2
Fundamental Concepts of Quantum Communication

2.1 Introduction

Quantum information and computation is an amalgamation of information theory and coding, computer science and engineering, quantum mechanics, communication theory and electrical engineering, as shown in Fig. 2.1. It is pertinent to understand the fundamentals of these subjects in connection with quantum information science [DiVincenzo et al., 2000].

In classical information theory, classical systems are based on classical bits 1 or 0. In the parlance of electrical engineering, this corresponds to the switch being ON or OFF. On the other side, quantum systems are based on qubit representation which is described by two orthogonal basis states. From the mathematical point of view, the inner product for a qubit system gives $\langle\psi|\psi\rangle = 1$. These qubits follow the linear superposition principle : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, here $|\alpha|^2 + |\beta|^2 = 1$ and α and β are complex numbers.
Qubits are represented by vectors on a unit Bloch sphere, as shown in the Fig. 2.2. In this representation, states which are lying opposite on the Bloch sphere are orthogonal to each other [Avella et al., 2010]. Pure states are of unit length on the said Bloch sphere. In terms of polar coordinates, the qubit state has the following general representation

$$|\psi(\theta,\varphi)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \tag{2.1}$$

where $\varphi \in [0, 2\pi]$, $\theta \in [0, \pi]$.

In quantum communication applications, photons are used as flying qubits to achieve long distance communication. These photons are easy to transfer and can be encoded on different degrees of freedom [Cerf et al., 2002].

2.1.1 Photons as quantum information carriers

In cryptographic applications, the information carriers are first encoded for protection from any eavesdropping. In our discussions, we consider photons as information carriers. These serve as qubits in quantum information processing and weakly interact with the external environment. The photon is a massless particle with energy $E = \frac{hc}{\lambda}$, where λ is the wavelength, h is the Planck constant and c is the speed of light. Various methods such as frequency, time-bin, location, and polarisation are used to encode qubits onto photons. Here we use encoding only in polarisation basis, where $|0\rangle_L$ is encoded as horizontal polarisation $|H\rangle$ and $|1\rangle_L$ is encoded as vertical polarisation $|V\rangle$. Other forms are $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_L \pm |1\rangle_L)$ or in

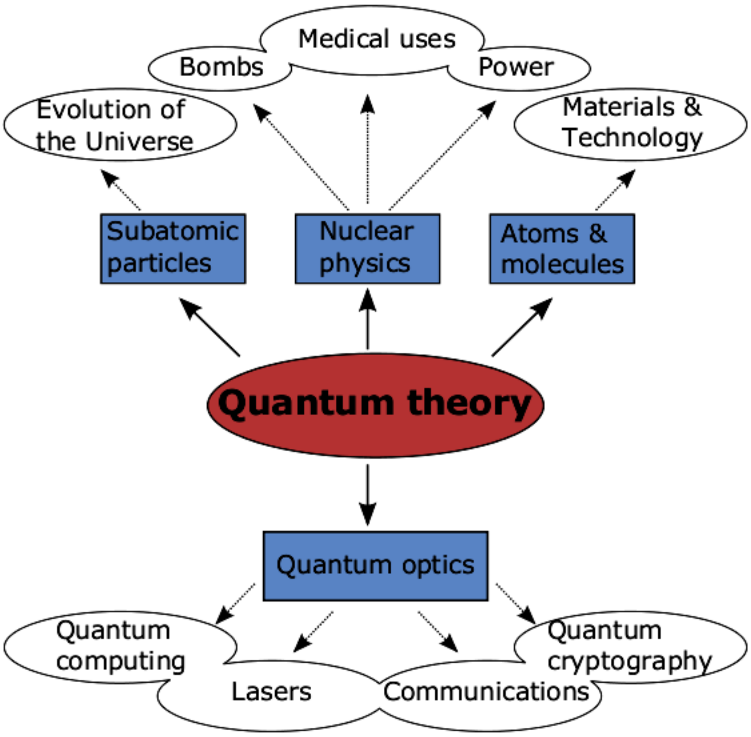

Figure 2.1: Various research areas born from Quantum theory. [Bacco et al., 2015].

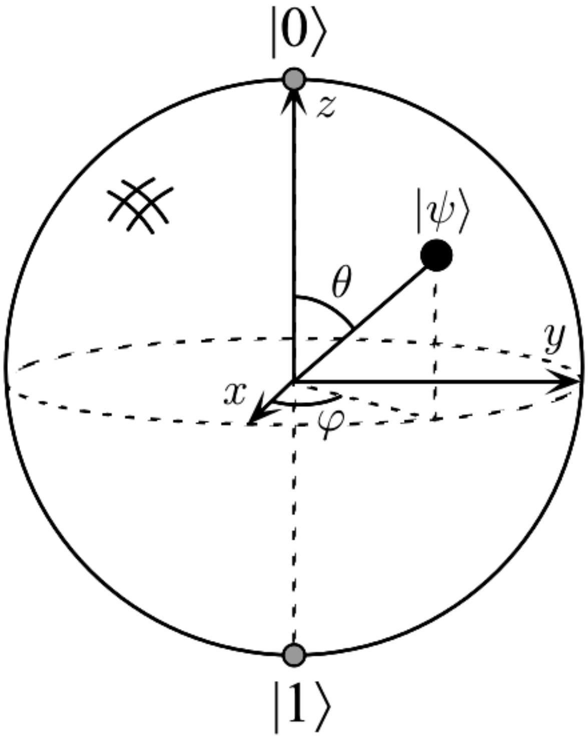

Figure 2.2: Bloch sphere representation of a qubit [Nielsen and Chuang, 2000].

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Figure 2.3: Pauli matrices used in quantum communication. [Nielsen and Chuang, 2002].

polarisation form , $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. The single and entangled qubits are implemented using quantum optics and other techniques like spontaneous parametric down-conversion [Klyshko, 1967].

2.1.2 The Pauli matrices

The Pauli matrices are used in many quantum communication operations. The mathematical form of these matrices, in the computational basis, is as shown in Fig. 2.3. The Pauli X gate corresponds to classical NOT gate and is also known as a bit-flip operator. The Pauli Z gate is a phase flip gate and Y gate performs both phase and bit-flip operations. The symbol I represents identity operation and does nothing when applied on any qubit.

2.1.3 Principles of Quantum Mechanics

The principles of quantum mechanics define how the qubits and operators interact with each other to bring about the operations related to quantum information and computation.

Postulate 1: State space of a System

The state of any quantum state lives in the Hilbert space [Dalla Chiara et al., 2013] and changes with time t. The quantum state $|\phi\rangle$ related to any quantum system provides information about that state. All the computations are performed by normalized states such that $\langle\psi|\psi\rangle = 1$. These normalized states are known as state vectors. The quantum state written in the form of $|\phi\rangle = a|0\rangle + b|1\rangle$ is in state vector form in a complex plane which is two-dimensional and its normalization is unity: $|a|^2 + |b|^2 = 1$.

Postulate 2: Observable Physical Quantities Represented by Operators

For every dynamical variable P which is a measurable quantity, a corresponding operator P exists. This operator P is a Hermitian operator and its corresponding eigenvectors make a full orthonormal basis of that vector space.

Postulate 3: Measurement

The measurement outcomes of any dynamical variable B are the eigenvalues b_n of the operator B associated to that dynamical variable. This operator B can be written in terms of its eigenvalue and the associated projection operators $P_n = |u_n\rangle\langle u_n|$ as $B = \sum_n b_n P_n$.

