Overview of Quantum Key Distribution

ZHOU Yun-ting[1, a], JI Feng-zhu[1], DENG Mao-lin[1], HE Xiao-gang[1] and TANG Qi-jie[1]

[1]Xichang Satellite Launch Center, XiChang, SiChuan 615000, China

[a]zhouyt01@yahoo.com.cn

Keywords: Quantum communication; Quantum; Quantum Key Distribution

Abstract

QKD (quantum key distribution) is core of quantum communication, it is not only the most extensive range of applications, and can also be served as a basis for other branches. In this paper, the theoretical basis and the basic idea of quantum key distribution has been described. Focus on several quantum key distribution schemes which are representative, some analysis and researches have been proposed. And sum up the pros and cons of these schemes after comparison.

Introduction

Different from the traditional cryptography, QKD is the product which is combined with cryptography and quantum mechanics. Its information carrier is based on the quantum state. Using some of the principles of quantum mechanics to transmit and protect information. Quantum Key Distribution usually treats quantum state as information carrier, using quantum mechanics, transmits between quantum channel, so that shared secret keys between communicating parties can be established[1].

In quantum key distribution, different sources will depend on different quantum properties and different quantum principles to ensure the security of communications. Therefore, we can generally divided into three categories according to the different sources of quantum key distribution. the first is the key distribution scheme, which is based on the quantum properties of a single-particle quantum system, the second is the key distribution scheme that is based on the nonlocality and correlation of a quantum entanglement particle system. The third is the key distribution scheme which is based on a system within entangled particles and single-particle quantum system.

Key distribution scheme based on the quantum properties of a single-particle quantum system

Among the key distribution schemes, the most representative schemes can be summarized as the following three parts. (1). The original quantum key distribution scheme ,which is raised by Bennett and Brassard in 1984, which can be recorded as BB84, short for Bennett-Brassard 1984.[2]; (2). In 1992, Bennett proposed a quantum key distribution scheme that can be noded as B92, short for Bennett 1992[3]; (3). And a quantum key distribution scheme was proposed by Hwang, Koh and Han in 1998, and It is abbreviated as HKH98[4]. BB84 protocol theoretically solves the problem of quantum key distribution, marking the birth of quantum cryptography.

Physical principles of BB84-QKD scheme. BB84 scheme treats polarization photons as quantum signal source to transmit keys. In quantum mechanics, two measure groups which are not commutative to each other are corresponding to the two mechanical quantity operators which are not commutative. Their important feature is their quantum measurement results meet the

(Grant from) The Youth Fund(2014sy27a006)

uncertainty principle of quantum mechanics.

