Principles of Quantum Communications and its Recent Advances

Zhuangyu Han (A paper written under the guidance of Prof. Raj Jain)   Download

Abstract

Quantum communication is becoming more and more practical based on recent research. This paper introduces simple quantum systems and the active/potential applications of quantum communication systems. Mathematics preliminaries and quantum information theory will be presented first. Then several simple applications of quantum systems in communication including quantum key distribution (QKD) will be mentioned. We can see that quantum information has completely different features compared to classical information. Th latest improvement based on satellite quantum channels allows us to expect a global quantum network. The inherent characteristic of quantum communication makes it theoretically immune to traditional eavesdropping.

Keywords: quantum communication, qubit, quantum entropy, quantum teleportation (QT), superdense coding (SDC), quantum key distribution (QKD), BB84, satellite-based quantum channel

Contents

1 Introduction

From the beginning of the 20th century, quantum physics is always an attractive discipline. The group of experiments about the unpredictable position of a particle and superposition of distribution density makes most of the people confused and surprised when they see such a phenomenon for the first time. An electron knows whether there is a wall before it hit the wall! Also, we can even not regard an electron as a particle before we see it detected because interacting with any piece of space where the wave function has non-zero value will change the state of an electron [Carnal91]. Quantum mechanics describes the states of a quantum system by vectors in Hilbert space, which will be defined below. All the observables can be represented by matrices or operators, which could be applied to a state vector or a density operator of a mixed state.

Quantum communication is a new field, in terms of communication, where people send or receive messages by transmitting quantum states of a specific quantum system, for example, a photon. Photons can be sent through free space or optical fibers. The quantum states are the physical characteristics of the photons, such as polarization. A 45-degree linearly polarized beam could penetrate a vertical polarizer with 50 percent energy loss. However, if people send photons in the same polarization state one by one to the polarizer, either zero or one photon will be observed with probability both 50 percent. Such a phenomenon can only interpreted by quantum mechanics with probability. The difference between quantum communication and classical communication is that the characteristics of quantum systems allow people to detect any traditional eavesdropping theoretically [Wilde13]. As eavesdropping on a mixed state of a quantum system will certainly destroy the state, we could design protocols where we have ways to detect adversaries by checking whether a mixed state is changed.

In Section 2, the fundamental knowledge of mathematics and information theory is necessary for quantum communication. From the quantum information theory, we could find some extraordinary features of quantum systems. Then quantum teleportation (QT), which is the transmission of a pure state with the help of classical channels [Pathak13], and superdense coding (SDC), which allows us to encode m bits of classical information with n qubit, where $n < m$ [Pathak13], will be introduced. In Section 5, the basic concepts of QKD will be presented. QKD is a hot topic these years, but the first protocol of QKD can date back to 1984 [Bennett84]. QKD allows us to share a key used to encrypt information which can be transmitted in classical channels. The point is that once there is an adversary who eavesdropped on the key, it will be detected definitely (with probability arbitrarily close to 1). In the last section, some recent

advances of quantum communication will be presented including satellite-based QKD [Liao17] and free-space quantum channel in daylight [Liao17a].

2 Mathematics Preliminary

In this section, some basic mathematics tools for dealing with quantum systems will be introduced. The Hilbert space where all the possible quantum states are vectors on it is the most important concept. Then, all the physics observables such as spin, position, and polarization direction are Hermitian matrices. Next, a density operator for a mixed state contains all the information of such a state. It is easy to calculate the expectation of an observable of a mixed state by its density operator. Then the most popular implementation of a qubit will be given.

2.1 Hilbert space and state vector of qubits

Hilbert space is very similar to Euclidean space, but the elements of Hilbert space could be complex, and there is an inner product defined on it.

Definition: An element of a d-dimensional Hilbert space $\mathbb{H}$ is a d-tuple

$$(x_1, x_2, \ldots \ldots, x_d) x_i \in \mathbb{C} \forall i \in \{1, ..., d\}$$

, which is also called a vector in $\mathbb{H}$.

The inner project defined in such a space is that

$$\langle a, b \rangle = \sum_i a_i^* b_i$$

where $a, b \in \mathbb{H}$ are both vectors. a_i^* represents the conjugate transpose of a_i. In matrix form, it is

$$\langle a, b \rangle = \begin{bmatrix} a_1^* & a_2^* & \ldots & a_d^* \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{bmatrix}$$

Obviously, $\langle a, a \rangle \in \mathbb{R}$ and is non-negative for any vector a in H.

Definition: The valid quantum states is the following set of vectors

$$\{a \in \mathbb{H} | \langle a, a \rangle = 1\}$$

For example, almost the simplest quantum system is called a **quantum bit** or a **qubit**, whose state can be represented by a vector in 2-dimensional Hilbert space.

E.g. $[10]^T$ is a state vector for a single qubit.

A state vector of a single qubit has a general form

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Where $|a|$ is the magnitude of a complex number a. The diagram below shows a qubit with real coefficients, but actually α,β can be complex.
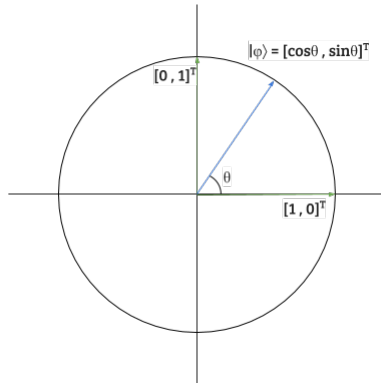

Fig. 1: A qubit with real coefficients

A qubit is an analog to a classical bit, such as a bit in our PCs' memory. The states of a qubit corresponding to the two states of a classical bit are $[10]^T, [01]^T$, which represents classical 0 and classical 1.

