Concurrent quantum key distribution using quantum teleportation and time division multiplexing

Xie Wu[1]*, Ouyang Shan[1, 2], Hailin Xiao[2]

[1]*School of Electronic Engineering, Xidian University, 710071, Xi'an, China*

[2]*School of Information and Communication, Guilin University of Electronic Technology, 541004, Guilin, China*

Received 1 May 2014, www.cmnt.lv

Abstract

In view of the problem that it is difficult to use only one typical channel to deal with many quantum channels during multi-channel QKD (Quantum Key Distribution), the method of TDM (Time Division Multiplexing) in typical channel is introduced to construct a new CQKD (concurrent QKD) system. Using multi-channel quantum teleportation, every concurrent quantum channel is mapped to a time slot of TDM. The results of case study with EPR (Einstein-Podolsky-Rosen) pairs show that this problem can be solved with the CQKD methods. Moreover, this CQKD scheme also has the advantage of unconditional security, while the QKD bit rates can be improved. It opens a new way to develop large-capacity long-distance quantum secure communications.

Keywords: quantum information security, concurrent quantum key distribution, quantum teleportation, time division multiplexing

1 Introduction

QKD (Quantum Key Distribution) is a newly emerging information security technique to get quantum keys by sending and receiving unknown quantum bits. It is a very important approach to implement quantum information security based on the interdisciplinary fields of quantum cryptology, quantum computation, quantum mechanics, quantum communication and traditional communication. As one of the strongest guarantees to transmit the secure information of unknown quantum bits for quantum keys, it is also becoming the core part of modern cryptology. Since Bennett and Brassard presented the first QKD protocol in 1984 [1], scholars from many countries have dealt with the theories and technologies of QKD, and a lot of important fruits have been achieved. Some valuable research progresses have been achieved in such fields as BB (Bennett-Brassard) 84 protocol [1], Bennett 92 protocol [2], BBM (Bennett-Brassard-Mermin) 92 protocol [3], Ekert 91 protocol [4] and the QKD protocol via quantum teleportation [5-6], etc.

These developments have promoted greatly the QKD techniques to the actual application. Since the quantum cryptogram technology via QKD is a crucial kind of physical cryptography in the world, the QKD systems have a wide range of competitive strategies applications in such fields as military affairs or wars, business, communication, finance, government, etc. Compared with traditional secure communications, the quantum channel capacities of QKD are far smaller, and the corresponding quantum bit rates of QKD are far lower. In recent years, to improve the performances of quantum communication, the multi-channel or parallel QKD techniques were introduced to the fields of quantum information security. For instance, in 2012, Antonio et al [7] combined the WDM (Wavelength Division Multiplexing) and SCM (Subcarrier Multiplexed) techniques to implement microwave photonics parallel QKD. The multiple keys can be delivered, and the final key rate can be increased, which affords the way to multi-QKD in optical fibre networks. In 2013, Zhao et al [8] utilized the forward spectral filtering structure and presented a scheme of parallel QKD, and the shared key generation rate could be increased enhanced several times in theory. Fang et al presented a CV (continuous variable) parallel QKD scheme with the subcarrier multiplexing technique in 2014 [9], and the total secret key rate was increased. In addition, MIMO (Multiple-Input Multiple-Output)-QKD [10-12] and subcarrier multiplexing QKD [9, 13-16] have also been developed to improve quantum channels. These QKD researches above are the early work of multi-channel QKD system with lots of active exploration and significant progresses. These QKD schemes not only remain the advantage of the unconditional security, but also have great capacity of quantum channels. Multi-channel QKD is becoming novel potential footholds of the most powerful quantum cryptography among diverse information security ways, providing much theoretical and technical support for the developments and designs of long-distance large-capacity QKD systems.

Unfortunately, the quantum channels in these multi-channel QKD schemes are considered more, while the indispensable typical channels are not emphasized much. Only one classical channel is not enough to be mapped to every quantum channels. The quantum key transmission in each quantum channel needs the help of the busy essential

*[*]**Corresponding author*** e-mail: xiewu588@126.com

classical channel, which are worth improving. In addition, the quantum computations processes of these multi-channel QKD schemes are very complicate lacking unified explicit quantum channel models. As a result, there are some troubles in practical applications and universal generalizations. From the development perspective of the current quantum technologies, the physical mechanisms of this multi-channel QKD system are so intricate that it has been still in the primary stage. The corresponding successful physical experiments of multi-channel QKD system are not many.

Therefore, motivated by ideas of the parallel QKD [7-9], MIMO-QKD [10-12], subcarrier multiplexing QKD [9, 13-16], QKD via quantum teleportation [5, 6], this paper introduces a novel CQKD (Concurrent QKD) system by applying TDM (time division multiplexing) method in the classical channel and concurrent quantum teleportation as multiple quantum channels. Differently from the QKD schemes [7-16], the quantum key string is transmitted currently by dividing the string into several sub-strings with CQKD. At a certain moment, one of concurrent quantum channels is processed, and the time slot resources of TDM typical channel are utilized fully.

