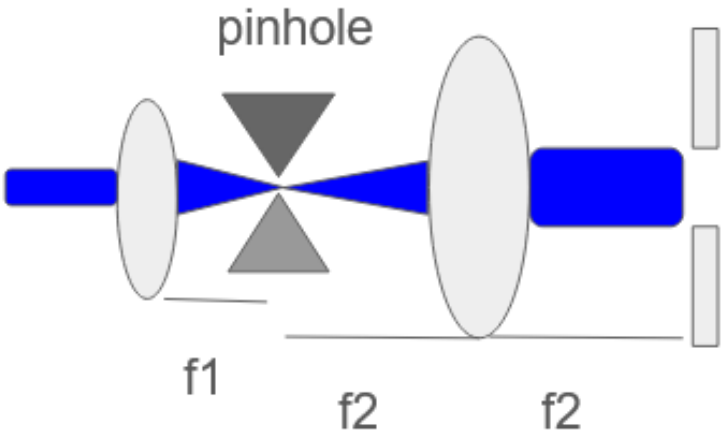


Figure 3.2: Set-up for Spatial filtering using 2 bi-convex lenses, a pinhole and an iris. The beam is focused by one lens on the pinhole and then collimated again using the other lens. Lastly the outer part is cut using the iris to form an Gaussian beam

The properties of the gaussian beam are [56]

$$Intensity : I(r) = I_0 e^{\frac{-2r^2}{w(z)^2}} \qquad Waist : w(z) = w_0\sqrt{1+(\frac{z}{z_R})^2}$$

We calculate the intensity profile of the beam using the CCD camera(Appendix) at different distances on the profile and then fit the above equation to calculate the waist of the gaussian beam. Afterwards we fit the waist with the distance giving the nature of the beam. This beam will act as the beam for creating the down converted photons.

Following the reference[57], we calculate the schimdt number of the beam being used as the pump on the crystal to quantify the efficiency of entangled photons generated[58]. When the schimdt number(K) is greater than 1 it signifies the entanglement[59]. For position it is calculated as,

$$K = (\frac{1}{b\sigma_k} + b\sigma_k)[57]$$

where b is the parameter of the crystal and σ_k is the inverse beam waist. Now, as discussed before we will be working with polarization degree of entanglement of the photons, if the photons gett entangled in the position-momentum basis, then we cant have 2-qubit entangled system, to avoid this schidmt number should be minimum that is only possible when b = $\frac{w_0}{2}$

In order to increase the intensity of the entangled photons, maximum intensity of the pump beam should be incident on the center of the crystal[54]. So we try to focus the maximum intensity of the pump using a biconvex lens. But non-intuitively, the maximum intensity of the beam is not at the focal length of the lens, it is ΔL distance away from the focal length[56]. When we use the lens, the beam waist at the distance L is calculated by

$$w_L = \frac{w_0}{z_R}(f^2 - 2(|s| - f)(L - f) + (\frac{L-f}{\alpha})^2)$$

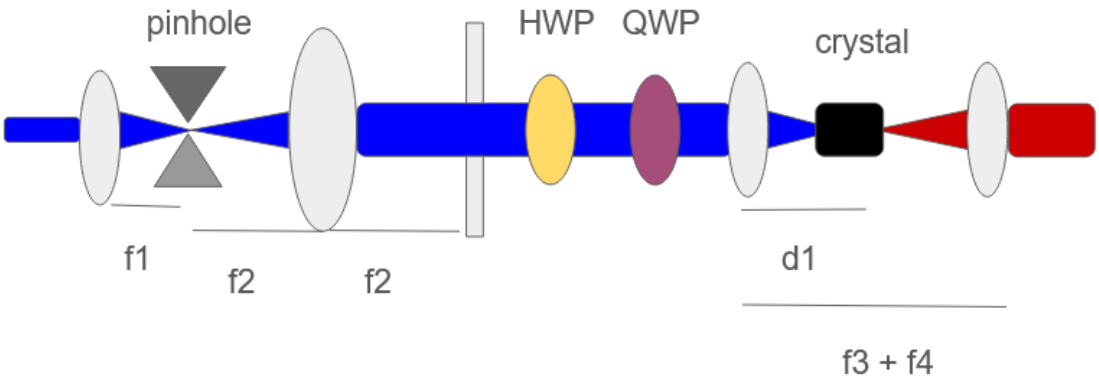


Figure 3.3: This figure shows the setup of optical random beam which was converted to Gaussian beam using the spatial filtering procedure as shown in Fig. 3.2 and then the Half Wave plate(HWP) and Quarter Wave Plate(QWP) are used to maximize the specific polarization of the light. Then using a lens the beam is focued onto the crystal to genrate the entangled photons

where s is the actual distance(L+ΔL) and α is the scaling of the beam. After differentiating the above equation with respect to the focal length(f), and imposing the maxima condition, we get,

$$\frac{dw_L(f)}{df} = 0 \quad at \quad \frac{1}{f} = (\frac{1}{L} + (|s| + \frac{z_R^2}{|s|})^{-1})$$

By simplifying these equations we get the adequate focal length and the distance of the crystal placement.

As seen in above figure, after we create a gaussian beam, we maximize the polarization using half wave plate and quarter wave plate, and then use one lens to pump maximum intensity on the crystal center and other to collimate the entangled photons beam.

3.2 Certification of Entanglement

3.2.1 Hong-Ou-Mandel Visibility

Hong-Ou-Mandel effect is observed in two-photon interference pattern, which states that *when two temporally coherent photons are identical in their properties and incident on 50:50 beam splitter the probability that both of them will be detected individually is zero[60].* Consider the following visual representation to understand this,

Here the case 2 and case 3 will cancel each other out due to the photons are identical and the phases are opposite leaving us with the outcome as case 1 and case 4.

Now, we have a entangled beam which is temporally coherent, and the state of the two-photons is $|\Psi\rangle = \frac{|(hv)\rangle + |vh\rangle}{\sqrt{2}}$. As they are not identical in nature, when the coincidences of them will be measure(discussed in section 2.3.5), they will be deteted with high coincidence rate.