However, a qubit could be in a state as a superposition of classical states, for example $\frac{1}{\sqrt{2}}(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ and $\frac{1}{2}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{\sqrt{3}}{2}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$.

In quantum mechanics, we usually use $|\phi\rangle$ to represent a state vector and $\langle\phi|$ to represent the conjugate transpose of the same state vector. They are called the Dirac notation. And we write the inner product of two state vector $|\phi\rangle$ and $|\psi\rangle$ as $\langle\phi|\psi\rangle$ The joint state of two systems could be written as $|\phi,\psi\rangle = |\phi\rangle\otimes|\psi\rangle$ Where $\otimes$ is the tensor product. In matrix form,

$$|\phi\rangle = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \quad |\psi\rangle = \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \Rightarrow |\phi,\psi\rangle = |\phi\rangle \otimes |\psi\rangle = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{bmatrix}$$

Hilbert space is the playground of quantum mechanics and quantum communications.

2.2 Quantum measurement and observables

When measuring such states not corresponding to classical 0 ($\begin{bmatrix} 1 \\ 0 \end{bmatrix}$) and 1 ($\begin{bmatrix} 0 \\ 1 \end{bmatrix}$) are measured, the possibility of getting 0 and getting 1 are both non-zero, which means sometimes 0 could be observed, and sometimes 1 could be observed from the devices. For the general form of a state of a qubit, $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, the probability of getting 0 is $|\alpha|^2$, and the probability getting 1 is $|\beta|^2$.

When we are talking about measurement, there is always a group of orthonormal basis

$$\{b_1, ..., b_d\}b_i \in \mathbb{H}, \langle b_i, b_j \rangle = \delta_{ij} \forall i, j \in \{1, .., d\}$$

where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$

This set of basis depends on the observable being measured. When we measure the position of a particle, we will have a set of basis that is different to the basis used to measure the momentum. The measurement will always make a quantum system be into a basis state. Besides, a state that is not a basis state, but the weighted sum of multiple bases states is measured, the superposition will be destroyed.

For example, if state $[\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}}]^T$ is measured with computational bases $[10]^T, [01]^T$. $[10]^T$ or $[01]^T$ with probability both $\frac{1}{2}$ will be observed. This indicated that the measurement makes the state of a quantum system collapse into one of the bases related to the measurement, and we could observe that the basis it collapsed into after measurement. Quantum measurement will change the state if a system but classical measurement will not. From next part, it shows that the measurement

result is the eigenvalue corresponding to the basis state, of a matrix.

Observables are physical quantities that can be measured, such as position, momentum, and spin of a particle. The value of a qubit is also an observable because we could measure to see that it is classical 0 or classical 1. In quantum mechanics, an observable is always related to a hermitian operator, which actually is a hermitian matrix when we are using linear algebra.

Definition: A is a hermitian matrix, if

$$A = A^\dagger \quad \text{where} M^\dagger = \text{conjugate transpose of } M$$

and vice verse, which is easy to prove that A's eigenvalues are all real numbers and eigenvectors all orthonormal.

If A is a hermitian matrix and λ is an eigenvalue of A with corresponding unit length eigenvector v, we have

$$Av = \lambda v$$

So the product of A and v is v itself times λ. Here the λ is the measured value corresponding to basis state v.

The measured value of a qubit is again a good example to an observable. The two bases of the measurement of a qubit here are the computational basis

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

The measurement outcome 1 corresponds to classical 0, and the measurement outcome -1 corresponds to classical 1. So the operator of computational measurement is

$$C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

We could trivially check that

$$C|0\rangle = 1 \text{ and } C|1\rangle = -1$$

The expectation of an observable A for a specific state $|\phi\rangle$ is

$$\langle\phi|A|\phi\rangle = (\sum_i a_i v_i)(\sum_i a_i \lambda_i v_i) = \sum_{ij} a_i a_j \lambda_i v_i^\dagger v_j = \sum_i a_i^2 \lambda_i$$

We could check this for a qubit in state

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

We have

$$\langle+|C|+\rangle = 0$$

so the expected value of measuring a qubit in $|+\rangle$ state is 0. The corresponding classical value is 0.5.

Operators are important tools for the analysis of a state.

2.3 Density operator of a quantum system

If we know that a quantum system is in a certain state, this system is called in a pure state. For example, a qubit could be in $|+\rangle = [\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}}]$ or $|-\rangle = [\frac{1}{\sqrt{2}} -\frac{1}{\sqrt{2}}]$. Both $|+\rangle$ and $|-\rangle$ are superpositions of bases states, but the state is determined to us, so they are called pure states.

If we cannot determine the state of a system, we say that this system is in a mixed state. For example, if we can only know that a qubit is in $|+\rangle$ with probability $\frac{1}{2}$ and in $|1\rangle$ with probability $\frac{1}{2}$ as well, we say that this qubit is in a mixed state. Obviously, the set of pure states is a subset of the set of mixed states.

To conveniently represent a mixed state, we usually use a density operator. If we know the possible pure state $|\phi_i\rangle i = 1,2,...$ and corresponding probability p_i, we have the density operator for this mixed state

$$\rho = \sum_i p_i |\phi_i\rangle \langle\phi_i|$$

here $|\phi\rangle\langle\phi|$ is the outer product of vector $|\phi\rangle$, resulting in a rank-one matrix.

