Review on Quantum Communication and Quantum Computation

Jiajun Chen*

Department of Physics and Astronomy, University College London, London, U.K.

*Corresponding author: jiajun.chen.19@ucl.ac.uk

Abstract. Quantum communication has made great breakthroughs in recent years. Because of its characteristics for strict information security transmission and high speed, it has received attention from related research fields around the world. This paper briefly reviews the progress in the field of quantum computing and communication. The basic functions of quantum mechanics related to the quantum communication are first introduced, including qubit, logic gates, postulates, polarization and quantum entanglement. Then the applications of quantum communication are discussed including teleportation, cryptography and quantum networks. Finally, advantages and disadvantages for the current applications are analyzed and the challenges remained in the current research are demonstrated.

Keywords: Quantum computing, quantum communication, quantum networks, quantum teleportation, quantum cryptography.

1. Introduction
Nowadays, with increasing needs for security and higher bandwidth, the classical approaches fail to provide a promising and effective solution in both fields of communication and computing [1]. This situation stimulates interests of researchers in the field of quantum computing and communication.

The theory of quantum communication was first proposed by Albert Einstein, who noticed the existence of microscopic phenomenon and defined it as “spooky action at a distance” [2]. In 1979, Shamir and Blakley proposed the secret sharing scheme, which was based on polynomial interpolation and hyperplane geometry [3, 4]. In 1981, Richard Feynman proposed the hypothesis of transmitting quantum information, which established the beginning of quantum information theory [5]. Then, a year later, in 1982, French scientist Alain Aspect offered an experimental answer to the debate between Albert Einstein and Nils Bohr of entangled photons with Bell's inequalities tests [6]. In 1984, Charles Bennett and Gilles Brassard proposed the first quantum key distribution scheme - BB84, which marked the birth of quantum communication theory [7]. In 2001, the University of Geneva in Switzerland first verified the quantum secret sharing scheme based on the GHZ triplet state with empirical evidence [8]. Recently, in 2016, the first quantum satellite, called Micius, launched from China to perform quantum experiments at space scale, which marked another important milestone for space science and scientific research of quantum communication [9]. Significant efforts made by these researchers contribute to the feasibility of quantum communication on both theoretical and experimental sides.
To provide a thorough review, we first provide descriptions of basic components of quantum mechanics, including qubits and quantum logic gates. Then we mention the postulates of quantum mechanics and talk about the polarization and entanglement. Finally, we explain the modern applications based on quantum communication, like teleportation, cryptography and quantum networks, and discuss the advantages and disadvantages involved. In the conclusion part, we summarize the challenges the field is currently facing and talk over the future developments of quantum communication.

2. Qubit and Logic Gate in Quantum Mechanics

2.1. Qubit

The qubit, also known as quantum bit, is the basic unit of quantum information, which corresponds to the basic information unit in classical theory—bit [10]. The state of a classic bit is 0 or 1, but the state of a qubit is described by a linear combination of computational basis states (0 or 1 state, corresponding to Dirac notation $|0\rangle, |1\rangle$), usually called superposition and can be represented as: $\varphi = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta$ are complex numbers and both satisfy normalization conditions. The state collapse principle of quantum mechanics results in one state when measuring a qubit. For example, when $|\alpha| = \frac{1}{\sqrt{2}}$ and $|B| = \frac{1}{\sqrt{2}}$ are calculated, since the calculation of the ground state is equal-probability superposition, there is a 50% chance that one will get a 0 state or 1 state before measurement. Once measured, the measured qubit will collapse into the 0 (or 1) state, and then it will remain in the 0 (or 1) state when there is no other external action. In other words, it collapsed from the superposition state to one of the calculated ground states.

As shown in Figure 1, Bloch sphere representation of qubits provides a useful means of visualizing the state of a single qubit and often serves as an excellent test-bed for ideas about quantum computation and quantum information [12]. The parameters $\theta$ and $\phi$ defining the quantum state are related to the azimuth and elevation angles that determine where the tip of this vector touches the surface of the Bloch sphere [13]. Infinite points are on the unit sphere and not determined unless there are measurements.