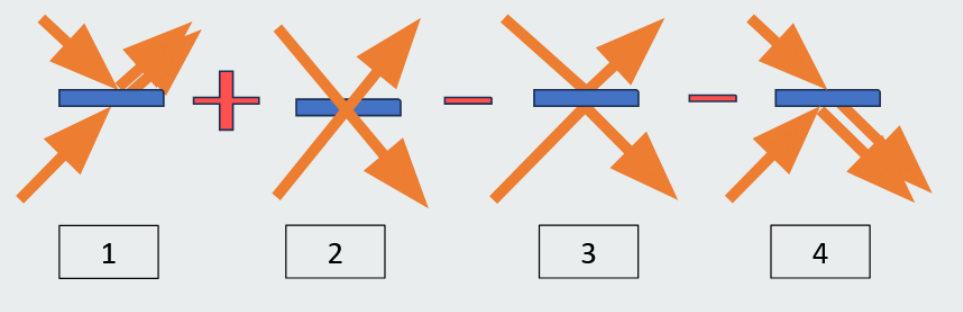


Figure 3.4: Four cases when the two identical photons are incident on the 50:50 beam splitter. The signs are accounted for the phase change in the path.

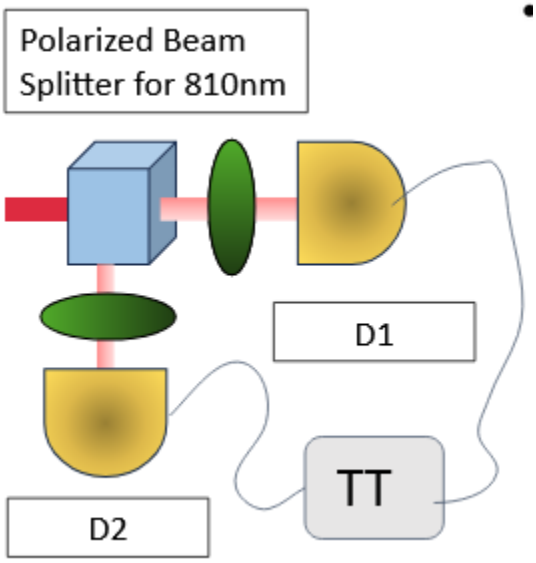


Figure 3.5: The figure shows the experimental setup for the measurement of the HOM-visibility. The beam of entangled photons is incident from the left side on a polarizing 50:50 beam splitter. It is then coupled with detector after incident on the Half wave plate which changes the polarization of the beam

But when we change the basis of measurement(discussed in section 2.3.2) by changing the half wave plate, the state is transformed to $|\Psi\rangle = \frac{|(hh)\rangle - |vv\rangle}{\sqrt{2}}$ which are now identical in nature. So, the coincidences in this case should be zero according to the Hong-Ou-Mandel effect.

This is the set-up for measuring the HOM counts. We incident the entangled photons beam created before on the BS and then change the measurement basis using the half wave plate and measure the coincidences in Z-basis(Both HWP at 0°) and X-basis(both HWP at 22.5°).

Then we calculate in visibility as $\frac{Coincidences\ \ in\ \ Z-basis\ \ -\ \ Coincidences\ \ in\ \ X-basis}{Coincidences\ \ in\ \ Z-basis\ \ +\ \ Coincidences\ \ in\ \ X-basis}$

We do this for different temperatures of the crystal and minimize the phase mismatch(section 3.1.1) and then select the adequate temperature.

3.2.2 S-Parameter

This is parameter calculated to certify the entangled photons are created[61].

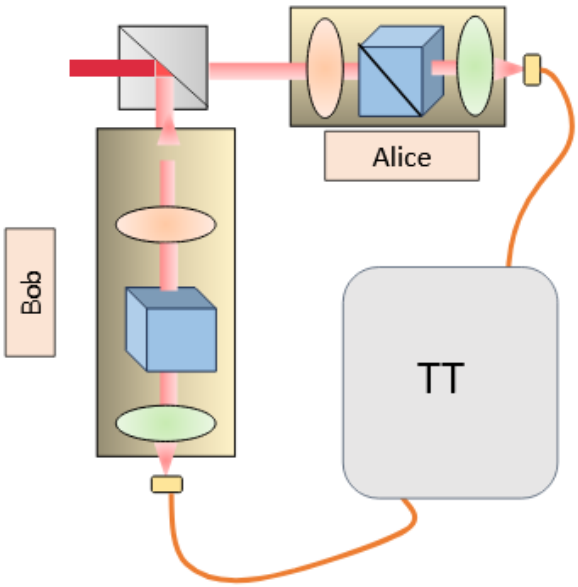


Figure 3.6: This figure shows the experimental setup for measurement of the S-parameter. The beam of entangled photons is incident from the left side on a polarizing 50:50 beam splitter and directed towards the two parties involved in the communication(Alice and Bob in this case). Then it is passed thorugh the quarter wave plate and half wave plate to ensure the required polarization of the beam

As, shown in the figure photons are incident on a 50:50 BS, and one part is transmitted to Alice and other to Bob, Then as done in the Bells inequality, here the measurement is done in four bases. The angles of the respective half wave plates are a = 0°, b = 22.5°, a' = 45° and b' = 67.5°. At each value of a and b number of coincidences is recorded in 4 categories $\{N_{++}, N_{+-}, N_{-+}, N_{--}\}$. And then the expectation at each combination is calculated as follows:

$$E = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{++} + N_{+-} + N_{-+} + N_{--}}$$

The S-parameter is then calculated as

$$S = E_{ab} - E_{ab'} + E_{a'b} + E_{a'b'}$$

3.3 Distribution of Entangled Photons

3.3.1 Mode-Matching

As, discussed in the introduction section, we cant transmit information to long distances using optical fibers. The reason it cant maintain the coherence for long distance inside the fiber due to leaking of mode inside the optical core, absorption by the media and bending of the signal during the transmission[62]. On the other hand, free-space communication maintains entanglement way more better when compared to optical fibers on large distances[15].