The expectation of an observable A of a mixed state ρ is $Tr(A\rho)$, where $Tr(M)$ is the trace of M [Cariolaro15].

The density operators are useful when we are talking about the entropy of a quantum system.

2.4 Physical implementations and transmission of a qubit

There are several ways to implement a qubit quantum system. The most popular approach is to use the polarization states of photons. We could code |0⟩ into horizontal polarization and code |1⟩ into vertical polarization. A photon can be in a superposition state of horizontal and vertical polarization. Here the 45-degree tilted linear polarized photons are in the |+⟩ or |-⟩ state. We could also use the spin of an electron or a nuclear to represent a qubit. The spin of a nuclear can be measured by the magnetic field. The nuclears with different spin will hit distinct spots after going through a magnetic field.

When it comes to the transmission of a qubit, there are many approaches, as well. Here only photon-based implementation will be discussed. We could use the optical fiber [Lucamarini18] or free-space [Liao17a] as the medium of the quantum transmission. The optical fiber is commonly used for the internet. Lasers are handy sources of photons because the spectrums of lasers are super narrow (~ 0.02*nm*) [King77]. We can use optical devices such as polarizers, beam splitters, and photon detectors, to modulate and detected photons.

2.5 Summary

Generally speaking, we use unit vectors in Hilbert space ℍ to represent quantum states. The observables are hermitian matrices, which could be applied to a state vector to get the possible measured values or the expectation value corresponding to the states. A density matrix/operator is used to represent a mixed state. When we are implementing a qubit, we could usually use the polarized photons and transmit them in optical fibers or free space. In the next section, the amount of information contained in a qubit will be elaborated. Actually, it depends on the state of the qubits.

3 Quantum Information Fundamental

When people are talking about classical communication, the Shannon information theory plays an indispensable role in calculating the channel capacities the minimum number of bits for transmitting a message. In quantum communications, we use quantum entropy to calculate the amount of information contained in a qubit. There are also some interesting features of quantum information. A classical system does not have the counterpart of the features.

3.1 Classical entropy and quantum entropy

Shannon entropy [Shannon48] is a critical concept in classical communications. It is used to measure the amount of information contained in the uncertainty of a symbol, a word, or a sequence.

Definition: If there is an alphabet Σ and for each element a_i in this alphabet there is a corresponding probability p_i to it, the classical entropy of a symbol c from this alphabet is

$$H(c) = \sum_i (-p_i log(p_i))$$

If we choose base 2 logarithm, the Shannon entropy tells us that how many classical bits do we need, on average, to contain the information in such a symbol.

The quantum entropy, or Von Neumann entropy [Cariolaro15], is very similar to Shannon entropy. If, for a quantum system, we do not exactly know the state of it but a distribution of all the possible states, we could have its density matrix. The Von Neumann entropy is defined on the density matrix of a system.

Definition: If there is a quantum system whose density matrix is ρ, the Von Neumann entropy of this system is

$$S(\rho) = -Tr[\rho log(\rho)]$$

Here the log function applied to a matrix is just the matrix logarithm. As we know that the outer product of a vector and itself is a Hermitian matrix, according to the definition of the density matrix, we know that all the eigenvalues of ρ are real numbers and all the eigenvectors of it are orthogonal. After a series of algebraic transform, we have

$$S(\rho) = -\sum_i \lambda_i log(\lambda_i)$$

Where λ_i is the i_{th} eigenvalue of ρ.

For example, [Cariolaro15], let us consider a qubit with probability $\frac{1}{2}$ in the state $|0\rangle$ and $\frac{1}{2}$ in the state $|+\rangle$. The density matrix of this mixed state is

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \frac{1}{2\sqrt{2}}\begin{bmatrix} \sqrt{2}+1 & 1 \\ 1 & 1 \end{bmatrix}$$

It is easy to calculate the eigenvalues and corresponding eigenvectors, which are

$$\{\cos^2\frac{\pi}{8}, \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle\} \text{and} \{\sin^2\frac{\pi}{8}, \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle\}$$

According to the formula above, we could calculate that the entropy of this qubit, which is approximately 0.6009 qubits. Here we see the intrinsic difference between a classical bit and a

qubit. If a classical system has 2 possible states with both possibility $\frac{1}{2}$, its entropy will be 1 bit. But for a quantum system, it is not necessarily 1 qubit.

3.2 Negative conditional quantum entropy

Definition: Conditional entropy

$$H(A|B) = H(AB) - H(B)$$

Where *H(AB)* is the joint entropy, and *H(B)* is marginal entropy [Wilde13].

This formula tells us that, in a joint system AB, if we have already known the state of system B, the total information from this system will decrease and the remaining part is *H(A|B)*. The more correlated A and B are, the less information there is after knowing B. People will have a good guess of symbol A after people know symbol B is these two symbols are strongly correlated.

In a classical joint system, a part of the system will never tell us the amount of information more than the information in the entire joint system, which could be expressed a non-negative conditional entropy

$$H(A|B) \geq 0$$

[Wilde13].

However, in a quantum system, the conditional quantum entropy could be negative, which implies that knowing a part of a system could make a system more uncertain [Wilde13].