The probability of measurement outcome b_n is written as

$$Pr(b_n) = \frac{|\langle u_n|\phi\rangle|^2}{\langle\phi|\phi\rangle} = \frac{|c_n|^2}{\langle\phi|\phi\rangle}, \tag{2.2}$$

here $c_n = \langle u_n|\phi\rangle$. For normalized state, $\langle\phi|\phi\rangle = 1$. According to measurement principle, it is the measurement outcome which collapses the wavefunction, that is, the system collapses into the state $|u_n\rangle$. The state of the system after measurement can be represented as

$$|\phi\rangle \xrightarrow{measurement} \frac{P_n|\phi\rangle}{\sqrt{\langle\phi|P_n|\phi\rangle}}. \tag{2.3}$$

Postulate 4: State Evolution

The Schrӧdinger equation for a closed quantum system is written as

$$i\hbar\frac{\delta}{\delta t}|\phi\rangle = H|\phi\rangle, \tag{2.4}$$

here H is the Hamiltonian operator which is nothing but the total energy associated with the quantum system. After any time instant t, the state of the system, assuming time independent Hamiltonian, is given by

$$|\phi(t)\rangle = e^{-iHt/\hbar}|\phi(0)\rangle. \tag{2.5}$$

Thus, the time evolution of any quantum system can be represented by the unitary operator U

$$U = e^{-iHt/\hbar}, \tag{2.6}$$

where H is the Hamiltonian operator of the system.

2.1.4 Quantum Measurement

Measurement of classical bits is quite different from that of qubits. The result and process of measurement are different in both bits and qubits. The output of classical bit gives either ‘0’ or ‘1’.

Any quantum state $|\phi_i\rangle$ when measured is projected onto subspace $|k\rangle\langle k|$. The probability of the projection onto $|k\rangle$ is given by

$$p = |\langle k|\phi_i\rangle|^2. \tag{2.7}$$

From above equation it is clear that the measurement result depends on the selected basis. Suppose the state to be measured in the basis $\{|0\rangle, |1\rangle\}$ is $|\phi\rangle = |0\rangle$, then it gets

projected onto $|0\rangle$ with probability 1. But, if we measure the same state in the basis $|+\rangle$, $|-\rangle$, projection onto the state $|+\rangle$ takes place with the probability $p = |\frac{1}{\sqrt{2}}|^2$. Hence $|0\rangle$ can be represented in terms of the basis states $\{|+\rangle, |-\rangle\}$ as $|0\rangle = \begin{pmatrix} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \end{pmatrix}$. After measurement a new quantum state is obtained.
Quantum measurement helps in detecting Eve in quantum cryptography applications as it is impossible for any eavesdropper to perform measurement on any single qubit for extracting information without disturbing the quantum state. Hence, measuring a single qubit on two different bases simultaneously is impossible.

2.1.5 Kraus Operators

In order to investigate the operation of a quantum channel on any quantum state, we use Kraus operator formalism [Kraus, 1983]. In general, quantum systems interact with their external environment, making the dynamics *open*. From the perspective of practical applications, we need to study the evolution of the open quantum systems. Interaction with the environment introduces noise into the system dynamics, resulting in errors and making the system mixed. For performing error-free quantum communication, it is essential to apply error correction methods. The study of open system effects on various facets of quantum communication is an integral part of this thesis. Kraus operators are an important tool in the use of open system ideas to quantum communication.

Power of quantum computation is based on the linear superposition of quantum states. Due to interaction with the external environment, this superposition is destroyed. This phenomenon is known as decoherence, in which a pure state becomes mixed.

Let us consider the dynamical evolution of a quantum system of interest, taking into account its interaction with the external environment. Let ρ be the density operator of the system and $\Phi(\rho)$ is a dynamical map. The density operator ρ evolves to another density operator $\rho^{'}$ as

$$\rho^{'} = \Phi(\rho). \tag{2.8}$$

The time evolution for any closed quantum system is governed by a unitary operator U and is

$$\Phi(\rho) = U\rho U^{\dagger}. \tag{2.9}$$

For open systems, the above relation is generalized to

$$\Phi(\rho) = \sum_{n=1}^{N} A_n \rho A_n^{\dagger}. \tag{2.10}$$

This is known as the operator-sum representation. Any operation expressed in this form is guaranteed to be completely positive. Here A_n, known as the Kraus operators, must satisfy the completeness relation

$$\sum_{n=1}^{N} A_n A_n^{\dagger} = I. \tag{2.11}$$

Further, the operation elements must be trace-preserving, that is, $\sum_{n=1}^{N} A_n A_n^{\dagger} = I$. For non-trace preserving elements, $\sum_{n=1}^{N} A_n A_n^{\dagger} < I$.

To obtain the operator-sum representation for any quantum system, the first task is to find out the A_n. Consider the following dynamical map

$$\Phi\Big(\rho\Big) = Tr_E\Bigg(U\Big(\rho\otimes\sigma\Big)U^\dagger\Bigg). \tag{2.12}$$

Here ρ is the density operator for the principal quantum system and σ denotes the density operator for the environment.

Let us assume that the basis states of the environment are $\{|b_n\rangle\}$ and the initial state of the environment is written as $\sigma = |b_0\rangle\langle b_0|$. The above equation can be written as

$$\begin{aligned}
\Phi(\rho) &= Tr_E\Bigg(U\Big(\rho\otimes\sigma\Big)U^\dagger\Bigg), && (2.13)\\
&= \Sigma_n\langle b_n|\Bigg(U\rho\otimes\sigma U^\dagger\Bigg)|b_n\rangle, && (2.14)\\
&= \Sigma_n\langle b_n|\Bigg(U\rho\otimes|b_0\rangle\langle b_0|U^\dagger\Bigg)|b_n\rangle, && (2.15)\\
&= \Sigma_n\langle b_n|U|b_0\rangle\rho\langle b_0|U^\dagger|b_n\rangle. && (2.16)
\end{aligned}$$

Comparing with equation 2.10, we can write the Kraus operators A_n as

$$A_n = \langle b_n|U|b_0\rangle. \tag{2.17}$$

The detailed description of different noisy models are given in Section 4.2 .

2.1.6 Entanglement

Entanglement plays an important role in quantum communication, not present in classical communication. Consider two independent qubits C and D, whose state is

$$|\phi_C\rangle\otimes|\phi_D\rangle \equiv |\phi_C\phi_D\rangle. \tag{2.18}$$

This is a separable state, also known as a product state. Further,

$$\begin{aligned}
|\phi_C\phi_D\rangle &= \Bigg(a|0_C\rangle + b|1_D\rangle\Bigg)\otimes\Bigg(a^{'}|0_D\rangle + b^{'}|1_D\rangle\Bigg), && (2.19)\\
&= R|0_C0_D\rangle + S|0_C1_D\rangle + T|1_C0_D\rangle + U|1_C1_D\rangle. && (2.20)
\end{aligned}$$

Here the coefficients R, S, T and U are written as $aa^{'}$, $ab^{'}$, $ba^{'}$ and $bb^{'}$, respectively. The states $|0_C0_D\rangle$, $|0_C1_D\rangle$, $|1_C0_D\rangle$ and $|1_C1_D\rangle$ form the basis for two qubit states.