This remainder of this paper is arranged as follows. In Section 2, the CQKD system is constructed using quantum entangled states to teleport multiple unknown quantum states, and Section 3 provides the case study of CQKD system by teleporting unknown quantum states of keys with several EPR (Einstein-Podolsky-Rosen) pairs. The performances of the CQKD are analysed in section 4. Finally in section 5, a brief summary is followed.

2 CQKD system using quantum teleportation and TDM

This CQKD system involves the process that legal sender (Alice) and receiver (Bob) send, transmit and obtain quantum keys through multiple quantum channels. The quantum states of the transmission performance by quantum mechanics are used as quantum information carriers. The core approaches to deal with the steps of CQKD are the quantum keys to transmit in every quantum channels with unknown quantum states. The CQKD system can be implemented using the quantum codebook of concurrent quantum key transmissions.

2.1 THE WHOLE SCHEMATIC CONSTRUCTION OF CQKD SYSTEM USING TDM AND QUANTUM TELEPORTATION

CQKD itself is a highly complex quantum system with the transmission of unknown quantum bits via quantum channels. It is also a difficult structural quantum project for physical experiments. From QKD to CQKD system, a potential problem occurs that it is very difficult to arrange and combine the complicate photonic components for the given QKD system, e.g. BS (Beam Splitter), PBS (polarizing beam splitter), BSM (Bell-state measurement), BBO (Beta Barium Borate) crystal, detectors and etc. In contrast to single channel QKD, it is meaningful to construct the CQKD for the unavoidable fact that the quantum components of CQKD are worth exploring.

To take advantage of high key rates of multi-channel quantum communication and explore novel approaches to transmit quantum key information in several quantum channels, the TDM technology is adopted in the classical channel, and a new CQKD system scheme is constructed as shown in Figure 1 by using quantum teleportation as concurrent quantum channels with quantum entangled states.

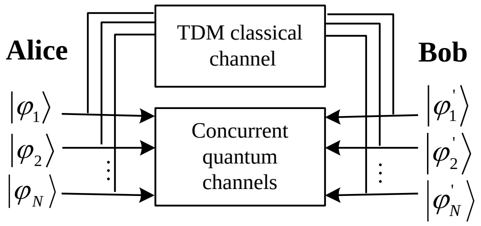

FIGURE 1 the whole schematic construction of CQKD system

Quantum key information of unknown quantum bits is transmitted through concurrent quantum channels. The concurrent processes of QKD can be implemented with N (N is a positive integer) quantum channels. The inputs are the unknown quantum states, while the outputs are the corresponding duplications of these inputs by teleportation with entangled states.

The quantum sources in Figure 1 are discrete with the representations as $|\varphi_1\rangle$, $|\varphi_2\rangle$, … , $|\varphi_N\rangle$, while the destinations are denoted as $|\varphi_1'\rangle$, $|\varphi_2'\rangle$, … , $|\varphi_N'\rangle$. The distances between any two senders (or receivers) are enough without mutual influences or interactions. The number of the senders and receivers of this CQKD system is less than the maximum amount of TDM slots.

2.2 QUANTUM CHANNELS OF CQKD SYSTEM VIA QUANTUM TELEPORTATION

It is feasible to construct the CQKD system via multi-channel quantum teleportation. The characteristics of quantum entangled states with some advantages from microscopic particle world as quantum entanglement resource can be utilized to construct the CQKD system. Therefore, it is necessary to utilize these good properties of quantum entangled particles to design and describe the CQKD system scheme for long-distance key transmission. The concurrent quantum channels can be mapped by diverse quantum entanglement sources, such as EPR states, GHZ (Greenberger-Horne-Zeilinger) states, W states, etc. The transmission distances of quantum bits for quantum key are not limited any more in theory. In quantum channels, no information carriers of quantum key and channels of physical systems for CQKD system interact and influence mutually, and different quantum systems for EPR pairs, GHZ states or W states are often handled differently.

For a CQKD system, the quantum bits are sent and received through multiple quantum channels for a period of time. The channels include TDM typical channel and multiple quantum entangled channels with entangled states. The latter is devised as Figure 2 to illustrate the concurrent processes for QKD with quantum entangled states via concurrent quantum teleportation.