The definition of quantum joint entropy, quantum marginal entropy and quantum conditional entropy are Joint quantum entropy:

$$S(AB) = -Tr[\rho_{AB} log(\rho_{AB})]$$

Marginal quantum entropy:

$$S(A) = -Tr[\rho_A log(\rho_A)] \quad S(B) = -Tr[\rho_B log(\rho_B)]$$

Conditional quantum entropy:

$$S(A|B) = S(AB) - S(B)$$

Here $\rho_A = Tr_B[\rho_{AB}]$ and $\rho_B = Tr_A[\rho_{AB}]$. $Tr_X[]$ is the partial trace operator.

Definition: Bell state is

$$|\psi\rangle_{Bell} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Assume there is a 2-qubit system in Bell state, the density matrix of this system is

$$\rho_{AB} = \frac{1}{2}(|00\rangle\langle00| + |00\rangle\langle11| + |11\rangle\langle00| + |11\rangle\langle11|) = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

As we know that the density matrix of a pure state is a rank 1 matrix, there is only one non-zero eigenvalue in the spectrum of ρ_{AB}, which is just 1. So according to the definition, the Von Neumann entropy of a pure state is 0.

Then we know that the $\rho_B = \frac{1}{2}I$ and it is easy to know that the Von Neumann entropy of qubit B is 1 qubit. According to the formula $S(A|B) = S(AB) - S(B)$, we have $S(A|B) = -1$.

The negative conditional quantum entropy is anti-intuitive, and the Nocloning theorem even tells us that a qubit cannot be copied.

3.3 Nocloning theorem

In quantum information theory, we have the Nocloning theorem, saying that we cannot copy a quantum state of a system to another system without destroying the original version.

Theorem [Wilde13]: In a Hilbert space $\mathbb{H}$, there is not a unitary transformation $U : \mathbb{H} \otimes \mathbb{H} \to \mathbb{H} \otimes \mathbb{H}$ such that there exists a state $|s\rangle \in \mathbb{H}$ satisfying

$$U(|r\rangle|s\rangle) = |r\rangle|r\rangle, \forall|r\rangle \in \mathbb{H}$$

$\mathbb{H} \otimes \mathbb{H}$ is the Hilbert space for a 2-qubit system. A unitary transform is just like an operator applied to qubits, and it could change the state of a system. We can also say that U is a quantum gate. Quantum gates will be discussed in the next section.

Proof: Assume that there is such a unitary matrix U realizing

$$U(|r\rangle|s\rangle) = |r\rangle|r\rangle$$

And

$$U(|t\rangle\,|s\rangle) = |t\rangle\,|t\rangle$$

Then we will have

$$\langle r|t\rangle = \langle r|\,\langle s|s\rangle\,|t\rangle = \langle r|\,\langle s|\,U^\dagger U\,|s\rangle\,|t\rangle = \langle r,r|t,t\rangle = \langle r|t\rangle^2$$

, which implies that $|r\rangle$ and $|t\rangle$ are either orthogonal or identical. This result indicates that U cannot copy arbitrary state we want, so the initial assumption is wrong.

This theorem tells us that an eavesdropper cannot copy a state and forward it without destroying the original version. In some aspects, this theorem reveals that quantum communication cannot be eavesdropped on in any traditional way.

3.4 Summary

In this section, some basic knowledge about quantum information theory is mentioned. The Shannon entropy measures the uncertainty of a classical symbol, and the Von Neumann entropy measures the information contained in a mixed state of a quantum system. We saw that a qubit having 2 equally possible states could contain less than 1 qubit of quantum information. Next, the conditional quantum entropy could be negative, which is a typical quantum characteristic and there is no classical counterpart. Finally, the state of a quantum system cannot be copied without destroying the original version. This quantum information feature guarantees the security of the quantum communication systems in some aspects. The extraordinary features of a quantum system enable us to realize many amazing applications such as QT, SDC, and QKD.

4 Quantum teleportation and superdense coding

QT [Bennett93] and SDC [Bennett92] are two well-known applications of quantum mechanics. QT allows two people to transmit an unknown state of a qubit with the help of classical channels, but the sender (Alice) and the receiver (Bob) must initially share an entangled pair of qubits. SDC enables us to encode 2 bits of classical information with 1 qubit, but priorly it also needs entangled pairs. In the beginning, quantum gates and the concept of entanglement will be introduced which are indispensable for the following applications.

4.1 Quantum gates and entanglement

Quantum gates are just matrices like the operators introduced in Section 1. A quantum gate must be a unitary matrix mapping one unit vector into another unit vector. When we apply a quantum gate to a qubit, the state of the involved qubits will change. Below are several common quantum gates used in quantum communication and quantum computing [Kaye07].

Identity gate:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Pauli X, Y, Z gates:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Controlled-Not (CNOT) gate:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Example: If we apply a Hadamard gate onto a qubit in state $|0\rangle$, we have

$$H |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

The entanglement states are a group of joint states of multiple quantum systems, for example, 2 qubits. If the joint state vector of 2 qubits cannot be written into the tensor product of two individual state vectors for single qubits, we say that these 2 qubits are entangled. For example, if we know that qubit q_1 is in $|0\rangle$ state and qubit q_2 is in $|0\rangle$ state, then the joint state vector for q_1 and q_2 is $|00\rangle$, in matrix form

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

So q_1 and q_2 are not entangled.

If we apply Hadamard gate to q_1, we have

$$H \left| 0 \right\rangle = \frac{1}{\sqrt{2}}(\left| 0 \right\rangle + \left| 1 \right\rangle)$$

Now the joint state is

$$\frac{1}{\sqrt{2}}(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}) \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Then, If we apply CNOT gate onto q_1 and q_2 at the same time, we have

$$CNOT \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(\left| 00 \right\rangle + \left| 11 \right\rangle)$$

We find out that

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

cannot be written as the tensor product of 2 single-qubit state vectors, so now q_1 and q_2 are entangled.