Entangled states are those states which cannot be written as the product state of their individual states. For example,

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\Bigg(|0_C0_D\rangle + |1_C1_D\rangle\Bigg). \tag{2.21}$$

When we measure the first qubit in above state, the value obtained is correlated with the outcome of the measurement performed on the second qubit. The important point to be noted here is that the result of the first measurement is quite random, but the result of the second measurement is always correlated. For example, if the first qubit is measured in $\{|0\rangle, |1\rangle\}$ basis, the result after measurement can be $|1\rangle$ or $|0\rangle$ with the probability $\frac{1}{2}$. After measurement, we find that the second qubit is correlated with the first qubit. Some of the two-qubit entangled states are

$$
\begin{aligned}
|\psi^{+}\rangle &= \frac{1}{\sqrt{2}}\Bigg(|00\rangle + |11\rangle\Bigg), \qquad (2.22)\\
|\psi^{-}\rangle &= \frac{1}{\sqrt{2}}\Bigg(|00\rangle - |11\rangle\Bigg),\\
|\phi^{+}\rangle &= \frac{1}{\sqrt{2}}\Bigg(|01\rangle + |10\rangle\Bigg),\\
|\phi^{-}\rangle &= \frac{1}{\sqrt{2}}\Bigg(|01\rangle - |10\rangle\Bigg),
\end{aligned}
$$

also called the Bell states.

2.1.7 CHSH inequality

The quantitative aspect of Bell's theorem is brought out by the Clauser-Horne-Shimony-Holt (CHSH) inequality, whose violation is an indication that the theory cannot be expressed in terms of local hidden variables [Clauser et al., 1969]. The CHSH inequality is

$$-2 \leq E(a,b) - E(a,b^{'}) + E(a^{'},b) + E(a^{'},b^{'}) \leq 2,$$

here a and $a^{'}$ denote the detector settings on side A and b, $b^{'}$ on side B. These four combinations are tested in separate subexperiments. $E(a,b)$ denotes quantum correlations of the particle pairs, where by quantum correlation we mean the expectation value of the product of the experimental outcomes, that is, the statistical average of $A(a).B(b)$, where A and B are separate outcomes using the coding 1 for the '$+'$ channel and -1 for the '$-'$ channel.

According to quantum mechanics, the maximum value of S is $2\sqrt{2}$, which is more than 2. Hence, CHSH violations are anticipated by quantum mechanics. In Fig. 2.4, S is the source which produces pairs of photons. After detection, these are stored in coincidence monitor CM. Here, light is preferred in place of electrons to perform Bell test. The coincidences or the simultaneous detections are stored, the outcomes being categorized as '- -', '+-', '++' or '-+' and corresponding counts accumulated. Here, four subexperiments are performed seprately, corresponding to four terms $E(a,b)$ as mentioned above in (2). We chose 0°, 45°, 22.5° and 67.5° values for a, $a^{'}$, b, $b^{'}$ respectively. These are Bell-test angles for which the violation of the inequality is greatest.

For a given value of a and b, the number of coincidences $(N_{++}, N_{--}, N_{-+}, N_{+-})$ are stored. Further, $E(a,b)$ is calculated as

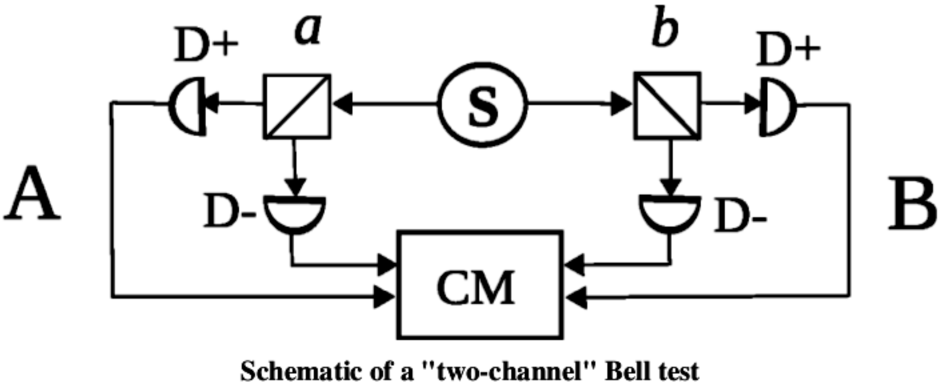

Figure 2.4: Experimental setup for two-channel Bell test [Aspect et al., 1982].

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

First, all the E's are estimated, then an appropriate experimental estimation of CHSH can be obtained.

Some of the important features of the Bell states are: a) These are the quantum states which exhibit quantum correlations. These quantum correlations are the foundation for generating secret keys between the authenticated users, as explained in [Ekert, 1991]. b) These states form the basis for any two-qubit quantum states.

2.1.8 The no-cloning theorem

Security of quantum key distribution (QKD) protocols is based on no-cloning theorem. According to no-cloning theorem, any unknown quantum state cannot be perfectly cloned [Dieks, 1982; Wootters and Zurek, 1982]. On the other side, in classical information theory, any classical information can be copied many times without any penalty. This is described as follows [Nielsen and Chuang, 2000]:

Suppose Eve has a quantum cloner with U as unitary operator. She tries to copy an unknown quantum state $|\psi\rangle$ to an ancilla qubit $|y\rangle$: $U|\psi\rangle \otimes |y\rangle = |\psi\rangle \otimes |\psi\rangle$. Eve also tries to use her quantum cloner to copy another state $|\phi\rangle : U|\phi\rangle \otimes |y\rangle = |\phi\rangle \otimes |\phi\rangle$. Now performing inner product of these two equations

$$\Bigg(\langle\phi| \otimes \langle y|U^\dagger\Bigg)\Bigg(U|\psi\rangle \otimes |y\rangle\Bigg) = \Bigg(\langle\phi| \otimes \langle\phi|\Bigg)\Bigg(|\psi\rangle \otimes |\psi\rangle\Bigg), \tag{2.23}$$

$$\langle\phi|\psi\rangle\langle y|y\rangle = \langle\phi|\psi\rangle\langle\phi|\psi\rangle, \tag{2.24}$$

$$\langle\phi|\psi\rangle = \Bigg(\langle\phi|\psi\rangle\Bigg)^2. \tag{2.25}$$

Solution to the above equation gives two answers either $\langle\phi|\psi\rangle = 0$ or $\langle\phi|\psi\rangle = 1$ which means that either both the quantum states must be same or orthogonal [Avella et al., 2010]. This proves that there is no perfect quantum cloner which can copy any arbitrary quantum state. Hence, no-cloning theorem with quantum measurements upholds the security of quantum cryptography.

2.1.9 Shannon entropy

The foundations of modern information theory could be said to be laid down by Claude Shannon in 1948 [Shannon, 1948; Liang et al., 2009]. He defined how we can mathematically define, encrypt and measure information under noisy channels ? The proposed theory includes many important applications in secure communication, one of the important aspects of quantum key distribution (QKD).