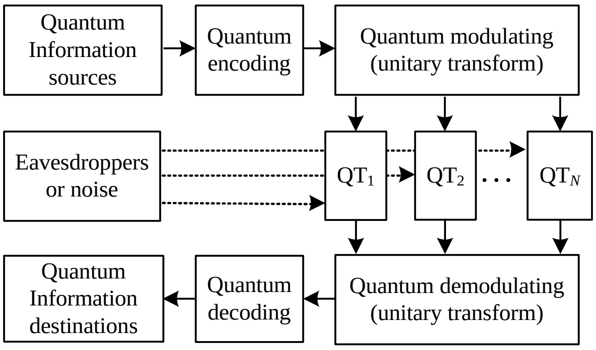
Quantum Information sources
Quantum encoding
Quantum modulating (unitary transform)
Eavesdroppers or noise
QT$_1$
QT$_2$
QT$_N$
Quantum Information destinations
Quantum decoding
Quantum demodulating (unitary transform)

FIGURE 2 Concurrent quantum channels of the CQKD system via quantum teleportation (QT)

The CQKD system in Figure 2 consists of quantum information sources, multiple quantum channels and information destinations. The antennas used in traditional multi-channel communication systems are replaced with several quantum channels where the concurrent quantum bits information is transmitted from the sender to the receiver. The quantum information sources and quantum information destinations are unknown quantum states for quantum keys with the corresponding quantum encoding and quantum decoding processes. The information sources are some quantum bits as the inputs of the CQKD system for Alice, while the outputs are the information destinations as the transmitted results of those quantum bits for Bob. During teleporting of quantum unknown states, the quantum bits of quantum keys in Figure 2 needs modulating and demodulating with unitary transforms.

It is necessary to construct the input-output model of CQKD system using quantum teleportation. Although there are no unified quantitative quantum channel models for the existing multi-channel QKD schemes. Most researchers' schemes for these kinds of QKD system are oriented to their own complex quantum systems, lacking the common formulae of quantum channels. The derivation processes of current theoretical formulae of multi-channel QKD system are exceedingly complicated. It is hard to calculate and compare general quantitative performance indices for QKD. The quantum channels with different quantum carriers are too complicate to describe just like common communications models. Yet, CQKD system emphasizes its multiple inputs and multiple outputs since the inner interacts are too complicate to operate and compute without the unified concept of multi-channel QKD. To abstract the problem of CQKD system with mathematical methods and describe the transmission process of quantum key bits in theory, the CQKD system of N quantum channels is modelled with the abstract input-output relationship between the senders and the receivers. If none of quantum channels are disturbed by various factors (such as environmental influence, etc.), the general explicit input-output model with quantum entangled states in Figure 1 can be represented as:

$$\begin{bmatrix} |\varphi_1'\rangle \\ |\varphi_2'\rangle \\ \vdots \\ |\varphi_N'\rangle \end{bmatrix} = \begin{bmatrix} \boldsymbol{P}(1|1) & \boldsymbol{P}(1|2) & \cdots & \boldsymbol{P}(1|N) \\ \boldsymbol{P}(2|1) & \boldsymbol{P}(2|2) & \cdots & \boldsymbol{P}(2|N) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{P}(N|1) & \boldsymbol{P}(N|2) & \cdots & \boldsymbol{P}(N|N) \end{bmatrix} \begin{bmatrix} |\varphi_1\rangle \\ |\varphi_2\rangle \\ \vdots \\ |\varphi_N\rangle \end{bmatrix}, \quad (1)$$

where $\boldsymbol{P}(i\,|\,j)$ means the operation $\boldsymbol{P}_{ij}|\varphi_i\rangle \to |\varphi_j'\rangle$ in terms of a series of unitary transforms ($\boldsymbol{P}_{ij}$) $i, j = 1, 2, \ldots, N$.

If there is no disturbs in each ideal quantum channel with some independent irrelevant discrete quantum entanglement sources, the input-output model can be simplified as follows:

$$\begin{bmatrix} |\varphi_1'\rangle \\ |\varphi_2'\rangle \\ \vdots \\ |\varphi_N'\rangle \end{bmatrix} = \begin{bmatrix} \boldsymbol{P}(1|1) & 0 & \cdots & 0 \\ 0 & \boldsymbol{P}(2|2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{P}(N|N) \end{bmatrix} \begin{bmatrix} |\varphi_1\rangle \\ |\varphi_2\rangle \\ \vdots \\ |\varphi_N\rangle \end{bmatrix}. \quad (2)$$

In a certain quantum channel, $|\varphi_j'\rangle$ is the input unknown quantum bit which carries the quantum key information to the output $|\varphi_j'\rangle$. The input-output relations of multiple quantum channels are determined by the variable $\boldsymbol{P}(i\,|\,j)$. According to quantum mechanics, $\boldsymbol{P}(i\,|\,j)$ are the results of a series of unitary transforms which are implemented in physics, which depends on the physical characteristics of quantum channels for CQKD.