Next, we will use a diagram to show how does QT work.

4.2 Quantum teleportation

QT allows us to transmit an unknown state of a qubit without really sending qubits in quantum channels. However, Alice and Bob must previously share a pair of entangled qubits. I will give an example here to interpret the entire transmission process [Wilde13].
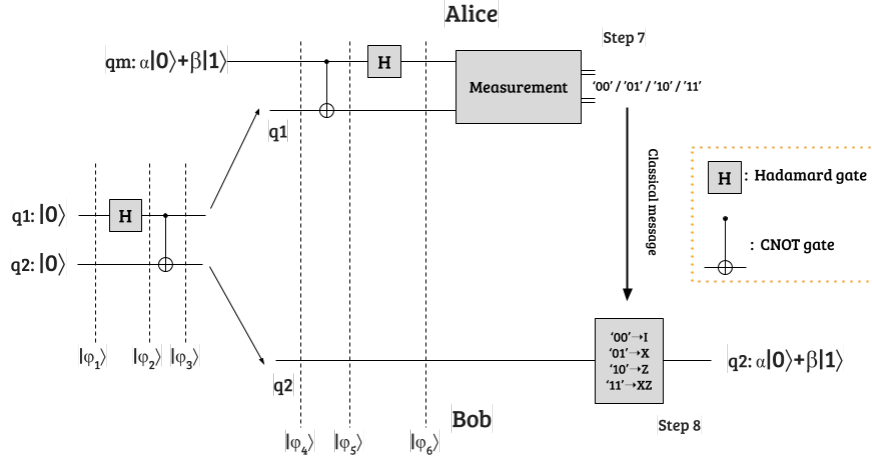
Fig. 2: Quantum circuit for a QT system [Wilde13]

Figure 2 shows the quantum circuit used for teleportation. I will show the effect of applying quantum gates onto the qubit step by step. The joint states of all the qubits will be shown after each step, like $|\phi_1\rangle$, $|\phi_2\rangle$,...

(1) Here we have two independent qubits both in $|0\rangle$ state.

$$|\phi_1\rangle = |00\rangle .$$

(2) After the Hadamard gate is applied to q_1, the joint state of q_1 and a2 becomes

$$|\phi_2\rangle = H\,|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

(3) Then we apply a CNOT gate to the two qubits.

$$|\phi_3\rangle = CNOT\,|\phi_2\rangle = CNOT\frac{1}{\sqrt{2}}[1010]^T = \frac{1}{\sqrt{2}}[1001]^T$$

which is just the Bell state.

(4) Then we send q_1 to Alice and q_2 to Bob with the joint state not changed. We introduce q_m, the qubit we want to transmit whose state. As we do not know the state of q_m, we assume that its state could be written as $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. The joint state of these three qubits is

$$|\phi_4\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\phi_3\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

(5) Then we apply the CNOT gate to q_m and q_1, we have

$$|\phi_5\rangle = CNOT|\phi_4\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$

(6) Next, we apply a Hadamard gate to q_m, we have

$$|\phi_6\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)|00\rangle + \alpha(|0\rangle + |1\rangle)|11\rangle + \beta(|0\rangle - |1\rangle)|10\rangle + \beta(|0\rangle - |1\rangle)|01\rangle]$$

$$= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

(7) If Alice measures q_m and q_1, she will have 4 possible outcomes 00, 01, 10, or 11. I call the result of Alice's measurement K.

(8) Alice tells Bob the K she got through a classical channel, for example an email. Bob applies a corresponding quantum gate to q_2. Table 1 gives the state of q_2 after step 7 and the corresponding gates.

Table. 1: The states after step 7 and the corresponding gates [Wilde13]

K	State of q_2 after step 7	The gate applied to q_2 by Bob	The final state of q_2
00	$\alpha|0\rangle + \beta|1\rangle$	I	$\alpha|0\rangle + \beta|1\rangle$
01	$\alpha|1\rangle + \beta|0\rangle$	X	$\alpha|0\rangle + \beta|1\rangle$
10	$\alpha|0\rangle - \beta|1\rangle$	Z	$\alpha|0\rangle + \beta|1\rangle$
11	$\alpha|1\rangle - \beta|0\rangle$	ZX	$\alpha|0\rangle + \beta|1\rangle$

Now we find out that the state of q_2 has become the same as the original state of q_m. Certainly, the state of q_m has changed because of the Nocloning theorem. This is what we called QT. Below SDC could realize information compression impossible in a classical communication system.

4.3 Superdense coding

In this example of SDC, I will show that Alice could send Bob two classical bits with sending only one qubit. They must previously share a pair of entangled qubits [Wilde13].

Firstly, we prepare two qubits q_1 and q_2, which are jointly in Bell state: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and send q_1 to Alice, q_2 to Bob.

The two classical bits Alice want to send will be one of the following 4 values: '00', '01', '10', '11'. For each value Alice wants to send, there is a corresponding single-qubit unitary matrix that can be applied to q_1.

Then Alice applies the gate to q_1, so we have the corresponding joint state of q_1 and q_2. For example, if Alice wants to send '10', she will use the gate iY.

$$(iY \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Table 2 shows all the joint state after applying the corresponding gate.