To be able to communicate/transmit the signal through the free space we need the to send the collimated beam(Appendix) and then the beam is needed to couple to the fiber in order to record the data. To be able to couple the optical signal to fiber, we need to establish mode-matching between the sender and the receiver. Mode matching is establishing adequate overlap of the phases between both the parties involved in the process. Consider the following illustration:

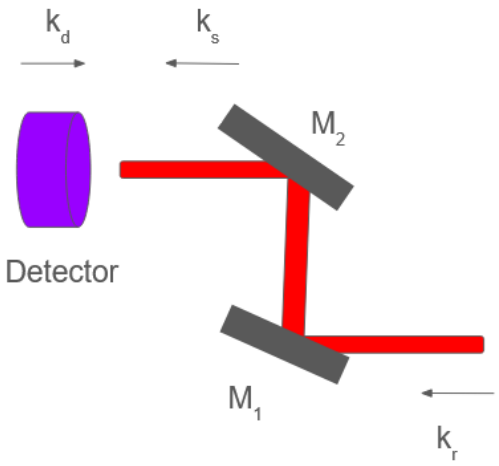


Figure 3.7: The procedure for the mode-matching. Here M1 and M2 are the mirrors with two degrees of freedom. This shows the typical set-up used in optical system to couple the light to the detector in order to record the data

Here, the k_r is any optical beam with random k-vector. M_1 and M_2 are the mirror with transverse and vertical degrees of freedom for moving the beam. k_s is the k-vector of the actual signal to be received by the detector and k_d is the k-vector of the detector. Now, for signal to be effectively detected by the detector, $k_s = k_d$ condition should be satisfied. This is the condition for the mode-matching. The algorithm for doing so is: Use M_1 to take the origin of k_s to same plane as the k_d and then use M_2 to align the propagation of the k_s. So, M_1 could be termed as *Coarse-alignment* and M_2 could be termed as the *Fine-alignment*.

3.3.2 Embedded systems and instrumentation

Before going to the final algorithm, I will explain about the control systems involved in tracking and there respective logic of feedback.

1. Servo motors: These are the stepper motors who have resolution of 360/4096 °. They can move in the speed off 1 steps/s to 500 steps/s.

   They will work as feedback to the Quadrant Photo Diodes(Appendix), to stabilize the laser beam on them. Algorithm:

   $$\text{Start QPD} \rightarrow \text{Check Beam Detection}$$

   $$\begin{cases} \text{Beam Detected} \rightarrow \text{Stop Servo Motor} \\ \text{No Beam Detected} \rightarrow \text{Spiral Scan Algorithm} \end{cases}$$

   Spiral Scan: $(Current\ Position + Step) \rightarrow (Current\ Position - Step) \rightarrow$ Increase Step $\rightarrow$ Repeat

2. Fast Steering mirror(fsm): This is a mirror which rotates in x-y direction reflecting the beam according. To start tracking with it, first the calibration of fsm needs to be done with the CCD detector on fixed length. The centering of the beam is dependent on the magnitude of it's center from the CCD's center and the direction(quadrant)

   So, we calculate the error function V = $\frac{1}{2}(e_x^2 + e_y^2)$

   $$\begin{pmatrix} \Delta FSM_x \\ \Delta FSM_y \end{pmatrix} = -\eta J \nabla_{fsm} V$$

