Modeling of Parallel Quantum Key Distribution System *via* UML

Xie Wu*, Ouyang Shan and Xiao Hailin

School of Electronic Engineering, Xidian University, Xi'an, Shaanxi, 710071, P.R. China

Abstract: There is a problem that it is difficult to express and understand the PQKD (Parallel Quantum Key Distribution) processes with quantum entanglement states for its novelty and complexity. To solve this problem, the control idea is adopted to model the PQKD system for the design of the corresponding PQKD schemes using the tool of UML (Unified Modeling Language). The results of demon animations by the UML models show that the dynamic processes of PQKD with entangled states can be illustrated more clearly and intuitively than before, while the PQKD control system remains the advantage of unconditional security. These models are important to develop large-capacity long-distance PQKD.

Keywords: Control system, modeling, parallel quantum key distribution, quantum private communication, UML.

1. INTRODUCTION

Parallel quantum key distribution (PQKD) is a quantum private communication approach with several parallelized quantum channels. It plays very important roles in national defense strategy, commercial competition, financial risks control, etc. It has experienced a certain developing progress for about two years. In 2012, Antonio *et al.* utilized MWP (Microwave Photonics) to implement originally two PQKD systems with the WDM (Wavelength Division Multiplexing) and SCM (Subcarrier Multiplexing) techniques respectively [1]. The QBER (Quantum Bit Error Rate) is less than 2% over an 11-km optical fiber link with a sifted key rate of 10 kb/s/channel for their four-independent channel PQKD system. In 2013, Zhao *et al.* [2] presented a PQKD system of a forward spectral filtering structure with the methods of polarization coding, and the corresponding key generation rate can be enhanced theoretically several times. Recently, Fang *et al.* put forward a CV (continuous-variable) PQKD scheme using the approach of SCM in MWP with Gaussian modulation [3], where the maximum transmission distance is shortened slightly by the non-Gaussian extra source noise in eaery channel, yet they increased the whole secret key rate greatly. These researches [1-3] have achieved some good performances in the parallel quantum channels, QKD (Quantum Key Distribution) bit rates and QBER for the PQKD system. These researches are important for the multi-channel and multi-user QKD network, and the transmission of the quantum key bits can be improved by the multiplexing methods.

However, there is a certain problem that corresponding communication processes of unknown quantum bits in the PQKD systems can not be understood easily for their novelty and complexity when the quantum entanglement states are employed in parallel quantum channels. From the work of the PQKD system, it is difficult to obtain the unified formula just like traditional wireless communications. At present, the corresponding mathematical models for the PQKD system are unthinkable for lacking unified theory supports and physical experiments with quantum entangled states. There is much work to do to implement the PQKD system for the developments of quantum private communication.

Therefore, motivated by current PQKD researches [1-3] and the quantum virtual private network [4], the PQKD schemes with quantum entangled states are modeled as a control system in this paper. The relevant communication models to transmit unknown quantum bits of quantum keys are described using UML (Unified Modeling Language).

The remainder of this paper is arranged as follows. Section 2 provides the statistic model of the PQKD control system using a block diagram, and then this block diagram is extended dynamically with the UML sequence diagram, collaboration diagram, state diagram and activity diagram in Section 3. In Section 4, the demon animation is developed to show the quantum bit transmission processes of the PQKD system by these UML diagrams, which performances are discussed. Finally, the brief conclusion appears in Section 5.

2. CONSTRUCTION OF THE PQKD SYSTEM

Generally, a traditional communication system consists of transmitting antennas, wireless channels and receiving antennas. With the development of quantum teleportation [5-7], these antennas can be replaced with the mapped microscopic entanglement particles as quantum channels of the PQKD system. To introduce this new technology to the public, the quantum keys in parallel transmitting processes need modeling, and the corresponding quantum information system is constructed to simplify appropriately the complex quantum communication procedures between Alice (the sender) and Bob (the receiver) by ignoring some unnecessary subsidiary factors.