2.2. Quantum Logic gates

A logic gate, whether classical or quantum, is a physics system that takes a set of binary input to output a single binary output. In classical computer, logic gates are required. Similarly, in order to build a universal quantum computer, quantum logic gates are important [14]. In analogy to classical
logic gates like AND, OR, and NOT, quantum logic gates of NOT, Controlled-NOT, Hadamard are basically the most fundamental ones that will be further introduced in the following.

NOT Gate can be represented as X. When the input is $\alpha|0\rangle + \beta|1\rangle$, the output is $\beta|0\rangle + \alpha|1\rangle$. Therefore, the basic function of X is:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$ (1)

Controlled-Not Gate, on the other hand, is a two-qubit gate, usually called CNOT. If the first bit is $|1\rangle$, it will change the second bit of its input to 0, and do nothing when the first bit is $|0\rangle$. Its output totally depends on the first input. In this way, the first qubit putting in is called the control qubit, and the second is the target qubit. It can be expressed as below:

$$\text{CNOT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$ (2)

As for Hadamard Gate, it is the gate used to create the quantum superposition. If we input 0, we will get $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, which is noted as $|\pm\rangle$, and if input is 1, we will get $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, which is noted as $|\mp\rangle$. Therefore, its basic function is:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ (3)

3. Postulates of Quantum Mechanics

In the quantum mechanics, there are five basic postulates connecting with quantum communication. We then have a look at the postulates below one by one:

3.1. First Postulate

It explains any isolated physical system will correspond to a vector space, which usually called a Hilbert space. The system state will be represented by a unit vector in this space [15].

3.2. Second Postulate

In quantum mechanics, the mechanical quantity $F$, which can be observed in any experiment, could be described by a linear Hermitian operator [15].

3.3. Third Postulate

It expresses that the evolution of any closed system over time can be characterized by unitary transformation, which only depends on the start and end time of the evolution [16].

3.4. Fourth Postulate

Considering a physical system composed by two individual system $A$ and $B$. The state space of composite system $H$ can be determined through the tensor product of $A$ and $B$, which is $H = A \otimes B$. Then if we define $a \in A$, $b \in B$, then we can get the joint state of the composite system to be $h = a \otimes b$ [16].

3.5. Fifth Postulate

For a collection of measurements operators $\{M_m\}$ of quantum measurements. It satisfies the completeness equation [16]:

$$\sum_m M_m^+ M_m = I$$ (4)
These operators are used on the state space of system measured. The index \( m \) is the possible results for the measurement. If the state of quantum system before the measurement is \( |\phi\rangle \), then the probability of obtaining the result \( m \) after the measurement is given by

\[
p(m) = \langle \phi | M_m^+ M_m | \phi \rangle
\]  
(5)

The state of the system after the measurement is:

\[
\frac{M_m |\phi\rangle}{\sqrt{\langle \phi | M_m^+ M_m | \phi \rangle}}
\]  
(6)

Finally, the completeness equation shows that the sum of probabilities is equal to one:

\[
\sum_m p(m) = \sum_m \langle \phi | M_m^+ M_m | \phi \rangle = 1
\]  
(7)

4. Polarization

Polarization is a characteristic performed by photons, which is the orientation of oscillations in the plane perpendicular to the transverse wave’s direction of travel [17]. Take a simple experiment as an example. All the photons are polarized in the direction same to the polarizer after passing through it. After passing through polarizer, all the photons of the light beam are polarized in the same direction as the polarizer.

As shown in Figure 2 above, if a polarizer is set perpendicular to polarizer #1, the probability for a photon to pass through both polarizers is 0.

But things changed when the middle polarizer is diagonal to polarizer #1, as shown in Figure 3, there are half of the photons passing respectively through first two polarizers. Then the photons are now oriented diagonally and pass through the last polarizer. Since each polarizer allows half of the photons pass through, only 1/8 of initial photons finally passes through all three polarizers.

5. Entanglement

Quantum entanglement occurs when a pair or group of particles interact in a way that each quantum state cannot be described independently of the states of the others [19]. It predicts that entities have correlated fates. When we measure an entangled photon or atom, it is found that they are highly correlated and maintain the quantum states even separated by large distance. This really provides a way to improve security and probability of future communication.