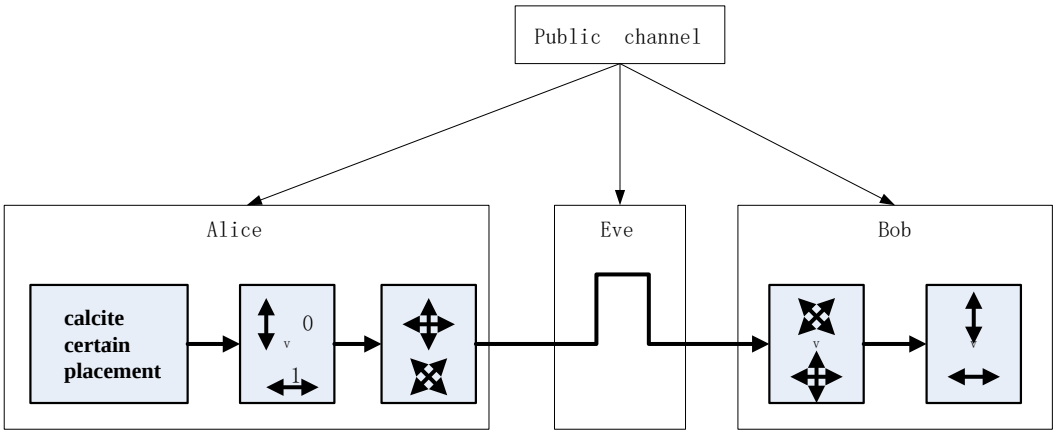

Fig.1 the Physical principles of BB84-QKD scheme

During the BB84-QKD communication process, each time Alice uses two groups ($\oplus$ or $\otimes$) with equal probability to send a binary 0 or 1. She can achieve quantum states by using single photon source, and applying a measuring device (such as calcite certain placement) to measure the photon. If a measured value can be measured, according to quantum mechanics, it must be the intrinsic value of the measured value. After the measurement, quantum state of the photon will collapse to the measured intrinsic value of the corresponding eigenstates. By selecting a different measure groups, Alice can get different quantum states.

And Bob has a 50% chance as Alice in selecting measurement group. So that in the ideal case, in the result, which Alice sends to Bob, there is 50% of binary code can be used as raw key. Alice and Bob choose s1(a small part of the results) from results S(from the same base) randomly. Compare through the classical channel, if the result of the error rate is lower than the error rate of pre-designed threshold ε, then their key transport process can be considered as safe. If the error rate in the result much greater than the threshold value somehow, then abandon the transmission of results. After the adoption of the quantum channel security checks, resume transmission key string.

Advantages and disadvantages of BB84-QKD scheme. One of the biggest advantages of BB84-QKD is that it has been proved to be an absolutely safe way to distribute keys[5-6]. In addition, its preparation and measurement of quantum signals is relatively easy to implement.

In BB84-QKD, both of the communications parties detect the eavesdropper by randomly selecting two groups in order to ensure the security of quantum key distribution, which is the source of shortcomings. During transmission, not all qubits are used in quantum key, only less than 50% of the qubits can be used, the utilization rate of its qubit is low[3]. On the coding capacity, two photons in quantum state can only transmit one bit of useful classic information. And four kinds of quantum state can only represent the "0" and "1" two codes. Coding capacity is low at the same time.Therefore, the total bit information transmission efficiency is low as well[7]. (<25%)。

$$\eta_t \equiv \frac{Q_u}{Q_t + b_t} \tag{1}$$

Q_u means the useful qubits that the communicating parties get, Q_t means the total quantum bits that transmitted. b_t means the classical bits that have to be exchanged Classical bits used to check the number of eavesdropping is often ignored, because it is a relatively small number when discussing the issue.

For quantum channel with noise, the security of BB84-QKD scheme also needs to be supplemented by ideal single photon source. That requires a signal within each time quantum signal source at most only issue a photon. if single photon source is replaced by a weak laser pulse in achievement of BB84 quantum key distribution scheme, its absolute security is threatened. Particularly in the quantum channel transmission of high losses, if the number of photons in a weak pulse contained in more than one. Then there may be a leakage of quantum information. Thus there are some security issues when the weak laser pulses instead of a single photon source to achieve BB84 quantum key distribution scheme in the fiber.

key distribution scheme based on the nonlocality and correlation of a quantum entanglement particle system

An entangled particle system in addition to have a superposition of quantum states, it also has some special features in quantum, which have more research value and information than a single particle and. Relevance and nonlocality of quantum entanglement make the quantum secure direct communication possible.

In the key distribution schemes based on the a quantum entanglement particle system, the most representative of the three programs can be described as followings: (1). Ekert proposed Ekert quantum key distribution scheme in 1991[8]. (2). In 1992, Bennett, Brassard and Mermin's made some modifications to Ekert91, which can be announced as BBM92[9]. (3). Long and Liu proposed a QKD scheme based on the EPR pairs in 2002[10].

Among them, the first based on entangled particles QKD scheme in history, is Ekert protocol scheme which is presented by Ekert of the University of Oxford. Its safety is judged by the famous Bell inequality [11]. Quantum signal in entanglement may violate Bell's inequality, but quantum signal not in entanglement does not violate Bell's inequality.