1874-110X/14 2014 Bentham Open

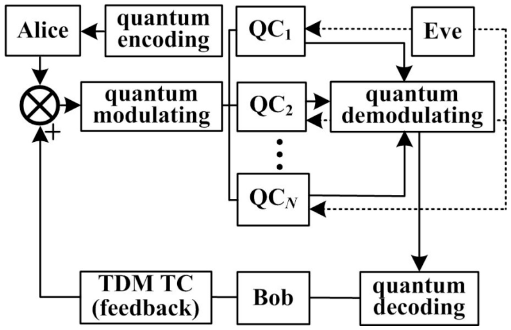


Fig. (1). A brief block diagram of the PQKD control system.

Similarly with the techniques of Ref. [1-3] and MIMO (Multiple-Input Multiple-Output) quantum communications with quantum entangled states [8-10], the block diagram of the PQKD system with a TDM (Time Division Multiplexing) classical channel and several irrelevant parallel quantum channels are designed briefly as shown in Fig. (**1**).

In this PQKD control system, Eve is the disturbance that needs controlling. Alice and Bob can analyze the parallel quantum channels to transmit certain quantum key bits. If most of quantum channels are intercepted by Eve, then this time Alice and Bob can reject the quantum bits for keys *via* the classical communication to control the waste and loss of quantum key bits. They can transmit pseudo-code quantum bits in these quantum channels to cheat Eve next time. So, Eve can not get quantum bits of quantum key. Alice and Bob then implement PQKD in those quantum channels of no Eve. The errors (or deviation) of quantum key bits for two times need controlling. By this kind of control, more and more quantum key bits can be transmitted for PQKD with the control system gain *via* the transfer function increasing.

3. THE MODELS OF THE PQKD SYSTEM *VIA* UML

For the PQKD system, unknown quantum states of quantum key are needed to transmit through independent irrelevant parallel quantum entangled channels in free space or optical fibers between Alice and Bob. The control theory can be introduced to deal with the corresponding quantum keys negotiations in the TDM typical channel.

A system of parallel quantum key transmission with the methods for quantum private communication over parallel quantum channels (*e.g.* photonic channels) between Alice and Bob can be described from the prospective of some event sequences in order. Different time sequences are the main topics for the UML modeling processes, and the users including Alice, Bob and Eve. They need to transmit some messages to control quantum bits during different time slots.

The quantum states of these unknown quantum bits for PQKD change with the time sequences of various events (*e.g.* sending, transmitting, receiving, restoring, eavesdropping, detecting, etc). These events are some dynamic behaviors which are often expressed as activities.

To describe the control processes of quantum key bit transmissions *via* quantum entangled communication, four relevant dynamic UML diagrams with Rational Rose are designed by resorting to the existing PQKD systems as follows [1-3].

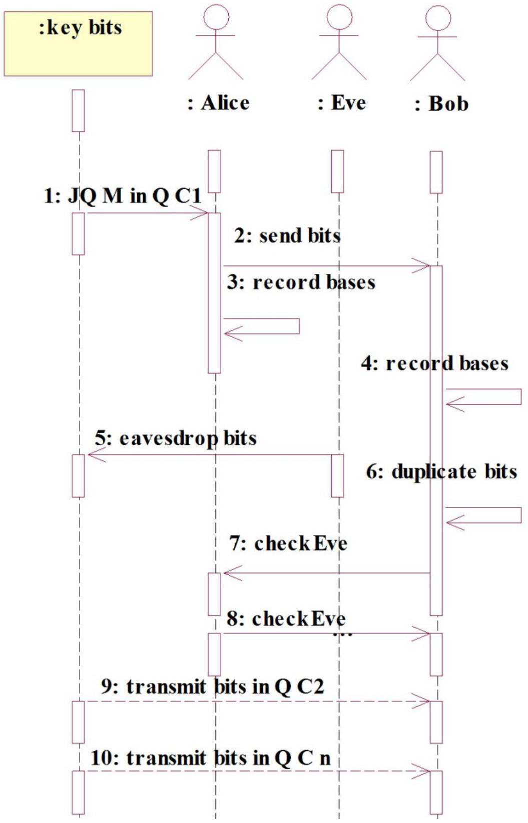


Fig. (2). The sequence diagram of the PQKD system.