2.3 EAVESDROPPING ANALYSIS OF CQKD SYSTEM IN QUANTUM CHANNELS AND TDM CLASSICAL CHANNEL

For the CQKD system, eavesdropping detection is essential in every quantum channels. The error quantum bits for CQKD can be from eavesdroppers and environment noise, which need to be distinguished. Although the quantum key transmission processes for CQKD are affected by environmental noise. For instance, the quantum key transmission in free space may be interfered by high buildings, mountains, dust, atmosphere and noise, etc. Yet concurrent quantum teleportation of unknown quantum bits in free space are affected little by environmental factors. The quantum bits information during teleporting in multiple quantum channels almost has little decay if the quantum entanglement sources are not affected. Potential noise in quantum channels for entangled states differs in free space or optical fibre. So, eavesdropping analysis for CQKD is crucial to obtain correct quantum bits of quantum keys.

Alice often transmits much quantum key information to Bob, and Bob then detects and determines the correctness of the received quantum bits. Alice and Bob need to identify the input and output parameters of quantum states in concurrent quantum channels. They also have to check whether the quantum key bits in concurrent quantum channels are influenced by the eavesdroppers during transmitting the keys. According to the theory of quantum signal detection, the behaviours of eavesdropping can be detectable in quantum systems. For a CQKD system, any eavesdropping in quantum channels will leave traces, providing the chance to detect the error quantum bits information. The quantum keys during concurrent quantum teleportation may be affected by potential eavesdroppers. According to the no-cloning quantum principle, none of them can copy accurately unknown quantum states which are adopted as information sources of this CQKD system. So, whenever the quantum channels between Alice and the Bob for the CQKD system are affected or eavesdropped on, Eve can be detected. In addition, data correction and privacy enhancing process are also required to realize CQKD.

3 Case study of CQKD system by concurrent quantum teleportation with EPR pairs and TDM

The quantum computing processes of a CQKD system need much work, and it is difficult to abstract the unified multiple channel models just like multi-channel quantum communications and the typical communication schemes [7-16]. It is also hard to achieve and solve universal general computational formulas and variables.

In order to simplify and derive the complex computation processes for the CQKD system, the quantum teleportation with EPR pairs are taken as an example of concurrent quantum channels to research the CQKD system according to Equation (2). So, for simply, it is supposed that there are no interacts in multiple quantum channels. Such quantum entanglement states as EPR states are taken as the transmission medium of the unknown quantum state to deal with quantum key bits by concurrent quantum teleportation just for the CQKD system.

3.1 SCHEME OF CQKD SYSTEM VIA CONCURRENT QUANTUM TELEPORTATION WITH EPR PAIRS

For the implementation for the detailed multiple quantum transmission of quantum keys with unknown quantum states, the antennae used in traditional multi-channel communications are replaced with multiple independent purified EPR pairs by the corresponding relationships between the quantum channels and quantum entangled states. These EPR pairs are mapped into the quantum channels for the CQKD system. The classical channel used in the quantum teleportation is divided into many time slots with the way from classical communications (such as a telephone), and the CQKD system scheme with EPR pairs is constructed and shown in Figure 3. Alice and Bob identify, negotiate and determine the unknown quantum bits of QKD through TDM typical channel.

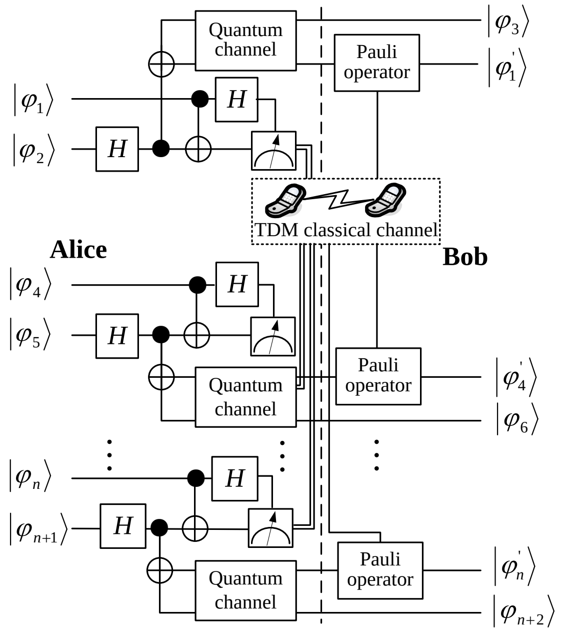

FIGURE 3 CQKD system by quantum teleportation with EPR pairs

H is a Hadamard gate, and ⊕ is a control-NOT gate. The quantum bits carrying quantum key information to be transmitted are denoted as the input unknown quantum particles $|\varphi_1\rangle$, $|\varphi_4\rangle$, …, $|\varphi_n\rangle$, while $|\varphi_1'\rangle$, $|\varphi_4'\rangle$, …, $|\varphi_n'\rangle$ is the corresponding outputs.

The EPR pairs in concurrent quantum channels are represented as $|\varphi_2\rangle$ and $|\varphi_3\rangle$, $|\varphi_5\rangle$ and $|\varphi_6\rangle$,… ,$|\varphi_{n+1}\rangle$ and $|\varphi_{n+2}\rangle$, which are from corresponding purified homotype independent quantum entangled sources. *n* is a positive integer.