Shannon defined entropy as a measure of information and represent the measurement outcome in terms of bits. A bit is the unit of classical information and defined as the mean of the information while tossing a fair coin. Random variables are generally used to represent the information. A discrete random variable is a finite set of elements y that captures values from the set Y. Here $p\big(Y = y\big) \equiv p\big(y\big)$. Every element $p(y)$ of the probability distribution fulfills the criteria $p\big(y\big) \geq 0 \; \forall y$ and $\sum_y p\big(y\big) = 1$. In tossing a coin the outcomes can be $Y = \{tails, heads\}$ and probability outcomes are $p\big(tails\big) = p\big(heads\big) = \frac{1}{2}$. In general, the nature of the information is additive which means information received from two independent random variables is equal to the sum of the information received from each random variable. In case of non-uniform sources, the received total information is not equal to the sum of the individual sources. From outcome y, the received information is $-\; log_2 p\big(y\big)$. According to Shannon, the entropy is defined as

$$h(Y) = -\sum_j p\Big(y_j\Big)\Big(log_2 p(y_j)\Big). \tag{2.26}$$

If $p = 0, 1$ then $h(Y) = 0$ bits, if $p = 1/2$ then $h(Y) = 1$ bit. Entropy is used to model information sources with the help of random variables. In such a scenario, the outcomes are related to some probability distribution. If the information source outcomes are nonuniform in $1s$ and $0s$, the messages being sent can be represented in comparatively shorter length without the loss of information. According to Shannons channel coding, the entropy $h(Y)$ is a measure of the maximum compression of any random variable Y.

In the QKD applications, the joint entropy $h(Y, Z)$ is used to analyze the relationship between the random variables Y and Z with a joint probability distribution $p(y, z)$. The joint entropy is calculated as

$$h(Y, Z) = -\sum_y \sum_z p\big(y, z\big) log\Big(p\big(y, z\big)\Big). \tag{2.27}$$

The conditional entropy is defined to measure the uncertainty in Y, provided that we know Z, considering all possible realizations of Z. We can write conditional entropy as

$$\begin{aligned} h(Y|Z) &= -\sum_{y} p(y)h\Big(Z|Y\Big), && (2.28)\\ &= -\sum_{y} p(y)\sum_{z} p(z|y)log\Big(p(z|y)\Big), && (2.29)\\ &= -\sum_{y}\sum_{z} p(y,z)log\Big(p(z|y)\Big). && (2.30) \end{aligned}$$

A binary symmetrical channel is defined in terms of conditional entropy function where input and output values are taken from the set $\{0,1\}$. Any noisy channel can be modeled with these properties.

Now we describe mutual information shared between the communicating parties which is helpful to judge the quality of the communication channel being used. Let Y and Z are related to the joint probability distribution $p(y,z)$. The information that Z gives about Y is:

$$I(Y:Z) = h\Big(Y\Big) - h\Big(Y|Z\Big). \qquad (2.31)$$

In case of $I\Big(Y:Z\Big) > 0$, measuring one variable provides the information about the other variable and hence they are partially correlated. In the same context, $I\Big(Z:Y\Big) = h\Big(Z\Big) - h\Big(Z|Y\Big)$ tells us how much information the variable Y provides about Z. It is mutual information which reduces the uncertainty about Y that results from learning the values of Z or vice versa, the average amount of information that Y gives about Z. If Y and Z are independent then $h\Big(Y|Z\Big) = h\Big(Y\Big)$ and $I\Big(Y:Z\Big) = 0$. This implies that Z does not provide any information about Y. From the above, communication is possible over noisy channels with the help of error correction schemes. The amount of extra information for error correction is $h(Z|Y)$.

All the concepts described so far are useful for quantum cryptographic protocols. In the following chapters, we will elaborate how the quantum properties enhance the computational speed and at the same time provide unconditional security.

2.2 Quantum cryptography

2.2.1 BB84 QKD protocol

Quantum cryptography, especially quantum key distribution (QKD) [Gerhardt et al., 2010], is the first technical demonstration in the field of quantum secure communication and free from any computational assumptions. In quantum cryptography, the basic concept behind the randomly chosen basis is that their measurement operators should be non-commuting so that any eavesdropper cannot reveal full information about the information being shared among the legitimate users. For initiating communication process, photons are

Basis	State	Linear polarisation	Bit value
Z	$\vert H\rangle$	0^o	0
	$\vert V\rangle$	90^o	1
X	$\vert D\rangle = \frac{1}{2}(\vert H\rangle + \vert V\rangle)$	45^o	0
	$\vert A\rangle = \frac{1}{2}(\vert H\rangle - \vert V\rangle)$	-45^o	1
Y	$\vert R\rangle = \frac{1}{2}(\vert H\rangle + i\vert V\rangle)$	–	0
	$\vert L\rangle = \frac{1}{2}(\vert H\rangle - i\vert V\rangle)$	–	1

Table 2.1: BB84 QKD protocol [Mélen, 2016].

prepared in two random polarization bases like H/V and $+/-$: suppose a photon is prepared in horizontal base $|H\rangle$, then measured in other base say $+/-$; it will provide outcome with equal probability and finally it will be in either $|-\rangle$ or $|+\rangle$ eigenstate. Hence, it leaves no loophole for stealing full information about the quantum states or single photons. The no-cloning theorem described above prevents any eavesdropper from extracting any useful information by doing repeated measurements [Dieks, 1982; Wootters and Zurek, 1982]. If eavesdropping is below a predefined threshold level, the protocol continues and finally a secure key is shared, known as Vernam cipher or one-time pad [Vernam, 1926]. The detailed analysis of QKD protocols will be described in coming chapters.

The BB84 protocol is easy to implement experimentally and its fundamentals and notations can be further extended to other protocols. The BB84 protocol is based on prepare and measure scheme, where the sender known as Alice, prepares the single qubit quantum states as the information carrier and transfers to the receiver, known as Bob, via a quantum channel. This quantum channel can be a free space or an optical fiber. Here the encoding is done on the polarization basis of single photons, hence, a discrete variable encoding protocol. The complete procedure is described as

1. The authenticated users Alice and Bob communicate by diagonal and rectilinear bases, $X = \{|D\rangle, |A\rangle\}$ and $Z = \{|H\rangle, |V\rangle\}$, respectively and the coding procedure, as shown in Table 2.1

2. Out of the four bases, Alice randomly selects a basis and a bit value. Based on these values, she prepares a single photon and transmits it to Bob through a secure quantum channel which is generally a polarization preserving channel. On the receiver side, Bob obtains the correct bit values when the detection and preparation bases match. This is one of the important steps of BB84 protocol which is repeated until all the bits have been exchanged.

3. Next, the authenticated users Alice and Bob perform post-processing operations which gives classical results. Here, Bob announces the detection events over a public channel and discards the bits which are lost during transmission. Alice and Bob agree on similar events, which results in a binary bit string known as a raw key.

Alice	Basis	Z	Z	X	Z	X	X
	Prepared state	$\|H\rangle$	$\|V\rangle$	$\|A\rangle$	$\|H\rangle$	$\|A\rangle$	$\|D\rangle$
Eve	Basis	X	X	Z	Z	X	Z
	Detected state	$\|D\rangle$	$\|A\rangle$	$\|H\rangle$	$\|H\rangle$	$\|A\rangle$	$\|V\rangle$
Bob	Basis	Z	X	X	Z	Z	X
	Detected state	$\|H\rangle$	$\|A\rangle$	$\|D\rangle$	$\|H\rangle$	$\|D\rangle$	$\|H\rangle$
	Sifted key	0		1	0		0

Table 2.2: Security of the BB84 QKD protocol under intercept-resend attack. [Mélen, 2016].

4. In the sifting procedure, Bob announces the basis he used for corresponding detected photons without disclosing the outcomes. Alice tells those time instances in which the same basis coincides. Both the legitimate users remove those bits which are undetected (around 50 %) and finally obtain the sifted key. This procedure is also known as reconciliation.