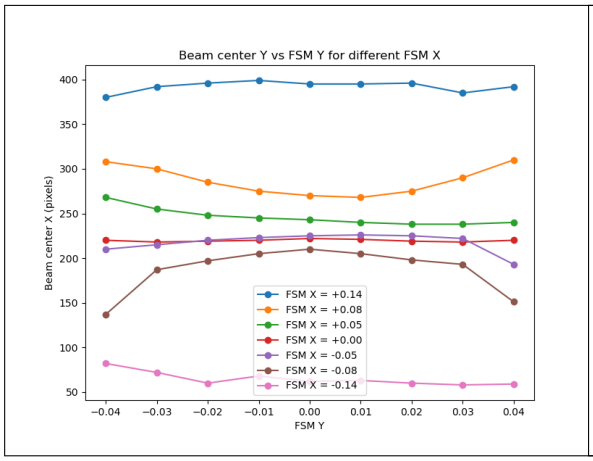


Figure 13: Data of FSM x-coordinate variation with beam center's y-coordinate

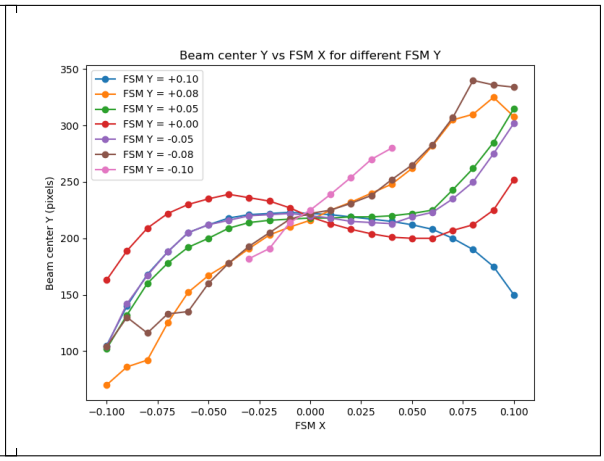


Figure 14: Data of FSM y-coordinate variation with beam center's y-coordinate

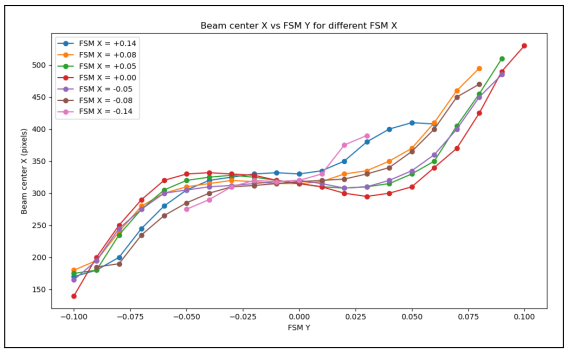


Figure 15: Data of FSM x-coordinate variation with beam center's x-coordinate

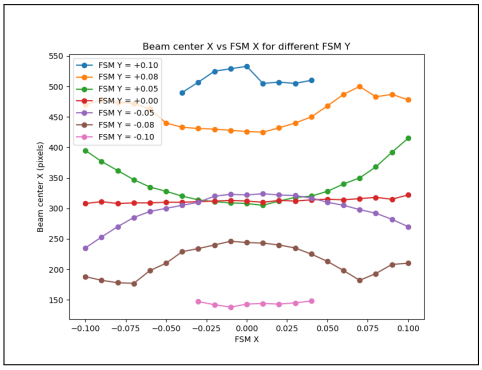


Figure 16: Data of FSM y-coordinate variation with beam center's x-coordinate

Using the above calibration data, we find a Jacobian [63] such that

$$\begin{pmatrix} \Delta FSM_x \\ \Delta FSM_y \end{pmatrix} = -KJ \begin{pmatrix} \Delta x_{pix} \\ \Delta y_{pix} \end{pmatrix}$$

where the J is the Jacobian $\begin{pmatrix} 50 & -1200 \\ 900 & 80 \end{pmatrix}$

Then it can deliver closed feedback with the same algorithm as before.

3. Motorized telescope Mount: This is a stepper motor with a maximum speed of $6^\circ/s$. The value given to control the motor using python code to drive it at maximum speed is $1000000(10^7)$.

   As, mentioned in the section of **Motivation**, we aim to do communication using the balloon. To track the balloon in turbulent environment, the feedback to this motor should be fast enough to track a fast moving object in air and stabilize an object at the center. For that to happen we have to map the center pixel to the minimum speed i.e. 10000 units and the corner pixels to the maximum speed i.e. 1000000 units and along with that it should not overshoot at any point. It can have 3 possibilities as the error function is monochromatic.

   From our data from field testing, we know that the quadratic function worked better.

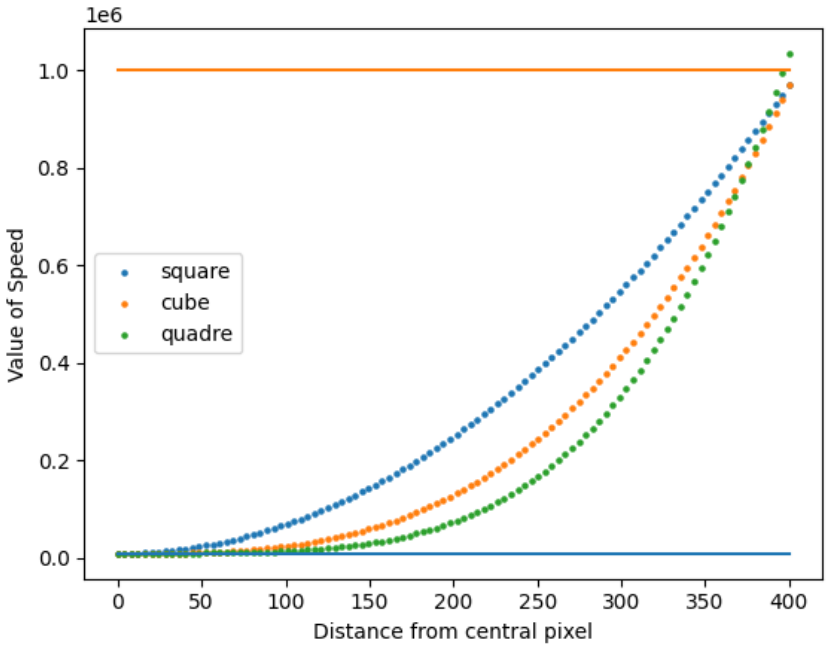


Figure 3.8: The three possible monotonic functions satisfying the boundary conditions of the speed for the motor control

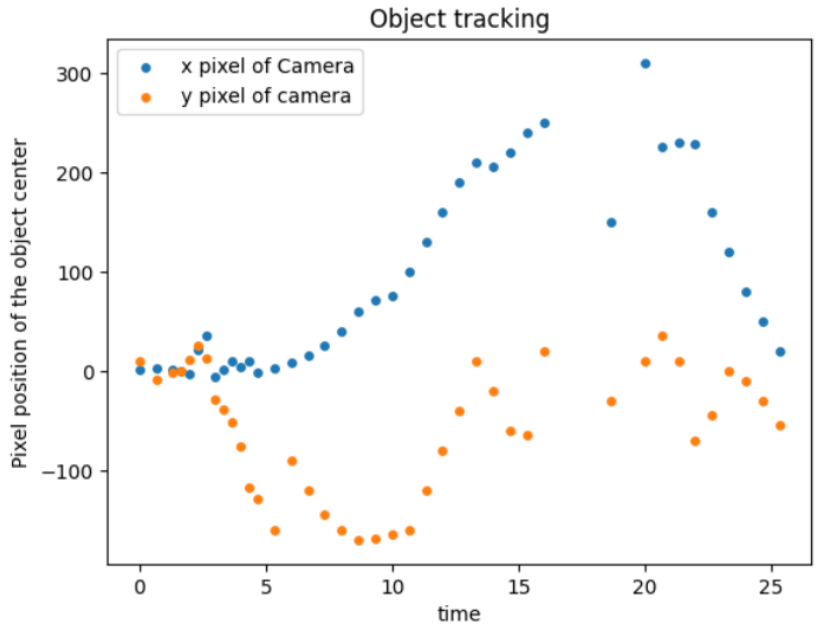
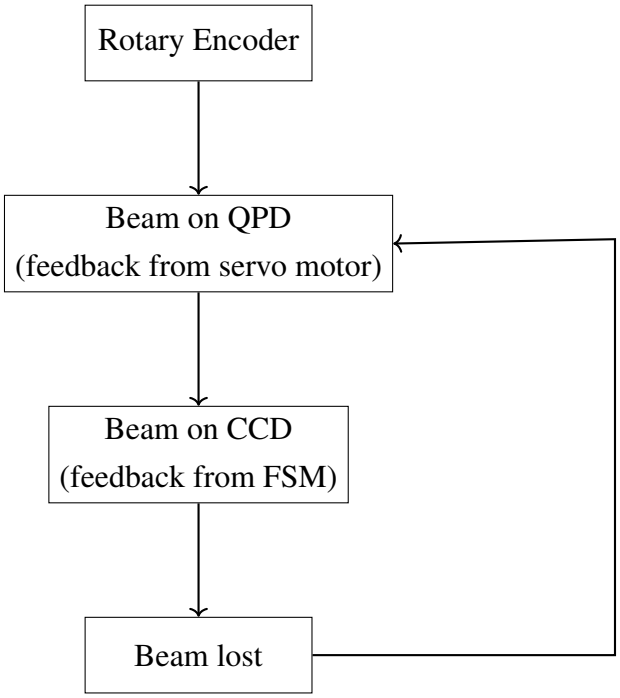