Physical principles of Ekert protocol scheme. Two particles in the quantum entanglement emitted by the signal source is sent separately to the sender Alice and the receiver Bob. Or quantum signals are prepared by the sender Alice, then send B particles to the recipient Bob. Alice and Bob randomly selects two sets of measurement group ($\oplus$ and $\otimes$) to measure the particles in their hands. Similar to the BB84-QKD scheme, When they use the same measurement group, their results are associated.

For part of the entangled particles pair. They can use a single particle in more than one directions measuring. According to the measurement results from multi-directional single particle to do analysis in Bell's inequality, in order to determine whether someone eavesdropping quantum channel.

$$E(\vec{a}_i,\vec{b}_j)=P_{++}(\vec{a}_i,\vec{b}_j)+P_{--}(\vec{a}_i,\vec{b}_j)P_{+-}(\vec{a}_i,\vec{b}_j)+P_{-+}(\vec{a}_i,\vec{b}_j) \tag{2}$$

$i, j = 1,2,3$, Indeed, $E(\vec{a}_i,\vec{b}_j)$ means Alice on $\vec{a}_i$、Bob on $\vec{b}_j$ measure A and B to give the expected value of the measurement, $P_{++}(\vec{a}_i,\vec{b}_j)$ means Alice on $\vec{a}_i$、Bob on $\vec{b}_j$ measure particle A and B to get the chance to spin the basic upward.

According to quantum mechanics, under the state of $\left|\psi^-\right\rangle_{AB}=\frac{1}{\sqrt{2}}(\left|01\right\rangle_{AB}-\left|10\right\rangle_{AB})$,

$$E(\vec{a}_i,\vec{b}_j)=-\vec{a}_i\cdot\vec{b}_j \tag{3}$$

According CHSH inequality, defined polarization correlation function S

$$S = E(\vec{a_1}, \vec{b_1}) - E(\vec{a_1}, \vec{b_3}) + E(\vec{a_3}, \vec{b_1}) + E(\vec{a_3}, \vec{b_3}) \tag{4}$$

$\left\{\vec{a_1}, \vec{a_2}, \vec{a_3}\right\}$ and $\left\{\vec{b_1}, \vec{b_2}, \vec{b_3}\right\}$ corresponds direction angle Respectively is $\left\{\phi_1^a = 0, \phi_2^a = \frac{\pi}{4}, \phi_3^a = \frac{\pi}{2}\right\}$ and $\left\{\phi_1^b = \frac{\pi}{4}, \phi_2^b = \frac{\pi}{2}, \phi_3^b = \frac{3\pi}{4}\right\}$.

According to quantum mechanics, In the ideal case, S = $2\sqrt{2}$. Due to the special quantum properties of particles entangled system, if an eavesdropper Eve eavesdropping on the quantum channel, her behavior would undermine the relevance of the communication between the two sides of the measurement results. That is, if no one bugs quantum channel, in principle, the measurements in the two communication sides from multi-directional single-particle can violate CHSH inequality. If there is eavesdropping, then the measurement results between A and B would have to comply with CHSH inequality on the contrary,

Advantages and Disadvantages of Ekert Protocol Scheme: The biggest advantage of Ekert 91 QKD scheme is that noise is present regardless of the quantum channel, it can safely generate keys. This is guaranteed by quantum mechanics.

The disadvantage is that: just as the BB84QKD scheme, communication between the parties randomly selects two sets of measurement group (and) to measure the particles in their hands. Thus there is a 50% non-associated measurement result, so that the correspondence between them can not be determined, therefore this part of the result would be left out. In addition, the total bit information transmission efficiency is very low(< 25%).

key distribution scheme based on a system within entangled particles and single-particle quantum system.