Firstly, the sequence diagram of the PQKD system. The message sequences of unknown quantum states for the keys of the PQKD system among Alice and Bob are sorted to represent their dynamic collaboration relations during the information transmissions of unknown quantum bits. Alice, Bob and Eve are considered as the actors to deal with the operated objects that are the carriers of the quantum bits in quantum channels for quantum key information. When a UML use case to transmit quantum key is performed in each quantum channel, the quantum operation triggers the events of quantum entanglement state changes according to the message in this sequence diagram. These events in the parallel quantum channels occur with a certain probability according to the time sequences, and the messages of the events using UML are denoted as Arabic numbers in Fig. (**2**).

Secondly, the collaboration diagram of the PQKD system. The sequence diagram can describe the concerned sorted events of unknown quantum bits through parallel quantum key transmission with typical channel. However, it becomes a big trouble to represent the clear structural relationships among Alice, Bob and Eve in the parallel entangled quantum channels and the shared classical channel.

The necessary orders of these actors are important to design this control system. So, a UML collaboration diagram is devised for the PQKD system as Fig. (**3**). Alice, Bob and Eve are also considered as the actors of quantum operations to obtain quantum key bit information. The labeled arrows denote the quantum message with the changed events during quantum key bits transmissions in parallel.

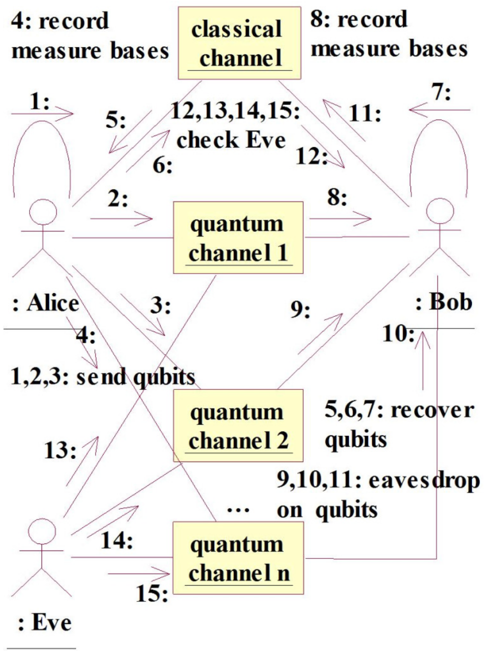


Fig. (3). The collaboration diagram of the PQKD system.

When Alice and Bob want to transmit an unknown quantum state in a certain quantum channel, they also exchange their messages to control measurement bases and quantum states *via* the classical channel for next time.

The transmitting messages are checked to determine if the quantum channels are intercepted by Eve. Meanwhile, Alice and Bob also control the transmission sequences (the numbers) across the parallel quantum channels in Fig. (**3**). Therefore, it is easier to describe the complicate quantum processes of parallel quantum key bits transmissions with the collaboration diagram than that sequence diagram. The dynamic message interaction processes can be demonstrated by sending and receiving unknown quantum bits between Alice and Bob in parallel quantum entangled channels.

Thirdly, the state diagram of the PQKD system. In order to control various states and the state changes of unknown quantum bits among Alice, Bob and Eve, the state diagram is elaborated as Fig. (**4**). Unknown quantum states with key information are treated as the main thread with the changed processes of the initial state, simple state, composite state and end state. Eve's eavesdropping behaviors need to be checked by the changed quantum states when Alice and Bob send and receive the unknown quantum bits.