In the ideal case, the sifted keys must be identical on both sides. It is the case when there is no eavesdropping inbetween the line. In intercept-resend attack, Eve tries to obtain meaningful information by attacking the communication channel. In this attempt, she does not know what basis should be used for measurement. She introduces errors in her eavesdropping attempts. Quantum bit error ratio (QBER) δ is a parameter to detect Eves presence. From the data shown in the Table 2.2, in the finally obtained sifted key, the QBER can be seen to be $\frac{4}{6}$, which is not acceptable and communication halts immediately. In general, Eve introduces 25 % QBER and selects the correct basis 50 % times.

Many bits get corrupt in the communication process because of noise present in the environment, imperfections in the experimental set-up or because of Eves presence. All these generate quantum bit error which is eliminated by error correction methods such as CASCADE protocol [Brassard and Salvail, 1993; ?]. The CASCADE protocol performs a binary search with the help of parity bit checks for various number of block sizes. Winnow protocol [Buttler et al., 2003] exchanges less amount of information over the classical channel for performing the error correction in lesser time and is based on Hamming codes. This approach is more advanced and efficient for different error rates as compared to Low-Density Parity Codes (LDPC).

Once it is confirmed that quantum bit error ratio is below the secure threshold value and protocol is secure, then quantum key distribution protocol halts and error correction techniques are applied to get the error free secure key. The following binary entropy function is used to calculate the discarded bits for error correction

$$H_2(\delta) = -\delta log_2\delta - \Big(1 - \delta\Big)log_2\Big(1 - \delta\Big). \tag{2.32}$$

Eve can extract maximum $H_2(\delta)$ information. To minimize this amount of information, the bits used in the final key are reduced to

$$N = N_{sift}\Big[1 - H_2\Big(\delta\Big) - f\Big(\delta\Big)H_2\Big(\delta\Big)\Big]. \tag{2.33}$$

Assuming, $\delta < 11\%$ and f(δ) =1, secure key of any bit length (N bits) can be distilled, if and only if N is positive. $f\big(\delta\big)$ is the parameter to decide Eves presence and the security of the protocol. Randomness extraction or privacy amplification is the final step where N_{sift} reduces to N bits. The detailed key analysis and practical implementation of QKD protocols have been studied in [Tomamichel et al., 2012; Lucamarini et al., 2013; Gisin et al., 2002]. There are a number of proposals for BB84 protocol [Lo et al., 2005a; Dynes et al., 2012]. The phase encoding method [Dynes et al., 2012] has been used to realize the BB84 protocol in optical fibers as birefringent quantum channels. The main issue in using this method is that we need a stable Mach-Zehnder interferometer on the receiver side.

2.2.2 SARG04 Protocol

The SARG04 protocol is similar to BB84 protocol at the level of quantum processing [Scarani et al., 2004]. It uses two different conjugate bases: $|+Z\rangle \equiv |0\rangle$, $|-Z\rangle \equiv |1\rangle$, $|+x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|-x\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alice transmits only one state to Bob prepared from these four bases. Bob measures this state in σ_z or σ_x. The main difference between SARG04 and BB84 protocols lie in encoding and decoding of classical information. In encoding procedure, it writes 0 for $|+z\rangle$ and $|-z\rangle$ and 1 for $|+x\rangle$ and $|-x\rangle$. To enhance the security during communication and to confuse Eve, SARG04 protocol randomly chooses the two bases with equal probability [Bennett, 1992].
During sifting phase, Alice declares only the already sent state. She does not disclose the basis, only declares one of the states that code for the other bit, not orthogonal [Avella et al., 2010] to the already sent bit. Hence the apriori sets are: $S_{++} = \{|+z\rangle, |+x\rangle\}$, $S_{--} = \{|-z\rangle, |-x\rangle\}$, $S_{+-} = \{|+z\rangle, |-x\rangle\}$ and $S_{-+} = \{|-z\rangle, |+x\rangle\}$. Let $|sent\rangle = |+z\rangle$ and $|declared\rangle = |+x\rangle$. These are four confirmed states. At this stage, Bob estimates for correct bit σ_x and $|right\rangle = |-x\rangle$; he gets wrong bit if he measures in σ_z and finds $|wrong\rangle = |-z\rangle$.

If Eve disturbs the state, an error will occur or error may be introduced due to dark counts. By analysis, it is found that the length of the sifted key is $\frac{1}{4}$ of the length of the raw key, in case of no error. On the other side, this length increases in presence of high value or error rate.

The SARG04 protocol is more robust against the photon number splitting (PNS) attack as compared to BB84 protocol [Scarani, 2004; Acin et al., 2004].

2.2.3 Quantum Bit Error Ratio

The quantum bit error ratio (QBER) is the ratio of error rate to the key rate [Gobby et al., 2004]. Mathematically, QBER can be written as

$$QBER = p_f + \frac{p_d n q \sigma f_r t_l}{2}\mu, \tag{2.34}$$

here n is the number of detections, μ is the attenuation for light pulses, p_f denotes probability of wrong photon detection, p_d is the probability of wrong photon signal, q represents type of encoding, σ refers the detector efficiency, f_r is the pulse repetition frequency and t_l denotes transmission rate. BB84 protocol is secure if the value of the QBER is below 11%[Gobby et al., 2004]. From Eq. (2.34), to maintain QBER within practical limitations, one need to set the experimental parameters accordingly. Other kind of errors can be due to basis misalignment. For example, let Alice transmits a vertically polarized photon to Bob, while Bob receives only single photon. The vertical photon sent by Alice is

$$|V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.35}$$

As per BB84 protocol scheme, Bob uses polarization beam splitter (PBS) and a photon detector to measure the incoming photons. Let θ be the misalignment angle. Bob measures the single photon as follows

$$|\psi\rangle = \cos^2\theta|V\rangle + \sin^2\theta|H\rangle. \tag{2.36}$$

The misalignment angle θ is responsible for QBER, hence proper polarization has to be maintained during the complete communication procedure.

2.2.4 Specific attacks in quantum communication

Intercept-resend attack

While designing new protocols, Eavesdroppers try to find loopholes and vulnerabilities to attack the QKD systems [Makarov et al., 2006]. In quantum communication, two specific attacks are intercept-resend attack and photon number splitting (PNS) attack. In intercept-resend attack Eve first measures the transmitted qubit sent by Alice and then based on her measurements, she sends a qubit to Bob. In PNS attack after measuring the transmitted qubits, Eve sends random qubits to Bob. Eve gets success in her attempts, such that depending on the amount of channel noise she can hide her presence [Gay et al., 2005].

Photon-number splitting attack

Single photon sources are preferred to avoid such attacks. But practically lasers are deployed to achieve long-distance quantum communication because of their good power handling capabilities. The attenuated laser pulses emit multi-photon pulses which follow the Poissonian distribution. This gives an opportunity to Eve to steal one photon out of the multiphoton. In this scenario, Eve measures a single photon and extracts the information without being noticed by the authenticated users while the other unmeasured photons reach Bob. This is known as photon number splitting (PNS) attack [Schmitt-Manderbach, 2007]. Hence Bob did not observe any error in received photons, and Eve gets success in her eavesdropping attempts.