Alice and Bob can implement remote quantum correlations with quantum entanglement states. To construct concurrent quantum channels, they can select purified entanglement photon sources to produce EPR pairs with polarization photos as the multiple quantum channels for the CQKD system.

3.2 PROCESSES OF CQKD SYSTEM VIA QUANTUM TELEPORTATION WITH EPR PAIRS

For simplification, three quantum channels for quantum communication are taken as examples to describe the principle of a CQKD system scheme to obtain the input-output transformations relations during the concurrent quantum key transmissions. The process of this scheme via concurrent teleportation with EPR pairs can be divided into the following steps as the main contents of the protocol [5, 6] for the CQKD system.

Firstly, unknown quantum states and EPR entangled pairs are prepared for the CQKD system. Assuming some independent purified quantum entangled photon sources are prepared in three quantum channels, and these EPR pairs are transmitted to Alice and Bob in the opposite direction respectively. As a result, Alice has quantum particles $|\varphi_2\rangle$, $|\varphi_5\rangle$ and $|\varphi_8\rangle$, while Bob holds the responding quantum particles $|\varphi_3\rangle$ and $|\varphi_6\rangle$, $|\varphi_9\rangle$. The initial quantum states of these EPR pairs are supposed as the following Bell states:

$$|\beta_{00}\rangle_{23} = |\Phi^+\rangle_{23} = \left(|00\rangle_{23} + |11\rangle_{23}\right)/\sqrt{2}, \qquad (3)$$

$$|\beta_{01}\rangle_{56} = |\Psi^+\rangle_{56} = \left(|01\rangle_{56} + |10\rangle_{56}\right)/\sqrt{2}, \qquad (4)$$

$$|\beta_{10}\rangle_{89} = |\Phi^-\rangle_{89} = \left(|00\rangle_{89} - |11\rangle_{89}\right)/\sqrt{2}, \qquad (5)$$

where 23, 56 and 89 are denoted as three pairs of quantum entangled particles respectively.

The quantum key information is contained in three unknown quantum particles $|\phi_1\rangle$, $|\phi_4\rangle$ and $|\phi_7\rangle$ which initial states are represented as:

$$|\varphi_1\rangle = a|0_1\rangle + b|1_1\rangle, \qquad (6)$$

$$|\varphi_4\rangle = c|0_4\rangle + d|1_4\rangle, \qquad (7)$$

$$|\varphi_7\rangle = e|0_7\rangle + f|1_7\rangle, \qquad (8)$$

where *a*, *b*, *c*, *d*, *e* and *f* are complex coefficients.

Theoretically, Alice and Bob are entangled through any quantum channels no matter how far away they are. So, the CQKD through quantum teleportation in every sub-channel is ready and practicable, and the quantum bit information is prepared to be transmitted and gained with a certain probability via quantum entangled states.

Secondly, unknown quantum states through EPR states are teleported and duplicated across three concurrent quantum channels. Alice and Bob teleport unknown quantum bit information for quantum keys in each quantum channel during different time slots of the TDM classical channel. The classical channel is divided into several discrete periodic time slots, so that Alice and Bob can observe and measure quantum entangled states to determine legal quantum bits for the CQKD system with the same physical connection of different TDM time slots.

During these time slots, Alice chooses unknown particles (such as $|\phi_1\rangle$, $|\phi_4\rangle$ and $|\phi_7\rangle$) to perform the joint measurement operations with the corresponding EPR pairs $|\phi_2\rangle$ and $|\phi_3\rangle$, $|\phi_5\rangle$ and $|\phi_6\rangle$, $|\phi_8\rangle$ and $|\phi_9\rangle$ respectively, that is, the tensor products are performed:

$$\begin{bmatrix} |\varphi_{123}\rangle \\ |\varphi_{456}\rangle \\ |\varphi_{789}\rangle \end{bmatrix} = \begin{bmatrix} \left(a|0_1\rangle + b|1_1\rangle\right) \otimes \left(|00\rangle_{23} + |11\rangle_{23}\right)/\sqrt{2} \\ \left(c|0_4\rangle + d|1_4\rangle\right) \otimes \left(|01\rangle_{56} + |10\rangle_{56}\right)/\sqrt{2} \\ \left(e|0_7\rangle + f|1_7\rangle\right) \otimes \left(|00\rangle_{89} - |11\rangle_{89}\right)/\sqrt{2} \end{bmatrix}. \qquad (9)$$