In the classical channel and parallel quantum channels, there are some conditions for Alice, Bob and Eve to generate and implement various dynamic events. These conditions are the states of unknown quantum bits, such as ready states, transmitted states, duplicated states, negotiated states, eavesdropped sates, rejected states, etc. When the conditions change and cause the sudden state variations of unknown quantum states, Alice and Bob trigger corresponding quantum operations, such as joint measure, key negotiation, eavesdropping detection and quantum states comparison, etc.

Meanwhile, Alice and Bob record the changed quantum entangled states results by quantum measurement bases and initial quantum states, and determine the legal unknown quantum bits of quantum keys by combining the parallel quantum channels with the shared TDM classical channel to carry out the quantum state transitions from the events of the PQKD system with quantum entangled states.

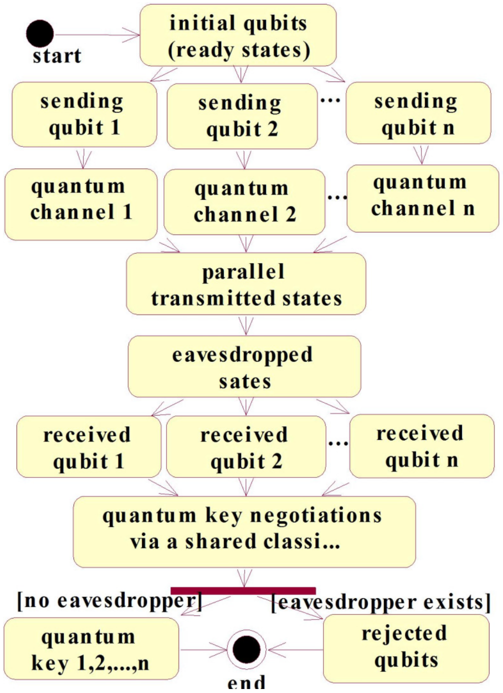


Fig. (4). The state diagram of the PQKD system.

Finally, the activity diagram of the PQKD system. The dynamic processes of PQKD involve in many actions and activities, such as sending, transmitting, measuring and receiving unknown quantum bits with quantum key negotiation (including comparisons of the bilateral measured bases and quantum state result), eavesdropping detection and rejections of unknown quantum bits, etc. Consequently, the UML activity diagram for the PQKD system is conceived to specify the work flows across parallel quantum channels in Fig. (**5**).