Table. 2: The gates applied to q_1 and the corresponding final joint state [Wilde13]

Value	Gate	The final joint state
00	I	$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
01	X	$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$
10	iY	$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

11	Z	$\frac{1}{\sqrt{2}}(|00\rangle\text{-}|11\rangle)$

It is easy to check that the four possible final joint states, in the right column, of q_1 and q_2, are orthogonal to each other, which compose a group of bases of the Hilbert space for 2 qubits. Now Alice will send q_1 to Bob. Then Bob has both q_1 and q_2.

Bob uses this group of bases to measure the q_1-q_2 system, and he will get one from the 4 bases with possibility one, which is just like measuring a photon, either horizontally polarized or vertically polarized, by using a polarizer in the horizontal direction.

As the result can be completely determined, Bob will know the value of two classical bits that Alice wants to send. In this process, Alice only sent one qubit to Bob after she determines her message, so this is called SDC. In total, Alice sends Bob 2 qubits, but the information could be coded into the first bit even after the first bit has been sent to Bob, which is amazing. This communication method could only be realized with quantum system.

4.4 Summary

In this section, two typical applications of quantum communications are described, QT and SDC. The former could send an unknown state from Alice to Bob with an existing pair of entangled qubits. The latter could encode two classical bits into one qubit with an existing pair of entangled qubits. In the next section, there is an overview of the most popular application of quantum cryptography, which is called quantum key distribution.

5 QKD and its Recent Advances

QKD allows us to share a common key for encrypting classical information, without being eavesdropped by the adversary in any traditional way. Eavesdropping the qubits in the quantum channel while distributing a key could be detected with probability arbitrarily close to 1. In some countries, banks have already deployed QKD systems for encrypting important messages transmitted between two cities [Zhang18]. Furthermore, recently there are lots of researches on QKD. A team has realized satellite-based QKD over thousands of miles [Liao17]. Others realized QKD in the noise background of sunlight [Liao17a].

5.1 BB84 protocol part 1: How to send, receive, and measure qubits

BB84 protocol is a well-known protocol for QKD developed by Charles Bennett and Gilles Brassard in 1984 [Bennett84]. The below figure shows the diagram of a BB84 QKD system.
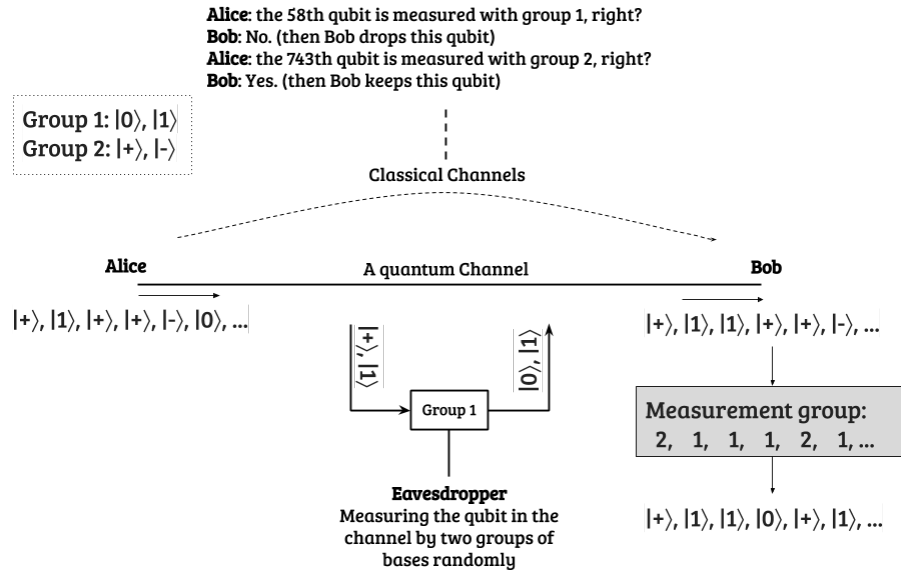
Fig. 3: BB84 QKD system diagram

The example [Bennett84] of sending and receiving qubits are elaborated in the table below.

Table. 3: A BB84 example [Bennett84]

Index	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Alice's group	2	1	2	2	1	1	1	2	2	2	1	2	2	1
State sent	$\lvert+\rangle$	$\lvert1\rangle$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert0\rangle$	$\lvert0\rangle$	$\lvert1\rangle$	$\lvert-\rangle$	$\lvert-\rangle$	$\lvert+\rangle$	$\lvert0\rangle$	$\lvert-\rangle$	$\lvert+\rangle$	$\lvert0\rangle$
Bob's group	1	1	2	1	2	2	1	1	2	1	1	1	2	1
Alice's reply	F	T	T	F	F	F	T	F	T	F	T	F	T	T
State received		$\lvert1\rangle$	×				$\lvert1\rangle$		$\lvert-\rangle$		$\lvert0\rangle$		$\lvert+\rangle$	$\lvert0\rangle$
Shared qubits							$\lvert1\rangle$		$\lvert-\rangle$					$\lvert0\rangle$
Unshared secret		$\lvert1\rangle$									$\lvert0\rangle$		$\lvert+\rangle$	

T: True, F: False, ×: Loss

In this protocol, Alice sends a series of qubits to Bob in two groups of bases. Each basis in group 1 is not orthogonal to each basis in group 2.

Group 1: $|0\rangle$ and $|1\rangle$

Group 2: $|+\rangle$ and $|-\rangle$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ We can see that in total there are 4 states in two groups of bases. Alice will randomly choose one state from the 4, with probability all $\frac{1}{4}$, to modulate a photon into corresponding polarization direction.