The principle of a key distribution scheme based on a system within entangled particles and single-particle quantum system, which combines the properties of a single particle and quantum entangled particle system, the main idea is to make an eavesdropper Eve still can not get accurate information quantum signal. In this kind of quantum key distribution scheme, the most representative one is a scheme that Cabello proposed in 2000 which is based on Holevo limit of quantum key distribution network solutions

Principle of Cabello-HolevoProtocol Scheme： in Cabello-Holevo QKD[11], carriers of quantum information can be divided as the following four quantum states:

$$\left|\psi_0\right\rangle = \left|HH\right\rangle \tag{5}$$

$$\left|\psi_1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|HV\right\rangle + \left|VH\right\rangle\right) \tag{6}$$

$$\left|\psi_2\right\rangle = \frac{1}{\sqrt{2}}\left(\left|HV\right\rangle - \left|VH\right\rangle\right) \tag{7}$$

$$\left|\psi_3\right\rangle = \left|VV\right\rangle \tag{8}$$

$|H\rangle$ and $|V\rangle$ Means the polarization state of the photon is in the horizontal direction and a vertical direction respectively. Each quantum signal consists of two photons. Their quantum state is one of the four states above, quantum signals are transmitted in two quantum channels. Photons that transmited in the up-channel can directly get into the quantum channel by Alice side, and photons that transmited in the down-channel need to choose a delay time, to ensure that when the photons that transmited in the down-channel leave security control area of Alice, the photons that transmited in the up-channel have come into the security control area of Bob. In order to enable two-way signal measurement alignment, Bob needs to select an appropriate time delay in the up-channel. To ensure that Eve can not get the two parts of each quantum signal at the same time, communicating parties need to select an appropriate delay time randomly.

