The Principle and Prospect of Quantum Communication

Yutong Liu
Institute of Physics, Beihang University, Beijing
Corresponding author’s address: Vivian.wang@cas-harbour.org

Abstract. With the progress of science and technology, as well as the development of the times, people begin to have higher requirements on the security and efficiency of communication, so quantum communication has attracted much more attention. Quantum communication has lots of advantages such as unconditional security, high transmission efficiency, strong anti-interference ability and good concealment performance. In this paper, the author analyzes the advantages and the present situation of quantum communication. This paper briefly introduces the model of quantum communication network, the quantum computing, data decoding based on quantum computation and the quantum search algorithm concepts, which are described in simple terms. Two quantum secure direct communication protocols are also introduced and analyzed, and the prospects of quantum communication are presented.

1. Introduction
With the development of science and technology in recent years, the numbers of communication equipment and communication data have increased explosively, which leads to the increasing demand for communication performance. To be specific, the coming next generation communication technology requires high reliability, low latency, high data throughput and dense connection[1]. However, due to the mutual restriction between complexity and communication performance, traditional communication signal processing methods cannot meet these requirements. Thanks to the quantum superposition effect and the principle of quantum parallelism, quantum computing has shown great potentials[2]. It has the advantages of unconditional security, high transmission efficiency and utilization of quantum physical entanglement resources. What is more, quantum communication can encrypt and transmit information, during which process the key is not constant and full of randomness. When intercepted by relevant personnel, it is difficult to obtain real information, so quantum communication is absolutely safe. The results can be obtained at a complexity far lower than that of classical algorithms for specific problems. Therefore, quantum communication has higher efficiency. In addition, quantum communication has strong anti-interference ability, good concealment performance, low noise ratio and the possibility of wide application. Currently, quantum communication technology is becoming a hot research project in the world. Some research teams have realized quantum teleportation and entangled distribution in free space on the order of 100 kilometers. However, there are some problems in the research of quantum communication, such as the storage problem. Researchers have carried out research on the realization of large-scale long-range quantum communication, and promoted the new development of quantum communication technology storage through quantum entanglement exchange, quantum storage technology and purification technology[3].
2. Network architecture model of quantum communication
Generally, the architecture of a quantum cryptographic communication network consists of three layers: application layer, key management layer and quantum layer. The quantum layer is used to realize end-to-end quantum key distribution and upload the generated key to key management. Key management is mainly for storing the key generated by the quantum layer and selecting the appropriate route. And the function of application layer is to access various kinds of transactions, including voice, video, etc. The quantum cryptographic communication network uses the quantum key stored by the key management to encrypt the transmitted information, so as to guarantee the security of the transmitted information[4].

3. Quantization of classical communication signals

3.1. Quantum computing
The fundamental units in the quantum field are called qubits, and quantum states represent the states of each qubit. The quantum state is divided into pure states and mixed states, among which the pure state can be divided into a single state and a superposition state. In the pure state, each quantum state appears in terms of probability, for the superposition state $|\psi\rangle = \alpha |0\rangle + \beta |0\rangle$. The sum of the probabilities of all the states coming out is 1, which is $|\alpha|^2 + |\beta|^2 = 1$. And in the mixed state, there are many pure states according to probability. The state of a quantum system composed of n qubits is the superposition state or mixed state of 2n ground states, and there is quantum entanglement among multiple quantum states. Quantum entanglement connects quantum particles, so the quantum computer can store much more information than the classical computer. The state of quantum memory can be controlled by the unitary operator $U$, which satisfies $U^{-1} = U^+$. Therefore, by designing a quantum algorithm represented by a unitary operator, the state of the quantum system can be controlled, so as to achieve a specific computational goal[5].

3.2. Data decoding based on quantum computing
The most widely used encryption algorithm, the RSA algorithm, is based on multiplication of large prime Numbers[6]. Its security is based on the assumption that factorization is computationally difficult. However, Shor used quantum computing to refute this hypothesis, and the computational efficiency was extremely high. The state space for possible keys is $2^n$ for an n bit long key, but Shor’s algorithm can pick the right key in $O(n^3)$ steps. If $n=1024$, the classical key cracking method will take at least a few years, while the quantum computation will only take 0.01 seconds. This means that the length of the key hardly makes it any harder to crack[7].

3.3. Quantum search algorithm
The quantum search algorithm has attracted much attention for its acceleration and wide applicability compared with classical search algorithms. Unlike that the traditional search algorithm is mainly to overcome the problem of too many search paths caused by enormous solution space, the main problem faced by the quantum algorithm is that the amplitude of the solution set is too small. Therefore, the core of the strategy of the quantum search algorithm is how to quickly make the amplitude to the solution set while considering the complexity of the transformation. Finding all the paths is not the problem for the quantum algorithm, which aims to reduce the amplitude of the path, eliminate the non-solution and transfer it to the path of the solution[8].

4. Quantum secure direct communication scheme
Quantum secure direct communication is a technology that transmits secret messages directly in the quantum channel. It does not need to transmit secret keys in advance, so it simplifies the communication process[9].