Alice will send such photons one by one through a quantum channel to Bob. The quantum channel here can be any type of physical system discussed before, which can encode a qubit and transmit it. After receiving the qubit, Bob randomly chooses group 1 or 2 as the bases to measure all the qubit. The quantum channel of lossy so some photons will be lost in the transmission. So sometimes Bob detects nothing when he measures a photon.

After Bob's measurement, Bob will tell Alice all the basis he used in the measurement in public classical channels. Alice will reply to Bob that which bases Bob used are right. They drop all the qubits processed with inconsistent bases.

Next, Alice and Bob will share a portion of the states with consistent bases. Here is the critical point, if there is no eavesdrop, all the results of Bob's measurement will be the same as the states Alice used. However, if the qubits are eavesdropped, with large probability, some of the shared states will be different. The probability could be arbitrarily close to 1 with the increment of the number of qubits they transmitted.

5.2 BB84 protocol part 2: How to detect the eavesdropper

Here I will show that at least one of the shared states will be different from a very large possibility if the transmission is eavesdropped on [Cariolaro15].

Assume that Eve is going to measure the qubits in the midway. As Eve does not know the group of bases used by Alice, she could only randomly choose a group. So for each qubit, with $\frac{1}{2}$ possibility, she chooses the right bases, and the other half is wrong.

If Eve chooses the right bases, the state of the qubit keeps. If she chooses the wrong bases, she will certainly change the state of the qubit. Bob measures the qubit, whose state has been

changed, and he will have $\frac{1}{2}$ possibility to get the inconsistent state as Alice. Here are all the circumstances where Eve chooses the wrong bases.

Table. 4: BB84 Eavesdropper detection

Alice sends	After Eve measures	After Bob measures
$|0\rangle$	$|+\rangle$	$|0\rangle$
$|0\rangle$	$|+\rangle$	$|1\rangle$
$|0\rangle$	$|-\rangle$	$|0\rangle$
$|0\rangle$	$|-\rangle$	$|1\rangle$
$|1\rangle$	$|+\rangle$	$|0\rangle$
$|1\rangle$	$|+\rangle$	$|1\rangle$
$|1\rangle$	$|-\rangle$	$|0\rangle$
$|1\rangle$	$|-\rangle$	$|1\rangle$
$|+\rangle$	$|0\rangle$	$|+\rangle$
$|+\rangle$	$|0\rangle$	$|-\rangle$
$|+\rangle$	$|1\rangle$	$|+\rangle$
$|+\rangle$	$|1\rangle$	$|-\rangle$
$|-\rangle$	$|0\rangle$	$|+\rangle$
$|-\rangle$	$|0\rangle$	$|-\rangle$
$|-\rangle$	$|1\rangle$	$|+\rangle$
$|-\rangle$	$|1\rangle$	$|-\rangle$

So for each qubit shared by Alice and Bob publicly, with the possibility $\frac{1}{4}$, the measurement result of Bob will be different from the state sent by Alice. If there are n qubits that are eavesdropped on, the possibility that all of them are consistent is $(1 - \frac{1}{4})^n = (\frac{3}{4})^n$. This probability could be arbitrarily small. So, in reality, it is impossible that Eve can eavesdrop without being detected.

If Alice and Bob do not find any adversary, they could use the qubits unreleased in the public channel as the secret key encrypting the messages. BB84 is simple and effective. Many advanced quantum communication experiments use BB84 to test the communication quality.

5.3 Recent advances in QKD

The early approaches to QKD are based on optical fibers. Even for the ultra-low loss optical fibers, the attenuation coefficient is 0.2 dB/km. Usually, people need to insert a quantum repeater, which is used to recover corrupted quantum states, about every 60 km in the midway of the quantum channels. However, because of the Nocloning theorem, a state cannot be amplified without any noise. So the optical-fiber-based QKD can only transmit quantum states for

hundreds of kilometers.

A team developed satellite-based QKD that can overcome the disadvantages of optical fibers [Liao17]. They use a green laser ($\lambda = 532$ nm) to transmit photons between a ground station and a satellite in a sun-synchronous orbit. They tested BB84 protocol on such a system and achieved a kilohertz key rate, which means that such a system could transmit thousands of qubits per second, over more than one thousand kilometers. Such a key rate achieved by using satellite is about 10^{20} times higher than the key rate we can reach with optical fibers in the same length. This QKD approach has the potential to be used to build an intercontinental quantum network.

However, the traditional satellite-based QKD experiments are conducted when the satellites are covered by the shadow of the earth in order to avoid being influenced by the sunlight, which is a strong noise source. Another team achieved long-distance free-space QKD in daylight by changing the working wavelength and photon detectors [Liao17a]. According to the radiation spectrum of the sun, the power of sunlight is stronger at 800 nm than 1550 nm. So the team selected 1550 nm as the working wavelength. In such wavelength, the Rayleigh scattering is only 7% of it in 800 nm, which dramatically increases the signal-to-noise ratio. They developed a new single-photon detector whose total detection efficiency is 8% under 200 mW pump power. The team transmitted standard BB84 bases with a key rate from 20 to 400 bits per second from one to the other side of a natural lake over 53 km. The total channel loss is 48 dB in local time from 15:30 to 17:00 on sunny days.

Such a result gives us confidence in inter-satellite quantum communication in daylight. As we know that geosynchronous orbit satellites are in the sunlight zone with a probability of about 99%, the daylight quantum QKD will improve the efficiency of the geosynchronous orbit satellite significantly.