Figure 3.9: Data of the object tracking done over 100 m of length.

3.3.3 One-sided tracking

As discussed in the **Motivation** section, we focus on a tethered balloon configuration, where the balloon is connected to a rope to suppress rapid and large-amplitude motion. To achieve mode matching (see **Section 3.3.1**) under these conditions, the following control algorithm is implemented:



We focus here on the last two feedback loops. The experimental setup is shown in Fig. 3.10. The transmitted beam consists of a collinear combination of a beacon (guiding beam) and a quantum signal beam (carrying the information). A 532 nm beacon laser is combined with a red laser, which serves as a proxy since the actual entangled photons lie in the near-infrared region of the spectrum.

The combined beam is first incident on a mirror mounted on a servo motor, followed by a 50:50 beam splitter. One output path is directed to a quadrant photodiode (QPD), while the other is sent to a fast steering mirror (FSM). The QPD provides feedback to the servo motor, enabling coarse beam stabilization.

Subsequently, the beam is separated into its 610 nm and 532 nm components using a dichroic mirror (DM). The FSM performs fine correction by centering the beacon beam on a CCD using the previously described algorithm, thereby ensuring efficient coupling of the red beam into the collimator.

The coupled signal is detected using an avalanche photodiode (APD) (see Appendix). The system is tested under controlled conditions by introducing beam obstructions and inducing small oscillations in the setup, while recording the corresponding APD response.

In the event of beam loss, the servo motor initiates a spiral scanning mode to reacquire the signal. Once the beam is detected again on the QPD, normal tracking resumes using the

feedback algorithm described in **Section 3.2.2**.

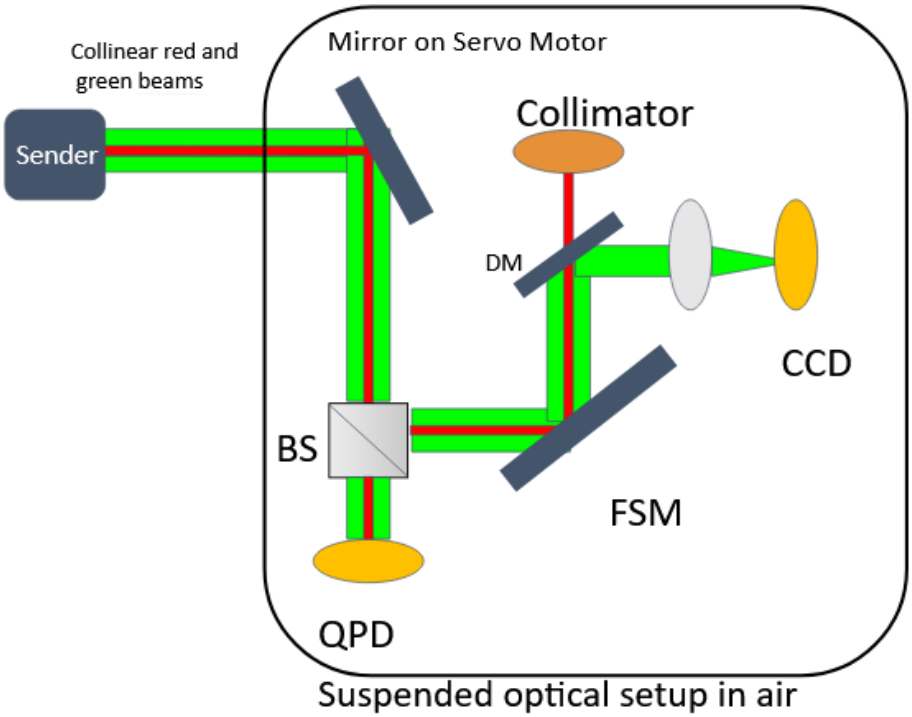


Figure 3.10: Schematic of the optical setup. A collinear red (610 nm) and green (532 nm) beam is transmitted from the source, where the green beam acts as a beacon for guiding and stabilizing the red beam used for coupling into the detector. DM denotes the dichroic mirror, which separates the two wavelengths. The mirror mounted on the servo motor and the fast steering mirror (FSM) correspond to coarse correction mirror and fine correction mirror, respectively; as in Fig. 3.7.

Chapter 4

Conclusion

4.1 Results

- **Gaussian Beam**: We first created an gaussian beam of waist 23 μm.