In real field QKD applications, attenuated laser pulses are used. For this, the spectral width of such laser pulses are much smaller than their mean wavelength. Hence it is approximated by a monochromatic coherent state. By phase randomization, these laser pulses are restricted to follow the Poissonian distribution. For such attenuated laser pulses, the probability of having n photons in a signal is

$$P_\mu(n) = \frac{\mu^n}{n!}e^{-\mu}, \tag{2.37}$$

where μ refers to mean number of photons, chosen by the sender. It is desired to have a low value of μ. In practical applications, it is observed that emitting photon sources have non-zero photon probability [Dušek et al., 1999; Brassard et al., 2000; Lütkenhaus, 2000; Dušek et al., 2000; Brida et al., 2000]. In PNS attack Eve splits one photon off from a multi-photon signal. To hide her presence, Eve can use a lossless channel so that the probability of the multi-photon signal reaching Bob's side increases and she can also steal one photon for extracting meaningful information without being noticed by authenticated users. Eve may also block single photon signals. In this way, Eve reduces a fraction of signals which contribute to the key generation, but she does not have full knowledge about single photon signals. Eve may apply coherent attack on those single photon signals which she did not block. Most of the errors are introduced in the sifted key because of the attack on single photon signals. Calculating fraction of the sifted key which is familiar to Eve and neglecting eavesdropping on single photon signals [Brassard et al., 2000], we have

$$f_{PNS} = \frac{p_{multi}}{p_{exp}} = \frac{1-(1+\mu)e^{-\mu}}{1-e^{-\eta\mu}}, \tag{2.38}$$

here p_{multi} refers to the probability for a multi-photon pulse emitted by Alice (transmitter) and p_{exp} refers to non-empty pulse detected by Bob. If the condition $p_{multi} > p_{exp}$, Eve gets full information about sifted key without notice or without introducing any error. Since Eve blocks all single-photon pulses, an important parameter is the critical transmission η_{crit}^{PNS}, which sets a threshold value known below which no secure key can be produced and is given by

$$\eta_{crit}^{PNS} = 1 - \frac{ln(1+\mu)}{\mu}. \tag{2.39}$$

Under PNS attack, Bob can detect the presence of Eve by monitoring photon number statistics [Lütkenhaus and Jahma, 2002; Nogues et al., 1999].

2.3 Quantum based satellite communication

Due to fiber imperfections and noise present in single photon detectors, quantum key distribution is limited to a few kilometers [Waks et al., 2002b; Gisin et al., 2002]. Quantum communication is possible in free-space with enhanced communication distance in certain wavelengths where polarization is maintained and absorption is minimum. In free-space, no birefringence occurs helping in maintaining quantum signal strength. Hence, polarization is preserved throughout the communication range. On the other side, in terrestrial free-space communication links performance is degraded due to high attenuation generated by objects and atmospheric effects in the line of sight. To avoid such situations, satellites are the best approach to deploy in free space communication. In ground-satellite quantum communication, only 30 kilometers communication distance is in within the grip of atmosphere, beyond that an effective communication set-up can be established.

It is necessary to investigate the link characteristics to perform quantum communication for the selection of a better quantum channel. Various factors such as detector inefficiencies, dark counts and beam diffraction are the main sources for channel attenuation. In the terrestrial implementation, parallel tracking channel has been used to stabilize the link, which further maintains proper basis alignment [Schmitt-Manderbach et al., 2007; Ursin et al., 2007]. Proper time synchronization is also important between the communicating parties [Scarani et al., 2009; Rarity et al., 2002]. In parallel tracking channels, GPS (Global Positioning System) is used to provide time synchronization. GPS is also used in satellite communication for time synchronization . Background noise is another source of error in quantum-based satellite communication. A number of techniques have been developed to mitigate the impact of background noise, see for example, [Er-long et al., 2005].

2.4 Effect of background noise on Quantum Key Distribution

Background light is the main factor as compared to dark counts of single photon detector (SPD) which increases quantum bit error rate (QBER). For this, noisy photons received from the varying intensity of the sky are analyzed. In a meaningful communication, the noise level needs to be decreased in order to increase the signal to noise ratio (SNR). Since in QKD, every pulse carry a single photon as an information carrier, we cannot increase signal power as we can in classical communication by increasing SNR.

Signal to noise ratio (SNR) is defined as the ratio of the average number of signal photons to noisy photons per pulse detected by single photon detector (SPD). Two major noise sources are background light and dark counts. For Silicon based APD (avalanche photo diodes), dark counts are less than 25 Counts s^{-1}. In free space, especially between satellite to ground quantum communication, the beam is open to the atmosphere, hence any background radiation can enter into the system as noise. Thus it is essential to protect the system from background radiation. The light reflected or radiated from the stars, moon, and sun produces the background light in the sky. In the atmosphere this light is scattered by fog, clouds, aerosols and molecules and finally received by receiving telescope as background noise. Further, this is detected by SPD even in a moonless night. Other sources of light may be city lights, but the solution for this is that the place to perform experiments can be selected far away from such areas. In addition, the satellite may be illuminated by the sun and become a noise source even at night.

Here we will discuss three methods to overcome the effect of noise and to increase the SNR.

2.4.1 Time-gate filters

SPDs are kept in off mode to decrease the number of dark and background counts. Only signal photons are allowed in a narrow time gate and noisy photons are blocked outside the window. This method is more efficient if this time window is maintained as narrow as possible. For this, proper synchronization has to be maintained between transmitter and receiver. To achieve proper synchronization, one can deploy quartz crystal oscillator of 100 MHz frequency and other software controlled phase-lock loop, which is operated by the detected photon signal maintaining 1 ns synchronization [Rarity et al., 2001]. For consecutive signal photons, to allow in time gate, periodic bright pulses of different wavelengths are used. The key rate in the earlier method is of several hundred bits per second and requires timing adjustment after every 100 ns. The latter method has an equal key rate to that of attenuated signal pulses but the problem of light interference from other bright pulses must be eliminated and proper adjustment on the same axis has to be maintained between two different wavelengths. The synchronization beacon light of acquisition, tracking and pointing (ATP) system must be used as a synchronization signal in QKD experiments which is best suited for satellite-to-ground QKD application.

2.4.2 Frequency Filter

It is required to deploy a narrow band filter before the detector to filter out the background light which is continuous in wavelength. The commonly used filters are atom filters, interference, and birefringence. All these filters have different bandwidth and transmittance. The transmittance and bandwidth of interference filters are $40 - 70$ % and $10 - 0.2$ nm,

respectively.
The bandwidth and transmittance for birefringence filters are 0.1 nm and nearly 20 %, respectively. In case of atom filters, the transmittance and bandwidth are relatively much better. For atom filters bandwidth is 0.01 nm and transmittance is greater than 90 % [Erlong et al., 2005]. While using atom filters, it is necessary to include Doppler effect as the satellite under consideration is a moving object. In case if the observer is located on the ground and source is placed on the satellite, the detected value of frequency f is

$$f = f_0 \frac{\nu}{\nu - \nu_r}. \tag{2.40}$$

Here f_0 represents emission frequency of the source. If 650 nm is the source wavelength, 7.8 $Km\ s^{-1}$ is the satellite velocity, we get Doppler shift of 0.01 nm. Hence, it is needed to compensate if atom filters are being used. It is also essential to control the temperature within 0.1 degrees when the diode laser drifts around 0.12 $nm/degree$ as its output wavelength.

2.4.3 Selection of spatial filters

Less background noise is collected if the detectors numerical aperture (NA) is small. For getting less value of numerical aperture (NA), an accurate, precise acquisition, tracking and pointing (ATP) system must be deployed. In addition to these, variations in atmosphere and weather conditions must be considered McFarland et al. [1997].