4.1. Quantum secure direct communication based on single photon
Suppose that Alice is the sender and Bob is the receiver, and the process is as follows:
Bob sends N single photons in one of the four quantum states $|H\rangle$, $|V\rangle$, $|L\rangle$, $|R\rangle$ to Alice in turn:

$$|H\rangle = |0\rangle$$

$$|V\rangle = |1\rangle$$

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

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

After receiving the photon, Alice conducts security detection, and sends the measured result and the position of the measured photon to Bob, who obtains the error rate based on the comparative analysis of the measured result. If the error rate is lower than the threshold value and the channel is safe, and the next step can be taken, otherwise the communication will be stopped.

According to the coding rules, Alice sends the quantum state coding to Bob. If the information transmitted is 0, then the photon sequence is operated by $U_0$; if the information transmitted is 1, then the photon sequence is operated by $U_3$.

$$U_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, U_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Alice sends the photon to Bob after the operation.

After Bob receives the photon sequence, he selects the correct measurement base for single photon measurement according to the preparation information to obtain the secret information. Alice publishes the coded location information and operation information, and Bob determines whether the channel is safe or not through analysis.

In this process, the first security check, the photon did not carry classified information, so the eavesdropper could not get useful information. And eavesdroppers can be found if they exist[10,11].

### 4.2. Quantum secure direct communication based on entangled photon pairs

(1) Coding rules: $U_0$ and $U_3$ are the same as in 4.1, Table 1. Coding rules

| Transmission of information | Unitary transformation | Quantum state |
|----------------------------|-----------------------|--------------|
| 00                         | $U_0$                 | $|\Psi^-\rangle$ |
| 01                         | $U_1$                 | $|\Psi^+\rangle$ |
| 10                         | $U_2$                 | $|\Psi^-\rangle$ |
| 11                         | $U_3$                 | $|\Psi^+\rangle$ |

$$U_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, U_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

| $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$……(a) |
| $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$……(b) |
| $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$……(c) |
| $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$……(d) |

(2) Alice divides N entangled photons in the state of equation (a) above into two sequences, SA and SB. A and B respectively represent two particles of each entangled pair. SA as the information sequence, SB as the detection sequence.

(3) Alice sends the SB detection sequence to Bob. After Bob receives it, he randomly selects part of the photons for an X or Z basis measurement, and tells Alice the information of the measurement basis adopted. Alice measures SA under the same measurement basis, and judges whether there was eavesdropping by comparing the measurement results. If the error rate is less than the acceptable range, the next step is carried out, otherwise, the first step is returned.
(4) Alice adds a partial check sequence to the information sequence, encodes the information sequence according to the previous coding rules, and sends it to Bob.

(5) After Bob receives the information sequence, Alice will tell Bob the position of the calibration sequence, and Bob will conduct a Bell base joint measurement on the photons in the corresponding position, and will judge the security of the quantum channel according to the results obtained.

This protocol adopts the method of dense coding and the coding capacity is larger, and also adopts the idea of block transmission, which guarantees the security of the scheme[10,11].

4.3. Quantum secure direct communication scheme based on hybrid particles
(1) Bob prepares the single-photon state and the Bell state, and composes the two particles in the Bell state into SA sequence and SB sequence respectively, and sends the SB sequence and single-photon sequence to Alice.

(2) After Alice receives the sequence, Bob is informed by the classical channel, and then both parties start the first security check. In the sent sequence, Bob randomly selects some single photons for security check, and tells Alice the selected location.

(3) Alice and Bob share the control code. After receiving the location information communicated by Bob, Alice selects the measurement base according to the control code at the corresponding location for measurement and informs Bob of the corresponding result.

(4) In the corresponding position, Bob compares Alice’s measurement results with the original state prepared by himself, and obtains an error rate. If the error rate is below the threshold, they will proceed to the next step; if it is above the threshold, the lines of communication will need to be checked and returned to the first step.

(5) After channel security is determined, Alice abandons the particles used for security check and encodes the remaining particles. The coding rules are as follows:

| Transmission of information | | |
|-----------------------------|-----------------|-----------------|
| | $|\psi^+\rangle|\psi^-\rangle$ | $|\psi^-\rangle|\psi^+\rangle$ |
| 000 | $U_0$ | $L+U_0$ |
| 001 | $U_1$ | $L+U_1$ |
| 010 | $L+U_0$ | $U_0$ |
| 011 | $L+U_1$ | $U_1$ |

Table 2. Bell state coding rules

| Transmission of information | Z basis measurement | X basis measurement |
|-----------------------------|---------------------|---------------------|
| 100 | $U_0$ | $H+U_0$ |
| 101 | $U_1$ | $H+U_1$ |
| 110 | $H+U_0$ | $U_0$ |
| 111 | $H+U_1$ | $U_1$ |

$u_0 = U_0 \otimes U_0$ (5)

$u_1 = U_1 \otimes U_1$ (6)

$L = U_0 \otimes U_3$ (7)

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (8)

(6) Alice will send the encoded particles to Bob. After Bob receives the particle sequence, Alice will tell Bob the position of H transformation and L transformation.