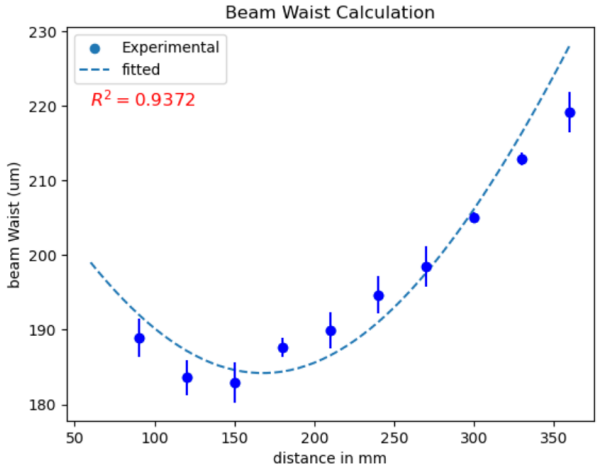


Figure 4.1: Gaussian beam profile vs the transverse position

- **Placement of the crystal:** As discussed in the **Section 3.1.3**, we need to get the beam waist as near to the schimdt number as possible(to avoid entanglement in position-momentum basis, and maximize the polarization entanglement) and the highest intensity of the beam should be focused on the center of the crystal. We used the bi-convex lens of the focal length 50mm and the point of highest intensity was found at 50.2$\pm$ 0.5 mm. So, we placed our crystal at that place to create high fraction of entangled photons. The intensity of the laser light 9.32 mW at the focal length of the mirror which corresponds to 10^10 photons/s. The down converted photons where in the order of 10^6.

- **Hong-Ou-Mandel Visibility:** We maximized the number of entangled photons and then changed the temperature of the crystal. The Fig. 4.2 shows the maximum HOM visibility reached at 36^{o}C which is 78.216%.

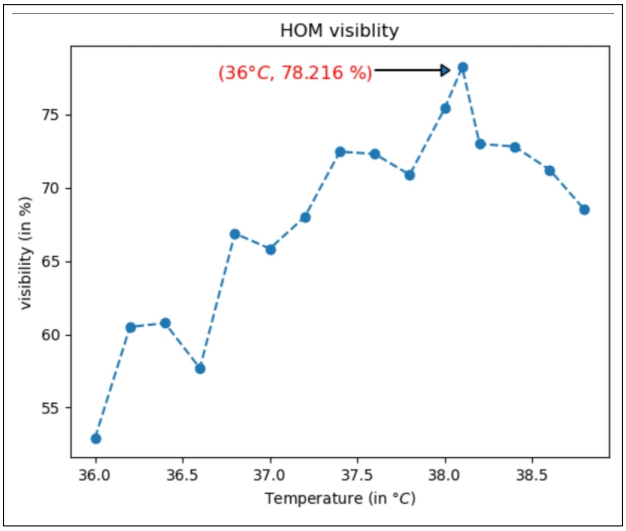


Figure 4.2: Variation of HOM visibility with change of the crystal temperature

- **S-parameter:** We measure the coincidences at the 16 different combinations of the Half wave plates as mentioned in **Section 3.2.2**

Angles (in °)	0.0	22.5	45.0	67.5
0.0	3615	271	2820	1175
22.5	411	3410	1249	2760
45.0	3068	941	3226	638
47.5	893	3015	816	3101

Table 4.1: Coincidences at different angles of the half-wave plates

According to the formula mentioned in **Section 3.2.2**, the Expectation values are:

$$E_{ab} = 0.8230, E_{a'b} = -0.5367, E_{ab'} = 0.3943, E_{a'b'} = 0.6263$$

$$S = E_{ab} - E_{ab'} + E_{a'b} + E_{a'b'} = 2.380$$

After repeating this experiments 3 more times, we calculate the S-parameter. The S-parameter was (2.380 ± 0.013).

This tells that our system has successfully generated the entangled photons.

- **Pointing System:** This system is designed for long-distance beam coupling. The setup and the algorithm described in **Section 3.3.3** were experimentally validated by monitoring the coupled signal using an APD. System robustness was assessed by manually blocking the beam at regular intervals to test autonomous reacquisition and recoupling. Additionally, controlled small-amplitude oscillations were introduced in the tethered configuration to emulate realistic environmental disturbances.

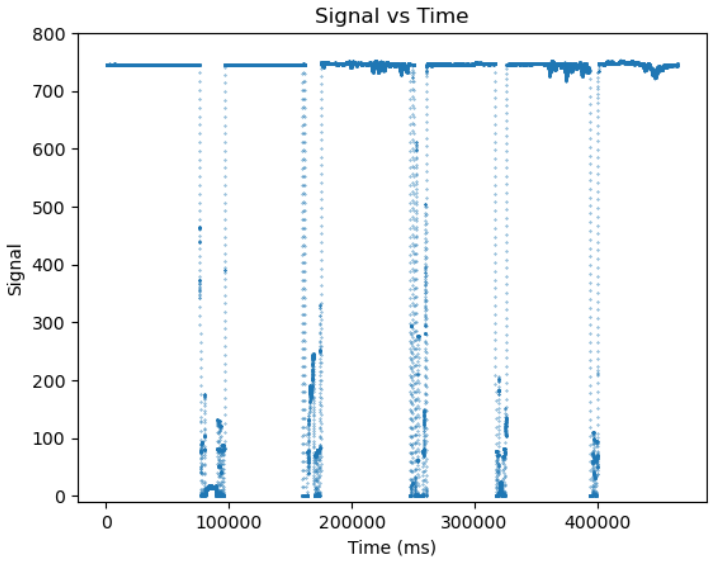


Figure 4.3: The power output of the APD proving the stable mode-matching. The dip shows the time when the beam was manually blocked and then the system automatically searched the beam in few seconds and then the coupling data is again recorded in the APD

4.2 Discussions

The air-to-ground quantum communication will be explored more in coming time. Along with the development in the free-space, quantum repeaters, quantum transduction using the NV centers interaction with the superconducting qubits and the robust engineering for the quantum internet and satellite communication. In my thesis I have explored the new avenue for the air-to-ground quantum communication to enable optical link on balloon to ground quantum communication and improving the key distribution time and making it more cost efficient.

To start with, we need to generate the entangled photons which are used in every protocol of the quantum key distribution. To create entangled photons we had used the down conversion method, where we have used the 405 nm laser and generated two 810 nm photons in bulk. To generate the entangled photons Then we tuned the temperature of the crystal and measured the HOM visibility (**Figure 9**), and find the suitable temperature where the entanglement was enhanced. Finally we calculate the S-parameter which was 2.38 ± 0.01 in our case which successfully violated the bell's inequality certifying the entanglement.