2.4.4 Precision in ATP system

To enhance the efficiency and stability of the distant communication links, it is very essential to deploy an ATP system. In free space quantum communication, it is essential to keep the small spot size at the collecting telescope for collecting most of the meaningful signal light. For achieving this, we need a precise ATP system and a small divergence of the signal beam.
The beams spot size must be large enough to cover the diameter of receiving telescope at the ATP aberration. If the telescope diameter is small as compared to spot size of the beam, the communication will suffer from a low-collection efficiency. The spot size of the receiving efficiency and the receiving beam is decided by the ATP aberration. In an ATP system, we can obtain maximum accuracy 10 μrad which implies that the spot size and the field of view of the collecting telescope must be greater than 10 μrad aberration. In addition to this, we need to take into account atmospheric turbulence. Jiaguang [1989].

2.4.5 Atmospheric Turbulence

Atmospheric turbulence is responsible for wandering and spreading of the laser beam. If the scale of the turbulent current is larger than the beam diameter, it randomly changes the beam direction. Other than these factors, speckle and lens effects of the turbulence are also effective. For a receiving station at a high mountain (around 2000 m), the wander will be about 10 μrad. Its value will be 100 μrad at sea level. If the transmitter is on satellite and receiver is at a high mountain (around 2000 m), according to [Rarity et al., 2002], taking atmospheric thickness into consideration, we get 1 m value of spreading and wander, due to turbulence.

2.4.6 Effect of background light

For the given values of brightness of the sky and telescope parameters, noise can be calculated. The received power P_b by the telescope can be written as Arnon [2003]

$$P_b = H_b \times \Omega_{fov} \times A_{rec} \times B_{filter}, \tag{2.41}$$

here B_{filter}, A_{rec} and Ω_{fov} are the filter bandwidth, telescope aperture and field of view, respectively. The effect of noise can be minimized by using a narrow band filter and reducing field of view. The SNR cannot be improved by reducing the aperture area. On the other hand, SNR can be relatively improved by using a time gate which blocks the noise outside the time gate. In addition to this, the weather conditions change the value of brightness of the sky background (H_b). If the bandwidth is within the range of $0.53 - 1.06$ μm, the cloud brightness is $120 - 240$ $Wm^{-2}Sr\mu m$. For better analysis, one can use 150 W m^{-2} Sr μ m as brightness of an illuminated cloud. For analysis, in addition to atmospheric turbulence, one can use 100 μ rad for receiving field, a time gate of 1-3 ns and 1 m ($A_{rec} = 0.785$ m^2) receiving telescopes aperture. Hence for different conditions and based on available technology, we can calculate number of background photons which are received per pulse. Reflection from the satellite is also a source of noise which must be taken into account.

2.5 Effect of the atmosphere on system efficiencies

In clear atmosphere, we observe a very high transmittance for certain windows. Scattering and absorption is neglected above 10 Km. For certain wavelength and in clear weather, 65% transmittance is achieved [Rarity et al., 2001]. It is observed that QKD fails in bad weather conditions such as clouds, noise, fog or rain. These bad weather conditions are the main obstacles for all quantum-based free space communications. To improve the QKD based satellite communication, ground station should be placed on a high mountain. For a Gaussian beam of radius $\omega_0(\frac{1}{e^2})$, the divergence half angle is

$$\theta = \frac{\lambda}{\pi\omega_0}, \tag{2.42}$$

where laser wavelength is λ, ω_0 is half the diameter D of the telescope. For $D = 10$ cm, $\lambda = 650$ nm, transmission distance $(L) = 1000$ Km, spot size becomes 8 m after reaching 1000 Km (for accounting atmospheric turbulence, it should be less than 10 m). A highly precise ATP system with accuracy greater than 5 μrad is required to collect the signals from satellite. For intercepting large Gaussian beam of diameter 200 by telescope diameter (D_T), the collected fraction is Theer and Denk [2006]

$$\eta = 1 - exp\Bigg[- \frac{2D_T^2}{2\omega^2}\Bigg] \approx \frac{D_T^2}{2\omega^2}. \tag{2.43}$$

The dB is used to represent a ratio in a logarithmic way. This ratio may be sound pressure, power, intensity or voltage, or many other things. It is mostly used in signals, electronics and communication. The losses are 17 dB for $D_T = 1$ m. The number of signal photons collected by ground based station is 6×10^{-4} per pulse for the following values, SPD efficiency = 70 %, transmittance = 60 %, coupling efficiency = 80 %, number of photons per pulse is 0.1. Silicon-based SPD has 25 counts s^{-1} dark count. It provides 2.5×10^{-7} counts $pulse^{-1}$; for 10 ns gate time, it gives error rate 0.2%. Here background light contributes more than dark counts of the single photon detector and is the main source of noise. If the error rate is within 10 %, which is the security level for QKD, then only the noise counts will be less than 6×10^{-5} counts $pulse^{-1}$.

The other sources of error which change the polarization are satellite vibration and rotation, cirrus clouds, reflection at curved mirrors and the Faraday effect of the ionosphere. The adaptive optics can be used to reduce the atmosphere turbulence, also it can minimize background noise and signal receiving efficiency can be increased [Tyson, 2002]. Coherent states contain on an average 0.1 photons $pulse^{-1}$ which improves system performance as compared to the multiphoton source. The decoy states are as proposed by [Lo et al., 2005b], [Wang, 2005] and [Scarani et al., 2004] can be used to attain better security with less errors.

As the satellite moves and passes through a noisy environment, the change in satellite coordinates is evaluated by applying suitable phase and rotational operators on the initial quantum state $|\phi\rangle$ and this change in coordinates is observed from the transformed state $|\phi'\rangle$.

The perfect coupling of information carrier photons from a free-space quantum channel into a single-mode optical fiber (SMF) has important implications for quantum network fundamentals involving SMF interfaces to quantum detectors, atomic systems, integrated photonics, and direct coupling to a fiber network. Propagation in atmospheric turbulence, results in wavefront errors that minimizes mode matching with SMFs. In a free-space quantum channel, this results in photon losses. This is a major issue for satellite-Earth quantum channels, where atmospheric turbulence results in significant wavefront errors Gruneisen et al. [2017].

The Adaptive optics (AO) compensates the effects of atmospheric distortion to maximize the quality of the optical link, thereby reducing atmospheric turbulence induced loss and noise at the receiver. An AO system measures the distorted wavefront caused by atmospheric turbulence with a wavefront sensor, and corrects these distortions with a device such as a deformable mirror. This restores the optical quality of the optical system, and allows the quantum state to be transmitted and detected after transmission through a turbulent atmosphere. At the same time, pre-and-post adaptive-optics compensation for an orbital angular momentum (OAM) encoded, bi-directional quantum communication link is achieved. The atmospheric turbulence-induced quantum-symbol-error-rates are improved in forward and backward channels using the compensation method Liu et al. [2018]; Tyson [2002].