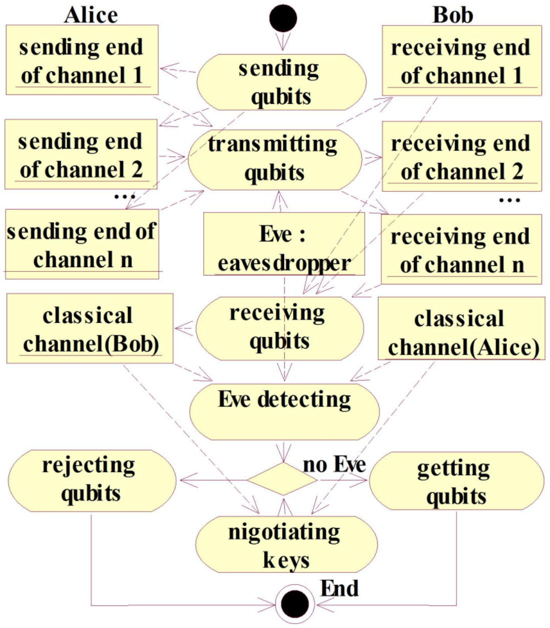


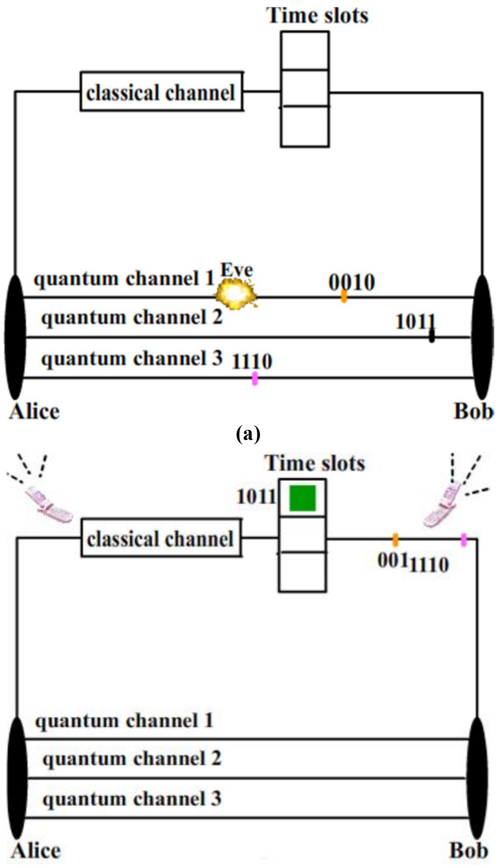
Fig. (5). The activity diagram of the PQKD system.

This UML activity diagram above can distinguish and control the responsibilities (*i.e.* activities) between Alice and Bob. Alice or Bob not only completes the communications in turn from top to bottom, but also they pay attention to the horizontal collaborative work. The orders of these arrows among the activities express the semantic orders of quantum key generation and eavesdropping detection. The dynamic relationships among the diverse activities for quantum keys can be illustrated visually, helping users to understand the exact quantum information changing processes to obtain the effective unknown quantum bits by PQKD control systems.

4. DEMON ANIMATION FOR THE PQKD SYSTEM

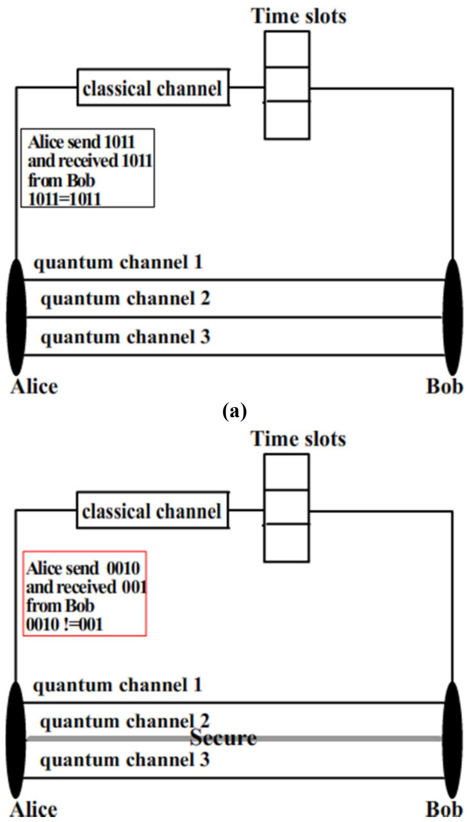
To provide the detailed dynamic process for the PQKD system, three quantum channels are taken as examples to develop the animation software with Flash and Visual Studio according to the these UML sequence diagram, collaboration diagram, state diagram and activity diagram. Some of main software interfaces are shown in Figs. (**6-8**).

Alice sends and transmits three hexadecimal codes (*i.e.* four binary bits) unknown quantum states of quantum keys to Bob. The first quantum channel is supposed to be intercepted by Eve. To negotiate quantum keys, Alice and Bob compare the information of their quantum bits during a time slot in Fig. **6**. They compare their bits and find the errors in the first quantum channel, while the other two quantum channels are secure in Figs. (**7**) and (**8**).



(b)

Fig. (6). The quantum key bits are transmitted *via* parallel quantum channels, and these key bits are controlled by eavesdropping detection with a TMD classical channel.