According to quantum mechanics, these joint quantum measurement operations will result in the instant collapse changes of each EPR pairs during the corresponding time slot, and the quantum entanglement between Alice and Bob are disentangled, while $|\phi_1\rangle$ and $|\phi_2\rangle$, $|\phi_4\rangle$ and $|\phi_5\rangle$, $|\phi_7\rangle$ and $|\phi_8\rangle$ are entangled separately. So, these quantum information of $|\phi_3\rangle$, $|\phi_6\rangle$ and $|\phi_9\rangle$ for Bob need separating, and the results are the following.

$$\begin{bmatrix} |\varphi_{123}\rangle \\ |\varphi_{456}\rangle \\ |\varphi_{789}\rangle \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} (a|00\rangle_{12} + b|10\rangle_{12})|0\rangle_3 + (a|01\rangle_{12} + b|11\rangle_{12})|1\rangle_3 \\ (c|01\rangle_{45} + d|11\rangle_{45})|0\rangle_6 + (c|00\rangle_{45} + d|10\rangle_{45})|1\rangle_6 \\ (e|00\rangle_{78} + f|10\rangle_{78})|0\rangle_9 - (e|01\rangle_{78} + f|11\rangle_{78})|1\rangle_9 \end{bmatrix}. \qquad (10)$$

Using the method of dual items, we have:

$$\begin{bmatrix} |\varphi_{123}\rangle \\ |\varphi_{456}\rangle \\ |\varphi_{789}\rangle \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} \begin{pmatrix} (a(|00\rangle_{12} + |11\rangle_{12}) + b(|01\rangle_{12} + |10\rangle_{12}) + a(|00\rangle_{12} - |11\rangle_{12}) + b(-|01\rangle_{12} + |10\rangle_{12}))|0\rangle_3 \\ +(b(|00\rangle_{12} + |11\rangle_{12}) + a(|01\rangle_{12} + |10\rangle_{12}) + b(-|00\rangle_{12} + |11\rangle_{12}) + a(|01\rangle_{12} - |10\rangle_{12}))|1\rangle_3 \end{pmatrix} \\ \begin{pmatrix} (d(|00\rangle_{45} + |11\rangle_{45}) + c(|01\rangle_{45} + |10\rangle_{45}) + d(-|00\rangle_{45} + |11\rangle_{45}) + c(|01\rangle_{45} - |10\rangle_{45}))|0\rangle_6 \\ +(c(|00\rangle_{45} + |11\rangle_{45}) + d(|01\rangle_{45} + |10\rangle_{45}) + c(|00\rangle_{45} - |11\rangle_{45}) + d(-|01\rangle_{45} + |10\rangle_{45}))|1\rangle_6 \end{pmatrix} \\ \begin{pmatrix} (e(|00\rangle_{78} + |11\rangle_{78}) + f(|01\rangle_{78} + |10\rangle_{78}) + e(|00\rangle_{78} - |11\rangle_{78}) + f(-|01\rangle_{78} + |10\rangle_{78}))|0\rangle_9 \\ -f(|00\rangle_{78} + |11\rangle_{78}) - e(|01\rangle_{78} + |10\rangle_{78}) + f(|00\rangle_{78} - |11\rangle_{78}) + e(-|01\rangle_{78} + |10\rangle_{78}))|1\rangle_9 \end{pmatrix} \end{bmatrix}. \qquad (11)$$

Four Bell states are used for Equation (11), and then we can get:

$$\begin{bmatrix} |\varphi_{123}\rangle \\ |\varphi_{456}\rangle \\ |\varphi_{789}\rangle \end{bmatrix} = \frac{1}{2}\begin{bmatrix} \left(|\beta_{00}\rangle_{12}(a|0\rangle_3 + b|1\rangle_3) + |\beta_{01}\rangle_{12}(b|0\rangle_3 + a|1\rangle_3) + |\beta_{10}\rangle_{12}(a|0\rangle_3 - b|1\rangle_3) + |\beta_{11}\rangle_{12}(-b|0\rangle_3 + a|1\rangle_3)\right) \\ \left(|\beta_{00}\rangle_{45}(d|0\rangle_6 + c|1\rangle_6) + |\beta_{01}\rangle_{45}(c|0\rangle_6 + d|1\rangle_6) + |\beta_{10}\rangle_{45}(-d|0\rangle_6 + c|1\rangle_6) + |\beta_{11}\rangle_{45}(c|0\rangle_6 - d|1\rangle_6)\right) \\ \left((e|\beta_{00}\rangle_{78} + f|\beta_{01}\rangle_{78} + e|\beta_{10}\rangle_{78} - f|\beta_{11}\rangle_{78})|0\rangle_9 + (-f|\beta_{00}\rangle_{78} - e|\beta_{01}\rangle_{78} + f|\beta_{10}\rangle_{78} - e|\beta_{11}\rangle_{78})|1\rangle_9\right) \end{bmatrix}. \qquad (12)$$