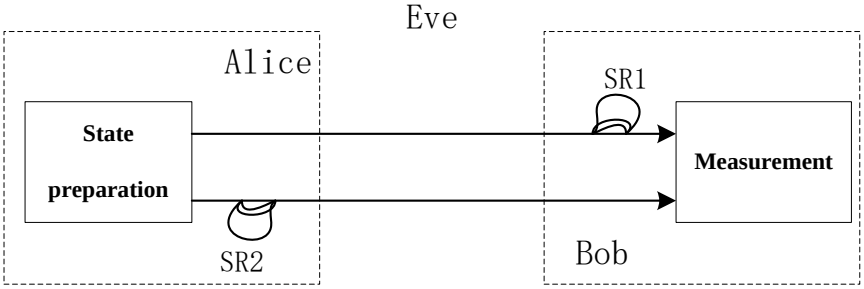

Fig.2 principle of Cabello-Holevo protocol scheme

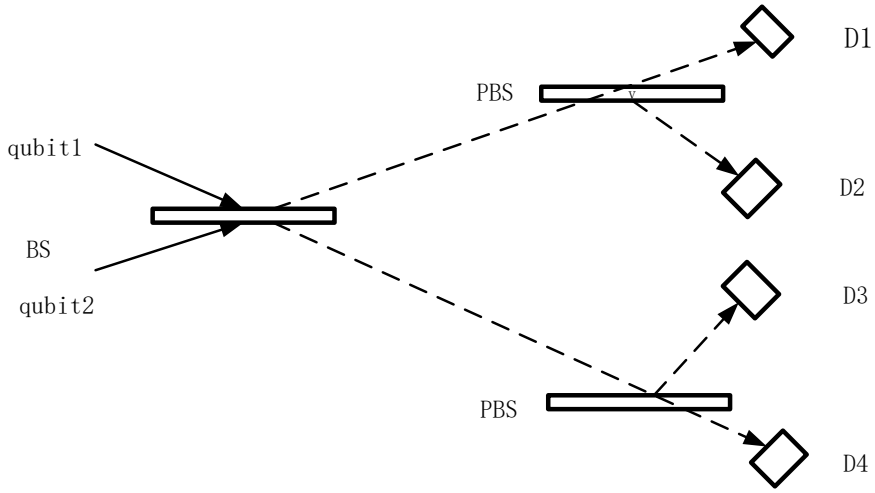

Fig.3 Bob detection system schematic diagram in Cabello-Holevo QKD

Formula (5)-(8) show a set of orthogonal basis vectors, So it is possible to do a complete measurement. Fig 3 shows that Bob detection system schematic diagram in Cabello-Holevo QKD. The BS in Fig.3 is a 50/50 beam slitter, the PBS is a polarization beam splitter, it can transmit horizontally polarized photons and reflect vertically polarized photon. Such correspondence between the four quantum states of the detector response can be announced as follows[11]:

$$|\psi_0\rangle \to \frac{1}{\sqrt{2}}\left(|D_1 D_1\rangle - |D_3 D_3\rangle\right) \tag{9}$$

$$|\psi_1\rangle \to \frac{1}{\sqrt{2}}\left(|D_1 D_2\rangle - |D_3 D_4\rangle\right) \tag{10}$$

$$|\psi_2\rangle \to \frac{1}{\sqrt{2}}\left(|D_2 D_3\rangle - |D_1 D_4\rangle\right) \tag{11}$$

$$|\psi_3\rangle \to \frac{1}{\sqrt{2}}\left(|D_2 D_2\rangle - |D_4 D_4\rangle\right) \tag{12}$$

So Bob can read the quantum state of photons over transmission from Alice accurately.

From the principle point of view, in Cabello-Holevo QKD, because Eve did not know the specific delay time that Alice and Bob choose, Eve could not get all the quantum signals, complete information in quantum state can not be tapped as well[11].

Summary

Quantum communication technology is based on the basic principles of quantum mechanics. In quantum states as a carrier to achieve high-performance, encryption of traditional transmission of information. Its typical feature is the strict security that is guaranteed by quantum mechanics. It is also the hot and difficult point in Network Communications Research currently. In this paper, related issues in quantum key distribution communication system have been studied and discussed in depth. The following aspects have been come to conclusions specifically.

(1)Based on extensive references, research background, current research of the quantum communication technology have been summarized and analyzed.

(2)In quantum key distribution, the different sources will depend on the characteristics of different quantum and quantum principles to ensure the security of communications. Separately, Elaborated the BB84 protocol scheme, Ekerts scheme and Cabello-Holevo QKD protocol scheme as representative. The theoretical principles, protocol analysis and other aspects of the advantages and disadvantages of them have been discussed in this paper.

References

[1] Wootters WK and Zurek WH. A single quantum cannot be cloned. Nature, 1982, 299:802–803.

[2] Bennett CH and Brassard G. Quantum cryptography: public key distribution and coin toss-ing. Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York), 1984:175–179.

[3] Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 1992, 68:3121–3124.

[4] Hwang WY, Koh IG and Han YD. Quantum cryptography without public announcement of bases. Phys. Lett. A, 1998, 244:489–494.

[5] Lo HK. Simple proof of the unconditional security of quantum key distribution. J. Phys. A: mathematical and general, 2001, 34:6957–6967.

[6] Xiao L, Long GL, Deng FG et al. Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A, 2004, 69(5):052307.

[7] Long GL and Liu XS. Theoretically efficient high-capacity quantum-key-distribution schemes. Phys. Rev. A, 2002, 65:032302.

[8] Ekert AK. Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett., 1991, 67:661–663.

[9] Bennett CH, Brassard G and Mermin ND. Quantum cryptography without Bell’s theorem. Phys. Rev. Lett., 1992, 68:557–669.

[10] Long GL and Liu XS. Theoretically efficient high-capacity quantum-key-distribution schemes. Phys. Rev. A, 2002, 65:032302.

[11] Shi BS, Jiang YK and Guo GC. Quantum key distribution using different-frequency pho-tons. Appl. Phys. B, 2000, 70:415–417.