Imagine that there are two coins which can be entangled. One person tosses a coin many times and records the times for the coin to show “heads” and “tails”, which is about half times each respectively. One thing to clarify is that each result is unpredictable before the measurement. Then this person tosses another coin that would generate similar but random results. After that, if we take a look at the
records of the experiment, it will show a correlation. When one coin shows “heads”, another must show “tails”. Since we have defined the states of the two coins to be entangled. Before the toss and measurement, the result is unknown, but will be correlated. As soon as one coin is tossed, the probability of results generated by tossing another coin is decided. Although people cannot predict each result individually, the final results are correlated and there will be no uncertainty of another coin if we already toss a coin. Now consider the photons, if they are entangled, they can be separated wide apart of infinite distance, but their measurement will still perform perfect correlation of the result.

The entanglement is very useful and important in the quantum world, and can be applied to many applications of communication [20].

6. Quantum Communication Applications

6.1. Quantum Teleportation
Quantum teleportation is a technology that uses the transformation between scattered quantum entanglements and some physical information to transmit quantum states to arbitrary distances [21].

It is an important communication method for transferring quantum states, and it is the basis of scalable quantum networks and distributed quantum computing. In quantum teleportation, the two communicating parties in two remote places first share a pair of entangled particles. Then one of them distinguishes the particles of the quantum state to be transmitted (generally not related to the entangled particles) from the entangled particles in its own hand, and informs the other party of the result of the discrimination. The other party will perform the corresponding unitary operation based on the obtained information. Entangled state pre-distribution, independent quantum source interference and pre-feedback are the three major elements of quantum teleportation.

6.2. Cryptography
Quantum cryptography uses quantum states as information carriers and transmits keys between legitimate users via quantum channels. The security of quantum cryptography is guaranteed by the principles of quantum mechanics [22].

The most famous application of quantum cryptography is quantum key distribution which is the process of using quantum communication to establish a shared key between two parties without a third-party learning anything about that key.

One of the most important and unique properties of quantum key distribution is that if a third party tries to eavesdrop on the password, the two conveniences of communication will be noticed [23]. This property is based on the basic principle of quantum mechanics: any measurement of a quantum system will interfere with the system. When a third party tries to eavesdrop on the password, it must be measured in some way, and these measurements will bring detectable anomalies. Through the quantum superposition state or quantum entangled state to transmit information, the communication system can detect whether there is eavesdropping. When the eavesdropping is lower than a certain standard, a secure key can be generated.

![A Quantum Cryptographic communication system for securely transforming random key](24).
6.3. Quantum networks

A quantum network is the network that adopts a quantum communication system. It consists of many separate nodes, and quantum information is stored in these nodes. It also facilitates the transmission of information in the form of qubits between physically separated quantum processor, which is a small quantum computer capable to perform quantum logic gates on a certain number of qubits. Generally, quantum networks work in a similar way as classical networks [25]. But it is better at solving some certain problems, like modeling quantum systems.

There are mainly two methods for operating quantum communication networks with a long distance, which are optical fiber network and free space network.

As for optical fiber networks, it has certain benefits. For example, it has a reduced chance of decoherence and people can use the optical fiber already existed. Multi-mode of fiber could also make communication more precise [26]. However, QKD in its basic form is limited in distance to a few hundred kilometers in optical fiber [26], and it is impossible, at least for now, to store the quantum information and use the optical fiber at the same time.

With respect to free space network, it is a communication technology that uses light waves as a carrier of quantum information to transmit in a vacuum or atmosphere, often called FSO. FSO networks are considered to be a strong supplementary option for quantum networks.

There are several advantages for using FSO networks [27-33]. First, optical wireless links provide high data rates and large bandwidth to support broadband data services. Second, the optical beams are immune to electromagnetic interference. Third, the cost of construction of FSO is relatively cheaper than that of optical fiber, as the optical spectrum is license free, which means there is no need to get permission for using the optical channels. It also has less power consumption because of its maintenance. Fourth, FSO uses a point-to-point system and narrow beams, which guarantee the security. And after determining the unobstructed passage between the sending and receiving points, it can generally be installed and put into operation within a few hours, which is really convenient.