The Equations (6)-(8) of the unknown particles are substituted into Equation (12), and the three-channel CQKD system via teleportation is expressed as Equation (13):

$$\begin{bmatrix} |\varphi_{123}\rangle \\ |\varphi_{456}\rangle \\ |\varphi_{789}\rangle \end{bmatrix} = \frac{1}{2}\begin{bmatrix} \left(|\beta_{00}\rangle_{12}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}|\varphi_3\rangle + |\beta_{01}\rangle_{12}\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}|\varphi_3\rangle + |\beta_{10}\rangle_{12}\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}|\varphi_3\rangle + |\beta_{11}\rangle_{12}\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}|\varphi_3\rangle\right) \\ \left(|\beta_{00}\rangle_{45}\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}|\varphi_6\rangle + |\beta_{01}\rangle_{45}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}|\varphi_6\rangle + |\beta_{10}\rangle_{45}\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}|\varphi_6\rangle + |\beta_{11}\rangle_{45}\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}|\varphi_6\rangle\right) \\ \left(|\beta_{00}\rangle_{78}\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}|\varphi_9\rangle + |\beta_{01}\rangle_{78}\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}|\varphi_9\rangle + |\beta_{10}\rangle_{78}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}|\varphi_9\rangle + |\beta_{11}\rangle_{78}\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}|\varphi_9\rangle\right) \end{bmatrix}. \qquad (13)$$

Using inverse unitary transform, Bob can duplicates the unknown quantum states $|\phi_1^{'}\rangle$, $|\phi_4^{'}\rangle$, $|\phi_7^{'}\rangle$ according to Equation (13), and $\boldsymbol{P}(i\,|\,j)$ in Equation (2) can be implemented. Consequently, the concurrent unknown quantum bits for quantum keys are transmitted from Alice to Bob.

Thirdly, quantum keys are obtained from these teleported unknown quantum states for CQKD system. Through the typical channel, Alice and Bob compare and find out those transmitted quantum bits where the measurement bases are the same during the time slot of the classical channel. They choose effective unknown quantum bits by identical measurement bases to establish the codebook for QKD. The QKD protocols [5, 6] of quantum teleportation can be adopted, and Eve can be checked whether they exist in each quantum channel or not. When the quantum channel is not eavesdropped on, the quantum bits for the corresponding QKD are legal, or the transmitted quantum bits have to be cancelled. By transmitting constantly unknown quantum states, the quantum bit string can be gained and determine whether the transmission process is effective to carry out the collection of quantum key information. After quantum error correcting code and privacy amplification, Alice and Bob combine the effective unknown quantum bits from concurrent quantum channel to build the codebook for the quantum key of the CQKD system.

Thus, results of three-channel CQKD system by concurrent quantum teleportation with EPR pairs are obtained as Equation (13). It is worth mentioning that the CQKD systems of four or more concurrent quantum channels are similar through those quantum channels of EPR pairs and TDM classical channel. The input-output relationship in Equation (13) is also in accordance with the quantum channel model of Equation (2), and the former can be generalized to the CQKD of *N* quantum channels under the ideal condition of no environmental impacts.

4 Discussion

Similarly, with the existing multi-channel QKD schemes, the CQKD system in this paper also has unconditional security according to the Heisenberg uncertainty principle and the quantum no-cloning theorem. Moreover, this CQKD scheme in our work brings two other advantages.

Firstly, QKD can be implemented through concurrent quantum channels in the CQKD system by TDM methods. Every quantum channel can be mapped with a time slots of classical channel for Alice and Bob to exchange the information of quantum states and measure bases. From the concurrent quantum channels of the instance with EPR pairs, not only the input-output models of are simpler than the multi-channel QKD schemes, but also the concurrent quantum teleportation process of unknown quantum bits can be implemented. So, the CQKD system has the crucial factors of TDM time slots for successful quantum keys, and the time slot resource is utilized fully.

Secondly, this CQKD system improves the performance of QKD bit rates. For the QKD scheme of only one typical channel, the error (from eavesdroppers) probability during transmitting unknown quantum bits is denoted as p_e, then the ideal maximum successful probability of QKD for Alice and Bob is $1 - p_e$ at a time. $0 \le p_e \le 1$. In contrast, for this CQKD system with TDM typical channel, Alice can transmit the quantum key information by teleporting multiple unknown quantum states to Bob when one or more of concurrent quantum channels are available. For instance, for a CQKD system of *N* irrelevant quantum channels, if the classical channel is divided into *N* time slots, then the ideal maximum successful probability of QKD is $1 - p_e^N$ at a time. So, the maximum probability for Alice and Bob to implement successful transmissions of unknown quantum bits for CQKD rises greatly with the increasing number of concurrent quantum channel. So, the high QKD bit rates for the CQKD system can be obtained by TDM technology, which was not be guaranteed with only one classical channel for every quantum channels before.