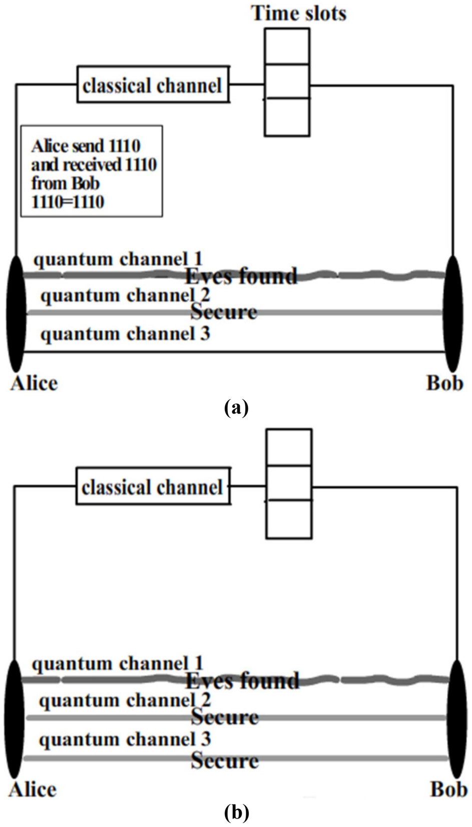


Alice send 1011
and received 1011
from Bob
1011=1011

Alice send 0010
and received 001
from Bob
0010 !=001

(b)

Fig. (7). Identical quantum bits in channel 2 and different quantum bits in channel 1 between Alice and Bob for the PQKD system.



Alice send 1110
and received 1110
from Bob
1110=1110

(b)

Fig. (8). Eve exists in channel 1 for control, and identical bits are in channel 3 with no Eve for the PQKD system.

Using these UML models and the demon animation software to understand the new PQKD system of quantum entanglement states, it is simple and friendly with some characteristics as follows.

(1) The dynamic processes of the PQKD system can be described intuitively, facilitating users to understand the principle of PQKD. In every parallel quantum channel, the software can directly illustrate the bits transmission process of quantum key *via* unknown quantum bits, and the abstract business of PQKD is transformed into the acceptant visual animation, helping us research the intrinsic relationships between the parallel quantum channels and the typical channel. The software can describe clearly the quantum key transmission for parallel quantum key step by step. A series of animations reveal vividly the detailed procedure of quantum state movements. For instance, those chronological orders to send, transmit, receive and compare quantum bits, eavesdropping detection are illustrated to demonstrate the principle of the PQKD system of quantum entangled states with the message sequences from the collaboration relations between Alice and Bob.

(2) The quantum states for the PQKD control system can be encoded and represented as classical binary bits of 0 and 1. Four bits compose a hexadecimal code. It can be seen from this animation software that Alice sends the coded quantum bits 0010, 1011 and 1110 of quantum key to Bob through three independent quantum channels respectively almost in the same time. The traditional channel is divided into three time slots. Each parallel quantum channel is controlled by the corresponding time slot. The quantum bits *via* control are effective for quantum keys if no Eve exists in this quantum channel. Therefore, the UML diagrams and this animation software in our work have favorable effects for intuitive demonstration with deep impression for users.

(3) This PQKD system has unconditional security which can be deduced from this software with our results in Fig. **6**, Alice and Bob can find and control the potential eavesdroppers that hide in parallel quantum channels by comparing their quantum bits and measuring bases *via* the shared classical channels in Fig **1**. The PQKD instance of three quantum channels shows that the eavesdroppers can be checked and controlled in the first channel in Figs. (**6**) and (**7**).

They can also find out the inconsistent quantum bits and determine that only the first quantum channel may be intercepted by Eve. Therefore, Alice and Bob can control the effective unknown quantum bit transmission of PQKD in the second and third secure channels separately. The security of the quantum channels in parallel for quantum private communication is also guaranteed according to Heisenberg's uncertainty principle and the quantum no-cloning principle in quantum mechanics. These data streams of the unknown quantum states for the PQKD system can be implemented and controlled through the parallel quantum channels of no eavesdroppers.