We introduced, step by step, the subsystems required for free-space beam mode matching. First, the QPD–servo motor loop was implemented, providing coarse feedback for beam alignment. Next, the fine feedback loop based on the FSM–CCD system and its associated control algorithm was developed. These subsystems were then integrated into a complete optical setup, along with a search-and-reacquisition algorithm for beam loss followed by stabilization.

The performance of the integrated system was evaluated using APD measurements, demonstrating reliable beam tracking and recoupling. These results indicate that, when deployed on a tethered balloon platform pointing toward a stable source, the system can establish and main-

tain a robust communication link.

4.3 Future Work

This system will work fine under controlled environment, but to sustain the turbulent environment the rotary encoder feedback should also come in play. This will ensure that the beam is always pointed towards the balloon and rest the coarse and fine feedback algorithm can handle. The system takes few seconds to search for beam again, we need to fasten this process in order to be able to send the sender in the free space where due to turbulent environment the beam will be changing it's position very fast as the slight movement will cause the beam to change drastically in the long range. We need to encode the beam with rotary encoder and the GPS pointing system which will be complimentary for that.

As shown in the **Section 3.3.2** Motorized telescope mount data, which is able to track the balloon in the turbulent environments, we need to send an beacon beam from the balloon for the both side-tracking. This will enable the tracking of balloon in the turbulent media taking us a step closer to efficient quantum key distribution methods in the coming age.

Appendix

1. **Collimation:**
   Diffraction is an wave property in which the waves reflect/bend when they are incident on edge or slit. Laser consists of EM-waves, so when travel through the free-space, they diffract and diverge out increasing the beam diameter and resulting in the loss of the optical data.

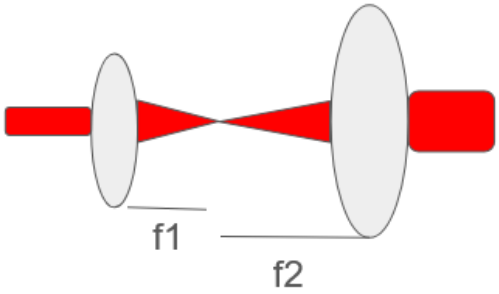


Figure 4.4: Collimation of an optical beam

   To tackle this issue, we use two biconvex lenses of focal length f1 & f2 and they are kept at a distance of (f1+f2) mm apart from each other. This ensures that the beam laser will remain parellel and the loss of the data is minimized.

2. **Detectors**

   - Charge Coupled Device(CCD): It is a device to detect photons. It very sensitive compared to normal camera. The detection is done on a silicon chip. When photons are incident on it, the corresponding area will be converted to intensity and then it is converted to electrical signal. Electrodes are attached above the CCD, when forward bias is applied, electrons are attracted and it causes to generate the electrical signal.
   - Avalanche Photo Diode(APD): Similar to CCD, but it is biased with high negative voltage. So, here the electrons are accelerated with high speed even when small amount of photons are detected.

- Single Photon Avalanche Detector(SPAD): The construction of SPAD's is same as APD, but here the negative bias is way high than the breakdown voltage. They are able to detect low intensity signals and detect the arrival time of photons with high temporal resolution.
- Quadrant Photo Diode(QPD): It is made by four InGaS semiconductor separated by small gaps. This allows high speed 2D positioning.

References

[1] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[2] Sushil Mujumdar, Vikas Bhat, and Rounak Chatterjee. A brief review of free-space quantum key distribution experiments towards satellite qkd. *Asian Journal of Physics*, 31(3–6):577–591, 2022.

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

[4] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[5] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[6] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 10th anniversary edition edition, 2010.

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

[8] Bryan C. Jacobs and James D. Franson. Quantum cryptography in free space. *Optics Letters*, 21(22):1854–1856, 1996.

[9] Karen J. Gordon, Veronica Fernandez, Paul D. Townsend, and Gerald S. Buller. A short wavelength gigahertz clocked fiber-optic quantum key distribution system. *IEEE Journal of Quantum Electronics*, 40(7):900–908, 2004.

[10] Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan. Micius quantum experiments in space. *Reviews of Modern Physics*, 90(3):035002, 2018.

[11] Hao-Ze Chen, Ming-Han Li, Yu Zhou Wang, Zhen-Geng Zhao, Cheng Ye, Fei Long Li, Zhu Chen, Sheng-Long Han, Bao Tang, Ya Jun Miao, and Wei Qi. Implementation of

carrier-grade quantum communication networks over 10000 km. *Nature*, 589:214–219, 2021.

[12] Nikolai Lauk, Neil Sinclair, Shabir Barzanjeh, Jacob P. Covey, Mark Saffman, Maria Spiropulu, and Christoph Simon. Perspectives on quantum transduction. *Quantum Science and Technology*, 5(2):020501, 2020.

[13] Chao Wang, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optics Express*, 23(25):32473–32481, 2015.

[14] A. A. Kalachev. Quantum repeaters: Current developments and prospects. *Bulletin of the Lebedev Physics Institute*, 50(Suppl. 12):S1312–S1329, 2023.

[15] Alessandro Fedrizzi, Rupert Ursin, Thomas Herbst, Matteo Nespoli, Robert Prevedel, Thomas Scheidl, Felix Tiefenbacher, Thomas Jennewein, and Anton Zeilinger. High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Physics*, 5:389–392, 2009.

[16] Morio Toyoshima. Comparison of free-space and fiber-based transmission systems for quantum cryptography. *Transactions of the Japan Society for Aeronautical and Space Sciences, Aerospace Technology Japan*, 7:Pj_7–Pj_12, 2009.

[17] Matteo Rosati and Albert Solana. Joint-detection learning for optical communication at the quantum limit. *Optica Quantum*, 2(6):390–396, 2024.

[18] Mustafa Gündoğan, Jasminder S. Sidhu, Markus Krutzik, and Daniel K. L. Oi. Time-delayed single satellite quantum repeater node for global quantum communications. *Physical Review Research*, 3(3):033167, 2021.

[19] IBM. What is cryptography? https://www.ibm.com/think/topics/cryptography, 2026.