5.4 Summary

In this section, we see how the BB84 protocol encrypts classical messages and prevent the qubits from being eavesdropped on. Then two recent works overcoming the disadvantages of optical fibers and night-time quantum communication are introduced. QKD is potentially the most popular encryption approach in the new era. We could also expect a global quantum network based on QKD from the satellites.

6 Summary

This paper shows a new type of communication method based on the quantum phenomenon. Starting with mathematics fundamental for understanding the representation of a quantum state and its revolution, it shows the differences between the classical and quantum information theory are presented. The state vectors of quantum systems can be expressed as unit vectors in Hilbert space. The density matrix is introduced to express a mixed state and to calculate the quantum

entropy of a qubit. Quantum measurement is one of the most critical concepts of quantum communication because the measurement introduces uncertainty into a quantum communication system. The uncertainty guarantee that measurement is not invertible.

We can see that there are many features to which we cannot find analogs in the classical world, for example, negative conditional quantum entropy. A quantum system could become more uncertain if a part of it is known. The Nocloning theorem prevents an eavesdropper from coping a qubit and forwarding the original one.

Next, QT and SDC show two anti-intuitive communication approaches. Actually, the shared entangled pair of qubits is the key to these two applications. The entanglement guarantees the relationship between two distant qubits so a state could be "transported" based on such relationship. In terms of physics, no information could be transmitted by operating an entangled pair because if so the information will have a speed exceeding the light speed. For SDC, in total there are 2 qubits sent, so the overall efficiency of transmission is the same as the classical channel. But with quantum entangled pair, a qubit could be encoded even after it has been sent out! This is the most amazing part of SDC.

Finally, QKD is described with its most famous BB84 protocol. From that example, it is shown that if the number of qubits sent is large enough, it is impossible to keep the state unchanged after measurement. In other words, any eavesdropping will definitely be detected. QKD also needs the assistant of classical channel.

In the end, we see that satellite-based daytime QKD is gradually becoming a reality. Sending qubits from satellite to ground and between satellite is exciting technology because it avoids the optical loss of optical fiber. The satellite link will become the most applicable implementation of QKD.

References

[Wilde13]   M. Wilde, "Quantum information theory," Cambridge University Press, 2013, ISBN: 9781107067844

[Carnal91]   O.Carnal and J. Mlynek, "Young's double-slit experiment with atoms: A simple atom interferometer," Physical review letters, 66(21), 1991, 2689 pp., https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.66.2689

[Pathak13]   A. Pathak, "Elements of quantum computation and quantum communication," CRC Press, 2013, ISBN: 978-1466517912

[Bennett84]   C. Bennett and G. Brassard, "Quantum cryptography: Qublic Key Distribution and Coin Tossing," In Proceedings of the International Conference on Computers, Systems and

Signal Processing, 1984,
https://cyberleninka.org/article/n/903792.pdf

[Liao17]   S. Liao, W. Cai, W. Liu, L. Zhang, Y. Li, J. Ren, J. Yin, et al, "Satellite-to-ground quantum key distribution," Nature 549, no. 7670, 2017, 43 pp.,
https://arxiv.org/ftp/arxiv/papers/1707/1707.00542.pdf

[Liao17a]   S. Liao, H. Yong, C. Liu, G. Shentu, D. Li, Jin Lin, H. Dai, et al, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," Nature Photonics 11, no. 8, 2017, 509 pp.,
https://sias.ustc.edu.cn/_upload/article/files/63/ae/36f6b0bd498595eb46eb5b6390b4/023b6b24-4045-4684-a494-b69b72bbf664.pdf

[Lucamarini18]   M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature 557, no. 7705, 2018, 400 pp., https://www.nature.com/articles/s41586-018-0066-6

[King77]   D. S. King, P. K. Schenck, K. C. Smyth, and J. C. Travis, "Direct calibration of laser wavelength and bandwidth using the optogalvanic effect in hollow cathode lamps," Applied optics 16, no. 10, 1977, 2617-2619 pp.,
https://www.osapublishing.org/ao/abstract.cfm?uri=ao-16-10-2617

[Cariolaro15]   G. Cariolaro, "Quantum communications," Heidelberg: Springer, 2015, ISBN: 978-3-319-15599-9

[Bennett93]   C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical review letters 70, no. 13, 1993, 1895 pp.,
https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.70.1895

[Bennett92]   C. H Bennett, and S. J. W. "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," Physical review letters 69, no. 20, 1992, 2881 pp.,
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.69.2881

[Kaye07]   P. Kaye, R. Laflamme, and M. Mosca "An introduction to quantum computing," Oxford University Press, 2007, ISBN: 978-0198570493

[Shannon48]   C. E. Shannon, "A mathematical theory of communication," Bell system technical journal 27, no. 3, 1948, 379-423 pp.,
https://pure.mpg.de/rest/items/item_2383162/component/file_2456978/content

[Zhang18]   Q. Zhang, F. Xu, Y. A. Chen, C. Z. Peng and J. W. Pan," Large scale quantum key distribution: challenges and solutions," Optics Express, 26(18), 2018, 24260-24273 pp.,
https://www.osapublishing.org/oe/abstract.cfm?uri=oe-26-18-24260

List of Acronyms

CNOT Controlled-NOT

QKD   Quantum Kry Distribution

QT   Quantum Teleportation

SDC   Superdense Coding

Last Modified: December 10, 2019

This and other papers on latest advances in computer networking are available on line at

http://www.cse.wustl.edu/~jain/cse570-19/index.html

Back to Raj Jain's Home Page