There are also many problems stuck in the way of the development [27-33]. First of all, FSO is a line-of-sight broadband communication technology. When the transmission exceeds a certain distance, the beam will widen, making it difficult for the receiving point to receive correctly. The environmental disturbance on the photons also enlarges with the increasing of distance. Moreover, the sensitivity to the weather of FSO system performance is another major problem. Sunny weather has the least impact on FSO transmission quality, while rain, snow and fog have a greater impact. Generally, higher power laser diodes, more advanced optics and multiple beams are used to solve the problem for now. Besides, in the city, due to the blocking and shaking of the building, the laser alignment between the two points will be affected.

The free space networks are also possible from satellite to ground. A quantum satellite is capable to have entanglement distribution over a distance of 1,203km [34], and the experimental exchange of single photons from a global navigation satellite system can have a slant distance of 20,000km [35].

Figure 5. Transmission of classical information through the quantum satellite quantum channel [36].

Figure 5 presents the transmission of classical information via a satellite quantum channel between the sender (Alice) and the receiver (Bob). The communication starts with classical input at the sender (Alice) and then encoded into quantum domain through two transformations—Box A and Box C.
Then the converted quantum states are sent through channel. Considering we are at a non-idealistic environment, there is noise operating in the quantum channel. The noise is basically the uncertainty which caused when the quantum states interact with the environment. After that, the receiver (Bob) receives a damaged state, and then decodes it through quantum transformations. Finally, Bob can measure the data.

The encoded quantum states are sent over the satellite quantum channel. The errors appearing in the quantum channel are different from the errors of the classical channels. The system is in contact with the environment, so the system and the environment together form a closed quantum system. This means that the reason for the noise is the uncertainty in the channel, so the noise is the result of interacting with the environment. Because of the non-ideal environment, Bob receives a damaged state due to the channel error. In the decoding phase, Bob performs quantum transformations on his qubit (marked D) and finally measures it. Based on the postulates of quantum mechanics, the final measurement is classical [37].

For now, the free space networks are becoming more realistic due to recent successful experiments around the world. A typical case concerns with 2000 kilometers quantum distribution network between Beijing and Shanghai opened in September, 2017 [38]. It used the satellite Micius as the main connection to achieve satellite to the ground space free communication network.

In general, it is a field still requires much more research to achieve the best performance in practice.

7. Conclusion
In the current paper, we have reviewed the basic functions of quantum computing, main postulates of quantum mechanics, polarization and quantum entanglement. We have also discussed various applications of quantum communication and mainly focused on the achievements and difficulties found in the current research of quantum networks. The quantum communication technology breaks a new ground in communicating and provides great potential of researching and development for numerous scientists. Although most of the achievements of quantum communication is under testing and mostly used in the lab, we believe the moment of quantum communication taking over the classical approaches due to its higher rate of security and large bandwidth is just around the corner.

References
[1] G. Arun and V. Mishra, "A review on quantum computing and communication," in 2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking, 2014: IEEE, pp. 1-5.
[2] A. Einstein, M. Born, and H. Born, The Born-Einstein letters: friendship, politics, and physics in uncertain times. correspondence between Albert Einstein and Max and Hedwig Born from 1916 to 1955 with commentaries by Max Born. Macmillan, 2005.
[3] G. R. Blakley, "Safeguarding cryptographic keys," in 1979 International Workshop on Managing Requirements Knowledge (MARK), 1979: IEEE, pp. 313-318.
[4] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.
[5] R. P. Feynman, "Simulating physics with computers," Int. J. Theor. Phys, vol. 21, no. 6/7, 1982.
[6] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities," Physical review letters, vol. 49, no. 2, p. 91, 1982.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and con tos5," in Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984.
[8] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," Physical Review A, vol. 63, no. 4, p. 042301, 2001.
[9] "FIRST QUANTUM SATELLITE SUCCESSFULLY LAUNCHED", Oeaw.ac.at, 2016. [Online]. Available: https://www.oeaw.ac.at/en/oeaw/press/public-relations-and-
communications/ pressefotos/ first-quantum-satellite-successfully-launched /. [Accessed: 29-Oct-2020].