[20] David Heath. One-time pad and perfect secrecy, n.d. Lecture notes, scribed by Nick Muskopf-Stone.

[21] Fernando Peralta Castro. The evolution of cryptography through number theory. *arXiv preprint*, 2024.

[22] Richard P. Feynman. Simulating physics with computers, 1981. Archived PDF from UC Berkeley.

[23] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Technical report, MIT Laboratory for Computer Science, 1977.

[24] L. et al. An efficient and high performance architecture design and implementation approach of cryptographic algorithm computation for authentication in modern wireless communication applications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(11):3206–3228, 2021.

[25] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[26] Luciano Floridi. *Information – A Very Short Introduction*. Oxford University Press, 2010.

[27] James Machta. Entropy, information, and computation. *American Journal of Physics*, 67(12):1074–1077, 1999.

[28] Daniel R. Lande. Development of the binary number system and the foundations of computer science. *The Mathematics Enthusiast*, 11(3):Article 6, 2014.

[29] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3–4):379–423, 623–656, 1948.

[30] Sheldon Goldstein, Joel L. Lebowitz, Roderich Tumulka, and Nino Zanghì. Gibbs and boltzmann entropy in classical and quantum mechanics, 2019. June 2, 2019.

[31] John Preskill. Quantum information, chapter 10: Quantum shannon theory, 2025. Lecture notes, California Institute of Technology, updated June 2025.

[32] P. A. M. Dirac. Development of the binary number system. Technical report, Karlsruhe Institute of Technology, 2014.

[33] Nivaldo A. Lemos. Are hilbert spaces unphysical? hardly, my dear! *arXiv preprint*, June 2025. Instituto de Física, Universidade Federal Fluminense, Niterói, Brazil.

[34] Eduard Prugovečki. *Quantum Mechanics in Hilbert Space*. Academic Press, New York, 2 edition, 1981. p. 215.

[35] David P. DiVincenzo. Topics in quantum computers, 1996. Bibcode: 1996cond.mat.12126D.

[36] Daniel A. Lidar. Lecture notes on the theory of open quantum systems, 2019. Version 2, revised February 2020.

[37] Martin B. Plenio and Shashank Virmani. An introduction to entanglement measures. *Quantum Information and Computation*, 7(1-2):1–51, 2007.

[38] Baris I. Erkmen and Jeffrey H. Shapiro. Ghost imaging: from quantum to classical to computational. *Advances in Optics and Photonics*, 2(4):405–450, 2010.

[39] Richard Jozsa and Noah Linden. On the role of entanglement in quantum computational speed-up. *Proceedings of the Royal Society A*, 459(2036):2011–2032, 2003.

[40] Leonard Susskind and Art Friedman. *Quantum Mechanics: The Theoretical Minimum*. Basic Books, New York, 2014.

[41] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.

[42] John S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195–200, 1964.

[43] G. C. Ghirardi, A. Rimini, and T. Weber. A general argument against superluminal transmission through the quantum mechanical measurement process. *Lettere al Nuovo Cimento*, 27(10):293–298, 1980.

[44] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, 2009.

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

[46] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68(5):557–559, 1992.

[47] Mark Fox. *Quantum Optics: An Introduction*. Oxford University Press, Oxford, 2006.

[48] P. A. Franken, A. E. Hill, C. W. Peters, and G. Weinreich. Generation of optical harmonics. *Physical Review Letters*, 7(4):118–119, 1961.

[49] A. Rice, Y. Jin, X. F. Ma, X. C. Zhang, D. Bliss, J. Larkin, and M. Alexander. Terahertz optical rectification from ¡110¿ zinc-blende crystals. *Applied Physics Letters*, 64(11):1324–1326, 1994.

[50] Richard A. Baumgartner and Robert L. Byer. Optical parametric amplification. *IEEE Journal of Quantum Electronics*, 15(6):432–444, 1979.

[51] Rüdiger Paschotta. Effective nonlinear coefficient. RP Photonics Encyclopedia. Accessed: 2026.

[52] Yilin Tang, Kabilan Sripathy, Hao Qin, Zhuoyuan Lu, Giovanni Guccione, Jiri Janousek, Yi Zhu, Md Mehedi Hasan, Yoshihiro Iwasa, Ping Koy Lam, and Yuerui Lu. Quasi-phase-matching enabled by van der waals stacking. *Nature Photonics*, 2024.

[53] Douglas W. Anthon and C. D. Crowder. Wavelength dependent phase matching in ktp. *Applied Physics Letters*, 16(5):186–188, 1970.

[54] Suman Karan, Shaurya Aarav, Homanga Bharadhwaj, Lavanya Taneja, Arinjoy De, Girish Kulkarni, Nilakantha Meher, and Anand K. Jha. Phase matching in β-barium borate crystals for spontaneous parametric down-conversion. *Journal of Optics*, 22:083501, 2020.

[55] Joseph W. Goodman. *Introduction to Fourier Optics*. Roberts and Company Publishers, Greenwood Village, CO, 3 edition, 2005.

[56] Edmund Optics. Gaussian beam propagation, 2024. Accessed: 15 Mar 2026.

[57] Vikas S. Bhat, Kiran Bajar, Rounak Chatterjee, and Sushil Mujumdar. Facile dual-shot measurement of schmidt number in type-0 and type-2 downconversion. *Physical Review Research*, 6:033151, 2024.

[58] C. K. Law and J. H. Eberly. Analysis and interpretation of high transverse entanglement in optical parametric down conversion. *Physical Review Letters*, 92(12):127903, 2004.

[59] J. Sperling and W. Vogel. The schmidt number as a universal entanglement measure. *Physica Scripta*, 83(4):045002, 2011.

[60] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044–2046, 1987.

[61] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[62] Tobias Rippchen, Ludovico Lami, Gerardo Adesso, and Mario Berta. Fundamental quality bound on optical quantum communication. *arXiv preprint arXiv:2510.07121*, 2025.

[63] George B. Arfken, Hans J. Weber, and Frank E. Harris. *Mathematical Methods for Physicists*. Elsevier, Amsterdam, 7th edition, 2012.