5. CONCLUSION

In this paper, the models of the PQKD control system of quantum entangled states have been constructed with the UML software engineering methods. The corresponding sequence diagram, collaboration diagram, state diagram and activity diagram have been modeled with the tool of IBM Rational Rose. The relevant animation software has been developed according to these UML diagrams. The instance results indicate that this software can help users express and understand more intuitively the dynamic processes and complex principles of the PQKD system with less difficulty than before, which can motivate more initial researchers to focus on the inherent mechanisms of the PQKD system. Analyses show that our PQKD system has unconditional security to transmit unknown quantum bits of keys with the control system methods. With the development of quantum information technology, the PQKD system models using UML are of great importance for the engineering practices and actual applications of larger-capacity and long-distance PQKD in future.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the financial support from the National Natural Science Foundation of China (Grant Nos. 61472094, 61371186) and the Guangxi Natural Science Foundation (No. 2013GXNS FFA019004). We also thank Wei Feng for his help.

REFERENCES

[1] R. A. Antonio, M. José, A. Waldimar, M. Alfonso, G. M. Víctor, C. David and C. José, “Microwave photonics parallel quantum key Distribution,” *IEEE Photo. J.*, vol. 4, pp. 931-942, 2012.

[2] G. H. Zhao, S. H. Zhao, Z. S. Yao, W. Meng, X. Wang, Z. H. Zhu, and F. Liu, “Forward spectral filtering parallel quantum key distribution system,” *Opt. Commun.*, vol. 298, pp. 254-259, 2013.

[3] J. Fang, P. Huang, G. H. Zeng, “Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation,” *Phys. Rev. A*, vol. 89, pp. 022315, 2014.

[4] L. H. Gong, Y. Liu and N. R. Zhou, “Novel quantum virtual private network scheme for PON *via* quantum secure direct communication,” *Int. J. Theor. Phys.*, vol. 52, pp. 3260–3268, 2013.

[5] J. Yin, J. G. Ren, H. Lu, Yuan Cao, Hai-Lin Yong, Y. Wu, C. Liu, S. Liao, F. Zhou, Y. Jiang, X. Cai, P. Xu, G. Pan, J. Jia, Y. Huang, H. Yin, J. Wang, Y. Chen, C. Peng, J. Pan “Quantum teleportation and entanglement distribution over 100-kilometre free-space channels,” *Nature*, vol. 488, pp. 185-188, 2012.

[6] X. S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, A. Zeilinger, “Quantum teleportation over 143 kilometres using active feed-forward,” *Nature*, vol. 489, pp. 269-273, 2012.

[7] N. R. Zhou, L. J. Wang, L. H. Gong, X. W. Zuo, and Y. Liu, “Quantum deterministic key distribution protocols based on teleportation and entanglement swapping,” *Opt. Commun.*, vol. 284, pp. 4836-4842, 2011.

[8] H. L. Xiao, S. Ouyang, and Z. P. Nie, “Capacity of multiple-input-multiple-output quantum key distribution channels”, *Acta Phys. Sin*, vol. 58, no. 10, pp. 6779-6785, 2009.

[9] H. L. Xiao and S. Ouyang, “Capacity of multiple-input multiple-output quantum depolarizing channels”, *J. Appl. Phys.*, vol. 112, pp. 034903 -1-5, 2012.

[10] R. H. Shi, J. J. Shi, Y. Guo, X. Q. Peng, and M.H. Lee, “Quantum MIMO communication scheme based on quantum teleportation with triplet states”, *Int. J. Theor. Phys.*, vol. 50, pp. 2334-2346, 2011.

Received: September 22, 2014 Revised: November 30, 2014 Accepted: December 02, 2014