[10] D. J. Griffiths and D. F. Schroeter, Introduction to quantum mechanics. Cambridge University Press, 2018.

[11] S. Meister, "File:Bloch sphere.svg - Wikimedia Commons", Commons.wikimedia.org, 2009. [Online]. Available: https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg. [Accessed: 29-Oct-2020].

[12] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," ed: American Association of Physics Teachers, 2002.

[13] P. K. Roy, "Quantum Logic Gates."

[14] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 400, no. 1818, pp. 97-117, 1985.

[15] A. I. M. Rae, Quantum Mechanics, Fifth Edition. London: London: CRC Press LLC (in eng), 2007.

[16] S. Imre and F. Balazs, Quantum computing and communications. Wiley Online Library, 2005.

[17] S. Huard, Polarization of light. 1997.

[18] P. E. Black, D. R. Kuhn, and C. J. Williams, "Quantum computing and communication," in Advances in Computers, vol. 56: Elsevier, 2002, pp. 189-244.

[19] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Reviews of modern physics, vol. 81, no. 2, p. 865, 2009.

[20] S. Imre, "Quantum computing and communications–Introduction and challenges," Computers & Electrical Engineering, vol. 40, no. 1, pp. 134-141, 2014.

[21] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical review letters, vol. 70, no. 13, p. 1895, 1993.

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of modern physics, vol. 74, no. 1, p. 145, 2002.

[23] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Reviews of Modern Physics, vol. 92, no. 2, p. 025002, 2020.

[24] R. Goel, M. Garuba, and A. Girma, "Research directions in quantum cryptography," in Fourth International Conference on Information Technology (ITNG'07), 2007: IEEE, pp. 779-784.

[25] H. J. Kimble, "The quantum internet," Nature, vol. 453, no. 7198, pp. 1023-1030, 2008.

[26] R. Van Meter, Quantum networking. John Wiley & Sons, 2014.

[27] C. C. Davis, I. I. Smolyaninov, and S. D. Milner, "Flexible optical wireless links and networks," IEEE Communications magazine, vol. 41, no. 3, pp. 51-57, 2003.

[28] A. Mahdy and J. S. Deogun, "Wireless optical communications: a survey," in 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733), 2004, vol. 4: IEEE, pp. 2399-2404.

[29] S. Vangala and H. Pishro-Nik, "Optimal hybrid RF-wireless optical communication for maximum efficiency and reliability," in 2007 41st Annual Conference on Information Sciences and Systems, 2007: IEEE, pp. 684-689.

[30] K.-D. Langer and J. Grubor, "Recent developments in optical wireless communications using infrared and visible light," in 2007 9th International Conference on Transparent Optical Networks, 2007, vol. 3: IEEE, pp. 146-151.

[31] I. K. Son and S. Mao, "A survey of free space optical networks," Digital communications and networks, vol. 3, no. 2, pp. 67-77, 2017.

[32] G. Hörack, P. Pezzei, E. Leitgeb, and M. Tischlinger, "Economic aspects of free space optics as an alternative broadband network connection for the last mile," in 2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2016: IEEE, pp. 1-5.
[33] A. Malik and P. Singh, "Free space optics: current applications and future challenges," International Journal of Optics, vol. 2015, 2015.

[34] J. Yin et al., "Satellite-based entanglement distribution over 1200 kilometers," Science, vol. 356, no. 6343, pp. 1140-1144, 2017.

[35] L. Calderaro et al., "Towards quantum communication from global navigation satellite system," Quantum Science and Technology, vol. 4, no. 1, p. 015012, 2018.

[36] L. Bacsardi, "On the way to quantum-based satellite communication," IEEE Communications Magazine, vol. 51, no. 8, pp. 50-55, 2013.

[37] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless," Proceedings of the IEEE, vol. 100, no. Special Centennial Issue, pp. 1853-1888, 2012.

[38] Z. Zhihao, "Beijing-shanghai quantum link a ‘new era’," China Daily, pp. 2017-09, 2017.