In the decoy state method, the weakness of practical QKD (quantum key distribution) is considered by using multiple intensity levels at the transmitter's end. The information carrier photons are transmitted by Alice using randomly chosen intensity levels (one signal state and many decoy states), which gives a variable photon number statistics throughout the channel. At the end of the transmission, Alice discloses publicly which intensity level has been deployed for the transmission of each photon. A successful PNS (photon number splitting) attack needs to maintain the bit error rate (BER) at the receiver, which can not be completed with multiple photon number statistics. By observing BER (bit error rate) corresponding to each intensity, the two authenticate users will detect a PNS attack, with improved secure transmission rates or maximum channel lengths, enabling QKD setups suitable for real field

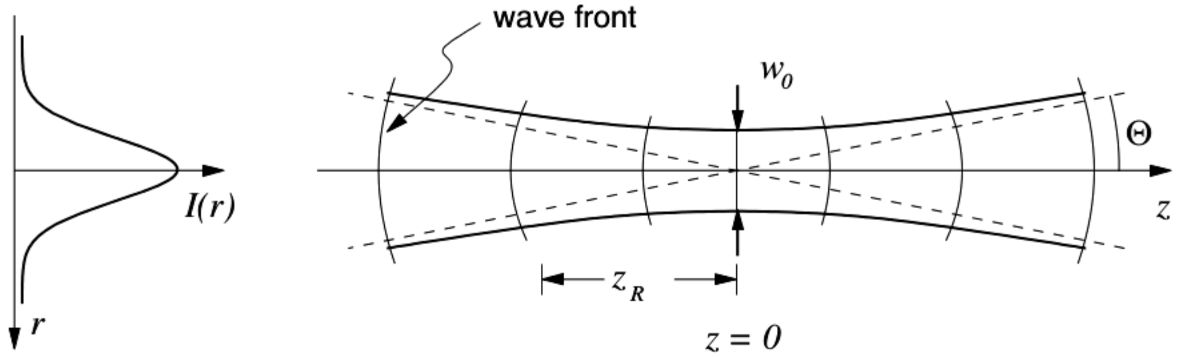

Figure 2.5: In a Gaussian beam wave: Rayleigh length (Z_R), divergence half angle in the limit $z \to \infty$ is denoted by Θ, minimum beam waist is denoted by ω_0. We get Gaussian shaped intensity profile for all values of z Louisell [1964]; Pantell and Puthoff [1969].

applications Lo et al. [2005b]; Wang [2005]; Scarani et al. [2004].

2.5.1 Free space propagation

In free space communication fog, snow and rain are the main obstacles in viewing distant objects. In quantum communication, same factors are responsible for limiting the communication to a few kilometers. The electromagnetic wave equation isWang [1986]

$$\bigtriangledown^2 E = \frac{1}{c^2}\frac{\delta^2 E}{\delta t^2}. \tag{2.44}$$

In free space communication, EM field is directed in a particular direction by a laser. Equation 2.44 is solved by a set of Gaussian beams in TEM_{00} (transverse electromagnetic wave) mode as Davis [1979]

$$I(r,z) = \frac{2P}{\pi\omega^2(z)} exp\bigg(-\frac{2r^2}{\omega^2(z)}\bigg), \tag{2.45}$$

where r represents distance from the optical axis, P denotes laser power and $\omega(z)$ is beam radius in propagation direction $\hat{z}$. Also,

$$\omega(z) = \omega_0\sqrt{1 + \frac{Z^2}{Z_R^2}}. \tag{2.46}$$

Here ω_0 denotes beam waist or minimum beam radius. It is related to beam divergence length (called Rayleigh length) $Z_R = \frac{\pi\omega_0^2}{\lambda}$. For $Z >> Z_R$, Davis [1979]

$$tan\Theta = \lim_{z\to\infty}\frac{\omega(z)}{|Z|} = \frac{\omega_0}{Z_R} = \frac{\lambda}{\pi\omega_0}, \tag{2.47}$$

where Θ is known as beam divergence half angle and Davis [1979]

$$R(z) = z\bigg(1 + \frac{Z_R^2}{Z^2}\bigg). \tag{2.48}$$

At $Z = 0$, we get planar wave front. At $Z = Z_R$ wave front curvature is more and then becomes plain for $Z \to \infty$.
It is desirable to increase the transmittance by minimizing beam spread, but it is limited by the diameter of transmitting telescope. For each distance, one can get a maximum initial beam radius which results into a minimum beam radius and minimum beam spread for a given distance. This is given as $\omega_0^{opt} = \sqrt{\frac{\lambda L}{\pi}}$ and it provides a beam spread $\frac{\omega_L}{\omega_0} = \sqrt{2}$.

Diffraction mainly causes beam spreading in vacuum. An extra beam spreading occurs under atmospheric turbulence which produces much larger beam spot size as compared to diffraction. The optical wave propagation is affected by the following three parameters

(i) Scattering,
(ii) Absorption,
(iii) Refractive index fluctuations (optical turbulence).

Absorption and scattering are considered under clear atmospheric conditions.

2.5.2 Scattering and Absorption

Scattering and absorption give attenuation which depends on the selected wavelength of EM radiation. These effects can also be classified according to the size of particles interacting: molecular effects and the effects generated by larger particles such as aerosols. The resulting effect can be explained by the Beer-Lambert law Calloway [1997]

$$I(\lambda, Z) = I_0(\lambda) exp\Big(-Z\alpha_{ext}(\lambda)\Big). \tag{2.49}$$

Here $\alpha_{ext}(\lambda)$ is the extinction coefficient which is wavelength dependent. This extinction coefficient is the addition of scattering and absorption [Churnside and Rothman, 2004].

(a) Absorption

In this process, rotational, vibrational and electronic properties of molecules change as they absorb energy from the incident photon. Hence the absorption spectrum of atmospheric molecules has different shapes depending on two line-broadening effects, is Doppler broadening and pressure broadening. In the series of discrete absorption lines, vibrational spectra are important which is in the wavelength range of visible to near-infrared.

For calculating extinction coefficient for a particular wavelength, we take help of molecular spectra and from the collection of molecules present in the atmosphere. This can be performed by atmospheric transmission programs, like LOWTRAN, FASCODE or MODTRAN [Anderson, 1995]. MODTRAN and LOWTRAN are band models, but FASCODE is a line model which gives comparatively higher resolution than band models.

(b) Scattering

(i) **Rayleigh scattering:** In the presence of EM model, the weak bound electronic cloud which is the gaseous molecule gets perturbed. Rayleigh scattering is present in haze and air molecules, which are small in comparison with the wavelength of the radiation. According to Rayleigh law, scattering coefficient is directly proportional to λ^{-4}. At $\lambda > 3\mu m$, scattering is very low for air molecules. Blue light is scattered relatively more than the red light, hence at $\lambda < 1\mu m$, Rayleigh scattering gives blue color of the sky Curcio et al. [1964].

(ii) **Mie Scattering:** It is also known as aerosol scattering. It is due to those particles whose size are comparable to that of radiation wavelength. With increasing wavelength, scattering losses become low and finally reach the Rayleigh scattering case. Atmospheric aerosols remain suspended in the atmosphere for longer time. These cover diameter in the range of 2 nm to 100 μm. Hence, aerosols are larger than molecules. Aerosols are produced by man-made and natural sources, like soil debris and rock particles developed by gaseous emissions and sea salt. The composition and particle size affects the radiation extinction which is generated by a single aerosol. It is important to take into consideration factors such as aerosol composition, particle size distribution and concentration for calculating aerosol-induced extinction. Many models describe aerosol conditions which are functions of the meteorological or local environment. Hence, to avoid experimental difficulties, all these factors need to be taken into account Curcio et al. [1964].

Primary radiation absorbers are water vapor ω_2, NO_2, ozone and CO. For $\lambda < 0.2\mu m$, absorption due to O_3 and Ozone O_2 diminishes propagation of radiation. Excluding H_2O absorption in between 0.65 to 1.0 μm, a small amount of absorption can be observed for visible wavelengths which are in the range of 0.4 to $0.7\mu m$. At infrared wavelength, water vapor and CO_2 absorb the radiation [Curcio et al., 1964]. During long horizontal paths at low altitude, the factors responsible for attenuation are humidity and environmental condition.