(7) The decoding rules are as follows:

| Original quantum state | No L transformation | After L transformation |
|------------------------|--------------------|-----------------------|
| | The measured results | The decoding results | The measured results | The decoding results |
Table 5. Single photon decoding rules

| Original quantum state | Measured with the X basis | Measured with the Z basis | Measured with the X basis | Measured with the Z basis |
|------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
|                        | The measured results     | The decoding results     | The measured results     | The decoding results     |
| | | | | |
| | | | |
| | | | |

(8) According to the above table, Bob selects the appropriate measurement base for measurement and decodes the secret information sent by Alice. This scheme adopts the idea of control code.

4.4. Efficiency analysis

Formula of efficiency of quantum communication scheme:

\[ \xi = \frac{b_s}{b_q + b_t} \]  

Where, \( b_s \) is the number of message bits transmitted, \( b_q \) is the number of quantum bits used, and \( b_t \) is the number of classical bits consumed. The number of qubits used for eavesdropping detection is not taken into account in the calculation[9].

5. The prospect of quantum communication

Quantum communication has the advantages of absolute security and high efficiency, so it has broad prospects in the future.

5.1. Use of quantum relay technology to expand the communication distance

Relay technology can solve the problem of large loss of single photon in long-distance transmission. However, due to the no-cloning principle of the quantum state, the quantum state is not replicable, so quantum relays cannot amplify weak signals and forward them, just like ordinary signal relays. Quantum relays can only receive a photon’s signal before it reaches its maximum distance, store it, read it, and send it as a single photon[12].

5.2. Use of satellite-ground communication to realize remote transmission

In the vacuum environment, the photon basically has no loss, and the loss mainly occurs in the lower atmosphere. Therefore, the quantum communication between the two places of satellite communication is more convenient and fast. According to the calculation, as long as the communication can be more
than ten kilometers in the earth’s atmosphere, there is no problem in the communication between the
satellite and the earth[12].

6. Conclusion
Quantum communication, as a new communication method for information transmission on the basis of
quantum entanglement effect, has the characteristics of high efficiency and absolute security, and is a
hot research topic for international quantum physics and information science. Based on the quantum
entanglement theory, in 1993, American scientist C. H. Bennett proposed the concept of Quantum
Teleportation. And after more than two decades of development, quantum communication has gradually
moved from theory to experiment and to practical development. At present, quantum communication
involves the following fields, which are quantum cryptographic communication, quantum teleportation
and quantum intensive coding. With the increasing requirement of communication security and
efficiency, the importance of quantum communication is self-evident. The author believes that it is
feasible to build a global quantum communication network in the future.

Acknowledgment
First and foremost, I would like to show my deepest gratitude to my teachers and professors in my
university, who have provided me with valuable guidance in every stage of the writing of this thesis.
Further, I would like to thank my friends and parents for their encouragement and support. Without all
their enlightening instruction and impressive kindness, I could not have completed my thesis.

References
[1] Andrews J and Buzzi S et al. 2014 What will 5G be? IEEE Journal on Selected Areas in
Communications
[2] Sandor I 2013 Quantum communications: Explained for communication engineers IEEE
Communications Magazine
[3] Xie Z 2018 Current Situation and Prospect of Quantum Communication Digital Communication
World Issue 12 doi:10.3969/j.ISSN.1672-7274.2018.12.136
[4] Li Q Ren T Y Wang X H Wang C Dong J H Guo G X Shi E H 2019 Design of quantum
cryptographic communication network based on OpenFlow technology Information Technology Issue 10
doi:10.13274/j.cnki.hd.zj.2019.10.032
[5] Fang Y Guo X Ye W J Chen W 2019 Quantum Processing for Classical Communication Signals:
Progress and Outlook Signal Processing Issue 10 doi:10.16798/j.issn.1003-0530.2019.10.001
[6] Ambika S Rajakumar S Anakath A S 2020 A novel RSA algorithm for secured key transmission in
a centralized cloud environment[J] International Journal of Communication Systems 33(5).
doi:10.1002/dac.4280
[7] Sándor Imre 2014 Quantum computing and communications- Introduction and challenges[J]
Computers and Electrical Engineering 40(1)
[8] Sun J G and He H G 2003 A Quantum Search Algorithm Journal of Software 3
[9] Long G L and Liu X S 2002 Theoretically efficient high-capacity quantum-key-distribution scheme
[J] Physical Review A 65(3):032302-1-032302-3
[10] Wang Z Y and Li H Y 2019 Research on the Scheme of Quantum Secure Direct Communication
Microprocessor issue 5 doi:10.3969/j.issn.1002-2279.2019.05.008
[11] Georgi Bebrov and Rozalina Dimova 2020 International Journal of Theoretical Physics vol 59 (2)
pp 426–435 doi: 10.1007/s10773-019-04336-9
[12] Zhao H L 2018 Development of quantum communication technology Nature 3
doi:10.3969/j.issn.0253-9608.2018.03.007