5 Conclusion

In this paper, the problem of only one typical channel to multiple quantum channels for multi-channel QKD schemes has been solved by the CQKD system. The TDM tool is used to ensure the one-to-one mapping of a time slot in classical channel and each quantum channel. The case study of EPR pairs illustrate that the model of CQKD system can be constructed via concurrent quantum teleportation. Performance analyses show that the CQKD system not only has the advantage of unconditional security, but also the QKD bit rates can be enhanced in contrast with the single-channel QKD. With the development of quantum information security, the model of CQKD system can be generalized with GHZ states, W states, etc. This CQKD scheme opens a novel way to develop large-capacity long-distance quantum secure communications.

Acknowledgments

We acknowledge the National Natural Science Foundation of China (Nos. 60972084 and 61261018).

References

[1] Bennett C H, Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proceeding IEEE Intenational Conference on Computers, Systems and Signal Processing* Bangalore India 175-79

[2] Bennett C H 1992 Quantum cryptography using any two nonorthogonal states *Physical Review Letters* **68**(21) 3121-4

[3] Bennett C H, Brassard G, Mermin N D 1992 *Physical Review Letters* **68**(5) 557-9

[4] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Physical Review Letters* **67**(6) 661-3

[5] Song H C, Gong L H, Zhou N R, 2012 Continuous-variable quantum deterministic key distribution protocol based on quantum teleportation *Acta Physica Sinica* **61**(15) 154206 *(in Chinese)*

[6] Zhou N R, Wang L J, Gong L H, Zuo X W, Liu Y 2011 Quantum deterministic key distribution protocols based on teleportation and entanglement swapping *Optics Communications* **284**(19) 4836-4842

[7] Ruiz-Alba A, Mora J, Amaya W, Martinez A, García-Muñoz V, Calvo D, Capmany J 2012 *IEEE Photonics Journal* **4**(3) 931-942

[8] Zhao G H, Zhao S H, Yao Z S, Meng W, Wang X, Zhu Z H, Liu F 2013 Forward spectral filtering parallel quantum key distribution system *Optics Communications* **298-299** 254-9

[9] Fang J, Huang P, Zeng G H 2014 Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation *Physical Review* A **89**(2) 022315

[10] Gabay M, Arnon S 2006 Quantum key distribution by a free-space MIMO system *Journal of Lightwave Technology* **24**(8) 3114-20

[11] Cui G Q, Lu Y, Zeng G H 2009 A new scheme for quantum key distribution in free-space *Preceeding in 15th Asia-Pacific Conference on Communications* Shanghai China 637-40

[12] Xiao H L, Ouyang S, Nie Z P 2009 Capacity of multiple-input-multiple-output quantum key distribution channels *Acta Physica Sinica* **58**(10) 6779-6785 *(in Chinese)*

[13] Ortigosa-Blanch A, Capmany J 2006 Subcarrier multiplexing optical quantum key distribution *Physical Review* A **73**(2) 024305

[14] Mora J, Ruiz-Alba A, Amaya W, Martinez A, García-Muñoz V, Calvo D, Capmany J 2012 Experimental demonstration of subcarrier multiplexed quantum key distribution system *Optics Letters* **37**(11) 2031-3

[15] Zhao G H, Zhao S H, Yao Z S, Meng W, Wang X, Zhu Z H, Liu F 2012 Subcarrier multiplexing quantum key distribution based on polarization coding *Acta Physica Sinica* **61**(24) 240306 *(in Chinese)*

[16] Bhattacharya S, Krishnamurthy P K 2013 Decoy-state method for subcarrier-multiplexed frequency-coded quantum key distribution *Journal of the Optical Society of America B-Optical Physics* 30(4) 782-7

Authors

Xie Wu, born June, 1979, Yichun, Jiangxi Province, P.R. China

Current position, grades: PhD candidate at the School of Electronic Engineering, Xidian University, Xi'an, China. Senior experimentalist at Guilin University of Electronic Technology since 2011.
University studies: BS and MS degrees at Guilin University of Electronic Technology (GUET), China, in 2002 and 2005.
Scientific interests: quantum information security distribution and group theory.
Publications: more than 5 papers.

Ouyang Shan, born in September, 1960, Anfu, Jiangxi Province, P.R. China

Current position, grades: professor at the School of Information and Communications, Guilin University of Electronic Technology (GUET), China.
University studies: MS and PhD degrees in electronic engineering at Xidian University, Xi'an, China, in 1992 and 2000.
Scientific interests: signal processing for communications and radar, adaptive filtering, and neural network learning theory and applications.
Publications: more than 70 papers.

Hailin Xiao, born in June, 1975, Machen, Hubei Province, P.R. China

Current position, grades: professor at the School of Information and Communications, Guilin University of Electronic Technology (GUET), China.
University studies: PhD degree at the University of Electronic Science and Technology of China (UESTC) in 2007.
Scientific interests: MIMO wireless communications, cooperative communications and smart antenna techniques.
Publications: more than 50 papers.